Understanding Quantum Technologies

Ninth edition – 2026

Part 4/5 – Communications and sensing

Olivier Ezratty

le lab quantique

le lab quantique

Le Lab Quantique is a supporter and promoter of this book, but not its publisher or editor.

Understanding Quantum Technologies

Ninth edition - 2026 - Version 9.0

Part 4/5 – Communications and sensing

Olivier Ezratty

Generated on September 28, 2026

About the author

Olivier Ezratty 0000-0003-3944-2896 olivier (at) oezratty.net
www.oezratty.net, @olivez
+33 6 67 37 92 41

Olivier Ezratty is an author, academic, teacher and advisor on quantum technologies. He started this endeavour in 2018.

He is the author of the reference book "Understanding Quantum Technologies" (September 2021, 2022, 2023, 2024, 2025 and 2026) following three previous editions in French in 2018, 2019 and 2020. The 2025 edition is also available in paperback version on Amazon. This 2026 edition's Amazon print version will be available before the end of 2026.

Since 2021, he has been teaching quantum technologies at EPITA, an IT engineering school in France, at Ecole Normale Supérieure Paris-Saclay since 2024 and CentraleSupelec since 2005. He's affiliated with the EPITA Research lab for his various research writings.

He is a cofounder of the Quantum Energy Initiative in 2022 with Alexia Auffèves (CNRS MajuLab Singapore), Robert Whitney (CNRS LPMMC) and Janine Splettstoesser (Chalmers University, Sweden), and member of its scientific board.

He acts as an independent expert for Bpifrance and at the Agence Nationale de Recherche (ANR) to evaluate quantum R&D projects, as a member of the European Quantum Computing Advisory Board (Q-CAB) since April 2026, and of the Inria expert group for the selection of risky research projects (Programme PIQ) since June 2024.

Since 2018, he has spoken in a large number of quantum technology events such as the Q2B Paris and Santa Clara organized by QC Ware, France Quantum, Lindau Nobel Laureate meeting, DPG, Q-Expo and other events, on top of presentations at Société Générale, BNPParibas, Crédit Agricole, Michelin, Adéo, L'Oréal, FIECC, IHEDN, Business France, CentraleSupelec, Avolta Partners, IHEDN, etc.

He coproduces two series of podcasts on quantum technologies along with Fanny Bouton (in French): a monthly "Quantum " on tech news (since September 2019) and Decode Quantum (2020-2026), with entrepreneurs and researchers, with a total of about 170 episodes as of September 2026.

He also lectures or lectured in various universities such as CentraleSupelec, ENSTA, Telecom Paristech, Les Gobelins, HEC, Neoma Rouen and SciencePo, on artificial intelligence, entrepreneurship and product management (until 2020) and on quantum technologies (since 2018), in French and English as needed. He is also the author of many open-source ebooks in French on entrepreneurship (2006-2019), the CES of Las Vegas yearly report (2006-2020) and on artificial intelligence (2016-2021).

Beforehand, Olivier Ezratty was specialized in many other topics since 2005, like digital television, internet of things and artificial intelligence. As such, he carried out various strategic advisory missions, conferences, or training assignments in different verticals and domains such as media and telecoms, finance and insurance, industry and services and the public sector.

Olivier Ezratty started in 1985 at Sogitec, a subsidiary of the Dassault group, where he was successively Software Engineer, then Head of the Research Department in the Communication Division. He initiated developments under Windows 1.0 in the field of editorial computing as well as on SGML, the ancestor of HTML and XML. Joining Microsoft France in 1990, he gained an extensive experience in many areas of the marketing mix: products, channels, markets and communication. He launched in France the first version of Visual Basic in 1991 and Windows NT in 1993. In 1998, he became Marketing and Communication Director of Microsoft France and in 2001, of the Developer Division, which he created in France to launch the .NET platform and promote it to developers, higher education and research, as well as to startups. Olivier Ezratty is a software engineer from Centrale Paris (1985), which became CentraleSupelec in 2015.

Cover illustration credits: personal creation associating a Bloch sphere describing a qubit and the symbol of peace (my creation, first published in 2018) above a long list of terms from the book glossary. This book contains about 1,325 illustrations. I have managed to give credit to their creators as much as possible. Most sources are credited in the captions. Only scientists' portraits are not credited since it's quite hard to track their original source. I have added my own credit in most of the illustrations I have created or modified. In some cases, I have redrawn some third-party illustrations to create clean vector versions or used existing third-party illustrations and added my own text comments. The originals are still credited in that case.

Table of contents

Table of contents iii

Foreword iv

Contents vi

1 Quantum communications and cryptography 1

1.1 Quantum computing threats 2
1.1.1 Public key cryptography 2
1.1.2 Shor's phantom menace 4
1.1.3 Grover, Dlog and Simon threats 5
1.1.4 Threat assessments 6
1.1.5 Mosca's inequality 7
1.1.6 Classical and quantum cryptanalysis records 8
1.1.7 Quantum cryptanalysis resource estimates 10
1.1.8 Blockchain and Cryptocurrencies vulnerabilities 13
1.1.9 Bibliography and notes 16
1.2 Post-quantum cryptography 20
1.2.1 PQC timeline 20
1.2.2 PQC protocols 23
1.2.3 PQC and blockchains 27
1.2.4 Commercial offering 28
1.2.5 PQC energy consumption 28
1.2.6 Bibliography and notes 29
1.3 Quantum Random Number Generators 31
1.3.1 Randomness and non-determinism 31
1.3.2 QRNG principles and methods 31
1.3.3 Figures of merit 34
1.3.4 Vendors 36
1.3.5 Use cases 38
1.3.6 Bibliography and notes 39
1.4 Quantum Key Distribution 42
1.4.1 QKD principles 42
1.4.2 QKD experiments and deployments 47
1.4.3 QKD by satellite 51
1.4.4 QKD by UAVs 55
1.4.5 Underwater QKD 55
1.4.6 QKD photon sources 55
1.4.7 QKD photon detectors 58
1.4.8 QKD nodes and repeaters 59
1.4.9 Securing QKD 61
1.4.10 QKD and the Blockchain 62
1.4.11 QKD over 5G 63
1.4.12 Market and standards 63
1.4.13 Bibliography and notes 64
1.5 Quantum telecommunications 76
1.5.1 Distributed quantum computing 76
1.5.2 Superconducting qubits interconnect 80
1.5.3 Optical interconnect 82
1.5.4 Electrons and ions shuttling 85
1.5.5 Architecture and infrastructures 86
1.5.6 Other use cases 89
1.5.7 QPU interconnect vendors 90
1.5.8 Bibliography and notes 95
1.6 Quantum Physical Unclonable Functions 105
1.6.1 Bibliography and notes 107
1.7 QKD and PQC vendors 108
1.7.1 Bibliography and notes 127
1.8 Quantum telecommunications and cryptography key takeaways 130

2 Quantum sensing 131

2.1 Quantum sensing use-cases and market .. 131
2.2 International System of Measurement 131
2.3 Quantum sensing taxonomy 133
2.4 Quantum gravimeters, gyroscopes and accelerometers 137
2.4.1 Quantum gravimeters 137
2.4.2 Quantum gradiometry 138
2.4.3 Quantum inertial sensors 138
2.4.4 Quantum rotation sensing 139
2.4.5 Vendors 139
2.5 Quantum clocks 143
2.5.1 Science 143
2.5.2 Vendors 147
2.6 Quantum magnetometers 149
2.6.1 Science 149
2.6.2 Vendors 152
2.7 Quantum electric field sensing 155
2.8 Quantum RF sensing 155
2.8.1 Science 155
2.8.2 Vendors 157
2.9 Quantum imaging 158
2.9.1 Science 158
2.9.2 NV centers imagers 161
2.9.3 OPMs 163
2.9.4 Quantum photometry 165
2.9.5 Ghost imaging 165
2.9.6 Vendors 167
2.10 Distance measurement 170
2.11 Quantum radars and LiDARs 171
2.12 Quantum thermometers 174
2.12.1 Science 174
2.12.2 Vendors 175
2.13 Quantum chemical sensors 175
2.13.1 Science 175
2.13.2 Vendors 175
2.14 Quantum pressure sensors 176
2.15 Quantum NEMS and MEMS 177
2.16 Dark matter sensing 177
2.16.1 Ultralight bosonic dark matter 178
2.16.2 Dark photons 181
2.16.3 Weakly Interacting Massive Particles 181
2.16.4 Dark energy detection 182
2.17 Quantum sensing key takeaways 185
2.18 Bibliography and notes 186

Foreword

The birth of the second quantum revolution may be reasonably settled to 1982, with two celebrated articles: "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers" by Alain Aspect and colleagues, and the famous theoretical paper "Simulating Physics with Computers" by Richard Feynman. They were quickly followed in 1985 by David Deutsch's "Quantum theory, the Church–Turing principle and the universal quantum computer", providing the birth certificate of what is known now as quantum computing. Incidentally, I got a position at CNRS also in 1982, a good spot to witness these developments. However these subjects, including the surprising quantum key distribution scheme proposed by Charlie Bennett and Gilles Brassard in 1984, were still quite confidential at that time. It took ten more years for the topic to attract broad international attention, with the articles "Algorithms for quantum computation: Discrete logarithms and factoring" (1994) and "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", both by Peter Shor.

This started an explosive development, which has not stopped since then. The big impact of Shor's algorithm is that it may break cryptographic codes that were considered fully secure at that time, and are still broadly used on internet - so each layman gets concerned. This, and other reasons, triggered a huge international effort to build a quantum computer. Since it was clear that such a computer was still far away, this effort was mostly academic during the next 20 years. But another earthquake happened in 2014, when large US companies, Google and IBM as the most visible ones, decided to get into the race. They set up heavily funded research programs, focused on a specific technology, superconducting quantum bits. This move stimulated a high level of private investment, leading to the creation of a flurry of dedicated companies, initially startups, but then quite respectable enterprises in terms of funding. They were not limited to superconductors, but included all quantum objects likely to become a quantum bit, a qubit : ions, atoms, photons, and even more exotic ones. One must honestly say that, from this time, the language used in this research field changed significantly: the way to speak with investors is not the same as the way to publish articles in reputable scientific journals. The result was a mixture of authentic scientific and technological progress, coming together with hype and overselling. This may be seen either as an unavoidable evil, or as the appropriate way to communicate in an extremely competitive high-tech environment.

A good example is the way to name the "ultimate goal", the point where a quantum computer can really achieve a useful task that no classical computer can do in any reasonable time. The first name that popped up was "quantum supremacy", but it did not make it, both for technical and political reasons. The next one was "quantum advantage", more politically correct, but still difficult to warrant. The next one is "quantum utility", clearly more modest, but more likely to be reached in a reasonable time span. In the current language, "utility" is used as a step towards "advantage", with some possible oscillations between the two due to progress in classical computing.

Then a question arises : given the very fast progress of the devices, their technical complexity, and the strange mixture of science and publicity used by companies to communicate their results, how to find one's way in the jungle, without getting lost or eaten ? One would need somebody with good scientific and technological knowledge, but also a huge talent for global accounts, given the many facets of these developments, involving physics, hardware, software, middleware, logistics, and finance. We are lucky enough that this person exists, his name is Olivier Ezratty, and you hold his book in your hands or on your computer screen. This is not a modest enterprise, and ≈1,822 pages carefully written in LaTeX is a minimal container. Go for it, it's free ! But how to approach such a monument ? Fortunately there is a reading guide in the first pages, able to orient you depending on your background and interests. It includes also an illustrated "Pandora's box", listing the main high level topics (physics, mathematics, human sciences, engineering, computer science, geopolitics), together with their inner content, opening doors towards many stimulating questions for science, technology, and society.

So where do we stand now, already 44 years after the baby was born ? The general idea is that the real stuff, the one needed for supremacy / advantage / utility for practical problems of industrial interest, requires what is called now "Fault Tolerant Quantum Computing" (FTQC), in the line of Deutsch's ideas; this is quite attractive for computer scientists, but very hard to achieve. Physicists tend to prefer quantum simulators, in line with Feynman's ideas, potentially useful for more fundamental physics problems. Myself, as a physicist, will go for the second trail, because one should not dismiss fundamental physics problems: it is by solving them that science made progress, and not necessarily by jumping right now into the market. Actually, it is not clear that all fundamental questions to be answered before being able to implement quantum computing have been solved, as summarized in the old joke : "Where is quantum computing? Somewhere between cold fusion and hot fusion", a physicist's warning that nature's laws are not to be fooled around.

Anyway, as we say in French, "*on ne discute pas des goûts et des couleurs*" (there's no accounting for tastes): whatever your personal interest is - physicist, computer scientist, or investor -, and wherever you may want to look at - computing, communications, sensors or metrology - the development of quantum technologies is a fascinating arena where much more is expected to come.

I cannot close this foreword without a few words about another ongoing revolution, artificial intelligence and large language models generative artificial intelligence (simplified as "LLM"). The most straightforward step forward, taking place currently in all domains of scientific and technical activities, is to use LLM as super-efficient assisting tools; their progress during the 2 or 3 last years has been astonishing, and it cannot be listed here. Another more speculative idea is to think about a "quantum AI", an AI running on a quantum computer. The mismatch between the current performances of quantum computers, and what is used now on supercomputers running AI, makes this objective extremely far-fetched. Still, blue-sky thinking about what might be achieved by such machines - and even the question of whether they will still be "machines", is attracting attention by some quantum theoreticians. Where will these revolutions lead humanity ? Only time will tell.

Philippe Grangier

Director of Research emeritus at CNRS, Institut d'Optique Graduate School (IOGS), and incoming President of the French Optical Society (SFO).

September 2026

Contents

This is **Part 4/5 – Communications and sensing** of the book "Understanding Quantum Technologies 2026", which is also downloadable using this link.

The downloadable PDFs are available in a single A4 and Letter version, containing the five parts in sequential order. You can also download compressed PDFs for the five parts in A4 and Letter formats. Their size fits the constraints of ebook readers like the Kindle from Amazon.

The e-reader and printed version of the book separates parts 1, 2, 3, 4 and 5.

- The **first part** contains a history of quantum physics, some quantum physics 101 and everything about quantum computing basics and engineering including quantum error correction, the energetics of quantum computing, a view on pessimism and optimism with regard to the advent of scalable and useful quantum computers, as well as some economic considerations.
- This **second part** contains the sections dedicated to quantum computing hardware with all types of qubits and their related industry vendors, enabling technologies, and unconventional computing solutions which are potential alternate routes between classical and quantum computing.
- The **third part** contains the sections dedicated to algorithms, software tools, and applications across multiple markets. It also contains an inventory of quantum computing software and service vendors.
- The **fourth part** covers quantum communications, quantum cryptography, post-quantum cryptography and quantum sensing.
- The **fifth part** describes the quantum ecosystem at the entrepreneurial level, the country level, on various societal topics, corporate adoption methodologies, quantum pseudosciences. It ends with a glossary, and book bibliography.

The book is split into five parts to make its printing easier, some online printing services including Amazon being limited to a maximum of 600 pages.

You can order the printed version of this book in five parts on all Amazon sites by searching for the book title, edition 2026, when it is released around October-November 2026.

1 Quantum communications and cryptography

Quantum telecommunications cover a wide spectrum of use cases including quantum communications between quantum sensors, quantum computers and quantum key distribution used in cryptography (Figure 1). Most of these technologies are using photon entanglement and quantum teleportation resources. The field started to develop experimentally and industrially with quantum cryptography, particularly quantum key distribution (QKD). It is already being deployed experimentally or on a large scale like in China, while quantum telecommunications associated with quantum computers are still in their infancy. In this part we describe three other related technologies: quantum random number generators, (classical) post-quantum cryptography that protects classical computers against the potential threats coming from future quantum computers and also quantum product unique identifiers, which is a class of technologies in itself, mixing classical and quantum artifacts to uniquely identify real-life objects.

The creation of Shor's integer factoring and discrete logarithm algorithms in 1994 triggered the interest in quantum cryptography (using various quantum effects like measurement randomness and/or entanglement as resources to generate identical secured encryption keys between two communication endpoints) as well as in post-quantum cryptography (classical cryptography using techniques that are resilient to attacks by quantum computers). Shor's algorithms theoretically enable the cryptanalysis of asymmetric public keys on a quantum computer in a reasonable amount of time, provided large scale quantum computers are available. These algorithms have been shaking the cybersecurity ecosystem since the advent of the first programmable quantum processors in the early 2000s and related scale-up promises and forecasts. It would make it possible to break many public key cryptography systems that are commonly used on the Internet, particularly those that are based on RSA. It is still highly hypothetical since quantum computers capable of executing Shor's algorithms for breaking RSA-2048 keys require millions of high-fidelity qubits that are quite far in the distant future at best.

Once they are aware of the threat, however, governments, counterintelligence, intelligence and sensitive industries become seriously concerned or at least interested. The threat of quantum computing to cybersecurity even touches critical parts of the Bitcoin and Blockchain signatures and some proof of work protocols. Even though the threat is quite remote, the readiness inertia to counter this potential quantum threat means, for some, that it is necessary to launch it now.

Even before Shor's phantom menace materializes, the cyber security industry started to prepare countermeasures. The markets affected first will be the IT and telecommunications industry in general, which will have to update many software and hardware offerings, financial institutions, the energy sector, healthcare, and government utilities and the military.

In this part, we will investigate the following domains:

- The basic principles of classical cryptography, in particular **public key cryptography,** with the example of RSA public keys. Classical cryptography involves mathematical concepts that are not always obvious. I share with you here what I have been able to understand about it and make it as accessible as possible.
- The **nature of the threats** coming from integer factoring and other quantum algorithms and the cryptographic systems involved. We will provide resource estimates on the required quantum computers to realize this threat.
- **Post-Quantum Cryptography** that is used to distribute public encryption keys using classical computation that is resilient to codebreaking from future quantum computers.
- **Quantum random number generators** which are a useful complement to classical cryptographic solutions as well as to quantum cryptography.
- **Quantum Key Distribution** based systems that secure the physical part of communications for the safe distribution of quantumly random symmetric keys.
- **Quantum telecommunications** applications, outside of those related to cryptography, and in particular for the creation of distributed quantum computing systems, *aka* "QPU interconnect" and distributed quantum computing solutions.
- **Quantum Physical Unclonable Functions** which sit between QRNG, embedded systems and cryptography to securely identify any sort of classical physical device, including a quantum computer.
- **Vendors** in the PQC and QKD domains around the world, in a market that already includes many players and startups. QRNG, QPUF and quantum interconnect vendors are spread in the related subsections.

1.1 Quantum computing threats

1.1.1 Public key cryptography

Cryptology is the science of secrets. It allows the transmission of sensitive information between a transmitter and a receiver in a secure manner. Cryptology includes cryptography, which secures transmitted and stored information, and cryptanalysis, which seeks to decrypt it by attack, or code breaking.

In asymmetric public-key cryptography, a public key is distributed while the corresponding private key remains secret. Depending on the scheme, the public key can be used for encryption or signature verification, while the private key can be used for decryption or signature generation. Public-key cryptanalysis does not necessarily consist only of recovering the private key. An attack may instead recover plaintexts, forge signatures, or otherwise defeat a security property.

Cryptography secures transmitted information in several ways:

- **Confidentiality**: only the recipient can retrieve the unencrypted version of the transmitted information.
- **Integrity**: the information has not been modified during its transmission.
- **Authentication**: the sender and receiver are who they claim to be.
- **Non-repudiation**: the issuer cannot deny having transmitted the encrypted information.
- **Access control**: only persons authorized by the issuer and the recipient can access unencrypted information.

Before computer telecommunications, confidentiality was ensured by the knowledge of a common secret between transmitters and receivers, the encryption and decryption codes, which could be the position of the wheels of a German Enigma machine during World War II. This worked in closed environments such as for military communications or between embassies and their home countries.

With Internet communications, relying only on pre-shared secrets does not scale well to large open networks. Public-key cryptography made scalable authentication and key establishment possible without requiring every pair of users to share a secret beforehand. Symmetric cryptography nevertheless remains the usual mechanism for bulk data encryption because it is much more computationally efficient.

Modern secure protocols therefore combine asymmetric and symmetric cryptography. For example, TLS uses public-key mechanisms for authentication and key establishment, then uses symmetric authenticated encryption for the application data. Messaging protocols similarly combine public-key or hybrid key-establishment mechanisms with symmetric encryption. The exact algorithms evolve over time, so it is safer not to associate a messaging application permanently with one specific cipher suite.

In a public-key encryption scheme, the receiver can publish an encryption key while keeping the corresponding private key secret. The sender encrypts using the public key and the receiver decrypts using the private key. A **PKI**, or Public Key Infrastructure, is a broader trust infrastructure using certificates, certification authorities, revocation mechanisms, and related procedures to bind public keys to identities. A public-key cryptosystem by itself is therefore not a PKI.

The **RSA** public-key cryptosystem was introduced by **Ron Rivest**, **Adi Shamir**, and **Leonard Adleman** in 1977 and published in 1978.

RSA key generation starts by choosing two large random prime numbers p and q. Their product $N = pq$ is the public modulus. RSA-2048 uses a 2,048-bit modulus and is commonly associated with about 112 bits of classical security, while RSA-3072 is associated with about 128 bits of classical security.

We then compute Euler's totient $\varphi(N) = (p-1)(q-1)$, which counts the integers between 1 and N that are coprime with N, not the prime integers below N. The public exponent e is chosen such that $\gcd(e, \varphi(N)) = 1$. It does not have to be prime, although the prime value 65,537 is commonly used. The private exponent d is the modular inverse of e, so that $ed \equiv 1 \pmod{\varphi(N)}$, or equivalently modulo Carmichael's function $\lambda(N)$ in common RSA constructions. The public key contains (N, e) and the private key contains d together with parameters derived from p and q.

RSA correctness follows from elementary number theory, in particular Euler's theorem or the corresponding result using Carmichael's function. The public and private exponents are modular inverses in the relevant exponent group.

Anyone can use the public key to perform the public operation. Only a holder of the private key should be able to efficiently perform the corresponding private operation under the assumed hardness of factoring and under the security assumptions of the complete RSA padding or signature scheme.

An attacker who factors the public modulus N into p and q can compute $\varphi(N)$ or $\lambda(N)$ and then recover the private exponent d from the public exponent e. This is why large-integer factorization is the mathematical problem targeted by Shor's RSA attack.

In the symmetric-key realm, AES has been standardized since 2001 and supports 128, 192, and 256-bit keys. Symmetric keys must be established securely between the communicating parties, but the key-establishment channel or time can be different from the subsequent encrypted-data transmission.

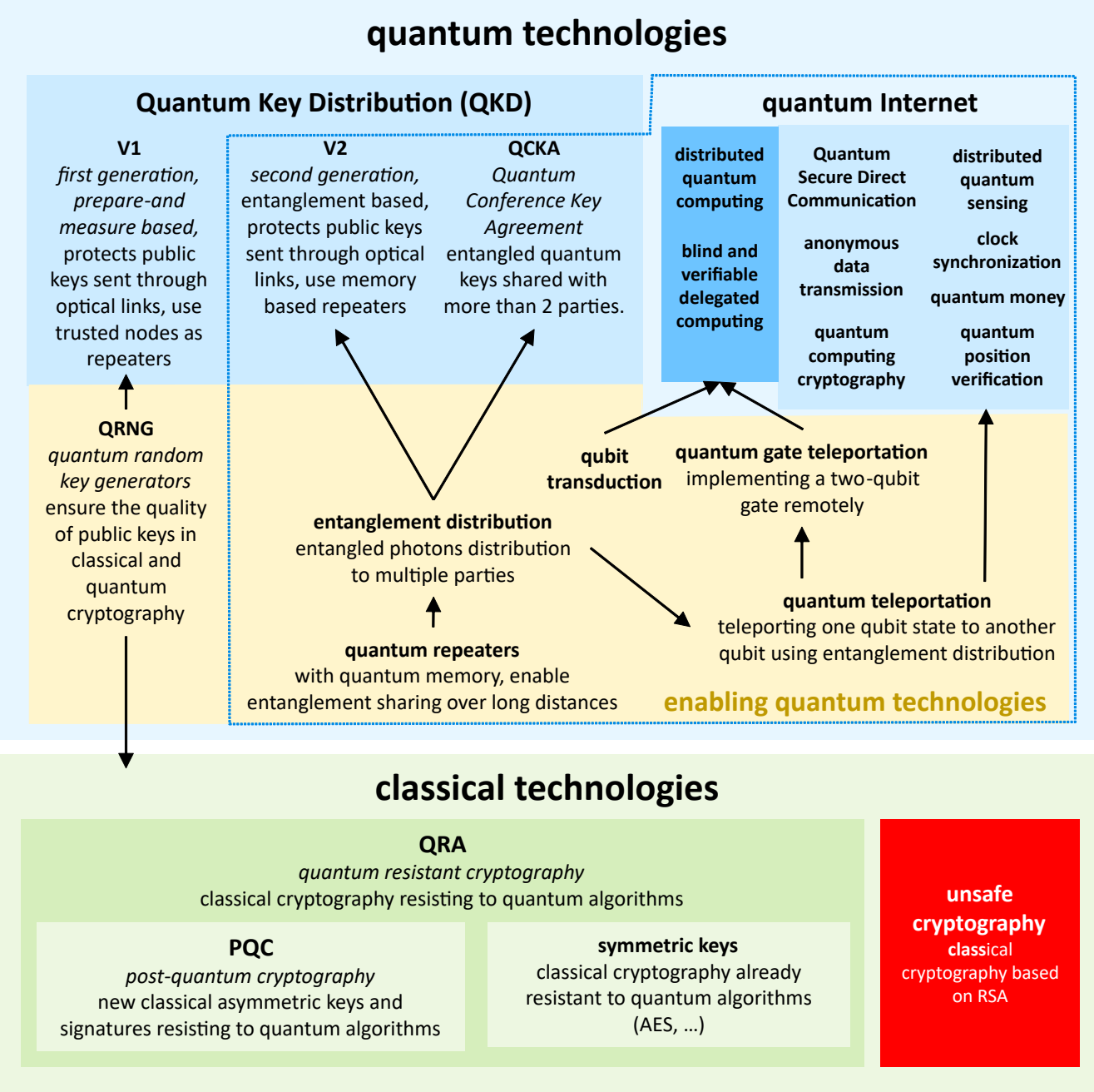


Figure 1: The various types of technologies covered in this section and their relationship. © Olivier Ezratty, 2023-2024. Inspired by [1].

The **one-time pad** provides information-theoretic perfect secrecy when the key is uniformly random, independent of the plain text, at least as long as the message is kept secret and never reused. Its main practical difficulty is therefore the generation, distribution, storage, and one-time use of a key as long as the protected data.

Assessing cryptanalysis threats for any deployed cryptography solution has always been critical. Classical cryptanalysis is one of the threats to the security of government, public services, businesses and consumers digital assets, on top of viruses, phishing, other social engineering tricks and various physical attacks. The looming threat of quantum computers adds to this already busy mix.

The diagram in Figure 3 points out the main encryption algorithms vulnerable or not to known quantum algorithms [2].

Broadly speaking, public-key systems based on integer factorization or discrete logarithms, such as RSA, finite-field Diffie-Hellman and DSA, and elliptic-curve schemes, are vulnerable to sufficiently large fault-tolerant quantum computers running Shor's algorithms. Symmetric ciphers and hash functions are not broken by Shor's algorithm and retain substantial security against known quantum attacks. Post-quantum cryptography is de-

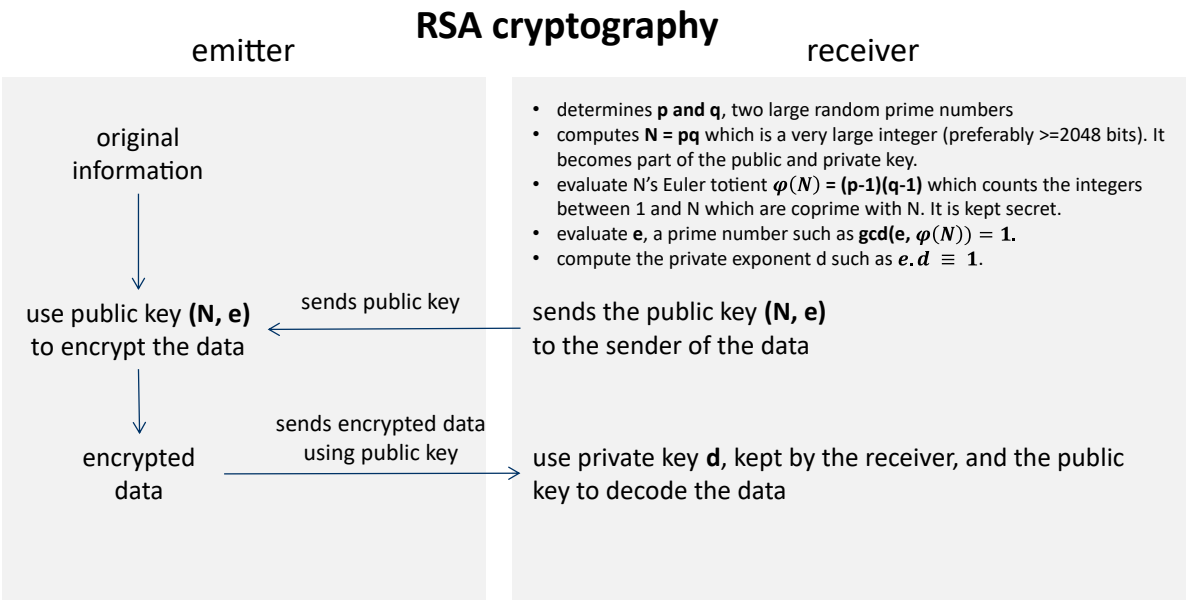


Figure 2: Description of the RSA key generation process. © Olivier Ezratty, 2022-September 2026.

signed to resist known classical and quantum attacks, although individual candidates can fail. A prominent example is SIDH/SIKE, which was broken classically during the NIST process [3]. NIST standardized ML-KEM, ML-DSA, and the hash-based SLH-DSA in 2024, illustrating that "PQC" is a family of encryption schemes rather than a guarantee attached to every candidate.

One reason to worry is that today's sensitive communications can be stored for a long time by private or state hackers, and exploited much later, when quantum computers are up to the task. This attack is nicknamed **Store Now, Decrypt Later** (SNDL) as well as Harvest Now Decrypt Later (HNDL). Some present day information may have some value later, whether it is financial transactions, private communications, healthcare records, trade secrets, diplomatic, military and various other state secrets.

Forward secrecy in protocols such as modern TLS prevents later compromise of a long-term classical private key from automatically exposing earlier session keys. It does not by itself protect a captured handshake against a future quantum attacker if the ephemeral key agreement used for that session is itself vulnerable to Shor's discrete-logarithm algorithm. This is one motivation for deploying post-quantum or hybrid key establishment before a cryptographically relevant quantum computer exists. The hardware timeline remains uncertain.

1.1.2 Shor's phantom menace

Peter Shor's 1994 factoring algorithm sparked major interest in quantum computing before programmable gate-based qubits existed. The important complexity result is that integer factorization and discrete logarithms can be solved by randomized quantum algorithms in a number of elementary steps that is **polynomial** in the input bit length, not linear in the number of key bits [4, 5]. By contrast, the best known general classical factoring algorithm, the General Number Field Sieve, has subexponential asymptotic complexity.

A sufficiently large FTQC system running Shor's integer factoring and discrete log algorithms would threaten RSA signatures and legacy RSA key transport, finite-field Diffie-Hellman and DSA, and ECDH and ECDSA. These primitives have historically been used in TLS, IPsec/IKE, SSH, PGP and S/MIME, VPNs, software signing, payment systems, and many hardware security modules. TLS 1.3 no longer supports RSA key exchange, although RSA signatures remain possible. Plain FTP is not encrypted, while FTPS protects FTP with TLS. It also can threaten automotive ECU (Electronic Control Unit) [6].

The quantum threat also concerns **digital signatures**, software-update authentication, **VPNs**, email security with **S/MIME**, online payment systems, and public-key primitives such as **ECDH** and **ECDSA**. **3-DES** is a legacy symmetric block cipher, not an elliptic-curve scheme, and its weaknesses are unrelated to Shor's discrete-logarithm algorithm.

Protocols in the Signal family historically relied heavily on elliptic-curve cryptography, but this is also an example of active migration toward hybrid post-quantum protection. The broader point remains that Internet security depends on several layers of cryptographic primitives, and the vulnerable public-key components must be replaced or hybridized.

Elliptic Curve Cryptography (ECC) was independently proposed in 1985 by Neal Koblitz and Victor Miller (Figure 5). Common applications include **ECDH** for key agreement and **ECDSA** for digital signatures. ECDSA was standardized in the 1990s, not launched in 2005.

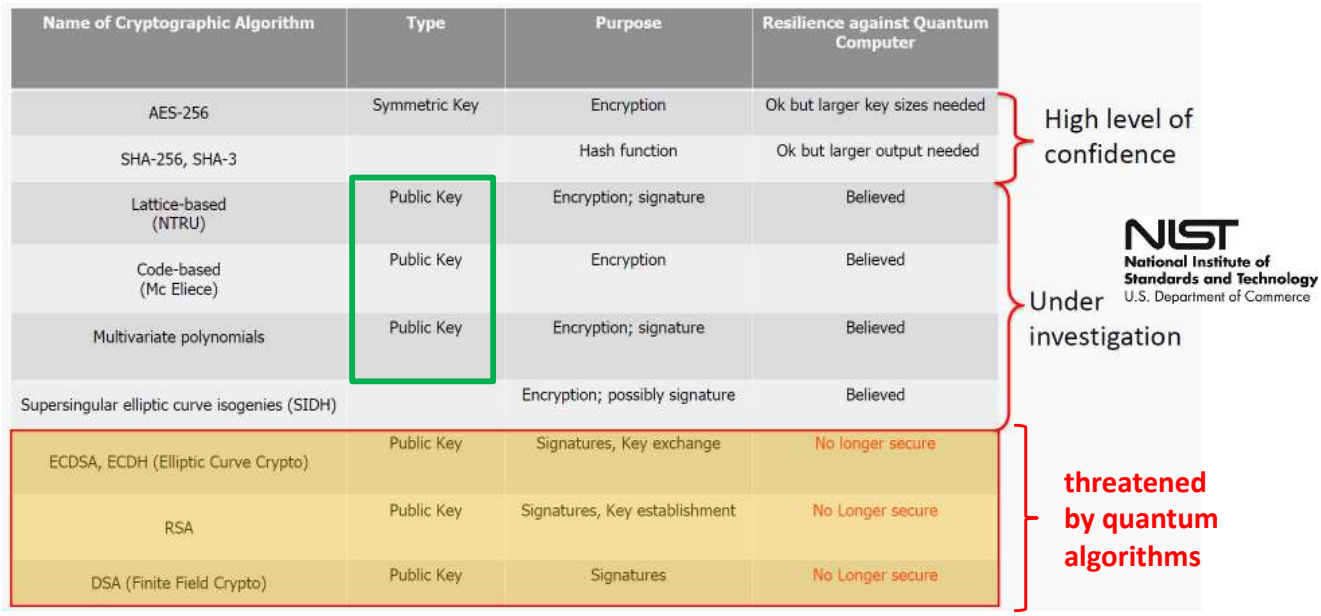


Figure 3: What key generation services are quantum safe or not. Source: NIST.

SNDL from the past

Many historical letters from the past between the 15^{th} and 19^{th} century were encrypted using techniques which are hard to decode even using the best contemporary cryptanalysis techniques. These letters were encrypted with classical ciphers and did not use public cryptographic keys. Renaissance cryptography used a homophonic substitution cipher combined with a nomenclator. Consonants and vowels had multiple ciphertext symbols (*aka* homophones). A private nomenclator supplied tokens for names and words. Vowels following consonants were hidden by using a complex consonant symbol decorated with diacritical marks encoding the ensuing vowel. The table was built with rotated symbol families and a few nulls, which implemented the cipher described in the paper [7, 8].

The letter decryption was based on transcribing the symbols, using frequency and pattern analysis aided by comparative letters to reconstruct the homophonic substitution table and nomenclator, then on applying that key to recover the plaintext.

Thousands of historical encrypted letters remain to be deciphered. Some use substantially stronger schemes than simple substitution ciphers, and difficult historical ciphers may remain unread for a long time. They must not, however, be described as one-time pads unless they actually satisfy the one-time-pad construction and key requirements.

Elliptic-curve cryptography became widely deployed much later than its 1985 proposal. Separately, elliptic curves were central to Andrew Wiles's proof of Fermat's Last Theorem. Wiles announced the proof in 1993, and the corrected proof was published in 1995. This mathematical connection has nothing to do with ECC cryptography itself.

One advantage of elliptic-curve cryptography is that it achieves a given classical security strength with much shorter keys than RSA. It is nevertheless vulnerable in principle to Shor's discrete-logarithm algorithm [9]. In a finite multiplicative group, the discrete-logarithm problem can be written as finding k such that $a^k \equiv b \pmod{p}$. For elliptic curves, the relevant ECDLP is instead to find k such that $Q = kP$ for known curve points P and Q. The controversial **Dual_EC_DRBG** random-number generator was a separate elliptic-curve construction and was not an ECDSA backdoor. After concerns intensified in 2013, NIST recommended against Dual_EC_DRBG in September 2013, removed it from draft guidance in 2014, and formally removed it from the revised recommendation in 2015 [10].

1.1.3 Grover, Dlog and Simon threats

Symmetric cryptography is not affected by Shor's factoring or discrete-logarithm algorithms. DES has a 64-bit key encoding but only 56 effective key bits and is obsolete. AES was standardized in 2001 and supports 128, 192, and 256-bit keys.

For exhaustive key search, Grover's algorithm provides an ideal quadratic reduction in the number of oracle queries, from order 2^k to order $2^{k/2}$ for a k-bit key. This

does not translate directly into a practical quadratic wall-clock speedup because the Grover iterations are largely serial and each quantum oracle is expensive under fault tolerance. NIST consequently considers AES-128 likely to remain secure for decades under known quantum attacks and AES-192 and AES-256 safe for substantially longer, absent new cryptanalytic weaknesses. Concrete resource estimates remain strongly architecture dependent.

Symmetric session keys are often established using public-key **key-agreement** mechanisms. Diffie-Hellman is not encryption. Classical finite-field Diffie-Hellman uses a multiplicative group, while ECDH is its elliptic-curve analogue. Both discrete-logarithm problems are vulnerable to sufficiently large fault-tolerant quantum computers running Shor's algorithm.

A cryptographic hash function maps data of arbitrary length to a fixed-length digest. It is used for integrity checking, digital signatures, password-processing constructions, and many other purposes. A cryptographic digest is not a key, and different inputs can in principle have the same digest because the output space is finite.

SHA denotes several standardized hash-function families. SHA-1 is obsolete because practical classical collision attacks exist. SHA-2, including SHA-256 and SHA-512, and SHA-3 are different modern families.

For an ideal n-bit hash, a generic quantum preimage search with Grover's algorithm takes order $2^{n/2}$ oracle queries, while generic quantum collision algorithms have a different complexity, of order $2^{n/3}$ queries in the standard model. For SHA-256 and SHA3-256, the idealized preimage-query exponent is therefore about 128. Concrete fault-tolerant circuits are much more expensive. One detailed study estimated a SHA-256 preimage circuit with about $2^{12.6}$ logical qubits and depth about $2^{153.8}$ surface-code cycles, and a SHA3-256 circuit with about 2^{20} logical qubits and depth about $2^{146.5}$ cycles [11].

The relevant security parameter for a hash function is its digest length and the attack goal, not a "key size". SHA-2 and SHA-3 both contain variants with several digest lengths. SHA-256 and SHA3-256 both have 256-bit digests, so their ideal generic quantum preimage complexity has the same order 2^{128}. SHA-1 is deprecated because of classical collision attacks, not because it has a uniquely unfavorable relationship with Grover's algorithm.

Shor's discrete-logarithm algorithm threatens DSA, Diffie-Hellman, ElGamal, ECDH, and ECDSA. Garn and Kan studied binary elliptic curves with field sizes from 163 to 571 bits and provided logical and physical resource estimates for both matter-based surface-code architectures and photonic fusion-based active-volume architectures [12].

The report from German's BSI security services which was updated in 2025 shows interesting estimates of the resources needed to break AES and SHA symmetric keys [13].

Simon's algorithm can be used in theoretical attacks on constructions such as Even-Mansour, but the cryptanalytic speedup relies on a strong quantum chosen-query model in which the attacker can query the keyed primitive on a coherent superposition of inputs under the same secret key [14]. A 2026 IBM-hardware demonstration attacked a toy 4-bit Even-Mansour instance [15]. It demonstrates the algorithmic mechanism, not a practical attack on production-size symmetric keys.

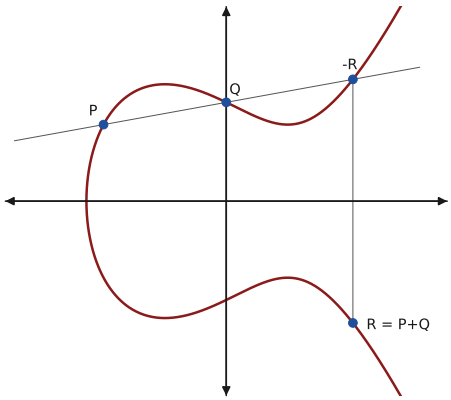


Figure 5: An elliptic curve.

All in all, Shor is not the only quantum threat to cybersecurity (Figure 4)!

1.1.4 Threat assessments

Some historical quantum-cybersecurity forecasts clearly underestimated the hardware difficulty. The ETSI-era chart in Figure 6, for example, should now be read as a historical forecast rather than a current timeline [16]. The lesson is not that quantum cryptanalysis is impossible, but that calendar dates inferred from qubit-count extrapolations are highly model dependent.

Threat assessment should distinguish three aspects: whether a quantum algorithm gives an asymptotic cryptanalytic advantage, what fault-tolerant resources are required to realize that advantage, and how long a PQC migration takes. The last question can justify action well before the hardware is available, particularly for long-lived data exposed to Harvest Now, Decrypt Later attacks.

Several predictions proved to be too aggressive, including claims of a near-term "quantum apocalypse" [17], analogies with a "nuclear threat" [18], and a 2020 prediction that Bitcoin security could be broken by 2022 [19]. Some surveys also mixed physical-qubit and logical-qubit requirements or did not state the hardware assumptions clearly [20]. Such examples show why cryptanalytic resource estimates should always specify logical resources, error-correction overhead, error rates, cycle times, classical reaction times, connectivity, and runtime assumptions.

Peter Shor factoring algorithm - 1994
integer factoring
exponential acceleration
$O(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}) \Rightarrow O((\log N)^2\ (\log log\ N))$
threatens public key-based cybersecurity
RSA, ECDH, ECDSA, SSL/TLS, VPNs (IPsec), SSH, PGP, S/MIME), Signal (WhatsApp), Bitcoin & Blockchain signatures

Lov Grover search algorithm - 1996
brute force to break symmetric codes
polynomial acceleration
$O(N) \Rightarrow O(\sqrt{N})$
threatens symmetric keys cybersecurity
improves brute force attack of hash functions (SHA) and block ciphers (AES) used in symmetric encryption

Peter Shor dlog algorithm - 1994
exponential acceleration
$O(e^{(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}) \Rightarrow O((\log N)^2\ (\log log\ N))$
threatens Digital Signature Algorithm, Diffie-Hellman key exchanges and El-Gamal encryption

David Simon algorithm - 1996
exponential acceleration
$O(2^{N/2}) \Rightarrow O(N)$
threatens Even-Mansour ciphers used in some disk encryptions

Figure 4: Shor's algorithm is not the only quantum algorithm that could threaten existing cybersecurity using symmetric and asymmetric cryptography. © Olivier Ezratty, 2021-September 2026.

A late-2022 X9 Financial Industry Standards report used the concept of a **Cryptographically Relevant Quantum Computer** (CRQC) to discuss when quantum hardware could threaten deployed public-key cryptography. CRQC had already been used in the broader quantum-security literature and policy discussion.

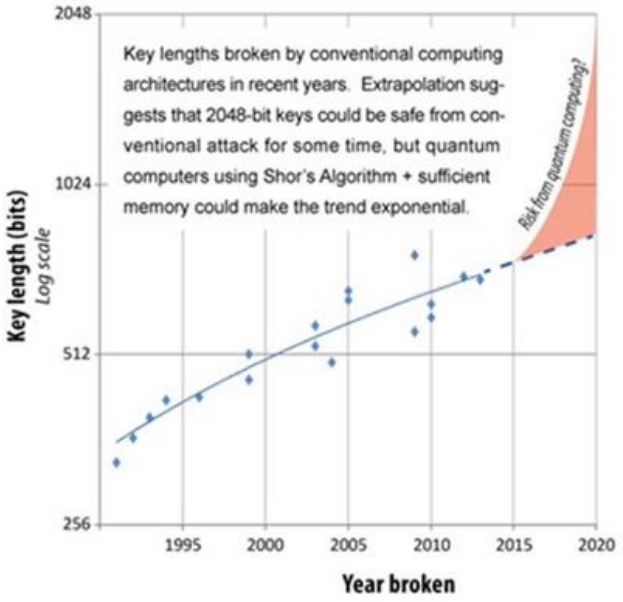


Figure 6: Historical example of an optimistic Shor-related risk forecast. Source: [16].

A Financial Times 2023 demonstration of how a quantum computer works and how it could break an RSA key contained lots of visuals and simplifications [21]. Peter Shor gave his best guess as to when this might happen: "*between 20 and 40 years,*" but he does not rule out the possibility that the physics challenges will prove too hard, and we will never build workable quantum computers. Other threats are supposed to come from AI and quantum AI [22, 23].

Assessments also differ because cybersecurity migration and quantum-hardware forecasting have different risk tolerances. Vendors and consultancies can have commercial incentives around migration services, while quantum-hardware vendors can have incentives around aggressive capability roadmaps. Those incentives are useful context but do not by themselves validate or invalidate a technical estimate. The relevant comparison is between the cryptanalytic resources, the hardware assumptions, the expected lifetime of the protected data, and the migration lead time.

Geopolitical competition between the United States, China, Europe, and other regions also raises the strategic value of conservative migration planning. The absence of a demonstrated CRQC does not remove the migration problem. When the lifetime of sensitive data and the time required to replace cryptographic infrastructure are long, a low-probability future capability can still justify migration. This is the practical logic behind post-quantum transition programs.

There is some disagreement about the urgency and cost of migration, but NIST and NSA guidance is better described as precautionary and deadline-driven than as alarmist. Their policies account for long migration times, cryptographic agility, and Harvest Now, Decrypt Later exposure, not only for a point estimate of CRQC arrival. A separate debate concerns the relative roles of PQC and QKD, which solve different security problems and impose very different deployment constraints [24].

1.1.5 Mosca's inequality

Michele Mosca's inequality expresses the migration timing problem as $D + T > G_c$, where D is the time for which today's protected data must remain secret, T is the time required to migrate the relevant systems to quantum-resistant cryptography, and G_c is the time until a cryptographically relevant quantum computer

can break the currently deployed public-key mechanism. D and T can be estimated for a specific organization. G_c is much more uncertain.

Estimating G_c is inherently uncertain because it depends on advances in qubits, control, fabrication, error correction, decoding, system architecture, and cryptanalytic circuits. Published forecasts span from the 2030s to much later or effectively never under pessimistic assumptions. A 2020 forecasting study attempted to quantify these timelines statistically [25].

With a form of logistic regression, their model produced a model-derived 90% forecast interval under the study's assumptions of 2026 to 2033 for proof-of-concept fault-tolerant quantum computers, with a median in early 2030, and of 2039 to 2058 for feasible RSA-2048 Shor attacks, with a median in 2050.

Such multi-decade forecasts should be interpreted as model-conditioned scenarios rather than confidence intervals with the same empirical meaning as those obtained from a stationary physical process. The underlying technology trajectory is itself changing.

Michele Mosca and Marco Piani from evolutionQ publish a report every year, collecting the opinion of experts on the potential advent of a quantum threat to public-key cryptography (26 in 2025, versus 29 in 2024, 37 in 2023, and 40 in 2022). The 2025 edition showcases similar results as in the previous editions (Figure 7). My take is that the best prediction one should make is: "*we don't know*"! And when you are paranoid, it easily becomes "*who knows?*". As an illustration, a US report from 2004 prepared with the best scientists of this period planned by the year 2012 to see the implementation of a concatenated quantum error-correcting code and to obtain 50 physical qubits [27].

Topological quantum-code ideas go back to Kitaev in the 1990s, and Dennis, Kitaev, Landahl, and Preskill provided a canonical fault-tolerance analysis of the surface code in 2002 [28]. Around 2012, several proposals made surface-code fault-tolerant architectures more concrete and practical. Experimental demonstrations since then are far off cryptanalytic scale.

1.1.6 Classical and quantum cryptanalysis records

Quantum cryptanalysis includes several qualitatively different attack models. RSA-2048 is threatened by Shor's integer-factoring algorithm, while generic attacks on SHA-256 use Grover-type preimage search or quantum collision algorithms, not Shor's discrete-logarithm algorithm. Resource estimates for these problems therefore cannot be compared only by qubit count.

Classical factoring records. The major public RSA-style factoring milestones include RSA-768 in 2009/2010, RSA-240 with 795 bits in 2019, and RSA-250 with 829 bits in February 2020 [29, 30] (Figure 9). The method is the **GNFS**, General Number Field Sieve, not GNSS. The RSA-250 computation used roughly 2,700 core-years in the reported accounting.

The public general-purpose factoring record has not approached RSA-2048. The relevant classical asymptotic scaling is nevertheless **subexponential**, not exponential in the RSA key length. GNFS has heuristic complexity of the form $L_N[1/3, (64/9)^{1/3}]$, which is still prohibitive for a well-generated RSA-2048 modulus with current classical computing.

In November 2023, Ed Gerck from Planalto Research, announced that he was able to break an RSA-2048 key with a quantum computer [31]. His communication was confusing since he was saying that his solution worked on a smartphone using classical mathematics. Cybersecurity challenged him to factor large integers that they provided, to no avail [32].

Tensor-network factoring. Classical tensor-network approaches have been explored for small integer-factorization instances [33, 34]. A 2026 Italian-German study reported a 100-bit instance using a tensor-network treatment of a Schnorr-style formulation [35]. Whatever favorable scaling appears in a restricted subroutine or fitted regime, the quoted extrapolation to the current 829-bit general factoring record remains enormous, of order 10^{48} to more than 10^{62} operations in the paper's analysis. This does not constitute a competitive path to RSA-2048.

Quantum factoring records. The most important scalable experimental implementation of Shor-style factoring at small size remains the trapped-ion factorization of 15 reported by Monz et al. and published in *Science* in 2016 [36]. Earlier NMR work had already factored 15 in 2001 [37]. These experiments are algorithmic demonstrations and are extremely far from cryptographically relevant integer sizes.

A team from IBM, Pakistan and New York factorized 35 (7×5) in 2019 with a 5-qubit IBM QPU [38] but it was not a real implementation of Shor algorithm. It used a compiled version tailored to factor 35, with parts being classically precomputed and hard-coded into the quantum circuit. It reduced the number of qubits and gates needed. It didn't contain any general period-finding which is the heart of Shor's algorithm. It was actually a sort of quantum emulation of a known solution. It is not far from the joke published in 1997 about factoring 3 with a "Heisenberg dog" [39]. Likewise, Craig Gidney explained in 2025 how small integers could be factorized with some random number generation [40]. This "precompilation" technique was also used by Infleqtion in September 2025 [41]. 35 was also factorized in 2026, using Regev's quantum factoring technique, and on a quantum emulator, by a team from Singapore and China [42]. This doesn't create any new threat. Likewise, the number 551 was factorized in 2026 in India using a three-qubit NMR and a Hamiltonian optimization scheme that doesn't scale [43].

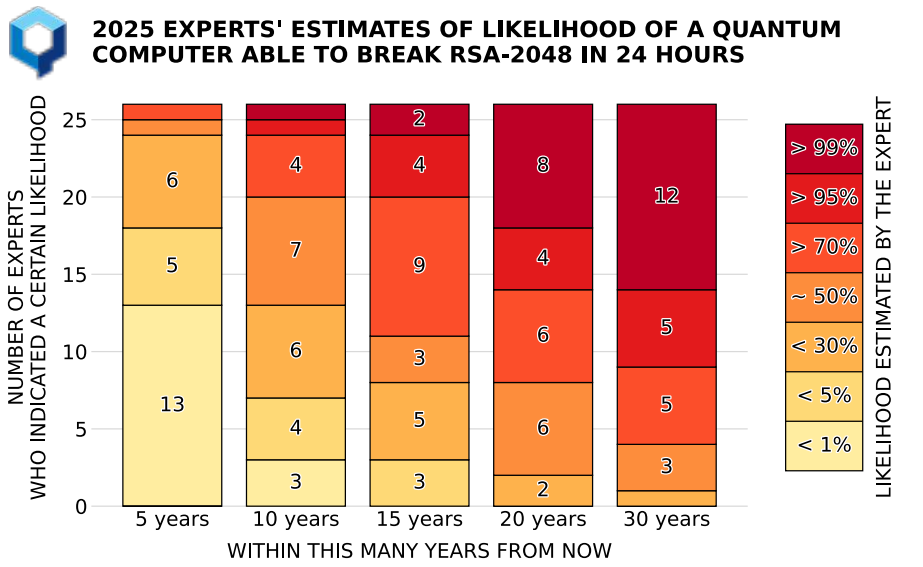


Figure 2 Experts' estimates of the likelihood of a cryptographically relevant quantum computer aggregated by likelihood bin and timeframe

Figure 7: Quantum Risk Institute poll in 2025. Source: [26].

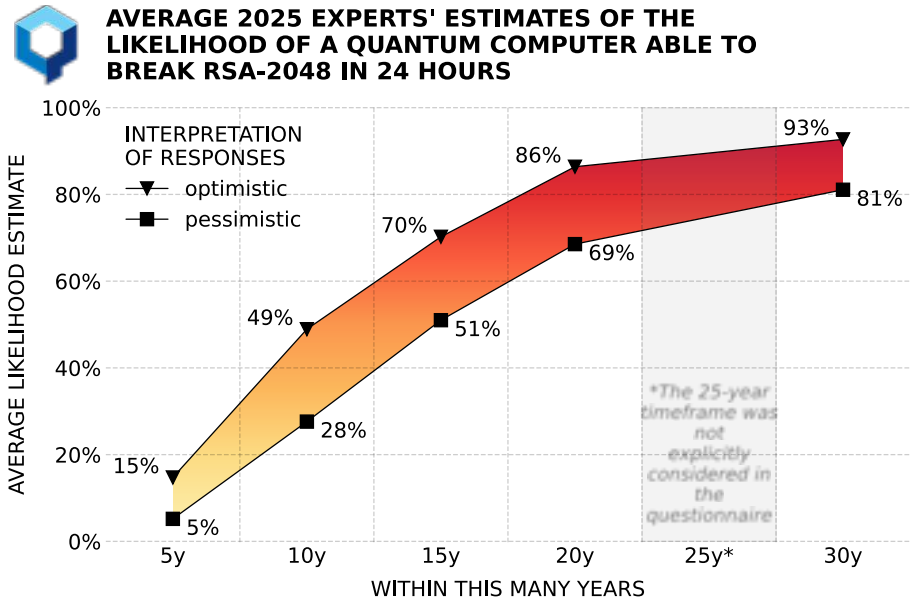


Figure 8: evolutionQ's yearly report on the quantum cyber risk as estimated by specialists from various disciplines and the way their opinion changed over that last five surveys. Source: [26].

A much larger integer, 549,755,813,701 = 712,321 × 771,781, was factored in a **classical GPU simulation** of a Shor-style quantum circuit in 2023 [44].

Using a hybrid Variational Quantum Factoring algorithm itself based on a QAOA algorithm, Zapata Computing factored the number 1,099,551,473,989 (=1,048,589 multiplied by 1,048,601) with 5 IBM superconducting qubits in 2021 [45]. The compiled instance is classically tractable and does not demonstrate cryptographic-scale advantage.

In September 2026, a team in China factorized 113,569 using analog superconducting qubits and an adiabatic method, but with no scaling claim [46].

D-Wave factoring. Several studies have mapped small factorization problems to quantum annealers [47–51]. The number of logical variables in these formulations is not directly comparable with the hardware qubit count because minor embedding and sparse hardware connectivity can require many physical qubits per logical variable. Published extrapolations to RSA-size instances remain noncompetitive and provide no demonstrated scalable advantage over classical factoring.

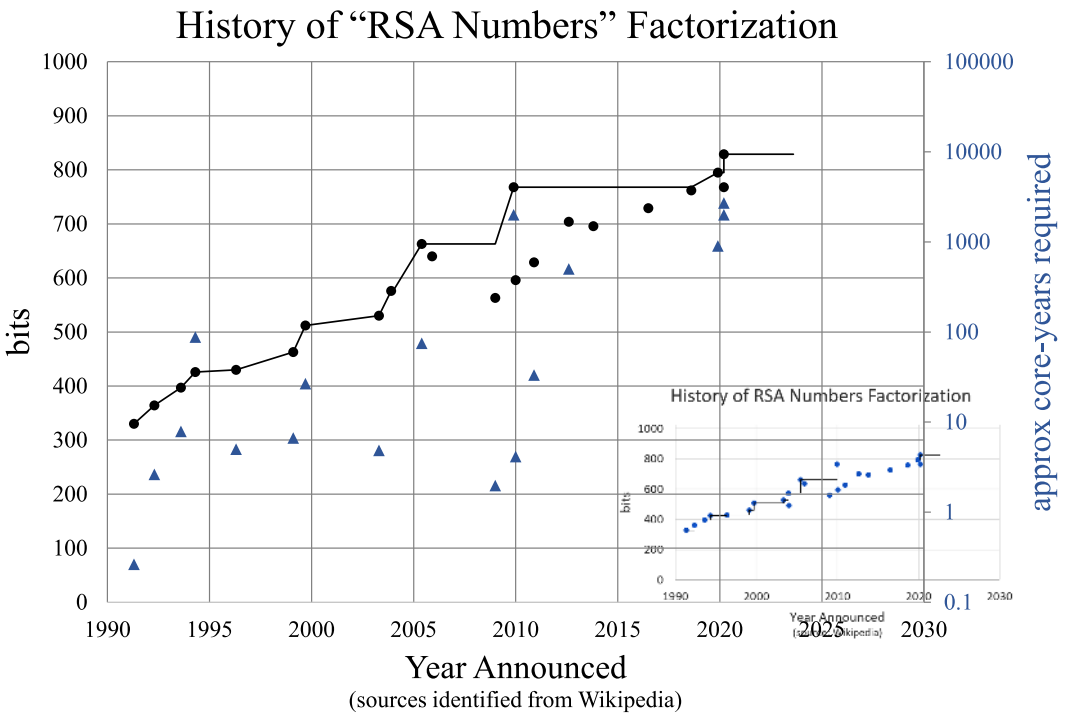


Figure 9: Evolution of record classical factorization of RSA keys. Source: Prime Factorization by Tristan Sharp and Fabio Traversa, DISA TEM, August 2023 (35 slides).

In 2021, Terra Quantum (Switzerland) announced that AES encryption was threatened by quantum algorithms running on some D-Wave annealer of the future [52]. It seemed to be a dubious claim [53].

In October 2024, a May 2024 paper from a Shanghai team attracted attention for hybrid quantum-annealing factorization [54]. The demonstrated instances were only tens of bits and no credible end-to-end resource estimate for a generic 2,048-bit RSA modulus was provided. A related study considered **PRESENT, GIFT-64, and RECTANGLE**. These are lightweight block ciphers with substitution-permutation-network structures. They are not protocols and they are not components of AES. Small-instance annealing speed comparisons can't be generalized to AES or military-grade cryptography without a scaling analysis [55].

In December 2024, another paper used a D-Wave annealer to treat specially structured 2,048-bit composite integers with only six variables [56]. The prime factors were constrained to be extremely close, which makes the instance far easier than factoring a generic RSA-2048 modulus generated according to cryptographic practice. It does not constitute a six-qubit attack on RSA-2048.

1.1.7 Quantum cryptanalysis resource estimates

After the track record, let's now look at the resource estimates to break RSA or ECC keys.

Gate-based resource estimates. In 2019, Craig Gidney and Martin Ekerå estimated that RSA-2048 could be factored in about 8 hours using roughly 20 million physical qubits in a surface-code architecture with a physical gate error rate around 10^{-3} [57]. This was an end-to-end fault-tolerant resource estimate, not a hardware roadmap. It also did not solve the engineering problem of building, controlling, decoding, and interconnecting a machine of that scale.

A 2026 paper from Brazil did present a NISQ method to determine if an integer is prime (but not find its dividers). It works with integers smaller than 30 and poses no threat to practical cryptanalytic tasks [58].

In May 2025, Craig Gidney reduced his RSA-2048 estimate to fewer than one million noisy physical qubits by combining approximate residue arithmetic, yoked surface-code memories, and more compact magic-state production [59]. Computing time increased to about five days. This is a space-time trade-off relative to the 2019 eight-hour estimate. It assumes a FTQC architecture and doesn't account for the quantum processors interconnect, cryogenic, control, decoding, or packaging engineering needed for a million-qubit machine.

In June 2025, yet another proposal coming this time from South Korea deals with using a constrained quadratic model (CQM) with D-Wave to factorize RSA keys up to 60-bits, with relatively bad scaling [60].

The logical-qubit requirement for RSA-2048 is algorithm and architecture dependent. Older Shor schemes used several thousand logical qubits, while more space-efficient variants can approach $n/2 + o(n)$ logical qubits at the cost of greater depth or other resources [61]. There is no universal lower bound of $2n + 2$ logical qubits for factoring. Converting logical to physical qubits also

depends on the error-correcting code, code distance, physical error rate, connectivity, and target runtime.

The QFT in Shor's algorithm contains controlled phase rotations. In FTQC circuits, arbitrary rotations are synthesized to a specified approximation accuracy from a discrete logical gate set, and sufficiently small QFT rotations can be omitted in an approximate QFT when the total algorithmic error budget permits it. In modern resource estimates, modular arithmetic and non-Clifford-state production dominate the cost much more strongly than the QFT itself.

Why has 21 not yet been demonstrated with a scalable implementation of Shor's algorithm on a QPU?

The best-known small experimental Shor demonstrations are highly optimized. Craig Gidney illustrated the sharp circuit-size jump between factorization instances in a 2025 analysis [62]. His example gives 21 entangling gates for a highly optimized factor-15 circuit versus 2,405 entangling gates for a more general factor-21 construction, mainly because the modular arithmetic ceases to collapse to a tiny compiled circuit Figure 11.

The resulting factor-21 circuit is still small by cryptographic standards but is large enough that coherent execution on present noisy hardware is difficult. A fault-tolerant implementation would add substantial overhead whose size depends on the physical error rate, code, decoder, target logical error budget, and circuit architecture.

For RSA-2048, the gap remains vastly larger. None of the NISQ, analog, annealing, or variational approaches discussed above has demonstrated a scalable route that competes with fault-tolerant implementations of Shor's algorithm.

Recent resource estimates illustrate very large architecture-dependent spreads. Cat-qubit proposals have reported about 349,133 physical cat qubits for RSA-2048 in four days and about 126,133 for a 256-bit elliptic-curve problem under their assumptions [63]. Other Alice & Bob analyses have explored lower physical-qubit counts with different code constructions. Garn and Kan published peer-reviewed 2025 estimates for binary-field elliptic-curve discrete logarithms on matter-based surface-code and photonic fusion-based architectures [12]. Such numbers should be compared only together with their physical error rates, code cycles, reaction times, connectivity, and runtime assumptions.

Late in 2022, **Classiq** reported an Azure Quantum Resource Estimator result of 354,562 physical qubits for an RSA-2048 scenario [64]. The assumed physical operation **fidelity** was 99.9%, corresponding to an error probability of about 10^{-3}, not a 99.9% error rate. The estimate used a surface-code distance of 13 and a quoted logical error probability of about 5.1×10^{-9}. As with all such estimates, the result is conditional on the estimator's hardware and error-correction assumptions.

Fujitsu published in 2023 its own estimate of the resources required to factor an RSA-2048 modulus using its 39-qubit classical quantum emulator [65]. They ended up with 10,000 logical qubits and 104 days of computing. They used their Fugaku supercomputer to factorize N = 253 in 463 seconds instead of 16 hours thanks to some optimization in their emulator. This could be done instantaneously using brute force on any classical computer!

A different space-time trade-off was proposed by Élie Gouzien and Nicolas Sangouard in 2021 [66]. Their peer-reviewed estimate factors RSA-2048 in 177 days with 13,436 physical processing qubits, assuming a physical error rate of 10^{-3}, a 1 μs processor cycle, and a multi-mode memory storing about 28 million spatial modes and 45 temporal modes with long storage time. The small processing-qubit count is therefore obtained by moving a very large part of the storage requirement into an extremely demanding quantum memory.

ParityQC has proposed a reversible parity architecture with resource estimates in the multi-million-qubit range for RSA-2048 [67]. Variational factoring demonstrations have also treated small integers such as 143 and 323 [68]. Without a favorable asymptotic scaling analysis and an end-to-end fault-tolerant resource estimate, such small demonstrations do not show any evidence of a competitive RSA-2048 attack.

Another gate-based proposal claims polynomial scaling using the evolution of linear entanglement entropy [69]. The paper does not provide sufficiently explicit end-to-end estimates of logical qubits, physical qubits, error rates, circuit depth, and wall-clock time for RSA-2048 to establish a practical cryptanalytic advantage.

A 2024 study involving Pasqal and South Korean researchers investigated analog neutral-atom factorization using a graph formulation [70]. The demonstrated instances were 15 and 35. The paper extrapolated to about 5,070 qubits for a 2,048-bit instance, but the decisive question is whether the required analog dynamics, control precision, connectivity, and noise scaling remain valid at that size. The qubit count alone is therefore not a cryptanalytic resource estimate comparable with a fully fault-tolerant Shor implementation.

A team in France also proposed to use cold atoms and a Grover search to factor integers but with no scalability in sight, concluding that "*the presented algorithm is likely not competitive against Shor's algorithm or the best classical factoring algorithms for large problem sizes, which highlights the need to exploit structure in the problem for achieving a practical quantum advantage over classical computers*" [71]. It makes sense since Grover's algorithm only brings a quadratic speedup.

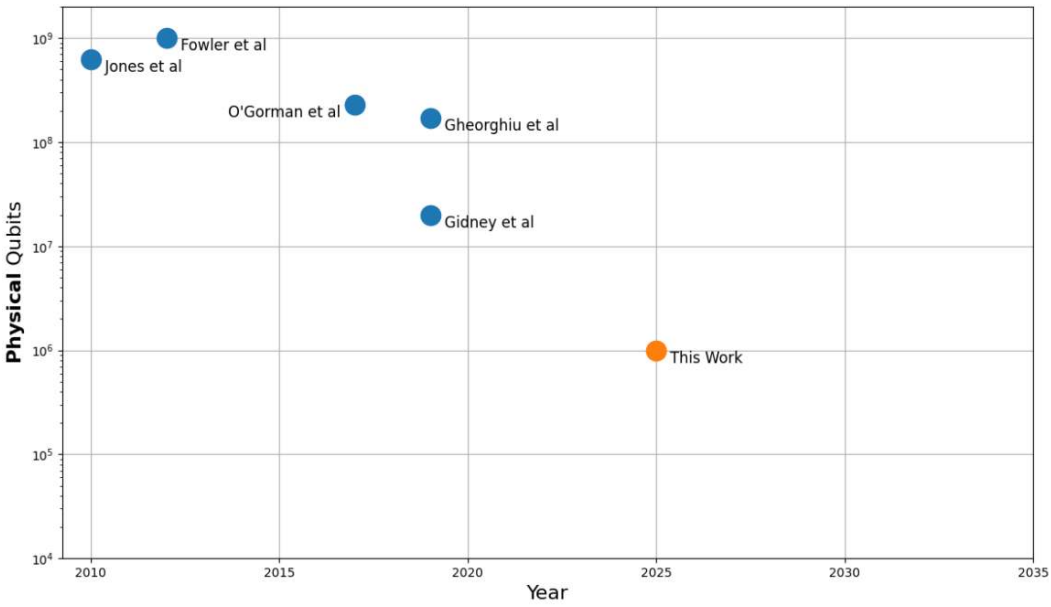


Figure 10: How the number of physical qubits required to factor a 2,048-bit RSA modulus evolved across selected resource estimates. Source: Craig Gidney in 2025 [59].

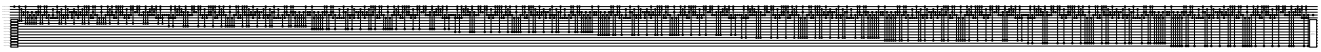


Figure 11: A Shor integer factoring circuit to factorize the integer 21. It contains 2,405 entangling gates as explained by Craig Gidney in August 2025 in [62]. You can zoom in on the PDF to look at the circuit gates since it is a vector image.

NISQ factoring? In December 2022, a China team of 25 researchers made the news with a so-called NISQ algorithm that could break an RSA 2048-bit key with only 372 physical qubits, using a hybrid lattice-based scheme based on the classical Schnorr factoring algorithm, accelerated by a QAOA quantum part [72]. It was demonstrated factoring a 48-bit key with only 10 superconducting qubits. It looked like the crypto-Armageddon was already there. Experts including Peter Shor and Scott Aaronson expressed doubts that it could be achieved practically [73, 74]. Reasons abound: the Schnorr algorithm is not necessarily competitive with classical and quantum NFS (Number Field Sieve) approaches to factorize integers [75, 76], the paper did not provide any indication of the required computing time and the runtime appeared to be in the million-year range, and no favorable end-to-end scaling was demonstrated for this QAOA-based factoring formulation in a NISQ regime, and on top of that, the algorithm needs 1,139 to 1,490 gate cycles, requiring qubit fidelities in the 5-nines range minimum, thus mandating some QEC and significant physical qubit overhead, invalidating their 372 qubits sizing claim. A Google team proved in July 2023 that the proposed algorithm cannot scale beyond a key of 70 bits, even with perfect qubits, by using a classical quantum emulator [77]. An IonQ team found in August 2023 that lattice-based factoring does not scale successfully to larger numbers, whatever the role of a quantum computer in the setup [78]. A team in Russia also proved that the classical part of the algorithm does not scale well [79]. Another one also expressed doubts on the scalability of another optimized QAOA method [80]. No scalable route has been established so far. A proposal to improve [72] by combining Schnorr with VQE came from Spain in November 2024, which could factor the number 1,961, but with no good scaling in sight [81].

A team from **Kipu Quantum** (Germany) proposed in January 2023 a lightly documented variation of the Schnorr/QAOA hybrid algorithm that would be adapted to their DAQC (digital analog quantum computing) architecture. They tested it at a small scale with a 48-bit key with 10 Quantinuum qubits but its potential scale is also in question [82].

Another China team proposed in April 2023 to turn Shor's integer factoring algorithm into a hybrid classical/quantum version by distributing its period-finding part over several QPUs [83]. They would implement nonlocal quantum gates thanks to some qubit teleportation in parallel for a number of qubits equivalent to the size of the RSA key to factorize which is not yet available, at least, deterministically. In a way, it is about moving the goal post elsewhere. In August 2023, an algorithm proposed by Oled Regev traded better computing time with some classical parallelization and post-processing and a larger number of logical qubits [84]. It does not increase the quantum computing threat to cybersecurity [85, 86]. And it seems to be even slower than Shor's algorithm [87].

The 2026 Q-Day Prize result and its validation method

The Canadian Project Eleven PQC company awarded the first edition of its Q-Day Prize endowed with a Bitcoin, to Giancarlo Lelli who managed to break a 15-bit elliptic curve key using an IBM quantum computer, using Shor's dlog algorithm [88]. Unfortunately, it was using a technique labeled "falling with style" as a reference to Toy Story. The Shor 65-qubit circuit contained 98,000. It was too large to run on a NISQ system, so its output was just random noise. The probability to run without an error was 10^{-215}. The method used a conventional checker to sort out the noise until stumbling on the right key by chance [89]. The communication around this feat generated some Streisand effect. Bad noise, but good enough to drive interest in the company behind the prize.

In October 2024, an international research team was able to factorize the integer 253 using a variation of a VQE NISQ algorithm, using 9 qubits. It could factorize 1,048,561 using a 27-qubit emulator [90]. But don't worry, this won't scale. In 2023, a US-India research team factorized integers with four and five prime factors, that is 4-almost-primes and 5-almost-primes, on an IBM QPU [91]. Such integers are easier to factor than integers with only two prime factors as in RSA keys. It was achieved with three and four qubits of a seven-qubit IBM quantim processor. Which means that there is no quantum advantage at all, since these qubits can be perfectly emulated on a Raspberry Pi, or even a microcomputer from the late 1970s! As usual, this kind of sensational paper generates some FUD (fear, uncertainty, and doubt) and leverages the famous Brandolini's law according to which the resources needed to counter an invalid claim are at least one order of magnitude larger than the ones used to broadcast the claim. The practical cryptanalytic risk therefore remains elsewhere in the cybersecurity stack.

Another potential threat came with a 2024 paper from Taiwan on a so-called single photon QPU that could run Shor's algorithm [92]. It is using a 32-time bin single photon created with a set of interferometers and could factor the integer 15 with 5 qubits. There is no indication on how this would scale to a larger dimension to factor large integers. A similar single photo proposal came from Germany in December 2024, but with infinite time and energy resources, which is not very practical [93].

In March 2025, Russian scientists proposed some improvement on a QAOA algorithm running on trapped-ions associated to the classical Schnorr algorithm. They factored 35183361263263 with 15 bits, which could be done on any laptop in emulation mode. But "the scalability of this approach both in classical and quantum domain still requires further studies". No favorable end-to-end scaling was demonstrated for this QAOA-based factoring formulation [94].

New 2026 resource estimates for RSA-2048 further widened the architecture-dependent range. Iceberg Quantum's Pinnacle preprint reports fewer than 10^5 physical qubits under QLDPC assumptions, a physical error rate of 10^{-3}, a 1 μs code cycle, and a 10 μs reaction time [95]. Other 2026 proposals explore neutral-atom, distributed, and heterogeneous architectures [96–98].

These estimates are not directly interchangeable. Current proposals span roughly 10^4 to 10^6 physical qubits in their most qubit-efficient configurations, with large differences in runtime, connectivity, code family, decoder assumptions, non-Clifford-state supply, modular communication, and physical clock rates. For example, the Pinnacle minimum-qubit regime can trade toward month- or year-scale runtimes, while the Xue and Covey modular-atom proposal assumes about half a million physical qubits, 10^5 inter-module Bell pairs per second, and 1 ms measurement time. The important trend is a reduction in estimated qubit count accompanied by increasingly demanding architectural assumptions, not a direct prediction of the date at which RSA-2048 will be broken.

1.1.8 Blockchain and Cryptocurrencies vulnerabilities

Bitcoin, other cryptocurrencies, and blockchain systems can be exposed to long-term quantum cryptanalysis, but there is no single "blockchain cryptography" stack. The risk depends on the hash functions, signature schemes, address types, consensus rules, and key-exposure behavior used by each protocol [99].

Bitcoin does not use a generic patchwork of AES, RSA, and SHA-3. Its proof-of-work and several integrity constructions rely on SHA-256, while transaction authorization has historically used ECDSA over secp256k1 and, since Taproot, also Schnorr signatures over the same secp256k1 group. Both ECDSA and Schnorr over secp256k1 are vulnerable in principle to Shor's ECDLP algorithm once the relevant public key is exposed. Ethereum's execution layer uses Keccak-256, whose padding differs from standardized SHA3-256, and secp256k1 ECDSA for externally owned accounts. Ethereum proof-of-stake validators use BLS signatures over BLS12-381. These elliptic-curve signature systems are also vulnerable in principle to sufficiently powerful quantum discrete-logarithm attacks.

Ethereum's proof-of-stake transition did **not** replace account ECDSA signatures with Lamport signatures. The consensus layer uses BLS signatures, while ordinary externally owned accounts continue to use secp256k1 ECDSA. Post-quantum migration therefore requires ex-

plicit protocol and account changes rather than relying on the Eth2 transition itself.

The JVG factorization claim

A hybrid algorithm by Jesse Van Griensven Thé, Victor Oliveira Santos, and Bahram Gharabaghi proposes a substantially smaller quantum circuit for integer factorization by replacing the QFT with a Quantum Number Theoretic Transform and moving modular exponentiation to a classical subroutine [100].

The proposal reports large reductions in the quantum register and gate budget on the tested small instances. The central methodological trade-off is that work normally represented coherently inside Shor's quantum order-finding circuit is moved into a classical component. The relevant question is therefore the end-to-end scaling of the hybrid algorithm, not only the size of its quantum circuit.

The paper projects an approximately 11-hour RSA-2048 runtime under its model, but this extrapolation has not been independently validated at cryptographic scale. The work was initially circulated on Preprints.org but was subsequently peer reviewed and published in the *Journal of Cybersecurity and Privacy* in April 2026 [100]. The conclusion is that the claimed asymptotic and end-to-end advantages require independent cryptanalytic scrutiny.

Quantum computing does not automatically let an attacker rewrite an existing blockchain. The most direct Bitcoin threat is to transaction authorization: secp256k1 signatures can be attacked with Shor's **elliptic-curve discrete-logarithm** algorithm, not Shor's integer-factoring algorithm. Bitcoin proof-of-work, which repeatedly evaluates SHA-256, is not broken by Shor's algorithm but can in principle receive a Grover-type quadratic search speedup. Current fault-tolerant resource estimates make that mining attack vastly less practical than the signature-layer ECDLP attack.

Webber et al. estimated that breaking a 256-bit elliptic-curve Bitcoin key within one hour would require about 317 million physical qubits in their surface-code model, assuming a 1 μs code cycle, 10 μs reaction time, and physical gate error probability 10^{-3}. Extending the allowed runtime to one day reduced their estimate to about 13 million physical qubits [102].

Those 2022 numbers are now useful as a historical baseline rather than a current lower bound. Resource estimations published in 2026 reduced some ECC attack physical qubit needs, while maintaining reasonable computing times.

Mitigations principally require migrating vulnerable signatures and key-establishment mechanisms to post-quantum alternatives. Encrypting blockchain payload data with AES-256 can protect confidentiality when a suitable symmetric-key distribution mechanism exists, but it does not by itself replace vulnerable transaction signatures. **Quantum Secure Direct Communication** (QSDC) is a distinct quantum-communication paradigm that sends protected messages directly through a quantum channel. It is **not a QKD protocol**, and the field predates 2020 [103]. Proposals that modify Bitcoin validation timing can affect the feasibility of rapid on-spend attacks, but the underlying quantum primitive being exploited is ECDLP, not integer factorization [104]. Bitcoin mining has a separate theoretical Grover threat, discussed below.

We can also mention the open-source Blockchain project resisting quantum attacks, Quantum Resistant Ledger.

The Quantum Resistant Ledger is based on hash-based XMSS signatures [105]. Bitcoin-style proof-of-work has a separate theoretical exposure to Grover search, but fault-tolerant physical-resource estimates are extraordinarily unfavorable [106–108]. This is a different problem from breaking transaction signatures.

The **Long Finance** material summarized several quantum risks for smart ledgers by separating data confidentiality, historical-record modification, and transaction forgery [101, 109] (Figure 13). The key distinction is whether a security property depends on a Shor-vulnerable public-key signature or key-agreement scheme, a symmetric cipher or hash, or an independent protocol assumption.

Google/PRX Quantum ECC threat assessment. A Google-led 2026 study [110] mentioned two optimized secp256k1 circuits with fewer than about 1,200 logical qubits and 90 million Toffoli gates, or fewer than about 1,450 logical qubits and 70 million Toffoli gates, without releasing the code. The authors estimated resources for about half a million physical qubits and minute-scale runtimes. This enables an on-spend attack scenario in which a public key revealed by a pending transaction could be attacked before confirmation. The same paper also analyzes at-rest bitcoin exposure, including about 1.7 million bitcoins in old pay-to-public-key outputs and additional exposure from address reuse and public-key-revealing script types such as P2TR.

Dormant outputs whose public keys are exposed and whose owners have lost the corresponding private keys create a difficult migration problem because the owners cannot simply sign a move to a post-quantum address. It is nevertheless too strong to say that these assets will "inevitably" be stolen because protocol-level responses such as freezes, burns, recovery rules, or contentious governance changes remain possible. On Ethereum, the 2026 analysis also highlights exposed secp256k1 account keys, vulnerable BLS proof-of-stake signatures, and high-value smart-contract administrative keys. The

Table 3. Main Algorithms Types Used for Cryptography, and Uses For Smart Ledgers[19]

Type of Algorithm	General Use	Example Algorithms of This Type	Example Uses for Smart Ledgers
Symmetric	Secret communications	AES, DES, 3DES, RC4	Protection of resources stored on ledger
Public key	Secret communications (including key exchange) or digital signature	RSA, Diffie-Hellman, El Gamal, ECDSA	User authentication; signature of transactions, data or software
Hash	Generating fixed-length digest of arbitrary-length text	SHA-256, SHA-512, SHA-3	Ensuring authenticity of blockchain

Figure 12: Algorithms used in cryptos and smart ledgers. Source: [101].

Table 4. Risks to Blockchain Architectures from Quantum Computing

	Transactions	Data on Blockchain	Software on Blockchain
Read historical records without authorization	No (blockchains are intended to allow access to transaction information)	No, unless confidential and secured with vulnerable cryptography	No, unless confidential and secured with vulnerable cryptography
Alter historical records	No	No	May be able to run software without authorisation if signature used
Spoof ongoing records	Yes, possibly	Yes, possibly	Yes, possibly

Figure 13: Potential long-term quantum threats to cryptocurrencies. Source: [99].

quoted ETH and tokenized-asset amounts are exposure estimates under particular key-compromise scenarios, not guaranteed losses [110].

Compromise of an administrative key could have consequences beyond theft of native ETH, including unauthorized token issuance or control of smart-contract governance. The resulting economic damage depends on contract design, issuer controls, emergency procedures, and protocol response. Hash-based proof systems such as STARK constructions avoid the same elliptic-curve discrete-logarithm dependency for their proof soundness, although complete applications can still contain other vulnerable keys. The PRX Quantum authors therefore argue for prompt post-quantum migration and discuss policy options for assets that cannot be migrated by their original owners [110].

A few weeks after the first Google preprint, three Inria researchers reported a more space-efficient 256-bit elliptic-curve discrete-logarithm circuit using 1,098 logical qubits and 22 repetitions of a circuit containing about 2.47×10^{11} Toffoli gates [111]. André Schrottenloher later published an optimized point-addition study with source code [112].

A Chinese team reported 1,333 logical qubits and about 1.64×10^{10} Toffoli gates for one construction [113]. A later 2026 version reduced the logical footprint to 835 qubits and about 1.9×10^{9} Toffoli gates for the 256-bit case [114].

Dallaire-Demers, Doyle, and Foo introduced a graded secp256k1 ECDLP benchmark suite and mapped Shor circuits to surface-code, repetition-cat, and LDPC-cat hardware scenarios [115] (Figure 15). Under their explicit and testable hardware assumptions, the full 256-bit challenge crosses their projected hardware curves in a 2027 to 2033 window.

In another 2026 paper, researchers from Caltech and Inria demonstrated that Regev's reduction currently cannot compete with or replace Shor's algorithm for breaking ECC keys [116].

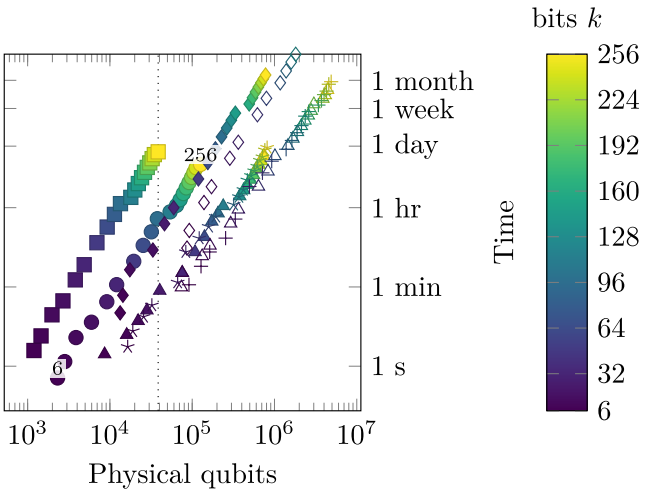


Figure 15: 2026 physical-resource scenarios for ECDLP using Shor's algorithm. Repetition-cat and LDPC-cat points are compared with conservative and aggressive surface-code baselines. The color scale represents the elliptic-curve bit size k, with 256-bit instances being the cryptographically relevant endpoint. Source: [115]. Added in 2026.

Quantum mining is not the leading practical threat. Dallaire-Demers estimated the fault-tolerant cost of Grover-accelerated Bitcoin mining and RIPEMD-160 preimage attacks [108]. Even a favorable partial-preimage setting requires about 10^8 physical qubits and 10^4 MW. At the January 2025 mainnet difficulty, the extrapolation reaches about 10^{23} physical qubits and 10^{25} W. The latter is a few percent of the Sun's luminosity, so it is stellar-scale but not equal to the Sun's full power output. Manson and Sanders independently found only a negligible change in the 51% attack threshold in their game-theoretic model [117]. Bitcoin ASIC miners do not "reset every 10 minutes". They hash continuously, while the accepted block and transaction template change on the roughly ten-minute average block timescale. The dominant plausible quantum risk is therefore the **secp256k1 signature layer**, which includes both ECDSA and Taproot Schnorr signatures, rather than mining.

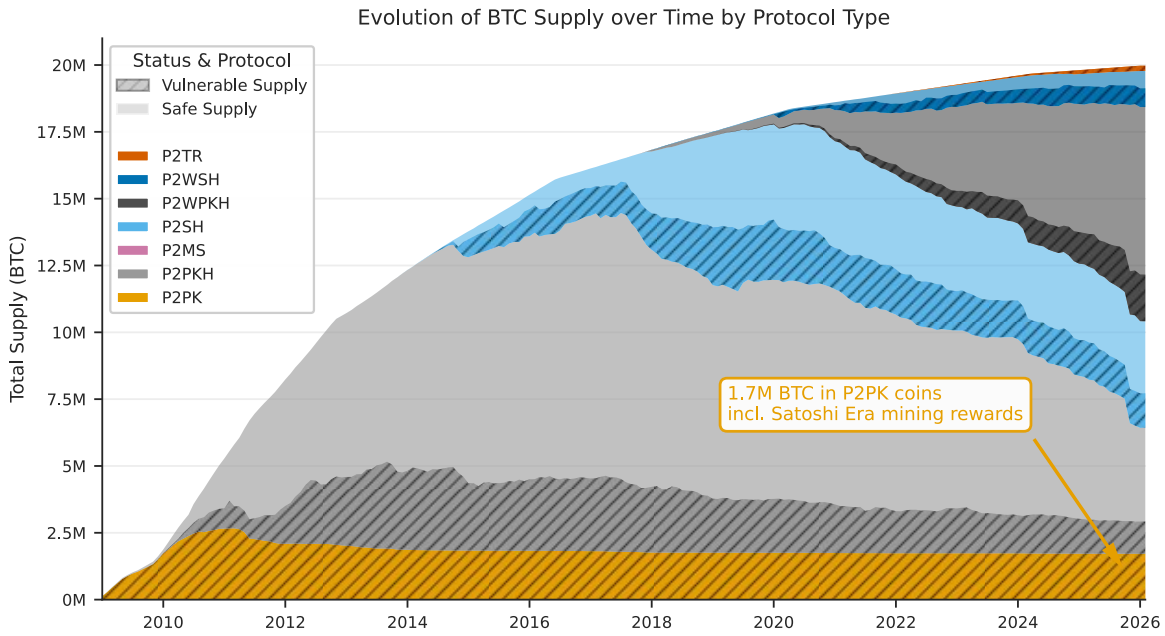


Figure 14: About 6.9 million BTC fall into categories that the 2026 Google-led analysis treats as having some form of public-key exposure or future quantum vulnerability. The categories are not equally vulnerable. Source: [110]. Added in 2026.

Q-Day timelines and market reaction. Project Eleven's May 2026 report is a useful industry scenario analysis, but its 2030, 2033, and 2042 Q-Day dates are not scientific confidence intervals. The company also sells post-quantum migration services, which is relevant context when interpreting its risk framing. Reports that institutional investors have changed allocations because of quantum risk illustrate that perception can affect markets well before a CRQC exists, but it is not possible to establish from public evidence that any one allocation change was the first such case.

PQC quantum threats?. Simon's algorithm is not a generic algorithm for solving the lattice problems underlying ML-KEM. Known quantum improvements for lattice attacks instead combine techniques such as amplitude amplification, quantum walks, and quantum-accelerated sieving. The failure of SIDH/SIKE is also a different story: SIKE was broken by **classical** cryptanalysis, including the polynomial-time key-recovery attack of Castryck and Decru [3]. NIST's first three PQC standards are not all lattice based: ML-KEM and ML-DSA are module-lattice schemes, while SLH-DSA is hash based. NIST also selected the code-based HQC as a second KEM for future standardization. For lattice attacks, Doriguello et al. analyzed quantum sieving for the Shortest Vector Problem and found that optimistic fault-tolerant assumptions can still lead to extraordinary costs, around 10^{13} physical qubits and 10^{31} years for one dimension-400 scenario [118].

1.1.9 Bibliography and notes

These are the bibliographical references and notes for the **Quantum computing threat** subsection.

[1] Towards Quantum-Native Communication Systems: State-of-the-Art, Trends, and Challenges, by Xiaolin Zhou, Ekram Hossain, et al., arXiv, May 2025 (49 pages).

[2] IDQ: Quantum-Safe Security relevance for Central Banks, by IDQ, June 2018 (27 slides).

[3] An Efficient Key Recovery Attack on SIDH, by Wouter Castryck and Thomas Decru, Advances in Cryptology – EUROCRYPT 2023, Lecture Notes in Computer Science, April 2023 (25 pages) (preprint on lirias.kuleuven.be).

[4] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, by Peter W. Shor, SIAM Journal on Computing, October 1997 (26 pages).

[5] On Shor's algorithms, the various derivatives, their implementation and their applications, by Martin Ekerå, 2019 (135 slides).

[6] Post-Quantum Secure Architectures for Automotive Hardware Secure Modules, by Wen Wang and Marc Stöttinger, 2020 (7 pages).

[7] Deciphering Charles Quint (A diplomatic letter from 1547), by Cécile Pierrot, Camille Desenclos, Pierrick Gaudry, and Paul Zimmermann, HAL Open Science, April 2023 (13 pages).

[8] Emperor Charles V's secret code cracked after five centuries, by Agence France-Presse in Nancy, The Guardian, November 2022.

[9] Shor's discrete logarithm quantum algorithm for elliptic curves, by John Proos and Christof Zalka, arXiv, January 2004 (34 pages).

[10] Elliptic Curve Cryptography and Government Backdoors, by Ben Schwennesen, 2016 (20 pages).

[11] Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3, by Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, and John M. Schanck, Selected Areas in Cryptography – SAC 2016, Lecture Notes in Computer Science, October 2017 (21 pages) 🔓.

[12] Quantum Resource Estimates for Computing Binary Elliptic Curve Discrete Logarithms, by Michael Garn and Angus Kan, IEEE Transactions on Quantum Engineering, July 2025 (23 pages).

[13] Status of quantum computer development, by BSI, BSI, January 2025 (222 pages).

[14] Breaking Symmetric Cryptosystems Using Quantum Algorithms, by Gaëtan Leurent, Marc Kaplan, Anthony Leverrier, and María Naya-Plasencia, 2016 (58 slides).

[15] Simon's Algorithm for the Even-Mansour Cipher on Quantum Hardware, by Anina Köhler, Jakob Murauer, Tim Heine, Stefan Rosemann, and Tobias Hemmert, arXiv, April 2026.

[16] Quantum Safe Cryptography and Security, by Matthew Campagna, June 2015 (64 pages).

[17] What is the quantum apocalypse and should we be scared?, by Frank Gardner, January 2022.

[18] 'Nuclear Threat to Cybersecurity' – Post-Quantum Cybersecurity Rapidly Gains Attention of U.S. Congress, Administration, by Matt Swayne, The Quantum Insider, July 2022.

[19] Quantum computers could crack Bitcoin by 2022, by Robert Stevens, May 2020.

[20] Cybersecurity Experts Say Quantum, Advanced Technology Will Break Standard Encryption Within Two Years, by Matt Swayne, The Quantum Insider, December 2021.

[21] Quantum computing could break the internet. This is how, by Sam Learner, John Thornhill, Sam Joiner, and Irene de la Torre Arenas, Financial Times, May 2023.

[22] Cryptography: Against AI and QAI Odds, by Sheetal Harris, Hassan Jalil Hadi, and Umer Zukaib, arXiv, September 2023 (7 pages).

[23] Advancements in Quantum Computing and AI May Impact PQC Migration Timelines, by Robert Campbell et al., March 2024 (13 pages).

[24] Quantum crypto-economics: Blockchain prediction markets for the evolution of quantum technology, by Peter P. Rohde, Vijay Mohan, Sinclair Davidson, Chris Berg, Darcy Allen, Gavin K. Brennen, and Jason Potts, arXiv, February 2021 (12 pages).

[25] Forecasting timelines of quantum computing, by Jaime Sevilla and C. Jess Riedel, arXiv, December 2020 (23 pages).

[26] Quantum Threat Timeline Report 2025, by Global Risk Institute, March 2026 (75 pages).

[27] A Quantum Information Science and Technology Roadmap Part 1: Quantum Computation, by Richard Hughes et al., ARDA (Advanced Research and Development Activity), April 2004 (268 pages).

[28] Topological quantum memory, by Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill, Journal of Mathematical Physics, September 2002 (54 pages) 🔓 (preprint on arXiv).

[29] The State of the Art in Integer Factoring and Breaking Public-Key Cryptography, by Fabrice Boudot et al., IEEE Security & Privacy, March 2022 🔓 (preprint on HAL).

[30] Factoring RSA-240 and computing discrete logarithms in a 240-digit prime field with the same software and hardware, by Fabrice Boudot et al., Journées GDR-IM, March 2021 (87 slides).

[31] Algorithms for Quantum Computation: The Derivatives of Discontinuous Functions, by Ed Gerck, Mathematics, December 2022.

[32] Researcher Claims to Crack RSA-2048 With Quantum Computer, by Mathew Schwartz, November 2023.

[33] Quantum inspired factorization up to 100-bit RSA number in polynomial time, by Marco Tesoro, Ilaria Siloi, Daniel Jaschke, Giuseppe Magnifico, and Simone Montangero, arXiv, December 2024 (9 pages).

[34] Hacking Cryptographic Protocols with Tensor Network Attacks, by Borja Aizpurua, Siddhartha Patra, Josu Etxezarreta Martinez, and Roman Orus, arXiv, September 2024 (10 pages).

[35] Quantum inspired factorization up to 100-bit RSA number in polynomial time, by Marco Tesoro, Ilaria Siloi, Daniel Jaschke, Giuseppe Magnifico, and Simone Montangero, arXiv, October 2024 (9 pages).

[36] Realization of a scalable Shor algorithm, by Thomas Monz, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl, Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang, and Rainer Blatt, Science, March 2016 (3 pages) 🔓 (preprint on arXiv).

[37] Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, by Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang, Nature, December 2001 🔓 (preprint on arXiv).

[38] An Experimental Study of Shor's Factoring Algorithm on IBM Q, by Mirko Amico, Zain H. Saleem, and Muir Kumph, arXiv, May 2019 (10 pages).

[39] Un-topical review: Heisenberg's dog and quantum computing, by JàNos a. Bergou and Berthold-Georg Englert, August 1997 (11 pages).

[40] Factoring all 8 bit integers, by Craig Gidney, Bluesky, April 2025.

[41] Infleqtion Unveils New Architecture to Accelerate Its Quantum Computing Roadmap To Achieve 1000 Logical Qubits by 2030, by Matt Stubbs, Infleqtion, September 2025.

[42] Space-Optimized and Experimental Implementations of Regev's Quantum Factoring Algorithm, by Wentao Yang, Bao Yan, Muxi Zheng, Quanfeng Lu, Shijie Wei, and Gui-Lu Long, arXiv, November 2025 (49 pages).

[43] Experimental prime factorization via the feedback quantum control, by K. B. Hari Krishnan, Vishal Varma, and T. S. Mahesh, arXiv, January 2026 (8 pages).

[44] Large-Scale Simulation of Shor's Quantum Factoring Algorithm, by Dennis Willsch, Madita Willsch, Fengping Jin, Hans De Raedt, and Kristel Michielsen, arXiv, October 2023 (32 pages).

[45] Analyzing the performance of variational quantum factoring on a superconducting quantum processor, by Amir H. Karamlou, William A. Simon, Amara Katabarwa, Travis L. Scholten, Borja Peropadre, and Yudong Cao, npj Quantum Information, October 2021.

[46] Factoring six-digit integers with superconducting quantum circuits, by Xi Zhang, Xinsheng Tan, and Yang Yu, arXiv, September 2026 (5 pages).

[47] Breaking RSA Security With A Low Noise D-Wave 2000Q Quantum Annealer: Computational Times, Limitations And Prospects, by Riccardo Mengoni, Daniele Ottaviani, and Paolino Iorio, arXiv, May 2020 (8 pages).

[48] HUBO and QUBO models for Prime factorization, by Kyungtaek Jun, arXiv, January 2023 (11 pages).

[49] Experimenting with D-Wave Quantum Annealers on Prime Factorization problems, by Jingwen Ding, Giuseppe Spallitta, and Roberto Sebastiani, arXiv, June 2024 (8 pages).

[50] Effective prime factorization via quantum annealing by modular locally-structured embedding, by Jingwen Ding,

Giuseppe Spallitta, and Roberto Sebastiani, Scientific Reports, February 2024 🔓 (preprint on dx.doi.org).

[51] Quantum Prime Factorization: A Novel Approach Based on Fermat Method, by Julien Mellaerts, arXiv, August 2025 (9 pages).

[52] Swiss firm Terra Quantum uncovers vulnerabilities that imperil encryption, by Ryan Gallagher, February 2021.

[53] Quantum Security Analysis of AES, by Xavier Bonnetain et al., 2019 (39 pages).

[54] Quantum annealing public key cryptographic attack algorithm based on D-Wave advantage, by Chao Wang et al., May 2024 (15 pages).

[55] China quantum tunneling breakthrough, by Natto Team, NattoThoughts, October 2024.

[56] A First Successful Factorization of RSA-2048 Integer by D-Wave Quantum Computer, by Chao Wang et al., Tsinghua Science and Technology, December 2024 (13 pages).

[57] How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, by Craig Gidney and Martin Ekerå, Quantum Journal, 2019 (28 pages).

[58] Prime Number Identification Demonstrated with Quantum Processors Using a New Rescaling-Based Noise Mitigation Technique, by Victor F. dos Santos, Victor P. Brasil, Pedro A. S. Contri, and Jonas Maziero, arXiv, May 2026 (17 pages).

[59] How to factor 2048 bit RSA integers with less than a million noisy qubits, by Craig Gidney, arXiv, May 2025 (40 pages).

[60] Quantum prime factorization algorithms using binary carry propagation, by Arim Ryou, Kiwoong Kim, and Kyungtaek Jun, arXiv, June 2025 (9 pages).

[61] Reducing the Number of Qubits in Quantum Factoring, by Clémence Chevignard et al., 2024 (42 pages).

[62] Why haven't quantum computers factored 21 yet?, by Craig Gidney, Craig Gidney blog, August 2025.

[63] Performance Analysis of a Repetition Cat Code Architecture: Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits, by Élie Gouzien, Physical Review Letters, July 2023 🔓 (preprint on HAL).

[64] Making academic quantum algorithms automatically executable, by Classiq, December 2022.

[65] Fujitsu quantum simulator assesses vulnerability of RSA cryptosystem to potential quantum computer cryptography threat, by Fujitsu, January 2023.

[66] Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory, by Élie Gouzien and Nicolas Sangouard, Physical Review Letters, September 2021 🔓 (preprint on arXiv).

[67] Scalable set of reversible parity gates for integer factorization, by Martin Lanthaler, Benjamin E. Niehoff, and Wolfgang Lechner, Communications Physics, April 2023.

[68] Shallow Depth Factoring Based on Quantum Feasibility Labeling and Variational Quantum Search, by Imran Khan Tutul, Sara Karimi, Mohammadreza Soltaninia, and Junpeng Zhan, arXiv, October 2023 (10 pages).

[69] Using quantum computers to identify prime numbers via entanglement dynamics, by Victor F. dos Santos and Jonas Maziero, arXiv, August 2024 (19 pages).

[70] A Rydberg-atom approach to the integer factorization problem, by Juyoung Park, Loïc Henriet, Jaewook Ahn, et al., arXiv, February 2024 (12 pages).

[71] Quantum Factoring Algorithm using Grover Search, by S. Whitlock and T. D. Kieu, arXiv, December 2023 (15 pages).

[72] Factoring integers with sublinear resources on a superconducting quantum processor, by Bao Yan, Gui-Lu Long, et al., arXiv, December 2022 (32 pages).

[73] Chinese researchers claim success in breaking encryption using quantum computers, by Richard Waters, December 2022.

[74] Cargo Cult Quantum Factoring, by Scott Aaronson, January 2023.

[75] A low-resource quantum factoring algorithm, by Daniel J. Bernstein et al., 2017 (17 pages).

[76] On speeding up factoring with quantum SAT solvers, by Michele Mosca, Joao Marcos Vensi Basso, and Sebastian R. Verschoor, Scientific Reports, September 2020.

[77] A comment on "Factoring integers with sublinear resources on a superconducting quantum processor", by Tanuj Khattar and Noureldin Yosri, arXiv, July 2023 (6 pages).

[78] Quantum and Classical Combinatorial Optimizations Applied to Lattice-Based Factorization, by Willie Aboumrad, Dominic Widdows, and Ananth Kaushik, arXiv, August 2023 (23 pages).

[79] Pitfalls of the sublinear QAOA-based factorization algorithm, by Sergey V. Grebnev, Maxim A. Gavreev, Evgeniy O. Kiktenko, Anton P. Guglya, Albert R. Efimov, and Aleksey K. Fedorov, arXiv, December 2023 (19 pages).

[80] Integer Factorization through Func-QAOA, by Mostafa Atallah, Haemanth Velmurugan, Rohan Sharma, Siddhant Midha, Shamim Al Mamun, Ludmila Botelho, Adam Glos, and Özlem Salehi, arXiv, September 2023 (25 pages).

[81] Factoring integers via Schnorr's algorithm assisted with VQE, by Luis Sánchez Cano, Ginés Carrascal de las Heras, Guillermo Botella Juan, and Alberto del Barrio García, arXiv, November 2024 (12 pages).

[82] Digitized-counterdiabatic quantum factorization, by Narendra N. Hegade and Enrique Solano, arXiv, January 2023 (3 pages).

[83] Distributed Phase Estimation Algorithm and Distributed Shor's Algorithm, by Ligang Xiao, Daowen Qiu, Le Luo, and Paulo Mateus, arXiv, December 2024 (9 pages).

[84] An Efficient Quantum Factoring Algorithm, by Oded Regev, arXiv, January 2024 (13 pages).

[85] A high-level comparison of state-of-the-art quantum algorithms for breaking asymmetric cryptography, by Martin Ekerå and Joel Gärtner, arXiv, May 2024 (34 pages).

[86] Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms, by Cédric Pilatte, arXiv, April 2024 (22 pages).

[87] Implementation and Analysis of Regev's Quantum Factorization Algorithm, by Przemysław Pawlitko, Natalia Moćko, Marcin Niemiec, and Piotr Chołda, arXiv, July 2025 (28 pages).

[88] 15-Bit ECC Key Broken on Quantum Hardware Wins Q-Day Prize, by Mohib Ur Rehman, The Quantum Insider, April 2026.

[89] The predictable failure of the QDay Prize, by Craig Gidney, Craig Gidney's blog, April 2026.

[90] Variational Quantum Eigensolver Approach to Prime Factorization on IBM's Noisy Intermediate Scale Quantum Computer, by Mona Sobhani, Yahui Chai, Tobias Hartung, and Karl Jansen, arXiv, March 2025 (13 pages).

[91] Factorization of large tetra and penta prime numbers on IBM quantum processor, by Ritu Dhaulakhandi, Bikash K. Behera, and Felix J. Seo, arXiv, April 2023 (12 pages).

[92] Implementation of Shor's algorithm with a single photon in 32 dimensions, by Hao-Cheng Weng, Physical Review Applied, September 2024 🔓 (preprint on arXiv).

[93] Factoring an integer with three oscillators and a qubit, by Lukas Brenner, Libor Caha, Xavier Coiteux-Roy, and Robert Koenig, arXiv, December 2024 (77 pages).

[94] Experimental factoring integers using fixed-point-QAOA with a trapped-ion quantum processor, by Ilia V. Zalivako, Nikolay N. Kolachevsky, et al., arXiv, March 2025 (4 pages).

[95] The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes, by Paul Webster, Lawrence Z. Cohen, et al., arXiv, February 2026 (22 pages).

[96] Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits, by Madelyn Cain, Qian Xu, Robbie King, Lewis R. B. Picard, Harry Levine, Manuel Endres, John Preskill, Hsin-Yuan Huang, and Dolev Bluvstein, arXiv, March 2026 (15 pages).

[97] Heterogeneous architectures enable a 138× reduction in physical qubit requirements for fault-tolerant quantum computing under detailed accounting, by Pranav S. Mundada, Aleksei Khindanov, Yulun Wang, Claire L. Edmunds, Paul Coote, Michael J. Biercuk, Yuval Baum, and Michael Hush, arXiv, April 2026 (34 pages).

[98] Factoring 2048 bit RSA integers with a half-million-qubit modular atomic processor, by Tian Xue and Jacob P. Covey, arXiv, May 2026 (29 pages).

[99] The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption, by Long Finance, 2018 (60 pages).

[100] A Novel Hybrid Quantum Circuit for Integer Factorization: End-to-End Evaluation in Simulation and Real Quantum Hardware, by Jesse Van Griensven Thé, Victor Oliveira Santos, and Bahram Gharabaghi, Journal of Cybersecurity and Privacy, April 2026 (26 pages).

[101] The Quantum Countdown Quantum Computing And The Future Of Smart Ledger Encryption, by Long Finance, Long Finance, February 2018 (62 pages).

[102] The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime, by Mark Webber, Vincent Elfving, Sebastian Weidt, and Winfried K. Hensinger, AVS Quantum Science, January 2022.

[103] The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet, by Dong Pan, Gui-Lu Long, Liuguo Yin, Yu-Bo Sheng, Dong Ruan, Soon Xin Ng, Jianhua Lu, and Lajos Hanzo, IEEE Communications Surveys & Tutorials, February 2024 (52 pages).

[104] Committing to Quantum Resistance A Slow Defence for Bitcoin against a Fast Quantum Computing Attack, by I. Stewart et al., 2018 (18 pages).

[105] Blockchained Post-Quantum Signatures, by Chalkias Browny Hearnz, 2018 (8 pages).

[106] On the insecurity of quantum Bitcoin mining, by Or Sattath, arXiv, February 2019 (22 pages).

[107] Navigating the Quantum Computing Threat Landscape for Blockchains: A Comprehensive Survey, by Hassan Khodaiemehr, Khadijeh Bagheri, and Chen Feng, TechRxiv, September 2023 🔓 (preprint on Figshare).

[108] Kardashev scale Quantum Computing for Bitcoin Mining, by Pierre-Luc Dallaire-Demers and BTQ Technologies Team, arXiv, March 2026 (32 pages).

[109] The quantum threat to payment systems, by Michele Mosca of the University of Waterloo, 2017.

[110] Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations, by Ryan Babbush, Adam Zalcman, Craig Gidney, Michael Broughton, Tanuj Khattar, Hartmut Neven, Thiago Bergamaschi, Justin Drake, and Dan Boneh, PRX Quantum, August 2026.

[111] Reducing the Number of Qubits in Quantum Discrete Logarithms on Elliptic Curves, by Clémence Chevignard, Pierre-Alain Fouque, and André Schrottenloher, Cryptology ePrint Archive, February 2026 (34 pages) 🔓 (preprint on HAL).

[112] Optimized Point Addition Circuits for Elliptic Curve Discrete Logarithms, by André Schrottenloher, arXiv, June 2026 (19 pages).

[113] Space-Efficient Quantum Algorithm for Elliptic Curve Discrete Logarithms with Resource Estimation, by Han Luo, Ziyi Yang, Ziruo Wang, Yuexin Su, and Tongyang Li, arXiv, April 2026 (35 pages).

[114] Quantum Algorithm for Elliptic Curve Discrete Logarithms with Space-Efficient Point Addition, by Han Luo, Ziyi Yang, Jingquan Luo, Ziruo Wang, Yuexin Su, Xiaoming Sun, Lvzhou Li, and Tongyang Li, arXiv, August 2026 (46 pages).

[115] Brace for impact: ECDLP challenges for quantum cryptanalysis, by Pierre-Luc Dallaire-Demers, William Doyle, and Timothy Foo, arXiv, March 2026 (39 pages).

[116] Regev's reduction as a candidate quantum algorithm for the discrete logarithm problem in finite abelian groups, by M. Isabel Franco Garrido and André Chailloux, arXiv, May 2026 (31 pages).

[117] Strategies for quantum-enabled Bitcoin miners, by Zach Manson and Barry C. Sanders, arXiv:2607.23952, July 2026 (53 pages).

[118] On the Practicality of Quantum Sieving Algorithms for the Shortest Vector Problem, by Joao F. Doriguello, George Giapitzakis, Alessandro Luongo, and Aditya Morolia, Post-Quantum Cryptography – PQCrypto 2026, Lecture Notes in Computer Science, April 2026 (34 pages) 🔓 (preprint on arXiv).

This **Quantum computing threat** subsection contains 118 bibliographical references and notes containing at least 2,417 pages.

1.2 Post-quantum cryptography

Quantum Key Distribution (QKD) is not easily generalized because it requires a dedicated quantum channel between communicating endpoints or trusted nodes, most commonly an optical fiber or free-space optical link. Microwave QKD has been proposed for specialized settings [119], but it is not an easy replacement for ordinary smartphone 4G-5G-6G-WiFi radio access. QKD-derived keys can nevertheless be used by higher-layer mobile-network security when the operator infrastructure provides the required quantum links.

Cybersecurity therefore requires public-key cryptography that remains secure against the best known classical and quantum attacks. This does not require the underlying computational problem to be NP-complete or NP-hard. Security is instead expressed through explicit hardness assumptions and concrete attack costs. Shor's algorithm directly threatens RSA and elliptic-curve public-key cryptography, whereas Grover's algorithm provides a generic quadratic speedup for exhaustive search and therefore mainly affects symmetric-key and hash-function security margins. Post-quantum cryptography (PQC) is classical cryptography designed to remain secure against a cryptanalytically relevant quantum computer (CRQC). It is generally easier to deploy at Internet scale than QKD because it runs over ordinary communications infrastructures. QKD and PQC can nevertheless be combined. A useful combination is to authenticate the classical QKD channel with PQC signatures, or to combine QKD-derived and PQC-derived key material [120–123]. Sending a PQC public key over QKD is normally unnecessary because a public key does not require confidentiality. Different PQC schemes involve trade-offs in public-key, ciphertext and signature sizes, latency, throughput, memory and implementation complexity (Figure 20).

1.2.1 PQC timeline

Let's look at the PQC timeline of PQC standards definition and their adoption [124]:

- **1978**: **Robert McEliece** proposes his code-based public-key cryptosystem. It predates quantum computing and was not designed as a post-quantum scheme, but it later became one of the oldest public-key constructions still considered resistant to known quantum attacks.
- **2003**: the term "post quantum cryptography" (PQC) is created by **Daniel Bernstein** [125].
- **2006**: the first international **PQCrypto** workshop is held in Belgium to study cryptography that could replace quantum-vulnerable public-key systems such as RSA and ECC [126]. The 12-person program committee includes, among others, Louis Goubin from the University of Versailles and Phong Nguyen and Christopher Wolf from ENS. Four major historical PQC families are already represented: code-based cryptography, lattice-based cryptography, hash-based signatures and multivariate cryptography. Isogeny-based cryptography becomes prominent later. Two French researchers present two of these tracks: Nicolas Sendrier, from Inria, with "Post-quantum code-based cryptography", and Jacques Stern from ENS with "Post-quantum multivariate-quadratic public key schemes" [127]. These workshops have since been held every one to two years around the world. The 2024 edition was organized at the University of Oxford.
- **2012**: the **NIST** (National Institute of Standards and Technology) launches its first projects and a team on PQC.
- **2014**: the European Horizon 2020 PQCRYPTO project is approved at the end of 2014 and starts in March 2015. ETSI's Industry Specification Group on Quantum-Safe Cryptography is approved in February 2015.
- **2015**: **NIST** organizes its first PQC workshop. ETSI publishes a reference report on quantum-safe cryptography [16]. The NSA publicly begins advising a transition toward quantum-resistant public-key algorithms for National Security Systems [128]. The European PQCRYPTO project coordinated by Tanja Lange starts in March 2015 [129].
- **2016**: NIST publishes NISTIR 8105, Report on Post-Quantum Cryptography and launches the formal PQC standardization process at the end of the year.
- **2017**: the first NIST submission phase ends. NIST accepts 69 candidate algorithms out of 82 submissions, with many lattice-based and code-based proposals. In the same year, the 8th PQCrypto workshop is held in Utrecht, the Netherlands. NIST defines five security categories rather than key-size thresholds. Categories 1, 3 and 5 use attack costs comparable to exhaustive key search against AES-128, AES-192 and AES-256, while categories 2 and 4 use collision-search benchmarks based on 256-bit and 384-bit hash functions. Key, ciphertext and signature sizes vary independently with the scheme and parameter set [130].

Figure 16: NIST PQC selection in 2019.

- **2019**: on January 30, NIST selected 26 candidates to move to the second stage, including 17 candidates for public-key encryption or key-establishment and 9 for signatures [130–132]. These include three projects involving Worldline, which until 2019 was part of the Atos Group. For its part, Inria (France) was involved in 7 of the 26 selected projects (Figure 16).

- **2020**: NIST announces the third-round candidates in July, retaining 15 of the 26 second-round candidates [133]. Seven are designated finalists and eight are alternate candidates. "Alternate" does not mean lower quality. It identifies schemes that NIST considered worth continued study for reasons such as mathematical diversity, performance trade-offs or the possibility of later standardization. The Bit-Flipping Key Encapsulation (BIKE) is a code-based KEM. One reported Intel Arria 10 FPGA implementation required about 1.3 million clock cycles for decoding at 110 MHz, corresponding to roughly 12 ms.

  It must be noted that the NIST challenge embedded some constraints on intellectual property. NIST doesn't object to the contestants having some patents related to their submitted protocols. But they favor royalty-free ones and IP licensing without compensation, under reasonable terms (RAND) and conditions that are demonstrably free of unfair discrimination. While this could certainly accelerate their adoptions, this may indirectly favor large cybersecurity vendors who already have an existing customer base.

  Figure 17 and Figure 18 show the participating countries, research teams and vendor organizations for each project. Green identifies algorithms selected by NIST for standardization in July 2022. Red identifies Rainbow and SIKE, whose security was broken in 2022.

- **2022**: in May, US National Security Memorandum 10 directs federal agencies to inventory cryptographic systems vulnerable to a future cryptanalytically relevant quantum computer and to prepare for migration to quantum-resistant cryptography. The policy is subsequently expanded and amended rather than canceled. Executive Order 14306 of June 2025 retains PQC migration actions while modifying Executive Order 14144.

- **2022**: in July, NIST selects four algorithms for standardization, not yet four final standards: CRYSTALS-Kyber for key encapsulation, and CRYSTALS-Dilithium, Falcon and SPHINCS+ for digital signatures [134]. Falcon was selected in part because of its relatively compact signatures. SPHINCS+ provides a mathematically diverse hash-based alternative. Rainbow, one of the 2020 signature finalists, was practically broken before the July selection. A key-recovery attack on its lowest NIST security category required about 53 hours on a standard laptop [135]. In August 2022, SIDH/SIKE was broken by an efficient classical key-recovery attack, eliminating SIKE from consideration [3].

  In July 2022, the NIST NCCoE (National Cybersecurity Center of Excellence), was tasked with working alongside federal agencies and industry vendors to accelerate the transition to PQC. The vendors are AWS, Cisco, Crypto4A Technologies, Cryptosense, InfoSec Global, ISARA Corporation, Microsoft, Samsung SDS, SandboxAQ, Thales and VMware. These players will provide deployment recommendations and their own software and services solutions. Simultaneously, the CISA (Cybersecurity and Infrastructure Security Agency), a US federal agency within the DHS (Department of Homeland Security) announced the creation of a PQC initiative to assist other federal agencies in the deployment of PQCs. Many PQC and other security vendors were already offering implementations aligned with the selected candidates. In 2022 the algorithms were selected but not yet standardized, so conformance claims should be tied to the final FIPS versions published in August 2024. They provide some encapsulation mechanisms for third-party and/or open-source PQCs in their cybersecurity management tools.

  In September 2022, the NSA released its Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Cybersecurity Advisory, defining future quantum-resistant algorithm requirements and transition milestones for National Security Systems [136]. The suite selected CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium for digital signatures, subsequently standardized as ML-KEM and ML-DSA. The names are science-fiction references as Kyber crystals appear in Star Wars, including on Jedha in Rogue One, and Dilithium crystals are used in Star Trek fictional matter-antimatter propulsion systems.

- **2023**: cryptanalysis and implementation-security research continues across PQC families. Algebraic distinguishers and attacks are studied for structured code-based systems such as McEliece [137, 138]. Work on coherent Ising machines explores lattice problems but does not constitute a practical break of lattice-based PQC [139]. Side-channel attacks against CRYSTALS-Dilithium and CRYSTALS-Kyber target implementations and generally require physical or otherwise privileged access [140, 141]. In August

NIST finalists

	finalists	research teams	vendors teams
Public-Key Encryption/KEMs	Classic McEliece	**UK**: U. London, U. Plymouth. **Switzerland**: ETH Zurich. **USA**: U. Illinois & Chicago, U. Florida, Yale. **Europe**: U. Ruhr Bochum, U. Eindhoven, U. Southern, Denmark, MPI, Inria (France). **Taiwan**: Academia Sinica.	Google PQ Solutions PQShield
	ML-KEM CRYSTALS-KYBER	**USA**: SRI. **Canada**: U. Waterloo. **Europe**: Radboud U. Netherlands, U. Ruhr Bochum, ENS Lyon.	IBM Research Europe Arm, PQShield NXP Semiconductors
	NTRU	**Europe**: Radboud U Netherlands, Eindhoven U. **USA**: Brown U. **Canada**: U. Waterloo.	Qualcomm NTT Algorand, PQShield
	SABER	**Europe**: KU Leuven (Belgium). **UK**: Birmingham U.	
Digital Signatures	**ML-DSA** CRYSTALS-DILITHIUM	**USA**: Florida Atlantic U. **Switzerland**: ETH Zurich. **Europe**: CWI Netherlands, U. Ruhr Bochum, MPI, ENS Lyon.	IBM Research Europe Google, PQShield
	FN-DSA FALCON	**Europe**: ENS Paris, U. Rennes (France). **USA**: Brown U.	IBM Research PQShield, Qualcomm Ethereum Foundation Thales
	Rainbow	**Europe**: FAU Erlangen Nuremberg, U. Versailles. **USA**: Cincinnati U. **Taiwan**: Academia Sinica, National Taiwan U.	

Grey: 2020 selection
Green: 2022 selection
Red: broken in 2022

Figure 17: NIST finalists' selection in 2020. In green, algorithms selected for standardization in 2022. CRYSTALS-Kyber became ML-KEM in FIPS 203 and CRYSTALS-Dilithium became ML-DSA in FIPS 204, both finalized in August 2024. Falcon is being standardized as FN-DSA in FIPS 206. As of September 2026, FIPS 206 is still under development according to the NIST PQC project page. The frequently cited constant-time and floating-point implementation difficulty is an interpretation and not a NIST-stated cause. In red, broken PQC. © Olivier Ezratty, 2022-2026.

NIST alternate candidates

	finalists	research teams	vendors teams
Public-Key Encryption/KEMs	BIKE	**USA**: U. Washington, Florida U. **Europe**: U. Limoges, ENAC & U. Toulouse, Inria, U. Bordeaux (France), U. Ruhr Bochum (Germany). **Israel**: U. Haifa.	Intel Google IBM **Worldline France**
	FrodoKEM	**USA**: U. Michigan. Stanford U. **Netherlands**: CWI. **Canada**: U. Waterloo. **Middle-East**: Ege University (Turkey).	NXP Microsoft Research PQShield
	HQC	**France**: ISAE-Supaero, Limoges U., ENAC, U. Toulouse, Toulon U., Bordeaux U. **USA**: Florida U.	Worldline France and Netherlands
	NTRU Prime	**Taiwan**: Academia Sinica, National Taiwan U. **Australia**: U. Adelaide. **Europe**: Eindhoven U (Netherlands), Hamburg U. (Germany), Tampere U. (Finland). **USA**: Illinois U.	NXP
	SIKE	**USA**: Florida U. **Canada**: Waterloo U., Toronto U. **Europe**: Radboud U. Netherlands, U. Versailles (France).	evolutionQ Amazon Microsoft Research Infosec Global Texas Instruments
Digital Signatures	GeMSS	**France**: Inria, University of Versailles and Sorbonne Université.	CryptoNext Orange
	Picnic	**USA**: Northwestern U., GeorgiaTech, U. Maryland., Princeton U. **Europe**: Austrian Institute of Technology, TU Graz (Austria), Aarhus U. (Denmark), DTU (Denmark).	Microsoft Research Dfinity
	SLH-DSA SPHINCS+	**Europe**: U.Ruhr Bochum, KU Leuven, TU Graz, Eindhoven U, Radboud U.	Cisco, Infineon Infosec Global Genua, Taurus

Grey: 2020 selection
Green: 2022 selection
Red: broken in 2022

Figure 18: NIST alternate candidates' selection in 2020. In green, SPHINCS+, which NIST selected for standardization in 2022 and standardized as SLH-DSA in FIPS 205 in August 2024. In red, broken PQC. © Olivier Ezratty, 2022-2026.

2023, NIST publishes draft standards for three of the four algorithms selected in July 2022. In December 2023, the KyberSlash timing vulnerability is disclosed

in some CRYSTALS-Kyber implementations and is rapidly patched.

- **2024**: on April 17th, **Yilei Chen** publishes a preprint claiming a polynomial-time quantum algorithm with implications for Learning with Errors (LWE) [142, 143]. The claim is withdrawn almost immediately after Hongxun Wu and Thomas Vidick identify a fatal flaw in the argument. It therefore does not constitute an attack on CRYSTALS-Kyber.

  On August 13, 2024, NIST publishes three final standards: FIPS 203 for ML-KEM, the Module-Lattice-Based Key-Encapsulation Mechanism derived from CRYSTALS-Kyber, FIPS 204 for ML-DSA, the Module-Lattice-Based Digital Signature Algorithm derived from CRYSTALS-Dilithium, and FIPS 205 for SLH-DSA, the Stateless Hash-Based Digital Signature Algorithm derived from SPHINCS+. Falcon is also selected and is being standardized separately as FN-DSA in FIPS 206. In October 2024, NIST advances 14 additional digital-signature candidates from 40 first-round candidates to a second evaluation round [144].

- **2025**: deployment shifts from algorithm selection to migration and implementation of the three standards finalized in 2024. In March, NIST selects the code-based HQC KEM as a backup to ML-KEM, providing mathematical diversity. NIST expects the HQC final standard in 2027. NIST HQC selection.

  In February 2025, ETSI publishes TS 104 015, "Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies". The specification describes a framework for hybrid pre-quantum and post-quantum key encapsulation with access-control policies, allowing encapsulated keys to be recovered only by users whose attributes satisfy the policy. ETSI TS 104 015.

  Deployment will take years because organizations must first discover where vulnerable public-key cryptography is used, define crypto-agility and migration plans, update products and protocols, and coordinate suppliers. The UK's NCSC gives concrete milestones: complete discovery and an initial plan by 2028, migrate the highest-priority systems by 2031, and complete migration across systems, services and products by 2035 [145, 146]. NCSC PQC migration timelines.

  In February 2025, the EU launched the 2-year project PQC4eMRTD (Post-Quantum Cryptography for electronic Machine-Readable Travel Documents) to secure future EU electronic passports with a PQC. The involved industry vendors are Infineon, Thales and CryptoNext Security.

- **2026**: the direction of policy is toward faster migration, not postponement. In May, NIST advances nine additional digital-signature candidates to round 3, expected to last about two years. HAWK is withdrawn in July after disclosure of a mathematical vulnerability, leaving eight active candidates in that group.

  On June 22, US Executive Order 14412 accelerates federal PQC migration. It requires high-value assets and high-impact federal systems to use PQC for key establishment by December 31, 2030 and for digital signatures by December 31, 2031. NIST additional signatures round 3. US Executive Order 14412.

- **2027**: NIST currently expects to finalize the HQC backup KEM standard. FN-DSA, derived from Falcon, remains under development in FIPS 206 as of September 2026, without a firm NIST publication date.

China is a particular case. Its large-scale QKD deployments have been visible since 2016, including fiber and satellite links, but PQC is still needed for endpoints and devices that cannot be served directly by QKD. China Telecom tested a hybrid QKD+PQC platform in 2025 to secure phone communications over more than 1,000 km, with PQC at the endpoints and QKD in the operator backbone [147]. China is also developing domestic PQC standards rather than simply adopting NIST or ETSI choices. On February 5, 2025, China's Institute of Commercial Cryptography Standards (ICCS) launched the Next-generation Commercial Cryptographic Algorithms Program (NGCC) and requested public comments on draft submission and evaluation criteria for public-key algorithms. The formal call for public-key algorithm proposals opened on October 9, 2025, with submissions and updates extending into 2026. This is broadly analogous to the call-for-proposals stage of NIST's process, while benefiting from a decade of NIST standardization and public cryptanalysis experience.

1.2.2 PQC protocols

PQC has historically been organized into several major algorithm families. The five families introduced below are useful for understanding the field, but they are not an exhaustive modern taxonomy and not all remain viable for general-purpose standardization [149].

Code-based cryptography

The McEliece cryptosystem was introduced in 1978 by **Robert McEliece**, long before Shor's algorithm. Its security has resisted decades of classical and quantum cryptanalysis for appropriately chosen parameters, although research continues to improve attacks and distinguishers. In the classic construction, a binary message vector of length k is encoded with a public generator matrix associated with a disguised binary Goppa code, producing a codeword of length n (Figure 21).

Encryption adds a random error vector of prescribed Hamming weight t to the encoded codeword. The Hamming weight is the number of nonzero bits in that error vector. The public key contains a representation of the disguised code, together with public parameters that determine the error weight. The secret key contains the

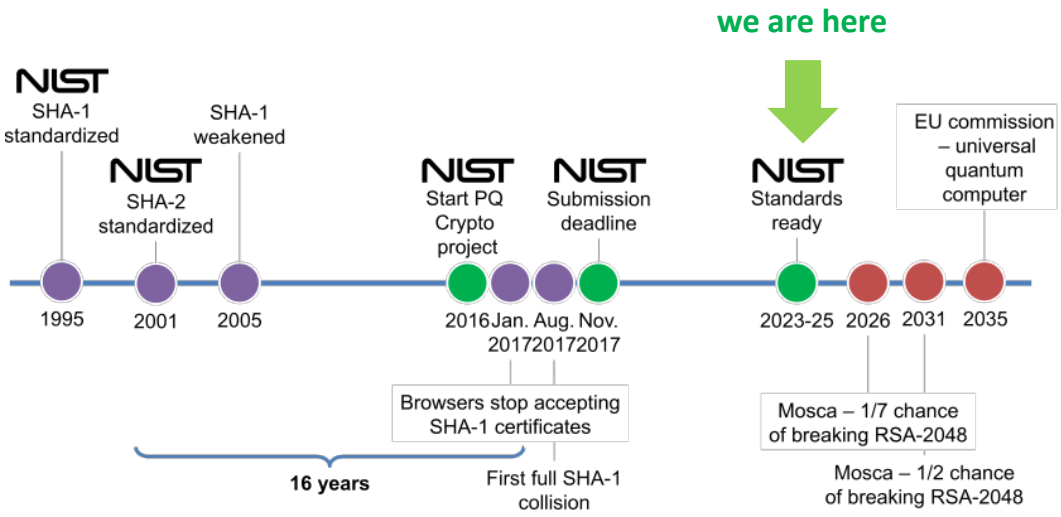


Figure 19: NIST PQC standardization planning as of 2019. NIST finalized three PQC standards in August 2024. Source: [148]. The Mosca probabilities shown here are historical forecasts. The 2019 estimate of a 1/7 chance of breaking RSA-2048 by 2026 had not materialized by 2026.

Table 2 - Comparison on encryption schemes (RSA decryption = 1, size in bits, k security strength)

Algorithm	*KeyGen (time compared to RSA decrypt)*	*Decryption (time compared to RSA decrypt)*	*Encryption (time compared to RSA decrypt)*	*PubKey (key size in bits to achieve 128 bits of security)*	*PrivateKey (key size in bits to achieve 128 bits of security*	*Cipher text (size of resulting cipher text)*	*Time Scaling*	*Key Scaling*
NTRU	*5*	*0.05*	*0.05*	*4939*	*1398*	*4939*	k^2	*k*
McEliece	*2*	*0.5*	*0.01*	*1537536*	*64861*	*2860*	k^2	k^2
Quasi-Cyclic MDPC McEliece	*5*	*0.5*	*0.1*	*9857*	*19714*	*19714*	k^2	*k*
RSA	*50*	*1*	*0.01*	*3072*	*24,576*	*3072*	k^6	k^3
DH	*0.2*	*0.2*	*0.2*	*3072*	*3238*	*3072*	k^4	k^3
ECDH	*0.05*	*0.05*	*0.05*	*256*	*256*	*512*	k^2	*k*

Note: in key scaling, the factor log k is omitted.

Figure 20: Historical 2015 comparison of key sizes for several cryptographic schemes. The parameter sets predate the final NIST PQC standards. Source: Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges, ETSI, 2015 (64 pages).

hidden algebraic structure that makes efficient decoding possible.

A common textbook description writes the public generator matrix as a scrambled version of a private Goppa-code generator matrix using an invertible scrambling matrix and a permutation matrix. This is useful intuition, but decryption is not performed by inverting the non-square generator matrix. It uses the private Goppa-code trapdoor and an efficient decoding algorithm to correct up to the designed number of errors, followed by reversal of the secret transformations.

The main practical drawback of Classic McEliece is its large public key. Current parameter sets have public keys from about 261 kB to 1.36 MB, while ciphertexts remain very small, about 96 to 208 bytes. This is orders of magnitude larger in public-key storage than RSA-2048, but code-based encapsulation and decapsulation can be fast and can also be accelerated in dedicated hardware [150].

The generic syndrome-decoding problem for linear codes is NP-complete [151], but this does not by itself prove that recovering a key or plaintext from a structured McEliece instance is NP-hard. Concrete security is as-

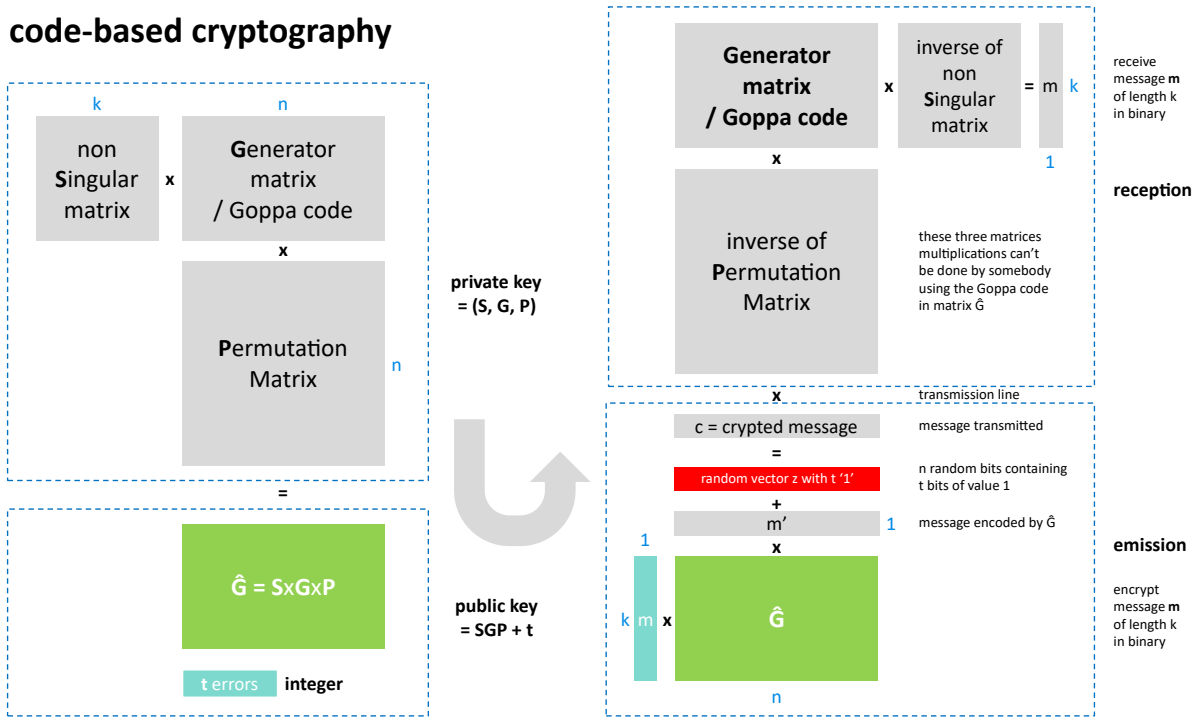


Figure 21: Simplified textbook view of McEliece code-based cryptography. The figure illustrates code scrambling and error injection, but a modern Classic McEliece implementation should be understood in terms of a hidden binary Goppa-code decoding trapdoor rather than inversion of the non-square generator matrix. Ⓒ Olivier Ezratty, from various sources. 2021.

sessed against the best known attacks on the selected Goppa-code parameters [152–154]. Large public keys are a performance trade-off rather than a proof of post-quantum security.

Lattice-based cryptography

Modern lattice-based cryptography builds on work by Miklós Ajtai in the 1990s and on Oded Regev's 2005 Learning With Errors (LWE) construction [155]. A lattice is a discrete set of points generated by integer combinations of basis vectors. LWE does not encrypt by simply choosing the nearest point in a two-dimensional lattice diagram. Instead, an attacker sees many noisy linear equations modulo an integer. The legitimate party knows a secret vector that makes the small error recoverable, while recovering the secret from the noisy samples is believed to be computationally hard. Figure 22 provides geometric intuition for lattices.

The security of LWE-based cryptography is supported by reductions connecting average-case LWE instances to worst-case lattice problems under specified approximation factors [155]. This is a stronger and more precise statement than saying that "decryption is NP-complete". Efficient structured-lattice constructions such as NTRU and later module-lattice schemes substantially improved practical performance and key sizes [156–158]. Patent status depends on the specific construction and is not a defining property of lattice-based cryptography.

The **NewHope** Ring-LWE key-exchange scheme was experimentally deployed by **Google** in Chrome in 2016 as part of CECPQ1. Later CECPQ experiments tested other post-quantum and hybrid constructions, including NTRU-HRSS variants [159, 160]. These experiments were important deployment precursors, but the NIST general-purpose KEM standardized in 2024 is ML-KEM, derived from CRYSTALS-Kyber.

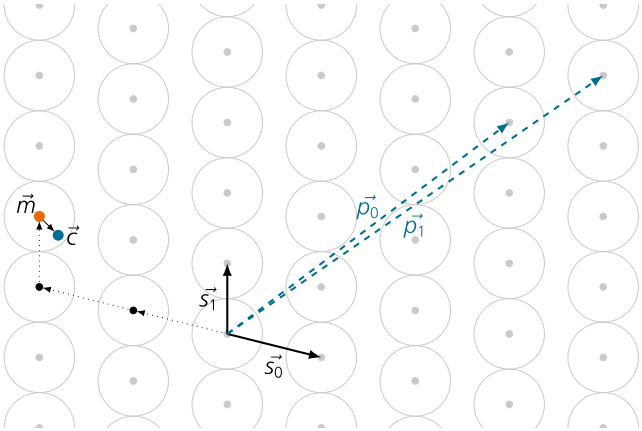


Figure 22: Geometric intuition for a lattice. This is not a literal representation of LWE or ML-KEM key generation. Source: [161].

In France, teams including IRISA and EMSEC have contributed to lattice-based cryptography. The standard mathematical term is "lattice", not "Euclidean network".

Damien Stehlé is a specialist in lattice cryptography at ENS Lyon and was a coauthor of CRYSTALS-Kyber. Kyber was a NIST finalist in 2020, was selected for

standardization in 2022 and became ML-KEM in FIPS 203 in 2024.

Isogeny-based cryptography

Isogeny-based cryptography uses algebraic maps called isogenies between elliptic curves. An isogeny is a non-constant morphism of elliptic curves that also preserves the group structure. Early ordinary-isogeny constructions motivated quantum cryptanalysis, and later work explored supersingular curves, including Supersingular Isogeny Diffie–Hellman (SIDH) [162–165]. This family was attractive because of its very small keys, but SIDH and its SIKE KEM were subsequently broken by efficient classical attacks in 2022.

Cloudflare's open-source CIRCL library, the Cloudflare Interoperable Reusable Cryptographic Library, has implemented several post-quantum constructions and historically included SIKE experiments. SIKE was submitted to the NIST process before its 2022 break.

In January 2019, SIKE was among the 17 second-round public-key encryption and KEM candidates, not yet a finalist [166, 167]. In 2022, Castryck and Decru demonstrated an efficient classical key-recovery attack on SIDH, with practical attacks on the NIST SIKE parameter sets. The peer-reviewed attack was published at EUROCRYPT 2023 [3].

Hash-based signatures

Hash-based signatures also predate quantum computing. They build on **Leslie Lamport**'s 1979 one-time signatures and on Merkle trees that authenticate many one-time or few-time signing keys (Figure 23). Their security relies primarily on well-studied hash-function properties. Modern hash-based schemes can have compact public keys but comparatively large signatures and slower signing, in exchange for conservative security assumptions. NIST standardized the stateless SPHINCS+-derived SLH-DSA in FIPS 205 [168–170].

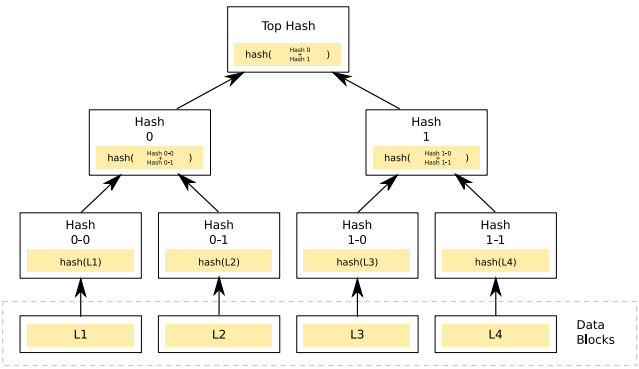


Figure 23: A binary hash tree, or Merkle tree. Source: Merkle tree[W], Wikipedia, CC BY-SA, accessed September 2026.

There are however also proposals to implement forms of quantum hash [171].

Multivariate polynomial cryptography

Multivariate public-key cryptography is based on systems of multivariate polynomial equations over finite fields, most commonly quadratic equations. A typical trapdoor construction hides a structured central quadratic map between secret affine transformations. The public key is the resulting system of quadratic polynomials, while the private key contains the hidden structure and transformations needed to invert it efficiently (Figure 24).

Solving generic systems of multivariate quadratic equations is computationally hard and related decision problems are NP-hard, but this does not prove that every multivariate cryptosystem is NP-hard to break. Cryptanalytic attacks exploit the additional algebraic structure of particular schemes. Multivariate public-key proposals predate 2009, and Rainbow itself was proposed in the mid-2000s.

Many multivariate proposals have relatively large public keys and have primarily targeted digital signatures rather than general-purpose encryption. Key and signature sizes vary widely across constructions.

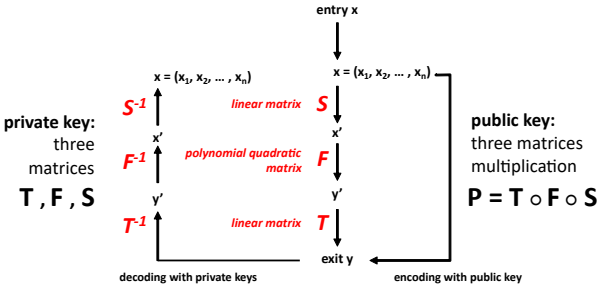


Figure 24: Multivariate polynomial cryptography. Source: Olivier Ezratty, reconstructed from other sources.

Rainbow, selected by NIST as a signature finalist in 2020, belongs to this family. Beullens' 2022 attack made secret-key recovery practical for the lowest NIST security category, requiring about 53 hours on a standard laptop in the reported experiment [135].

QKD and PQC solve partly different problems and can be combined. QKD distributes symmetric key material over a quantum channel but still requires an authenticated classical channel. PQC provides KEMs and digital signatures over ordinary networks. Because public keys do not require confidentiality, transporting a PQC public key through QKD normally adds little. A more natural hybrid uses PQC signatures to authenticate QKD classical messages, as demonstrated experimentally [120], or combines independently derived QKD and PQC secrets. When PQC alone already supplies key establishment, a parallel QKD key-establishment layer can be redundant unless the architecture explicitly seeks defense in depth [172].

1.2.3 PQC and blockchains

PQC can protect blockchain transaction authorization by replacing quantum-vulnerable public-key signatures with quantum-resistant signatures, with trade-offs in key size, signature size, verification cost and protocol compatibility [173]. Research prototypes and experimental quantum-resistant blockchains have been proposed [174]. Some work also combines PQC and QKD in Industry 4.0 and IoT architectures [175].

Such a proposal was made in 2023 by LACChain, Quantinuum and Tecnologico de Monterrey. LACChain is a blockchain infrastructure from the Innovation Lab of the Inter-American Development Bank, IDB Lab, built with the Hyperledger Besu Ethereum client [176]. The project uses Falcon-512 digital signatures in X.509 certificates. Falcon was one of the four algorithms selected by NIST for standardization in July 2022. It also uses the Quantinuum Quantum Origin entropy service, whose randomness source is based on quantum-computer measurements.

Bitcoin PQC migration. Concrete Bitcoin migration proposals appeared before 2026 and became more visible in 2026. BIP-360 was assigned in December 2024 and renamed Pay-to-Merkle-Root (P2MR) in February 2026. It proposes a Taproot-like output without the quantum-vulnerable key-path spend, reducing persistent exposure of public keys. BIP-361 was assigned in February 2026 and proposes a staged sunset of quantum-vulnerable signature paths after a post-quantum output mechanism exists. Both BIPs remain drafts as of September 2026 and are not Bitcoin consensus rules. Galaxy Digital committed up to $5M in July 2026 to a "Bitcoin Quantum Readiness Initiative" for developer grants, post-quantum signature integration, wallet migration tooling and security audits. The migration challenge is both technical and organizational. Post-quantum signatures are typically kilobyte-scale rather than the tens-of-bytes scale of current Bitcoin signatures, so naive substitution would increase transaction weight, fees and bandwidth.

A tooling market is forming around blockchain migration. In 2026, 01 Quantum and qLABS announced a Layer 1 migration toolkit for smart-contract chains using dual legacy and post-quantum signatures and zero-knowledge techniques. Postquant Labs announced the Quip.Network testnet with a post-quantum wallet layer and a separate proof-of-useful-work concept involving annealers, CPUs and GPUs. The latter is not a substitute for quantum-resistant transaction signatures and, without a published security reduction, should be treated as an experimental consensus proposal. Project Eleven has pursued readiness assessments and wallet-recovery concepts with the Solana ecosystem.

BTQ Technologies

Taiwan-Canada, 2021

BTQ Technologies is a company led by Olivier Roussy Newton (CEO) that develops post-quantum cryptography and blockchain-security technologies. The listed Canadian company was formerly Sonora Gold & Silver Corp and acquired BTQ AG in 2023. BTQ AG had been incorporated in Liechtenstein in 2021. The transaction provided the route for the operating business to become publicly listed. BTQ Technologies is traded on Nasdaq.

Their product line contains PQScale (an efficient quantum resistant blockchain scaling technique based on Falcon signatures) and Kenting, with specialized hardware for zero-knowledge provers.

The company has also patented a method at the USPTO to "*secure transmission of confidential information between entities using private cryptographic keys generated from a random vector shared between the entities*". It has proposed coarse-grained boson sampling, or CGBS, for a proof-of-work consensus scheme [177]. In January 2026, BTQ launched its experimental Bitcoin Quantum testnet, replacing ECDSA with NIST-standardized ML-DSA in that fork. The company reported support for draft BIP-360-style transactions on its testnet in March 2026. A resource-estimate paper involving BTQ and Pauli Group concluded that Grover-accelerated Bitcoin mining would require a vastly larger quantum computer than signature attacks, by more than fifteen orders of magnitude in the paper's qubit-count comparison [108].

In October 2023, BTQ announced a partnership with ITRI in Taiwan to develop a security chip using its QCIM, Quantum Computation in Memory, technology for cryptographic key generation and computation with CRYSTALS-Kyber, subsequently standardized as ML-KEM. In July 2024, the company announced a partnership with ID Quantique around QRNG and PQC [178].

In January 2025, they made the acquisition of the Cimtech Technology IP, from a company specialized in the field of in-memory computing, which is supposed to help them develop their PQC solutions, mainly by reducing energy consumption. Their goal is to reduce the energetic footprint of Bitcoin mining and proof-of-work and proof-of-stake blockchain protocols. Consequently, in 2025, they launched various investigative projects with QPerfect (in cold-atom quantum computing), Quandela (on boson sampling [179]) and with the University of Cambridge Integrated Quantum Photonics team (for the development of a quantum-photonics solution).

ChainMaker

China

ChainMaker, *aka* Chang'an Chain, announced in 2021 a 96-core blockchain accelerator chip reported to process up to 100,000 transactions per second for signature verification and smart-contract workloads.

In 2023, ChainMaker developers reported an aggregate benchmark of 240 million transactions per second across a 1,000-server cluster. This aggregate laboratory figure is not directly comparable with the end-to-end consensus throughput of a single public blockchain. ChainMaker reported integrating post-quantum digital signatures into its open-source blockchain stack in 2022, in work involving Tsinghua University, Beihang University, Tencent and Baidu.

1.2.4 Commercial offering

Now that the first NIST PQC standards are final, cybersecurity vendors are integrating them into software, hardware and services. Relevant secure protocol stacks include TLS, SSH, IPsec, IKE, VPNs, DNSSEC, S/MIME and authentication layers used with messaging and application protocols [180, 181]. PQC is also appearing in business computers [182], defense systems [183], hardware security modules [184], silicon IP [185, 186], payment and PKI services [187], and embedded or IoT products. Migration is challenging because larger keys, ciphertexts and signatures affect protocol messages, certificates, hardware roots of trust, constrained devices and network middleboxes. SSL itself is obsolete, while DHCP, FTP and SMTP are not cryptographic algorithms and require migration of the security mechanisms layered around them.

There is a wealth of startups in that space, covered in the vendors section of this part. The date of a cryptanalytically relevant quantum computer remains uncertain, but migration should not be postponed until such a machine is imminent. Organizations should prioritize systems with long migration cycles, long-lived roots of trust, high-value assets and data whose confidentiality must survive long enough to be exposed to "harvest now, decrypt later" attacks [188]. NIST's current guidance is that migration should begin now, while national roadmaps typically extend into the early-to-mid 2030s.

Established companies are also involved. In September 2023, the **PQC Coalition** was created by Microsoft, IBM Quantum, MITRE, PQShield, SandboxAQ and the University of Waterloo to accelerate standardization and adoption of PQC in commercial and open-source technologies.

IBM announced in August 2019 a prototype for long-term archiving on magnetic tape using quantum-resistant cryptography [189]. The cryptography was lattice-based. Long-term archives create a particular migration problem because encrypted data and the software, metadata and keys needed to interpret it may have to remain usable for decades. IBM has also participated in NIST PQC submissions. In October 2024, IBM introduced Guardium Quantum Safe as part of its Guardium Data Security Center portfolio to help discover cryptographic usage and support migration planning [190].

In February 2024, **Apple** introduced PQ3 for iMessage. PQ3 combines classical elliptic-curve cryptography with CRYSTALS-Kyber key encapsulation, using Kyber for post-quantum key establishment and rekeying. Kyber is a KEM, not a signature scheme [191].

Zoom added post-quantum end-to-end encryption in May 2024 using Kyber-768 for key establishment in Zoom Workplace [192].

1.2.5 PQC energy consumption

PQC deployment spans servers, clouds, laptops, smartphones and embedded devices. Its energy impact cannot be reduced to a universal multiplicative penalty. It depends strongly on the algorithm, parameter set, operation, implementation, hardware and network protocol. Saarinen's 2020 measurements on a 96 MHz Cortex-M4 illustrate this spread. Kyber768 consumed about 0.77 mJ for key generation, 0.92 mJ for encapsulation and 0.88 mJ for decapsulation, versus about 3.66 mJ, 7.27 mJ and 3.66 mJ for the corresponding secp256r1 ECDH operations. By contrast, Falcon-1024 key generation consumed about 233 mJ, around $\times 65$ the ECDSA-secp256r1 key-generation energy, while Falcon-1024 verification consumed about 0.69 mJ, roughly six times less than ECDSA verification on the same platform [193]. These are measurements of 2020 candidate implementations, not universal constants. Larger public keys, ciphertexts or signatures can also increase communication energy even when the local computation is efficient. FPGA and embedded-device measurements likewise show strong scheme- and platform-dependence [194–196].

Should we worry about this? The relevant quantity is energy per completed security service, including key generation or encapsulation, decapsulation, signature generation, verification, certificate transfer, handshake retransmissions and network traffic. For many consumer workloads, public-key operations occupy only a small fraction of total device energy, but this cannot be assumed for high-rate authentication, constrained IoT nodes, large certificate infrastructures or network services processing very large numbers of handshakes.

1.2.6 Bibliography and notes

These are the bibliographical references and notes for the **Post-Quantum Cryptography** subsection.

[3] An Efficient Key Recovery Attack on SIDH, by Wouter Castryck and Thomas Decru, Advances in Cryptology – EUROCRYPT 2023, Lecture Notes in Computer Science, April 2023 (25 pages) (preprint on lirias.kuleuven.be).

[16] Quantum Safe Cryptography and Security, by Matthew Campagna, June 2015 (64 pages).

[108] Kardashev scale Quantum Computing for Bitcoin Mining, by Pierre-Luc Dallaire-Demers and BTQ Technologies Team, arXiv, March 2026 (32 pages).

[119] Wireless Microwave Quantum Communication, by Tasio Gonzalez-Raya, arXiv, January 2024 (226 pages).

[120] Experimental authentication of quantum key distribution with post-quantum cryptography, by Liu-Jun Wang, Jian-Wei Pan, et al., npj Quantum Information, May 2021.

[121] Towards efficient and secure quantum-classical communication networks, by Pei Zeng, Debayan Bandyopadhyay, José A. Méndez Méndez, Nolan Bitner, Alexander Kolar, Michael T. Solomon, F. Joseph Heremans, David D. Awschalom, Liang Jiang, and Junyu Liu, arXiv, November 2024 (4 pages).

[122] Practical hybrid PQC-QKD protocols with enhanced security and performance, by Pei Zeng, Debayan Bandyopadhyay, José A. Méndez Méndez, Nolan Bitner, Alexander Kolar, Michael T. Solomon, Ziyu Ye, Filip Rozpędek, Tian Zhong, F. Joseph Heremans, David D. Awschalom, Liang Jiang, and Junyu Liu, arXiv, November 2024 (6 pages).

[123] On Post-Quantum Cryptography Authentication for Quantum Key Distribution, by Juan Antonio Vieira Giestinhas and Timothy Spiller, arXiv, July 2025 (63 pages).

[124] Quantum cryptanalysis - the catastrophe we know and don't know, by Tanja Lange, 2017 (33 slides).

[125] Post-Quantum Cryptography, by Daniel Bernstein et al., 2009 (254 pages).

[126] PQCrypto 2006 International Workshop on Post-Quantum Cryptography, by PQCrypto, May 2006 (254 pages).

[127] Quantum Computing and Cryptography Today, by Travis L. Swaim, (22 pages).

[128] Commercial national security algorithm suite and quantum computing FAQ IAD, by NSA, January 2016 (11 pages).

[129] Post-Quantum Cryptography for Long-Term Security, by Technische Universiteit Eindhoven, March 2015 (10 pages).

[130] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, by NIST, 2019 (27 pages).

[131] NIST Post-Quantum Cryptography - A Hardware Evaluation Study, by Kanad Basu, Deepraj Soni, Mohammed Nabeel, and Ramesh Karri, 2019 (16 pages).

[132] Recent Developments in Post Quantum Cryptography, by Tsuyoshi Takagi, November 2018 (38 slides).

[133] PQC Standardization Process: Third Round Candidate Announcement, by NIST, July 2020.

[134] NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, by NIST, July 2022.

[135] Breaking Rainbow Takes a Weekend on a Laptop, by Ward Beullens, Advances in Cryptology - CRYPTO 2022, August 2022 (16 pages).

[136] Announcing the Commercial National Security Algorithm Suite 2.0, by NSA, September 2022 (10 pages).

[137] A New Approach Based on Quadratic Forms to Attack the McEliece Cryptosystem, by Alain Couvreur, Rocco Mora, and Jean-Pierre Tillich, Advances in Cryptology - ASIACRYPT 2023, Lecture Notes in Computer Science, pages 3–38, December 2023 (36 pages).

[138] The syzygy Distinguisher, by Hugues Randriambololona, SpringerLink, April 2025 (30 pages) (preprint on arXiv).

[139] Quantum algorithmic solutions to the shortest vector problem on simulated coherent Ising machines, by Edmund Dable-Heath, Laura Casas, Victor Hertz, Christian Porter, Florian Mintert, and Cong Ling, arXiv, January 2025 (15 pages).

[140] Exploiting Intermediate Value Leakage in Dilithium: A Template-Based Approach, by Alexandre Berzati, July 2023 (23 pages).

[141] Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste, by Elena Dubrova et al., March 2023 (22 pages) (preprint on urn.kb.se).

[142] Quantum Algorithms for Lattice Problems, by Yilei Chen, April 2024 (64 pages).

[143] That IACR preprint, by Scott Aaronson, April 2024.

[144] Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process, by NIST, October 2024 (30 pages).

[145] Preparing for the Post Quantum Era: Quantum Ready Architecture for Security and Risk Management (QUASAR) – A Strategic Framework for Cybersecurity, by Abraham Itzhak Weinberg, arXiv, May 2025 (63 pages).

[146] The PQC Migration Handbook, by TNO, TNO, December 2024 (117 pages).

[147] China Telecom Launches Hybrid Quantum-Safe Encryption System, Completes 1,000-Kilometer Secure Call, by Matt Swayne, The Quantum Insider, May 2025.

[148] Introduction to post-quantum cryptography and learning with errors, by Douglas Stebila, 2018 (106 slides).

[149] A Guide to Post-Quantum Cryptography, by Ben Perez, October 2018.

[150] Code-Based Cryptography for FPGAs, by Ruben Niederhagen, 2018 (73 slides).

[151] On the inherent intractability of certain coding problems, by Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. van Tilborg, IEEE Transactions on Information Theory, volume 24, issue 3, pages 384–386, May 1978 (3 pages).

[152] Code-Based Cryptography, by Tanja Lange, 2016 (38 slides).

[153] Code Based Cryptography, by Alain Couvreur, 2018 (122 slides).

[154] Some Notes on Code-Based Cryptography, by Carl Löndahl, 2014 (192 pages).

[155] On lattices, learning with errors, random linear codes, and cryptography, by Oded Regev, Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC 2005), May 2005 (10 pages).

[156] Lattice-based cryptography: a practical implementation, by Michael Rose, 2011 (103 pages).

[157] Lattice-based Cryptography, by Daniele Micciancio et al., 2008 (33 pages).

[158] Overview of Lattice based Cryptography from Geometric, by Leo Ducas, 2017 (53 slides).

[159] Experimenting with Post-Quantum Cryptography, by Matt Braithwaite, July 2016.

[160] Google starts CECPQ2, a new postquantum key exchange for TLS, by Feisty Duck, January 2019.

[161] Practical Post-Quantum Cryptography, by Ruben Niederhagen et al., 2017 (31 pages).

[162] 20 years of isogeny-based cryptography, by Luca De Feo, 2017 (84 slides).

[163] An introduction to supersingular isogeny-based cryptography, by Craig Costello, 2017 (78 slides).

[164] Isogeny Graphs in Cryptography, by Luca De Feo, 2018 (73 slides).

[165] An introduction to isogeny-based crypto, by Chloe Martindale, 2017 (78 slides).

[166] Cloudflare wants to protect the internet from quantum computing, by Christine Fisher, Engadget, June 2019.

[167] Introducing CIRCL: An Advanced Cryptographic Library, by CloudFlare, June 2019.

[168] Hash-based Signatures: An Outline for a New Standard, by Andreas Hülsing et al., 2015 (12 pages).

[169] Design and implementation of a post-quantum hash-based cryptographic signature scheme, by Guillaume Endignoux, 2017 (102 pages).

[170] SPHINCS: practical stateless hash-based signatures, by SPHINCS, 2015 (30 pages).

[171] Fully Quantum Hash Function, by Shreya Banerjee, Harshita Meena, Somanath Tripathy, and Prasanta K. Panigrahi, arXiv, August 2024 (10 pages).

[172] Post-quantum cryptography - dealing with the fallout of physics success, by Daniel Bernstein and Tania Lange, 2017 (20 pages).

[173] A Survey and Comparison of Post-quantum and Quantum Blockchains, by Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto Di Pietro, and Aiman Erbad, arXiv, September 2024 (39 pages).

[174] From Portfolio Optimization to Quantum Blockchain and Security: A Systematic Review of Quantum Computing in Finance, by Abha Naik, Esra Yeniaras, Gerhard Hellstern, Grishma Prasad, and Sanjay Kumar Lalta Prasad Vishwakarma, arXiv, June 2023 (64 pages).

[175] A Blockchain-based Quantum Binary Voting for Decentralized IoT Towards Industry 5.0, by Utkarsh Azad, Bikash K. Behera, Houbing Song, and Ahmed Farouk, arXiv, March 2025 (9 pages).

[176] Quantum-resistance in blockchain networks, by Marcos Allende, Diego López León, Sergio Cerón, Adrián Pareja, Erick Pacheco, Antonio Leal, Marcelo Da Silva, Alejandro Pardo, Duncan Jones, David J. Worrall, Ben Merriman, Jonathan Gilmore, Nick Kitchener, and Salvador E. Venegas-Andraca, Scientific Reports, April 2023.

[177] Proof-of-work consensus by quantum sampling, by Deepesh Singh, Gopikrishnan Muraleedharan, Boxiang Fu, Chen-Mou Cheng, Nicolas Roussy Newton, Peter P. Rohde, and Gavin K. Brennen, arXiv, September 2024 (24 pages).

[178] BTQ And ID Quantique Sign MOU to Develop Authentication Systems, by Matt Swayne, The Quantum Insider, August 2024.

[179] Proof-of-work consensus by quantum sampling, by Deepesh Singh, Gavin K Brennen, et al., Quantum Science and Technology, February 2025 (31 pages).

[180] Sparkle tests VPN protected with quantum encryption, by Saf Malik, May 2024.

[181] Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways, by Jakub Sowa, Bach Hoang, Advaith Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, and Phuong Cao, arXiv, August 2024 (12 pages).

[182] HP Launches World's First Business PCs to Protect Firmware Against Quantum Computer Hacks, by HP, March 2024.

[183] Secure Drones for Defense and Public Safety Applications, by Novuslight, December 2023.

[184] Thales and Quantinuum Launch Starter Kit to help Enterprises prepare for Post-Quantum Cryptography, by Thales Group, January 2024.

[185] Rambus Protects Data Center Infrastructure with Quantum Safe Engine IP, by Rambus, December 2023.

[186] Getting Ready For The Quantum Computing Era: Thoughts On Hybrid Cryptography, by Bart Stevens, Semiconductor Engineering, July 2024.

[187] Entrust Introduces First Commercially Available "Post Quantum Ready" PKI platform, by Entrust, January 2024.

[188] Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective, by Javier Oliva del Moral, Antonio deMarti iOlius, Gerard Vidal, Pedro M. Crespo, and Josu Etxezarreta Martinez, arXiv, June 2024 (27 pages).

[189] IBM's quantum-resistant magnetic tape storage is not actually snake oil, by Kevin Coldewey in TechCrunch, TechCrunch, August 2019.

[190] IBM Guardium Data Protection, by IBM, October 2024.

[191] iMessage with PQ3: The new state of the art in quantum-secure messaging at scale, by Apple Security Research, February 2024.

[192] Zoom bolsters security offering with the inclusion of post-quantum end-to-end encryption in Zoom Workplace, by Bridget Moriarty, May 2024.

[193] Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards, by Markku-Juhani O. Saarinen, 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pages 23–30, August 2020 (8 pages) 🔓 (preprint on arXiv).

[194] FPGA Energy Consumption of Post-Quantum Cryptography, by Luke Beckwith et al., 2022 (10 pages).

[195] Energy Consumption Framework and Analysis of Post-Quantum Key-Generation on Embedded Devices, by J. Cameron Patterson, William J. Buchanan, and Callum Turino, Journal of Cybersecurity and Privacy, July 2025 🔓 (preprint on doi.org).

[196] Energy Consumption Evaluation of Post-Quantum TLS 1.3 for Resource-Constrained Embedded Devices, by George Tasopoulos et al., Cryptology ePrint Archive, April 2023.

This **Post-Quantum Cryptography** subsection contains 81 bibliographical references and notes containing at least 2,210 pages.

1.3 Quantum Random Number Generators

Quantum, post-quantum and traditional cryptographic systems all need high-quality randomness for key generation and for protocol values such as nonces, salts and challenges. In practical cryptographic systems, a physical entropy source commonly seeds a deterministic cryptographically secure pseudorandom number generator (CSPRNG), also called a deterministic random bit generator (DRBG). A QRNG is one possible physical entropy source. Its specific advantage is that its entropy model can be tied to quantum measurement statistics and, for some protocols, accompanied by a quantitative or device-independent randomness certificate [197].

1.3.1 Randomness and non-determinism

Randomness, nondeterminism and unpredictability should be distinguished. An ideal fair-bit source is often modeled by independent and identically distributed outcomes with $P(0) = P(1) = 1/2$, but raw physical entropy sources can be biased and correlated. Conversely, a CSPRNG is deliberately deterministic once its internal state is fixed, while remaining computationally unpredictable to an adversary who does not know that state. Reproducibility is therefore a feature of ordinary PRNGs and simulations.

A PRNG deterministically expands an internal state into a long output sequence. For cryptographic use, the initial state must be seeded from a high-entropy source. Public or predictable values such as time or GPS coordinates should not be treated as adequate entropy by themselves. Physical noise can contribute entropy when its statistical model and implementation are properly characterized.

Physical entropy is commonly conditioned or processed by a randomness extractor before or while it seeds a DRBG. A finite-state PRNG necessarily has a period, but for a modern CSPRNG the relevant security issues are state size, seed entropy, prediction resistance and resistance to state compromise, not merely the existence of an astronomically long mathematical period. Deterministic generators are also useful whenever reproducibility is required, and they can generate bits at very high rates [198] (Figure 25).

To obtain fresh physical entropy, one can use a **TRNG** (True Random Number Generator). A TRNG exploits a physical noise process such as thermal noise, avalanche noise, oscillator jitter or a quantum measurement. A classical chaotic process can be practically unpredictable but remains deterministic in principle, so chaos by itself can't be identified with intrinsic randomness.

One common technique consists of measuring electronic noise. Intel introduced the RDRAND instruction with third-generation Core processors in 2012, and AMD added support in the 2015 generation. Intel's on-chip DRNG does not return raw thermal-noise samples directly. A thermal-noise entropy source feeds a conditioner and then an AES-CTR DRBG, whose output is returned by RDRAND. RDSEED, introduced later, is intended to provide seed material. Other classical physical entropy sources include Johnson-Nyquist noise, avalanche or Zener noise, metastability and oscillator jitter.

1.3.2 QRNG principles and methods

So here come QRNGs (Quantum Random Number Generators), a subclass of physical random number generators. They exploit quantum measurement statistics. In the standard formulation of quantum mechanics, Schrödinger's equation governs unitary state evolution, while the Born rule is a separate measurement postulate assigning probabilities to possible outcomes, for example $p_i = \langle\psi|\Pi_i|\psi\rangle$. Operational quantum theory therefore provides intrinsically probabilistic measurement outcomes, although the philosophical interpretation of this randomness remains interpretation-dependent [197, 199, 200].

Quantum measurements can provide a well-defined entropy source, but this does not make an implemented QRNG automatically secure. A beam splitter is itself a quantum-optical component. Practical weaknesses arise from nonideal or adversarially controlled sources and detectors, optical loss, detector saturation, analog electronics and ADCs, side channels, calibration, and incorrect entropy estimation or extraction. This is why a security claim must specify both the physical entropy model and the adversary model.

Important QRNG differentiation criteria include the certified output rate rather than only the raw sampling rate, the conditional min-entropy per sample, latency and start-up health checks, resistance to source or detector manipulation, the assumptions made about the devices, the extraction method, independent certification and continuous health monitoring. Full device independence provides the strongest reduction in device-trust assumptions but currently comes with a large throughput and implementation penalty. Semi-device-independent approaches trade some assumptions for much higher rates.

Vendor trust is also a security criterion, particularly for systems used to generate cryptographic key material. Historical backdoors in commercial cryptographic equipment [201] illustrate the importance of supply-chain provenance, transparent entropy models, independent evaluation, secure firmware and interfaces, and continuous health monitoring. Country of origin alone is not a scientific security metric. Many QRNG techniques have been created to date, with photonic implementations being particularly attractive because they can reach small form factors and high bit rates.

Radioactive decay was one of the first developed QRNG technologies, based on the random timing of de-

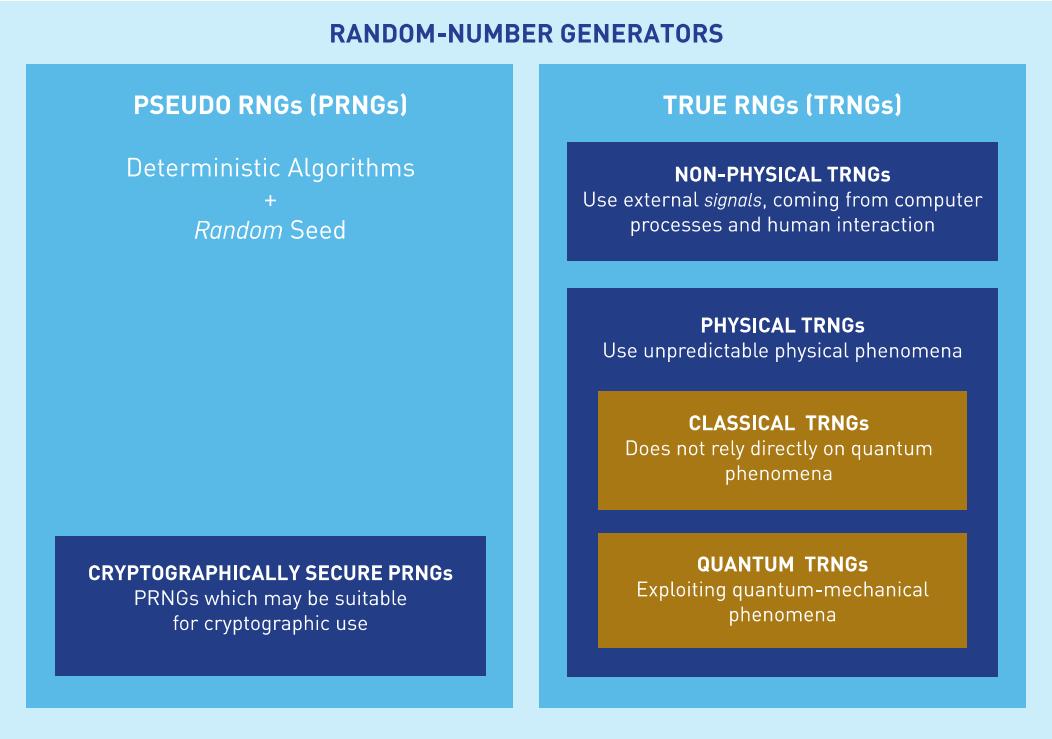


Figure 25: Taxonomy of random numbers generators. Source: [198].

cay of radioactive atoms, detected with a Geiger counter. It has limited bit rates and is not widely used, on top of not being very practical to implement given it is based on radioactive materials. There is however a vendor in that space, **EYL**.

Single-photon path measurement is one of the earliest QRNG methods. A photon incident on a nominally 50:50 beam splitter is detected in one of the two output ports, which can be mapped to 0 or 1 [197, 202]. Threshold single-photon detectors are sufficient. Jennewein et al. demonstrated a compact beam-splitter QRNG at 1 Mbit/s in 2000 [202]. Each accepted detection event can contribute at most one raw bit in this two-output architecture, while loss, detector dead time and saturation reduce the usable rate. ID Quantique was an early commercializer of this approach, but the beam-splitter QRNG concept was already demonstrated in peer-reviewed experiments in 2000. A further security issue is that the photon source and detectors can deviate from their assumed models or be influenced by an adversary.

Source-device-independent optical protocols can tolerate an untrusted light source while keeping the measurement apparatus trusted. Drahi et al. demonstrated composably secure real-time random-number generation at 8.05 Gbit/s in 2020 [203].

Miniaturized QRNG chips can instead measure photon-number or shot-noise fluctuations with integrated optoelectronics. ID Quantique's Quantis QRNG chipset uses an LED, a CMOS image-sensor array and digital post-processing. A QRNG first appeared in Samsung's Galaxy A Quantum smartphone in Korea in 2020. The Galaxy Quantum 4 followed in 2023. The Galaxy Quantum 5 was unveiled in August 2024 with an IDQ QRNG chipset measuring 2.5 mm × 2.5 mm, together with Samsung Knox.

In April 2021, Samsung announced the Galaxy Quantum2 with similar QRNG functionality. In February 2023, IDQ launched the IDQ250C3 QRNG chip, measuring 3 mm × 3 mm × 0.8 mm. In January 2025, IDQ and Elmos Semiconductor announced a collaboration to develop a monolithically integrated **QRNG**, not a QKD chip, targeting a 2 mm × 2 mm form factor. **Q→NU**, **CryptaLabs** and **Qrypt** also commercialize QRNG-related products.

Photon arrival-time QRNGs exploit the stochastic detection time or inter-arrival time of photons [204]. For an ideal Poissonian photon stream, the waiting-time distribution is exponential. Implementations can use one detector with high-resolution timing or multiple detectors and time tagging [205]. SPAD arrays have reached hundreds of Mbit/s [206], while newer demonstrations use integrated plasmonic waveguides [207] or NV centers as photon sources [208].

Spontaneous-emission-based QRNGs exploit optical amplitude, intensity or phase noise whose quantum contribution originates in spontaneous emission. Implementations use sources such as superluminescent diodes or LEDs [209, 210]. Entangled-photon sources and measurement-device-independent protocols are related but distinct architectures. For example, the perovskite-LED experiment by Argillander et al. demonstrated a

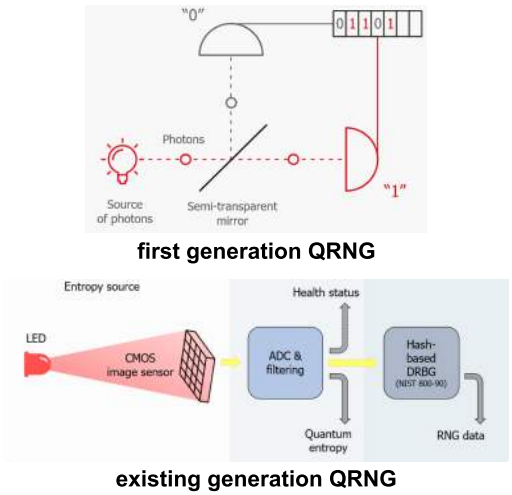


Figure 26: IDQ quantum number generators principles. Source: IDQ.

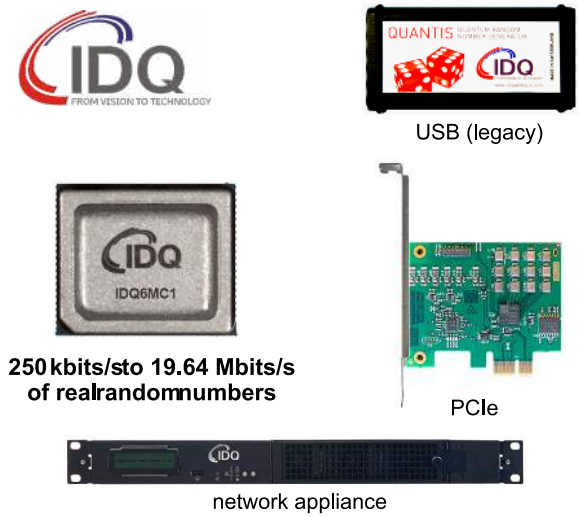


Figure 27: IDQ QRNG products. Source: IDQ.

measurement-device-independent QRNG, in which state preparation is trusted and the measurement device is treated as untrusted [211].

Phase noise and **phase diffusion** QRNGs exploit spontaneous-emission-induced phase fluctuations of a laser [212]. An unbalanced interferometer or delayed self-homodyne arrangement converts a random phase difference into an intensity fluctuation that is detected by a photodiode and digitized by an ADC. This is normally an analog interferometric measurement rather than single-photon counting. Qi et al. demonstrated 500 Mbit/s in 2010 [213], while Guo et al. demonstrated 20 Mbit/s with a VCSEL-based implementation [214]. More recent phase-noise architectures have reported rates in the tens to hundreds of Gbit/s range [215].

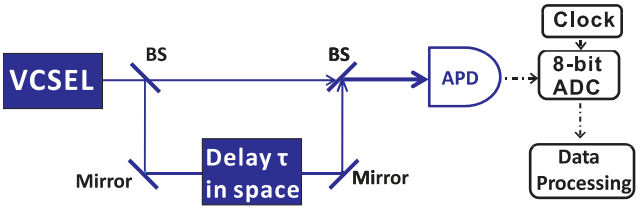


Figure 28: An APD (avalanche photodetector) operating principle. Source: [214].

Spatial noise can be another source of quantum randomness as tested in India in 2026, with a limited bandwidth of 7.5 Mbps [216].

Quantum vacuum-fluctuation QRNGs commonly measure an electromagnetic-field quadrature using balanced homodyne or heterodyne detection. In balanced homodyne detection, a vacuum input is mixed with a strong local oscillator on a nominally 50:50 beam splitter and the difference photocurrent samples a field quadrature. The relevant quantity is vacuum noise, not information encoded as a phase or frequency modulation, and the optical wavelength is implementation-dependent [217, 218]. Symul et al. demonstrated up to 2 Gbit/s of real-time generation in 2011 [219]. Haw et al. later demonstrated 14 Mbit/s/MHz and estimated a potential rate above 70 Gbit/s for their setup [220]. A 100 Gbit/s integrated vacuum-fluctuation QRNG was published in 2023 [221]. Semi-device-independent variants can also be very fast: Avesani et al. reached 17.42 Gbit/s in a source-device-independent heterodyne protocol in 2018 [222], and Kincaid et al. reported 35 Gbit/s with a monolithically integrated source-device-independent device in 2026 [223].

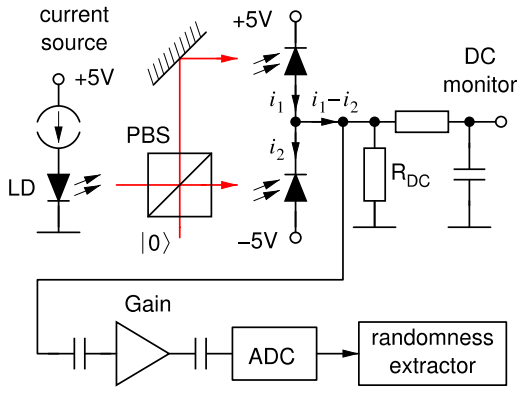


Figure 29: Quantum vacuum fluctuation QRNG. Source: [217].

Qubit measurement can also generate quantum randomness on a gate-based QPU. The simplest ideal example is sufficient in principle: initialize a qubit in $|0\rangle$, apply a Hadamard gate to prepare $|+\rangle$, then measure in the computational basis to obtain 0 or 1 with equal probability. Entanglement is not required for basic random-bit generation. It becomes useful when stronger certification is sought through Bell inequalities, contextuality or related protocols. Quantinuum's Quantum Origin current architecture pre-generates a quantum seed on Quantinuum Systems hardware and combines

that seed with local entropy through a strong-seeded extractor. Quandela's compact two-qubit photonic demonstration uses contextuality and explicitly accounts for information leakage, rather than implementing a standard spacelike-separated full-DI Bell protocol [224]. A separate 2025 experiment used Quantinuum's 56-qubit H2-1 trapped-ion processor for computationally certified randomness [225].

There are variations of QRNG exploiting quantum processors and other quantum systems, including quantum walks [226, 227], randomized benchmarking [228], electromechanical resonators [229], boson sampling [230], more complex quantum circuits [231], and quantum annealers [232]. Qutrit-based QRNGs provide a different type of certification based on contextuality and the Kochen-Specker theorem [233].

3D QRNG. A qutrit QRNG can certify value indefiniteness using a localized form of the Kochen-Specker theorem [234]. Theoretical results establish incomputability or bi-immunity properties for idealized infinite output sequences under explicit physical assumptions. No finite measured bit string can itself be proved algorithmically random [235]. A superconducting-transmon qutrit realization was reported in 2017 [235]. A later experiment analyzed 100 Gbit of output with a 3.2 μs experimental cycle, corresponding to 312.5 kcycles/s [236]. The superconducting implementation requires cryogenic hardware, calibration and classification of imperfect qutrit readout, which makes it far more complex than an integrated room-temperature photonic QRNG. A photonic implementation was proposed in 2026 [237].

Certified randomness covers several non-equivalent protocol families. In full device-independent QRNG, a loophole-free Bell-inequality violation bounds an adversary's guessing probability without trusting the internal operation of the source or measurement devices, subject to assumptions such as no signaling and independent setting choices [238]. One-sided device-independent protocols use quantum steering and trust one side of the experiment [239]. Contextuality and Leggett-Garg approaches provide certification under different physical assumptions [240]. Computationally certified randomness is another category: a classical verifier sends challenge computations to an untrusted quantum prover and derives a randomness guarantee from a computational-hardness model [241].

In 2025, a computationally certified-randomness experiment used the 56-qubit Quantinuum H2-1 trapped-ion QPU [225]. For a soundness parameter of 10^{-6}, the experiment certified 71,313 bits of smooth min-entropy and extracted 71,273 bits from 1,680,560 raw measurement bits, while using a 32-bit initial random seed. The guarantee was proved against a restricted class of near-term adversaries whose classical computing power was bounded, including a reference case four times more powerful than Frontier.

As inventoried by Marco Pistoia et al. in 2025 [241], **proposed** applications of certified randomness include public randomness beacons, strengthening systems containing potentially compromised pseudorandom generators, some constructions of non-interactive zero-knowledge proofs, differential-privacy mechanisms, fair allocation mechanisms and decentralized applications.

For fairness and privacy, certified randomness can provide "everlasting privacy" for Differential Privacy (DP) pipelines, protecting against inversion of randomized noise mechanisms by even unbounded adversaries.

In financial services, public randomness beacons powered by certified randomness can increase the transparency and trustworthiness of operations such as fair allocation of scarce resources in oversubscribed Initial Public Offerings (IPOs) and improving the perceived fairness of market order execution by introducing random or fixed delays.

In blockchain and decentralized applications, certified randomness can augment native on-chain randomness sources like block hashes or RANDAO, mitigating security concerns where blockchain actors might influence generated randomness. It also serves as a secure alternative off-chain randomness source, such as through certified randomness amplification, avoiding the trust assumptions associated with Verifiable Random Functions (VRFs). These applications demonstrate the potential of certified randomness to address vulnerabilities present in classical systems.

Other QRNG techniques are available but seemingly not widely used such as **Quantum Speed Limit** that can also be a good resource of quantum randomness [242], **laser chaos** that creates a time-delayed optical feedback via a reflector, **Raman scattering**, **attenuated pulse** and **Optical Parametric Oscillators (OPO)**, and as proposed in 2022, **skyrmions**-based QRNGs [243]. Another technique consists of merging on a single platform several QRNG methods. That's what a Chinese team released in July 2021 on an Alibaba Cloud server, mixing four types of QRNGs: single-photon detection, photon-counting detection, phase-fluctuations, and vacuum-fluctuations [244]. Three of these QRNG sources were off-the-shelf (Quantis-PCIe-16M from ID Quantique, QRG-100E from QuantumCTek and QRN-16 from MPD). In 2025, Cisco created a QRNG producing three distribution types of random numbers at over 60 Gbps raw bits by measuring the quantum vacuum noise [245].

1.3.3 Figures of merit

Here are some detailed key figures of merit of QRNG systems.

Device independence describes how many internal device assumptions are removed from the security proof. A trusted or device-dependent QRNG assumes that its source and measurement chain are correctly char-

acterized. Semi-device-independent protocols remove selected assumptions. In a source-device-independent QRNG, the source is untrusted while the measurement apparatus is trusted. In a measurement-device-independent QRNG, the prepared states are trusted while the measurement device is untrusted. Full device-independent QRNG treats both boxes as untrusted and certifies randomness from a loophole-free Bell violation [238]. Throughput does not follow a simple "Gbps for trusted, kbit/s for SDI" rule. Source-device-independent continuous-variable systems have demonstrated 17.42 Gbit/s [222] and 35 Gbit/s [223], while rigorous full-DI experiments have historically been much slower. Liu et al. extracted 6.2469×10^7 certified bits in 96 h, about 181 bit/s, in a loophole-free full-DI experiment [238]. A 2025 Optics Express experiment reported a 1.8 Mbit/s architecture labeled device-independent by its authors [246].

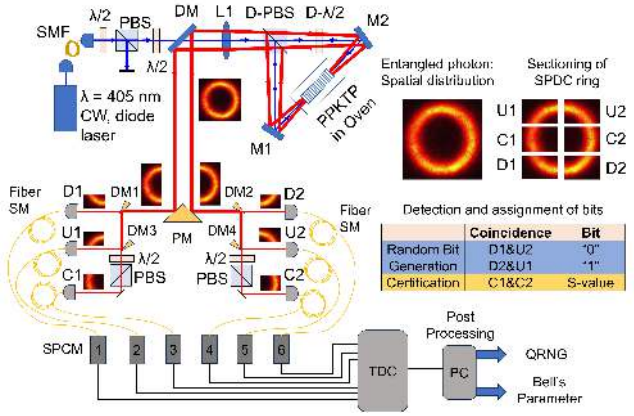


Figure 30: A 1.8 Mbit/s QRNG architecture reported as device-independent by an Indian-Spanish team in 2025. Source: [246].

Source-device-independent QRNG does not require a Bell violation. Its security proof assumes trusted measurements and estimates the conditional entropy of data produced by an untrusted source. Loophole-free Bell violation is instead the characteristic certification resource of full device-independent QRNG [238]. Semi-device-independent protocols can also use dimension bounds, energy bounds, trusted state preparation or trusted measurement models.

Avesani et al. demonstrated 17.42 Gbit/s of **secure random-bit generation** using a source-device-independent heterodyne protocol with security against general attacks in the finite-key scenario [222]. The result is a useful illustration that semi-device-independent certification can retain very high throughput.

There are also MDI-QRNGs, where the state-preparation source is trusted and the measurement device is untrusted. A typical protocol prepares a small characterized set of quantum states, for example $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, and uses test rounds to bound the behavior of the untrusted measurement device [247].

Full DI-QRNG remains predominantly an R&D technology because loophole-free Bell tests, space-like separation or equivalent stringent isolation requirements, high detection efficiency and finite-statistics security proofs impose large complexity and rate penalties. Semi-device-independent QRNGs make explicit, weaker device assumptions and can therefore reach much higher rates and smaller form factors [248–252]. Commercial products such as those from Quantum Dice belong to this broader semi-device-independent category rather than to full DI.

Quality and security. QRNGs are not equivalent merely because their output passes statistical tests. Vulnerabilities can arise from source manipulation [253], detector saturation or blinding, optical injection, analog front-end and ADC imperfections, calibration drift, side channels, extractor implementation and software interfaces [254, 255]. A robust design therefore needs an explicit entropy model, conservative conditional min-entropy bounds, secure extraction and continuous health monitoring.

Evaluation. A finite output sequence cannot be proved algorithmically random or incompressible. Borel normality is an asymptotic frequency property: in a base-2 normal infinite sequence, every n-bit word occurs with limiting frequency 2^{-n}. Normality is not equivalent to unpredictability or algorithmic randomness, since explicitly computable normal sequences exist [256]. Statistical suites such as NIST SP 800-22 can detect some biases, correlations and structural defects, but they do not estimate the physical entropy source and cannot prove nondeterminism or cryptographic security [257, 258]. For physical entropy sources, the more relevant methodology is to model the noise source, estimate min-entropy or conditional min-entropy, validate digitization and conditioning, apply online health tests and then use a suitable extractor.

Machine-learning tools can also search for patterns or implementation defects [260, 261], but no battery of output-only statistical tests can establish the physical origin of entropy. Loophole-free Bell tests are required only for full device-independent certification. Trusted and semi-device-independent QRNGs instead rely on their respective physical assumptions, entropy bounds, calibration or tomography procedures, health tests and extraction proofs.

Security. QRNG security must cover the complete chain from entropy source to delivered random bits. Relevant threats include optical or electrical injection, source manipulation, detector saturation or blinding, ADC imperfections, environmental perturbations, firmware and software compromise, post-processing errors and side channels [255]. Statistical quality of the final stream is necessary but not sufficient.

Test	Defect detected	Property
Frequency (monobit)	Too many zeroes or ones	Equally likely (global)
Frequency (block)	Too many zeroes or ones	Equally likely (local)
Runs test	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (locally)
Longest run of ones in a block	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (globally)
Binary matrix rank	Deviation from expected rank distribution	Linear dependence
Discrete fourier transform (spectral)	Repetitive patterns	Periodic dependence
Non-overlapping template matching	Irregular occurences of a prespecified template	Periodic dependence and equally likely
Overlapping template matching	Irregular occurences of a prespecified template	Periodic dependence and equally likely
Maurer's universal statistical	Sequence is incompressible	Dependence and equally likely
Linear complexity	Linear feedback shift register (LFSR) too short	Dependence
Serial	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Approximate entropy	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Cumulative sums (cusum)	Too many zeroes or ones at either an early or late stage in the sequence	Sequential dependence
Random excursions	Deviation from the distribution of the number of visits of a random walk to a certain state	Sequential dependence
Random excursions variants	Deviation from the distribution of the number of visits (across many random walks) to a certain state	Sequential dependence

Figure 31: The NIST test suite for QRNG. Source: [259].

1.3.4 Vendors

Let's now look at the QRNG industry vendor's landscape (Figure 32). As said before, this technique has been mastered for a long time by **ID Quantique** (IDQ), a company cofounded by Nicolas Gisin, which was acquired by IonQ in 2025. Other players abound like **CryptoMathic**, **Crypta Labs**, **Quside**, **InfiniQuant**, **Kets**, **PicoQuant** and **Quantropi**. **Axion Technologies** (2017, Canada) also created a random number generator competing with the Swiss IDQ. You can decrypt some of the vendor's lingua in this post from Marin Ivezic published in May 2026 [262].

Alea Quantum Technologies

Denmark, 2023

Alea Quantum Technologies provides a simplified vacuum based QRNG solution using an arbitrary transmissivity beam splitter (η<1) and replacing one of the photodiodes by a beam dump, allowing a compact implementation. The entropy source uses a VCSEL laser source, a single photodetector and a photodiode.

ComScire

USA, 1994

ComScire is the developer of several random number generators including PureQuantum QRNG, which is vendor-reported to create 4 to 128 million bits per second. The available documentation does not establish that its entropy source is quantum rather than classical.

Its entropy source seems to be coming from CMOS shot noise, using an Altera FPGA [263]. The company also markets QNGmeter 3.6, a software tool testing the randomness and nondeterministic nature of generated numbers.

CryptoMathic

Denmark, 1986

CryptoMathic develops quantum random key generators and various keys generation systems.

EYL

USA, 2015, $900K

EYL sells radioactive-isotope-based entropy chips and QRNG products. Their form factor includes a USB key.

Palo Alto Networks

USA, 2005

Palo Alto Networks is a software cybersecurity company which announced its QRNG Open API framework in 2025. It was developed with six QRNG partners: Anametric, ID Quantique, Quside, Qrypt, Quantinuum and Quantropi.

Figure 32: Map of QRNG vendors. © Olivier Ezratty, 2022-2026.

PicoQuant

Germany, 1996

PicoQuant is a Berlin-based SME specialized in photonics and which markets photon counters (SPADs) and diode lasers. But they are here because they also offer a photon arrival time QRNG, the PQRNG 150, with a throughput of 150 Mbits/s. It is much less miniaturized than the random number generator component from IDQ that is integrated into Samsung's Galaxy 5G announced in May 2020 [264].

Qrypt

USA, 2018

Qrypt develops cryptographic solutions using a high speed QRNG powered by multiple entropy sources exclusively licensed from Oak Ridge National Lab and other labs. Qrypt supports post-quantum and hybrid cryptographic deployments, including ML-KEM-based configurations aligned with NIST's finalized PQC standards. Qrypt invested in Quside (Spain), which is developing high quality and high speed QRNGs. They also work with the Los Alamos National Labs.

Qnu Labs

India, 2016, $11.5M

Qnu Labs sells its Tropos Quantum Random Number Generator. The vendor reports products spanning Mbit/s-class output and higher-throughput configurations. It also sells a QKD solution, Armos, and a quantum-secure key-management platform, Hodos.

Quside

Spain, 2017, €10.1M

Quside proposes a QRNG using phase diffusion, with a 400 Mbits/s key generation rate. It is a spin-off of ICFO, the Institute of Photonics of Barcelona with a staff of 30 as of January 2023. Quside QRNGs were used in many of the 2015 loophole-free Bell test experiments thanks to their high key rate. Their latest offering is the miniaturized QN 100 Quantum Entropy Source built with CMOS manufacturing techniques. In April 2024, they announced a partnership with Equinix which now provides a QRNG service based on Quside QRNG. It is using VCSEL photon sources from Coherent.

Quantum Dice

UK, 2020, $8.9M

Quantum Dice is a spin-off from the University of Oxford selling a "true" "self-certified" and fast QRNG device, which are actually Semi-Device-Independent QRNGs. It uses a patented DISC protocol ensuring that randomness comes only from the quantum process and is protected from external influences. Their commercial products include the VERTEX QD-1100 PCIe card. The QRNG business also provides Monte Carlo simulation entropy for financial applications, with an HSBC proof-of-concept underway. In 2025, they pivoted on the creation of some sort of probabilistic photonic computer supporting 64,000 logical p-bit which we cover in the unconventional computing section in this book [265].

Quantropi

Canada, 2018

Quantropi is a company created in Ottawa by James Nguyen (CEO) and Randy Kuang (Chief Scientist).

It was initially created to distribute a software generator of "lightweight ultra-high-entropy" random encryption keys. It then evolved into selling cybersecurity offerings combining custom-made PQC and a proprietary key-distribution scheme [266]. The vendor documentation

mixes classical and quantum terminology, and the quantum nature of several components cannot be verified from the public material.

Their QiSpace end-to-end quantum security SaaS platform contains a lot of stuff:

- **MASQ**, their asymmetric encryption offering, with a PQC for key exchange and digital signature containing a MPPK for Multivariate Polynomial Public Key, but they also have a Quantum Permutation Pad *aka* QPP. These things are supposed to support NIST PQC finalists and Quantropi's own PQC.

- **QEEP**, their symmetric encryption offering, providing "quantum-secure symmetric encryption that's up to 18 times faster than AES-256".

- **SEQUR**, their "quantum entropy as a service" (QEaaS) offering which contains some form of QRNG, branded QiSpace SEQUR NGen pseudo-QRNG (so, it is not a real QRNG) and their SEQUR SynQK, a sort of QKD that is supposed to deliver 5 simultaneous Quantum-key streams over distances ranging from 4,000 to 15,000 km at 130 to 190 megabits per second, all vendor-reported. The component presented as quantum is their "coherent-based Two-Field Quantum Key Distribution (CTF-QKD)", a signal modulation scheme using coherent optical communications hardware and infrastructure [267]. In December 2025, they documented their classical random number generator that is supposed to behave like a QRNG using classical hardware timing jitter [268].

SeQure Quantum

Chile-Poland, 2019

SeQure Quantum was created by Paulina Assmann (CEO), Guille Zedan (CCO), Gustavo Lima (COO), Marcin Pawlowski (COO) and Stephen Walborn (CTO). It sells a patented QRNG solution, SeQRNG, associated with perovskite light-emitting-diode technology and **measurement-device-independent** projective measurements [211]. The company partners with Thales to target space applications.

Terra Quantum (Switzerland) provides a photonic based QRNG generated 1.2 Mb/s of random bits.

1.3.5 Use cases

Here are some applications of random number generators and particularly the ones which can benefit from QRNG. We'll describe how PQC and QKD operate later on in this part.

Post-quantum cryptography requires cryptographically secure randomness for seeds, nonces and ephemeral values, depending on the algorithm. It does not require a high-throughput QRNG or "large random keys" directly from a physical source. In normal implementations, a few tens of bytes of fresh seed material can be expanded by a CSPRNG or DRBG into the pseudorandom material needed by the cryptographic algorithm. A QRNG can strengthen or diversify the physical entropy source feeding that architecture, but Gbit/s throughput is usually unnecessary for PQC key generation itself.

Quantum Key Distribution (QKD) requires private random choices whose details depend on the protocol, including bit values, measurement or preparation bases and, in decoy-state protocols, intensity choices [269]. At high optical clock rates these choices can require high-rate local randomness, potentially from hundreds of Mbit/s to Gbit/s if fresh choices are made at comparable rates. Some systems can also derive entropy from photon detection timing [270].

Other applications. QRNGs can be used for lotteries and gaming, randomized sampling, Monte Carlo simulation, scientific experiments and distributed public-randomness services. A random sequence is not characterized by the absence of repeated patterns. Repetitions are expected in genuinely random data. For ideal independent fair bits, any specified k-bit word has probability 2^{-k} at a given position, and finite samples need not contain exactly equal numbers of 0s and 1s. The decimal expansion of π is also a poor example of physical randomness: π is a deterministic computable number, and its normality has not been proved.

Zero-knowledge proofs (ZKPs) allow a prover to convince a verifier that a statement is true, or that the prover knows a witness, without revealing the witness beyond what follows from validity [271, 272]. Non-interactive zero-knowledge (NIZK) removes the interactive exchange by using a setup model, a common reference string, a random oracle or another construction-specific mechanism. ZKP and NIZK security can require cryptographically secure randomness, but it does not in general require intrinsically quantum randomness. A QRNG can provide entropy to the cryptographic RNG used by such protocols, but it is optional rather than foundational.

1.3.6 Bibliography and notes

These are the bibliographical references and notes for the **Quantum Random Numbers Generators** subsection.

[197] Quantum random number generators, by Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin, Reviews of Modern Physics, February 2017 🔓 (preprint on arXiv).

[198] Quantum Random-Number Generators: Practical Considerations and Use Cases Report, by Marco Piani et al., January 2021 (38 pages).

[199] A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness, by Vaisakh Mannalath, Sandeep Mishra, and Anirban Pathak, arXiv, December 2023 (44 pages).

[200] Quantum Random Number Generators : Benchmarking and Challenges, by David Cirauqui, Maciej Lewenstein, et al., arXiv, June 2022 (15 pages).

[201] The intelligence coup of the century' - For decades, the CIA read the encrypted communications of allies and adversaries, by Greg Miller et al., February 2020.

[202] A fast and compact quantum random number generator, by Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger, Review of Scientific Instruments, April 2000 (6) 🔓 (preprint on arXiv).

[203] Certified Quantum Random Numbers from Untrusted Light, by David Drahi, Physical Review X, December 2020.

[204] Photon arrival time quantum random number generation, by Michael A. Wayne et al., Journal of Modern Optics, April 2008 (7 pages) 🔓 (preprint on hdl.handle.net).

[205] A simple low-latency real-time certifiable quantum random number generator, by Yanbao Zhang, William J. Munro, et al., Nature Communications, February 2021.

[206] A High Speed Integrated Quantum Random Number Generator with on-Chip Real-Time Randomness Extraction, by Francesco Regazzoni, Edoardo Charbon, et al., arXiv, February 2021 (9 pages).

[207] Quantum random number generation using an on-chip nanowire plasmonic waveguide, by C. Strydom, M. S. Tame, et al., arXiv, April 2024 (12 pages).

[208] Demonstration of quantum random number generation using nitrogen vacancy centres, by Conrad Strydom and Mark Tame, arXiv, April 2026 (15 pages).

[209] Quantum Random Number Generator Based on LED, by Mohammadreza Moeini, Mehrdad Malekian, et al., arXiv, February 2024 (8 pages).

[210] Micro-LED-based quantum random number generators, by Heming Lin, Boon S. Ooi, et al., Optics Express, May 2025 (11 pages).

[211] Quantum random number generation based on a perovskite light emitting diode, by Joakim Argillander, Alvaro Alarcón, Chunxiong Bao, Chaoyang Kuang, Gustavo Lima, Feng Gao, and Guilherme B. Xavier, Communications Physics, June 2023.

[212] A quantum entropy source on an InP photonic integrated circuit for random number generation, by Carlos Abellan, Valerio Pruneri, et al., arXiv, September 2016 (7 pages).

[213] High-speed quantum random number generation by measuring phase noise of a single-mode laser, by Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo, and Li Qian, Optics Letters, February 2010 (3) 🔓 (preprint on arXiv).

[214] Truly random number generation based on measurement of phase noise of a laser, by Hong Guo, Wenzhuo Tang, Yu Liu, and Wei Wei, Physical Review E, May 2010 🔓 (preprint on arXiv).

[215] An Ultra-fast Quantum Random Number Generation Scheme Based on Laser Phase Noise, by Jie Yang, Bin Luoand Hong Guo, et al., arXiv, November 2023 (25 pages).

[216] Quantum random number generation using spatial quantum noise of light, by Mohamed Armoon Shaliq and Ashok Kumar, arXiv, August 2026 (7 pages).

[217] Random numbers from vacuum fluctuations, by Yicheng Shi, Brenda Chng, and Christian Kurtsiefer, arXiv, February 2016 (5 pages).

[218] A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers, by Francesco Raffaelli, Jonathan C F Matthews, et al., Quantum Science and Technology, February 2018.

[219] Real time demonstration of high bitrate quantum random number generation with coherent laser light, by T. Symul, S. M. Assad, and P. K. Lam, Applied Physics Letters, June 2011 (3) 🔓 (preprint on arXiv).

[220] Maximization of Extractable Randomness in a Quantum Random-Number Generator, by J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Physical Review Applied, May 2015 🔓 (preprint on arXiv).

[221] 100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations, by Cédric Bruynsteen, PRX Quantum, March 2023.

[222] Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, by Marco Avesani, Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi, Nature Communications, December 2018 (7 pages).

[223] Source-device-independent monolithically integrated QRNG in a black box with a generation rate in excess of 30 Gbit/s, by Peter Seigo Kincaid, Lorenzo De Marinis, Francesco Testa, Nicola Andriolli, and Giampiero Contestabile, Optica Quantum, April 2026 (6 pages).

[224] Certified Randomness in Tight Space, by Andreas Fyrillas, Boris Bourdoncle, Alexandre Maïnos, Pierre-Emmanuel Emeriau, Kayleigh Start, Nico Margaria, Martina Morassi, Aristide Lemaître, Isabelle Sagnes, Petr Stepanov, Thi Huong Au, Sébastien Boissier, Niccolo Somaschi, Nicolas Maring, Nadia Belabas, and Shane Mansfield, PRX Quantum, May 2024 (19 pages).

[225] Certified randomness amplification by dynamically probing remote random quantum states, by Minzhao Liu, Michael Foss-Feig, Ruslan Shaydulin, et al., arXiv, November 2025 (91 pages).

[226] Quantum Walk Random Number Generation: Memory-based Models, by Minu J. Bae, arXiv, October 2022 (12 pages).

[227] Generation of True Quantum Random Numbers with On-Demand Probability Distributions via Single-Photon Quantum Walks, by Chaoying Meng, Franco Nori, et al., arXiv, March 2024 (10 pages).

[228] Certified Randomness from Quantum Supremacy, by Scott Aaronson and Shih-Han Hung, arXiv, March 2023 (84 pages).

[229] Random number generation with a chaotic electromechanical resonator, by Guilhem Madiot, Franck Correia, Sylvain Barbay, and Rémy Braive, arXiv, April 2022 (8 pages).

[230] A Study of Gate-Based and Boson Sampling Quantum Random Number Generation on IBM and Xanadu Quantum Devices, by Mohamed Messaoud Louamri, Mohamed Taha Rouabah, et al., arXiv, July 2025 (4 pages).

[231] A Quantum Algorithm for Random Number Generation, by Aastha Kataria, Devansh Desai, Ashwini Dalvi, Sagar Korde, Abhijeet Pasi, Irfan N A Siddavatam, and Sudhir Ranjan Jain, arXiv, June 2026 (22 pages).

[232] Analysis of a Programmable Quantum Annealer as a Random Number Generator, by Elijah Pelofske, arXiv, February 2024 (11 pages).

[233] Binary Quantum Random Number Generator Based on Value Indefinite Observables, by Cristian S. Calude and Karl Svozil, arXiv, June 2024 (10 pages).

[234] Strong Kochen-Specker theorem and incomputability of quantum randomness, by Alastair A. Abbott, Cristian S. Calude, Jonathan Conder, and Karl Svozil, Physical Review A, December 2012 (11 pages) 🔓 (preprint on arXiv).

[235] Realization of a Quantum Random Generator Certified with the Kochen-Specker Theorem, by Anatoly Kulikov, Markus Jerger, Anton Potocnik, Andreas Wallraff, and Arkady Fedorov, Physical Review Letters, December 2017 (5 pages) 🔓 (preprint on arXiv).

[236] How real is incomputability in physics?, by José Manuel Agüero Trejo, Cristian S. Calude, Michael J. Dinneen, Arkady Fedorov, Anatoly Kulikov, Rohit Navarathna, and Karl Svozil, Theoretical Computer Science, July 2024.

[237] ND-Photonic QRNGs in a Noisy Environment, by J. M. Agüero Trejo, Cristian S. Calude, and O. C. Stoica, arXiv, August 2026 (20 pages).

[238] Device-independent quantum random-number generation, by Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, Hao Li, W. J. Munro, Zhen Wang, Lixing You, Jun Zhang, Xiongfeng Ma, Jingyun Fan, Qiang Zhang, and Jian-Wei Pan, Nature, October 2018 (4) 🔓 (preprint on arXiv).

[239] Quantum Steering, by Roope Uola, Ana C. S. Costa, H. Chau Nguyen, and Otfried Gühne, arXiv, March 2020 (43 pages).

[240] Leggett-Garg Inequalities, by Clive Emary, Neill Lambert, and Franco Nori, arXiv, January 2014 (49 pages).

[241] Applications of Certified Randomness, by Omar Amer, Marco Pistoia, et al., arXiv, March 2025 (15 pages).

[242] Certified randomness from quantum speed limits, by Caroline L. Jones, Markus P. Mueller, et al., arXiv, June 2025 (4 pages).

[243] Single skyrmion true random number generator using local dynamics and interaction between skyrmions, by Kang Wang, Gang Xiao, et al., Nature Communications, February 2022.

[244] Quantum random number cloud platform, by Leilei Huang, Chongjin Xie, et al., npj Quantum Information, July 2021.

[245] 40Gbps Tri-type Quantum Random Number Generator, by Jiapeng Zhao, Reza Nejabati, et al., arXiv, June 2025 (19 pages).

[246] Device-independent, megabit-rate quantum random number generator with beam-splitter-free architecture and live Bell test certification, by Ayan Kumar Nai, Vimlesh Kumar, M. Ebrahim-Zadeh, and G. K. Samanta, Optics Express, October 2025 (12 pages).

[247] Experimental measurement-device-independent quantum random number generation, by You-Qi Nie, Jian-Wei Pan, et al., arXiv, December 2016 (15 pages).

[248] Quantum random-number generator with non-demolition measurements: semi-device-independent implementation, by Paolo Solinas and Giovanni Chesi, arXiv, August 2026 (14 pages).

[249] Efficient Energy-Constrained Semi-Device-Independent QRNG with an Integrated Heterodyne Receiver, by Mattia Sabatini, Marco Avesani, et al., arXiv, June 2026 (14 pages).

[250] On-Chip Quantum Randomness Amplification, by Lang Li, Yutian Wu, Giulio Chiribella, and Ravishankar Ramanathan, arXiv, June 2026 (53 pages).

[251] Semi-Device-Independent Quantum Random Number Generator Resistant to General Attacks, by Zhenguo Lu, Jundong Wu, Yu Zhang, Shaobo Ren, Xuyang Wang, Hongyi Zhou, and Yongmin Li, arXiv, February 2026 (10 pages).

[252] On-chip semi-device-independent quantum random number generator exploiting contextuality, by Maddalena Genzini, Caterina Vigliar, Mujtaba Zahidy, Hamid Tebyanian, Andrzej Gajda, Klaus Petermann, Lars Zimmermann, Davide Bacco, and Francesco Da Ros, arXiv, June 2026 (12 pages).

[253] Out-of-Band Electromagnetic Injection Attack on a Quantum Random Number Generator, by P.R. Smith, Physical Review Applied, April 2021.

[254] Improved Real-time Post-Processing for Quantum Random Number Generators, by Qian Li, Xiaoming Sun, Xingjian Zhang, and Hongyi Zhou, arXiv, January 2024 (11 pages).

[255] Statistical Invisibility of a Physical Attack on QRNGs After Randomness Extraction, by Yifan Chen, Yang Zhang, et al., arXiv, August 2025 (8 pages).

[256] A zoo of computable binary normal sequences, by Steve Pincus and Burton H. Singer, Proceedings of the National Academy of Sciences, November 2012 (6) 🔓 (preprint on ncbi.nlm.nih.gov).

[257] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, by Andrew Rukhin, 2010 (131 pages).

[258] Recommendations and illustrations for the evaluation of photonic random number generators, by Joseph D. Hart, Yuta Terashima, Atsushi Uchida, Gerald B. Baumgartner, Thomas E. Murphy, and Rajarshi Roy, APL Photonics, August 2017 (22 pages).

[259] Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators, by Charmaine Kenny, April 2005 (107 pages).

[260] Machine Learning Cryptanalysis of a Quantum Random Number Generator, by Nhan Duy Truong, Omid Kavehei, et al., arXiv, May 2025 (14 pages).

[261] Benchmarking a Quantum Random Number Generator with Machine Learning, by Jing Yan Haw et al., 2020 (26 slides).

[262] The Quantum Random Number Generator (QRNG) Gold Rush, by Marin Ivezic, PostQuantum, May 2026.

[263] Entropy Analysis and System Design for Quantum Random Number Generators in CMOS Integrated Circuits, by Scott A Wilber, 2013 (28 pages).

[264] Ultrafast quantum key distribution using fully parallelized quantum channels, by Robin Terhaar and Wolfram H.P. Pernice et al), arXiv, July 2022 (13 pages).

[265] Self-correcting High-speed Opto-electronic Probabilistic Computer, by Ramy Aboushelbaya, Marko von der Leyen, et al., arXiv, November 2025 (17 pages).

[266] Startup: Only Quantum Cryptography Can Save The $100 Trillion Global Digital Economy, by John Koetsier in Forbes, March 2021.

[267] Quantum Public Key Distribution using Randomized Glauber States, by Randy Kuang et al., 2020 (7 pages) 🔓 (preprint on arXiv).

[268] Digital Coherent-State QRNG Using System-Jitter Entropy via Random Permutation, by Randy Kuang, arXiv, December 2025 (13 pages).

[269] Integration of quantum random number generators with post-quantum cryptography algorithms, by Paula Alonso Blanco, Valerio Pruneri, et al., arXiv, July 2025 (5 pages).

[270] Practical random number generation protocol for entanglement-based quantum key distribution, by G. B. Xavier, J. P. von der Weid, et al., arXiv, January 2010 (10 pages).

[271] Experimental Implementation of A Quantum Zero-Knowledge Proof for User Authentication, by Marta I. Garcia-Cid, Laura Ortiz, et al., arXiv, January 2024 (16 pages).

[272] A classical proof of quantum knowledge for multi-prover interactive proof systems, by Anne Broadbent, Arthur Mehta, et al., arXiv, June 2025 (28 pages).

This **Quantum Random Numbers Generators** subsection contains 76 bibliographical references and notes containing at least 1,213 pages.

1.4 Quantum Key Distribution

Quantum key distribution (QKD) is the most mature branch of quantum cryptography. It allows two authenticated parties to establish a shared symmetric secret key over a quantum optical channel, typically an optical fiber, a free-space link or a satellite optical link, while using an authenticated classical channel for sifting and post-processing [273, 274]. QKD does not literally detect every intrusion. Under the assumptions of a given security proof, Alice and Bob estimate channel parameters such as error rates and either extract a key whose information leakage is bounded by a chosen security parameter or abort when the observed statistics are incompatible with secure key generation [275].

1.4.1 QKD principles

Prepare-and-measure QKD. The first widely used QKD protocol is BB84, introduced by Charles Bennett and Gilles Brassard in 1984 [276]. Bennett and Brassard were already using the expression "quantum cryptography" in work presented in 1982 [277].

This protocol can encode each signal in one of four polarization states belonging to two mutually unbiased bases: the rectilinear basis, 0°/90°, and the diagonal basis, 45°/135°. The two states within each basis are orthogonal, while states from different bases are non-orthogonal. Alice randomly chooses a bit value and a basis for each signal and Bob independently chooses a measurement basis. After transmission, they announce their basis choices over an authenticated classical channel and retain the events for which Bob used the same basis as Alice, forming the sifted key.

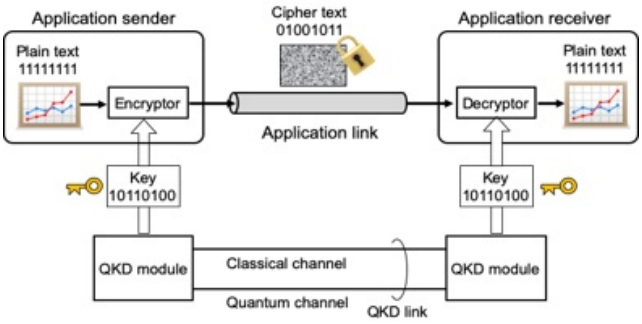


Figure 33: General principle of entanglement-based quantum key distribution. 1) Alice and Bob receive photons from entangled pairs, 2) they measure them using randomly chosen settings, 3) they exchange the settings over an authenticated classical channel, 4) they keep the events selected by the protocol to form a sifted key, 5) they estimate security parameters from a disclosed data subset, and 6) after error correction and privacy amplification, the generated key can be used by a classical cipher. Source: [278].

In ideal single-photon BB84, a simple intercept-resend attack on every signal introduces a 25% QBER in the sifted key: Eve chooses the wrong basis half of the time and, in those cases, Bob obtains the wrong sifted bit with probability one half. More general security follows from the quantum information-disturbance tradeoff and the impossibility of perfectly copying unknown non-orthogonal states, quantified statistically during parameter estimation [279]. Monogamy of entanglement is central to many entanglement-based security arguments, but it is not the operational name of the BB84 intercept-resend mechanism. If the estimated parameters do not permit secure key extraction, Alice and Bob abort [280].

Entanglement-based QKD. Artur Ekert introduced the E91 protocol in 1991 using entangled pairs and Bell nonlocality [281]. A source distributes one member of each pair to Alice and the other to Bob, and the source itself need not be trusted in the idealized security model. Alice and Bob randomly choose measurement settings. Some setting combinations contribute to the raw key while others are used to estimate a Bell inequality and constrain the correlations that an eavesdropper could share with them. For CHSH, the maximum quantum value is the Tsirelson bound $|S| = 2\sqrt{2}$, but a practical protocol does not require the measured value to equal this ideal maximum. Noise and loss lower the observed violation, and secure key extraction depends on the applicable security threshold and finite-key analysis, not on a binary test against $2\sqrt{2}$.

Both BB84 and E91 require private and unpredictable random choices. In BB84, Alice needs randomness for raw bits and basis choices and Bob needs randomness for his measurement bases. In E91, the correlated measurement outcomes provide intrinsic quantum randomness, but Alice and Bob still need random measurement settings. QRNGs are therefore a natural implementation choice for both families. Using a conventional PRNG can instead make security depend on the secrecy and computational unpredictability of its seed and internal state.

QKD has moved from laboratory demonstrations to operational deployments, most visibly in China, while large-area terrestrial networks still rely mainly on trusted relays. At a trusted node, key material is handled classically and the node must therefore be physically and operationally trusted. There is no universal 80 km spacing limit: practical spans depend on fiber attenuation, detector performance and the required secret key rate. In the 2025 China Quantum Communication Network, the average distance between adjacent backbone QKD nodes is about 70 km [282]. Quantum repeaters that preserve end-to-end quantum correlations without trusted key access remain experimental.

CV-QKD. Continuous-variable QKD encodes information in optical field quadratures and commonly uses coherent states with Gaussian or discrete modulation [283, 284]. It is attractive for telecom integration because coherent detection can reuse technologies derived from classical optical communications, and quantum and classical channels can be multiplexed on the same fiber [285]. Frédéric Grosshans and Philippe Grangier introduced the coherent-state protocol commonly called

GG02 in 2002. This complements discrete-variable QKD (DV-QKD). Practical DV-QKD does not necessarily require deterministic single-photon sources: many systems use weak coherent laser pulses with decoy states, while single-photon detectors may require cooling depending on the detector technology. CV-QKD receivers use homodyne or heterodyne detection. In 2025, a Chinese team demonstrated an integrated silicon-photonic CV-QKD system over 50.4 km of standard fiber with an asymptotic secret key rate of 5.05 Mbit/s using 8-PSK discrete phase modulation, not eight independent amplitude-and-phase combinations [286]. A 2026 follow-up from TU Eindhoven implemented a monolithic dual-polarization silicon photonic transceiver reaching 1.9 Mbit/s over 25 km with 64-QAM modulation [287]. CV-QKD often targets metropolitan distances, but there is no categorical distance boundary separating CV-QKD from DV-QKD.

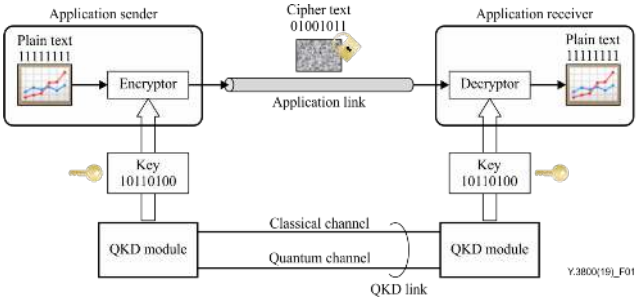


Figure 34: DV and CV in QKD. Source: [278].

Figure 34 and Figure 35 make a rough comparison between DV-QKD and CV-QKD. CV-QKD is attractive for telecom-fiber integration because it can reuse existing optical components, while DV-QKD remains widely deployed and commercially mature [288]. Figure 38 describes a typical prepare-and-measure coherent-state CV-QKD architecture, rather than BB84 itself. It uses an optical source in the telecom wavelength band around 1,550 nm followed by amplitude and phase or in-phase/quadrature modulators. CV-QKD can also be formulated with entanglement-based protocols.

	DV-QKD	**CV-QKD**
Quantum state	Polarization, phase, or time bin of a single photon	Quadrature components of quantized electromagnetic field
Source	Single-photon source	Coherent-state or squeezed-state source
Detector	Single-photon detector	Homodyne or heterodyne detector
Channel model	Lossy qubit channel	Lossy bosonic channel
Distance limitation	Performance of single-photon detectors	Efficiency of post-processing techniques

Figure 35: Comparison between DV-QKD and CV-QKD protocols. Source: [274].

The integration of QKD with conventional optical telecommunications can use wavelength-division multiplexing (WDM), for instance with a quantum channel around 1,310 nm and classical data around 1,550 nm, time-division multiplexing (TDM), or a physically dedicated fiber in the same cable. SDM denotes multiplexing distinct spatial channels such as multiple cores or modes within a fiber. China has significant experience with quantum-classical coexistence on telecom infrastructure [289, 290] (Figure 37).

QKD does not evade the Holevo bound by using prior entanglement. The Holevo theorem bounds the accessible classical information encoded in a quantum ensemble under specified communication resources. Protocols such as superdense coding use pre-shared entanglement as an additional resource and therefore do not violate the theorem. In QKD, the quantum channel is used to establish correlated secret key material, while the data encrypted with that key is transmitted over a classical channel [291]. The two physical paths can differ. For example, a key can be established through a satellite QKD link while encrypted data travels through terrestrial fiber or even wireless communications.

The payload can then be protected with conventional symmetric cryptography, for example AES within TLS, IPsec, MACsec or an application-specific protocol. SSL is obsolete and has been superseded by TLS for HTTPS.

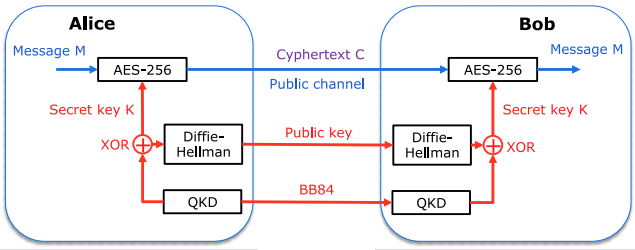


Figure 36: Description of the data and key transmission with QKD applicable to both prepare-and-measure and entanglement based QKD. Source: [292].

QKD engineering. In practice, QKD uses a classical post-processing chain commonly called key distillation. It includes sifting when required, parameter estimation, information reconciliation with classical error-correcting codes, privacy amplification and authentication (Figure 39). These classical codes are unrelated to the QEC codes used in FTQC. Authentication prevents an active adversary from impersonating Alice or Bob on the classical channel and can be bootstrapped from a short pre-shared secret or, with different security assumptions, from digital signatures. The quantum bit error rate (QBER) is the fraction of erroneous sifted bits, not a general "infidelity" of the link. The often quoted approximately 11% threshold applies to asymptotic one-way post-processing for idealized BB84 under specific security assumptions [279].

Post-processing reduces the raw or sifted key to a shorter secret key by an amount that depends on QBER, reconciliation efficiency, parameter-estimation sampling, finite-size effects and the chosen security parameter. Implementing QKD combines private randomness, an

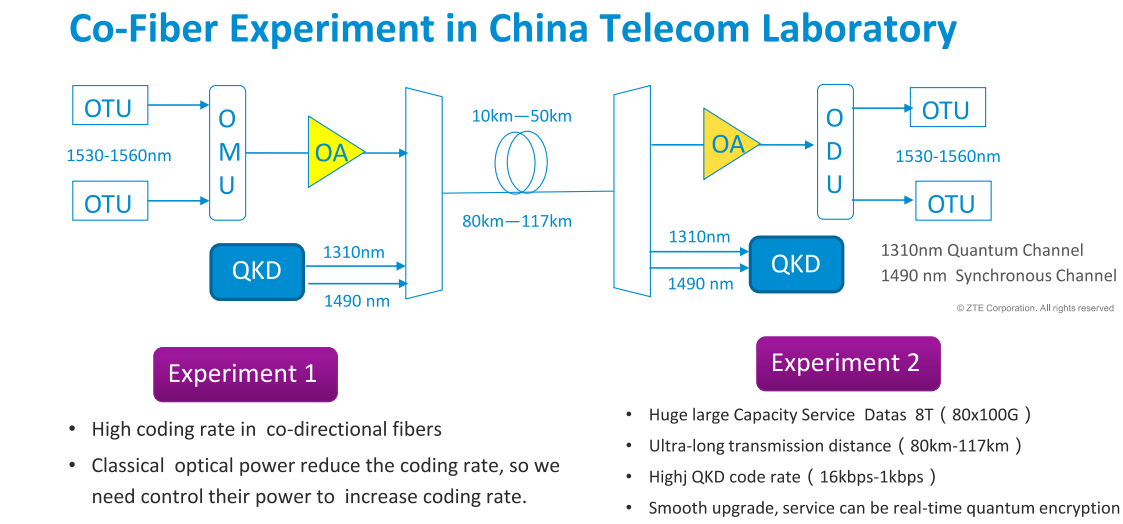


Figure 37: Co-fiber experiment in China Telecom laboratory distributing quantum keys over telecom fiber lines. Source: [293].

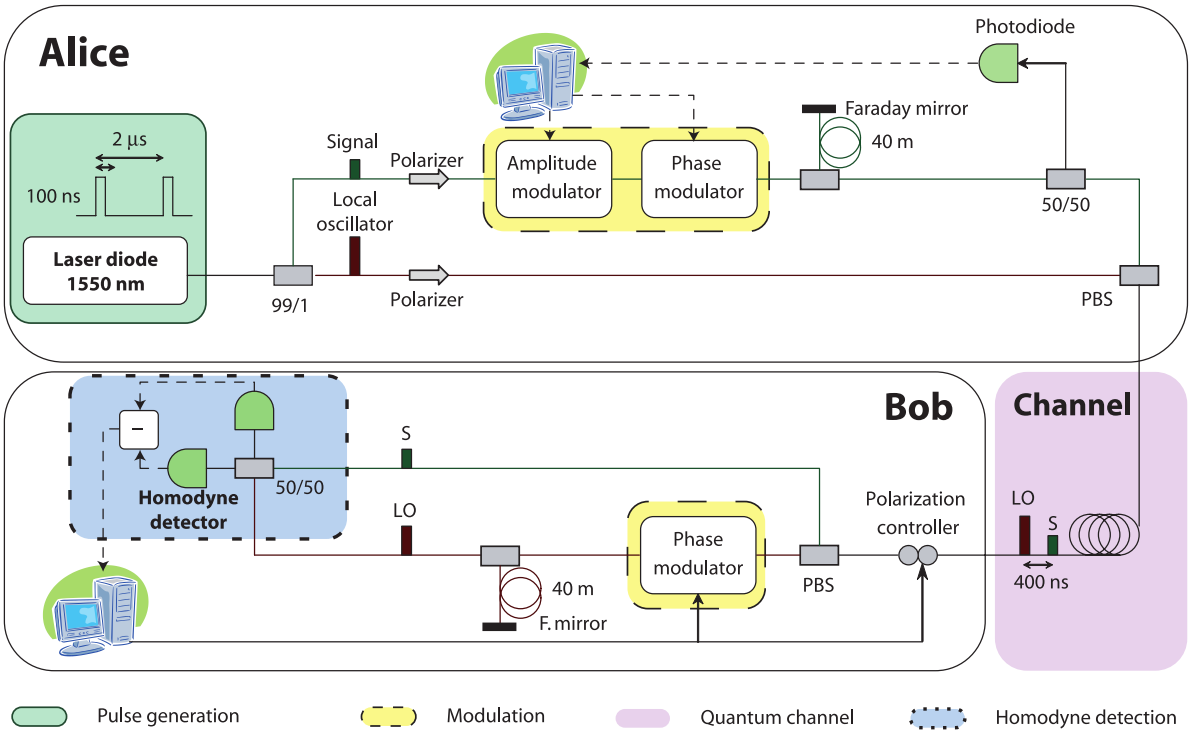


Figure 38: Example of a prepare-and-measure coherent-state CV-QKD optical architecture. Source: [294].

authenticated classical channel for protocol messages and a quantum channel. The quantum channel can use a dark fiber, a wavelength coexisting with classical traffic, or a free-space optical link depending on the architecture.

The useful data is normally encrypted with QKD-derived keys using classical symmetric cryptography such as AES and transmitted over a conventional channel, which may be optical fiber, radio or another medium (Figure 39). A one-time pad can also use QKD-generated key material. Information-theoretic secrecy then requires a uniformly random secret key at least as long as the message, used only once. Because practical secret key rates are usually far below payload data rates, QKD is more commonly used to refresh keys for high-rate symmetric ciphers.

This is well documented by ETSI [296]. On arrival, a quantum key receiver and the system for decrypting the signal arriving via the traditional channel is used (Figure 40).

The secret-key throughput, *aka* secret key rate (SKR), is an important figure of merit. It remains far below the Tbit/s capacity of modern optical links. Reference [297] describes high-speed CV-QKD over 5 to 50 km with secret-key generation ranging from 7.6 Mbit/s to 288 Mbit/s. Reference [298] reports an ultra-bright telecom-

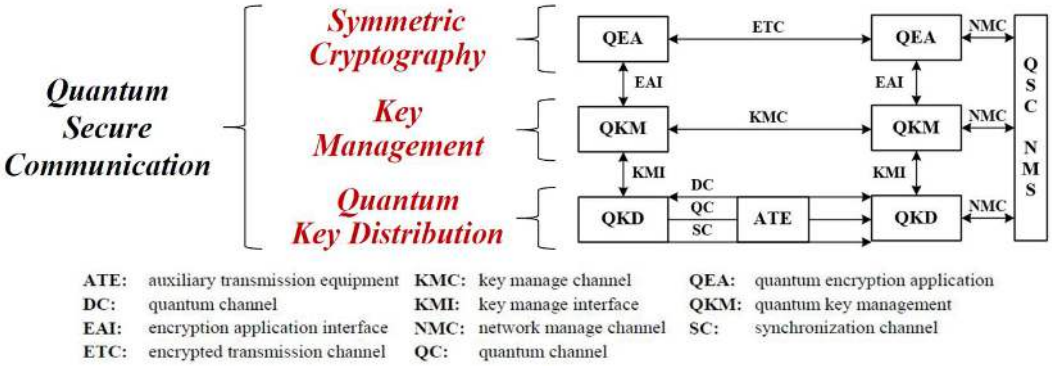


Figure 39: The three components of quantum secure communication with a symmetric cryptography, key management and a QKD. Source: [295].

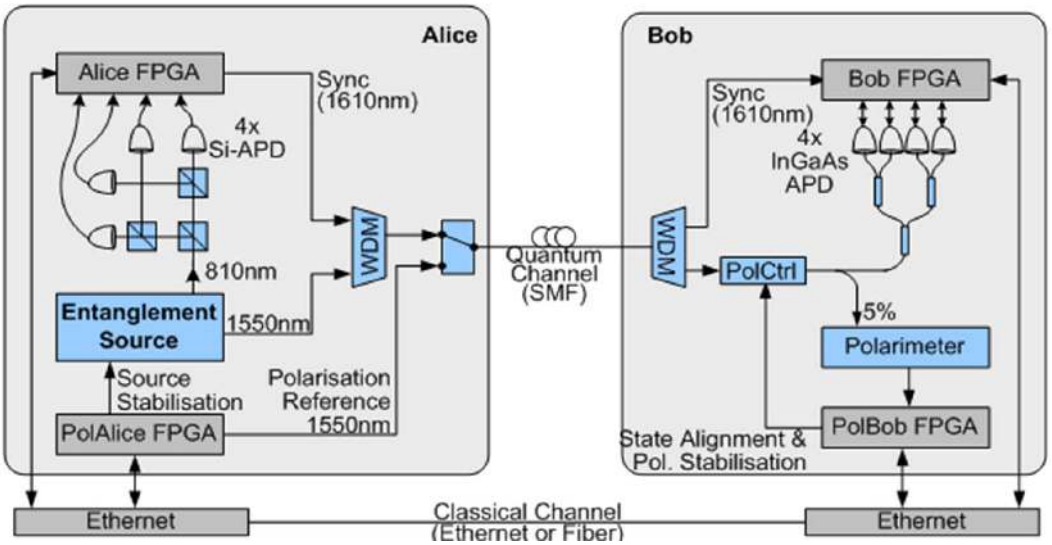


Figure 40: Entanglement-based QKD architecture, as documented by ETSI in 2018. Source: [296].

wavelength entangled-photon source with a projected secure key generation potential beyond 1 Gbit/s under favorable link conditions, rather than an end-to-end long-distance final-key rate of 1 Gbit/s. Practical SKR falls rapidly with channel loss and depends on detector noise, protocol overhead and finite-key effects. QKD engineering must also close implementation loopholes, including Bell-test post-selection loopholes for protocols whose security relies on Bell correlations [299].

Other improvements come with clock synchronization without an additional dedicated channel and protocols to increase raw key rates [300]. The quantum keys transfer rate can be much lower than the physical data rate available. There are fundamental bounds on how many secret keys can be generated over a noisy quantum channel. A 2023 record was broken by a team in China, with secret keys generated at 115.8 Mb/s over a 10 km standard optical fiber, and distributed keys over up to 328 km of ultralow-loss fiber for more than 50 hours. The precedent record secret key rate was of 10 Mb/s over 10 km standard optical fiber [301]. At longer distances, a China team did support entanglement-based key rates of up to 440.80 bits/s over 200 km and a maximum distance of 404 km, but with a much lower rate of 1.55×10^{-3} bits/s, all of it in the 1,560 nm telecommunication band. The system relies on an ultra-bright polarization-entangled photon source using a type-0 QPM PPLN (quasi-phase-matching, periodically poled lithium niobate) waveguide driven by a 780 nm pump laser [302]. On the chip side, a USTC team demonstrated in December 2025 a 5 GHz integrated polarization-encoding QKD system combining a new polarization-state preparation scheme, an ultra-low time-jitter laser source and SNSPDs, generating 1.076 Mbps over 150 km and 105 kbps over 200 km of standard single-mode fiber, with average QBERs of 0.52% and 0.44% in the Z and X bases and a stable 1.025 Mbps output over 6 hours of continuous operation at 150 km [303]. This is 1 to 2 orders of magnitude above the previous integrated QKD systems at these distances.

The QKD quantum channels and classical data can be conveyed on the same fiber. It was experimented in 2023 by Orange and Toshiba Europe over 50 km using a 1,310 nm fiber for the co-propagation of a QKD quantum channel and classical signals using 60-channel

WDM (wavelength division multiplexing) at 100 Gb/s [304]. It can even be done the same frequency [305].

Other fundamental questions abound about the overall architecture and topology of QKD networks, most of the time working in "point to point" and relying on so-called trusted nodes, which can be considered as "classical" repeaters [306]. Proposals abound to create point-to-multipoint [307], large multi-point networks and routing protocols [308–314] and on entanglement distribution optimization [315, 316].

Comparison of Different Cryptosystems in the Presence of Quantum Computers

Cryptosystem	Type	Impact
RSA	Public-key	Insecure
Diffie-Hellman	Public-key	Insecure
ECC	Public-key	Insecure
AES	Symmetric-key	Larger key sizes required
OTP	Symmetric-key	Proven secure
Code-based	Post-quantum	Not yet broken
Hash-based	Post-quantum	Not yet broken
Lattice-based	Post-quantum	Not yet broken
Multivariate	Post-quantum	Not yet broken
QKD	Quantum	Proven secure

Figure 41: Table of QKD protocols between DV and CV ones. I don't cover them all in this book. Sources: Source: [274].

There are several QKD trust models beyond the basic DV/CV distinction, as shown in Figure 42. **DI-QKD** (device-independent QKD) derives security from observed Bell correlations and substantially reduces the need to model the internal behavior of the quantum devices, but it does not eliminate every side channel or laboratory assumption [317–321]. It still requires, among other conditions, secure laboratories, private randomness, an authenticated classical channel and closure of the relevant Bell-test loopholes. **MDI-QKD** (measurement-device-independent QKD) removes detector-side-channel assumptions by allowing the central measurement station to be untrusted [322, 323]; it still relies on assumptions about the users' state preparation, and it also has CV variants [324]. [325] proposed in 2026 to make CV-MDI-QKD relay chains fault-tolerant with bosonic GKP codes, although its numerical assumptions remain far beyond current implementations. A loophole-free DI-QKD experiment using two independently trapped rubidium atoms in buildings about 400 m apart was reported in 2022 [326]. A 2026 Chinese experiment extended a memory-assisted DI-QKD building block to a 10 km physical fiber link and reported positive asymptotic key calculations at longer effective loss [327].

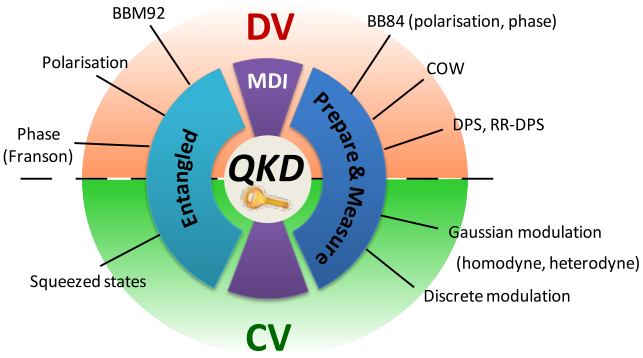


Figure 42: Map of QKD protocols. Source: slide 9 in [328].

Quantum Conference Key Agreement (QCKA) is an extension of QKD protocols to enable the generation of quantum secret keys among several users. The protocol can make use of N-dimension entangled GHZ states share across the parties or work with continuous variable photons [329]. There is even an MDI-QCKA variant using post-selected GHZ states [330, 331] and an anonymous QCKA version [332]. A phase-matching QCC variant was experimentally demonstrated in 2026 by Jian-Wei Pan's team over intercity fiber channels in both symmetric and asymmetric loss configurations, the asymmetric one being the realistic case in deployed networks where users sit at different distances from the relay [333]. [334] surveys the broader multiparty quantum key agreement architectures, their state of the art and their open problems.

Quantum Secret Sharing (QSS) is a multiparty cryptographic primitive related to QKD. A dealer can distribute a classical or quantum secret so that only authorized subsets of participants can reconstruct it. In a simple threshold example, Alice may require Bob and Charlie to cooperate because neither participant alone is authorized to recover the secret. Security can use entanglement, measurement disturbance and no-cloning, but the exact guarantees depend on the QSS protocol and threat model. QSS can therefore protect keys, classical secrets or quantum states, rather than being restricted to key distribution [335].

Quantum Random Access Codes (QRACs) are quantum information protocols encoding classical information into quantum states so that a receiver can retrieve any one of the encoded classical bits with higher success probability than would be possible classically [336]. Superdense coding can transmit two bits of information on a single qubit, but with the use of entanglement.

High-dimensional QKD encodes more than one bit per photon using time-bin, frequency or orbital angular momentum (OAM) modes, which raises the information capacity per detected photon and the tolerance to noise, at the cost of much more complex state analyzers. A 2026 UCLA, TU Wien and JPL collaboration certified 5.7 entanglement bits (ebits) in a time and frequency entangled biphoton frequency comb, using a witness that avoids the intractable full state tomography

of large Hilbert spaces [337]. Bright high-dimensional temporal entanglement sources were also demonstrated in Vienna [338] while [339] surveys the OAM-encoded high-dimensional QKD experiments. The practical figure of merit remains the secret key rate per second at a given channel loss and not the Hilbert space dimension, and high-dimensional setups seldom win on that metric once their analyzer losses are accounted for.

Quantum digital signatures (QDS) extend quantum cryptography to message integrity, authenticity and non-repudiation instead of key exchange. A 2026 experiment from Guangxi University combined a phase-stable Sagnac polarization modulator, gigahertz-rate encoding and low-jitter SNSPDs with a one-time universal hashing QDS protocol, reaching 250 km of fiber and improving the signature rate by more than two orders of magnitude over previous demonstrations [340]. Signature rates are still counted in signatures per second or worse for megabit messages, which shows how far QDS sits from operational use. **Quantum secure direct communication** (QSDC) transmits the message itself instead of a key, with a one-way variant using the measurement basis choice as the shared secret [341]. At last, "quantum telepathy" revisits pseudo-telepathy nonlocal games as a near-term application of small quantum processors sharing entanglement [342]. The naming is unfortunate since nothing is transmitted, and the proposed use cases are so far of a benchmarking nature.

1.4.2 QKD experiments and deployments

China operates by far the largest intercity QKD infrastructure, while Europe, Korea, Japan and other regions host a mix of research experiments, telecommunication operator pilots and limited commercial deployments. Outside China, most networks are still smaller-scale pilots rather than nationwide production infrastructure. Many breakthrough experiments have been conducted both in free space and over optical fiber, particularly in Europe (Figure 43), with prepare-and-measure QKD still more common in deployed systems than entanglement-based networking.

Open-air or free-space QKD demonstrations started in 1996 in the USA on a distance of 75 m, then on 144 km to connect the islands of La Palma and Tenerife in the **Canary Islands** and conducted by Austrians in 2007 and 2010 [343, 344], in 2019 in urban areas in Italy with a distance of 145 m [345]. It took place at 1,550 nm in the infrared band that is commonly used in fiber optic transmissions and therefore compatible with many existing telecommunication equipment. They used a silicon chipset doing all the work with an error rate of only 0.5% and a data rate of 30 kbits/s. Their QCosOne ("Quantum Communication for Space-One") used telescopes with 120 and 315 mm optics for transmission and reception. It worked during daytime, but there were still problems in case of turbulence and depending on the time of day and the side effects coming from the sun. Performance was better in the evening. They used triple photon encoding: temporal, spatial and spectral. It was achieved in India in 2022 over 300 m [346] and in Austria in 2023 over a distance of 10 km [347]. While these experiments used optical photons, other approaches are investigated like using mm and THz electromagnetic waves, requiring photon sources and detectors operating at 4K, which is not very practical on a large scale [348]. Free-space QKD distribution has its own challenges due to various atmospheric perturbations [349, 350].

An experiment took place in **Vienna** in 2008 as part of the European **SECOQC** (*SEcure COmmunication* based on Quantum Cryptography) project launched in 2004, involving some 40 research laboratories and vendors, using a "mesh" architecture and a CV-QKD optical link [294]. This went on in Switzerland with **IDQ** with local banks. In 2007 they also piloted an election vote counting system based on a QKD.

UK deployed in 2018 its UK Quantum Communications hub between Bristol, London, Cambridge and Ipswich. The network was extended in Cambridge in 2019 as seen in [351]. In 2023, HSBC protected some AI-power foreign exchange trading with a QKD, but without explaining which parties were securely connected [352].

In France, **Orange** announced in May 2019 the launch of tests of a QKD protected communication with the University Côte d'Azur (UCA) which provides the solution via the InPhyNi laboratory. It connects the Valrose and Inria campuses in Sophia Antipolis with an access point on the Plaine du Var IMREDD campus in Nice, using dark fibers over 48 km [353]. In January 2025 the team presented the implementation of a time synchronization protocol using two rubidium clocks [354]. The test network was operational in September 2021. Orange is studying the reliability of trusted optical network nodes in such a configuration. The operator is also looking to combine QKD solutions to protect physical links and PQC solutions that could be used as a method of encrypting data transmitted in association with a QKD. This was done in 2025 by securing the so-called trusted nodes with PQC [355]. In November 2025, the same InPhyNi team described the complete automation of this energy-time entanglement link, with a continuous key generation over 325 hours on the 50 km path between downtown Nice and Inria in Sophia-Antipolis, an extension to a 100 km four-node path reaching the GéoAzur optical ground station at Caussols which prepares future satellite links, and a wavelength-demultiplexed BBM92 operation serving up to 36 users on different ITU channels [356]. Their setup needs no additional synchronization or analyzer-stabilization signal, which saves fiber resources and removes an auxiliary classical synchronization channel, but not the authenticated classical channel required by QKD itself.

In **the Netherlands**, QuTech, TNO and TU Delft team connected in 2024 two NV center based QPUs across 25 km between Delft and The Hague using telecom fibers,

and in collaboration with Fraunhofer Institute for Laser Technology (Fraunhofer ILT) [357].

Denmark's DTU launched a CV-QKD trial with Danske Bank in 2022 [358] and another one between NBI and DTU [359].

Ireland announced in 2022 the creation of a Quantum Communications Infrastructure network, cofounded by the EU as part of the EuroQCI project, with a total investment of $10M. The project is run by 6 local universities along with HEAnet and ESB Telecoms.

Greece's Space Hellas and the University of Athens launched in 2022 a pilot QKD deployment after having started an OpenQKD project in 2019 with Datacom.

Cyprus announced in 2022 its deployment of a QKD network with a EuroQCI EU funding of €7.5M as part of the CYQCI project.

Poland launched a QKD network using trusted nodes with 1,700 km of connections with the help of IDQ [360].

OpenQKD

European Union

The European consortium **OpenQKD** is experimenting a terrestrial QKD network. It prepares the ground for the launch of the **EuroQCI** network which would be an operational implementation of a terrestrial and satellite European QKD network [361, 362]. This involves in particular France, Germany, Austria, Italy, Spain, the Netherlands, Greece, Switzerland and Poland and vendors like Thales Alenia Space (satellite communication), Orange and Mellanox (a subsidiary of Nvidia). It is about deploying a large interoperable experimental QKD network on a European scale, exploited by applications in various fields (healthcare, energy grids, transportation, finance, government, education, and the like). The consortium also intends to influence QKD standardization. And as far as possible, it is also about contributing to the development of a European industry offering in QKD and associated technologies. There is finally a deployment of QKD across Italy, Slovenia and Croatia [363].

In France, the test area is the Paris region and its major research laboratories with the Institut d'Optique, Telecom Paris, LIP6 in Paris and Nokia labs in Villarceaux, the project having received €15M from Horizon 2020, independently of the Quantum Flagship. Thales announced in December 2021 that it was participating in the QSAFE consortium with Deutsche Telekom, Telefonica and the AIT (Austrian Institute for Technologies) to create a European quantum telecommunication infrastructure as part of EuroQCI, with both terrestrial and satellite links. Another inter-country experiment is being run between Spain, Germany and Poland, including terrestrial and satellite QKD distribution and its hybridization with PQC [364, 365]. In October 2024, EuroQCI got a new EU funding of €97M.

A 2026 Austrian study addressed the planning and sizing of national terrestrial QKD networks, optimizing the number and the placement of trusted nodes given the 80 km span constraint of deployed fibers and the resulting end-to-end key rates [366].

Latvia's state operator LVRTC also announced in 2025 the creation of the first quantum communications backbone of the Baltic region [367].

USA's first experiments were conducted in Boston by **DARPA** between 2004 and 2007. A QKD network piloted by **Battelle** was tested in Ohio in 2013 [368]. Tests were also conducted in 2015 at **MIT**, linking two sites 43 km apart. It became the Boston-Area Quantum Network (BARQNET) linking the MIT Lincoln Laboratory, MIT, and Harvard University [369, 370]. A commercial deployment of QKD on an unused 800 km fiber optic network connecting Boston to Washington DC is also being deployed by **Quantum Xchange** and **Zayo**, to connect Wall Street finance businesses with their back-offices in New Jersey. It uses some trusted node technology [371]. An 85 km facility was also deployed in Chicago in 2019 [372]. In July 2020, the Department of Energy announced the expansion of the QKD network to link all its research laboratory sites [373]. In 2022, it connected the DoE Argonne and Fermi labs and enabled fast network synchronization of quantum and classical signals coexisting on the same optical fiber over 59 km [374]. Argonne lab develops the InterQnet architecture to advance scalable quantum communications [375]. In 2023, **Stony Brook University** was awarded a $6.5M grant from the Long Island Investment Fund to build a Quantum Internet Test Bed.

Similar efforts are conducted with UMass (Massachusetts) as part of the Center for Quantum Networks, a $26M, five-year, effort led by the University of Arizona, one of the NSF Quantum Engineering Research Centers [376]. The University of Rochester and Rochester Institute of Technology built in 2025 an experimental QKD network, RoQNET, connecting their campuses over 11 miles of optical fiber [377]. At last, the University of Chicago and Caltech are proposing a nationwide QKD deployment using vacuum beam guides using arrays of lenses that avoids the need for quantum repeaters [378]. In August 2026, Quantum Corridor, Ciena and Toshiba tested a 1.6 Tb/s quantum-safe encrypted transmission on a live optical network, combining Toshiba QKD systems with Ciena optical transport encryption [379]. As always with these announcements, the quantum part is only the key delivery, the encrypted data remaining classical and symmetric, and the headline Tb/s figure is the classical data rate, not the key rate.

In the ambitious **DARPA QuANET** (Quantum Augmented Network) project that was launched with a RFP in June 2023 [380], a 51-month project, DARPA is asking bidders to propose architecture and technology solutions to merge entanglement distribution and regular fiber optics lines for various applications involving quantum sensors and quantum computers. The constraints are

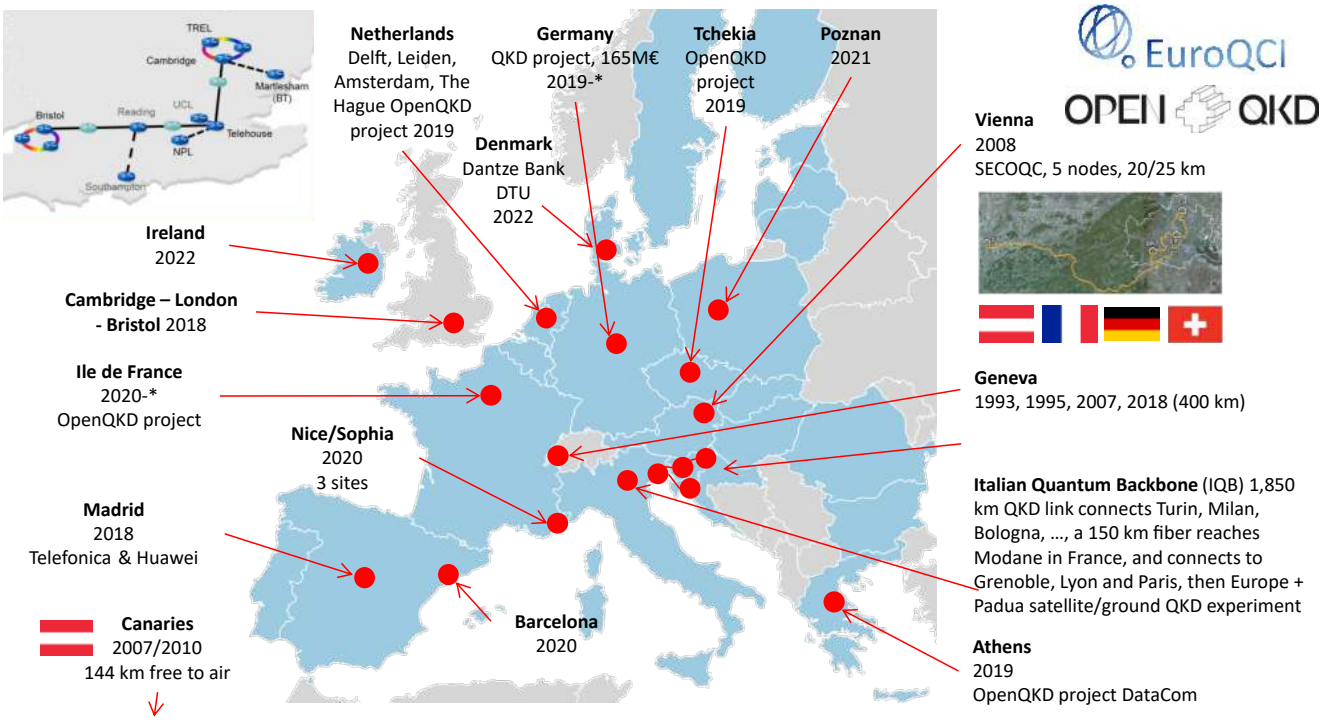


Figure 43: Map of QKD test deployments throughout Europe. © Olivier Ezratty, 2022-2023.

that no QKD should be proposed nor any repeaters. They want qNIC (quantum network cards) able to handle both classical and quantum communications. It looks like being a very low TRL project.

Canada launched in November 2020 its Canada Quantum Network through a partnership between Xanadu, the Creative Destruction Lab and the startups service company MaRS around Toronto. Another similar testbed project was launched in Quebec in October 2023, around Sherbrooke.

India's Defence Research and Development Organisation (DRDO) with IIT Delhi demonstrated a QKD for a distance of 100 km in 2022. The country launched its first operational QKD network in 2023 between two sites in Delhi.

In **Japan**, Toshiba announced in September 2018 that a QKD solution co-developed with the Tohoku Medical Megabank Organization (ToMMo) at Tohoku University had achieved a QKD throughput of more than 10 Mbps during one month.

South Korea deployed a QKD network with SK Telecom and IDQ that connects 48 government sites over a single 800 km network. It was certified by the South Korean National Intelligence Service (NIS) in February 2025.

Singapore's Quantum Engineering Program (QEP, 2018) from the National University of Singapore (NUS) launched the National Quantum-Safe Network (NQSN) which is starting classical and quantum network trials supporting both QKD and PQC. They planned to have 10 fiber nodes. This is done in partnership with AWS and Thales. One of the challenges in deploying QKD is the miniaturization of its components. Whereas initially a complete rack of hardware was needed for quantum key transmitting/receiving stations, the goal is to fit everything in a photonics component a few mm long. This is what **NTU** researchers in Singapore did in 2019 to manage a CV-QKD supporting existing telecom operators' fiber infrastructures [381]. But this miniaturization deals here only with the photonics part (Figure 44). These photonic circuits must be completed by classical electronic components.

The development of such integrated photonics components will also be supported in the framework of European Horizon Europe projects that follow Europe 2020 projects over the 2021-2027 period. A point-to-point 3 km QKD testbed was deployed in 2023 with the help of AWS, Horizon Quantum Computing and Fortinet, with a VPN tunnel using both a QKD and AWS Edge Compute hardware [382]. A larger 46 km QKD network named Q-CAN was launched by JPMorganChase in 2024, with 100 Gbps network secured with IDQ QKD [383].

The local operator Singtel is also building a country-wide QKD-based network [384] as part of the National Quantum-Safe Network Plus (NQSN+) project. Among others, they partner with IDQ and Cisco.

South Korea has an ongoing project with 800 km of QKD implementing any-to-any connections, also with the help of IDQ. In 2024, SK Telecom launched the X Quantum Alliance to develop a quantum secured communications network for South Korea. It was about building a Q-HSM cryptography chip containing a QRNG coupled to PQC. It seems to use a QRNG chip from ID

Quantique [385], itself using a Single Photon Avalanche Diode (SPAD) from Wooriro (South Korea) and an encryption module from KCS (South Korea). X Quantum launched Q-HSM commercially in 2024, combining QRNG and PQC technologies. SK Telecom has since then extended its quantum-security work toward PIC-based, wireless and satellite QKD.

Brazil operates the Hermes quantum network run by the Military Institute of Engineering (IME) in Rio de Janeiro. A 2026 study characterized an ID Quantique Clavis XGR over long continuous periods on a 40.3 km indoor spooled fiber and on a 3.5 km deployed underground fiber between IME and the CBPF physics research center, keeping an interferometric visibility above 97% and a QBER below 1% on average, but showing that the dominant instability comes from the internal device temperature under unregulated tropical ambient conditions rather than from the fiber itself [386].

China stands out since 2016 with impressive QKD experiments and large scale deployments. The country invests heavily in QKD with a now classical multi-pronged strategy: to protect its sensitive communications against any attacker and to develop an industry in a promising emerging technology field. A first deployment was carried out in 2012 in the Hefei area to link various Chinese government entities [387]. It was then expanded with an installation of a QKD-secured fiber optic link between Shanghai and Beijing, covering 2,000 km.

The line installed between 2013 and 2016 was deployed by a local startup, **QuantumCTek**. The network relies on 32 transponders with secured physical access [388]. Indeed, the signal attenuation was then too strong beyond about 50 km on one optical fiber.

The entities using this line are government agencies, including various financial sector regulatory agencies and banks.

The country also plans to protect its energy grid infrastructure with this network [389].

China announced several successive national-scale quantum-secure communication plans after completion of the Beijing-Shanghai backbone. The newer China Quantum Communication Network (CN-QCN) is a trusted-relay backbone integrated with metropolitan networks and satellite ground stations [282]. Earlier metropolitan deployments include the Hefei network described in [390].

As reported in 2025, the new CN-QCN backbone contains approximately 10,103 km of fiber, 145 fiber backbone nodes, 20 metropolitan networks and 6 satellite ground-station backbone nodes linked with the Jinan-1 microsatellite, covering 17 provinces and 80 cities [282]. CN-QCN is interconnected with the earlier Beijing-Shanghai Backbone Network, and the combined fiber mileage exceeds 12,000 km. The deployed network mixes several QKD equipment types and remains based on trusted relays.

In September 2023, a team led by Jian-Wei Pan reported the deployment of a three-node entanglement-based QKD setup at a city scale in Hefei using quantum nodes with atomic quantum memories [391].

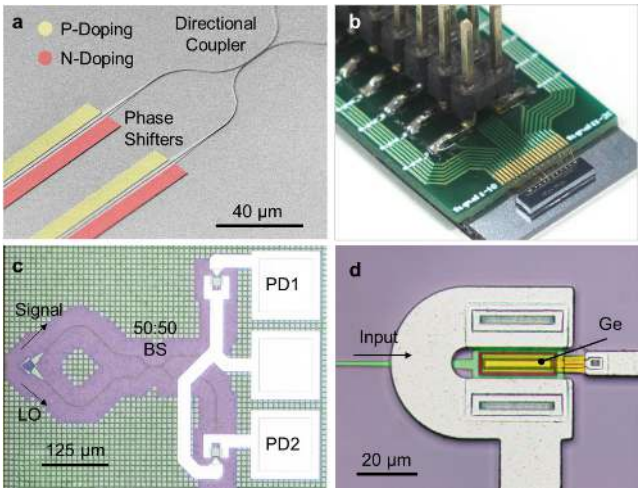


Figure 44: A QKD photonic chip developed in China in 2019. Source: [392].

China Telecom announced in 2023 an investment of $438M in quantum communications research and development [393]. In November 2023, China Telecom announced the introduction of a QKD smartphone, the Huawei Mate 60 Pro. It seems that the only item being quantum in the smartphone is a QRNG chip, coming from QuantumCTek. It probably also uses some PQC encryption, potentially coupled to some telecom operator backend QKD [394]. In March 2024, China Telecom announced the acquisition of a majority stake in QuantumCTek. Also in 2024, a research team prototyped a small scale experiment of QKD-protected e-commerce architecture, which will not be easy to scale practically [395].

In France, the civil cybersecurity agency **ANSSI** published an information note in May 2020 in which it expressed certain reserves about the QKD [396]. It highlighted the fact that it does not address a common problem, cannot guarantee perfect inviolability, and requires dedicated optical infrastructures. Instead, it recommends focusing on PQC.

This followed a memo of equivalent content from their British **NCSC** counterparts published in April 2020 [397, 398]. A similar publication from the **NSA** was released in October 2020 [399]. It was renewed in 2021 and 2022. Again, in 2024, a joint note from ANSSI and its German, Swedish and Dutch peers showcased the same objections [400]. Scientists from ETH Zurich published a documented rebuttal to these objections in 2023 [401], followed by another one from Terra Quantum [402]. The bulk of the answers is: "*work in progress*", particularly as QKD related hardware is being shrunk-wrapped and commoditized. Also, it would make sense to deploy quantum networks implementing entanglement resources, which are the only ones enabling a

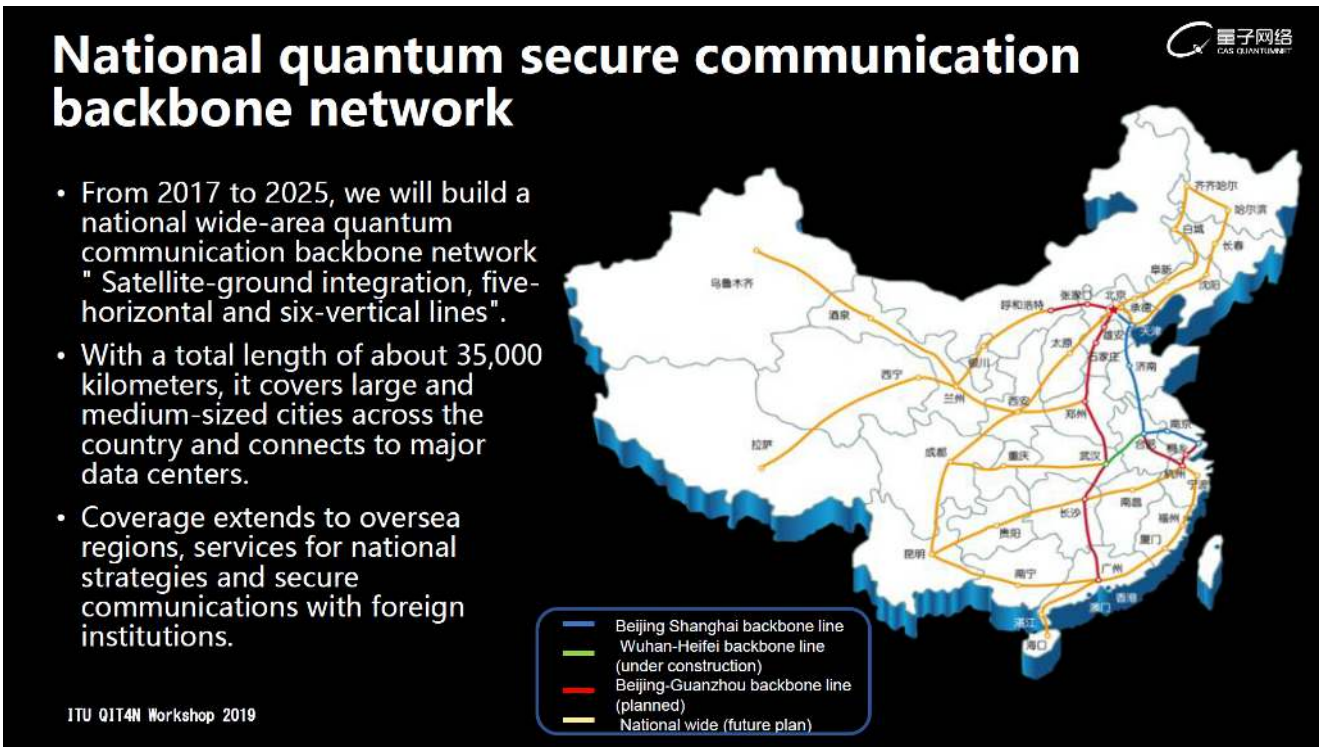


Figure 45: China's 33,000 km QKD backbone plan as presented in 2019. The operational CN-QCN reported in 2025 contains approximately 10,103 km of newly deployed backbone fiber, interconnected with the earlier Beijing-Shanghai backbone and metropolitan networks [282].

broad scope of use cases including connecting quantum networks, quantum computers and quantum sensors.

Emulation and control software. Given the cost of QKD hardware, the domain research increasingly relies on software emulators of QKD architecture, particularly for deployment planning. Quditto emulates and orchestrates distributed QKD network deployments with virtualized nodes, allowing to test key management and applications without any quantum hardware [403]. Arqon is a suite of control applications aiming at reliable quantum networks, coming from Stephanie Wehner's team at TU Delft [404]. [405] describes a CV-QKD channel emulator built for the SPOQC mission, reproducing on the bench the loss and excess noise budget of the space link. And [406] covers a multi-purpose quantum communication network stack going beyond QKD, with actual protocol implementations.

1.4.3 QKD by satellite

Satellite quantum communication is another way to distribute quantum keys that makes sense over long distance. They can also potentially enable other quantum communications applications like distributed quantum computing based on entanglement distribution [407]. In quantum communications, quantum keys can be created across two locations while the encrypted data will be transported in classical terrestrial or satellite communication channels.

For intercontinental distances, satellite links can avoid the exponential attenuation accumulated by thousands of kilometers of terrestrial fiber without requiring a chain of quantum repeaters [408]. The atmospheric part of a satellite link is concentrated near Earth, but there is no generic 3 dB atmospheric-loss figure. The total optical link budget also includes diffraction, finite telescope apertures, pointing error, turbulence, detector efficiency and background noise, and is commonly tens of decibels for satellite QKD.

Still, atmospheric refractive-index inhomogeneity produces beam wander, wavefront distortion and beam broadening [409]. Turbulence is generally more severe for uplinks because the beam encounters the strongest near-ground turbulence before it has expanded, and it can degrade entanglement distribution [410, 411] (Figure 46). Above the atmosphere, absorption is negligible, but free-space loss remains dominated by geometric diffraction and pointing. In the far field, received geometric power scales approximately as $1/R^2$ for fixed apertures, whereas fiber transmissivity decreases exponentially with distance as $10^{-\alpha L/10}$. It means that for long communicating distances of several hundred km, satellite-ground channels have an advantage over fiber-based channels in terms of channel losses [412]. This explains China's strategy which combines satellite QKD for connecting large urban nodes which use terrestrial QKD.

However, free-space channels are vulnerable to denial-of-service attacks and to weather-dependent availability

that requires operational countermeasures [413]. Clouds can completely block an optical link, but a statement such as "available only half of the time" is site- and climate-dependent rather than a universal property of satellite QKD [414].

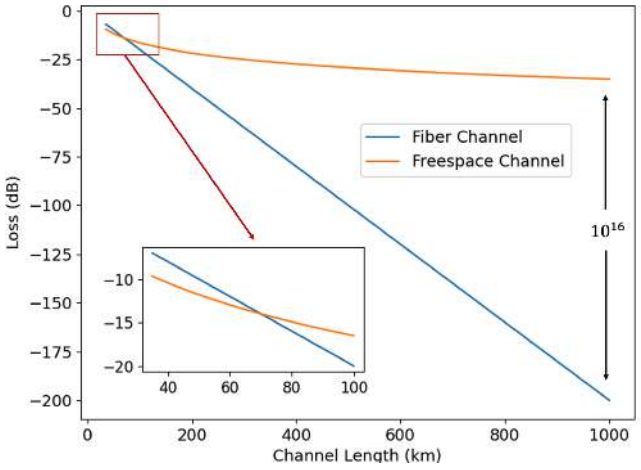


Figure 46: How photon losses compare between fiber and free-space channel using satellite. The free-space channel exhibits an advantage beyond approximately 70 km for the assumptions used in [412]. Source: [412].

Wavelength choice strongly affects detector technology, solar background, atmospheric transmission and diffraction, but it does not impose a strict day/night boundary. The 700–900 nm band benefits from efficient low-noise silicon detectors and has been used for daylight QKD demonstrations, while the 1,550 nm telecom band offers lower solar spectral background and direct compatibility with telecom components [415, 416]. For equal transmitter aperture, the diffraction-limited angular divergence scales approximately with wavelength, so 1,550 nm has about 1.9 times the divergence of 800 nm and about 3.8 times the far-field beam area, all else equal. Micius operated mainly at night because of its complete link and detector design, not because 800 nm QKD is fundamentally impossible in daylight. Turbulence-induced beam wander can be mitigated with adaptive optics or spatially adaptive detection [417].

If satellite QKD matures, multiple QKD satellites operating in low Earth orbit will require coordinated resource allocation and optimization [418–422] as well as satellite identification [423]. Digital twins could support the management of the managed satellite network [424], replicating the whole Quantum Satellite Network (QSN) [425, 426].

China satellite QKD experiments

China has been a pilot country in satellite QKD distribution, having launched two QKD satellites [427]:

- **Micius-1**, launched in 2016, *aka* Mozi, the name of a Chinese philosopher who lived circa 470–391 BCE (Figure 48). It was used for running several different experiments: a satellite-to-ground decoy-state QKD with kHz-level key rates over up to 1,200 km and satellite-replayed intercontinental key exchange, a satellite-based entanglement distribution to two Earth locations separated by 1,205 km and a ground-to-satellite qubit teleportation as part of the QUESS project (Quantum Experiments at Space Scale) [428–432]. The satellite weighs 640 kg, consumes 560 W and is positioned in low Earth orbit (LEO) at about 600 km [433]. We detail these experiments below.

- **Jinan-1,** launched in 2022 and operating in LEO at about 500 km, was reported in a peer-reviewed Nature paper in 2025 [434]. Its QKD payload is of about 23 kg and the portable optical ground station about 100 kg. The experiment demonstrated real-time key distillation with multiple ground stations and generated up to 1.07 million secure key bits during one satellite pass. It also established a key between China and South Africa, separated by more than 12,900 km, which was used for one-time-pad image encryption (Figure 51).

- China also plans the launch of a low-Earth-orbit satellite constellation by 2030 dedicated to sending quantum keys by repeating this process [435].

A 2018 experiment demonstrated a secure videoconference between China and Austria using keys distributed through Micius-1. Jian-Wei Pan had completed his PhD in Vienna under Anton Zeilinger, who led the European side of the collaboration. The Micius entangled-photon source generated about 5.9 million pairs per second, while the end-to-end two-ground-station experiment detected only about one coincident pair per second because of the very large optical link loss and finite detector efficiency [436]. Satellite scheduling and key buffering are therefore important operational issues [435]. The original Micius experiments were operated mainly at night because of the link background and detector configuration.

China announced in 2020 the miniaturization of its ground receiving station from 10 tons to 80 kg. The key bitrate was reduced, from 40 Kbits/s to 4-10 Kbits/s. The experiment took place, on the Earth side, in Jinan and Shanghai, so it seems at sea level [438, 439].

In 2021, China reported the first large integrated space-to-ground quantum communication network, combining more than 700 fiber-QKD links with two satellite-to-ground links and enabling secure user connections over separations up to 4,600 km [440].

A paper published in 2022 reported a space-to-ground QKD network experiment performed with the Tiangong-2 space laboratory and four ground stations [441]. The underlying passes had been performed before Tiangong-2 was deorbited in 2019. Tiangong-2 acted as a trusted QKD relay for the ground stations, while the same ground network could also receive keys from Micius. It was therefore not a quantum repeater preserving an end-to-end quantum state.

Figure 47: The Micius QKD satellite from China that was launched in 2016.

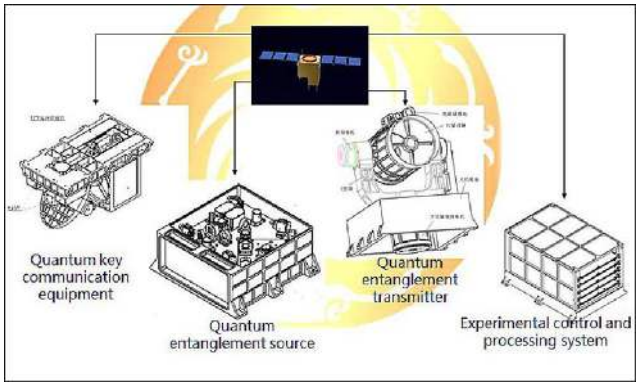


Figure 48: The Micius satellite payload. Sourve: [437].

In 2023, a QKD test was done using Micius satellite between a China ground station in Urumqi and a Russia ground station near Moscow over 3,800 kilometers [442].

Other satellite QKD experiments

But China is not alone in testing satellite QKD links.

In **Europe**, satellite-QKD plans and architecture proposals started well before 2020, including projects in France [416, 443], Germany [444] and the UK [445]. The EU is also developing secure-connectivity satellite infrastructure with quantum-key-distribution components. EAGLE-1 is led by SES with ESA and a consortium of more than 20 European companies. As of September 2026, ESA schedules its launch for late 2026 or early 2027, followed by three years of in-orbit QKD validation [446–448].

It will use a **Tesat** QKD satellite payload. TeQuants is an EU supported research project led by Thales Alenia Space and Airbus Defence and Space that is about preparing space quantum network technologies supporting entanglement and its applications. Based on these technologies, Airbus Defence and Space and Thales Alenia Space are working on a space entanglement distribution satellite demonstrator called QINSAT (Figure 49).

On the science front, Eleni Diamanti's LIP6 team in France is working on using adaptive optics to improve key sharing with satellite [449, 450]. Her team is also working with InPhyNi and Thales on satellite QKD architecture designs and simulations [416, 451]. The European collaborative project **QUDICE** gathers various universities (ICFO, Padova, Sorbonne, Malta) and vendors like Thales Alenia Space, Sateliot (Spain) and ThinkQuantum (Italy) for the development of hardware components for satellite-based QKD communication networks. LIP6 is as well preparing the reference architecture of future QIN including space component, notably within a PhD with Airbus Defence and Space.

On the source side, a Singapore, France and Sorbonne collaboration ran a terrestrial readiness campaign with a space-qualified entangled photon-pair system ahead of a space-to-ground demonstration [454]. The Nice team designed a dual-wavelength source of entanglement dedicated to space quantum communication [455], and [456] presents a scalable near-visible integrated photon-pair source targeting satellite quantum science. QuaNTUM is a modular quantum communication testbed designed in Germany to combine fiber and satellite links in the same architecture [457].

Canada is developing **QEYSSat** (Quantum Encryption and Science Satellite), a space-QKD demonstration mission [452]. As of September 2026, the Canadian Space Agency lists the mission as "in development" with launch no earlier than 2026 and a nominal mission duration of one year, extendable by one additional year. The project involves the University of Waterloo and Thomas Jennewein's team [458], with UK partners including Craft Prospect, the University of Strathclyde and the University of Bristol. The University of Ottawa is working on adaptive optics for the ground station [459].

Singapore and its universities and startups are working on CubeSat-based tiny QKD distribution satellites [460].

UK's Quantum Communications Hub is running the In Orbit Demonstration (IOD) mission to demonstrate QKD from space with a satellite payload supporting new quantum signal transmission and quantum receivers in its Hub Optical Ground Station (OGS). It will rely on ISISPACE Group (the Netherlands) for satellite systems and services. As mentioned before, UK universities and vendors are teaming up with Canada as well for space QKD applications.

NASA's SEAQUE (Space Entanglement and Annealing QUantum Experiment) is a small quantum-communication technology experiment that launched

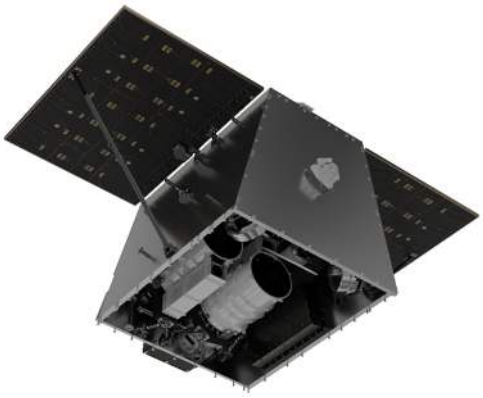


Figure 49: Airbus Defence and Space entanglement demonstrator mission based on a low-Earth-orbit (LEO) platform and heritage optical communications terminals. Source: Airbus Defence and Space. It shows a possible solution for QINSAT including an entanglement-based source and two optical terminals for the photon pair distribution. October 2025.

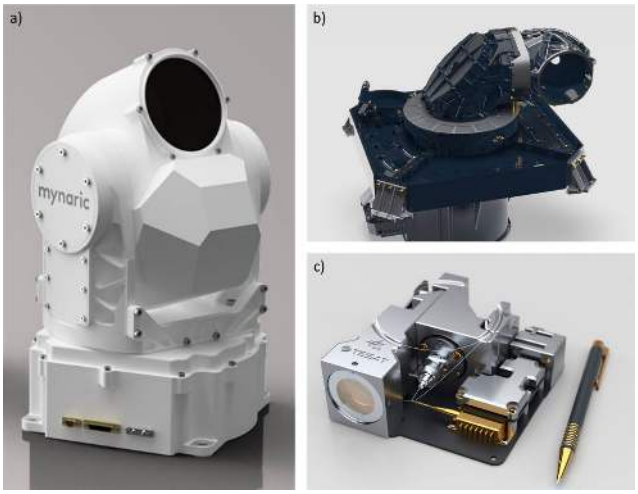


Figure 50: Examples of optical terminals for satellite-to-satellite and satellite-to-ground communication, including a Mynaric Condor MK3 ground station (a), a Coarse Pointing Assembly (CPA) from Tesat (b), and a satellite optical module (c). Source: [452].

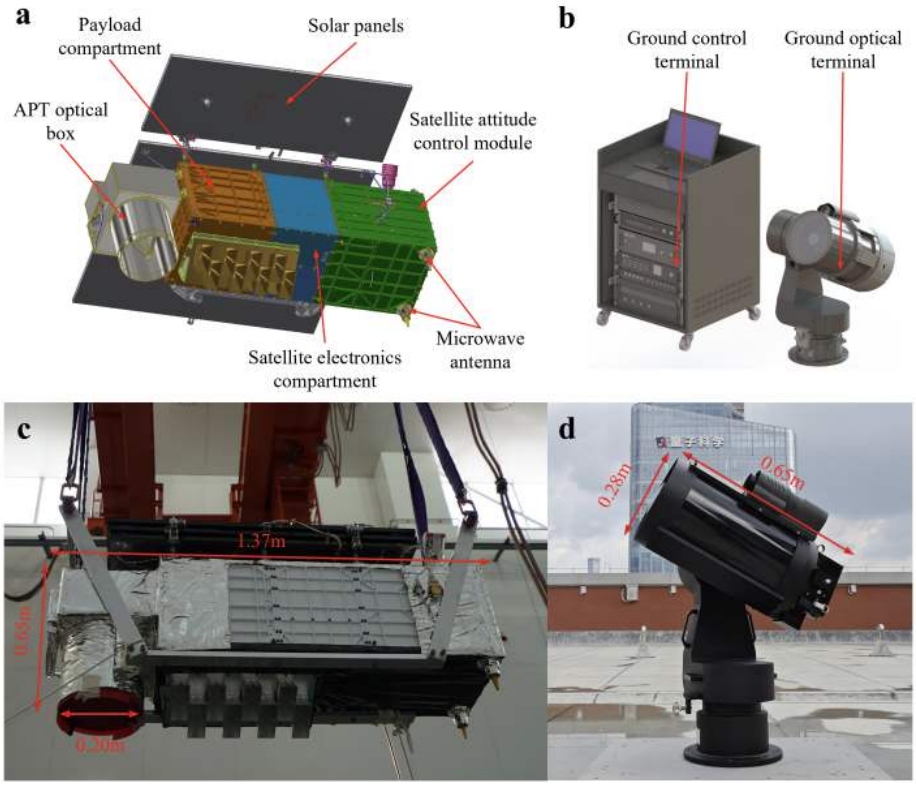


Figure 51: The QKD microsatellite and portable optical ground station (OGS) used in a 2024 Chinese experiment. Source: [453].

to the ISS aboard SpaceX CRS-31 in November 2024 and was installed on the station exterior. It tests an entangled-photon source and detector annealing intended to mitigate radiation damage [461]. HRL Laboratories and Boeing are also developing the Q4S satellite mission to demonstrate entanglement swapping on space-qualified hardware. In June 2026, Boeing reported successful high-fidelity ground testing and final spacecraft integration, with launch planned for 2027.

Many 2026 studies assessed the operational capabilities of satellite QKD [462]. [463] evaluated the limits of entanglement-based satellite QKD, showing how finite-

key effects, pointing errors and the short usable duration of a LEO pass, typically a few hundred seconds, cap the key length obtainable per pass. [464] analyzed a single satellite carrying its own quantum memory and acting as a repeater between two ground stations that are never simultaneously visible, [465] looked at satellite-augmented global repeater networks and [466] did show how multimode memories raise the throughput of satellite entanglement distribution. These are all multiplexing gains applied on top of a still very low baseline rate. On the industry side, IonQ acquired the American optical communications specialist Skyloom Global in November 2025 to build its own space quantum networking and sensing infrastructure [467].

QKD distribution was even tested in zero-G flights to see the impact of gravity changes, with positive results [468].

Satellite quantum computing

Using satellites for QKD is just a starter. They could also host onboard quantum computers, particularly using photons. This was demonstrated in 2025 by an European team using a small 6-mode quantum photon processor [469]. It could provide some local encoding capability for broad QKD networks, or to encode data coming from onboard quantum sensors (Figure 52).

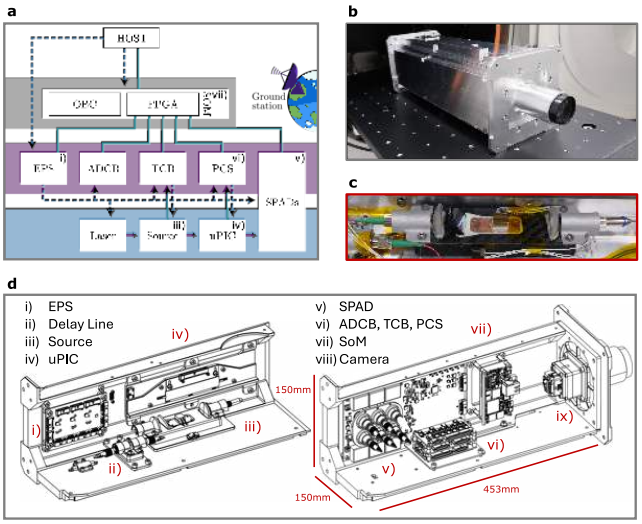


Figure 52: The onboard small photonic quantum computing unit embedded in a nanosatellite, built by an European consortium led by Austrian scientists in 2025/2026. Source: [469].

And beyond Earth, some are even devising how some extraterrestrial civilization could communicate with us with entangled photons. I am just wondering how these photon sources could be detected out of the noise coming from distant stars, even using all the technologies around to detect exoplanets (transit methods, spectrography, etc.) [470–472]. A BB84 QKD network was even deployed in a nuclear reactor by Toshiba, at the experimental reactor PUR-1 in Purdue University, Indiana [473].

1.4.4 QKD by UAVs

There are various proposals for the establishment of QKD networks using low-altitude platforms such as drones (UAVs) or balloons. These are “nice to have” experiments that may make sense for the military or other specific situations where a broad and dynamic coverage is required and landline capabilities are insufficient.

Chinese researchers announced in June 2019 that they had demonstrated optical QKD aerial links established within a network of 35 kg octocopter UAVs (unmanned aerial vehicles) spaced 200 m apart during a 40-minute flight at an altitude of 100 m [476, 477]. The payload handling quantum communication weighed 11.8 kg. It can still be miniaturized, since China is planning to integrate it into mass-market UAVs. In another paper from 2025, Chinese scientists proposed to use small chains of balloons flying at an altitude of 24 km [475].

QKD is also experimented with balloons (Figure 54).

Drone QKD is now also investigated in the USA [474] (Figure 53) and in India [478].

1.4.5 Underwater QKD

Underwater free-space QKD is also under investigation in Türkiye and China [479, 480]! The first simulations deal with 10 to 40 m distances. It is far from sufficient to enable communications with submarines, including nuclear-powered submarines. Unfortunately, water is not a clean medium and a lot of workarounds must be found to make it possible, like using CV-QKD [481]. Two 2026 papers refined these estimates, with a finite-key analysis of underwater QKD showing how the required block sizes bite when the channel is that lossy [482], and a comparison of BB84, SARG04 and BBM92 in seawater channels where absorption and scattering vary strongly with the water turbidity [483]. Even in the clearest Jerlov water types, the practical range stays in the tens of meters, restricting the use cases to short-range links like a submarine to underwater sensor connection.

Another option is underwater fiber, which avoids free-space attenuation in the water column but still has deployment, maintenance, endpoint and implementation-security constraints. It was tested in 2023 between Italy and Malta over 100 km as part of the NATO project SEQUEL (Secure Quantum Communication Undersea Link) [484] and between the UK and Ireland over 224 km [485].

1.4.6 QKD photon sources

We have already covered photon sources for quantum computing and seen some of their requirements like the creation of deterministic and indistinguishable photons, on top of the even harder challenge to create large clusters of entangled photons.

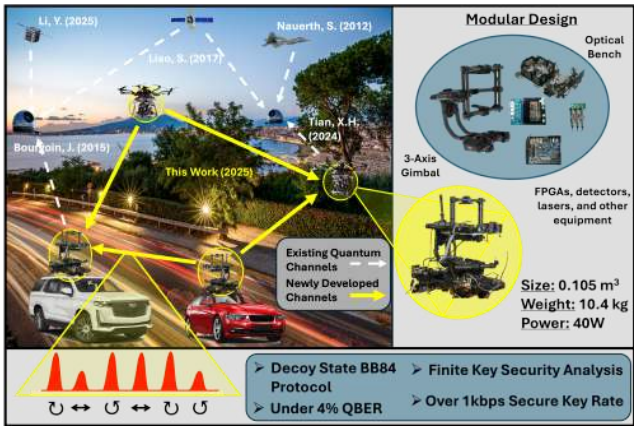


Figure 53: QKD experiments using small drones in the USA. Source: [474].

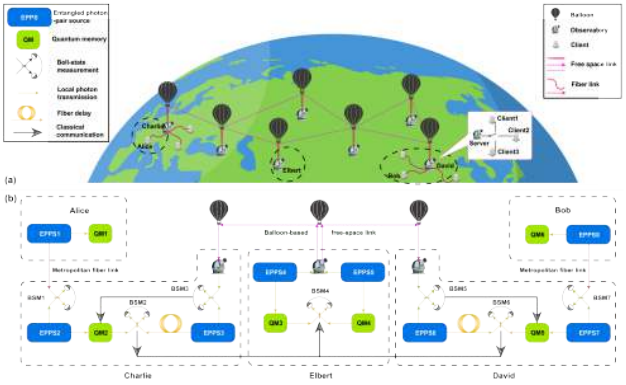


Figure 54: QKD using balloons flying at 24 km could provide broad regional ground coverage and, for some use cases, offer different operational trade-offs from LEO satellites. Source: [475].

The photon-source requirements for QKD differ substantially across protocols. Prepare-and-measure DV-QKD is commonly implemented with strongly attenuated coherent laser pulses plus decoy states, so deterministic single-photon emission is not a general requirement. Entanglement-based protocols require entangled-pair sources, while CV-QKD uses coherent or squeezed optical states rather than single-photon streams. Telecom wavelengths around 1,300 nm and 1,550 nm are advantageous for fiber links, whereas free-space QKD can also use visible or near-infrared wavelengths. Practical sources should be compact, stable and power-efficient; room-temperature operation is advantageous but not a security requirement.

The breadth of technologies used or investigated for photon generation is amazing [486]. Let's mention a few of these recent advances, first with color center defects [487]:

- **Vanadium defects in silicon-carbide** operating between 100mK and 3K with the benefit from a relative long stability [488].

- **Silicon with carbon atoms defects** aka G centers creating optical wavelength photons at 1,279 nm [489–493]. As shown in Figure 55, the electronically active G center is a complex of two substitutional carbon atoms and an interstitial silicon atom. Another intrinsic silicon defect resulting from irradiation of Si crystals is also studied, aka the W-center [494]. [495] covers the controllable fabrication of single G and W centers in silicon wafers using focused ion beams (FIB) with a probability exceeding 50%. The electron spin resonances of G centers were optically detected for the first time in 2026 by a Montpellier team, which turns them from mere photon emitters into candidate spin-photon interfaces usable in quantum repeater nodes [496].

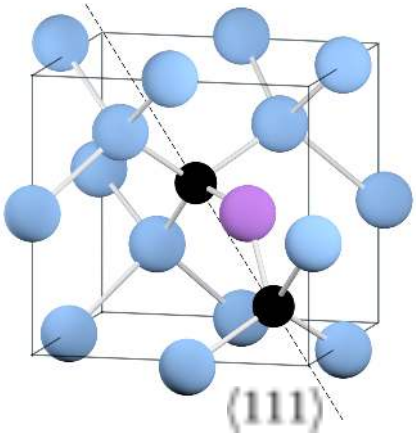


Figure 55: A G center and its two carbon atoms. Source: [497].

- **NV center-based** sources [498], like the ones studied by AWS and Element Six [499].

- **Other defects like SnV** (silicon-tin vacancies) which can even be used in cavities to improve their photon emission efficiency [500] and indistinguishability [501], as well as GeV (germanium vacancies) [502]. SnV spin qubits now emit highly indistinguishable photons [503] and were integrated in diamond nanobeams bonded onto Al_2O_3 waveguides, which is a path to scalable diamond photonic chips [504].

- **T-centers** in silicon emitting at 1,326 nm directly in the telecom O-band, now created epitaxially in silicon-on-insulator wafers instead of by ion implantation [505], with the broader question of controlling color center formation in SOI for on-chip photonic integration [506] and controlling charge noise [507].

- **Silicon carbide** with nitrogen vacancies coupled to nanophotonic resonators [508], embedded in nanopillars [509], with single erbium ions Purcell-enhanced at room temperature in silicon-carbide-on-insulator

microring resonators, emitting directly in the telecom C-band [510]. RF-free driving of the nuclear spins of these SiC color centers is also feasible, which simplifies the control hardware [511].

- **hBN** hexagonal boron nitride emitters, with a near-infrared emission from oxygen-related defects [512], cooperative emission between emitters sitting in the same layer [513] and the coupling of color centers with hyperbolic phonon polaritons [514]. Their emission wavelengths remain mostly outside the telecom bands, which mandates a frequency conversion stage.
- **Carbon defects in transition metal dichalcogenides** (TMDs) which are predicted to emit at telecommunication wavelengths [515].
- **A new diamond defect** showing a millisecond-scale spin relaxation time at room temperature, which would remove the cryogenic constraint for diamond-based spin-photon interfaces [516].

All these defects enable the creation of spin-photon or matter-photon entanglement, enabling to entangle remote quantum nodes at long distance [517, 518].

Then we have other photon sources, arbitrarily sorted by used materials, like:

- **InAs** quantum dots embedded in GaAs with a conversion to telecom wavelength at 1,550 nm generating indistinguishable photons [519, 520].
- **GaAs and InGaAs quantum-dot** single photon sources with high-source brightness ensuring high-speed quantum communication [521–527]. Many quantum dots are variants of the quantum dot pioneered by Pascale Senellart (C2N) and Quandela which are in InGaAs and are surrounded by stacked Bragg-reflectors made respectively with layers of GaAs and $Al_{0.9}Ga_{0.1}As$ (aluminum, gallium, arsenide). A record of 175 km distance was broken in 2022 using GaAs/InGaAs quantum dots and a finite key rate of 13 kbps over 100 km [528]. These quantum dot sources however suffer from low brightness. An October 2025 preprint from Quandela, C2N and Max Planck Institute for the Science of Light proposed to combined quantum dot sources with more traditional Poisson-distributed sources (PDS) such as attenuated laser pulses to maximize efficiency and prepare-and-measure QKD security [529].

  A rack-integrated quantum dot source of single and entangled photons in the telecom C-band was demonstrated in 2026 by Stuttgart and Würzburg teams, with an end-to-end transmission efficiency above 50% for both the exciton and the biexciton photons [530]. Gigahertz-clocked generation of highly indistinguishable C-band photons was also achieved [531]. [532] reviews the droplet etching epitaxy growth of these quantum dots and [533] the designs a broadband nanowire quantum dot cavity for the efficient extraction of entangled photons.
- **AlGaAs sources** with spontaneous parametric down-conversion (SPDC) enabling the creation of polarization and/or frequency entangled sources of photons or "biphotons" at telecom wavelengths [534–539].
- **GaN** sources can operate at room temperature and generate 1310 nm telecom wavelengths photons [540].
- **Silicon-nitride spontaneous parametric down-conversion** (SPDC) to create pairs of entangled photons [541].
- **Silicon-nitride MRR** microring resonator that can generate 8 pairs of heralded entangled photons directly at telecommunications wavelengths around 1,550 nm [542]. Microring resonators are tiny optical waveguides looped back onto themselves in circle or spiral, usually implemented in silicon semiconductors. They enable interference phenomena, the creation of delay lines, and the like [543–545]. Silicon-nitride waveguides can be combined with a laser using an InP based optical amplifier [546].
- **SiGe** first demonstrated in Austria in 2025 [547].
- **Silicon chip**, with an example demonstrated in Singapore, reporting a final secret-key rate of 1.213 Gbit/s over 10 km using a 40-Gbaud polarization-multiplexed CV-QKD system, with only the laser source outside the silicon chip [548] (Figure 56).
- **Thin-film lithium niobate** (TFLN) generating tunable entangled pairs [549], also used on the receiver side with a gigahertz-rate time-bin analyzer [550], with a poling-free SPDC scheme avoiding the periodic poling step in both lithium niobate and silicon carbide [551], and in a heterogeneous diamond-on-lithium-niobate platform combining diamond color centers with the fast electro-optic modulation of lithium niobate [552].
- **III-V on silicon nitride** with a wafer-scale heterogeneous quantum photonic platform [553], and **gallium phosphide on diamond** for a scalable spin-photon interface [554].
- **Van der Waals materials** with a monolithic and telecom-fiber-compatible tunable source of polarization entangled photon pairs [555].
- **Fiber-based Sagnac sources** of entangled pairs with a brightness suited to wavelength-multiplexed networks, as designed in Nice [556], alongside heralded quasi-deterministic SPDC sources which multiplex many probabilistic pairs to approach determinism [557, 558].
- **On-chip squeezing** with the generation and the detection of squeezed light on a single silicon photonic chip, which is the building block of a chip-scale CV-QKD transceiver [559].

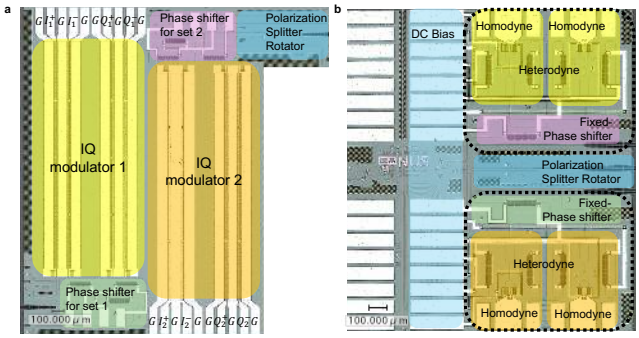


Figure 56: An example silicon-based chip for QKD distribution. Source: [548].

- **Spontaneous four-wave mixing** (SFWM) sources using nonlinear materials and generating entangled photon pairs and single photons [560]. It can use silicon on insulator (SOI), silicon nitride (Si_3N_4), Hydex, AlGaAs, and various other III-V semiconductor materials.

- **Fibers doped with rare-earth atoms or ions** with potential room-temperature operation [561], like neodymium ions in silica fiber [561–564], with rare-earth-doped TiO_2 thin films grown on III-V semiconductors as a route to hybrid quantum photonic interfaces [565]. In 2019, Chinese researchers demonstrated qutrit teleportation [566, 567]. High-dimensional encodings can in principle carry more than one raw bit per detected photon.

- Organic molecular sources, like a dibenzoterrylene (DBT) organic molecule embedded in a para-dichlorobenzene (p-DCB) host crystal, integrated within a planar metallo-dielectric antenna and solid immersion lens (SIL), which operates at ≈ 1.4 K [568].

The photonic integrated circuits (PIC) containing the photon sources or receiving single photons from external sources usually incorporate a mix of waveguides and interferometers (MZI). The waveguide can be realized with lithium niobate (good for high-speed modulation [569]), GaAs (efficient light-emitter due to its direct bandgap, fast operations, but complex to manufacture), InP (used for both active and passive components), silicon (highly refractive, easy to manufacture in CMOS process), silicon nitride (low propagation losses, highly transparent to visible and infrared light). Complete QKD transmitters are now built on these platforms, with a time-bin BB84 system combining an indium phosphide modulator chip with a silicon nitride interferometer chip [570] and with a highly integrated silicon photonics QKD transmitter from a Chinese team [571]. The recurring limitation is that the laser source and the single-photon detectors usually stay off-chip.

Some sources like quantum dots, and NV centers and atoms do not generate photons in telecom wavelengths, in the 1300 to 1550 nm range. Quantum Frequency Conversion (QFC) is therefore required from lower wavelengths (in the 600-950 nm range) to these telecom wavelengths. Various techniques exist like Four-Wave Mixing (FWM) which involves two pump photons and one signal photon to generate an idler photon at a new frequency, sum-frequency generation (SFG) where two photons of different frequencies interact with a nonlinear material and combine to produce a third photon whose frequency is the sum of the two originals, or Difference Frequency Generation (DFG) which mixes the input photon with a strong pump laser in a nonlinear medium to generate a photon at the difference frequency [572, 573]. [574] demonstrated in 2026 a high-performance conversion from the ultraviolet to the telecom band, which matters for trapped-ion and atom-based nodes whose transitions sit in the UV or in the visible, and [575] implemented in 2025 a channel-selective up-conversion enabling frequency-multiplexed quantum networks where a given wavelength channel is routed without disturbing the others.

Some multiparty applications such as secret sharing, conference key agreement, anonymous communication, electronic voting [576] and distributed sensing can use multipartite entanglement such as GHZ states [577]. GHZ states are an important resource, but they are not required by every protocol in these application classes.

1.4.7 QKD photon detectors

QKD systems also require photon detectors or photon-counting receivers, depending on the protocol. **SPD** (single-photon detectors) are used after the photons traverse a polarization filter with several variants:

- **APD**, avalanche photodiodes which can detect single photons [578].

- **SPAD**, single photon avalanche photodiode which can also detect single photons. They can now operate at room temperature and for the detection of telecom wavelength single photons [579, 580].

- **SNSPD**, superconducting nanowire single-photon detectors, requiring <4K cooling [581–583]. It can work for the detection of multiple photons [584].

- **VLPC** (visible light photon counter) which are silicon based.

- **Bi-CMOs** on photonic integrated circuits [585].

- **Si SPDs**, silicon single-photon detectors with efficiencies reaching 84.4% at 785 nm, obtained by Jian-Wei Pan's team in China [586].

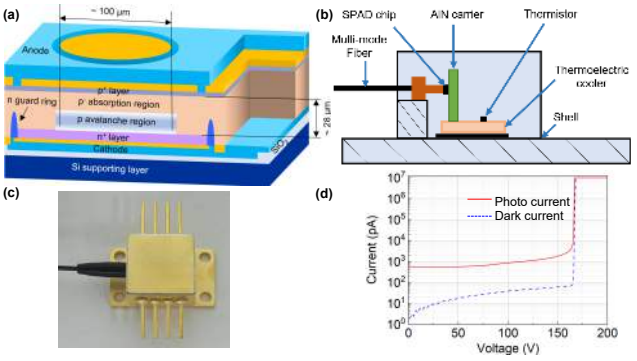


Figure 57: The silicon single-photon detectors from Jian-Wei Pan's team. Source: [586].

Researchers and industry vendors are creating integrated solutions fitting in silicon and GaAs photonic circuits with DV or CV photon source, receiver and amplifiers [587]. Also, color center nuclear spin single-shot readout in silicon carbide is now possible with fidelity of 99.5% [588] as well as Bell states with a fidelity of 94% [589].

1.4.8 QKD nodes and repeaters

The experimental range of QKD increased rapidly in the 1990s. Bennett and colleagues' first apparatus operated over an optical path of about 32 cm on a laboratory bench, not through fiber [590]. The University of Geneva then demonstrated polarization QKD over more than 1 km of optical fiber in 1993, followed by 23 km through installed under-lake telecom fiber in 1996 [591].

Chinese researchers demonstrated a 404 km QKD fiber connection without a repeater in 2016 [592], then extended this record in 2020 to 509 km of transmission without repeater [593] and to 511 km using the TF-QKD protocol (*aka* twin-field QKD), which can also improve free-space QKD [594–596]. Reference [597] improved the experiment without using phase locking, the synchronization of the phase of optical signals between the sender and receiver. The technique was enhanced in 2020 by a mix of British and American researchers to reach 605 km with a key bit every 30 seconds and 357 bits per second at a distance of 368 km [598]. The record was broken in 2022 with 833 km, but with a 140 dB loss and a key rate of 0.014 bps, as shown in Figure 58 [599]. In Austria, an entanglement distribution was achieved over 248 km in 2022 [600]. In a 2026 experiment, Jian-Wei Pan beat a record with a 1.57 Mbps rate over 201.1 km [601].

Another repeaterless distance record was reported in China in 2023 with twin-field QKD over 1,002 km of fiber [602]. The 1,002 km result was obtained in the asymptotic-key regime with a secret-key rate of 9.53×10^{-12} bit per emitted pulse, corresponding to about 0.0034 bit/s for that experiment; finite-key security was demonstrated to 952 km. At such distances, the main limitation is extreme optical loss and the resulting signal-to-noise ratio, not simply a generic "error rate above 400 km".

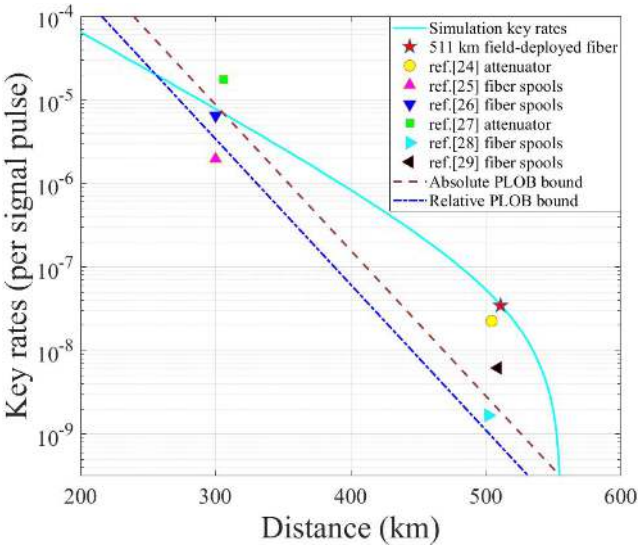


Figure 58: Relationship of QKD key rates and distance without repeaters. Source: [595].

For a repeaterless point-to-point pure-loss bosonic channel of transmissivity η, with unlimited two-way classical communication, the secret-key capacity is the PLOB bound $-\log_2(1-\eta)$ secret bits per channel use [603]. At high loss, it approaches 1.44η bit per channel use. This is not a universal bound for arbitrary channels or architectures containing quantum repeaters.

Quantum channels used for QKD are subject to loss and noise. In ordinary telecom fiber, the channel transmissivity decreases exponentially with distance, so the probability of a useful detection event also falls exponentially in the repeaterless regime. The conditional fidelity of a photon that is successfully received does not itself have to decay exponentially with distance. Instead, as the signal becomes weak relative to dark counts, background photons and other noise, the QBER rises and the extractable secret-key fraction falls. Trusted relays, untrusted measurement relays or future quantum repeaters can therefore be used to improve network reach or useful key rate.

Before adding repeaters, the first lever is the fiber attenuation itself, given the exponential loss dependency with distance. The best silica single-mode fibers have been stuck at about 0.14 dB/km at 1,550 nm for four decades. In September 2025, a University of Southampton team reported a double-nested antiresonant nodeless hollow-core fiber guiding light in air, with a measured 0.091 dB/km attenuation at 1,550 nm which stays below 0.2 dB/km over a 66 THz window against 26 THz for silica, and with a 45% higher group velocity [604]. At a constant loss budget, going from 0.14 to 0.091 dB/km extends the reachable distance by 54%, which is more than most protocol refinements have delivered lately, and the air core also removes most of the Raman scattering that plagues the co-propagation of quantum and classical channels. It remains to be demonstrated over deployed multi-hundred-km cables, with splices, and

with the polarization and chromatic dispersion stability that entanglement-based QKD analyzers require.

Relays or repeaters become useful when direct links no longer provide the required secret-key rate. Repeaterless QKD has been demonstrated over hundreds of kilometers and twin-field variants beyond 1,000 km at very low rates [602, 605]. QKD networks also use classical optical switching and wavelength routing, as well as software-defined networking (SDN), to dynamically configure links and trusted nodes.

There are three main categories of nodes and repeaters:

Trusted node relays where keys must be revealed classically in the intermediate stations, thus the need for it to be in "trusted" locations. These nodes are mostly used with the BB84 protocol but can also work with entanglement based QKDs. They can be implemented to create an arbitrary distance QKD connection. This is the dominant solution. It is used in the 2,000 km Beijing-Shanghai QKD line and in the various EU OpenQKD projects.

Untrusted measurement relays remove the need to trust the relay's measurement device. MDI-QKD is the canonical example: Alice and Bob prepare states and send them to a central station that performs a Bell-state measurement, while security can hold even if that station is controlled by Eve. Twin-field and related interference-based protocols also use an untrusted central measurement station. Complex networks can combine trusted relays and untrusted measurement relays. Satellite implementations are protocol-specific, and their required aperture, adaptive optics and secret-key rate depend on the complete link budget [606, 607].

Quantum repeaters aim to distribute end-to-end entanglement without revealing the final key at intermediate stations [608]. Repeater protocols typically create entanglement over shorter elementary links and connect them by entanglement swapping, which explicitly uses Bell-state measurements (BSM) [609]. Some architectures also use entanglement purification or quantum error correction. First- and second-generation designs commonly require quantum memories to hold successful elementary links while neighboring links are established [610], although all-photonic repeater architectures avoid long-lived matter memories. Memory requirements scale beyond one qubit per link when multiplexing is used to raise entanglement rates [611]. These components are key parts of entanglement-based quantum networks [612, 613], and network scheduling, heralding and swapping also impose classical-control workloads [614].

Quantum-memory figures of merit include storage time or coherence time, efficiency, fidelity, multiplexing capability, bandwidth and operating wavelength. Telecom-band operation around 1,550 nm is advantageous for direct fiber compatibility. Many high-performance memories operate at atomic or solid-state transition wavelengths and use quantum frequency conversion to interface with low-loss telecom fiber.

Quantum memories used with quantum repeaters can be implemented with many tools, the following list being essentially a topic bibliography:

- **SiC** silicon vacancies [615], **SiV** silicon vacancies [616–618], **nitrogen** [619, 620] vacancies in diamond, which can also be arranged in arrays [621]. Spin ensemble quantum memories are also proposed [622]. Remote entanglement between solid-state spin qubits integrated in broadband waveguides was obtained in 2026 by Ronald Hanson's team at QuTech, the broadband waveguide removing the need for a narrow cavity resonance and its associated tuning [623]. On the software side, [624] proposes an instruction-set architecture to program NV center quantum repeater nodes, which is a sign that these nodes are becoming programmable systems and not only physics experiments.
- **Optomechanical memories**, as proposed by NBI in Denmark, using optomechanical induced transparency [625, 626].
- **x-ray memory** operating at ambient temperature [627].
- **Nanophotonic lithium niobate** storing telecom wavelength photons for more than one microsecond, which is short compared with rare-earth crystals but sits directly at 1,550 nm and on a chip, avoiding any frequency conversion [628].
- **All-optical** quantum memories using only polarization beam splitters (PBS), reflecting mirrors, and pockels cell crystal (PC) [629].
- **Fiber optics** delay lines used as memory given the challenge is to limit their losses [630, 631].
- **All-photonic quantum repeaters** (APQR) using a photonic graph state and Shor error correction code [632]. A 2026 architecture from UMass Amherst concatenates bosonic GKP codes with the [[7,1,3]] Steane code to cover 1,000 km with repeater stations every 9 km, requiring only a few thousand GKP qubits per station against much more in previous third generation proposals, and using multi-reflection mirror cavities as free-space photonic memories [633]. The resource reduction is significant but generating thousands of GKP states per station is well beyond the state of the art, which is at a handful of them in superconducting and trapped-ion systems.
- **Rare-earth-ion-doped crystals** (REICs) using for example ytterbium and yttrium [634, 635], europium and ytterbium [636, 637], europium doped crystals in a 20 ms quantum memory operating near 0K [638], europium and yttrium [639], erbium [640–642] erbium-yttrium crystals [643] and praseodymium [644–647].
- **Trapped ions**, whose strong optical transitions are generally in the visible or near-UV rather than directly in the telecom C band. Long-distance ion-photon networking therefore often uses quantum fre-

quency conversion or specially chosen transitions/interfaces to reach telecom wavelengths [648–653], and some architectures use two ion species [650].

- **Atoms** and light matter interaction with single cold atoms [654–657], atom arrays [658], atomic vapors [659, 660] or room temperature atom ensembles [659, 661, 662], with spinwave compaction techniques bringing broadband atomic memories close to unit efficiency [663]. A 2024 experiment did show the capacity to have 72 optical qubits carried by 144 spatially separated atomic ensembles [664]. Infleqtion created an atom ensemble based memory for NASA in 2024.
- **Superconducting qubits** in an original proposal from Italian researchers in 2026 [665].

These repeaters technologies are still at basic research stage and with some limitations [666–668].

The most advanced experimental milestone so far came in February 2026 from USTC, with two trapped-ion memory nodes entangled through an efficient telecom interface over a 10 km fiber, a memory-memory entanglement coherence time of 550 ± 36 ms and an entanglement establishment time short enough to maintain the link at that distance. They distilled 1,917 secret bits out of 4.05×10^5 Bell pairs in a device-independent QKD run over 10 km, and computed a positive key rate at 101 km in the asymptotic limit, extending the DI-QKD reach by more than two orders of magnitude [669]. It remains a two-node link with no entanglement swapping between successive segments, thus a repeater building block and not yet a repeater chain, and the secret key volume, under 2 kbit, shows the distance to any practical usage.

The DLCZ protocol, proposed in 2001 by Duan, Lukin, Cirac and Zoller, introduced a quantum-repeater architecture based on atomic ensembles and linear optics, improving entanglement sharing on lossy communication channels, and it has been continuously refined since then [670]. It is based on using clouds of identical atoms instead of individual atoms, beam splitters and single-photon detectors with moderate efficiencies with a communication efficiency that scales polynomially with distance. It led to a record with two atom ensemble memories connected over 420 km of low loss fiber (0.17 dB/km at 1,552 nm) in China in 2025 [671], although with a very low probability of 1.09×10^{-6}, but a more reasonable one of 3.74×10^{-4} at 120 km.

1.4.9 Securing QKD

In 2000, Peter Shor and John Preskill published a theoretical proof that BB84 is a secure protocol [672]. But QKD is not the solution-that-fixes-all-problems. It can still be subject to jamming, denial-of-service attacks and various other attacks which we cover later. Its safety also depends on the security of both communication endpoints, as with any other solution.

Securing a chain depends on its weakest links and here it is the transmitters and receivers before they even exchange via a QKD. Furthermore, QKD is not a panacea because it depends on a point-to-point link and *not yet* on routing techniques that allow several paths to be used.

Blocking or strongly perturbing the physical channel can create a denial of service, and rerouting techniques are therefore investigated [673]. Transmission loss and noise do not themselves create a Trojan-horse attack (THA). A THA is an active side-channel attack in which Eve injects bright probe light into a QKD device and analyzes back-reflections to infer internal settings such as basis choices or intensity levels [674].

The table in Figure 59 lists many implementation vulnerabilities in QKD. Several now have protocol-specific countermeasures [675]. They are mitigated under explicit implementation assumptions rather than “fixed” in a general way. Weak randomness can compromise basis or intensity choices [676]. Optical, RF and other side channels can be reduced with monitoring, filtering, isolation and protocol changes [677–682]. Power side channels remain relevant for classical electronics [683]. Detection-efficiency mismatch and Trojan-horse attacks have dedicated countermeasures [684, 685], while authenticated classical communication is required against man-in-the-middle attacks [686]. New attack schemes continue to appear, including continuous-measurement and other implementation attacks [687, 688].

Entanglement-based QKD is not intrinsically more secure than prepare-and-measure BB84, and it does not automatically provide device independence. Indeed, an entanglement-based EPR protocol can be mathematically equivalent to BB84 under trusted-device assumptions [689]. Device-independent QKD is a stronger trust model in which security is inferred from a loophole-free Bell violation while still assuming secure laboratories, private randomness, authenticated classical communication and no unintended information leakage [690, 691]. Entanglement-based CV-QKD also has implementation loopholes and proposed countermeasures [692].

The attack surface is not limited to the quantum channel. A 2026 analysis argued that the classical control and post-processing plane of QKD systems, with its key management, authentication, synchronization and parameter negotiation messages, is an under-examined attack surface which concentrates many of the exploitable weaknesses of a deployed system. It is consistent with the ANSSI and NCSC objections mentioned earlier [693]. New attack schemes keep appearing, like the manipulate-and-observe attack where the eavesdropper manipulates the channel and observes how the protocol reacts [694], and post-selective attacks projecting the received multimode state onto Fock subspaces [695]. Authentication is a research topic of its own in quantum networks, since QKD requires an already authenticated classical channel and therefore depends either on a pre-shared secret or on PQC signatures, which is one of the recurring criticisms

Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.*, Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.*, poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et al.*, Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.*, poster at QCrypt (2018)	any	5 commercial & 1 research systems
Spatial efficiency mismatch M. Rau *et al.*, IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)	receiver optics	2 research systems
Pulse energy calibration S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.*, presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.*, New J. Phys. **16**, 123030 (2014); S. Sajeed *et al.*, Sci. Rep. **7**, 8403 (2017)	phase modulator in Bob	ID Quantique
Detector saturation H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.*, Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research system
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	single-photon detector	research system
Channel calibration N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011); L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research systems

Figure 59: QKD implementation vulnerabilities. The source is from 2014 and many listed attacks now have protocol-specific countermeasures, but implementation security remains an active field. Entanglement-based QKD is not automatically device-independent. DI-QKD requires additional Bell-test and laboratory assumptions. Source: [673].

of QKD [696]. Adjacent primitives include quantum position verification, now made arbitrarily loss-tolerant in a single execution [697], and the use of sub-vacuum noise as a jamming resource for secure communication [698].

Cryptography is fascinating for the speed at which implementation assumptions are tested before technologies are deployed en masse. Bell-test-based and device-independent schemes can be spoofed when detector-control or other loopholes invalidate the assumptions of the security test [699]. Better detectors can close some loopholes, but detector quality alone is not a universal remedy because security depends on the complete implementation and threat model. It is a never-ending race!

1.4.10 QKD and the Blockchain

QKD could be used to secure a blockchain, but this is delicate to deploy end-to-end on a large scale. Blockchain users do not have a satellite link or a secured fiber on hand, even when they are mobile. QKD requires controlled links and trusted infrastructure, so its fit with open, permissionless and geographically diffuse blockchains is limited and must be justified by a defined threat model.

This is the proposal of Evgeny Kiktenko of the Russian Quantum Center in Moscow [700] and Del Rajan and Matt Visser of Victoria University of Wellington in New Zealand [701]. Why exactly is not all data transmitted protected in the same way as the QKD? It seems at least to be limited by the low bitrate of existing QKDs. Still, JPMorganChase, Toshiba and Ciena are piloting a QKD network of 100 km mixed fibers (handling both QKD and classical data distribution) to secure a "mission critical Blockchain application" [702, 703]. When an application is critical enough to justify a dedicated QKD network among identified parties, the added value of a blockchain layer over a permissioned database should be established explicitly.

Other theoretical architectures have been proposed in various places like India and Turkey that would rely on quantum computing to improve Blockchain security [704–707]. There are even proposals for a sort of quantum Bitcoin and smart contracts coming from Israel [708].

Also, quantum computing could be potentially used to mine Bitcoin with the proof-of-work method although its resources estimate is not clear [709]. Stacking several complex systems does not by itself improve security, and each layer must be justified by a defined threat model. A similar proposal was made by D-Wave in 2025 [710]. There is even a proposal to create a quantum proof-of-stake "quantum Blockchain", which seems highly theoretical [711].

The stack adds another layer with a 2026 proposal combining a variational quantum circuit sandwiched between classical neural layers, homomorphic encryption, threshold secret sharing, QKD-based keying and a permissioned blockchain for financial fraud detection, reporting a fraud recall of 94.6% against 93.2% for a size-matched classical baseline [712]. The reported recall difference is 1.4 percentage points. Without repeated runs, confidence intervals and a fixed evaluation protocol

on this imbalanced dataset, its statistical significance cannot be assessed, and none of the five stacked technologies is shown to be individually necessary.

Chinese teams moved these proposals from paper to hardware in 2026. Weng et al. from Nanjing University and Renmin University first proposed a multiparty circular quantum Byzantine agreement that removes both the exponential communication complexity and the multipartite entanglement requirement of earlier high-fault-tolerance protocols, replacing them by circular message gathering and quantum digital signatures, which brings the communication complexity down to a quadratic scaling using only weak coherent states on a star-shaped network, with consensus rates simulated on a global satellite-to-ground configuration [713]. Xie et al. then implemented that protocol on a photonic integrated circuit across a six-node network deployed on commercially available telecom infrastructure [714], and Du et al. assembled a complete hybrid quantum blockchain on the same platform, reaching a fault tolerance close to one-half against the classical one-third bound, a consensus latency of a few seconds and a throughput of about 500 transactions per second on a deployed food traceability application [715]. The 500 TPS figure is fine for a first demonstration but is several orders of magnitude below what classical permissioned ledgers claim, the six nodes are a long way from a public network, and the guarantee obtained concerns consensus among a small set of identified nodes and not the open permissionless setting that makes Bitcoin interesting in the first place.

Quantum money is an older idea than QKD itself since it was proposed by Wiesner around 1970 and published in 1983, and it resurfaced in 2026 with a broad German perspective paper from Munich, Berlin and Kassel reviewing the physical implementations of quantum tokens with integrated quantum memories, along with their remaining bottlenecks which are memory lifetime, verification loss and multiphoton side channels [717]. Tsunaki and Naydenov proposed a quantum vault variant addressing an overlooked attack surface, namely the classical description of the token states held by the issuing bank, whose theft allows forging valid tokens without ever violating the no-cloning theorem. Their scheme stores a quantum copy of the token at the bank instead, consuming the token pair at verification, and was benchmarked on three IBM cloud processors within a hardware agnostic framework [718]. These are elegant primitives, but they require the token holder to carry a quantum memory, which puts them significantly further from deployment than QKD, itself already constrained as discussed above.

Quantum Financial System (QFS) is not a technical system. It is an online narrative circulated in parts of the cryptocurrency world, describing a parallel banking system that would compete with SWIFT and be backed by gold, platinum and silver [719, 720]. It has no documented architecture, no standards body, no peer-reviewed literature and no operational infrastructure, and "quantum" carries no technical meaning in the name. Like Bitcoin, it has no identified creator [721, 722]. A few companies trade on the label like QFS Ledger and Quantum Financial System but are not associated with academic scientific quantum-finance research.

1.4.11 QKD over 5G

You may hear about plans to deploy QKD security in 5G networks. QKD itself requires an optical quantum channel and is therefore not normally run over the ordinary RF air interface between a handset and a base station. QKD-derived keys can nevertheless protect 5G transport infrastructure such as fronthaul, midhaul, backhaul and core-network links, and those keys can ultimately be consumed by services used from smartphones [723].

1.4.12 Market and standards

What about the size of the QKD market? **Inside Quantum Technology** (a UK analyst company) made an estimate with a first $1B dollars reached in 2024, then an exponential growth leading to $7B in 2028 [716] (Figure 60). This market size was seemingly not reached in 2024. These are simplistic exponential growth curves, as usual. We'll see. One key market driver would be the adoption of QKD by cloud and data center operators [724]. It also depends on QKD adoption in various vertical markets, such as healthcare, where protected links could be used for sensitive medical data [725].

China is very active in defining a set of QKD standards [726]. The ITU is also working on QKD standards [727]. Europe is represented in the standardization work carried out at ISO, IEEE, ETSI and CEN-CENELEC, the European Committee for Standardization in Electronics and Electrotechnology.

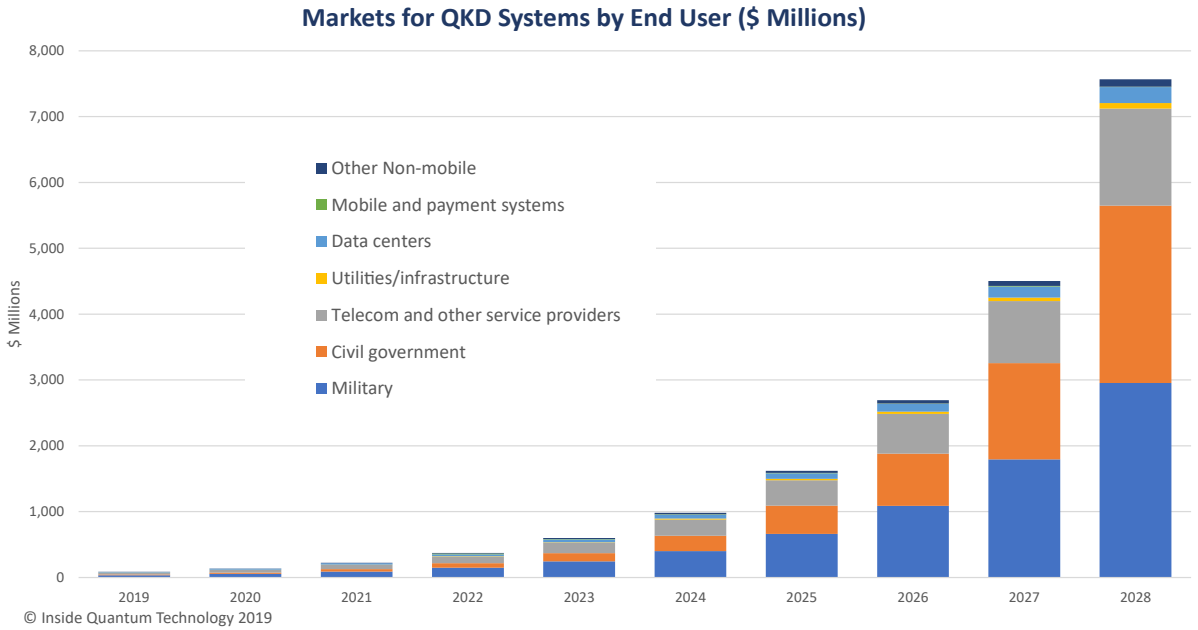


Figure 60: Inside Quantum Technology's QKD market forecast published in 2019, not actual market data. Source: [716]. The forecast revenue of about $1 billion in 2024 was not reached.

1.4.13 Bibliography and notes

These are the bibliographical references and notes for the **Quantum Cryptography** subsection.

[273] Quantum Key Distribution Secured Optical Networks: A Survey, by Purva Sharma, September 2021 (35 pages).

[274] The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet, by Yuan Cao, IEEE, 2021 (59 pages).

[275] Advances in Quantum Cryptography, by S. Pirandola, P. Wallden, et al., arXiv, June 2019 (118 pages).

[276] Quantum cryptography : public key distribution and coin tossing, by Charles H. Bennett and Gilles Brassard, arXiv, December 1984 (5 pages).

[277] The Impact of Quantum Computing on Present Cryptography, by Vasileios Mavroeidis, Audun Jøsang, et al., arXiv, March 2018 (10 pages).

[278] Overview on networks supporting quantum key distribution, by ITU-T, Recommendation ITU-T Y.3800, ITU-T Study Group 13, October 2019 (18 pages).

[279] Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, by Peter W. Shor and John Preskill, Physical Review Letters, July 2000 (4 pages) 🔓 (preprint on arXiv).

[280] A quantum key distribution protocol for rapid denial of service detection, by Alasdair Price, 2020 (20 pages).

[281] Quantum Cryptography Based on Bell's Theorem, by Artur K. Ekert, Physical Review Letters, August 1991 (3 pages) 🔓.

[282] Implementation of carrier-grade quantum communication networks over 10000 km, by Hao-Ze Chen, Wei Qi, et al., npj Quantum Information, August 2025 (7).

[283] Continuous-variable quantum communication, by Vladyslav C. Usenko, Antonio Acín, Romain Alléaume, Ulrik L. Andersen, Eleni Diamanti, Tobias Gehring, Adnan A.E. Hajomer, Florian Kanitschar, Christoph Pacher, Stefano Pirandola, and Valerio Pruneri, arXiv, January 2025 (53 pages).

[284] Continuous Variable Quantum Cryptography Using Coherent States, by Frédéric Grosshans and Philippe Grangier, Physical Review Letters, January 2002 (4 pages).

[285] A polychromatic continuous-variable quantum communication network enabled by optical frequency combs, by Yuehan Xu, Guihua Zeng, et al., arXiv, June 2025 (10 pages).

[286] Continuous-Variable Quantum Key Distribution over 50.4 km Fiber Using an Integrated Silicon Photonic Transmitter and Receiver, by Shuaishuai Liu, Yanxiang Jia, Yuqi Shi, Yizhuo Hou, Pu Wang, Yu Zhang, Shiwei Yang, Zhenguo Lu, Xuyang Wang, and Yongmin Li, Photonics Research, October 2025 (10 pages) 🔓 (preprint on arXiv).

[287] Compact Continuous-Variable Quantum Key Distribution System Employing Monolithically Integrated Silicon Photonic Transceiver, by Denis Fatkhiev, João dos Reis Frazão, Alireza H. Derkani, Kadir Gümüş, Menno van den Hout, Aaron Albores-Mejia, and Chigo Okonkwo, arXiv, March 2026 (4 pages).

[288] Experimental demonstration of Continuous-Variable Quantum Key Distribution with a silicon photonics integrated receiver, by Yoann Piétri, Philippe Grangier, Amine Rhouni, Eleni Diamanti, et al., arXiv, November 2023 (11 pages).

[289] Quantum Encrypted Signals on Multiuser Optical Fiber Networks Simulation Analysis of Next Generation Services and Technologies, by Rameez Asif, 2017 (6 pages).

[290] Quantum experiments explore power of light for communications, computing, by Elizabeth Rosenthal, January 2020.

[291] Continuous-variable quantum key distribution system: past, present, and future, by Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu, and Hong Guo, arXiv, February 2024 (55 pages).

[292] How to Quantum-Secure Optical Networks?, by Helmut Griesser, 2016 (31 slides).

[293] QKD Application: Coexistence QKD Network and Optical Networking the same optical fiber network, by JiDong Xu, June 2019 (15 slides).

[294] The SECOQC quantum key distribution network in Vienna, by Romain Alléaume, 2016 (39 pages).

[295] Development and evaluation of QKD-based secure communication in China, by Wen-yu Zhao, June 2019 (15 slides).

[296] Quantum Key Distribution (QKD) Components and Internal Interfaces, by ETSI, ETSI, 2018 (47 pages).

[297] Experimental Demonstration of High-Rate Discrete-Modulated Continuous-Variable Quantum Key Distribution System, by Yan Pan, Bingjie Xu, et al., arXiv, March 2022 (5 pages).

[298] Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s, by Sebastian Philipp Neumann, Rupert Ursin, et al., arXiv, September 2022 (8 pages).

[299] 'Frequency-modulated' pulsed Bell setup avoids post-selection, by Mónica Agüero, Alejandro Hnilo, Marcelo Kovalsky, and Myriam Nonaka, arXiv, July 2023 (4 pages).

[300] Operational entanglement-based quantum key distribution over 50 km of real-field optical fibres, by Yoann Pelet, Sébastien Tanzilli, et al., arXiv, August 2022 (6 pages).

[301] High-rate quantum key distribution exceeding 110 Mb/s, by Wei Li, Jian-Wei Pan, et al., arXiv, July 2023 (27 pages).

[302] Ultrabright Entanglement Based Quantum Key Distribution over a 404 km Optical Fiber, by Shi-Chang Zhuang, Jian-Wei Pan, et al., arXiv, June 2025 (27 pages).

[303] 5-GHz chip-based quantum key distribution with 1Mbps secure key rate over 150 km, by Guo-Wei Zhang, Guang-Can Guo, Wei Chen, Zheng-Fu Han, et al., arXiv, December 2025 (8 pages).

[304] Co-propagation of 6 Tb/s (60100Gb/s) DWDM & QKD channels with 17 dBm aggregated WDM power over 50 km standard single mode fiber, by P. Gavignet, F. Mondain, E. Pincemin, A. J. Grant, L. Johnson, R. I. Woodward, J. F. Dynes, and A. J. Shields, arXiv, May 2023 (3 pages).

[305] Quantum and coherent signal transmission on a single-frequency channel via the electro-optic serrodyne technique, by Philip Rübeling et al., July 2024 (7 pages).

[306] Trusted Node QKD at an Electrical Utility, by Philip G. Evans, Nicholas A. Peters, et al., arXiv, March 2021 (10 pages).

[307] High-Rate 16-node quantum access network based on passive optical network, by Yan Pan, Bingjie Xu, et al., arXiv, March 2024 (7 pages).

[308] A Quantum Internet Architecture, by Rodney Van Meter, Ryosuke Satoh, Naphan Benchasattabuse, Takaaki Matsuo, Michal Hajdušek, Takahiko Satoh, Shota Nagayama, and Shigeya Suzuki, arXiv, December 2021 (17 pages).

[309] Cost and Routing of Continuous Variable Quantum Networks, by Federico Centrone, Frederic Grosshans, and Valentina Parigi, arXiv, June 2023 (21 pages).

[310] A quantum router architecture for high-fidelity entanglement flows in quantum networks, by Yuan Lee, Eric Bersin, Axel Dahlberg, Stephanie Wehner, and Dirk Englund, npj Quantum Information, June 2022.

[311] An Efficient Routing Protocol for Quantum Key Distribution Networks, by Jia-Meng Yao, Ya-Xing Wang, Qiong Li, Hao-Kun Mao, Ahmed A.Abd El-Latif, and Nan Chen, arXiv, July 2022 (27 pages).

[312] Multipartite Entanglement for Multi-node Quantum Networks, by E. M. Ainley, A. Agrawal, D. Main, P. Drmota, D. P. Nadlinger, B. C. Nichol, R. Srinivas, and G. Araneda, arXiv, July 2024 (36 pages).

[313] Entanglement routing via passive optics in CV-networks, by David Fainsin, Antoine Debray, Ilya Karuseichyk, Mattia Walschaers, and Valentina Parigi, arXiv, March 2025 (13 pages).

[314] RELiQ: Scalable Entanglement Routing via Reinforcement Learning in Quantum Networks, by Tobias Meuser, Jannis Weil, Aninda Lahiri, and Marius Paraschiv, arXiv, November 2025 (16 pages).

[315] 40-user fully connected entanglement-based quantum key distribution network without trusted node, by Xu Liu, January 2022 (15 pages).

[316] Genuinely Multipartite Entanglement vias Shallow Quantum Circuits, by Ming-Xing Luo and Shao-Ming Fei, arXiv, December 2022 (5 pages).

[317] Device-Independent Quantum Key Distribution: Protocols, Quantum Games, and Security, by Syed M. Arslan, Saif Al-Kuwari, M. T. Rahim, and Hashir Kuniyal, arXiv, May 2025 (23 pages).

[318] Advances in device-independent quantum key distribution, by Víctor Zapatero, Tim van Leent, Rotem Arnon, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty, arXiv, August 2022 (15 pages).

[319] Experimental quantum key distribution certified by Bell's theorem, by D. P. Nadlinger, Chris J. Ballance, Renato Renner, Nicolas Sangouard, J.-D. Bancal, et al., Nature, July 2022 🔓 (preprint on arXiv).

[320] The future of secure communications: device independence in quantum key distribution, by Seyed Arash Ghoreishi, Giovanni Scala, Renato Renner, Letícia Lira Tacca, Jan Bouda, Stephen Patrick Walborn, and Marcin Pawłowski, arXiv, April 2025 (96 pages).

[321] Towards Device-Independent Quantum Key Distribution with Photonic Devices, by Corentin Lanore, Xavier Valcarce, Jean Etesse, Anthony Martin, and Jean-Daniel Bancal, arXiv, January 2026 (21 pages).

[322] Measurement-device-independent quantum key distribution, by Hoi-Kwong Lo, Marcos Curty, and Bing Qi, arXiv, May 2012 (7 pages).

[323] Practical challenges in quantum key distribution, by Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan, arXiv, June 2016 (14 pages).

[324] An Overview of CV-MDI-QKD, by Alasdair I. Fletcher, Tobias Gehring, Stefano Pirandola, et al., arXiv, January 2025 (11 pages).

[325] Fault-tolerant measurement-device-independent quantum key distribution with noisy non-Gaussian error correction, by Zhiyue Zuo and Stefano Pirandola, arXiv, May 2026 (15 pages).

[326] A device-independent quantum key distribution system for distant users, by Wei Zhang, Harald Weinfurter, et al., Nature, July 2022.

[327] Device-independent quantum key distribution over 100 km with single atoms, by Bo-Wei Lu, Jian-Wei Pan, et al., arXiv, February 2026 (27 pages).

[328] Quantum gives and quantum takes away, by Austrian Institute of Technology, arXiv, June 2019 (23 slides).

[329] Quantum Conference Key Agreement: A Review, by Gláucia Murta et al., September 2020 (13 pages).

[330] Breaking universal limitations on quantum conference key agreement without quantum memory, by Chen-Long Li, Zeng-Bing Chen, et al., Communications Physics, May 2023.

[331] Advantage of multi-partite entanglement for quantum cryptography over long and short ranged networks, by Janka Memmen, Jens Eisert, and Nathan Walk, arXiv, May 2025 (20 pages).

[332] Experimental anonymous quantum conferencing, by Jonathan W. Webb, Alessandro Fedrizzi, et al., arXiv, November 2023 (16 pages).

[333] Experimental Phase-Matching Quantum Cryptographic Conferencing in Symmetric and Asymmetric Fiber Channels, by Mi Zou and Jian-Wei Pan, arXiv, January 2026 (14 pages).

[334] Multiparty Quantum Key Agreement: Architectures, State-of-the-art, and Open Problems, by Malik Mouaji and Saif Al-Kuwari, arXiv, March 2026 (19 pages).

[335] Device-Independent Quantum Secret Sharing Protocol Enhanced by Advantage Distillation, by Yong-Hui Yang, Jian-Hong Shi, Hong-Wei Li, Hai-Long Zhang, Yun-Teng Yang, Yu-Bing Zhu, and Yan-Yang Zhou, arXiv, May 2026 (12 pages).

[336] Quantum Random Access Codes Implementation for Resource Allocation and Coexistence with Classical Telecommunication, by Domenico Ribezzo, Alessandro Zavatta, et al., arXiv, March 2024 (11 pages).

[337] High-dimensional quantum communication with scalable photonic entanglement in time and frequency, by Kai-Chi Chang, Marcus Huber, Chee Wei Wong, et al., arXiv, March 2026 (20 pages).

[338] Bright Source of High-Dimensional Temporal Entanglement, by Dorian Schiffer, Robert Kindler, Alexandra Bergmayr-Mann, Florian Kanitschar, Amin Babazadeh, Paul Erker, Marcus Huber, and Anton Zeilinger, arXiv, January 2026 (12 pages).

[339] A Survey of OAM-Encoded High-Dimensional Quantum Key Distribution: Foundations, Experiments, and Recent Trends, by Huan Zhang, Zhenyu Cao, Yu Sun, and Hu Jin, arXiv, December 2025 (20 pages).

[340] High-rate quantum digital signatures over 250 km of optical fiber, by Jiemin Lin, Kejin Wei, et al., arXiv, March 2026 (10 pages).

[341] One-Way Quantum Secure Direct Communication with Choice of Measurement Basis as the Secret, by Santiago Bustamante, Boris A. Rodríguez, and Elizabeth Agudelo, arXiv, February 2026 (9 pages).

[342] Quantum Telepathy: A Quantum Technology with Near-Term Applications, by Dawei Ding and Xinyu Xu, arXiv, March 2026 (17 pages).

[343] Second Generation QKD System over Commercial Fibers, by Laszlo Bacsardi et al., 2016 24th European Signal Processing Conference (EUSIPCO), 2016 (5 pages) 🔓 (preprint on Eurasip).

[344] Feasibility of 300 km Quantum Key Distribution with Entangled States, by Thomas Scheidl, Anton Zeilinger, et al., arXiv, July 2010 (14 pages).

[345] Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics, by M. Avesani, P. Villoresi, et al., arXiv, July 2019 (7 pages).

[346] Indian Scientists Demonstrate Wireless Quantum Key Distribution Over 300 Meters, by Matt Swayne, The Quantum Insider, February 2022.

[347] Distribution of genuine high-dimensional entanglement over 10.2 km of noisy metropolitan atmosphere, by Lukas Bulla, Marcus Huber, Martin Bohmann, Rupert Ursin, Matej Pivoluska, et al., arXiv, January 2023 (6 pages).

[348] Millimetre-waves to Terahertz SISO and MIMO Continuous Variable Quantum Key Distribution, by Mingqi Zhang, Stefano Pirandola, and Kaveh Delfanazari, arXiv, January 2023 (9 pages).

[349] A Review on Practical Challenges of Aerial Quantum Communication, by Umang Dubey, Anirban Pathak, et al., arXiv, September 2023 (21 pages).

[350] Free-Space Quantum Networks and Optimized Fiber-Reinforcement, by Alasdair I. Fletcher, Ignazio Pedone, and Stefano Pirandola, arXiv, August 2026 (21 pages).

[351] Cambridge quantum network, by J. F. Dynes, A. J. Shields, et al., npj Quantum Information, November 2019.

[352] HSBC pioneers Quantum protection for AI-powered FX trading, by HSBC, December 2023.

[353] Experimenting quantum key exchange over the Côte d'Azur, by Orange, December 2019.

[354] Entanglement-based clock syntonization for quantum key distribution networks. Demonstration over a 50 km-long link, by Yoann Pelet, Grégory Sauder, Sébastien Tanzilli, Olivier Alibart, and Anthony Martin, arXiv, January 2025 (6 pages).

[355] Quantum Key Distribution with Efficient Post-Quantum Cryptography-Secured Trusted Node on a Quantum Network, by Yoann Piétri, Romain Alléaume, Eleni Diamanti, et al., arXiv, April 2025 (8 pages).

[356] Deployed quantum key distribution network: further, longer and more users, by Nathan Lecaron, Yoann Pelet, Grégory Sauder, Nils Raymond, Julien Chabé, Clément Courde, Anthony Martin, Sébastien Tanzilli, and Olivier Alibart, arXiv, November 2025 (8 pages).

[357] Metropolitan-scale heralded entanglement of solid-state qubits, by Adrian J. Stolk, Ronald Hanson, et al., Science, October 2024.

[358] First quantum-safe data transfer in the Nordic region, by Anne Kirsten Frederiksen, February 2022.

[359] Quantum Key Distribution using Deterministic Single-Photon Sources over a Field-Installed Fibre Link, by Mujtaba Zahidy, Peter Lodahl, Leif K. Oxenløwe, Davide Bacco, Leonardo Midolo, et al., arXiv, April 2023 (9 pages).

[360] A new 380 km-long intercity QKD infrastructure in Poland, by IDQ, IDQ, September 2022.

[361] Nine more countries join initiative to explore quantum communication for Europe, by EU, December 2019.

[362] Quantum communications infrastructure architecture: theoretical background, network structure and technologies. A review of recent studies from a European public infrastructure perspective, by Adam M. Lewis and Petra F. Scudo, arXiv, January 2022 (23 pages).

[363] Deploying an inter-European quantum network, by Domenico Ribezzo, Alessandro Zavatta, et al., arXiv, March 2022 (8 pages).

[364] Linking QKD testbeds across Europe, by Max Brauer, Juan P. Brito, et al., arXiv, January 2024 (23 pages).

[365] Quantum Key Distribution in the Iberian Peninsula, by Vicky Domínguez Tubío, Johannes Borregaard, et al., arXiv, October 2025 (13 pages).

[366] Towards National Quantum Communication in Europe: Planning and Sizing Terrestrial QKD Networks, by Sebastian Raubitzek, arXiv, April 2026 (33 pages).

[367] Latvia creates the Baltic region's first quantum communications backbone, by LVRTC, LVRTC, October 2025.

[368] Battelle Installs First Commercial Quantum Key Distribution Protected Network in U.S. by Batelle, 2013.

[369] Development of a Boston-area 50-km fiber quantum network testbed, by Eric Bersin, Dirk Englund, P. Benjamin Dixon, et al., arXiv, January 2024 (9 pages).

[370] Mass Quantum Transit – Harvard Physicists Demonstrate World's Longest Fiber Distance Between Quantum Memory Nodes, by Matt Swayne, The Quantum Insider, May 2024.

[371] New plans aim to deploy the first US quantum network from Boston to Washington, DC, by Zack Whittaker, TechCrunch, October 2018.

[372] Argonne and UChicago scientists take important step in developing national quantum internet, by Louise Lerner, February 2020.

[373] Department of Energy (DOE) Unveils Blueprint for a U.S. Quantum Internet, by Doug Finke, July 2020.

[374] Picosecond Synchronization of Photon Pairs through a Fiber Link between Fermilab and Argonne National Laboratories, by Keshav Kapoor, Emma E. Wollman, et al., arXiv, August 2022 (7 pages).

[375] InterQnet: a heterogeneous full-stack approach to co-designing scalable quantum networks, by ANL, Argonne National Laboratory, March 2024.

[376] UMass Amherst Researchers Join $26 Million Quantum Computing Effort to Build Internet of the Future |UMass Amherst, by UMass Amherst, March 2024.

[377] Heralded telecom single photons from a visible–telecom pair source on a hybrid PPKTP

PIC platform, by Vijay S. S. Sundaram et al., Optica Quantum, April 2025.

[378] Vacuum Beam Guide for Large Scale Quantum Networks, by Yuexun Huang, Physical Review Letters, July 2024 🔓 (preprint on osti.gov).

[379] Quantum Corridor, Ciena and Toshiba Test 1.6 Tb/s Quantum-Safe Network Encryption, by Mohib Ur Rehman, The Quantum Insider, August 2026.

[380] A Network Security Revolution Enhanced by Quantum Communication, by DARPA, DARPA, June 2023.

[381] An integrated silicon photonic chip platform for continuous-variable quantum key distribution, by G. Zhang, December 2019 (5 pages).

[382] Implementing a quantum-secured network in a metropolitan area, by Juan Moreno et al., March 2023.

[383] 100 Gbps Quantum-safe IPsec VPN Tunnels over 46 km Deployed Fiber, by Obada Alia, Albert Huang, Huan Luo, Omar Amer, Marco Pistoia, and Charles Lim, arXiv, May 2024 (7 pages).

[384] Singtel to Build Singapore's First Country-Wide Quantum-Secure Network Plus for Businesses, by Ray Sharma, March 2024.

[385] SK Telecom, ID Quantique et al form a quantum alliance, by Mat Maundrill, March 2024.

[386] Long-term Performance Analysis of a Commercial QKD Device Under Real-world Deployment Conditions, by Alisson Tezzin, Gustavo M. Uhdre, Oscar Martins, Sabrina Rufo, and Vitor G.A. Carneiro, arXiv, April 2026 (12 pages).

[387] Unhackable Chinese Communication Network Launches Soon, by Rechelle Ann Fuertes, 2017.

[388] Security assessment and key management in a quantum key distribution network, by Xiongfeng Ma, June 2019 (21 slides).

[389] Application In Power Industry Promotes the Development of Quantum Cryptography Technology, by Yonghe Guo, June 2019 (13 slides).

[390] Implementation of a 46-node quantum metropolitan area network, by Teng-Yun Chen, Jian-Wei Pan, et al., arXiv, September 2021 (14 pages).

[391] A multinode quantum network over a metropolitan area, by Jian-Long Liu, Jian-Wei Pan, et al., arXiv, September 2023 (21 pages).

[392] An integrated silicon photonic chip platform for continuous-variable quantum key distribution, by G. Zhang, L. C. Kwek, A. Q. Liu, et al., Nature Photonics, August 2019 🔓.

[393] China Telecom establishes quantum technology group, by Casey Hall, May 2023.

[394] China Telecom launches custom Huawei Mate 60 Pro with 'Quantum Security', by Deng Li, November 2023.

[395] Experimental quantum e-commerce, by Xiao-Yu Cao et al., January 2024 (9 pages).

[396] L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés?, by ANSSI, May 2020 (6 pages).

[397] Quantum Security Technologies, by NCSC, March 2020 (4 pages).

[398] Quantum safe cryptography - the big picture - Fact Based Insight, by David Shaw, 2020.

[399] NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography, by NSA, NSA, 2020.

[400] The uses and limits of quantum key distribution, by ANSSI, NLNCSA, BSI, and Swedish National Communications Security Authority, January 2024 (7 pages).

[401] The debate over QKD: A rebuttal to the NSA's objections, by Renato Renner and Ramona Wolf, arXiv, July 2023 (14 pages).

[402] Applicability of QKD: TerraQuantum view on the NSA's scepticism, by D. Sych, A. Kodukhov, V. Pastushenko, N. Kirsanov, D. Kronberg, and M. Pflitsch, arXiv, March 2024 (4 pages).

[403] Quditto: Emulating and Orchestrating Distributed QKD Network Deployments, by Blanca Lopez, Angela Diaz-Bricio, Javier Perez, Ivan Vidal, and Francisco Valera, arXiv, December 2025 (8 pages).

[404] Arqon: A suite of control applications enabling a reliable quantum network, by Scarlett Gauthier, Thomas R. Beauchamp, and Stephanie Wehner, arXiv, April 2026 (61 pages).

[405] Continuous variable quantum key distribution channel emulator for the SPOQC mission, by Emma Tien Hwai Medlock, Vinod N. Rao, Ry Render, Timothy Spiller, and Rupesh Kumar, arXiv, February 2026 (11 pages).

[406] Toward multi-purpose quantum communication networks: from theory to protocol implementation, by Lucas Hanouz, Marc Kaplan, Jean-Sébastien Kersaint Tournebize, Chin-te Liao, and Anne Marin, arXiv, March 2026 (23 pages).

[407] The Role of the Satellite in Quantum Information Networks, by Luca Paccard, Mathias van den Bossche, et al., arXiv, August 2025 (28 pages).

[408] Assessment of practical satellite quantum key distribution architectures for current and near-future missions, by Davide Orsucci, Florian Moll, et al., arXiv, April 2024 (37 pages).

[409] Satellite-based Quantum Network: Security and Challenges over Atmospheric Channel, by Hong-fu Chou, Symeon Chatzinotas, et al., arXiv, September 2023 (6 pages).

[410] Satellite-based entanglement distribution and quantum teleportation with continuous variables, by Tasio Gonzalez-Raya, Stefano Pirandola, and Mikel Sanz, arXiv, March 2023 (16 pages).

[411] Phase Correction using Deep Learning for Satellite-to-Ground CV-QKD, by Nathan K. Long, Robert Malaney, and Kenneth J. Grant, arXiv, May 2023 (6 pages).

[412] Micius quantum experiments in space, by Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan, arXiv, August 2022 (53 pages).

[413] Quantum Communication Countermeasures, by Michal Krelina, arXiv, October 2023 (25 pages).

[414] Optical Ground Station Diversity for Satellite Quantum Key Distribution in Ireland, by Naga Lakshmi Anipeddi, Jerry Horgan, Daniel K L Oi, and Deirdre Kilbane, arXiv, August 2024 (30 pages).

[415] Full Daylight Quantum-Key-Distribution at 1550 nm Enabled by Integrated Silicon Photonics, by M. Avesani, P. Villoresi, et al., npj Quantum Information, June 2021.

[416] Satellite-based quantum information networks: use cases, architecture, and roadmap, by Laurent de Forges de Parny, Eleni Diamanti, Sébastien Tanzilli, Mathias Van Den Bossche, et al., Communications Physics, January 2023.

[417] Spatially Adaptive Detection for Satellite-based QKD under Atmospheric Turbulence Channel, by Yaoxuan Yang, Ivi Afxenti, and Majid Safari, arXiv, May 2026 (6 pages).

[418] Optimizing Global Quantum Communication via Satellite Constellations, by Yichen Gao, Guanqun Song, and Ting Zhu, arXiv, December 2024 (7 pages).

[419] Towards A Global Quantum Internet: A Review of Challenges Facing Aerial Quantum Networks, by Nitin Jha and Abhishek Parakh, arXiv, May 2025 (5 pages).

[420] Satellites promise global-scale quantum networks, by Sumit Goswami, Christoph Simon, et al., arXiv, May 2025 (19 pages).

[421] Optimizing Orbital Parameters of Satellites for a Global Quantum Network, by Athul Ashok, Owen DePoint, Jackson MacDonald, Albert Williams, and Don Towsley, arXiv, March 2026 (8 pages).

[422] End-to-End QKD Using LEO Satellite Networks, by Sumit Chaudhary, Baqir Kazmi, and Janis Nötzel, arXiv, March 2026 (7 pages).

[423] Quantum Entanglement and Measurement Noise: A Novel Approach to Satellite Node Authentication, by Pooria Madani and Carolyn McGregor, arXiv, January 2025 (10 pages).

[424] Hybrid satellite-fiber quantum network, by Yanxuan Shao, Saikat Guha, and Adilson E. Motter, arXiv, July 2025 (10 pages).

[425] Towards Digital-Twin Assisted Software-Defined Quantum Satellite Networks, by Francesco Chiti, Tommaso Pecorella, Roberto Picchi, and Laura Pierucci, Sensors, January 2025.

[426] Emulation of satellite up-link quantum communication with entangled photons, by Thomas Jaeken, Alexander Pickston, Faris Redza, Thomas Jennewein, and Alessandro Fedrizzi, arXiv, February 2025 (10 pages).

[427] China's Quantum Ambitions: A Multi-Decade Focus on Quantum Communications, by Ciel Qi, February 2024.

[428] Satellite-to-ground quantum key distribution, by Sheng-Kai Liao, Jian-Wei Pan, et al., arXiv, July 2017 (18 pages).

[429] Satellite-relayed intercontinental quantum network, by Sheng-Kai Liao, Jian-Wei Pan, et al., arXiv, January 2018 (10 pages).

[430] Ground-to-satellite quantum teleportation, by Ji-Gang Ren, Jian-Wei Pan, et al., arXiv, July 2017 (16 pages).

[431] Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, by David Lindley, Physical Review Letters, March 1993.

[432] Quantum Communication at 7,600km and Beyond, by Chao-Yang Lu, Jian-Wei Pan, et al., Communications of the ACM, November 2018 🔒.

[433] Micius, the world's first quantum communication satellite, was hackable, by Alexander Miller, arXiv, May 2025 (8 pages).

[434] Microsatellite-Based Real-Time Quantum Key Distribution, by Yang Li, Jian-Wei Pan, et al., Nature, March 2025 (8 pages) 🔓 (preprint on arXiv).

[435] Exploiting potentialities for space-based quantum communication network: downlink quantum key distribution modelling and scheduling analysis, by Xingyu Wang, Shanghong Zhao, et al., arXiv, October 2022 (20 pages).

[436] A step closer to secure global communication, by Eleni Diamanti, Nature, June 2020 🔒.

[437] QUESS (Quantum Experiments at Space Scale) / Micius, by eoPortal Editorial Team, eoPortal, ESA, March 2026.

[438] China has developed the world's first mobile quantum satellite station, by Donna Lu, January 2020.

[439] Portable ground stations for space-to-ground quantum key distribution, by Ji-Gang Ren, Jian-Wei Pan, et al., arXiv, May 2022 (9 pages).

[440] An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres, by Yu-Ao Chen, Jian-Wei Pan, et al., Nature, January 2021 (6 pages) 🔒.

[441] Space–ground QKD network based on a compact payload and medium-inclination orbit, by Yang Li, August 2022 (6 pages).

[442] Russia and China successfully test quantum communication over satellite - 3,800-kilometer test explores possible encrypted networks for BRICS countries, by Christopher Harper, January 2024.

[443] Nanobob CubeSat mission, by Erik Kerstel et al., 2018 (31 pages).

[444] Quantum Photonics Technologies for Space, by QTSpace, October 2018 (22 pages).

[445] QUARC: Quantum Research CubeSat - A Constellation for Quantum Communication, by Luca Mazzarella, 2020 (27 pages).

[446] EAGLE-1: Advancing Europe's Leadership in Quantum Communications, by SES, 2022.

[447] Building Europe's first space-based Quantum Key Distribution system – The German Aerospace Center's role in the EAGLE-1 mission, by Gabriela Calistro-Rivera, Matthias Wagner, et al., arXiv, December 2024 (9 pages).

[448] The European Satellite-Based QKD System EAGLE-1, by Thomas Hiemstra, David Hasler, Domenico Paone, Fabian Reichert, Frank Heine, and Julian Struck, arXiv, May 2025 (7 pages).

[449] Analysis of satellite-to-ground quantum key distribution with adaptive optics, by Valentina Marulanda Acosta, Daniele Dequal, Matteo Schiavon, Aurélie Montmerle-Bonnefois, Caroline B. Lim, Jean-Marc Conan, and Eleni Diamanti, arXiv, November 2021 (17 pages).

[450] Increasing the secret key rate of satellite-to-ground entanglement-based QKD assisted by adaptive optics, by Valentina Marulanda Acosta, Daniele Dequal, Matteo Schiavon, Aurelie Montmerle-Bonnefois, Caroline B. Lim, Jean-Marc Conan, and Eleni Diamanti, arXiv, November 2024 (5 pages).

[451] Connecting Quantum Cities: Simulation of a Satellite-Based Quantum Network, by Raja Yehia, Matteo Schiavon, Valentina Marulanda Acosta, Tim Coopmans, Iordanis Kerenidis, David Elkouss, and Eleni Diamanti, arXiv, July 2023 (24 pages).

[452] QEYSSat 2.0 – White Paper on Satellite-based Quantum Communication Missions in Canada, by Thomas Jennewein, Denis Panneton, et al., arXiv, January 2024 (108 pages).

[453] Microsatellite-based real-time quantum key distribution, by Yang Li, Jian-Wei Pan, et al., arXiv, August 2024 (40 pages).

[454] Terrestrial readiness campaign for space-to-ground quantum communications with a space-qualified entangled photon-pair system, by Gianluca De Santis, Eleni Diamanti, Alexander Ling, and James A. Grieve, arXiv, May 2026 (11 pages).

[455] Dual wavelength source of entanglement for space quantum communication, by Valentin Dumas, Alek Lagarrigue, Tess Troisi, Gregory Sauder, Sebastien Tanzilli, Anthony Martin, and Olivier Alibart, arXiv, May 2026 (6 pages).

[456] A scalable near-visible integrated photon-pair source for satellite quantum science, by Yi-Han Luo, Junqiu Liu, et al., arXiv, January 2026 (28 pages).

[457] QuaNTUM: A Modular Quantum Communication Testbed for Scalable Fiber and Satellite Integration, by Julien Chénedé, Tjorben Matthes, Josefine Krause, Asli Cakan, and Tobias Vogl, arXiv, March 2026 (7 pages).

[458] A reconfigurable entanglement distribution network suitable for connecting multiple ground nodes with a satellite, by Stéphane Vinet, Ramy Tannous, and Thomas Jennewein, arXiv, August 2024 (20 pages).

[459] Fast Adaptive Optics for High-Dimensional Quantum Communications in Turbulent Channels, by Lukas Scarfe, Felix Hufnagel, Manuel F. Ferrer-Garcia, Alessio D'Errico, Khabat Heshami, and Ebrahim Karimi, arXiv, November 2023 (8 pages).

[460] A CubeSat platform for space based quantum key distribution, by Srihari Sivasankaran, Clarence Liu, Moritz Mihm, and Alexander Ling, arXiv, April 2022 (6 pages).

[461] NASA is launching a new quantum entanglement experiment in space, by Charlotte hu, March 2022.

[462] Free-space and Satellite-Based Quantum Communication: Principles, Implementations, and Challenges, by Georgi Gary Rozenman, Alona Maslennikov, Sara P. Gandelman, Yuval Reches, Sahar Delfan, Neel Kanth Kundu, Leyi Zhang, and Ruiqi Liu, arXiv, February 2026 (57 pages).

[463] Operational limits to entanglement-based satellite quantum key distribution, by Jasminder S. Sidhu, Sarah E. McCarthy, Cameron Paterson, and Daniel K. L. Oi, arXiv, February 2026 (19 pages).

[464] Single-Satellite Quantum Repeater Performance Analysis, by Cameron Paterson, Jasminder S. Sidhu, Thomas Brougham, Sarah E. McCarthy, and Daniel K. L. Oi, arXiv, April 2026 (30 pages).

[465] Feasibility of satellite-augmented global quantum repeater networks, by Manik Dawar, Clement Paillet, Nilesh Vyas, Andrew Thain, Rodrigo Henriques Guilherme, and Ralf Riedinger, arXiv, March 2026 (22 pages).

[466] Multi-Mode Quantum Memories for High-Throughput Satellite Entanglement Distribution, by Connor Casey, Albert Williams, Catherine McCaffrey, Eugene Rotherham, and Nathan Darby, arXiv, November 2025 (17 pages).

[467] IonQ to Acquire U.S. Optical Communications Leader Skyloom Global to Accelerate Worldwide Quantum Networking and Sensing Infrastructure, by IonQ, BusinessWire, November 2025.

[468] Photonic entanglement during a zero-g flight, by Julius Bittermann, Marcus Huber, Rupert Ursin, et al., arXiv, February 2024 (12 pages).

[469] In-orbit operation of a programmable quantum photonic processor, by Simon Steiner, Philip Walther, et al., arXiv, September 2026 (98 pages).

[470] Viability of quantum communication across interstellar distances, by Arjun Berera and Jaime Calderón-Figueroa, arXiv, May 2022 (18 pages).

[471] Mathematical calculations show that quantum communication across interstellar space should be possible, by Bob Yirka, July 2022.

[472] On Interstellar Quantum Communication and the Fermi Paradox, by Latham Boyle, arXiv, August 2024 (3 pages).

[473] Demonstration of Quantum-Secure Communications in a Nuclear Reactor, by Konstantinos Gkouliaras, Stylianos Chatzidakis, et al., arXiv, May 2025 (42 pages).

[474] Drone- and Vehicle-Based Quantum Key Distribution, by Andrew Conrad, Paul G. Kwiat, et al., arXiv, May 2025 (31 pages).

[475] Global-scale quantum networking using hybrid-channel quantum repeaters with relays based on a chain of balloons, by Pei-Xi Liu, Guang-Can Guo, et al., arXiv, July 2025 (21 pages).

[476] Drone-based all-weather entanglement distribution, by Hua-Ying Liu, Shi-Ning Zhu, et al., arXiv, May 2019 (16 pages).

[477] World's First "Quantum Drone" for Impenetrable Air-to-Ground Data Links Takes Off, by Charles Q. Choi, IEEE Spectrum, June 2019.

[478] India To Advance Drone-Based Quantum Security with C-DOT and Synergy Quantum Partnership, by Cierra Choucair, The Quantum Insider, May 2025.

[479] On the Optimization of Underwater Quantum Key Distribution Systems with Time-Gated SPADs, by Amir Hossein Fahim Raouf and Murat Uysal, arXiv, June 2022 (6 pages).

[480] Practical underwater quantum key distribution based on decoy-state BB84 protocol, by Shanchuan Dong, Yonghe Yu, Shangshuai Zheng, Qiming Zhu, Lei Gai, Wendong Li, and Yongjian Gu, arXiv, March 2022 (10 pages).

[481] Continuous Variable Based Quantum Communication in the Ocean, by Ramniwas Meena and Subhashish Banerjee, arXiv, January 2024 (15 pages).

[482] Finite Key Underwater Quantum Key Distribution: Performance Analysis and Improvements, by Trevor Thomas, Michael Warnock, and Walter O. Krawec, arXiv, July 2026 (14 pages).

[483] Performance Analysis of Underwater Quantum Key Distribution Protocols: BB84, SARG04, and BBM92, by Nour Rizk, Angélique Drémeau, and Arnaud Coatanhay, arXiv, May 2026 (38 pages).

[484] Quantum Key Distribution over 100 km underwater optical fiber assisted by a Fast-Gated Single-Photon Detector, by Domenico Ribezzo, Alessandro Zavatta, et al., arXiv, March 2023 (6 pages).

[485] Quantum communications feasibility tests over a UK-Ireland 224-km undersea link, by Ben Amies-King, Marco Lucamarini, et al., arXiv, March 2024 (11 pages).

[486] A Concise Primer on Solid-State Quantum Emitters, by Shicheng Yu, Xiaojie Zhang, Xia Lei, and Liang Zhai, arXiv, June 2025 (19 pages).

[487] Solid-State Color Centers for Single-Photon Generation, by Greta Andrini, Valerio Vitali, et al., Photonics, February 2024.

[488] Vanadium in Silicon Carbide: Telecom-ready spin centres with long relaxation lifetimes and hyperfine-resolved optical transitions, by T. Astner, M. Trupke, et al., arXiv, June 2022 (9 pages).

[489] Single G centers in silicon fabricated by co-implantation with carbon and proton, by Yoann Baron, Jean-Michel Gérard, Vincent Jacques, Guillaume Cassabois, Anaïs Dréau, et al., arXiv, April 2022 (5 pages).

[490] A bright future for silicon in quantum technologies, by Mario Khoury et al., Journal of Applied Physics, May 2022.

[491] Genuine and faux single G centers in carbon-implanted silicon, by Alrik Durand, Vincent Jacques, Guillaume Cassabois, Anaïs Dréau, et al., arXiv, February 2024 (5 pages).

[492] Quantum communication networks with defects in silicon carbide, by Sebastian Ecker, Michael Trupke, et al., arXiv, March 2024 (20 pages).

[493] Bright single-photon source in a silicon chip by nanoscale positioning of a color center in a microcavity, by Baptiste Lefaucher, Anaïs Dréau, Jean-Michel Gérard, et al., arXiv, January 2025 (40 pages).

[494] Detection of single W-centers in silicon, by Yoann Baron, Vincent Jacques, Guillaume Cassabois, Anaïs Dréau, et al., arXiv, April 2022 (10 pages).

[495] Wafer-scale nanofabrication of telecom single-photon emitters in silicon, by M. Hollenbach, G. V. Astakhov, et al., arXiv, April 2022 (8 pages).

[496] Optical detection of the electron spin resonances of G centers in silicon, by Félix Cache, Krithika V.R., Tobias Herzig, Vincent Jacques, and Anaïs Dréau, arXiv, May 2026 (9 pages).

[497] Hopping of the center-of-mass of single G centers in silicon-on-insulator, by Alrik Durand, Jean-Michel Gérard, Vincent Jacques, Guillaume Cassabois, Anaïs Dréau, et al., arXiv, April 2024 (13 pages).

[498] Coherent microwave, optical, and mechanical quantum control of spin qubits in diamond, by Laura Orphal-Kobin, Tim Schröder, et al., arXiv, December 2023 (27 pages).

[499] Perfect imperfections: how AWS is innovating on diamond materials for quantum communication with Element Six, by Bart Machielse et al., April 2023.

[500] High-efficiency vertical emission spin-photon interface for scalable quantum memories, by Siavash Mirzaei-Ghormish, Jeddy Bennet, and Ryan M. Camacho, arXiv, March 2025 (10 pages).

[501] Full-Stack High-Volume Quantum Networking Architecture based on Photonic-Integrated Tin Vacancy Centers in Diamond, by Hamza Raniwala, Ian Christen, Helaman Flores, David Starling, Ryan Murphy, Eric Bersin, Kevin Chen, Marc Davis, Maxim Sirotin, Mahmoud Jalali Mehrabad, Ethan G. Arnault, Matthew E. Trusheim, P. B. Dixon, and Dirk R. Englund, arXiv, August 2026 (34 pages).

[502] High-Fidelity Single-Shot Readout and Selective Nuclear Spin Control for a Spin-1/2 Quantum Register in Diamond, by Prithvi Gundlapalli, Fedor Jelezko, et al., arXiv, October 2025 (15 pages).

[503] Highly indistinguishable photons from a tin-vacancy spin qubit in diamond, by Dennis Herrmann, Robert Morsch-Golsong, and Christoph Becher, arXiv, July 2026 (18 pages).

[504] Integration of diamond nanobeams with SnVs on Al2O3 waveguides for scalable quantum photonic chip application, by Yeting Yang, arXiv, June 2026 (12 pages).

[505] Epitaxial single T centres in silicon-on-insulator, by Christian H. Christiansen, Peter Krogstrup, and Stefano Paesani, arXiv, July 2026 (9 pages).

[506] Colour Centre Formation in Silicon-On-Insulator for On-Chip Photonic Integration, by Arnulf J. Snedker-Nielsen, Peter Krogstrup Jeppesen, Marianne E. Bathen, Lasse Vines, Peter Granum, and Stefano Paesani, arXiv, January 2026 (22 pages).

[507] Resolving and resetting the charge environment of single T-centers in silicon p-i-n waveguides, by Chaoshen Zhang, Hanbin Song, Lukasz Komza, Aaron M. Day, Enrique Garcia, Donald Witt, Mihir K. Bhaskar, Alp Sipahigil, and Evelyn L. Hu, arXiv, August 2026 (17 pages).

[508] Coupling nitrogen vacancy centers in silicon carbide to nanophotonic resonators, by Ivan Zhigulin, Konosuke Shimazaki, Samuel M. Stephens, Angus Gale, Karin Yamamura, Hark Hoe Tan, Igor Aharonovich, and Mehran Kianinia, arXiv, February 2026 (13 pages).

[509] Scalable integration of silicon carbide color centers into nanophotonic structures, by Raphael Wörnle, Jonas Schmid, Dennis Grüner, Jonah Heiler, Flavie Davidson-Marquis, Georgy V. Astakhov, Vadim Vorobyov, Florian Kaiser, Jonathan Körber, and Jörg Wrachtrup, arXiv, September 2026 (24 pages).

[510] Room temperature Purcell enhanced single erbium ions in silicon-carbide-on-insulator microring resonators, by Joshua Bader and Stefania Castelletto, arXiv, May 2026 (10 pages).

[511] RF-free driving of nuclear spins with color centers in silicon carbide, by Raphael Wörnle, Jonathan Körber, Timo Steidl, Georgy V. Astakhov, Durga B. R. Dasari, Florian Kaiser, Vadim Vorobyov, and Jörg Wrachtrup, arXiv, January 2026 (21 pages).

[512] Near-Infrared Quantum Emission from Oxygen-Related Defects in hBN, by Sean Doan and Galan Moody, arXiv, December 2025.

[513] Cooperative Emission from Quantum Emitters in Hexagonal Boron Nitride Layers, by Igor Khanonkin, Amir Sivan, Le Liu, Johannes Eberle, Kenji Watanabe, Takashi Taniguchi, Gadi Eisenstein, and Meir Orenstein, arXiv, January 2026 (12 pages).

[514] Color Centers and Hyperbolic Phonon Polaritons in Hexagonal Boron Nitride: A New Platform for Quantum Optics, by Jie-Cheng Feng, Johannes Eberle, Sambuddha Chattopadhyay, Johannes Knörzer, Eugene Demler, and Ataç İmamoğlu, arXiv, February 2026 (17 pages).

[515] Quantum Emitters at Telecommunication Wavelengths based on Carbon Defects in Transition Metal Dichalcogenides, by Chanaprom Cholsuk, Sujin Suwanna, and Tobias Vogl, arXiv, May 2026 (11 pages).

[516] A defect in diamond with millisecond-scale spin relaxation time at room temperature, by Sounak Mukherjee, Anran Li, and Nathalie P. de Leon, arXiv, March 2026 (17 pages).

[517] Experimental Generation of Spin-Photon Entanglement in Silicon Carbide, by Ren-Zhou Fang, Jian-Wei Pan, et al., arXiv, November 2023 (8 pages).

[518] Spin-photon qubits for scalable quantum network, by Md Sakibul Islam, Wayesh Qarony, et al., Light Science & Applications, March 2026 (31 pages).

[519] A Pure and indistinguishable single-photon source at telecommunication wavelength, by Beatrice Da Lio, Arne Ludwig, Peter Lodahl, Leonardo Midolo, et al., arXiv, January 2022 (7 pages).

[520] On-Demand Generation of Indistinguishable Photons in the Telecom C-Band using Quantum Dot Devices, by Daniel A. Vajner, Tobias Heindel, et al., arXiv, January 2024 (24 pages).

[521] Enhancing quantum cryptography with quantum dot single-photon sources, by Mathieu Bozzio, Philip Walther, et al., arXiv, March 2023 (39 pages).

[522] Quantum-dot single-photon sources for the quantum internet, by Chao-Yang Lu and Jian-Wei Pan, Nature Nanotechnology, December 2021 🔓 (preprint on arXiv).

[523] Telecom-band quantum dot technologies for long-distance quantum networks, by Ying Yu, Shunfa Liu, Chang-Min Lee, Peter Michler, Stephan Reitzenstein, Kartik Srinivasan, Edo Waks, and Jin Liu, Nature Nanotechnology, December 2023 🔓 (preprint on arXiv).

[524] Deterministic fabrication of GaAs-quantum-dot micropillar single-photon sources, by Abdulmalik A. Madigawa, Niels Gregersen, et al., arXiv, February 2025 (11 pages).

[525] A Versatile Chip-Scale Platform for High-Rate Entanglement Generation using an AlGaAs Microresonator Array, by Yiming Pang, Galan Moody, et al., arXiv, December 2024 (13 pages).

[526] An ultra-compact deterministic source of maximally entangled photon pairs, by M. Langer, C. Hopfmann, et al., arXiv, March 2025 (14 pages).

[527] Tunable polarization-entangled near-infrared photons from orthogonal GaAs nanowires, by Elise Bailly-Rioufreyt, Rachel Grange, et al., arXiv, December 2025 (34 pages).

[528] Single-emitter quantum key distribution over 175 km of fiber with optimised finite key rates, by Christopher L. Morrison, Alessandro Fedrizzi, et al., arXiv, September 2022 (9 pages).

[529] Benchmarking quantum key distribution by mixing single photons and laser light, by Yann Portella, Aristide Lemaître, Niccolo Somaschi, Loïc Lanco, Pascale Senellart, Dario A. Fioretto, et al., arXiv, October 2025 (14 pages).

[530] Rack-integrated quantum dot-based source of single and entangled photons at telecom C-band, by Michal Vyvlecka, Peter Michler, et al., arXiv, July 2026 (8 pages).

[531] Gigahertz-clocked Generation of Highly Indistinguishable Photons at C-band Wavelengths, by Robert Behrends, Lucas Rickert, and Tobias Heindel, arXiv, March 2026 (6 pages).

[532] Growth of quantum dots by droplet etching epitaxy in molecular beam epitaxy: theory, practice, and review, by Declan Gossink, Undurti S. Sainadh, and Glenn S. Solomon, arXiv, April 2026 (19 pages).

[533] A Broadband Nanowire Quantum Dot Cavity Design for the Efficient Extraction of Entangled Photons, by Sayan Gangopadhyay, Sasan V. Grayli, Sathursan Kokilathasan, and Michael E. Reimer, arXiv, January 2026 (18 pages).

[534] On-chip generation of hybrid polarization-frequency entangled biphoton states, by S. Francesconi, A. Raymond, R. Duhamel, P. Filloux, A. Lemaître, P. Milman, M. I. Amanti, F. Baboux, and S. Ducci, arXiv, August 2022 (10 pages).

[535] Broadband biphoton generation and polarization splitting in a monolithic AlGaAs chip, by Félicien Appas, Othmane Meskine, Aristide Lemaître, José Palomo, Florent Baboux, Maria I. Amanti, and Sara Ducci, arXiv, May 2023 (21 pages).

[536] Multimode Squeezed State for Reconfigurable Quantum Networks at Telecommunication Wavelengths, by Victor Roman-Rodriguez, David Fainsin, Guilherme L. Zanin, Nicolas Treps, Eleni Diamanti, and Valentina Parigi, arXiv, February 2024 (12 pages).

[537] Tunable Generation of Spatial Entanglement in Nonlinear Waveguide Arrays, by A. Raymond, Sara Ducci, F. Baboux, et al., arXiv, December 2024 (6 pages).

[538] Biphoton state generation and engineering with bright hybrid III-V/Silicon photonic devices, by Lorenzo Lazzari, Aristide Lemaître, Sara Ducci, et al., arXiv, November 2025 (9 pages).

[539] Nonlinear integrated quantum photonics with AlGaAs, by F. Baboux, G. Moody, and S. Ducci, arXiv, February 2026 (18 pages).

[540] An all-fibred, telecom technology compatible, room temperature, single-photon source, by Nathan Lecaron, Max

Meunier, Grégory Sauder, Romain Dalidet, Yoann Pelet, Sébastien Tanzilli, Jesus Zuniga-Pérez, and Olivier Alibart, arXiv, April 2025 (10 pages).

[541] Near perfect two-photon interference out a down-converter on a silicon photonic chip, by Romain Dalidet, Camille-Sophie Brès, et al., arXiv, February 2022 (8 pages).

[542] High-quality multi-wavelength quantum light sources on silicon nitride micro-ring chip, by Yun-Ru Fan, Qiang Zhou, et al., arXiv, September 2022 (7 pages).

[543] Silicon microring resonators, by Wim Bogaerts, 2012 (27 pages).

[544] Scalable Feedback Stabilization of Quantum Light Sources on a CMOS Chip, by Danielius Kramnik, Miloš A. Popović, et al., arXiv, November 2024 (45 pages).

[545] Generation of hyperentangled photon pairs in the time and frequency domain on a silicon photonic chip, by Sara Congia, Ségolène Olivier, Matteo Galli, Daniele Bajoni, et al., arXiv, June 2025 (6 pages).

[546] Integrated InP-based transmitter for Continuous-Variable Quantum Key Distribution, by Jennifer Aldama, Eleni Diamanti, Valerio Pruneri, et al., arXiv, February 2025 (14 pages).

[547] World's First Monolithic SiGe QKD Transmitter Chip, by Florian Honz, Philip Walther, Hannes Hübel, Bernhard Schrenk, et al., arXiv, April 2025 (4 pages).

[548] Gigabit-rate Quantum Key Distribution on Integrated Photonic Chips, by Si Qi Ng, Florian Kanitschar, Gong Zhang, and Chao Wang, Optica, June 2026.

[549] Generation of Tunable Entanglement from Thin-Film Lithium Niobate, by Saniya Shinde, Maximilian A. Weissflog, Sina Saravi, Andrey A. Sukhorukov, and Frank Setzpfandt, arXiv, April 2026 (7 pages).

[550] Gigahertz-rate thin-film lithium niobate receiver for time-bin quantum communication, by Andrea Bernardi, Marco Clementi, and Daniele Bajoni, arXiv, April 2026 (19 pages).

[551] Poling-free Spontaneous Parametric Down Conversion for Silicon Carbide and Lithium Niobate photonics, by Tim F. Weiss, Hamed Arianfard, Yang Yang, and Alberto Peruzzo, arXiv, April 2026 (9 pages).

[552] Heterogeneously Integrated Diamond-on-Lithium Niobate Quantum Photonic Platform, by Sophie W. Ding, Chang Jin, Zixi Li, Nicholas Achuthan, Kazuhiro Kuruma, Xinghan Guo, Brandon Grinkemeyer, David D. Awschalom, Nazar Delegan, F. Joseph Heremans, Alexander A. High, and Marko Loncar, arXiv, March 2026 (14 pages).

[553] A Wafer-Scale Heterogeneous III-V-on-Silicon Nitride Quantum Photonic Platform, by Lillian Thiel, Boqiang Shen, and Galan Moody, arXiv, May 2026 (9 pages).

[554] A scalable gallium-phosphide-on-diamond spin-photon interface, by Nicholas S. Yama, Chun-Chi Wu, Fariba Hatami, and Kai-Mei C. Fu, arXiv, January 2026 (39 pages).

[555] Demonstration of a Monolithic and Fully Telecom-Fiber-Compatible Tunable Source of Polarization Entangled Photon Pairs Based on a van der Waals Material, by Benjamin Laudert, Fatemeh Abtahi, Duk Choi, Dragomir Neshev, and Falk Eilenberger, arXiv, June 2026 (20 pages).

[556] High-brightness fiber-based Sagnac source of entangled photon pairs for multiplexed quantum networks, by Tess Troisi, Yoann Pelet, Romain Dalidet, Gregory Sauder, Olivier Alibart, Sébastien Tanzilli, and Anthony Martin, arXiv, February 2026 (7 pages).

[557] Heralded quasi-deterministic entanglement sources based on spontaneous parametric down-conversion, by Yousef K. Chahine, J. Gabriel Richardson, Evan J. Katz, Adam J. Fallon, and John D. Lekki, arXiv, March 2026 (15 pages).

[558] Simulation-guided design of an integrated photonic cavity for frequency-multiplexed Spontaneous Parametric Down Conversion, by Benjamin Szamosfalvi, Michael Raymer, CJ Xin, Leticia Magalhaes, Jarrett Nelson, Marko Lončar, and Ryan M. Camacho, arXiv, May 2026 (19 pages).

[559] Generation and detection of squeezed light on a single silicon photonic chip, by Oliver M. Green and Giacomo Ferranti, arXiv, July 2026 (9 pages).

[560] Progress on Chip-Based Spontaneous Four-Wave Mixing Quantum Light Sources, by Haoyang Wang et al., Advanced Devices $ Instrumentation, January 2024.

[561] Room-temperature addressing of single rare-earth atoms in optical fiber, by Mikio Takezawa, Kaoru Sanaka, et al., Physical Review Applied, October 2023 🔒 (preprint on arXiv).

[562] Single-photon generation from a neodymium ion in optical fiber at room temperature, by Kaito Shimizu, Kai Inoue, Kazutaka Katsumata, Ayumu Naruki, Mark Sadgrove, and Kaoru Sanaka, arXiv, February 2024 (7 pages).

[563] A reconfigurable silicon photonics chip for the generation of frequency bin entangled qudits, by Massimo Borghi, Daniele Bajoni, et al., arXiv, January 2023 (9 pages).

[564] Spin–orbit microlaser emitting in a four-dimensional Hilbert space, by Zhifeng Zhang, Liang Feng, et al., Nature, November 2022 🔒 (preprint on hdl.handle.net).

[565] Controlled growth of rare-earth-doped TiO2 thin films on III-V semiconductors for hybrid quantum photonic interfaces, by Henry C. Hammer and Ravitej Uppu, arXiv, November 2025 (30 pages).

[566] Experimental high-dimensional quantum teleportation, by Xiao-Min Hu, Guang-Can Guo, et al., arXiv, December 2020 (20 pages).

[567] Quantum teleportation in high dimensions, by Yi-Han Luo, Anton Zeilinger, Jian-Wei Pan, et al., arXiv, August 2019 (23 pages).

[568] 100 million photons per second from a single organic molecule, by Siwei Luo, Tim Hebenstreit, Alexey Shkarin, Jan Renger, Tobias Utikal, and Stephan Goetzinger, arXiv, September 2026 (21 pages).

[569] Large-scale quantum-dot-lithium-niobate hybrid integrated photonic circuits enabling on-chip quantum networking, by Xudong Wang, Quan Zhang, et al., arXiv, March 2025 (10 pages).

[570] Time-Bin BB84 QKD System Using Indium Phosphide and Silicon Nitride Photonic Integrated Circuits, by Denis Fatkhiev, Chigo Okonkwo, and Idelfonso Tafur Monroy, arXiv, June 2026 (4 pages).

[571] Highly integrated quantum key distribution transmitter enabled by silicon photonics, by Rende Liu, Yan-Lin Tang, Shuai Li, Mi Zou, Hao Liang, and Shi-biao Tang, arXiv, July 2026 (9 pages).

[572] Quantum Frequency Conversion of Single Photons from a Tin-Vacancy Center in Diamond, by Julia M. Brevoord, Ronald Hanson, Florian Elsen, Bernd Jungbluth, et al., arXiv, September 2025 (9 pages).

[573] Electrically pumped ultra-efficient quantum frequency conversion on thin film lithium niobate chip, by Xina Wang, Jian-Wei Pan, et al., arXiv, September 2025 (20 pages).

[574] High-Performance Quantum Frequency Conversion from Ultraviolet to Telecom Band, by Yi Yang, Jian-Wei Pan, et al., arXiv, March 2026 (13 pages).

[575] Channel-selective frequency up-conversion for frequency-multiplexed quantum network, by Shoichi Murakami, Shunsuke Hiraoka, Toshiki Kobayashi, Takashi Yamamoto, and Rikizo Ikuta, arXiv, November 2025 (10 pages).

[576] Experimental Quantum Electronic Voting, by Nicolas Laurent-Puig, Matilde Baroni, Federico Centrone, and Eleni Diamanti, arXiv, December 2025 (11 pages).

[577] Realizing a Compact, High-Fidelity, Telecom-Wavelength Source of Multipartite Entangled Photons, by Laura dos Santos Martins, Nicolas Laurent-Puig, Pascal Lefebvre, Simon Neves, and Eleni Diamanti, arXiv, June 2024 (12 pages).

[578] Compact InGaAs/InP single-photon detector module with ultra-narrowband interference circuits, by Yan Zhengyu,

Shi Tingting, Fan Yuanbin, Zhou Lai, and Yuan Zhiliang, arXiv, January 2024 (11 pages).

[579] Highly sensitive and efficient 1550 nm photodetector for room temperature operation, by Rituraj, Zhi Gang Yu, R.M.E.B. Kandegedara, Shanhui Fan, and Srini Krishnamurthy, arXiv, May 2024 (7 pages).

[580] Room Temperature Single Photon Detection at 1550 nm using van der Waals Heterojunction, by Nithin Abraham, Kenji Watanabe, Takashi Taniguchi, and Kausik Majumdar, arXiv, September 2025 (40 pages).

[581] High-speed detection of 1550 nm single photons with superconducting nanowire detectors, by Ioana Craiciu, Matthew D. Shaw, et al., arXiv, October 2022 (12 pages).

[582] GHz detection rates and dynamic photon-number resolution with superconducting nanowire arrays, by Giovanni V. Resta, Félix Bussières, et al., arXiv, June 2023 (28 pages).

[583] Sub-2 Kelvin characterization of nitrogen-vacancy centers in silicon carbide nanopillars, by Victoria A. Norman, Marina Radulaski, et al., arXiv, January 2025 (21 pages).

[584] Optical Bias and Cryogenic Laser Readout of a Multipixel Superconducting Nanowire Single Photon Detector, by Frederik Thiele, Niklas Lamberty, Thomas Hummel, and Tim Bartley, arXiv, March 2024 (9 pages).

[585] A Bi-CMOS electronic photonic integrated circuit quantum light detector, by Joel F. Tasker et al., May 2024 (7 pages).

[586] Silicon single-photon detector achieving over 84% photon detection efficiency with flexible operation modes, by Dong An, Jian-Wei Pan, et al., arXiv, July 2025 (6 pages).

[587] Continuous-Variable Quantum Key Distribution at 10 GBaud using an Integrated Photonic-Electronic Receiver, by Adnan A.E. Hajomer, Tobias Gehring, et al., arXiv, May 2023 (7 pages).

[588] Single-Shot Readout of a Nuclear Spin in Silicon Carbide, by Xiao-Yi Lai, Ren-Zhou Fang, Tao Li, Ren-Zhu Su, Jia Huang, Hao Li, Li-Xing You, Xiao-Hui Bao, and Jian-Wei Pan, arXiv, January 2024 (5 pages).

[589] Room-Temperature Storage of Entanglement in a Silicon Carbide Quantum Node, by Shuo Ren, Guang-Can Guo, et al., arXiv, September 2026 (7 pages).

[590] Experimental Quantum Cryptography, by Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin, Journal of Cryptology, January 1992 (26 pages).

[591] Quantum Cryptography over 23 km in Installed Under-Lake Telecom Fibre, by A. Muller, H. Zbinden, and N. Gisin, Europhysics Letters, February 1996 (6 pages).

[592] Measurement device independent quantum key distribution over 404 km optical fibre, by Hua-Lei Yin, Jian-Wei Pan, et al., arXiv, June 2016 (15 pages).

[593] Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km, by Jiu-Peng Chen et al., Physical Review Letters, February 2020 🔓 (preprint on arXiv).

[594] Free-Space Twin-Field Quantum Key Distribution, by Yu-Huai Li, Jian-Wei Pan, et al., arXiv, March 2025 (17 pages).

[595] Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans, by Jiu-Peng Chen, Jian-Wei Pan, et al., arXiv, January 2021 (32 pages).

[596] Twin-Field Quantum Key Distribution: Protocols, Security, and Open Problems, by Syed M. Arslan, Syed Shahmir, Noureldin Mohammad, Saif Al-Kuwari, and Muataz Alhussein, arXiv, October 2025 (28 pages).

[597] Twin-field quantum key distribution without phase locking, by Wei Li, Jian-Wei Pan, et al., arXiv, July 2023 (31 pages).

[598] 600 km repeater-like quantum communications with dual-band stabilisation, by Mirko Pittaluga, Andrew J. Shields, et al., arXiv, May 2022 (18 pages).

[599] Twin-field quantum key distribution over 830-km fibre, by Shuang Wang, Zheng-Fu Han, et al., Nature Photonics, January 2022 🔓.

[600] Continuous entanglement distribution over a transnational 248 km fibre link, by Sebastian Philipp Neumann, Rupert Ursin, et al., arXiv, March 2022 (23 pages).

[601] 1-Mbps Twin-Field Quantum Key Distribution over 200 km Using Independent Dissipative Kerr Solitons, by Hao Dong, Tian-Jiao Zhang, Yan-Wei Chen, Wei Sun, Cong Jiang, Sanli Huang, Shuyi Li, Di Ma, Xiang-Bin Wang, Yang Liu, Junqiu Liu, Qiang Zhang, and Jian-Wei Pan, arXiv, April 2026 (26 pages).

[602] Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance, by Yang Liu, Jian-Wei Pan, et al., Physical Review Letters, May 2023 🔓 (preprint on arXiv).

[603] Fundamental Limits of Repeaterless Quantum Communications, by Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, Nature Communications, April 2017.

[604] Broadband optical fibre with an attenuation lower than 0.1 decibel per kilometre, by Marco Petrovich, Francesco Poletti, et al., Nature Photonics, September 2025 (11 pages).

[605] Viewpoint: Record Distance for Quantum Cryptography, by Marco Lucamarini, November 2018.

[606] Hybrid Implementation for Untrusted-node-based Quantum Key Distribution Network, by Jingyang Liu, Qin Wang, et al., arXiv, March 2025 (33 pages).

[607] Analysis of untrusted-node quantum key distribution from a geostationary satellite, by Thomas Liege, Perrine Lognone, Matteo Schiavon, Caroline B. Lim, Jean-Marc Conan, Eleni Diamanti, and Daniele Dequal, arXiv, July 2025 (16 pages).

[608] Quantum repeaters: From quantum networks to the quantum internet, by Koji Azuma, Sophia E. Economo, Ilan Tzitrin, et al., arXiv, July 2023 (75 pages).

[609] Quantum Internet Protocol Stack: a Comprehensive Survey, by Jessica Illiano, Marcello Caleffi, Antonio Manzalini, and Angela Sara Cacciapuoti, arXiv, May 2022 (31 pages).

[610] Quantum Nodes for Quantum Repeaters, by Hugues de Riedmatten, January 2021 (60 slides).

[611] Multichannel and high dimensional integrated photonic quantum memory, by Zhong-Wen Ou, Tian-Xiang Zhu, Peng-Jun Liang, Xiao-Min Hu, Zong-Quan Zhou, Chuang-Feng Li, and Guang-Can Guo, arXiv, August 2025 (18 pages).

[612] A Metropolitan-scale Multiplexed Quantum Repeater with Bell Nonlocality, by Tian-Xiang Zhu, Guang-Can Guo, et al., arXiv, August 2025 (7 pages).

[613] Remote Quantum Networks based on Quantum Memories, by Tian-Xiang Zhu, Xiao Liu, Zong-Quan Zhou, and Chuan-Feng Li, arXiv, August 2025 (19 pages).

[614] Engineering Challenges in All-photonic Quantum Repeaters, by Naphan Benchasattabuse, Michal Hajdušek, and Rodney Van Meter, arXiv, May 2024 (9 pages).

[615] Scalable quantum memory nodes using nuclear spins in Silicon Carbide, by Shravan Kumar, Roland Nagy, et al., arXiv, February 2023 (15 pages).

[616] A Quantum Repeater Platform based on Single SiV- Centers in Diamond with Cavity-Assisted, All-Optical Spin Access and Fast Coherent Driving, by Gregor Bayer, Alexander Kubanek, et al., arXiv, October 2022 (6 pages).

[617] Telecom networking with a diamond quantum memory, by Eric Bersin, Dirk R. Englund, Mikhail D. Lukin, et al., arXiv, July 2023 (9 pages).

[618] Efficient Photonic Integration of Diamond Color Centers and Thin-Film Lithium Niobate, by Daniel Riedel, Jelena Vučković, et al., arXiv, June 2023 (21 pages).

[619] Proposal for room-temperature quantum repeaters with nitrogen-vacancy centers and optomechanics, by Jia-Wei Ji, Christoph Simon, et al., arXiv, August 2023 (22 pages).

[620] A fully packaged multi-channel cryogenic module for optical quantum memories, by David J. Starling, P. Benjamin Dixon, et al., arXiv, May 2023 (10 pages).

[621] Electric-Field Programmable Spin Arrays for Scalable Quantum Repeaters, by Hanfeng Wang, Matthew E. Trusheim, Laura Kim, and Dirk R. Englund, arXiv, May 2022 (7 pages).

[622] Optimal absorption and emission of itinerant fields into a spin ensemble memory, by Linda Greggio, Tristan Lorriaux, Alexandru Petrescu, Mazyar Mirrahimi, and Audrey Bienfait, arXiv, June 2025 (16 pages).

[623] Remote Entanglement of Solid-State Spin Qubits Integrated in Broadband Waveguides, by Christopher Waas and Ronald Hanson, arXiv, July 2026 (22 pages).

[624] Instruction-Set Architecture for Programmable NV-Center Quantum Repeater Nodes, by Vinay Kumar, Claudio Cicconetti, Riccardo Bassoli, Marco Conti, and Andrea Passarella, arXiv, February 2026 (7 pages).

[625] A Long-lived and Efficient Optomechanical Memory for Light, by Mads Bjerregaard Kristensen, Nenad Kralj, Eric Langman, and Albert Schliesser, arXiv, August 2023 (10 pages).

[626] Non-classical correlations between photons and phonons of center-of-mass motion of a mechanical oscillator, by Ivan Galinskiy, Georg Enzian, Michał Parniak, and Eugene Polzik, arXiv, August 2024 (6 pages).

[627] Nuclear quantum memory for hard x-ray photon wave packets, by Sven Velten et al., ScienceAdvances, June 2024.

[628] Telecom quantum memory over one microsecond in nanophotonic lithium niobate, by Priyash Barya, Daren Chen, and Elizabeth A. Goldschmidt, arXiv, May 2026 (9 pages).

[629] On-demand storing time-bin qubit states with optical quantum memory, by Ming-Shuo Sun, Chun-Hui Zhang, Yi-Zhen Luo, Shuang Wang, Yun Liu, Jian Li, and Qin Wang, arXiv, February 2025 (5 pages).

[630] A fiber-integrated quantum memory for telecom light, by K. A. G. Bonsma-Fisher, C. Hnatovsky, D. Grobnic, S. J. Mihailov, P. J. Bustard, D. G. England, and B. J. Sussman, arXiv, March 2023 (8 pages).

[631] Fiber Loop Quantum Buffer for Photonic Qubits, by Kim Fook Lee, Gamze Gul, Zhao Jim, and Prem Kumar, arXiv, September 2023 (12 pages).

[632] Loss-tolerant all-photonic quantum repeater with generalized Shor code, by Rui Zhang, Li-Zheng Liu, Zheng-Da Li, Yue-Yang Fei, Xu-Fei Yin, Li Li, Nai-Le Liu, Yingqiu Mao, Yu-Ao Chen, and Jian-Wei Pan, arXiv, March 2022 (8 pages).

[633] High-Rate and Resource-Efficient All-Photonic Quantum Repeater Architectures with 9 km Repeater Spacing, by Ryosuke Shiina, Kenneth Goodenough, Nathan Arnold, and Filip Rozpędek, arXiv, June 2026 (36 pages).

[634] Entanglement distribution and quantum storage of more than 8000 modes over a metropolitan network, by Angelo Gelmini Rodriguez, Louis Nicolas, Théo Sanchez Mejia, Pavel Sekatski, Nicolas Brunner, Towsif Taher, Rob Thew, Philippe Goldner, and Mikael Afzelius, arXiv, August 2026 (9 pages).

[635] Remote distribution of non-classical correlations over 1250 modes between a telecom photon and a $^{171}Yb^{3+}$ Y_2SiO_5 crystal, by Moritz Businger, Louis Nicolas, Théo Sanchez Mejia, Alban Ferrier, Philippe Goldner, and Mikael Afzelius, arXiv, May 2022 (8 pages).

[636] Integrated spin-wave quantum memory, by Tian-Xiang Zhu, Guang-Can Guo, et al., National Science Review, May 2024.

[637] A millisecond integrated quantum memory for photonic qubits, by Yu-Ping Liu, Guang-Can Guo, et al., arXiv, April 2025 (28 pages).

[638] Storage of photonic time-bin qubits for up to 20 ms in a rare-earth doped crystal, by Antonio Ortu, Mikael Afzelius, et al., npj Quantum Information, March 2022.

[639] On-demand Integrated Quantum Memory for Polarization Qubits, by Tian-Xiang Zhu, Guang-Can Guo, et al., arXiv, January 2022 (20 pages).

[640] Quantum storage of entangled photons at telecom wavelengths in a crystal, by Ming-Hao Jiang, Xiao-Song Ma, et al., Nature Communications, November 2023 🔓 (preprint on arXiv).

[641] Indistinguishable telecom band photons from a single Er ion in the solid state, by Salim Ourari, Nathalie P. de Leon, Jeff D. Thompson, et al., Nature, August 2023 🔓 (preprint on osti.gov).

[642] Millisecond optical coherence and strong collective coupling in an integrated telecom rare-earth photonic platform, by Kah Jen Wo, Pavel A. Dmitriev, Karthik Dasigi, Fumiya Hanamura, and Steven Touzard, arXiv, August 2026 (25 pages).

[643] On-demand storage of photonic qubits at telecom wavelengths, by Duan-Cheng Liu, Pei-Yun Li, Tian-Xiang Zhu, Liang Zheng, Jian-Yin Huang, Zong-Quan Zhou, Chuan-Feng Li, and Guang-Can Guo, arXiv, November 2022 (13 pages).

[644] Storage and analysis of light-matter entanglement in a fiber-integrated system, by Jelena V. Rakonjac et al., Science, July 2022 (6).

[645] Multiplexed storage and real-time manipulation based on a multiple-degree-of-freedom quantum memory, by Tian-Shu Yang, Guang-Can Guo, et al., arXiv, September 2018 (9 pages).

[646] Efficient cavity-assisted storage of photonic qubits in a solid-state quantum memory, by Stefano Duranti, Hugues de Riedmatten, et al., arXiv, October 2024 (7 pages).

[647] High-Efficiency Quantum Memory of Full-Bandwidth Squeezed Light, by Jinxian Guo, Weiping Zhang, et al., arXiv, June 2025 (9 pages).

[648] A memory-based quantum network node with a trapped ion in an optical fibre cavity, by Pascal Kobel et al., 2021 (222 pages).

[649] Telecom-Wavelength Quantum Repeater Node Based on a Trapped-Ion Processor, by V. Krutyanskiy, Physical Review Letters, May 2023.

[650] Robust Quantum Memory in a Trapped-Ion Quantum Network Node, by P. Drmota, C. J. Ballance, D. M. Lucas, et al., arXiv, April 2023 (10 pages).

[651] Telecom Quantum Photonic Interface for a ${40}Ca^+$ Single-Ion Quantum Memory, by Elena Arenskötter, Christoph Becher, et al., arXiv, November 2022 (16 pages).

[652] Quantum repeater node with free-space coupled trapped ions, by Max Bergerhoff, Omar Elshehy, Stephan Kucera, Matthias Kreis, and Jürgen Eschner, arXiv, September 2024 (8 pages).

[653] Realization of a crosstalk-free two-ion node for long-distance quantum networking, by P.-C. Lai, L.-M. Duan, et al., arXiv, March 2025 (7 pages).

[654] Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution, by S. Langenfeld et al., Physical Review Letters, June 2021.

[655] Entangling single atoms over 33 km telecom fibre, by Tim van Leent, Harald Weinfurter, et al., Nature, July 2022.

[656] Highly efficient storage of 25-dimensional photonic qudit in a cold-atom-based quantum memory, by Ming-Xin Dong, Bao-Sen Shi, et al., arXiv, January 2023 (14 pages).

[657] Hybrid Quantum Repeaters with Ensemble-based Quantum Memories and Single-spin Photon Transducers, by Fenglei Gu, Johannes Borregaard, et al., arXiv, April 2024 (16 pages).

[658] Proposal of quantum repeater architecture based on Rydberg atom quantum processors, by Yan-Lei Zhang, Chang-Ling Zou, et al., arXiv, October 2024 (7 pages).

[659] Optical Memory in a Microfabricated Rubidium Vapor Cell, by Roberto Mottola, Gianni Buser, and Philipp Treutlein, Physical Review Letters, December 2023 🔒 (preprint on arXiv).

[660] Standalone mobile quantum memory system, by Martin Jutisz, Alexander Erl, Janik Wolters, Mustafa Gündoğan, and Markus Krutzik, arXiv, October 2024 (8 pages).

[661] Broadband Quantum Memory in Atomic Ensembles, by Kai Shinbrough, Donny R. Pearson Jr., Bin Fang, Elizabeth A. Goldschmidt, and Virginia O. Lorenz, arXiv, February 2023 (40 pages).

[662] Single-Photon Storage in a Ground-State Vapor Cell Quantum Memory, by Gianni Buser, PRX Quantum, June 2022.

[663] Near-perfect broadband quantum memory enabled by intelligent spinwave compaction, by Jinxian Guo, Zeliang Wu, Guzhi Bao, Peiyu Yang, Yuan Wu, L. Q. Chen, and Weiping Zhang, arXiv, May 2025 (6 pages).

[664] Realization of a Programmable Multipurpose Photonic Quantum Memory with Over-Thousand Qubit Manipulations, by Sheng Zhang, Physical Review X, April 2024.

[665] Transduction-Enabled Superconducting Quantum Repeater: Toward Deterministic Entanglement Distribution with High-Fidelity Gates, by Francesco Fiorini, Jing Wu, Andrew Cameron, Changqing Wang, Doga M. Kurkcuoglu, Rosario G. Garroppo, Michele Pagano, and Silvia Zorzetti, arXiv, September 2026 (21 pages).

[666] Tutorial on quantum repeaters, by Rodney Van Meter et al., 2019 (178 slides).

[667] Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters, by Marco Lucamarini, Zhiliang Yuan, James F. Dynes, and Andrew J. Shields, arXiv, November 2018 (4 pages).

[668] An Information-Theoretic Framework for Quantum Repeaters, by Roberto Ferrara, 2018 (144 pages).

[669] A building block of quantum repeaters for scalable quantum networks, by Wen-Zhao Liu, Jian-Wei Pan, et al., arXiv, February 2026 (21 pages).

[670] Long-distance quantum communication with atomic ensembles and linear optics, by Lu-Ming Duan, Mikhail Lukin, Ignacio Cirac, and Peter Zoller, arXiv, May 2001 (11 pages).

[671] Entangling quantum memories over 420 km in fiber, by Xi-Yu Luo, Jian-Wei Pan, et al., arXiv, April 2025 (15 pages).

[672] Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, by Peter W. Shor and John Preskill, arXiv, May 2000 (5 pages).

[673] QKD Measurement Devices Independent, by Joshua Slater, Vienna Centre for Quantum Science & Technology University of Vienna, September 2014 (83 slides).

[674] Countermeasures for Trojan-Horse Attacks on self-compensating all-fiber polarization modulator, by Alberto De Toni, Paolo Villoresi, et al., arXiv, October 2025 (14 pages).

[675] Certification of cryptographic tools, by Vadim Makarov from Quantum Hacking Lab in Moscow, 2019 (15 slides).

[676] Randomness determines practical security of BB84 quantum key distribution, by Hong-Wei Li, Zhen-Qiang Yin, Shuang Wang, Yong-Jun Qian, Wei Chen, Guang-Can Guo, and Zheng-Fu Han, Scientific Reports, November 2015.

[677] Side-channel-secure quantum key distribution, by Cong Jiang, Xiao-Long Hu, Zong-Wen Yu, and Xiang-Bin Wang, arXiv, May 2023 (10 pages).

[678] Deep-Learning-Based Radio-Frequency Side-Channel Attack on Quantum Key Distribution, by Adomas Baliuka, Markus Stöcker, Michael Auer, Peter Freiwang, Harald Weinfurter, and Lukas Knips, arXiv, October 2023 (14 pages).

[679] Hidden multi-dimensional modulation side channels in quantum protocols, by Amita Gnanapandithan, Li Qian, and Hoi-Kwong Lo, arXiv, February 2025 (9 pages).

[680] Countermeasure against Detector Blinding Attack with Secret Key Leakage Estimation, by Dmitry M. Melkonian, Daniil S. Bulavkin, Kirill E. Bugai, Kirill A. Balygin, and Dmitriy A. Dvoretskiy, arXiv, May 2025 (12 pages).

[681] Experimental Side-Channel-Secure Quantum Key Distribution over 200 km, by Yang Zhou, Jian Li, Qin Wang, et al., arXiv, May 2025 (9 pages).

[682] Hardware-Agnostic Modeling of Quantum Side-Channel Leakage via Conditional Dynamics and Learning from Full Correlation Data, by Brennan Bell and Paul Erker, arXiv, February 2026 (8 pages).

[683] Power-consumption Backdoor in Quantum Key Distribution, by Beatriz Lopes da Costa, Yasser Omar, et al., arXiv, March 2025 (11 pages).

[684] Practical Countermeasure Against Attacks Exploiting Detection Efficiency Mismatch in Quantum Key Distribution, by Ben J. Taylor, Peter R. Smith, James F. Dynes, Robert I. Woodward, Marco Lucamarini, R. Mark Stevenson, and Andrew J. Shields, arXiv, May 2026 (7 pages).

[685] Improved security bounds against the Trojan-Horse attack in decoy-state quantum key distribution, by Zijian Li, Bingbing Zheng, Chengxian Zhang, Zhenrong Zhang, Hong-Bo Xie, and Kejin Wei, arXiv, December 2023 (25 pages).

[686] Man-in-the-Middle Attacks Targeting Quantum Cryptography, by Abel C. H. Chen, arXiv, February 2025 (7 pages).

[687] Deep-learning-based continuous attacks on quantum key distribution protocols, by Théo Lejeune and François Damanet, arXiv, July 2025 (17 pages).

[688] High Dimensional Quantum Eavesdropping: A Hypothetical Attack on BB84 & SSP, by Christopher Dunne, arXiv, December 2024 (29 pages).

[689] Quantum Cryptography Without Bell's Theorem, by Charles H. Bennett, Gilles Brassard, and N. David Mermin, Physical Review Letters, February 1992 (3 pages) 🔒.

[690] Cryptographic Security Concerns on Timestamp Sharing via Public Channel in Quantum Key Distribution Systems, by Melis Pahalı, Utku Tefek, and Kadir Durak, arXiv, March 2022 (6 pages).

[691] Improved Finite-Key Security Analysis of Quantum Key Distribution Against Trojan-Horse Attacks, by Álvaro Navarrete and Marcos Curty, arXiv, February 2022 (18 pages).

[692] Quantum hacking: Induced-photorefraction attack on a practical continuous-variable quantum key distribution system, by Yiliang Wang, Yi Zheng, Chenlei Fang, Haobin Shi, and Wei Pan, arXiv, September 2024 (11 pages).

[693] Beyond the Quantum Promise: A Security Analysis of Classical Control in Quantum Key Distribution, by Ali Hamza Malik, Raja Hasnain Anwar, and Muhammad Taqi Raza, arXiv, August 2026 (12 pages).

[694] The Manipulate-and-Observe Attack on Quantum Key Distribution, by William Tighe, George Brumpton, Mark Carney, and Benjamin T. H. Varcoe, arXiv, March 2026 (26 pages).

[695] Post-selective attack with multi-mode projection onto Fock subspace, by Andrei Gaidash, George Miroshnichenko, and Anton Kozubov, arXiv, March 2026 (9 pages).

[696] Authentication in Quantum Networks, by Christopher Battarbee, Suchetana Goswami, Elham Kashefi, and Mina Doosti, arXiv, June 2026 (37 pages).

[697] Arbitrarily Loss-Tolerant Quantum Position Verification in a Single Execution, by Llorenç Escolà-Farràs, Boris Škorić, and Florian Speelman, arXiv, June 2026 (27 pages).

[698] Sub-Vacuum Jamming for Secure Communication, by S. Barzanjeh, A. Poostindouz, and B. C. Sanders, arXiv, August 2026 (19 pages).

[699] Breaking the Unbreakable Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography, by Jonathan Jogenfors, 2017 (254 pages).

[700] Quantum-secured blockchain, by E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, and A.K. Fedorov, arXiv, June 2018 (7 pages).

[701] Quantum Blockchain using entanglement in time, by Del Rajan and Matt Visser, arXiv, April 2019 (5 pages).

[702] JPMorganChase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application, by JPMorganChase, February 2022.

[703] DV-QKD Coexistence With 1.6 Tbps Classical Channels Over Hollow Core Fibre, by Obada Alia, Dimitra Simeonidou, et al., arXiv, March 2022 (7 pages).

[704] Quantum blockchain using weighted hypergraph states, by Shreya Banerjee, Physical Review Research, March 2020.

[705] Quantum Blockchain Based on Dimensional Lifting Generalized Gram-Schmidt Procedure, by Kumar Nilesh and P. K. Panigrahi, arXiv, October 2022 (11 pages).

[706] The Next Generation of Blockchain: Quantum Blockchain Networks, by Manan Narang from OneQuantum et al., March 2022.

[707] A High-Dimensional Quantum Blockchain Protocol Based on Time-Entanglement, by Arzu Aktaş and İhsan Yılmaz, arXiv:2512.20489, December 2025 (12 pages).

[708] Quantum Prudent Contracts with Applications to Bitcoin, by Or Sattath, arXiv, September 2022 (50 pages).

[709] Quantum advantage on proof of work, by Dan A Bard et al., 2022 🔓 (preprint on doi.org).

[710] Blockchain with proof of quantum work, by Mohammad H. Amin, Andrew D. King, Samuel Kortas, et al., Physical Review A, March 2026 (24 pages) 🔓 (preprint on arXiv).

[711] A Feasible Quantum Walk-Enabled Blockchain with Quantum Delegated Proof-of-Stake Consensus, by Chong-Qiang Ye, Heng-Ji Li, Jian Li, and Xiao-Yu Chen, arXiv, October 2025 (13 pages).

[712] QuantumChain: Blockchain-Backed Quantum Federated Learning for Financial Fraud Detection, by Epameinondas Douros, Konstantinos Dalampekis, Nouhaila Innan, Ioannis Theodonis, and Muhammad Shafique, arXiv:2607.21449, July 2026 (4 pages).

[713] Scalable and Highly Fault-Tolerant Circular Quantum Byzantine Agreement, by Chen-Xun Weng, Ming-Yang Li, Shi-Gen Li, Mengya Zhu, Xiao-Ran Sun, Hua-Lei Yin, and Zeng-Bing Chen, arXiv:2602.11592, February 2026 (20 pages).

[714] Experimental demonstration of scalable quantum blockchain with exponentially superior quantum communication complexity, by Feng Xie, Ming-Yang Li, Yongqiang Du, Chen-Xun Weng, Mingxuan Zhang, Xin Hua, Xiang Guan, Xin An, Jingzhe He, Xin Liu, Zhenrong Zhang, Xi Xiao, Hua-Lei Yin, and Kejin Wei, arXiv:2607.12250, July 2026 (14 pages).

[715] A fault-tolerant quantum blockchain deployed on commercial telecommunications network, by Yongqiang Du, Chen-Xun Weng, Feng Xie, Ming-Yang Li, Mingxuan Zhang, Xin Hua, Xin An, Xiang Guan, Xin Liu, Zhenrong Zhang, Xi Xiao, Hua-Lei Yin, and Kejin Wei, arXiv:2607.12249, July 2026 (16 pages).

[716] The Future of the Quantum Internet A Commercialization Perspective, by Lawrence Gasman, June 2019 (11 slides).

[717] Practical quantum tokens: challenges and perspectives, by Nadezhda P. Kukharchyk, Janik Wolters, et al., arXiv:2602.10621, February 2026 (36 pages).

[718] Quantum Vault: Secure Token Authentication Without Classical State Information Benchmarked on IBMQ, by Lucas Tsunaki and Boris Naydenov, arXiv:2605.03564, May 2026 (11 pages).

[719] The Quantum Financial System (QFS) A Paradigm Shift in Banking, by Harmoney-Monica Jenkins, July 2024.

[720] Quantum Financial System: Revolutionizing Finance or Conspiracy Theory?, by George Kingslay, April 2024.

[721] What is the "New Quantum Financial System"?, by Altcoin Investor et al., March 2024.

[722] The Quantum Financial System: What to Know, by Owais Ali, October 2023.

[723] Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions, by Mohd Hirzi Adnan et al., 2022 (28 pages).

[724] Quantum key distribution for data center security – a feasibility study, by Nitin Jain, Ulrich Hoff, Marco Gambetta, Jesper Rodenberg, and Tobias Gehring, arXiv, July 2023 (23 pages).

[725] Secure Medical Data Transmission Using Quantum Key Distribution and Post-Quantum Cryptography in Real-World Fiber Networks, by Vasile-Laurentiu Dosan, Oliver de Vries, et al., arXiv, August 2026 (9 pages).

[726] Introduction of Quantum secured Communication Standardization in CCSA, by Zhangchao Ma, June 2019 (16 slides).

[727] ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N), by ITU, 2019.

This **Quantum Cryptography** subsection contains 455 bibliographical references and notes containing at least 6,548 pages.

1.5 Quantum telecommunications

QKD-based quantum cryptography is just one application of quantum telecommunications [728]. Quantum telecommunications and quantum networks use entanglement resources in various use cases that we present in this section [729, 730].

1.5.1 Distributed quantum computing

Distributed quantum computing (DQC) is about expanding the computing power of individual quantum computers by interconnecting them with quantum networks. It follows the example of classical distributed computing architectures that exist on the Internet, in data centers and within supercomputers.

Modular scale-out will become important as quantum processors grow in size as they face platform-dependent limitations in qubit and chip size, crosstalk effects, manufacturing yield, control wiring, cryogenic capacity, and, for neutral atoms, optical access and beam-steering resources, as illustrated in Figure 61. The pressure to modularize differs strongly by platform and there is no universal qubit-count threshold. Trapped-ion architectures have long emphasized modularity, while superconducting, cat-qubit, neutral-atom and other platforms may reach different monolithic scales before interconnect becomes necessary. Large fault-tolerant workloads may ultimately require thousands of logical qubits, making modular quantum processor interconnect a plausible, but architecture-dependent and still challenging, route to scale.

Interconnecting quantum computers is not limited to classical inputs/outputs, memory sharing or storage sharing as in classical scale-out architectures. A quantum link can directly transfer a quantum state, or, more commonly in lossy photonic networks, distribute heralded entanglement that is later consumed by state teleportation or gate teleportation. These capabilities have profound implications for quantum-system and network architectures [731].

Apart from photonic processors, qubits are most often encoded in electron or nuclear spins, atomic energy levels, or superconducting circuit states. This explains the many efforts to interface stationary qubits with flying photons in visible or near-infrared bands. Depending on the protocol, photons can carry a quantum state directly or distribute and herald entanglement between distant devices [732].

No faster classical connectivity. Quantum telecommunications do not transmit controllable information faster than light. Entanglement correlations obey quantum no-signaling as a local operation or measurement choice by Alice cannot change the unconditional statistics observed by Bob. In standard qubit teleportation, Alice consumes a previously shared Bell pair, performs a Bell-state measurement and sends two classical bits to Bob, who applies a conditional correction. The classical feed-forward therefore preserves the relativistic causal limit.

Larger computational state space. Inter-QPU connectivity is mainly about creating a much larger coherent quantum processor than the separate QPUs. Two isolated N-qubit QPUs independently manipulate two quantum states, each described by 2^N complex amplitudes, so about 2×2^N amplitudes in total. Once they are coherently interconnected through entanglement and nonlocal gates, they can manipulate a general joint $2N$-qubit state described by up to 2^{2N} complex amplitudes modulo the small normalization constraint. Formally, the tensor-product Hilbert space of the two systems already has dimension 2^{2N} whether or not the interconnect is active. Without an entangling resource, the accessible joint states remain product states, which form a nonlinear subset of that space and not a 2×2^N-dimensional subspace. Counting 2×2^N separate state-vector coefficients is a description of the local parameterization, not of the available computational space. While a quantum interconnect does not increase classical signaling speed, it can enable quantum algorithms and sensing protocols that require coherent nonlocal quantum operations or that avoid intermediate measurement and classical re-encoding of quantum states.

Quantum gate teleportation (QGT) is a major technique for interconnecting quantum processors. It uses previously distributed entanglement, local operations, measurements and classical feed-forward to implement a nonlocal gate. In the trapped-ion experiment of Main et al., two modules separated by about 2 m implemented a teleported CZ gate with an average gate fidelity of 86.2(9)% [733]. A different trapped-ion network experiment reported 96.8±0.4% heralded ion-photon entanglement fidelity over a 3 m fiber [734]. These numbers are not directly comparable because the latter is an entanglement-state fidelity, not a remote-gate fidelity. Once a Bell pair is available, a gate-teleportation step can be executed deterministically with measurement-conditioned feed-forward even when remote entanglement generation itself is probabilistic. Scalable architectures therefore need asynchronous Bell-pair generation, heralding, buffering or multiplexing so that the computation can consume entanglement resources when required [735].

Entanglement forging is better described as a circuit-knitting or decomposition technique. It can reduce or eliminate physical quantum connectivity between partitions at the cost of additional circuit executions and classical post-processing, rather than directly creating a remote quantum gate [736].

Circuit partitioning. Minimizing two-qubit interactions across different QPUs is an important challenge in distributed quantum computing, also known as the circuit partitioning problem (see Figure 62). Its overhead is driven by the number and structure of circuit cut interactions, the required remote gates or Bell pairs, communi-

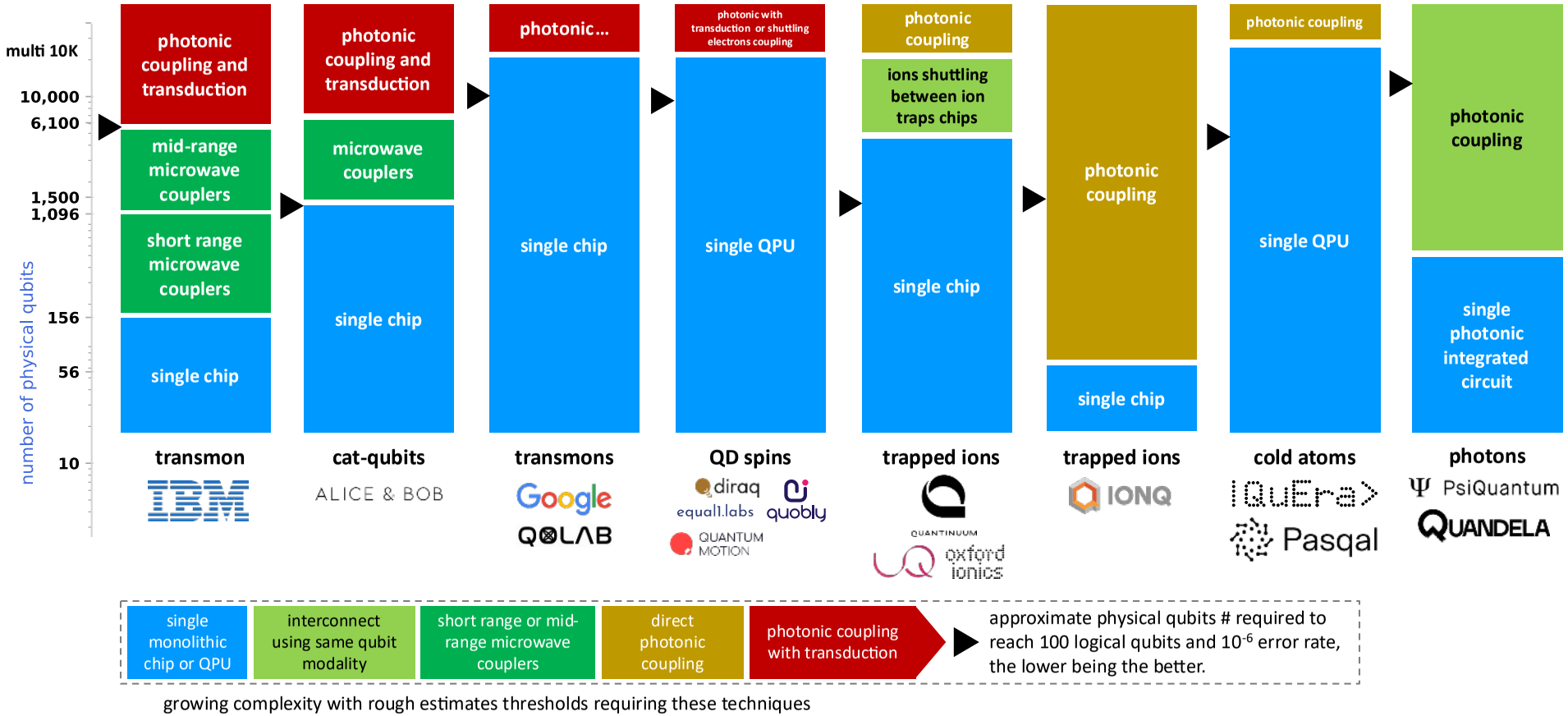


Figure 61: Scalable implementations of many qubit technologies are likely to require processor interconnects at some point. Some platforms may be able to create 100 logical qubits (black triangle) on a single monolithic QPU, while others may require multiple modules connected by microwave, optical or matter-qubit interconnects. The thresholds shown are rough, architecture-dependent estimates based on public roadmaps and current knowledge, not physical limits. The interconnect technologies are colored by their perceived implementation complexity from light green to dark red. © Olivier Ezratty, September 2025.

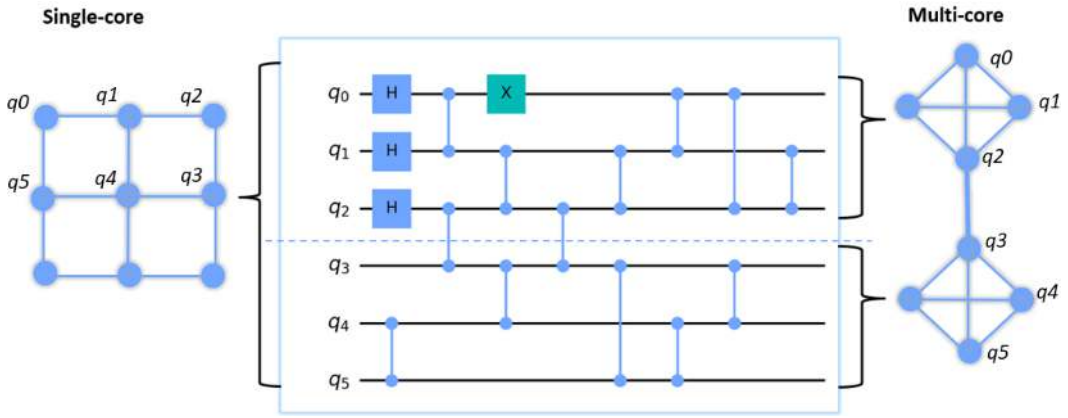


Figure 62: Example of circuit partitioning to distribute it on two processors connected through one link. Source: [737].

cation latency, link topology and scheduling constraints, rather than simply by the number of connected qubits [738]. It requires routing and graph optimization at scale to minimize inter-module entangling operations [739–742]. Related formulations include graph-cut and MaxCut-like objectives [743–747], machine-learning approaches including reinforcement learning [748], simulated annealing and evolutionary algorithms [749]. Some frameworks jointly optimize qubit allocation, entanglement management and gate scheduling, for example by pre-establishing EPR pairs on idle communication qubits to hide generation latency behind circuit execution [750].

Two main techniques of circuit partitioning are used [751–753]:

- The **gate-cut** approach cuts a multi-qubit gate, such as a CNOT, that spans across two different partitions of the circuit. The cut replaces the original multi-qubit gate with a series of single-qubit operations, measurements, and state preparations on the individual subcircuits. It partitions the circuit in space based on the entanglement dependencies between qubits.
- The **wire-cut** approach cuts a continuous qubit "wire" in the circuit's timeline, which represents the evolution of a single qubit's state over time. This is typically done between gates, where the qubit's state is measured and then prepared for the next part of the circuit. It partitions the circuit in time, breaking a single qubit's evolution into separate, manageable segments [754].

Why examine DQC at the algorithm level? Generic circuit partitioners treat a circuit as an anonymous graph to be cut. But the interconnect cost is driven by the algorithm entanglement structure, not by its qubit count. A QFT with its controlled rotations, a QAOA ansatz over a sparse graph and a Trotterized Hamiltonian simulation do not incur the same distribution overhead, and a gate-packing scheme tailored to a QFT beats general-purpose partitioners on the ebit count, meaning the number of Bell pairs consumed across the interconnect. This is also what sizes the physical link, since an entanglement generation rate requirement only becomes a number once an algorithm and its partitioning scheme are fixed. Many algorithms also contain a native decomposition at the problem level, where sub-problems are recombined by classical post-processing rather than by quantum operations, which changes the nature of the interconnect they need. And more entanglement is not uniformly better: in a distributed binary classification task, accuracy improves with the entanglement shared between nodes but degrades beyond a certain amount, which reduces the effective dimension of the parameter space [755].

There are specific proposals to distribute specific quantum algorithms across multiple QPUs: quantum simulations and Grover algorithms [756, 757], quantum dynamics simulations [758], Deutsch-Jozsa algorithm [759], Simon's algorithm [760], Shor's integer factoring [761] and discrete log algorithms [762], quantum neural networks [763], quantum walks, solving the problem of leader election and agreement among the participating QPUs in a distributed quantum computing setup [764], variational algorithms [765, 766], combinatorial optimization with higher-order unconstrained binary formulations [767–769], chemical wavepacket dynamics [770], the QFT [771] and quantum machine learning [755, 772].

Two meanings of "distributed". Most of these algorithm-level proposals require no quantum interconnect at all. In the higher-order optimization frameworks above, a large problem is split into sub-problems solved on independent QPUs while an HPC or GPU layer orchestrates the parts and stitches the results together classically, reaching 500 variables in 170 seconds in one case [767], 1,000 variables with a truncated higher-order SVD preserving inter-variable dependencies in another [766], and using a trained generative model to emit the sub-circuits instead of running a variational loop in a third [769]. Tensor-network decompositions follow the same logic, turning an entangled evolution into a set of independent lower-dimensional propagations executed

asynchronously on trapped-ion hardware [770], and one framework explicitly cuts a 50-qubit search space into 5-qubit sub-circuits precisely to bypass cross-register entanglement [768]. This is quantum-accelerated distributed computing, much closer to classical HPC task farming than to the entanglement-based DQC covered in this section. A distributed quantum extreme learning machine study illustrates where the boundary sits: independent multiplexed units are enough to recover linear properties of an input state, while entanglement between subsystems becomes necessary for nonlinear ones such as Rényi entropy or entanglement measures [772]. Only the works accounting for ebits, remote CNOTs and EPR pair scheduling [750, 771] address the regime that quantum telecommunications must actually serve. Both families are useful, but they do not answer the same question and their speedup figures are not comparable.

The circuit partitioning technique must also account for the fact that inter-QPU entangling gates are less reliable than gates within a chip [773]. It can be adapted to nearby chip-to-chip coupling [774–776].

There is even a so-called Hungarian Qubit Assignment (HQA) algorithm, a multi-core mapping algorithm designed to optimize qubit assignments to cores with the aim of reducing inter-core communications [777].

New simulation tools like Qcom were created to assess the impact of entanglement sharing in QPU interconnect solutions [778]. Finally, techniques are created to distribute logical qubits and quantum error correction across interconnected QPUs [779, 780].

With the notion of virtual gates or circuit cutting, some researchers decompose two-qubit operations into local operations, measurements and classical reconstruction [781, 782]. Such methods are not fundamentally restricted to NISQ hardware, but their sampling and classical post-processing overhead can grow rapidly, which can make them unattractive for large fault-tolerant computations. Other researchers study distributed architectures that partition quantum tasks without attempting to create one large virtual QPU [783].

One important consideration is the time and space overhead of DQC relative to a monolithic QPU. In the peer-reviewed resource estimate of Hugo Jacinto, Élie Gouzien and Nicolas Sangouard [785], a surface-code architecture with physical gate error rate 10^{-3} and a 1 μs processor cycle can factor an RSA-2048 integer using 379 processors with 89,781 physical qubits each, about 3.4×10^7 physical qubits in total. Their model obtains negligible space and time overhead relative to a non-parallelized monolithic architecture provided about 70 Bell pairs are available per processor cycle between processors with fidelity above 98.1%. These figures are architecture- and error-model-dependent requirements, not generic DQC thresholds.

Fault Tolerant Distributed Quantum Computation (FTDQC). Interconnect architectures must support encoded logical qubits and fault-tolerant operations, for example surface-code operations across multiple quantum processors [786–789]. A logical qubit may fit within one module or may itself span several modules, depending on the code, physical error rates, link quality and module size. This motivates full-stack approaches spanning physical qubits, interconnects, error correction, networking and software [790, 791]. QNodeOS provides an operating-system abstraction for executable quantum-network applications [792], while Qoala provides an application execution environment and compilation framework [793, 794].

Blind and verifiable delegated computing is a variation of distributed quantum computing in which a client delegates computation while hiding some or all of the input, algorithm and output from the server. In the BFK universal blind quantum computation protocol, the client prepares randomly rotated single qubits and sends them to the server. The server constructs and measures a measurement-based resource state according to adaptive classical instructions whose randomization hides the computation [795–797]. The computation is therefore not simply prepared locally and teleported wholesale to the server.

Blind quantum computing is sometimes compared conceptually with homomorphic encryption because computation is delegated while information is hidden, but the cryptographic resources and security models are different. Resource costs have been estimated for trapped-ion implementations [798], and remote-device certification can also use Bell-test or self-testing techniques [799]. Fault-tolerant blind quantum computation places error correction within the delegated protocol [800]. In 2025, Mikhail Lukin's team experimentally demonstrated a universal set of blind single- and two-qubit gates over a two-node solid-state network based on SiV centers and optical links [784] (Figure 63).

The implementation of blind quantum computing is related to measurement based quantum computing (MBQC). It can be done with three main client types: emission-based, measurement-based, and rotation-based, each with multiple variants [801]. A measurement-based approach was tested with 3-qubit superconducting processors at ETH Zurich in 2026 [802].

Physical interconnect. The principal physical channels explored for modular quantum computing include microwave links, optical photons, shuttled matter qubits such as electrons or ions, and phononic or acoustic links. Optical links are especially attractive for longer distances because they can exploit low-loss fiber infrastructure, while microwave, shuttling and acoustic links are generally oriented toward same-site or on-package connectivity [803].

We first consider microwave quantum links, which have been investigated mainly for superconducting circuits and, to a lesser extent, semiconductor spin qubits. They are naturally adapted to short-range or same-site con-

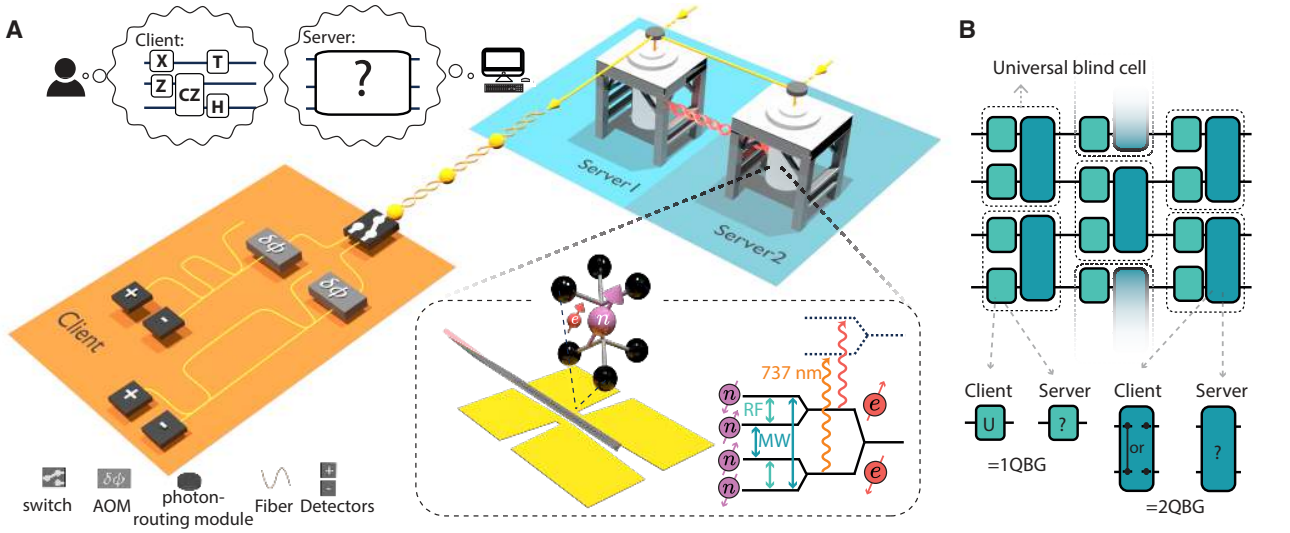


Figure 63: The setup used by Mikhail Lukin's Harvard team to implement blind quantum computing across two nodes containing silicon-vacancy (SiV) centers in nanophotonic diamond cavities. Each node uses an electron-spin communication qubit coupled to the 737 nm optical transition and a nearby ^{29}Si nuclear-spin memory qubit. Source: [784].

nectivity and can avoid microwave-to-optical conversion when the distance remains modest.

1.5.2 Superconducting qubits interconnect

Superconducting qubits belong to circuit quantum electrodynamics (cQED) and are controlled and read out with microwave-frequency fields, typically in the few-gigahertz range. In dispersive readout, the qubit state changes the response of a resonator to a microwave probe. This is not by itself a coherent conversion of an arbitrary qubit state into a propagating microwave photon. Separate state-transfer or emission protocols are used to establish microwave quantum links and remote entanglement.

The first way to implement this is to connect qubit chips next to one another in chiplets [804]. This was tested by NIST, is used by Rigetti and is planned to be adopted by IBM [805, 806]. In 2023, a joint China and USA team tested a short-range connection between five superconducting qubit chips using low-loss aluminum cables with relatively good fidelities [807] (Figure 64 and Figure 65). And when the main qubit interactions are microwave-based but long distance connectivity is required, microwave from/to optical photons must be implemented, which adds some more overhead [808]. And both in the microwave and optical photon regimes, photon losses are to be dealt with. One way to address this problem is to use microwave photon heralding as experimented in 2025 at Yale [809].

Longer-distance superconducting links have also been tested with cryogenic coaxial cables. In the University of Chicago experiment reported in 2021, two three-qubit nodes were connected over a 1 m niobium-titanium coaxial cable. The single-qubit state-transfer process fidelity was 0.911±0.008, while the transferred three-qubit GHZ-state fidelity was 0.656±0.014 [810]. More recent detachable-device links have reported state-transfer efficiencies and fidelities approaching 99% under their respective metrics [811].

Later in 2020, an ETH Zurich and University of Sherbrooke team led by Andreas Wallraff connected superconducting circuits housed in separate cryogenic systems through a 5 m microwave link [812] (Figure 66). A loophole-free Bell test between superconducting circuits separated by about 30 m was reported in 2023 [813].

It was completed in 2026 by a complete hardware solution, modular design, and thermal models [814]. Similar distances were tested by a team led by Technische Universität München, WMI and VTT in 2023 and 2024 [815] (6.5 meters, using an NbTi cable at 50 mK between two cryostats). The University of Chicago and Argonne National Laboratory are conducting similar research and tests, on smaller distances (2 meters) [816].

A Chinese team demonstrated deterministic quantum-state and gate teleportation between superconducting chips connected by a 64 m cryogenic microwave cable. The cable attenuation was 0.32 dB/km at cryogenic temperature and the remote EPR-pair fidelity was 94.2±0.6%. The reported state-teleportation process fidelity was 78.3±0.8% and the teleported CNOT process fidelity was 70.2±0.6% [817]. The experiment is an important point-to-point demonstration, although scaling such dedicated long cryogenic microwave links to many modules remains an architectural challenge.

In 2021, a TUM, RIKEN and Aalto University team demonstrated deterministic teleportation of propagating coherent microwave states over 42 cm using two-mode squeezing and analog feed-forward. The average teleportation fidelity was 0.689 ± 0.004, above the 2/3 no-cloning threshold for the tested coherent states [819].

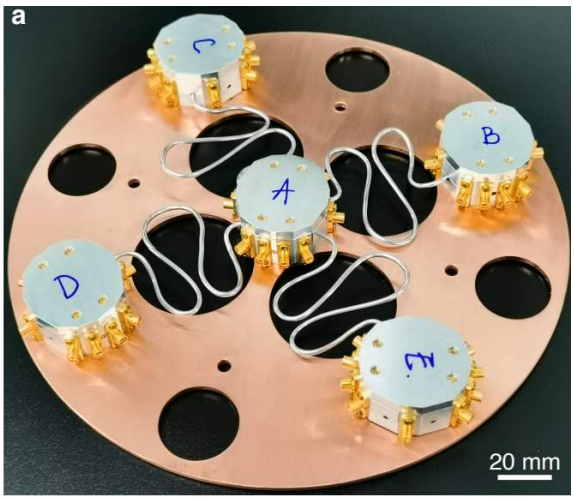


Figure 64: Short-range connection between five superconducting qubit chips. Source: [807].

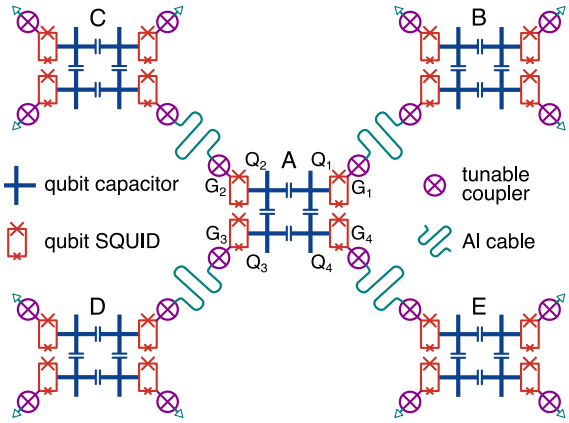


Figure 65: The five-superconducting-chip layout implementing short-range connectivity. Source: [807].

Figure 66: ETH Zurich 5-meter cryogenic microwave link. The waveguides were cooled to below 20 mK. Source: [812].

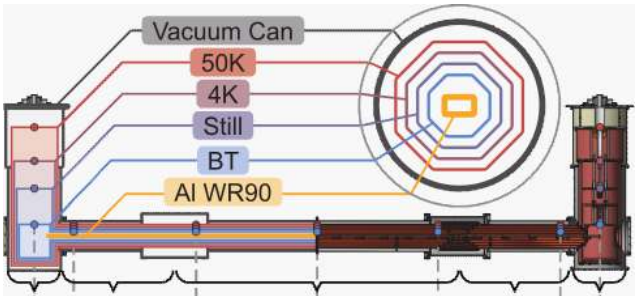


Figure 67: The layout of the ETH Zurich 5-meter cryogenic microwave link experiment. Source: [812].

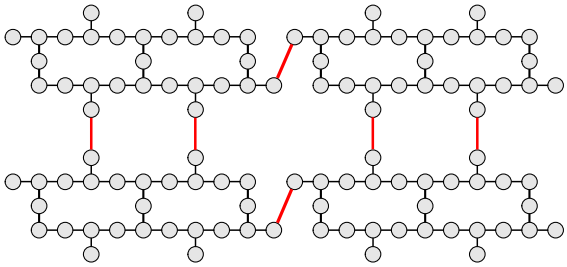


Figure 68: Minimum connectivity between chips, here with an example using 4 chips and one or two connections between chip pairs. Source: [805].

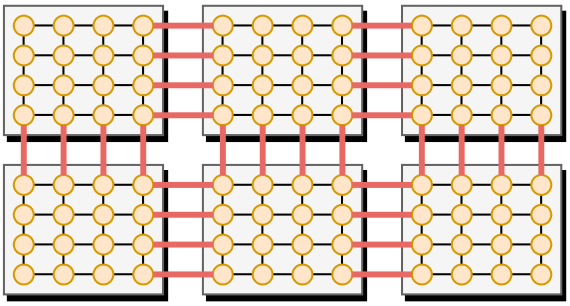


Figure 69: For some two-dimensional nearest-neighbor chip layouts, the number of links crossing a module boundary scales as $O(\sqrt{N})$. The topology studied here gives roughly $2\sqrt{N}$ to $4\sqrt{N}$ links for an N-qubit module. Source: [818].

This was a continuous-variable microwave teleportation experiment.

Scaling to larger chiplets requires enough boundary connectivity to keep routing and remote-gate overhead acceptable. The example in Figure 69 uses a 27-qubit heavy-hex-like topology [805]. Additional multiplexing or multimode microwave links may increase the number of effective inter-module channels [820].

A scalable modular architecture requires a nonlocal entangling primitive, such as a remote CNOT or CZ or an equivalent teleportation-based operation, together with universal local control. SWAP is useful for routing but is not a mandatory primitive.

Various other superconducting qubit to other quantum states have been reported, like:

- **Microwave coupling** can connect superconducting processors through resonators or coaxial modes. In 2025, two processors separated by 30 cm were used to implement direct remote CNOT and CZ entangling gates. The reported CNOT cross-entropy-benchmarking fidelity was 99.15±0.02%, with a gate time of about 200 ns [821]. The experiment used one participating qubit in each processor. Detachable-cable architectures have also reported inter-module state-transfer efficiencies near 99% on their own metrics [822], while earlier protocols had substantially larger photon loss and lower two-qubit-gate fidelity [823].

- **Microwave from/to optical photons transduction** which is quite challenging, using cold atoms [824, 825], nonlinear effects [826, 827], ring resonators [828], Opto-Electro-Mechanical Modulators (OEMM) [829], electro-optomechanical transduction [830–837], piezo-optomechanical transduction [838, 839], magnetomechanical transduction [840], other cavity-based electro-optical devices [841–845], high-speed photodiodes (HSPD) [846], silicon with color centers [847], thin-film lithium niobate (TFLN) based electro-optic transducers [848, 849], and even SQUIDs [850]. It can use a quantum memory for synchronization [851–854]. A kilometer-scale photonic link between superconducting-circuit cryostats using microwave-to-optical and optical-to-microwave transducers was demonstrated in 2025 [855] (Figure 74). Present end-to-end efficiencies remain at roughly the 10^{-3} to 10^{-2} level. Many proposed fault-tolerant interconnect architectures target order-10% or higher efficiencies, but the required value depends on loss, added noise, multiplexing, error correction and the heralding protocol [856]. Thermal-noise suppression remains a major challenge [857], driving interest in pump-free, heralded teleportation-based transduction schemes to prevent optical heating and quasiparticle generation at mK stages [858].

- **Down-conversion transduction** between microwave and lower radio frequencies was proposed by a Stanford team using a multi-octave asymmetrically threaded SQUID (MOATS). The modeled device converts signals in the 4–8 GHz range to roughly 100–500 MHz to reduce attenuation in cryogenic NbTi coaxial cables. For a modeled 100 m link at 200 MHz with cable internal quality factor $Q_i = 10^5$ at 10 mK, the paper estimates a single-photon transmission fidelity of about 0.962. This is an end-to-end modeled transmission fidelity, not a measured 96.2% transducer conversion efficiency [859].

- **RF-to-Microwave transduction** is also possible, with electromechanical systems and a superconducting electromechanical cavity [862].

- Coupling between cold atoms and a superconducting qubit resonator [863, 864].

- Various spin-photon conversion techniques, adapted to quantum dots spin qubits [865, 866].

- Inversely, using transmon qubits to interconnect quantum dots spin qubits [867].

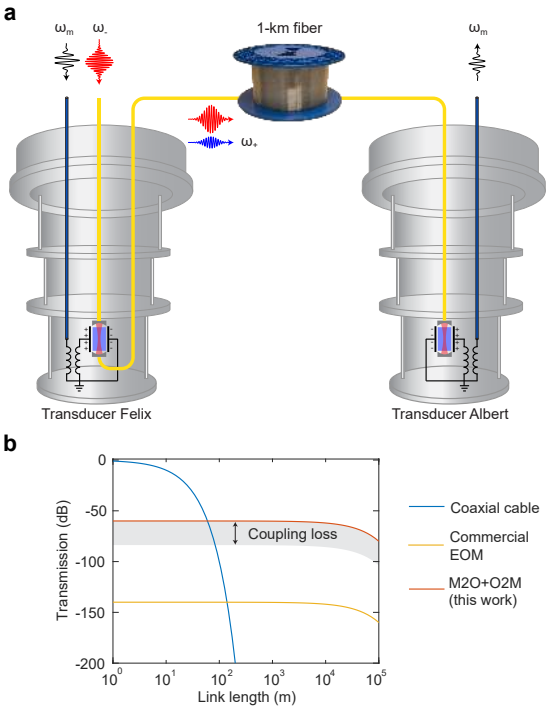


Figure 74: The setup used by Yale researchers to test a transduction-based link between two superconducting-circuit cryostats connected by 1 km of fiber. The reported end-to-end efficiency remains far below the values targeted by most practical modular-QPU architectures. Source: [855].

Microwave-based interconnects are also investigated for creating quantum links between electron-spin qubits [870–872].

1.5.3 Optical interconnect

Optical photons and fibers provide the most generic route to long-distance QPU interconnect, although attenuation, coupling loss and finite entanglement-generation rates still limit distance and throughput. Such links may require deterministic or heralded photon sources, qubit-to-photon or microwave-to-photon interfaces [873, 874], quantum frequency conversion (QFC) toward low-loss telecom bands [875–878], and, in protocols that require synchronization or repeater operation, quantum memories.

Optical interconnect is especially natural for photonic qubits and for matter qubits with efficient optical transitions, such as neutral atoms, trapped ions and color centers [879]. Even photonic systems may still require wavelength or encoding conversion when their native photons are not compatible with the transmission fiber or network protocol.

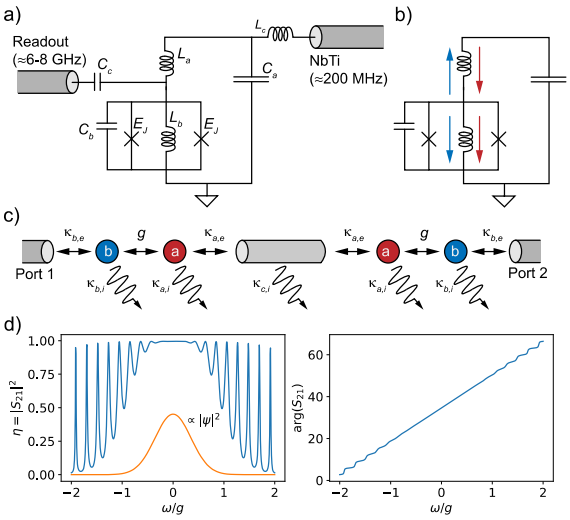


Figure 70: Circuit concept for multi-octave microwave-to-radio-frequency transduction using an asymmetrically threaded SQUID architecture. Source: [859].

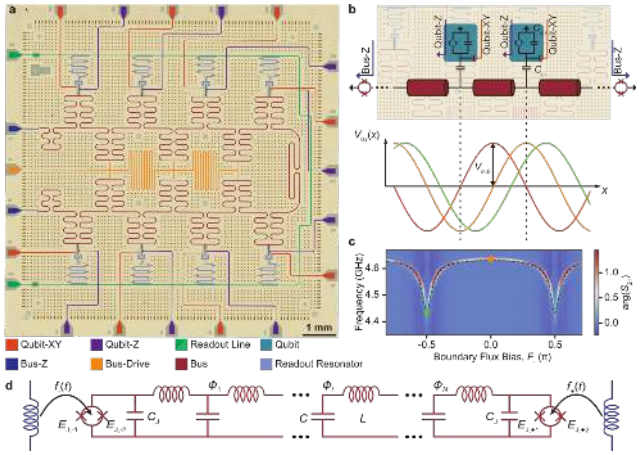


Figure 71: Dynamic coupling from Berkeley, within a single chip. Source: [860].

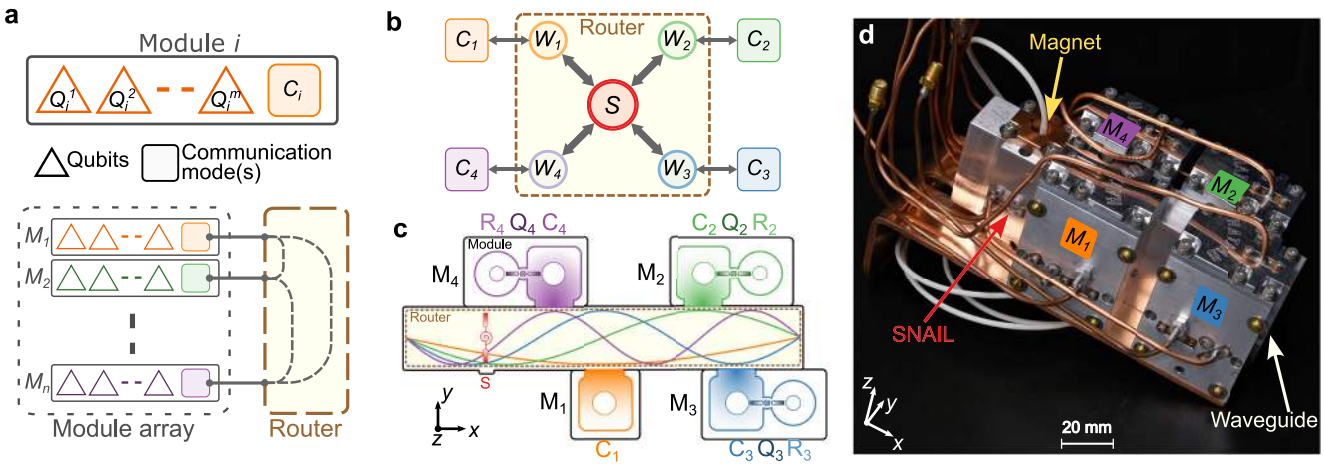


Figure 72: This superconducting qubit inter-module exchange developed in China in 2022 had distant iSWAP fidelities of 96.9%. Source: [861].

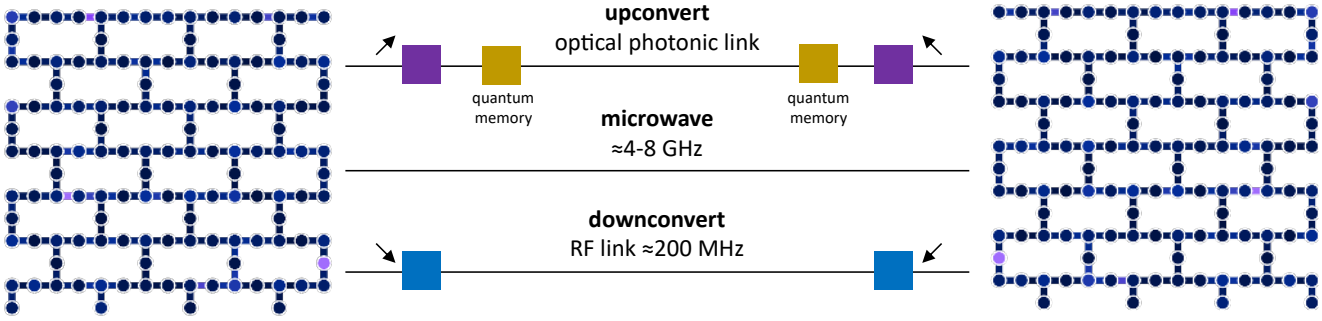


Figure 73: Simplified view of three different techniques to interconnect two superconducting qubit processors. The top one uses a source of entangled photons, quantum memories and upconversion of microwaves into the optical regime. The middle one uses microwave connectors between qubits with no frequency conversion, used as interqubit couplers. The bottom one uses downconversion of microwave signals in the radio-frequency regime at around 500 MHz. © Olivier Ezratty, August 2024.

As described in the previous part, other types of qubits require some conversion, usually between the microwave and optical visible or infrared photon regimes to enable photon mediated remote entanglement [880].

Several experiments of distant entanglement between atoms in two neutral atoms QPUs were achieved in 2023 and 2024 with single atoms [881] and multiple atoms trapped in optical cavities [882]. It even reached three

What is the difference between direct and heralded transduction?

Direct transduction attempts to coherently map a quantum state between microwave and optical modes in one physical conversion chain. High efficiency and very low added noise are both required. In the ideal bosonic pure-loss model, the unassisted one-way quantum capacity becomes zero when the channel transmissivity is at or below 50% [868]. This 50% value is therefore a channel-capacity threshold in that model, not a universal rule saying that a physical transducer cannot operate below 50% efficiency.

Heralded schemes instead probabilistically generate microwave-optical entanglement and subsequently transfer a state by teleportation. They can trade deterministic throughput for conditioned success and can tolerate losses that would make direct one-way transmission unattractive. Their costs include probabilistic entanglement generation, heralding, buffering and classical feed-forward [869].

systems, generating a GHZ_3 state in Gerhard Rempe's team from MPQ in Munich in 2026 [883].

A team from NanoQT from Japan published in July 2024 a blueprint on how to interconnect cold atom based QPUs using nanofibers as conveyors of photons being emitted by atom fluorescence which are detected by two SNSPDs at the two exits of the fiber [884] (Figure 76). Interestingly, they defined some generic criteria to implement QPU interconnect which are independent from the qubit type. An alternative design consists of sending readout photons to a waveguide array coupled to SNSPDs [885] (Figure 75).

- Fixed-size module with a finite number of qubits.
- Initialization operation to set the state of the qubits within each module into a fixed state, such as $|000\ldots\rangle$, with a finite error rate below a threshold constant.
- Gate operations on the qubits in each module with a finite error rate below a threshold constant.
- Universal gate set composed of a finite number of gates.
- Measurement operation on the qubits in each module with a finite error rate below a threshold constant.
- The interface of each module to be linked with other modules, with a finite error rate below a threshold constant.
- The link connecting the interfaces of different modules to transmit quantum states within, at most, a fixed distance, with a finite error rate below a threshold constant.

To which we can add:

- Fast enough entanglement generation between modules to keep pace with module quantum computing processes.
- Gate teleportation fidelities in line with module fidelities.
- Number of connections between modules sufficient for the chosen code and routing topology. For some two-dimensional nearest-neighbor layouts, the number of boundary links scales as $O(\sqrt{N})$ for an N-qubit module, but there is no universal minimum equal to $\sqrt{N}$.
- Ability to handle gate teleportation at the speed required by QEC implementation across multiple modules.
- Switching capability to dynamically interconnect various QPUs in a network [886].

In August 2024, teams from Harvard and MIT proposed fault-tolerant optical interconnects for neutral-atom modules using remotely generated Bell pairs (Figure 77). Their analysis identified a regime with local two-qubit-gate errors below about 1% and nonlocal Bell-pair errors below about 10%, with projected error-correction cycle rates extending into the range compatible with a 100 kHz logical clock under favorable hardware assumptions [887, 888]. These are modeled architecture-dependent thresholds, not a generic statement that 10% interconnect error is acceptable for every surface-code implementation.

A variant is investigated at Princeton University which is using photon switches to connect multiple QPUs using a similar principle (Figure 78).

Trapped-ion QPUs have also been interconnected through photonic links [891–895]. Photonic modularity was a major part of IonQ's historical scale-out strategy [896], while matter-qubit shuttling is another route represented by Oxford Ionics [897]. IonQ agreed to acquire Oxford Ionics in June 2025 and completed the acquisition in September 2025. In September 2025, IonQ also announced experimental frequency conversion of photons associated with barium-ion transitions toward telecom wavelengths in an AFRL-funded project.

One proposal from Berkeley uses temporal multiplexing to entangle streams of moving ions in an RF Paul trap [898]. A European team demonstrated entanglement of trapped-ion qubits separated by 230 m [899]. In 2026,

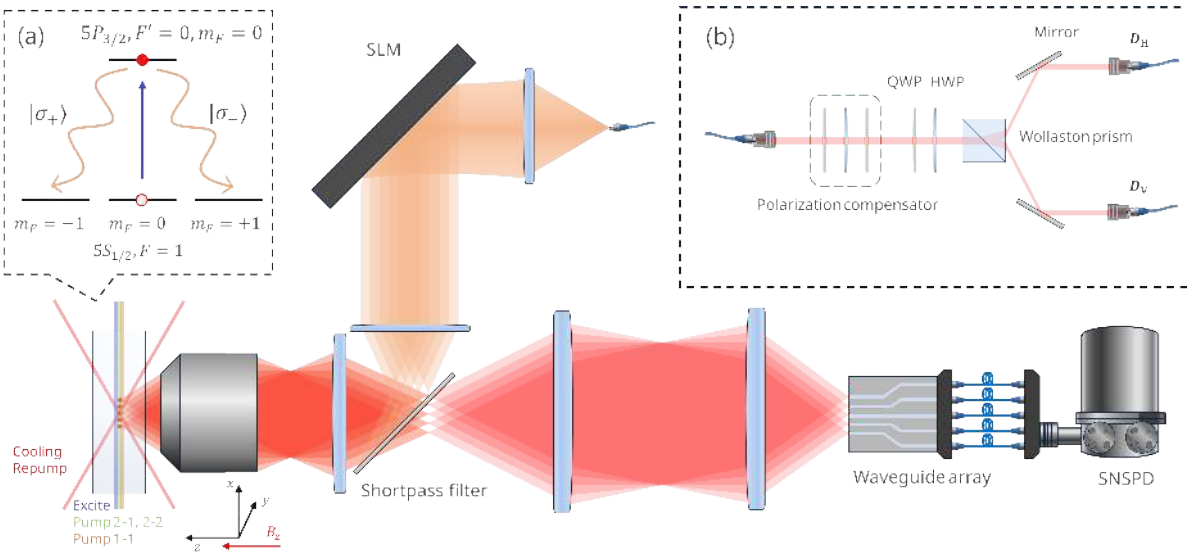


Figure 75: A multiplexed photonic interface guiding photons from a rubidium atom array controlled by SLMs to a single-mode waveguide array fabricated on a glass-based photonic integrated circuit and feeding SNSPD single photon detectors. Source: [885]. Added in 2026.

a Chinese team demonstrated heralded ion-ion entanglement over 1.2 km of fiber using ten temporal modes, obtaining a 4.59× generation-rate enhancement and an entanglement fidelity of 95.9±1.5% [900] (Figure 81).

At some point, interconnect architectures may someday mix various techniques, with short-range interconnect techniques using microwaves and longer range techniques based on photons entanglement. It may also be useful to convert optical photons used for atomic qubit interactions from/to infrared photons which are easier to transport on telecom fibers [901].

Photon-based chip-to-chip teleportation has been demonstrated in silicon photonic circuits [902]. Separately, rare-earth erbium spin ensembles have been strongly coupled to superconducting microwave resonators [903], illustrating a hybrid spin-microwave interface rather than an NV-center photonic interconnect.

Another solid-state network-node architecture couples the electron spin of a silicon-vacancy (SiV) center, acting as a communication qubit, to a nearby ^{29}Si nuclear spin acting as a memory qubit [904, 905].

Other researchers encode quantum information in different photonic degrees of freedom. Polarization itself is a quantum discrete-variable encoding, not a classical encoding. Caltech researchers demonstrated teleportation of time-bin qubits at 1,536.5 nm over fiber, with conditional teleportation fidelities above 90% rather than a 90% transmission success probability [906]. Christopher Monroe's team also proposed networking ion-based qudits with time-bin encoded photons to increase the information carried per successful photonic link [907].

Experiments have also converted between DV (discrete-variable) and CV (continuous-variable) optical qubits, including conversion of single-photon qubits to cat-state qubits [908]. A separate microwave experiment demonstrated a deterministic SWAP between a superconducting artificial atom and a frequency-encoded microwave-photon qubit [909]. Interconnects also require photon routing and multiplexing [910–912], and proposed quantum data buses can route entanglement over multiple network paths [913].

1.5.4 Electrons and ions shuttling

Electrons shuttling is a technique envisioned to enable interconnection of silicon spin qubits [914]. It would have a very short range.

QUASAR was a German semiconductor project investigating coherent electron shuttling with a QuBus (Figure 79), targeting transport over distances of about 10 μm. Partners included Infineon, HQS, Fraunhofer IAF and IPMS, Leibniz institutes IHP and IKZ, and the Universities of Regensburg and Konstanz. The project targeted a 25-qubit demonstrator and received €7.5M from BMBF [915]. Jülich also participated in the European Quantum Flagship QLSI project led by CEA-Leti.

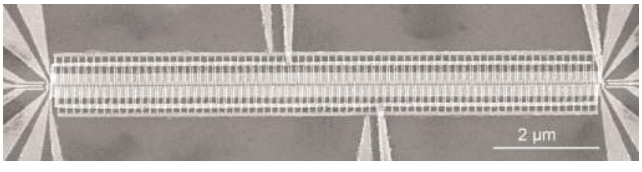


Figure 79: An electron shuttling waveguide. Source: [915].

Ion shuttling is central to QCCD trapped-ion architectures such as Quantinuum's and Oxford Ionics' processors. Since IonQ acquired Oxford Ionics in 2025, it is also part of IonQ's roadmap, but is different from the architecture of IonQ's earlier ion linear-chain systems (Forte, Tempo).

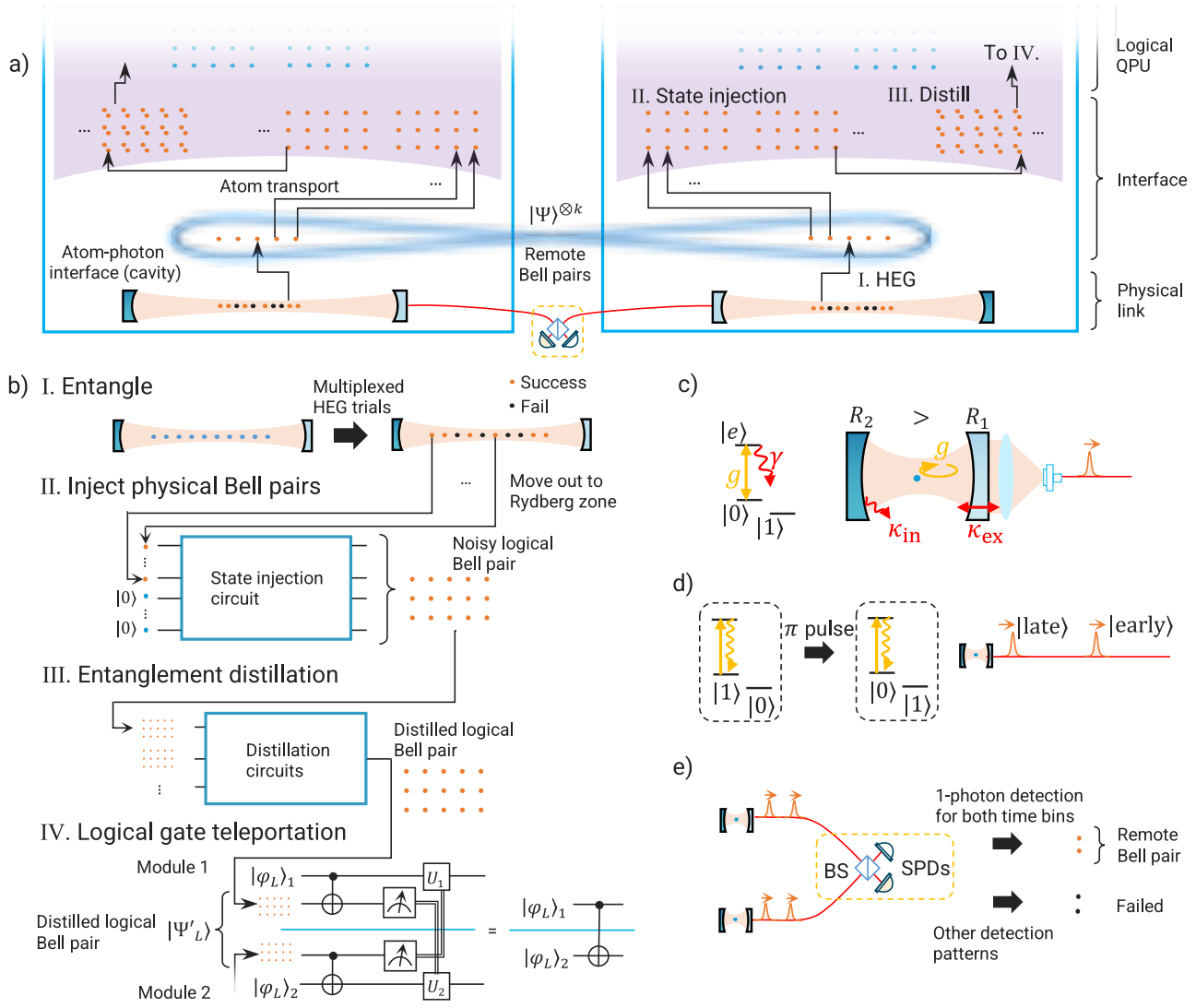


Figure 76: Full-stack blueprint to implement cold-atoms QPU interconnect by NanoQT. I to IV describe the layers between a CNOT gate teleportation and its underlying implementation. Source: [884].

Finally, superconducting circuits can also exchange quantum information through itinerant surface-acoustic-wave phonons, providing a solid-state acoustic communication channel [916] (Figure 80).

1.5.5 Architecture and infrastructures

One major architectural question is whether quantum-processor interconnect will first be deployed inside a quantum data center or between geographically separated parties in multi-tenant networks [917]. Near-term modular FTQC is likely to begin within a site, where optical or microwave links can join multiple QPUs into one computing resource, the "Quantum Datacenter" concept [918, 919] (Figure 82). The required proximity of classical computing is workload-dependent. Real-time control, decoding, feed-forward, timing and network scheduling can have microsecond-scale or tighter latency constraints and may need close integration with the QPUs, while compilation, job planning and other non-real-time functions can be farther away (Figure 83).

Building network services with sufficiently high entanglement rate, fidelity, availability and quality of service remains a major challenge [920].

Many key areas must make progress to enable the deployment of quantum telecommunications networks: protocols [921–923], repeaters [924–927], switches and routers [803, 928–931], quantum memories [932, 933], distributed quantum error correction schemes and determining the related entanglement fidelity thresholds and how it can be relaxed [934–942], compilers and other various methods and software tools to distribute processing over several QPUs with optimizing circuit partitioning [943–962], DQC emulators or simulators [963–967], resource estimators [968, 969], DQC scheduling tools [970], distributed databases [971], and at last benchmarking techniques [972]. All these components bear their own complicated scientific and technological challenges [973, 974].

We can add resource-estimation tools such as the one proposed in 2025 in [975]. In its studied configuration

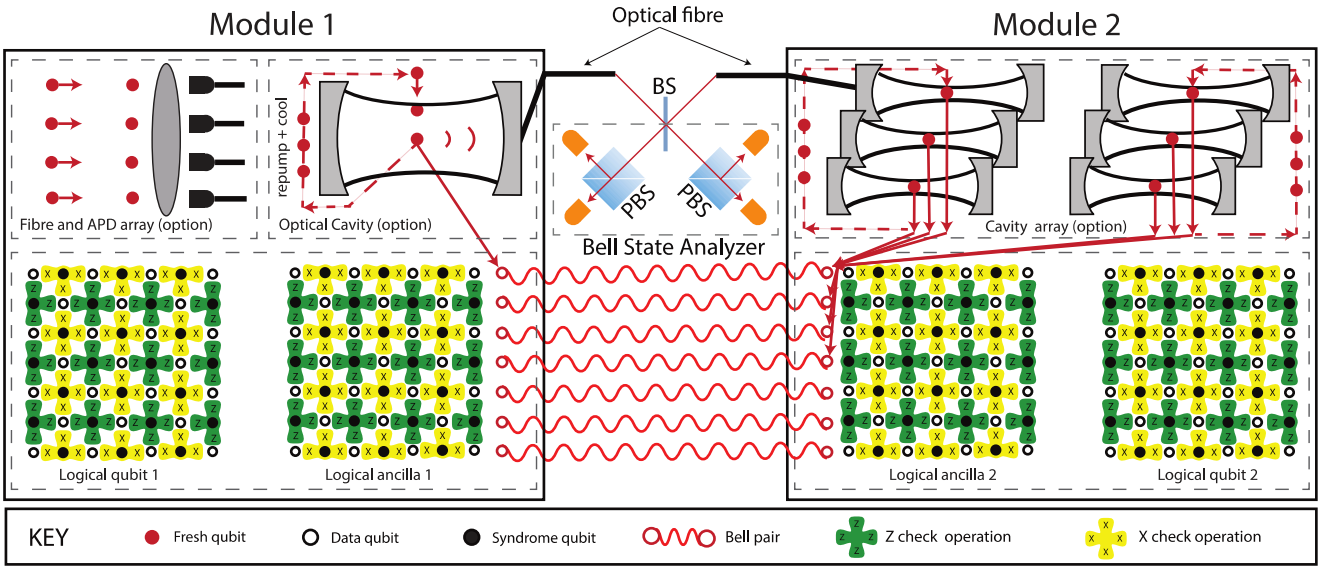


Figure 77: Interconnect architecture proposal for two cold-atom QPUs, proposed by Harvard University and collaborators. Source: [888]. See also [889], which details the cavity implementation.

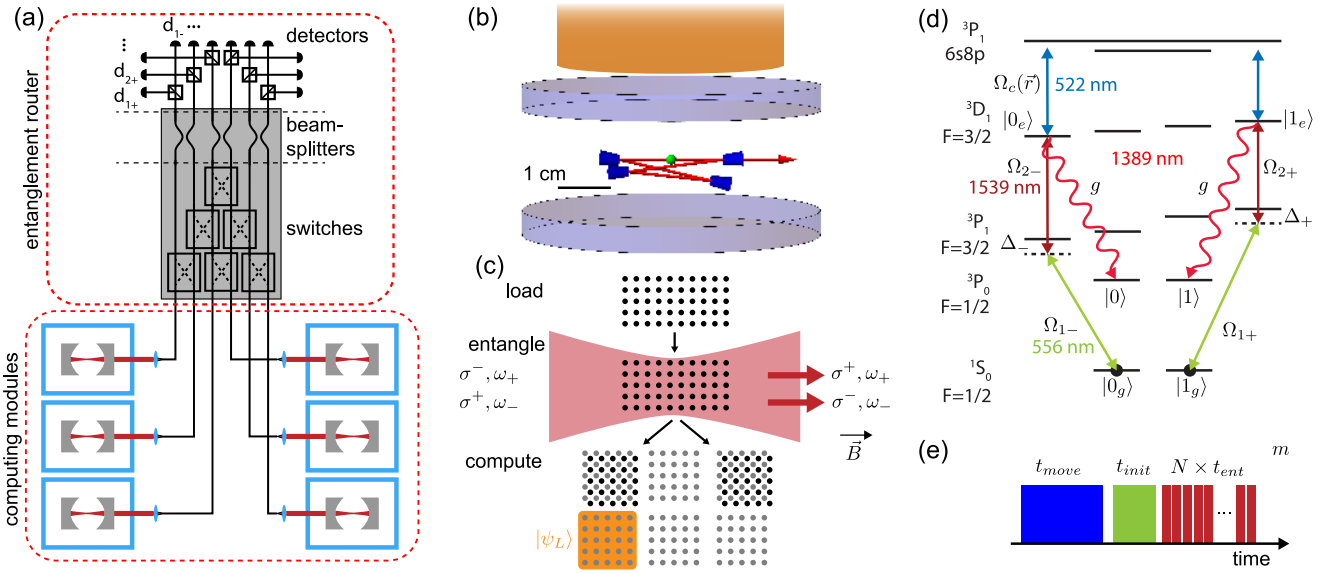


Figure 78: Entanglement between modules is mediated by 1,389 nm infrared photons emitted into single-mode fibers. This wavelength has lower fiber attenuation than visible light and can support kilometer-scale links, but propagation still incurs finite optical loss. The photons are emitted after a two-color excitation involving 556 nm and 1,539 nm transitions (Ω_1 and Ω_2). Source: [890].

with 45,000 qubits per node, the distributed architecture used on average about 1.4× more physical qubits and 4× more execution time than its monolithic baseline before optimization. Another 2026 estimate [976] assumed intrachip two-qubit error rate 10^{-3}, interchip error rate 10^{-2} and interchip gates 25× slower. In that model, RSA-2048 factoring required about 2.0 million physical qubits and 4.4 days, compared with 1.3 million qubits and 3.4 days for the monolithic baseline, while the surface-code distance increased from $d = 27$ to $d = 31$. This corresponds to roughly 54% space overhead and 29% time overhead.

Communication bandwidth is already a major challenge. As a useful metropolitan-scale reference point, a 2023 experiment demonstrated quantum teleportation over 64 km of fiber at 7.1±0.4 successful teleportations per second, with average single-photon teleportation fidelity of at least 90.6±2.6% [977]. This is many orders of magnitude below local two-qubit gate rates, illustrating why entanglement-generation rate and allocation become first-class architecture resources [978].

Another architecture variable is how physical and logical qubits are distributed across interconnected processors. Possible regimes range from unencoded multi-QPU NISQ execution [979, 980], through logical qubits or lattice-surgery operations spanning modules, to modules that each contain many complete logical qubits. The physical-qubit overhead per logical qubit is not fixed by

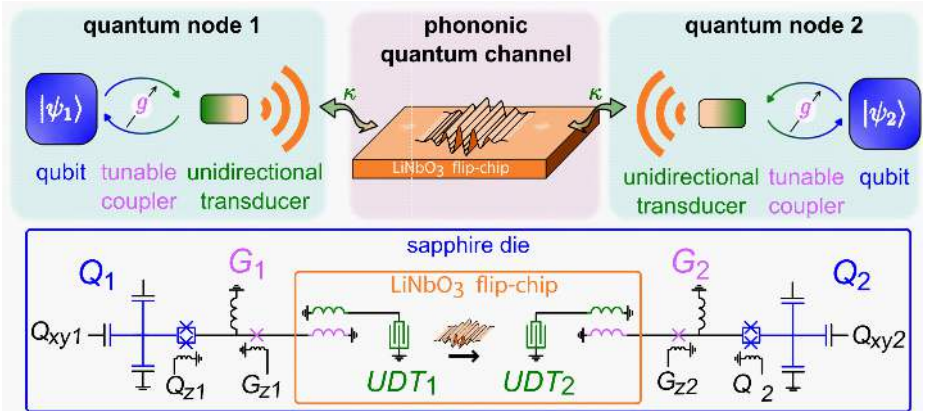


Figure 80: An interconnect technique for superconducting qubits using surface-acoustic-wave-based phononic communication. Source: [916].

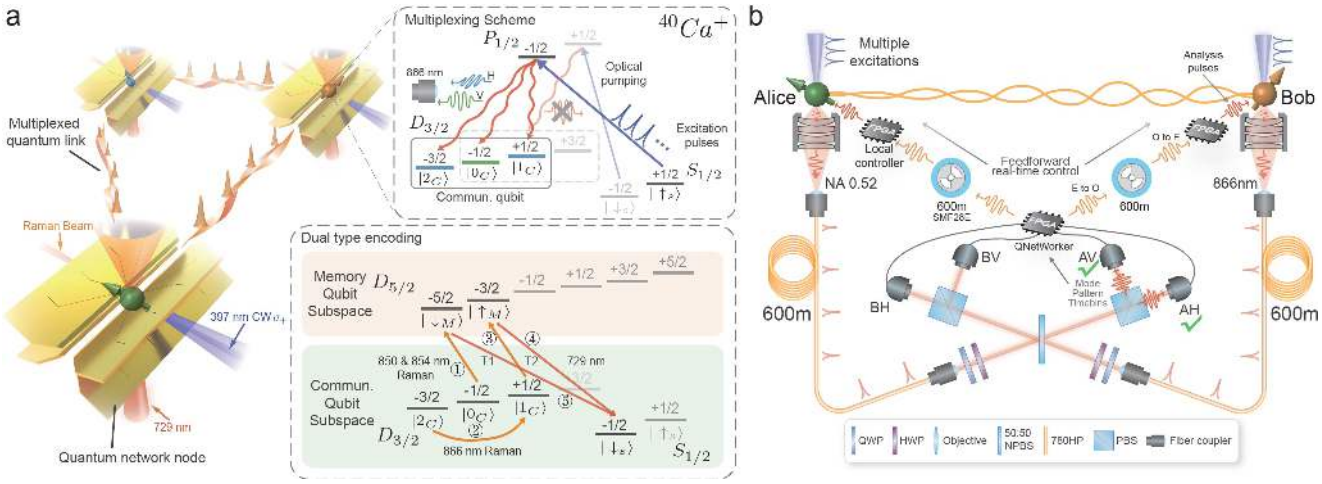


Figure 81: A trapped-ion interconnect experiment over 1.2 km of fiber using ten temporal photonic modes, published in 2026. The reported ion-ion entanglement fidelity was 95.9±1.5%. Source: [900].

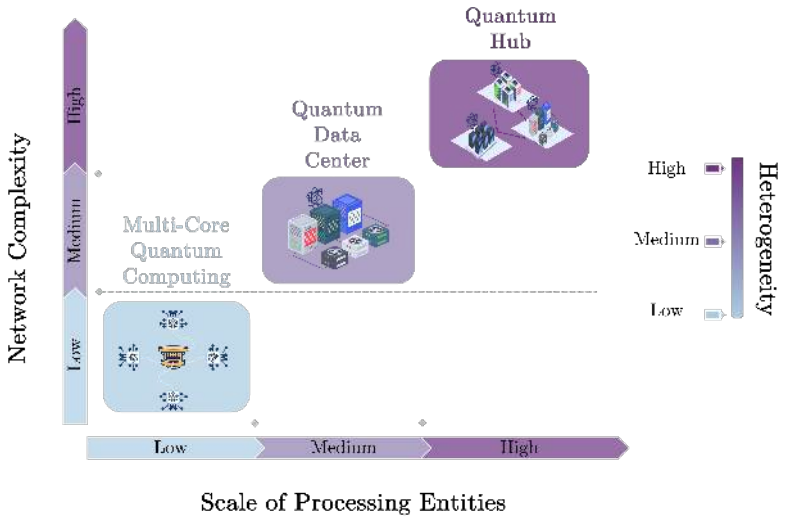


Figure 82: Positioning the notion of Quantum Data Center which hosts multiple QPUs connected with each other in a given location. Source: [919].

circuit size alone. It depends on physical error rates, the target logical failure probability, the error-correcting code and the circuit volume or algorithm duration. As those requirements tighten, the necessary code distance can increase enough that one logical qubit or one logical operation spans more than one module. Module capacity is itself platform- and maturity-dependent (Figure 84). In 2026, a U.S. team reported space-time resource esti-

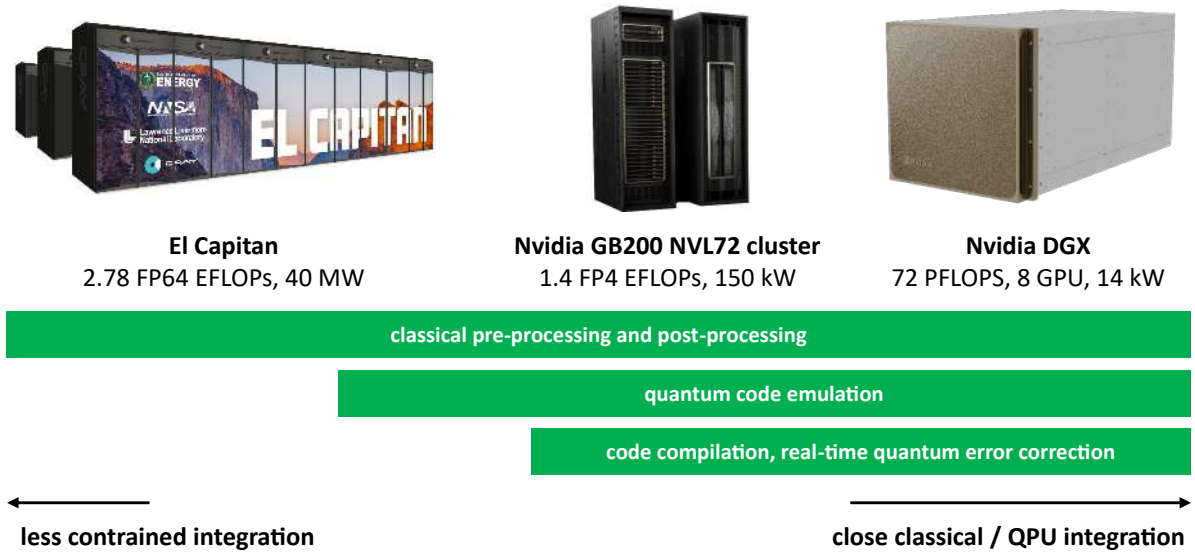


Figure 83: How close must classical computing resources be to the quantum processors? This is still an open question. © Olivier Ezratty, June 2025.

mates for RSA-2048 factoring using between 3 and 13 quantum nodes [98].

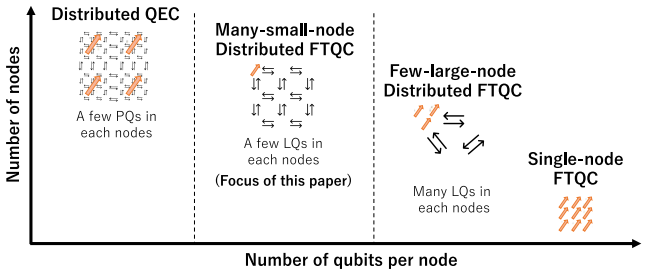


Figure 84: Different DQC regimes depend on the physical-qubit capacity of each node and on the physical-qubit overhead required per logical qubit. That overhead varies with physical error rates, target logical error budget, error-correcting code and circuit volume, while achievable node size depends on the qubit technology and system maturity. Image source: [981].

We will then probably see evolving schemes in a nested architecture, with point-to-point interconnection between parties, then, metropolitan level connectivity with evolving network layouts [982, 983], then, with longer distance connectivity, potentially using satellites [984, 985], more global connectivity, creating what could be called a global quantum Internet. It will require that these systems not only enable easy point-to-point communications between different parties but also make them interoperable with shared protocols, optimized resource allocations and quality of service [986, 987], addressing [988], and naming standards. Resources will also have to be evaluated on how to build these networks, including assessing their potential cost and economic value [989, 990].

Classical networking resource estimates will have to be done and may also create their own latency bottlenecks, particularly for DQC distributed over multiple quantum data centers and for configuration exceeding a million physical qubits [991].

1.5.6 Other use cases

Quantum telecommunications have multiple use cases beyond distributed quantum computing:

Quantum digital signatures aim to authenticate classical messages while providing unforgeability, transferability and non-repudiation under the assumptions and threat model of the particular protocol. These properties are cryptographic guarantees, not unconditional properties of every implementation.

Quantum-computing-based cryptography also includes research proposals that use quantum processors to construct symmetric-key primitives, including quantum permutation-pad schemes. This is a narrower research topic than QKD or post-quantum cryptography and is not yet a standardized networking service.

Distributed quantum sensing can combine quantum states or entanglement shared among spatially separated sensors to improve estimation precision for suitable observables [992], including interferometric and telescope-network proposals, and can protect or authenticate some sensing resources [993], such as by certifying multipartite states against dishonest participants to ensure the privacy of local node parameters during distributed estimation [994]. A coherent quantum interface between a sensor and a quantum processor could avoid measuring and classically re-encoding an intermediate quantum state in some protocols.

Clock synchronization using entangled photons and related quantum protocols has been experimentally explored since the early 2000s and is relevant to timing, telecommunications and navigation systems such as GNSS [995].

Quantum Secure Direct Communication (QSDC) denotes protocols in which the message itself is encoded into quantum states rather than first using the quantum channel only to establish a secret key. Early entanglement-based proposals date to 2002 [996], and later protocols use both discrete- and continuous-variable optical encodings [997, 998]. As in QKD, security depends on authenticated protocol steps, channel testing, implementation assumptions and a bounded eavesdropper information model. Some QSDC protocols still require classical communication for control, authentication or parameter estimation. Experimental and industrial variants continue to be investigated [999, 1000].

Quantum Public Key Encryption (PKE) denotes proposed cryptographic schemes in which at least one public-key resource or encryption step is quantum. Depending on the construction, the public key may be a quantum state, a hybrid quantum-classical object or a classically described state-preparation procedure, while the ciphertext may be quantum or classical. These proposals are distinct from standardized post-quantum public-key cryptography and generally rely on construction-specific computational and noise assumptions [1001].

Quantum money originates from Stephen Wiesner's conjugate-coding idea, proposed around 1970 and published in 1983. Its core principle is that a banknote contains quantum states whose valid preparation is difficult to reproduce because unknown quantum states cannot be perfectly cloned. This is not simply a one-use classical token. Later quantum-money and S-token protocols use different security models. A photonic S-token experiment reported 88.24% system efficiency and analyzed robustness against multiphoton attacks [1002, 1003].

Anonymous quantum communication protocols aim to hide the identity of a sender, a receiver, or both from specified adversaries or other network participants while still delivering classical or quantum information. Their anonymity and auditability depend on the protocol, trust assumptions, metadata leakage and classical control infrastructure.

Quantum pseudotelepathy describes nonlocal games in which spatially separated players sharing entanglement achieve correlations impossible for classical players under the same communication constraints, while still obeying no-signaling [1004, 1005]. Examples include the Mermin-Peres magic-square game, in which Alice and Bob answer coordinated row and column queries without communicating during the game [1006].

Quantum position verification (QPV) uses relativistic signaling constraints together with quantum-information limits so that spatially separated verifiers can test whether a prover is located near a claimed position. It is a position-based cryptographic primitive, not a form of QKD [1007].

Detecting extra-terrestrial quantum communication. SETI-oriented work has discussed whether intentionally engineered quantum optical signals could have observables distinguishable from natural astrophysical light [1008]. This remains a speculative search concept rather than an established application of quantum telecommunications.

1.5.7 QPU interconnect vendors

Bohr Quantum Technology

USA, 2022

Bohr Quantum Technology is a stealth startup working on a quantum interconnect system based on some Caltech and Fermilab research. It is supposed to enable quantum computing scale-out architectures with interconnecting QPUs and/or quantum memories. The company was created by Paul Dabbar (CEO, a former U.S. Under Secretary for Science at the Department of Energy) and Conner Prochaska (Chief of Strategic Partnerships, also formerly at the Department of Energy).

CavilinQ

USA, 2025, $8.8M

CavilinQ is a spin-off from Harvard and the University of Chicago created by Shankar G. Menon (CEO) and Brandon Grinkemeyer (CTO) with Mikhail Lukin (Harvard) and Hannes Bernien (University of Innsbruck) being scientific co-founders and advisors.

They develop ultra-high-finesse optical micromirrors, microcavities, and packaged cavity assemblies for atom-based quantum processors which are used for interconnecting cold-atom and trapped-ion-based quantum processors. They trap single rubidium atoms in optical tweezers to a Fabry-Perot fiber cavity. The technology enables nondestructive qubit readout with 99.96% fidelity and fast remote entanglement generation for quantum networking with an entanglement fidelity of 52.5% [889, 1009, 1010]. Their target market also includes metrology, optical clocks, and inertial navigation.

Cisco Systems

USA, 1984

On top of its investments in QKD which are described later in 1.7, Cisco is also developing quantum processor interconnect technologies.

They announced in April 2026 the development of a prototype quantum switch to connect different quantum computers and sensors into a single network, enabling distributed quantum computing. It routes entangled photon signals using telecom fiber at room temperature [1011]. The switch is built with thin-film lithium niobate that is capable of dynamic entanglement routing with reconfiguration speeds up to 1 GHz.

At the system architecture level, they benchmarked quantum data center topologies such as QFly, BCube, Clos, and Fat-Tree to evaluate how physical-layer constraints like optical loss, EPR pair generation delays, and resource contention impact end-to-end execution latency systematically [1012].

At the software and compilation levels, they introduced ATHENA, a DQC compiler that mitigates the latency and error overhead of non-local CNOTs by utilizing utility-driven lookahead and early scheduling to optimize teleportations [1013].

They also analyzed distributed quantum error correction in [1014, 1015], examining how network partitioning and noisy non-local gates affect the logical error suppression with Bivariate Bicycle codes like the $[\![144, 12, 12]\!]$ code deployed across multiple interconnected processors. This relates to their announced technology partnership with IBM on these topics in November 2025. Cisco is also partnering with Atom Computing.

Entangled Networks

Canada, 2020-2023

Entangled Networks was a startup developing a set of protocols and software for multi-QPU environment (multi-qubit gates implementation across distributed QPUs, performance optimization). The hardware part requires optical quantum interconnect solutions including a high-resolution optical collection system and a low loss Bell state analyzer. The company created by Aharon Brodutch (CEO) and Ilia Khait (CTO), two Israeli researchers in Toronto, was acquired by IonQ in January 2023.

Lightsynq Technologies

USA, 2024-2025, $18M

Lightsynq Technologies was created by Mihir Bhaskar (CEO), Bart Machielse (CTO) and David Levonian (CPO) out of Harvard. It developed photonic interconnect and quantum-memory technologies intended to support atoms [800], ions, photons and superconducting qubits [1016]. IonQ completed its acquisition of Lightsynq in 2025.

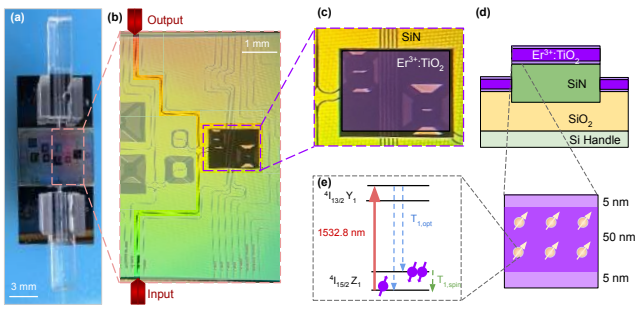


Figure 85: The erbium-based memory from memQ. It is using thin films of titanium dioxide (TiO2) doped with erbium (Er) and deposited on silicon nitride nanophotonic waveguides. Source: [1017].

memQ

USA, 2022, $12M

memQ is creating some solid-state erbium-based quantum repeater and memory targeting quantum Internet use cases [1018, 1019] (Figure 85). The Chicago-based startup was seed funded by Quantonation, Exposition Ventures, and the George Schultz Innovation Fund.

NanoQT

Japan, 2022, $24M

NanoQT, *aka* Nanofiber Quantum Technologies, is a quantum computing startup launched out of Waseda University by Takao Aoki (CSO), Masaru Hirose (CEO) and Akihisa Goban (CTO) [1020].

Their technology is based on the Nanofiber QED resonator invented by Takao Aoki [1021]. These are neutral atom-based qubits (^{171}Yb) that are connected with each other through photons and a nanofiber that receives fluorescence photons to be detected by SNSPDs (nanowire superconducting photon detectors). It enables n-to-n two-qubit gates full-connectivity between these qubits [1022]. They currently support only a few qubits and say it could scale to 10,000 qubits [1023]. In July 2024, they published an interesting blueprint pre-print on how they plan to use these fibers to interconnect cold-atoms QPUs. Interestingly, a team in China is working on a similar technology [1024]. The company is focused on its interconnect technology. It is partnering with QuEra for the integration of their nanofiber interconnect technology with QuEra QPUs and with Mitsubishi Electric Corporation for the association of Mitsubishi qubit control and NanoQT nanofiber cavity technology.

NanoQT plans to support logical Bell pair generation by 2028 with 200 physical qubits per interconnection unit and 99% fidelity and then, FTQC support with 2,000 connections and 99.9% fidelity (that's quite ambitious [1025]), using multichannel support and time-multiplexing. Their technology uses telecommunication wavelength thanks to the use of ytterbium atoms as demonstrated in September 2026 [1026, 1027], and supports quantum repeater features.

The University of Maryland is also working on the development of interconnection between nanofiber and cold atoms lattices [1028].

Nu Quantum

UK, 2018, $72.8M

Nu Quantum is a spin-off from the University of Cambridge co-founded by Carmen Palacios-Berraquero (CEO) which creates a full-stack photonic-based QPU interconnect solution, focused for the moment on cold-atom and trapped-ion based QPUs. They had a staff of 65 people as of June 2025. In February 2026, they created a trapped-ion quantum networking laboratory in

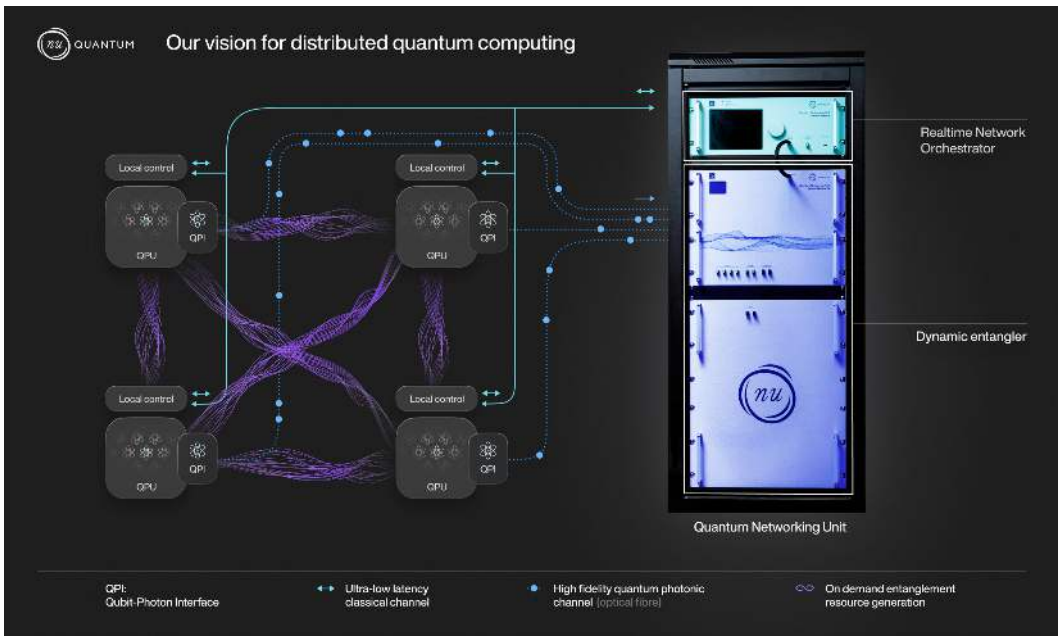


Figure 86: Nu Quantum QPI interconnect platform connecting four trapped-ion QPUs, tested in 2025. Source: Nu Quantum website, vendor-reported.

Cambridge, UK, next to their home base. The company is also behind the creation of the Quantum Datacenter Alliance (QDA) in 2025 along with multiple vendors and academic partners including Cisco.

Initially, it was developing QKD optical links and satellite systems using proprietary single-photon components. They also created their own source of single photons and had the ambition to create a photon-based quantum computer.

In January 2024, Nu Quantum won a contract from the UK government to deliver a modular, rackmount and scalable enabling QPU interconnect as part of the project LYRA. It is teaming up on the project with Cisco. Nu Quantum and SoftwareQ (quantum software) announced in 2024 a collaboration to build a theoretical framework for a distributed FTQC architecture [1029]. It is funded by the UK and Canadian governments quantum initiatives. It will quantify the efforts to create a quantum network of quantum computing nodes encompassing the compiler needs to optimize the algorithm distributed circuit based on the characteristics of the QPUs, network topologies, and error correction. The project uses SoftwareQ's compiler and Nu Quantum's control system real-time firmware. In September 2024, Nu Quantum and NQCC (UK) launched the first phase of the 4-year Project IDRA that is designing a multi-node optical distributed quantum computing network.

Figure 87: Nu Quantum QPI microcavities. Source: Nu Quantum website, vendor-reported.

In October 2024, Nu Quantum presented the first generation of their Qubit-Photon Interface (QPI) prototype which connects a cold-atom QPU to a quantum network. The photon sources are optical microcavities and nanostructured mirrors (Figure 87). They are sealed in ultra-vacuum. Their length depends on the used photon wavelength: 2 mm for cold-atoms and 400 μm for trapped ions. The cavity principle is inspired by the work of Tracy Northup from Innsbruck University and Matthias Keller from the University of Sussex [1030, 1031]. They can host either a single ion or a cold atom. These are "communication qubits" that are connected to QPU computing qubits using laser-based entanglement. A drive laser pulse sent on the atoms generates the

emission of a photon that is then later used to generate entanglement with a photon emitted by another cavity.

As of 2025, they generated entangled photons with up to 99.7% fidelities. It was extended in 2025 by a version for connecting 4 trapped ions QPUs. The QPI is integrated into their Quantum Networking Unit (QNU) rackmount solution (Figure 86).

Nu Quantum developed a photonic integrated circuit (PIC) for optical switching and detection that creates and distributes entanglement across multiple computing nodes. They proposed in 2025 the use of hyperbolic Floquet error correction codes that are adapted to the implementation of distributed quantum error correction with fewer constraints on qubit connectivity than with the popular qLDPC codes [1032, 1033]. In 2026, their researchers also demonstrated how a failing quantum processing node can be dynamically replaced in a DQC architecture [1034].

Nu Quantum also created a control architecture for distributed timing and feed-forward, with CERN to integrate CERN's White Rabbit technology into the QNU to enable improved timing synchronization.

Quantum Datacenter Alliance

UK, 2025

In 2025, Nu Quantum and industry partners including Quantinuum, Cisco, NTT Data, OQC, QphoX and QuEra launched the Quantum Datacenter Alliance, a consortium aimed at cross-industry collaboration across multiple layers of the quantum-computing stack, including QPUs, QPU interconnects, entanglement networks, middleware, error correction, HPC integration and software. The inaugural event took place at Battersea Power Station in London in June 2025, followed by another event at the same location on October 1, 2026.

QphoX

the Netherlands, 2021, €12.5M

Given it is still the dominant architecture, superconducting to photons connectivity is an intense field of research. In that case, microwaves could be converted to another frequency range while keeping the quantum state alive.

This conversion can be done with opto-electromechanical systems [1035, 1036]. TU Delft researchers led by Simon Gröblacher experimentally achieved this in 2018, at 20 mK, close to superconducting qubits operating temperature [1037] (Figure 88). As of 2024, it seemed that the technology could be used to teleport a qubit state. Their electro-optic transducers modulate optical signals with microwave fields by leveraging the Pockels effect in materials such as lithium-niobate on silicon. A small block of lithium niobate converts weak microwave signals into mechanical motion (vibrations), which is then used to convert the signal to optical frequencies, while silicon is used for the photonic cavity and waveguides [1038]. They also investigate the use of thin-film gallium phosphide to achieve ultra-low-noise photon conversion [1039].

This led to the creation of QPhoX by Simon Gröblacher (CEO). The research project turned into a "quantum modem for the quantum Internet" [1040–1043]. Although QPhoX is a startup, it seems still operating fundamental and experimental research, like many quantum startups [1044]. In September 2022, the startup announced a partnership with IQM to scale-out superconducting qubit quantum computers. The company had a staff of about 40 as of September 2026.

In May 2025, QPhoX published an end-to-end architecture study for superconducting-QPU interconnect using microwave-optical transduction [1045]. Its Quantum Transducer was commercially launched in March 2026. Reported conversion efficiencies remain far below those required by most proposed high-rate interconnect architectures [1043, 1046, 1047]. For a direct ideal pure-loss bosonic channel, 50% transmissivity is the threshold below which the unassisted one-way quantum capacity is zero [868], but this is not a universal physical-transducer efficiency requirement. In September 2026, related work from the Gröblacher group reported 76% optical-to-mechanical photon-phonon conversion near the single-quantum regime [1048]. That result is an optical-to-mechanical conversion stage, not an end-to-end microwave-to-optical transducer.

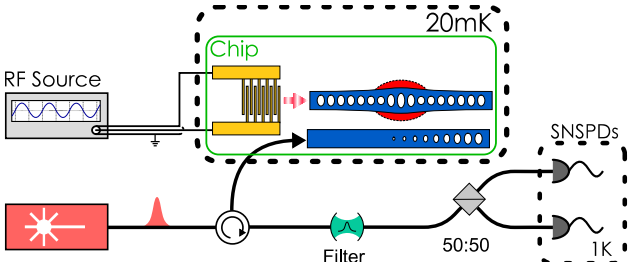


Figure 88: QPhox transduction architecture using an opto-electromechanical chip for the transduction of microwave photons to optical photons. Source: [1037].

The company is also developing optical-based multiplexing technologies for the downlink control [1049] and uplink readout of superconducting qubits [1050].

Silq Connect

Canada, 2024

Silq Connect is a company creating a microwave-optical quantum interconnect solution connecting QPUs. The company does not provide scientific data on its technology, which appears to be a transduction solution similar to the one from QphoX. Its capabilities are therefore unable to be verified from public material.

Welinq

France, 2022, €5M

Welinq is a startup created by Tom Darras (CEO), Julien Laurat and Eleni Diamanti (both scientific advisors). It is a spin-off from two laboratories from Sorbonne Université: the Laboratoire Kastler Brossel (LKB) and the Laboratoire d'Informatique (LIP6). The company had a staff of over 40 as of mid-2026.

They develop a full-stack hardware and software quantum-link solution for interconnecting quantum processors. Their links use cold-atom-ensemble quantum memories (Figure 89), with the goal of supporting modular quantum computing and repeater-based quantum networking.

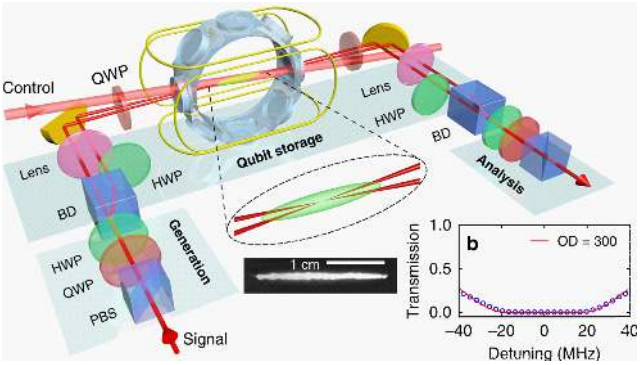


Figure 89: Welinq's quantum memory architecture. Source: [1051].

Their first product, called *QDrive*, is a compact and transportable quantum memory intended to be deployed in quantum computing infrastructures to perform first proof of concepts with providers of quantum computing [1052]. Their memory technology is based on an elongated quasi-2D magneto-optical trap of alkali atoms cooled at a temperature close to 20 μK by lasers and adapted to DV photons (discrete variable). It enables the on-demand (i.e., the storage time is adjustable by the user) and efficient storage of photonic qubits and entangled states with a world record efficiency of 90%, qubit fidelity above 99%, a storage time of 200 μs and storage retrieval efficiency >90% [1051, 1053]. This is becoming a real commercial product. Welinq also develops a parametric source to convert photons wavelength from 795 nm (adapted to rubidium atoms interactions) and 1550 nm (for telecoms). It is prototyping a solution for routing guided single photons by combining atom trapping and transverse light confinement with an optical nanofiber and with ultra-low power [1054].

Welinq also develops software to distribute and optimize circuits across multiple QPUs. In 2025, it unveiled araQne, a compiler for distributed quantum circuits. araQne was tested with algorithms including the QFT and QAOA [954]. In 2026, Welinq researchers analyzed distributed rotated-surface-code operation on their architecture [1055] (Figure 90).

In September 2022, Welinq announced a partnership with ixBlue (now Exail) for the procurement of lasers adapted to their needs. It also launched in 2024 a partnership with Pasqal to develop inter-QPU connectivity, with EDF (project AQADOC) to estimate the impact and algorithmic cost of QPU interconnect solutions, and also with Quandela, to develop an interconnect solution for photon qubits. This was completed by the partly-publicly funded €4M InterQo project also with Pasqal. Welinq also partners with QphoX, as part of the formalized Meet-Q project announced in October 2025, their respective offering being quite complementary (quantum transduction vs quantum memory).

In January 2026, Welinq announced the first commercial sale of QDrive to the Institute of Physics of the Slovak Academy of Sciences as part of Slovakia's quantum-communication infrastructure. The deployment is associated with the skQCI ecosystem, including QUTE.sk.

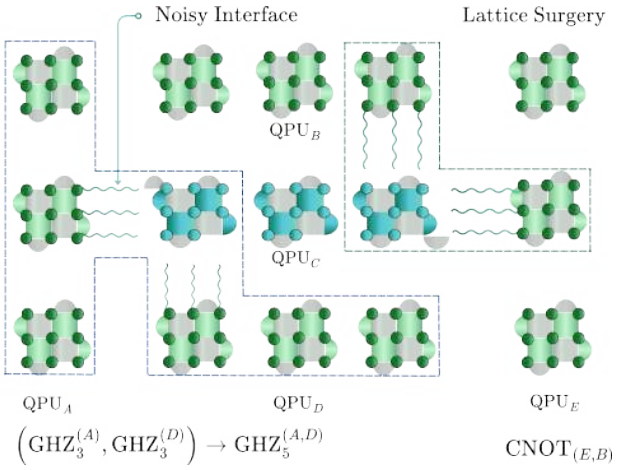
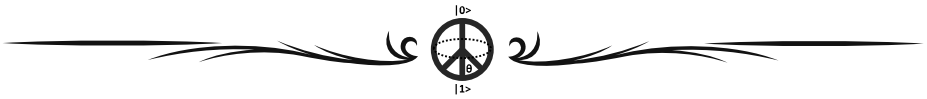


Figure 90: Welinq investigated the capability of their interconnect technology to support distributed logical CNOT gates implemented with lattice surgery and rotated surface codes. The green-grey patches represent distance-3 logical data qubits, blue-grey patches are logical ancilla qubits for the implementation of lattice surgery. Remote fault tolerant CNOT gates are implemented by lattice surgery across noisy interfaces corresponding to the wiggly lines. Such setup can be used to generate large GHZ states. Source: [1055].

In the quantum memory realm, researchers in China succeeded in 2019 to entangle two rubidium atom ensembles quantum memories via entangled photons at a distance of 50 km and with SNSPD single photon detectors (cooled at 4K) [1056]. In 2025, another team in China tested a multiplexed memory with a cold rubidium ensemble using encoding photons carrying high-dimensional orbital angular momentum (OAM), with storage fidelities exceeding 83% on all channels in a 4-dimensional Hilbert space [1057]. This contrasts with a UK experiment in 2024 with rubidium atoms vapor memory operating at telecom wavelength, capturing a photon coming from a quantum dot III/V source but with a mere 12% memory efficiency [1058], which may be sufficient for QKD applications but probably not for QPU interconnect. Also, the topology for quantum net-

works and quantum memories will require some specific architectural designs [1059].

Other efforts are undertaken to connect heterogeneous quantum networks with hybrid entanglement swapping between DV and CV photonic systems [1060]. More classically, qubits can be distantly connected through a photonic link, as MPQ researchers in Germany showed in 2021 [1061].



1.5.8 Bibliography and notes

These are the bibliographical references and notes for the **Quantum Telecommunications** subsection.

[98] Factoring 2048 bit RSA integers with a half-million-qubit modular atomic processor, by Tian Xue and Jacob P. Covey, arXiv, May 2026 (29 pages).

[728] Quantum internet: A vision for the road ahead, by Stephanie Wehner, October 2018 (11 pages) 🔓 (preprint on resolver.tudelft.nl).

[729] Quantum Networking Fundamentals: From Physical Protocols to Network Engineering, by Athanasios Gkelias, Felix T. A. Burt, and Kin K. Leung, arXiv, April 2026 (55 pages).

[730] Advanced Quantum Communication and Quantum Networks – From basic research to future applications, by Björn Kubala, Alexander Sauer, Alessandro Tarantola, David Fabian, Anke Ginter, Olga Kulikovska, Fabio Di Pumpo, Johannes Seiler, Wolfgang P. Schleich, and Matthias Zimmermann, arXiv, February 2026 (113 pages).

[731] Distributed Quantum Information Processing: A Review of Recent Progress, by Johannes Knörzer, Jordi Tura, et al., arXiv, October 2025 (72 pages).

[732] Distributed Quantum Computing: A path to large scale quantum computing, by Stephen DiAdamo, August 2021.

[733] Distributed quantum computing across an optical network link, by D. Main, P. Drmota, D. P. Nadlinger, E. M. Ainley, A. Agrawal, B. C. Nichol, R. Srinivas, G. Araneda, and D. M. Lucas, Nature, February 2025.

[734] Metropolitan-scale ion-photon entanglement via a quantum network node with hybrid multiplexing enhancements, by Z.-B. Cui, Z.-Q. Wang, P.-C. Lai, Y. Wang, J.-X. Shi, P.-Y. Liu, Y.-D. Sun, Z.-C. Tian, Y.-B. Liang, B.-X. Qi, Y.-Y. Huang, Z.-C. Zhou, Y.-K. Wu, Y. Xu, L.-M. Duan, and Y.-F. Pu, Nature Communications, December 2025.

[735] Hardware-Software Co-design for Distributed Quantum Computing, by Ji Liu, Allen Zang, Martin Suchara, Tian Zhong, and Paul D Hovland, arXiv, March 2025 (8 pages).

[736] Distributed Quantum Computation via Entanglement Forging and Teleportation, by Tian-Ren Jin, Kai Xu, and Heng Fan, arXiv, September 2024 (8 pages).

[737] Profiling quantum circuits for their efficient execution on single- and multi-core architectures, by Medina Bandic, Sebastian Feld, et al., arXiv, July 2024 (38 pages).

[738] Quantum Routing and Entanglement Dynamics Through Bottlenecks, by Dhruv Devulapalli, Chao Yin, Andrew Y. Guo, Eddie Schoute, Andrew M. Childs, Alexey V. Gorshkov, and Andrew Lucas, arXiv, May 2025 (24 pages).

[739] Generalised Circuit Partitioning for Distributed Quantum Computing, by Felix Burt, Kuan-Cheng Chen, and Kin Leung, arXiv, January 2025 (10 pages).

[740] ECDQC: Efficient Compilation for Distributed Quantum Computing with Linear Layout, by Kecheng Liu, Yidong Zhou, Haochen Luo, Lingjun Xiong, Yuchen Zhu, Eilis Casey, Jinglei Cheng, Samuel Yen-Chi Chen, and Zhiding Liang, arXiv, November 2024 (7 pages).

[741] Optimizing Resource Allocation in a Distributed Quantum Computing Cloud: A Game-Theoretic Approach, by Bernard Ousmane Sane, Rodney Van Meter, et al., arXiv, April 2025 (11 pages).

[742] A Multilevel Framework for Partitioning Quantum Circuits, by Felix Burt, Kuan-Cheng Chen, and Kin K. Leung, arXiv, April 2025 (42 pages).

[743] Distributed Quantum Computation with Minimum Circuit Execution Time over Quantum Networks, by Ranjani G Sundaram, Himanshu Gupta, and C.R. Ramakrishnan, arXiv, May 2024 (11 pages).

[744] A Genetic Approach to Minimising Gate and Qubit Teleportations for Multi-Processor Quantum Circuit Distribution, by Oliver Crampton, Panagiotis Promponas, Richard Chen, Paul Polakos, Leandros Tassiulas, and Louis Samuel, arXiv, May 2024 (9 pages).

[745] Minimizing the Number of Teleportations in Distributed Quantum Computing Using Alloy, by Ali Ebnenasir and Kieran Young, arXiv, April 2024 (12 pages).

[746] Scalability enhancement of quantum computing under limited connectivity through distributed quantum computing, by Shao-Hua Hu, George Biswas, and Jun-Yi Wu, arXiv, June 2024 (13 pages).

[747] Circuit Partitioning and Transmission Cost Optimization in Distributed Quantum Circuits, by Xinyu Chen, Zilu Chen, Pengcheng Zhu, Xueyun Cheng, and Zhijin Guan, arXiv, March 2025 (14 pages).

[748] Compiler for Distributed Quantum Computing: a Reinforcement Learning Approach, by Panagiotis Promponas, Leandros Tassiulas, et al., arXiv, April 2024 (12 pages).

[749] Circuit Partitioning for the Quantum Internet, by Leo Sünkel, Thomas Gabor, and Claudia Linnhoff-Popien, arXiv, September 2025 (8 pages).

[750] UNIQ: Communication-Efficient Distributed Quantum Computing via Unified Nonlinear Integer Programming, by Hui Zhong, Jiachen Shen, Lei Fan, Xinyue Zhang, Hao Wang, Miao Pan, and Zhu Han, arXiv, November 2025 (10 pages).

[751] Distributed Quantum Circuit Cutting for Hybrid Quantum-Classical High-Performance Computing, by Mar Tejedor, Berta Casas, Javier Conejero, Alba Cervera-Lierta, and Rosa M. Badia, arXiv, May 2025 (12 pages).

[752] Hardware-aware Circuit Cutting and Distributed Qubit Mapping for Connected Quantum Systems, by Zefan Du, Yanni Li, Zijian Mo, Wenqi Wei, Juntao Chen, Rajkumar Buyya, and Ying Mao, arXiv, December 2024 (8 pages).

[753] Circuit Folding: Modular and Qubit-Level Workload Management in Quantum-Classical Systems, by Shuwen Kan, Yanni Li, Hao Wang, Sara Mouradian, and Ying Mao, arXiv, December 2024 (15 pages).

[754] LarQucut: A New Cutting and Mapping Approach for Large-sized Quantum Circuits in Distributed Quantum Computing (DQC) Environments, by Xinglei Dou, Lei Liu, Zhuohao Wang, and Pengyu Li, arXiv, February 2025 (20 pages).

[755] The power of entanglement in distributed quantum machine learning, by Yerim Kim, Kiwmann Hwang, Hyukjoon Kwon, and Yosep Kim, arXiv, May 2026 (13 pages).

[756] Distributed Quantum Simulation, by Tianfeng Feng, Jue Xu, Wenjun Yu, Zekun Ye, Penghui Yao, and Qi Zhao, arXiv, November 2024 (24 pages).

[757] Analyzing Common Electronic Structure Theory Algorithms for Distributed Quantum Computing, by Grier M. Jones and Hans-Arno Jacobsen, arXiv, July 2025 (6 pages).

[758] Distributed Quantum Dynamics on Near-Term Quantum Processors, by Vladyslav Bohun, Maxence Grandadam, and Maciej Koch-Janusz, arXiv, February 2025 (15 pages).

[759] Gate teleportation-assisted routing for quantum algorithms, by Aravind Plathanam Babu, Oskari Kerppo, Andrés Muñoz Moller, Majid Haghparast, and Matti Silveri, arXiv, April 2025 (16 pages).

[760] Improved distributed quantum algorithm for Simon's problem, by Hao Li and Daowen Qiu, arXiv, April 2025 (10 pages).

[761] Exploration of Design Alternatives for Reducing Idle Time in Shor's Algorithm: A Study on Monolithic and Distributed Quantum Systems, by Moritz Schmidt, Abhoy Kole, Leon Wichette, Rolf Drechsler, Frank Kirchner, and Elie Mounzer, arXiv, March 2025 (19 pages).

[762] Distributed quantum algorithm for discrete logarithm problem, by Hao Li and Daowen Qiu, arXiv, April 2025 (21 pages).

[763] Distributed Quantum Neural Networks on Distributed Photonic Quantum Computing, by Kuan-Cheng Chen, Chen-Yu Liu, Yu Shang, Felix Burt, and Kin K. Leung, arXiv, May 2025 (12 pages).

[764] Quantum Communication Advantage for Leader Election and Agreement, by Fabien Dufoulon, Frédéric Magniez, and Gopal Pandurangan, arXiv, February 2025 (33 pages).

[765] Distributed Variational Quantum Algorithm with Many-qubit for Optimization Challenges, by Seongmin Kim and In-Saeng Suh, arXiv, February 2025 (50 pages).

[766] Tensor Network Assisted Distributed Variational Quantum Algorithm for Large Scale Combinatorial Optimization Problem, by Yuhan Huang, Siyuan Jin, Yichi Zhang, Qi Zhao, Jun Qi, and Qiming Shao, arXiv, January 2026 (8 pages).

[767] Distributed Quantum Optimization for Large-Scale Higher-Order Problems with Dense Interactions, by Seongmin Kim, Vincent R. Pascuzzi, Travis S. Humble, Thomas Beck, Sanghyo Hwang, Tengfei Luo, Eungkyu Lee, and In-Saeng Suh, arXiv, April 2026 (46 pages).

[768] Distributed Quantum-Enhanced Optimization: A Topographical Preconditioning Approach for High-Dimensional Search, by Dominik Soós, Marc Paterno, John Stenger, and Nikos Chrisochoides, arXiv, April 2026 (12 pages).

[769] DQAOA-GPT: AI-Accelerated Distributed Quantum Optimization for Combinatorial Problems, by Seongmin Kim, Abhinav Rijal, Yuri Alexeev, Nora Bauer, Martin Roetteler, Mina Yoon, George Siopsis, and In-Saeng Suh, arXiv, July 2026 (7 pages).

[770] Tensor-Network-Based Distributed Quantum Dynamics on Independent Quantum Computers, by Anurag Dwivedi, Melissa C. Revelle, Daniel S. Lobser, Brian K. McFarland, Edward C. Tortorici, Christopher G. Yale, Susan M. Clark, Philip Richerme, and Srinivasan S. Iyengar, arXiv, June 2026 (28 pages).

[771] Towards an Optimally Distributed Quantum Fourier Transform Circuit, by Zachary Vernec, Michael Silver, and Hans-Arno Jacobsen, arXiv, June 2026 (22 pages).

[772] Learning functions of quantum states with distributed architectures, by Marta Gili, Eliana Fiorelli, Ane Blázquez-García, Gian Luca Giorgi, and Roberta Zambrini, Quantum Machine Intelligence, February 2026 (18 pages).

[773] Distributing circuits over heterogeneous, modular quantum computing network architectures, by Pablo et al., August 2024 (32 pages).

[774] Hardware-aware Compilation for Chip-to-Chip Coupler-Connected Modular Quantum Systems, by Zefan Du, Ying Mao, et al., arXiv, May 2025 (10 pages).

[775] Distributed quantum computing with black-box subroutines, by X. Xu, Y.-D. Liu, S. Shi, Y.-J. Wang, and D.-S. Wang, arXiv, May 2025 (16 pages).

[776] Modular Compilation for Quantum Chiplet Architectures, by Mingyoung Jessica Jeng, Nikos Hardavellas, et al., arXiv, April 2025 (13 pages).

[777] Revisiting the Mapping of Quantum Circuits: Entering the Multi-Core Era, by Pau Escofet, Carmen G. Almudéver, et al., arXiv, March 2024 (26 pages).

[778] Assessing the Role of Communication in Scalable Multi-Core Quantum Architectures, by Maurizio Palesi, Enrico Russo, Davide Patti, Giuseppe Ascia, and Vincenzo Catania, arXiv, May 2024 (8 pages).

[779] Towards Distributed Quantum Error Correction for Distributed Quantum Computing, by Shahram Babaie and Chunming Qiao, arXiv, September 2024 (12 pages).

[780] Fault-tolerant interfaces for modular quantum computing on diverse qubit platforms, by Frederik K. Marqversen, Johannes Borregaard, et al., arXiv, October 2025 (18 pages).

[781] Scaling Quantum Computations via Gate Virtualization, by Nathaniel Tornow, Emmanouil Giortamis, and Pramod Bhatotia, arXiv, June 2024 (16 pages).

[782] Constructing a virtual two-qubit gate by sampling single-qubit operations, by Kosuke Mitarai and Keisuke Fujii, February 2021 (15 pages).

[783] Towards Distributed Quantum Computing by Qubit and Gate Graph Partitioning Techniques, by Marc Grau Davis, Joaquin Chung, Dirk Englund, and Rajkumar Kettimuthu, arXiv, October 2023 (7 pages).

[784] Universal distributed blind quantum computing with solid-state qubits, by Yan-Cheng Wei, Mikhail D. Lukin, et al., Science, May 2025 (5 pages) 🔓 (preprint on arXiv).

[785] Network Requirements for Distributed Quantum Computation, by Hugo Jacinto, Élie Gouzien, and Nicolas Sangouard, Physical Review Research, February 2026 (7 pages).

[786] Modular Architectures and Entanglement Schemes for Error-Corrected Distributed Quantum Computation, by Siddhant Singh, Fenglei Gu, Sébastian de Bone, Eduardo Villaseñor, David Elkouss, and Johannes Borregaard, arXiv, August 2024 (34 pages).

[787] Upper Bounds for the Clock Speeds of Fault-Tolerant Distributed Quantum Computation using Satellites to Supply Entangled Photon Pairs, by Hudson Leone, Simon Devitt, et al., arXiv, February 2024 (11 pages).

[788] Assessing Teleportation of Logical Qubits in a Distributed Quantum Architecture under Error Correction, by John Stack, Ming Wang, and Frank Mueller, arXiv, April 2025 (11 pages).

[789] A quantum-logic gate between distant quantum-network modules, by Severin Daiss, Stefan Langenfeld, Stephan Welte, Emanuele Distante, Philip Thomas, Lukas Hartung, Olivier Morin, and Gerhard Rempe, Science, February 2021 🔓 (preprint on arXiv).

[790] Will Quantum Computers Scale Without Inter-Chip Comms? A Structured Design Exploration to the Monolithic vs Distributed Architectures Quest, by Santiago Rodrigo, 2020 (6 pages).

[791] Towards a Distributed Quantum Computing Ecosystem, by Daniele Cuomo, Marcello Caleffi, and Angela Sara Cacciapuoti, arXiv, March 2020 (8 pages).

[792] An operating system for executing applications on quantum network nodes, by C. Delle Donne, Ronald Hanson, Stephanie Wehner, et al., Nature, March 2025.

[793] Qoala: an Application Execution Environment for Quantum Internet Nodes, by Bart van der Vecht, Atak Talay Yücel, Hana Jirovská, and Stephanie Wehner, arXiv, February 2025 (12 pages).

[794] Compilation strategies for quantum network programs using Qoala, by Samuel Oslovich, Bart van der Vecht, and Stephanie Wehner, arXiv, May 2025 (12 pages).

[795] Universal Blind Quantum Computation, by Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, October 2009 (10 pages) 🔓 (preprint on arXiv).

[796] Blind quantum computing can always be made verifiable, by Tomoyuki Morimae, arXiv, March 2018 (5 pages).

[797] Experimental Blind Quantum Computing for a Classical Client, by He-Liang Huang, Barry C. Sanders, Chao-Yang Lu, Jian-Wei Pan, et al., arXiv, July 2017 (5 pages).

[798] Hardware requirements for trapped-ion based verifiable blind quantum computing with a measurement-only client, by Janice van Dam, Tracy E Northup, Stephanie Wehner, et al., arXiv, September 2024 (16 pages).

[799] Complete Self-Testing of a System of Remote Superconducting Qubits, by Simon Storz, Nicolas Sangouard, Andreas Wallraff, et al., arXiv, August 2024 (17 pages).

[800] Designing Fault-Tolerant Blind Quantum Computation, by Gefen Baranes, Mikhail D. Lukin, et al., arXiv, May 2025 (12 pages).

[801] Verifiable blind quantum computing: Comparative analysis and design considerations for client architectures, by Janice van Dam, Jeroen Grimbergen, and Stephanie D.C. Wehner, arXiv, July 2026 (27 pages).

[802] Blind Quantum Computation on a Modular Superconducting Processor, by Yongxin Song, Johannes Knörzer, Kieran Dalton, Andreas Wallraff, and Jean-Claude Besse, arXiv, May 2026 (16 pages).

[803] Development of Quantum InterConnects for Next-Generation Information Technologies, by David Awschalom, Ronald Walsworth, Andrew M. Weiner, Zheshen Zhang, et al., arXiv, January 2020 (31 pages).

[804] Optimizing Inter-chip Coupler Link Placement for Modular and Chiplet Quantum Systems, by Zefan Du, Ying Mao, et al., arXiv, September 2025 (13 pages).

[805] Modeling Short-Range Microwave Networks to Scale Superconducting Quantum Computation, by Nicholas LaRacuente, Kaitlin N. Smith, Poolad Imany, Kevin L. Silverman, and Frederic T. Chong, arXiv, December 2024 (33 pages).

[806] Mechanically-intermixed indium superconducting connections for microwave quantum interconnects, by Yves Martin, Jason S. Orcutt, et al., arXiv, September 2024 (6 pages).

[807] Low-loss interconnects for modular superconducting quantum processors, by Jingjing Niu, Dapeng Yu, et al., arXiv, February 2023 (28 pages).

[808] Quantum Transduction: Enabling Quantum Networking, by Marcello Caleffi, Laura d'Avossa, Xu Han, and Angela Sara Cacciapuoti, arXiv, May 2025 (17 pages).

[809] Robust quantum communication through lossy microwave links, by James D. Teoh, Nathanael Cottet, Patrick Winkel, Luke D. Burkhart, Luigi Frunzio, and Robert J. Schoelkopf, arXiv, September 2025 (37 pages).

[810] Deterministic multi-qubit entanglement in a quantum network, by Youpeng Zhong, Hung-Shen Chang, Audrey Bienfait, Étienne Dumur, Ming-Han Chou, Christopher R. Conner, Joel Grebel, Rhys G. Povey, Haoxiong Yan, David I. Schuster, and Andrew N. Cleland, Nature, February 2021 🔓 (preprint on arXiv).

[811] A high-efficiency elementary network of interchangeable superconducting qubit devices, by Michael Mollenhauer, Abdullah Irfan, Xi Cao, Supriya Mandal, and Wolfgang Pfaff, Nature Electronics, June 2025 🔓 (preprint on arXiv).

[812] Microwave Quantum Link between Superconducting Circuits Housed in Spatially Separated Cryogenic Systems, by Paul Magnard, Alexandre Blais, Andreas Wallraff, et al., Physical Review Letters, December 2020 (13 pages) 🔓 (preprint on arXiv).

[813] Loophole-free Bell inequality violation with superconducting circuits, by Simon Storz, Alexandre Blais, Andreas Wallraff, et al., Nature, May 2023.

[814] A Modular Cryogenic Link for Microwave Quantum Communication Over Distances of Tens of Meters, by Josua D. Schär, Simon Storz, Paul Magnard, Philipp Kurpiers, Janis Lütolf, Melvin Gehrig, Jean-Claude Besse, Anatoly Kulikov, and Andreas Wallraff, arXiv, April 2026 (24 pages).

[815] Cryogenic microwave link for quantum local area networks, by W. K. Yam, R. Gross, K. G. Fedorov, et al., npj Quantum Information, May 2025 (10 pages).

[816] Bidirectional Multiphoton Communication between Remote Superconducting Nodes, by Joel Grebel et al., Physical Review Letters, January 2024 🔓 (preprint on arXiv).

[817] Deterministic quantum state and gate teleportation between distant superconducting chips, by Jiawei Qiu, Yang Liu, Ling Hu, Yukai Wu, Jingjing Niu, Libo Zhang, Wenhui Huang, Yuanzhen Chen, Jian Li, Song Liu, Youpeng Zhong, Luming Duan, and Dapeng Yu, Science Bulletin, February 2025 (8 pages) 🔓 (preprint on arXiv).

[818] Route-Forcing: Scalable Quantum Circuit Mapping for Scalable Quantum Computing Architectures, by Pau Escofet, Alejandro Gonzalvo, Eduard Alarcón, Carmen G. Almudéver, and Sergi Abadal, arXiv, July 2024 (12 pages).

[819] Experimental quantum teleportation of propagating microwaves, by Kirill G. Fedorov, Rudolf Gross, Frank Deppe, et al., Science, December 2021.

[820] High-contrast interaction between remote superconducting qubits mediated by multimode cable coupling, by Jiajian Zhang, Ji Chu, Jingjing Niu, Youpeng Zhong, and Dapeng Yu, arXiv, May 2025 (13 pages).

[821] Realization of High-Fidelity Perfect Entanglers between Remote Superconducting Quantum Processors, by Juan Song, Shuang Yang, Pei Liu, Hui-Li Zhang, Guang-Ming Xue, Zhen-Yu Mi, Wen-Gang Zhang, Fei Yan, Yi-Rong Jin, and Hai-Feng Yu, Physical Review Letters, July 2025.

[822] A high-efficiency plug-and-play superconducting qubit network, by Michael Mollenhauer, Abdullah Irfan, Xi Cao, Supriya Mandal, and Wolfgang Pfaff, arXiv, July 2024 (15 pages).

[823] Error-Detected State Transfer and Entanglement in a Superconducting Quantum Network, by Luke D. Burkhart, PRX Quantum, August 2021.

[824] Continuous wideband microwave-to-optical converter based on room-temperature Rydberg atoms, by Sebastian Borówka, Uliana Pylypenko, Mateusz Mazelanik, and Michał Parniak, Nature Photonics, October 2023.

[825] A superconducting on-chip microwave cavity for tunable hybrid systems with optically trapped Rydberg atoms, by Benedikt Wilde, Daniel Bothner, et al., arXiv, March 2025 (19 pages).

[826] Scalable microwave-to-optical transducers at single photon level with spins, by Tian Xie, Rikuto Fukumori, Jiahui Li, and Andrei Faraon, arXiv, July 2024 (23 pages).

[827] Enhancing Microwave-Optical Bell Pairs Generation for Quantum Transduction Using Kerr Nonlinearity, by Fangxin Li, Ming Yuan, Zhaoyou Wang, Changchun Zhong, and Liang Jiang, arXiv, May 2025 (24 pages).

[828] Optomechanical ring resonator for efficient microwave-optical frequency conversion, by I-Tung Chen, Bingzhao Li, Seokhyeong Lee, Srivatsa Chakravarthi, Kai-Mei Fu, and Mo Li, arXiv, November 2023 (11 pages).

[829] Low Noise Opto-Electro-Mechanical Modulator for RF-to-Optical Transduction in Quantum Communications, by Michele Bonaldi, David Vitali, et al., arXiv, July 2023 (14 pages).

[830] Quantum-enabled continuous microwave-to-optics frequency conversion, by Han Zhao, William David Chen, Abhishek Kejriwal, and Mohammad Mirhosseini, arXiv, June 2024 (23 pages).

[831] Quantum-enabled microwave-to-optical transduction via silicon nanomechanics, by Han Zhao, William David Chen, Abhishek Kejriwal, and Mohammad Mirhosseini, Nature Nanotechnology, March 2025 🔓 (preprint on arXiv).

[832] Quantum entanglement between optical and microwave photonic qubits, by Srujan Meesala, Liang Jiang, Oskar Painter, et al., arXiv, December 2023 (14 pages).

[833] Microwave-Optical Entanglement from Pulse-pumped Electro-optomechanics, by Changchun Zhong, Fangxin Li, Srujan Meesala, Steven Wood, David Lake, Oskar Painter, and Liang Jiang, arXiv, July 2024 (10 pages).

[834] High-Efficiency Low-Noise Optomechanical Crystal Photon-Phonon Transducers, by Sameer Sonar, Utku Hatipoglu, Srujan Meesala, David Lake, Hengjiang Ren, and Oskar Painter, arXiv, June 2024 (18 pages).

[835] Long-range optomechanical interactions in SiN membrane arrays, by Xiong Yao, Matthijs H. J. de Jong, Jie Li, and Simon Gröblacher, arXiv, August 2024 (13 pages).

[836] High-throughput electro-optic upconversion and downconversion with few-photon added noise, by M. D. Urmey, S. Dickson, K. Adachi, S. Mittal, L. G. Talamo, A. Kyle, N. E. Frattini, S.-X. Lin, K. W. Lehnert, and C. A. Regal, arXiv, July 2025 (11 pages).

[837] Two-dimensional optomechanical crystal resonator in gallium arsenide, by Rhys G. Povey, Andrew N. Cleland, et al., arXiv, July 2023 (13 pages).

[838] Principles for Optimizing Quantum Transduction in Piezo-Optomechanical Systems, by James Schneeloch, Erin Sheridan, A. Matthew Smith, Christopher C. Tison, Daniel L. Campbell, Matthew D. LaHaye, Michael L. Fanto, and Paul M. Alsing, arXiv, January 2025 (29 pages).

[839] A two-dimensional piezo-optomechanical transducer, by Tian Xie, Nelson Ooi, Linus Woodard, Sultan Malik, Felix Mayor, Oliver A. Hitchcock, André G. Primo, Wentao Jiang, Samuel Gyger, and Amir H. Safavi-Naeini, arXiv, July 2026 (19 pages).

[840] Optics-microwave entanglement and state teleportation mediated by a cavity magnomechanical system, by F. Engelhardt, A. V. Bondarenko, A. Metelmann, Ya. M. Blanter, S. Viola Kusminskiy, and V. A. S. V. Bittencourt, arXiv, June 2026 (18 pages).

[841] Entangling microwaves with optical light, by Rishabh Sahu, Liu Qiu, William Hease, Georg Arnold, Yuri Minoguchi, Peter Rabl, and Johannes M. Fink, arXiv, January 2023 (6 pages).

[842] Intra-band entanglement-assisted cavity electro-optic quantum transducer, by Yu-Bo Hou, Rui-Zhe You, Di-Jia Zhang, Pengbo Li, and Changchun Zhong, arXiv, March 2025 (9 pages).

[843] Microwave-to-Optical Quantum Transduction via Defect-Mediated Scattering in Diamond, by Kyosuke Goto, Hodaka Kurokawa, Hideo Kosaka, and Kazuki Koshino, arXiv, May 2026 (6 pages).

[844] Pump Free Microwave-Optical Quantum Transduction, by Fangxin Li, Jaesung Heo, Zhaoyou Wang, Andrew P. Higginbotham, Alexander A. High, and Liang Jiang, arXiv, December 2025 (21 pages).

[845] A frequency-agile microwave-optical interface for superconducting qubits, by Yufeng Wu, Yiyu Zhou, Haoqi Zhao, Danqing Wang, Matthew D. LaHaye, Daniel L. Campbell, and Hong X. Tang, arXiv, February 2026 (16 pages).

[846] Error-Detected State Transfer and Entanglement in a Superconducting Quantum Network, by Luke D. Burkhart et al., PRX Quantum, August 2021.

[847] Robust microwave-optical photon conversion using cavity modes strongly hybridized with a color center ensemble, by M. Khalifa, P. S. Kirwin, Jeff F. Young, and J. Salfi, npj Quantum Information, June 2025.

[848] Stable, bidirectional electro-optic transduction in thin film lithium tantalate, by Christopher J. Axline, Stephan Gamper, Phoebe M. Tengdin, Moritz Businger, Guilhem Alma, Marina A. Roquet, Nicola Brusadin, Robin Giroud, and Luis G. Villanueva, arXiv, June 2026 (16 pages).

[849] All-Dielectric Resonant Cavity Electro-Optic Transduction Between Microwave and Telecom, by Mihir Khanna, Yang Hu, and Thomas P. Purdy, arXiv, January 2026 (10 pages).

[850] Approaching optimal microwave-acoustic transduction on lithium niobate using SQUID arrays, by A. Hugot, Q. Greffe, G. Julie, E. Eyraud, F. Balestro, and J. J. Viennot, arXiv, January 2025 (14 pages).

[851] Quantum-memory-assisted on-demand microwave-optical transduction, by Hai-Tao Tu, Kai-Yu Liao, Si-Yuan Qiu, Xiao-Hong Liu, Yi-Qi Guo, Zheng-Qi Du, Yang Xu, Xin-Ding Zhang, Hui Yan, and Shi-Liang Zhu, arXiv, September 2025 (17 pages).

[852] Memory-assisted multimode microwave-to-optical transduction, by Ujjwal Gautam, Nasser Gohari Kamel, Sourabh Kumar, and Daniel Oblak, arXiv, May 2026 (22 pages).

[853] A high-performance quantum memory for quantum interconnects, by H.-X Luo, C. Li, J.-L. Ren, Y. Yuan, Y.-L. Wen, J.-F. Li, Y.-F. Wang, S.-C. Zhang, H. Yan, and S.-L. Zhu, arXiv, March 2026 (7 pages).

[854] Fast Quantum Interconnects via Neutral Atom Ensembles, by Sina Zeytinoglu, Wenchao Xu, and Thomas Pohl, arXiv, August 2026 (5 pages).

[855] A kilometer photonic link connecting superconducting circuits in two dilution refrigerators, by Yiyu Zhou, Hong X. Tang, et al., arXiv, August 2025 (15 pages).

[856] Perspectives on quantum transduction, by Nikolai Lauk, Mark Saffman, Maria Spiropulu, Christoph Simon, et al., Quantum Science and Technology, March 2020 (16 pages).

[857] High-Performance Quantum Transduction with Correlated Noise, by Yu-Bo Hou, Xiaoan Ai, Pengbo Li, and Changchun Zhong, arXiv, August 2026 (12 pages).

[858] Pump-Free Microwave-Optical Bell Pair Generation for Teleportation-Based Quantum Transduction, by Fangxin Li, Jaesung Heo, Zhaoyou Wang, Benjamin Pingault, Xingyu Gao, Tengyang Ruan, Anjun Chu, David D. Awschalom, Andrew N. Cleland, Andrew P. Higginbotham, Alexander A. High, and Liang Jiang, arXiv, September 2026 (29 pages).

[859] Proposal for Superconducting Quantum Networks Using Multi-Octave Transduction to Lower Frequencies, by Takuma Makihara, Wentao Jiang, and Amir H. Safavi-Naeini, arXiv, July 2024 (8 pages).

[860] Dynamically Reconfigurable Photon Exchange in a Superconducting Quantum Processor, by Brian Marinelli, Irfan Siddiqi, et al., arXiv, March 2023 (9 pages).

[861] Realizing all-to-all couplings among detachable quantum modules using a microwave quantum state router, by Chao Zhou, Michael Hatridge, et al., npj Quantum Information, June 2023.

[862] Cryogenic RF-to-Microwave Transducer based on a DC-Biased Electromechanical System, by Himanshu Patange, Kyrylo Gerashchenko, Rémi Rousseau, Paul Manset, Léo Balembois, Thibault Capelle, Samuel Deléglise, and Thibaut Jacqmin, arXiv, August 2025 (14 pages).

[863] Continuous wideband microwave-to-optical converter based on room-temperature Rydberg atoms, by Sebastian Borówka, Uliana Pylypenko, Mateusz Mazelanik, and Michał Parniak, arXiv, October 2023 (20 pages).

[864] Quantum-enabled millimetre wave to optical transduction using neutral atoms, by Aishwarya Kumar, David I. Schuster, Jonathan Simon, et al., Nature, March 2023 🔓 (preprint on arXiv).

[865] Dielectric microwave resonator with large optical apertures for spin-based quantum devices, by Tatsuki Hamamoto, Amit Bhunia, Rupak Kumar Bhattacharya, Hiroki Takahashi, and Yuimaru Kubo, arXiv, March 2024 (6 pages).

[866] Coherent Interaction of a Few-Electron Quantum Dot with a Terahertz Optical Resonator, by Kazuyuki Kuroyama,

Physical Review Letters, February 2024 🔓 (preprint on arXiv).

[867] Remote Entangling Gates for Spin Qubits in Quantum Dots using a Charge-Sensitive Superconducting Coupler, by Harry Hanlim Kang, Ilan T. Rosen, Max Hays, Jeffrey A. Grover, and William D. Oliver, arXiv, February 2025 (25 pages).

[868] Quantum Capacities of Bosonic Channels, by Michael M. Wolf, David Pérez-García, and Geza Giedke, Physical Review Letters, March 2007 🔓 (preprint on arXiv).

[869] Proposal for Heralded Generation and Detection of Entangled Microwave–Optical-Photon Pairs, by Changchun Zhong, Zhixin Wang, Changling Zou, Mengzhen Zhang, Xu Han, Wei Fu, Mingrui Xu, S. Shankar, Michel H. Devoret, Hong X. Tang, and Liang Jiang, Physical Review Letters, January 2020 🔓 (preprint on arXiv).

[870] Long-Range Microwave Mediated Interactions Between Electron Spins, by F. Borjans, X. G. Croot, X. Mi, M. J. Gullans, and J. R. Petta, arXiv, May 2019 (6 pages).

[871] Strong coupling between a photon and a hole spin in silicon, by Cecile X. Yu, Simon Zihlmann, Jose C. Abadillo-Uriel, Vincent P. Michal, Nils Rambal, Heimanu Niebojewski, Thomas Bedecarrats, Maud Vinet, Etienne Dumur, Michele Filippone, Benoit Bertrand, Silvano De Franceschi, Yann-Michel Niquet, and Romain Maurand, Nature Nanotechnology, March 2023 (6 pages) 🔓 (preprint on HAL).

[872] Coherent Spin-Spin Coupling Mediated by Virtual Microwave Photons, by Patrick Harvey-Collard, Physical Review X, May 2022.

[873] Large-bandwidth Transduction Between an Optical Single Quantum Dot Molecule and a Superconducting Resonator, by Yuta Tsuchimoto, PRX Quantum, September 2022.

[874] Coherent control of a superconducting qubit using light, by Hana K. Warner, Marko Loncar, et al., arXiv, January 2025 (28 pages).

[875] Low noise quantum frequency conversion of photons from a trapped barium ion to the telecom O-band, by Uday Saha, James D. Siverns, John Hannegan, Qudsia Quraishi, and Edo Waks, arXiv, May 2023 (16 pages).

[876] Quantum frequency conversion of memory-compatible single photons from 606 nm to the telecom C-band, by Nicolas Maring, Dario Lago-Rivera, Andreas Lenhard, Georg Heinze, and Hugues de Riedmatten, Optica, March 2018 (7 pages).

[877] Low-noise quantum frequency conversion in a monolithic cavity with bulk periodically poled potassium titanyl phosphate, by Felix Mann, Helen M. Chrzanowski, Felipe Gewers, Marlon Placke, and Sven Ramelow, arXiv, October 2023 (7 pages).

[878] High-performance quantum frequency conversion using programmable unpoled nanophotonic waveguides, by Jierui Hu, Kejie Fang, et al., arXiv, October 2025 (18 pages).

[879] Realization of a multi-node quantum network of remote solid-state qubits, by Matteo Pompili, Ronald Hanson, et al., arXiv, February 2021 (9 pages).

[880] Tutorial: Remote entanglement protocols for stationary qubits with photonic interfaces, by Hans K.C. Beukers, Ronald Hanson, Johannes Borregaard, et al., arXiv, October 2023 (27 pages).

[881] Quantum networks with neutral atom processing nodes, by Jacob P. Covey, Harald Weinfurter, and Hannes Bernien, arXiv, April 2023 (10 pages).

[882] A quantum-network register assembled with optical tweezers in an optical cavity, by Lukas Hartung, Matthias Seubert, Stephan Welte, Emanuele Distante, and Gerhard Rempe, Science, July 2024 🔓 (preprint on arXiv).

[883] Efficient entanglement of three remote single-atom quantum-network nodes, by Matthias Seubert, Leonardo Ruscio, Tobias Frank, Philip Thomas, Maya Büki, Gianvito Chiarella, Pau Farrera, Olivier Morin, and Gerhard Rempe, arXiv, June 2026 (9 pages).

[884] Scalable Networking of Neutral-Atom Qubits: Nanofiber-Based Approach for Multiprocessor Fault-Tolerant Quantum Computer, by Shinichi Sunami, Shiro Tamiya, Ryotaro Inoue, Hayata Yamasaki, and Akihisa Goban, arXiv, July 2024 (22 pages).

[885] Waveguide-array-based multiplexed photonic interface for atom array, by Yuya Maeda, Toshiki Kobayashi, Takuma Ueno, Kentaro Shibata, Shinichi Takenaka, Kazuki Ito, Yuma Fujiwara, Shigehito Miki, Hirotaka Terai, Tsuyoshi Kodama, Hideki Shimoi, Rikizo Ikuta, Makoto Yamashita, Shuta Nakajima, and Takashi Yamamoto, arXiv, December 2025 (9 pages).

[886] An Optical Interconnect for Modular Quantum Computers, by Daisuke Sakuma, Shota Nagayama, et al., arXiv, December 2024 (14 pages).

[887] Fault-tolerant connection of error-corrected qubits with noisy links, by Joshua Ramette, Josiah Sinclair, Nikolas P. Breuckmann, and Vladan Vuletić, npj Quantum Information, June 2024.

[888] Fault-tolerant optical interconnects for neutral-atom arrays, by Josiah Sinclair, Mikhail Lukin, Vladan Vuletić, et al., arXiv, August 2024 (11 pages).

[889] High finesse buckled microcavitiesHigh finesse buckled microcavities, by Brandon Grinkemeyer, Vladan Vuletić, Mikhail D. Lukin, et al., Optica, February 2026 (6 pages).

[890] High-rate and high-fidelity modular interconnects between neutral atom quantum processors, by Yiyi Li and Jeff Thompson, arXiv, January 2024 (13 pages).

[891] Fast Photon-Mediated Entanglement of Continuously Cooled Trapped Ions for Quantum Networking, by Jameson O'Reilly et al., Physical Review Letters, August 2024 🔓 (preprint on osti.gov).

[892] High-fidelity remote entanglement of trapped atoms mediated by time-bin photons, by Sagnik Saha, Mikhail Shalaev, Jameson O'Reilly, Isabella Goetting, George Toh, Ashish Kalakuntla, Yichao Yu, and Christopher Monroe, arXiv, June 2024 (10 pages).

[893] Generation of multipartite photonic entanglement using a trapped-ion quantum processing node, by Marco Canteri, James Bate, Ida Mishra, Nicolai Friis, Victor Krutyanskiy, and Benjamin P. Lanyon, arXiv, October 2025 (5 pages).

[894] SDQC: Distributed Quantum Computing Architecture Utilizing Entangled Ion Qubit Shuttling, by Seunghyun Baek, Seok-Hyung Lee, Dongmoon Min, and Junki Kim, arXiv, December 2025 (31 pages).

[895] Advantage in distributed quantum computing with slow interconnects, by Evan E Dobbs, Nicolas Delfosse, and Aharon Brodutch, arXiv, December 2025 (8 pages).

[896] Large Scale Modular Quantum Computer Architecture with Atomic Memory and Photonic Interconnects, by C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim, arXiv, July 2013 (16 pages).

[897] A high-fidelity quantum matter-link between ion-trap microchip modules, by M. Akhtar, Winfried K. Hensinger, et al., Nature Communications, February 2023.

[898] Temporally multiplexed ion-photon quantum interface via fast ion-chain transport, by Bingran You, Qiming Wu, David Miron, Wenjun Ke, Inder Monga, Erhan Saglamyurek, and Hartmut Haeffner, arXiv, May 2024 (6 pages).

[899] Entanglement of trapped-ion qubits separated by 230 meters, by V. Krutyanskiy, Tracy E. Northup, et al., arXiv, August 2022 (22 pages).

[900] Temporally Multimode Ion-Ion Entanglement over 1.2 Kilometer Fibers, by Z.-B. Cui, L.-M. Duan, et al., Physical Review Letters, July 2026 🔓 (preprint on arXiv).

[901] Room-temperature amplified transduction of infrared to visible photons, by Gibeom Son, Songky Moon, Seunghoon Oh, Junseo Ha, and Kyungwon An, arXiv, November 2024 (8 pages).

[902] Chip-to-chip quantum teleportation and multi-photon entanglement in silicon, by Daniel Llewellyn, Yunhong Ding, Imad I. Faruque, Stefano Paesani, Davide Bacco, Raffaele Santagati, Yan-Jun Qian, Yan Li, Yun-Feng Xiao, Marcus Huber, Mehul Malik, Gary F. Sinclair, Xiaoqi Zhou, Karsten Rottwitt, Jeremy L. O'Brien, John G. Rarity, Qihuang Gong, Leif K. Oxenlowe, Jianwei Wang, and Mark G. Thompson, Nature Physics, February 2020 (6 pages) 🔓 (preprint on research-information.bris.ac.uk).

[903] Anisotropic rare-earth spin ensemble strongly coupled to a superconducting resonator, by S. Probst, H. Rotzinger, S. Wünsch, P. Jung, M. Jerger, M. Siegel, A. V. Ustinov, and P. A. Bushev, Physical Review Letters, April 2013 🔓 (preprint on arXiv).

[904] Robust multi-qubit quantum network node with integrated error detection, by Pieter-Jan Stas, Mikhail D. Lukin, et al., arXiv, July 2022 (24 pages).

[905] A scalable photonic quantum interconnect platform, by Daniel Riedel, Bartholomeus Machielse, et al., Physical Review X, March 2026 (16 pages).

[906] Teleportation Systems Toward a Quantum Internet, by Raju Valivarthi et al., PRX Quantum, December 2020.

[907] Photonic Networking of Quantum Memories in High-Dimensions, by Mikhail Shalaev, Christopher Monroe, et al., arXiv, May 2025 (15 pages).

[908] A quantum-bit encoding converter, by Tom Darras, Beate Elisabeth Asenbeck, Giovanni Guccione, Adrien Cavaillès, Hanna Le Jeannic, and Julien Laurat, Nature Photonics, February 2023 (6 pages) 🔓 (preprint on HAL).

[909] Demonstration of deterministic SWAP gate between superconducting and frequency-encoded microwave-photon qubits, by Kazuki Koshino and Kunihiro Inomata, arXiv, February 2023 (14 pages).

[910] Photon routing in disordered chiral waveguide QED ladders: Interplay between photonic localization and collective atomic effects, by Nishan Amgain and Imran M. Mirza, arXiv, June 2024 (10 pages).

[911] Physical Layer Aspects of Quantum Communications: A Survey, by Seid Koudia, Leonardo Oleynik, Mert Bayraktar, Junaid ur Rehman, and Symeon Chatzinotas, arXiv, July 2024 (35 pages).

[912] Crosstalk-resilient quantum MIMO for scalable quantum communications, by Seid Koudia and Symeon Chatzinotas, npj Quantum Information, October 2025.

[913] A flexible quantum data bus, by Julia Freund, Alexander Pirker, and Wolfgang Dür, arXiv, April 2024 (11 pages).

[914] Multicore Quantum Computing, by Hamza Jnane, Brennan Undseth, Zhenyu Cai, Simon C Benjamin, and Bálint Koczor, arXiv, November 2022 (26 pages).

[915] Quanten-Shuttle zum Quantenprozessor "Made in Germany" gestartet, by FZJulich, February 2021.

[916] Quantum communication with itinerant surface acoustic wave phonons, by É. Dumur, Andrew N. Cleland, et al., npj Quantum Information, December 2021.

[917] CloudQC: A Network-aware Framework for Multi-tenant Distributed Quantum Computing, by Ruilin Zhou, Yuhang Gan, Yi Liu, and Chen Qian, arXiv, April 2025 (11 pages).

[918] Review of Distributed Quantum Computing: From single QPU to High Performance Quantum Computing, by David Barral et al., Computer Science Review, 2025.

[919] Quantum Data Centers: Why Entanglement Changes Everything, by Angela Sara Cacciapuoti, Claudio Pellitteri, Jessica Illiano, Laura d'Avossa, Francesco Mazza, Siyi Chen, and Marcello Caleffi, arXiv, June 2025 (17 pages).

[920] No quantum advantage without classical communication: fundamental limitations of quantum networks, by Justus Neumann, Tulja Varun Kondra, Kiara Hansenne, Lisa T. Weinbrenner, Hermann Kampermann, Otfried Gühne, Dagmar Bruß, and Nikolai Wyderka, arXiv, March 2025 (20 pages).

[921] Protocol Library, by Quantum Protocol Zoo, 2026.

[922] Towards a Unified Quantum Protocol Framework: Classification, Implementation, and Use Cases, by Shraddha Singh, Harold Ollivier, Elham Kashefi, et al., arXiv, December 2023 (12 pages).

[923] Benchmarking of Quantum Protocols, by Chin-Te Liao, Sima Bahrani, Francisco Ferreira da Silva, and Elham Kashefi, arXiv, July 2022 (16 pages).

[924] Adaptive bandwidth management for entanglement distribution in quantum networks, by Navin B. Lingaraju, Joseph M. Lukens, et al., arXiv, October 2020 (5 pages).

[925] Telecom-heralded entanglement between remote multimode solid-state quantum memories, by Dario Lago-Rivera, Samuele Grandi, Hugues de Riedmatten, et al., Nature, June 2021.

[926] Realistic Simulation of Quantum Repeater with Encoding and Classical Error Correction, by Sagar Patange, Caitao Zhan, Bikun Li, Joaquin Chung, Allen Zang, Liang Jiang, and Rajkumar Kettimuthu, arXiv, August 2026 (11 pages).

[927] Gate-Based Microwave Quantum Repeater Via Grid-State Encoding, by Hany Khalifa and Matti Silveri, arXiv, July 2026 (15 pages).

[928] Quantum Routing for Emerging Quantum Networks, by Wenbo Shi and Robert Malaney, arXiv, November 2022 (6 pages).

[929] A Quantum Router Architecture for High-Fidelity Entanglement Flows in Quantum Networks, by Yuan Lee, Eric Bersin, Axel Dahlberg, Stephanie Wehner, and Dirk Englund, arXiv, October 2022 (10 pages).

[930] Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels, by Marcello Caleffi and Angela Sara Cacciapuoti, arXiv, July 2019 (14 pages).

[931] Quantum router of silicon-vacancy centers via a diamond waveguide, by Wen-Jie Zhang, Xi Yan, and Jun-Hong An, arXiv, September 2025 (10 pages).

[932] Optical Quantum Memory and its Applications in Quantum Communication Systems, by Lijun Ma, 2020 (13 pages).

[933] Towards real-world quantum networks: a review, by Shi-Hai Wei, Qiang Zhou, et al., arXiv, January 2022 (71 pages).

[934] Parallel QEC Decoding Applied to Distributed Quantum Computing, by Gabriele Incardona, Davide Ferrari, and Michele Amoretti, arXiv, July 2026 (8 pages).

[935] Networked Realization of Quantum LDPC Codes, by Swayangprabha Shaw and Narayanan Rengaswamy, arXiv, April 2026 (9 pages).

[936] Quantum teleportation of physical qubits into logical code spaces, by Yi-Han Luo et al., July 2021 (5 pages).

[937] Optimized noise-resilient surface code teleportation interfaces, by Mohamed A. Shalby, Renyu Wang, Denis Sedov, and Leonid P. Pryadko, arXiv, March 2025 (7 pages).

[938] Distributed fault-tolerant quantum memories over a 2xL array of qubit modules, by Edwin Tham, Min Ye, Ilia Khait, John Gamble, and Nicolas Delfosse, arXiv, August 2025 (9 pages).

[939] Distributed Realization of Color Codes for Quantum Error Correction, by Nitish Kumar Chandra, David Tipper, Reza Nejabati, Eneet Kaur, and Kaushik P. Seshadreesan, arXiv, May 2025 (11 pages).

[940] Distributed Quantum Error Correction with Permutation-Invariant Approximate Codes, by Connor Clayton and Bruno Avritzer, arXiv, September 2025 (16 pages).

[941] Fault-tolerant distributed quantum computing with a single nucleus per node, by Yotam Vaknin, Shoham Jacoby, Roi Nevo, Aleksander Kubica, and Alex Retzker, arXiv, July 2026 (17 pages).

[942] Error Correction in a Distributed Quantum Computer, by E. M. Ainley, A. Agrawal, T. Araki, A. R. Martínez, D. Main, E. Malinowski, J. A. Blackmore, S. Chen, P. Drmota, M. Mallweger, D. P. Nadlinger, R. Srinivas, S. C. Benjamin,

G. Araneda, and D. M. Lucas, arXiv, September 2026 (11 pages).

[943] Optimized compiler for Distributed Quantum Computing, by Daniele Cuomo, Angela Sara Cacciapuoti, et al., arXiv, December 2021 (15 pages).

[944] Distributed Shor's algorithm, by Ligang Xiao, Daowen Qiu, Le Luo, and Paulo Mateus, arXiv, July 2022 (15 pages).

[945] Mapping quantum algorithms to multi-core quantum computing architectures, by Anabel Ovide, Carmen G. Almudever, et al., arXiv, March 2023 (5 pages).

[946] Mapping quantum circuits to modular architectures with QUBO, by Medina Bandic, Sebastian Feld, et al., arXiv, May 2023 (12 pages).

[947] A Modular Quantum Compilation Framework for Distributed Quantum Computing, by Davide Ferrari, Stefano Carretta, and Michele Amoretti, arXiv, May 2023 (13 pages).

[948] Software for Massively Parallel Quantum Computing, by Thien Nguyen, Daanish Arya, Marcus Doherty, Nils Herrmann, Johannes Kuhlmann, Florian Preis, Pat Scott, and Simon Yin, arXiv, December 2022 (21 pages).

[949] D-NISQ: A reference model for Distributed Noisy Intermediate-Scale Quantum computers, by Giovanni Acampora et al., January 2023 🔒.

[950] Optimizing Compilation for Distributed Quantum Computing via Clustering and Annealing, by Ruilin Zhou, Jinglei Cheng, Yuhang Gan, Junyu Liu, and Chen Qian, arXiv, August 2025 (7 pages).

[951] Quantum Circuit Optimization for the Fault-Tolerance Era: Do We Have to Start from Scratch?, by Tobias Forster, Nils Quetschlich, and Robert Wille, arXiv, September 2025 (7 pages).

[952] Improving Hardware Requirements for Fault-Tolerant Quantum Computing by Optimizing Error Budget Distributions, by Tobias Forster, Nils Quetschlich, Mathias Soeken, and Robert Wille, arXiv, September 2025 (7 pages).

[953] QNPU: Quantum Network Processor Unit for Quantum Supercomputers, by Peiyi Li, Ang Li, et al., arXiv, September 2025 (16 pages).

[954] Efficient Gate Reordering for Distributed Quantum Compiling in Data Centers, by Riccardo Mengoni, Walter Nadalin, Mathys Rennela, Jimmy Rotureau, Tom Darras, Julien Laurat, Eleni Diamanti, and Ioannis Lavdas, arXiv, July 2025 (11 pages).

[955] Joint Optimization of Qubit Leasing and Quantum Circuit Distribution, by Anoushka Dey and Gaurav S. Kasbekar, arXiv, August 2026 (23 pages).

[956] Quantum circuit partition as a maze: emerging percolation transition via path finding, by P. Zentilini, M. Guatto, F. Preti, D. Arya, F. A. Cárdenas-López, F. Motzoi, and E. Prati, arXiv, June 2026 (16 pages).

[957] A Scalable Distributed Quantum Optimization Framework via Factor Graph Paradigm, by Yuwen Huang, Xiaojun Lin, Bin Luo, and John C.S. Lui, arXiv, March 2026 (72 pages).

[958] Parallelizing Program Execution on Distributed Quantum Systems via Compiler/Hardware Co-Design, by Folkert de Ronde, Alexander Knapen, Stephan Wong, and Sebastian Feld, arXiv, November 2025 (18 pages).

[959] Optimized Compilation for Distributed Quantum Computing, by Michele Bandini, Davide Ferrari, Stefano Carretta, and Michele Amoretti, arXiv, February 2026 (13 pages).

[960] Quantum Hamlets: Distributed Compilation of Large Algorithmic Graph States, by Anthony Micciche, Naphan Benchasattabuse, Andrew McGregor, Michal Hajdušek, Rodney Van Meter, and Stefan Krastanov, arXiv, May 2026 (14 pages).

[961] Chipmunq: A Fault-Tolerant Compiler for Chiplet Quantum Architectures, by Peter Wegmann, Aleksandra Świerkowska, Emmanouil Giortamis, and Pramod Bhatotia, arXiv, March 2026 (14 pages).

[962] Logical-to-Physical Compilation for Reducing Depth in Distributed Quantum Systems, by Folkert de Ronde, Stephan Wong, and Sebastian Feld, arXiv, March 2026 (9 pages).

[963] A Framework for Quantum Data Center Emulation Using Digital Quantum Computers, by Seyed Navid Elyasi, Seyed Morteza Ahmadian, Paolo Monti, Jun Li, and Rui Lin, arXiv, September 2025 (10 pages).

[964] CUNQA: a Distributed Quantum Computing emulator for HPC, by Jorge Vázquez-Pérez, Tomás F. Pena, et al., arXiv, November 2025 (21 pages).

[965] An End-to-End Distributed Quantum Circuit Simulator, by Sen Zhang, Weiwen Jiang, et al., arXiv, November 2025 (5 pages).

[966] Benchmarking Distributed Quantum Computing Emulators, by Guillermo Díaz-Camacho, Andrés Gómez, et al., arXiv, December 2025 (27 pages).

[967] Simulating Circuit Layout for Distributed Quantum Computing, by Sen Zhang, Yipie Liu, Brian Mark, Weiwen Jiang, Zebo Yang, and Lei Yang, arXiv, December 2025 (22 pages).

[968] A Resource Estimation Model for the Hardware-Software Co-Design of Distributed Quantum Architectures, by Raymond P. H. Wu, Chathurika Ranaweera, Sutharshan Rajasegarar, Ria Rushin Joseph, Jinho Choi, and Seng W. Loke, arXiv, July 2026 (4 pages).

[969] Lattice Surgery Aware Resource Analysis for the Mapping and Scheduling of Quantum Circuits for Scalable Modular Architectures, by Batuhan Keskin, Cameron Afradi, Sylvain Lovis, Maurizio Palesi, Pau Escofet, Carmen G. Almudever, and Edoardo Charbon, arXiv, November 2025 (20 pages).

[970] Advanced Scheduling Strategies for Distributed Quantum Computing Jobs, by Gongyu Ni, Davide Ferrari, Lester Ho, and Michele Amoretti, arXiv, July 2026 (14 pages).

[971] SupercheQ: Quantum Advantage for Distributed Databases, by P. Gokhale, T. Tomesh, et al., arXiv, December 2022 (16 pages).

[972] Quantum Network Utility: A Framework for Benchmarking Quantum Networks, by Yuan Lee, Wenhan Dai, Don Towsley, and Dirk Englund, arXiv, October 2022 (23 pages).

[973] The Quantum Internet (Technical Version), by Peter P. Rohde et al., arXiv, January 2025 (370 pages).

[974] Entanglement-Assisted Quantum Networks: Mechanics, Enabling Technologies, Challenges, and Research Directions, by Zhonghui Li, Jun Lu, et al., arXiv, July 2023 (58 pages).

[975] Architecting Distributed Quantum Computers: Design Insights from Resource Estimation, by Dmitry Filippov, Peter Yang, and Prakash Murali, arXiv, August 2025 (14 pages).

[976] Taming Spacetime Overhead and Design Complexity in Distributed Fault-Tolerant Superconducting Quantum Computation, by Qinjing Yu and Ke Liu, arXiv, August 2026 (19 pages).

[977] Hertz-rate metropolitan quantum teleportation, by Si Shen, Guangcan Guo, Qiang Zhou, et al., Light: Science & Applications, May 2023 🔓 (preprint on doi.org).

[978] Elastic Entangled Pair and Qubit Resource Management in Quantum Cloud Computing, by Rakpong Kaewpuang, Jiawen Kang, et al., arXiv, July 2023 (30 pages).

[979] Q-DICE: Quantum Distributed Interconnect Compiler and Emulator, by Michael Silver, Zachary Vernec, and Hans-Arno Jacobsen, arXiv, June 2026 (11 pages).

[980] Distributed quantum architecture search using multi-agent reinforcement learning, by Mikhail Sergeev, Georgii Paradezhenko, Daniil Rabinovich, and Vladimir V. Palyulin, arXiv, November 2025 (13 pages).

[981] Network-Based Quantum Computing: an efficient design framework for many-small-node distributed fault-tolerant quantum computing, by Soshun Naito, Yasunari Suzuki, and Yuuki Tokunaga, arXiv, January 2026 (29 pages).

[982] A trusted-node-free eight-user metropolitan quantum communication network, by Siddarth Koduru Joshi, Rupert Ursin, et al., arXiv, September 2020 (16 pages).

[983] Flexible entanglement-distribution network with an AlGaAs chip for secure communications, by F. Appas, F. Baboux, M. I. Amanti, A. Lemaître, F. Boitier, E. Diamanti, and S. Ducci, arXiv, April 2021 (12 pages).

[984] Towards a Global Scale Quantum Information Network: A Study Applied to Satellite-Enabled Distributed Quantum Computing, by Laurent de Forges de Parny, Mathias van den Bossche, et al., arXiv, September 2025 (23 pages).

[985] Scheme for Transport-based Global Entanglement Distribution using Quantum Processors, by Erik Lundblad, Mira Abu Yahia, Antonius Johannes Renders, Andreas Walther, Adam Kinos, and Lars Rippe, arXiv, June 2026 (6 pages).

[986] Quality of Service in quantum networks, by Nicolò Lo Piparo, William J. Munro, and Kae Nemoto, arXiv, January 2025 (11 pages).

[987] Optimizing Quantum Communication for Quantum Data Centers with Reconfigurable Networks, by Hezi Zhang, Yiran Xu, Haotian Hu, Keyi Yin, Hassan Shapourian, Jiapeng Zhao, Ramana Rao Kompella, Reza Nejabati, and Yufei Ding, arXiv, December 2024 (13 pages).

[988] Quantum Internet Addressing, by Angela Sara Cacciapuoti, Jessica Illiano, and Marcello Caleffi, arXiv, September 2023 (8 pages).

[989] Quantum City: simulation of a practical near-term metropolitan quantum network, by Raja Yehia, Simon Neves, Eleni Diamanti, and Iordanis Kerenidis, arXiv, November 2022 (28 pages).

[990] Simulators for Quantum Network Modelling: A Comprehensive Review, by Oceane Bel and Mariam Kiran, arXiv, August 2024 (17 pages).

[991] On the Impact of Classical and Quantum Communication Networks Upon Modular Quantum Computing Architecture System Performance, by Pau Escofet, Carmen G. Almudéver, et al., arXiv, July 2025 (12 pages).

[992] An elementary quantum network of entangled optical atomic clocks, by B. C. Nichol, C. J. Ballance, D. M. Lucas, et al., Nature, September 2022 🔓 (preprint on arXiv).

[993] Distributed quantum sensing with optical lattices, by Jose Carlos Pelayo, Karol Gietka, and Thomas Busch, arXiv, August 2022 (7 pages).

[994] Experimental Private Quantum Networked Sensing, by Nicolas Laurent-Puig, Laura dos Santos Martins, Luis Bugalho, Santiago Scheiner, Majid Hassani, Sean William Moore, Damian Markham, and Eleni Diamanti, arXiv, September 2026 (15 pages).

[995] Distant Clock Synchronization Using Entangled Photon Pairs, by Alejandra Valencia, Giuliano Scarcelli, and Yanhua Shih, arXiv, July 2004 (10 pages).

[996] Deterministic Secure Direct Communication Using Entanglement, by Kim Boström and Timo Felbinger, Physical Review Letters, October 2002 🔓 (preprint on arXiv).

[997] The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet, by Dong Pan, Gui-Lu Long, Liuguo Yin, Yu-Bo Sheng, Dong Ruan, Soon Xin Ng, Jianhua Lu, and Lajos Hanzo, arXiv, December 2024 (54 pages).

[998] Practical quantum secure direct communication with squeezed states, by Iris Paparelle, Faezeh Mousavi, Francesco Scazza, Angelo Bassi, Matteo Paris, and Alessandro Zavatta, arXiv, July 2025 (18 pages).

[999] High-dimensional single photon based quantum secure direct communication using time and phase mode degrees, by Byungkyu Ahn, Jooyoun Park, Jonghyun Lee, and Sangrim Lee, Scientific Reports, January 2024.

[1000] Novel Long Distance Free Space Quantum Secure Direct Communication for Web 3.0 Networks, by Yifan Zhou, Xinlin Zhou, Zi Yan Li, Yew Kee Wong, and Yan Shing Liang, arXiv, August 2024 (17 pages).

[1001] Quantum Public Key Encryption for NISQ Devices, by Nishant Rodrigues, Walter O. Krawec, Brad Lackey, Deb Mukhopadhyay, and Bing Wang, arXiv, September 2025 (11 pages).

[1002] Experimental practical quantum tokens with transaction time advantage, by Yang-Fan Jiang, Jian-Wei Pan, et al., arXiv, September 2024 (74 pages).

[1003] Quantum Perspective on Digital Money: Towards a Quantum-Powered Financial System, by Artur Czerwinski, arXiv, July 2025 (20 pages).

[1004] The cost of exactly simulating quantum entanglement with classical communication, by Gilles Brassard, Richard Cleve, and Alain Tapp, arXiv, January 1999 (9 pages).

[1005] Quantum Pseudo-Telepathy, by Gilles Brassard, Anne Broadbent, and Alain Tapp, arXiv, November 2004 (31 pages).

[1006] Experimental Demonstration of Quantum Pseudotelepathy, by Jia-Min Xu, Yi-Zheng Zhen, Yu-Xiang Yang, Zi-Mo Cheng, Zhi-Cheng Ren, Kai Chen, Xi-Lin Wang, and Hui-Tian Wang, arXiv, August 2022 (5 pages).

[1007] Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers, by Llorenç Escolà-Farràs and Florian Speelman, arXiv, July 2025 (41 pages).

[1008] Searching for interstellar quantum communications, by Michael Hippke, arXiv, July 2021 (14 pages).

[1009] Error-detected quantum operations with neutral atoms mediated by an optical cavity, by Brandon Grinkemeyer, Elmer Guardado-Sanchez, Ivana Dimitrova, Danilo Shchepanovich, G. Eirini Mandopoulou, Johannes Borregaard, Vladan Vuletić, and Mikhail D. Lukin, Science, March 2025 (5 pages) 🔓 (preprint on arXiv).

[1010] An integrated atom array-nanophotonic chip platform with background-free imaging, by Shankar G. Menon, Noah Glachman, Matteo Pompili, Alan Dibos, and Hannes Bernien, Nature Communications, July 2024 (7 pages).

[1011] A Universal Quantum Information Preserving Photonic Switch for Scalable Quantum Networks, by Jiapeng Zhao, Stéphane Vinet, Amir Minoofar, Michael Kilzer, Lucas Wang, Galan Moody, Vijoy Pandey, Ramana Kompella, and Reza Nejabati, arXiv, April 2026 (12 pages).

[1012] Benchmarking Quantum Data Center Architectures: A Performance and Scalability Perspective, by Shahrooz Pouryousef, Eneet Kaur, Hassan Shapourian, Don Towsley, Ramana Kompella, and Reza Nejabati, arXiv, January 2026 (15 pages).

[1013] ATHENA: A Compiler For Optimized Scheduling In Distributed Quantum Computers, by Won Joon Yun, Dhilan Nag, Sneha Ballabh, Jiapeng Zhao, Eneet Kaur, and Poulami Das The University of Texas at Austin Cisco Quantum Lab), arXiv, May 2026 (18 pages).

[1014] Distributed Quantum Error Correction with Bivariate Bicycle Codes in a Modular Architecture, by Nitish Kumar Chandra, Eneet Kaur, Reza Nejabati, and Kaushik P. Seshadreesan, arXiv, May 2026 (11 pages).

[1015] Impact of Network Constraints on Fault-Tolerant Distributed Quantum Computing, by Eneet Kaur, Shahrooz Pouryousef, Nitish Kumar Chandra, Hassan Shapourian, Jiapeng Zhao, Ramana Kompella, and Reza Nejabati, arXiv, June 2026 (22 pages).

[1016] Cryogenic packaging of nanophotonic devices with a low coupling loss < 1 dB, by Beibei Zeng, Mikhail Lukin, Marko Loncar, Bart Machielse, et al., arXiv, August 2023 (12 pages).

[1017] Erbium Quantum Memory Platform with Long Optical Coherence via Back-End of Line Deposition on Foundry-Fabricated Photonics, by Shobhit Gupta, Sean E. Sullivan, et al., arXiv, June 2025 (14 pages).

[1018] A perspective on the pathway to a scalable quantum internet using rare-earth ions, by Robert M. Pettit, Farhang

Hadad Farshi, Sean E. Sullivan, Álvaro Véliz-Osorio, and Manish Kumar Singh, arXiv, May 2023 (31 pages).

[1019] Quasi-deterministic localization of Er emitters in thin film TiO2 through submicron-scale crystalline phase control, by Sean E. Sullivan et al., Applied Physics Letters, December 2023 (7 pages) (preprint on arXiv).

[1020] Waseda University Ventures Invests in Japanese Quantum Computer Hardware Startup, by Matt Swayne, The Quantum Insider, February 2023.

[1021] Fiber-optic quantum interface with an array of more than 100 individually addressable atoms on an optical nanofiber, by Mitsuyoshi Takahata, Jameesh Keloth, Takashi Yamamoto, Ken-ichi Harada, Shigehito Miki, and Takao Aoki, arXiv, March 2026 (16 pages).

[1022] Addressing requirements for crosstalk-free quantum-gate operation in many-body nanofiber cavity QED systems, by Tim Keller, Seigo Kikura, Rui Asaoka, Yasunari Suzuki, Yuuki Tokunaga, and Takao Aoki, arXiv, September 2025 (19 pages).

[1023] Photon transport enhancement through a coupled-cavity QED system with dynamic modulation, by Shinya Kato et al., 2022 (10 pages).

[1024] A fiber array architecture for atom quantum computing, by Xiao Li, Ming-Sheng Zhan, et al., arXiv, November 2024 (12 pages).

[1025] Passive Quantum Interconnects: High-Fidelity Quantum Networking at Higher Rates with Less Overhead, by Seigo Kikura, Kazufumi Tanji, Akihisa Goban, and Shinichi Sunami, arXiv, July 2025 (26 pages).

[1026] Strong coupling of a reconfigurable ^{171}Yb atom array to a tunable telecom-band nanofiber cavity, by Hideki Ozawa, Ryotaro Inoue, et al., arXiv, September 2026 (18 pages).

[1027] A dual-region ytterbium tweezer apparatus with an in-vacuum nanofiber cavity, by Shunichiro Hashimoto, Hideki Ozawa, Yusuke Hisai, Takao Aoki, and Ryotaro Inoue, arXiv, September 2026 (6 pages).

[1028] Interfacing of an Optical Nanofiber with Tunably Spaced Atoms in an Optical Lattice, by Hyok Sang Han, S. L. Rolston, et al., arXiv, September 2025 (8 pages).

[1029] International Collaboration Will Create a Theoretical Blueprint for a Modular Fault-Tolerant Quantum Computer, by NuQuantum, March 2024.

[1030] Strong Coupling of a Single Ion to an Optical Cavity, by Hiroki Takahashi, Physical Review Letters, January 2020 (preprint on arXiv).

[1031] Interface between Trapped-Ion Qubits and Traveling Photons with Close-to-Optimal Efficiency, by J. Schupp, Tracy Northup, et al., PRX Quantum, June 2021 (16 pages).

[1032] Distributed quantum error correction based on hyperbolic Floquet codes, by Evan Sutcliffe, Bhargavi Jonnadula, Claire Le Gall, Alexandra E. Moylett, and Coral M. Westoby, arXiv, March 2025 (8 pages).

[1033] Logical gates on Floquet codes via folds and twists, by Alexandra E. Moylett and Bhargavi Jonnadula, arXiv, January 2026 (49 pages).

[1034] Tolerating Device Failure in Distributed Quantum Computing, by Evan Sutcliffe and Coral M. Westoby, arXiv, May 2026 (9 pages).

[1035] A quantum microwave-to-optical transducer, by Thibaut Jacqmin of LKB, 2019 (17 slides).

[1036] Optomechanical quantum teleportation, by Niccolò Fiaschi, Bas Hensen, Andreas Wallucks, Rodrigo Benevides, Jie Li, Thiago P. Mayer Alegre, and Simon Gröblacher, arXiv, November 2022 (14 pages).

[1037] Microwave-to-optics conversion using a mechanical oscillator in its quantum groundstate, by Moritz Forsch, Robert Stockill, Simon Gröblacher, et al., arXiv, May 2020 (11 pages).

[1038] Monolithic high density integrated photonics on bulk lithium niobate, by Zizheng Li, Harmen Smedes, Bruno Lopez-Rodriguez, Thomas Scholte, Simon Groeblacher, and Iman Esmaeil Zadeh, arXiv, August 2026.

[1039] Ultra-low-noise Microwave to Optics Conversion in Gallium Phosphide, by Robert Stockill, Simon Gröblacher, et al., Nature communications, November 2022 (12 pages).

[1040] The widely anticipated quantum internet breakthrough is finally here, by Maija Palmer, May 2021.

[1041] A perspective on hybrid quantum opto- and electromechanical systems, by Yiwen Chu and Simon Gröblacher, arXiv, July 2020 (7 pages).

[1042] Coherent feedback in optomechanical systems in the sideband-unresolved regime, by Jingkun Guo and Simon Gröblacher, arXiv, October 2022 (20 pages).

[1043] An integrated microwave-to-optics interface for scalable quantum computing, by Matthew J. Weaver, Simon Gröblacher, Robert Stockill, et al., Nature Nanotechnology, October 2023 (14 pages) (preprint on arXiv).

[1044] Proposal for optomechanical quantum teleportation, by Jie Li, Simon Gröblacher, et al., arXiv, September 2020 (9 pages).

[1045] Scalable Quantum Computing with Optical Links, by M.J. Weaver, G. Arnold, H. Weaver, Simon Gröblacher, and Robert Stockill, arXiv, May 2025 (23 pages).

[1046] Bidirectional microwave-optical transduction based on integration of high-overtone bulk acoustic resonators and photonic circuits, by Terence Blésin, Wil Kao, Anat Siddharth, Rui N. Wang, Alaina Attanasio, Hao Tian, Sunil A. Bhave, and Tobias J. Kippenberg, Nature Communications, July 2024 (10 pages).

[1047] Bad gateway Error code 502 , by David Awschalom, Dirk Englund, Andrei Faraon, et al., Nature Communications, February 2021 (21 pages).

[1048] Efficient Conversion of Optical to Mechanical States Close to the Single-Quantum Level, by Alexander Rolf Korsch, Liu Chen, Pedro V. Pinho, Boris Müllendorff, Jan N. Kirchhof, Yong Yu, Thiago P. Mayer Alegre, and Simon Gröblacher, arXiv, September 2026 (21 pages).

[1049] Comparing optical-microwave conversion and all-microwave control schemes for a transmon qubit, by Volodymyr Monarkha, Massimo Borrelli, Reza Hajitashakkori Kenari, Mohammad Kobba, Eugenio Cataldo, Beer de Zoeten, Mahnaz Zarrinfar, Kamal Pandey, Abhinand Pusuluri, Filippo D. Michelacci, Eliot Jouan, Bennett Sprague, Simon Groeblacher, Thierry C. van Thiel, Robert Stockill, and Russell E. Lake, arXiv, March 2026 (6 pages).

[1050] Optical readout of a superconducting qubit using a piezo-optomechanical transducer, by T. C. van Thiel, Simon Gröblacher, et al., Nature Physics, February 2025 (preprint on arXiv).

[1051] Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble, by Pierre Vernaz-Gris, Kun Huang, Mingtao Cao, Alexandra S. Sheremet, and Julien Laurat, Nature Communications, January 2018 (7 pages).

[1052] Deterministic photon waveform adaptation for quantum connectivity, by Jeffrey Mohan, Jérémy Berroir, Filippo Borselli, David Libault, Ferhat Loubar, Kilian Müller, Jed Rowland, Félix Hoffet, Eleni Diamanti, Tom Darras, Tommaso Mazzoni, and Julien Laurat, arXiv, September 2026 (15 pages).

[1053] Connecting heterogeneous quantum networks by hybrid entanglement swapping, by G. Guccione, T. Darras, H. Le Jeannic, V. B. Verma, S. W. Nam, A. Cavaillès, and J. Laurat, arXiv, April 2021 (15 pages).

[1054] Ultralow-power single-pass all-optical photon router, by Jérémy Berroir, Tridib Ray, Alban Urvoy, and Julien Laurat, Optica, August 2025 (2 pages).

[1055] Fault-Tolerant Logical Operations and Efficient State Preparation in Modular Quantum Architectures with Noisy Interfaces, by Siddardha Chelluri, Riccardo Mengoni, Tom

Darras, Julien Laurat, Eleni Diamanti, and Ioannis Lavdas, arXiv, July 2026 (10 pages).

[1056] Entanglement of two quantum memories via fibres over dozens of kilometres, by Yong Yu, Jian-Wei Pan, et al., Nature, February 2020 🔓 (preprint on arXiv).

[1057] Efficient multiplexed quantum memory with high dimensional orbital angular momentum states in cold atoms, by Xin Yang, Hong Gao, et al., arXiv, March 2025 (9 pages).

[1058] Deterministic storage and retrieval of telecom light from a quantum dot single-photon source interfaced with an atomic quantum memory, by Sarah E. Thomas et al., April 2024 (7 pages).

[1059] Quantum Networks Enhanced by Distributed Quantum Memories, by Xiangyi Meng, Nicolò Lo Piparo, Kae Nemoto, and István A. Kovács, arXiv, March 2024 (6 pages).

[1060] Connecting heterogeneous quantum networks by hybrid entanglement swapping, by Giovanni Guccione, May 2020 (7 pages).

[1061] Quantum systems learn joint computing - MPQ researchers realize the first quantum-logic computer operation between two separate quantum modules in different laboratories, by MPQ, February 2021.

This **Quantum Telecommunications** subsection contains 335 bibliographical references and notes containing at least 5,035 pages.

1.6 Quantum Physical Unclonable Functions

Quantum physical unclonable functions (QPUFs) are still a relatively small and immature branch of quantum security [1062]. They sit at the crossroads of cryptography, embedded hardware, quantum communications and quantum hardware security. A classical physical unclonable function (PUF) is a hardware security primitive whose input-output behavior depends on uncontrollable physical variations introduced during fabrication. A challenge C applied to a given device produces a response $R = f_{\mathrm{PUF}}(C)$ that should be difficult to predict or reproduce with another device, while remaining reproducible on the same device within a finite noise tolerance [1063, 1064]. This reproducibility is essential. A PUF is therefore not a true random number generator (TRNG). A TRNG should generate a new unpredictable value at each readout, whereas a PUF should recover the same device-specific response for a given challenge. In practice, error correction or a fuzzy extractor is often needed to derive a stable cryptographic key from a noisy raw PUF response [1064].

PUFs can exploit optical multiple scattering, propagation-delay variations such as ring oscillators, coating capacitance, SRAM power-up states, DRAM characteristics, or quantum-confined semiconductor structures. Their security does not simply improve as semiconductor nodes shrink. It depends on the entropy, stability, challenge-response space and attack model. Classical PUFs can be vulnerable to mathematical or machine-learning modeling attacks when many challenge-response pairs are exposed, as well as to side-channel leakage, fault injection and invasive probing [1064]. For binary responses, an ideal population has an inter-device Hamming distance close to 50% and an intra-device Hamming distance close to 0%, corresponding respectively to uniqueness and repeatability.

Samsung provides a useful commercial example. The Exynos 9820 used in some Galaxy S10 models included a silicon PUF to provide a device-unique key for its secure key manager. Separately, Samsung and SK Telecom launched the Galaxy A Quantum in 2020 with an ID Quantique QRNG chip. The latter was not a replacement for the Exynos PUF. It was a different security primitive used as an entropy source.

The term QPUF is used in several distinct contexts in the literature. In the formal cryptographic model, a QPUF is a physical device implementing an unknown quantum transformation, with quantum challenge and response states and security properties such as uniqueness, robustness, testability and unforgeability [1062, 1065]. A Quantum Readout PUF (QR-PUF) is the physical token which can remain a classical optical PUF, while non-orthogonal or low-photon quantum challenges limit the information that an attacker can extract from the interrogation signal. The first experimental quantum-secure authentication of this kind used a classical multiple-scattering optical key illuminated with fewer photons than spatial degrees of freedom [1066]. A third category, sometimes also called a quantum PUF, uses quantum-scale material properties or hardware-specific QPU noise to generate a classical fingerprint. These architectures rely on different security assumptions.

QPUFs are not necessarily "better" than classical PUFs. The no-cloning theorem is a useful security resource, but it does not by itself provide an unforgeability proof. Arapinis et al. showed that, within their unitary-QPUF framework, quantum existential unforgeability cannot be achieved against a general quantum polynomial-time adversary, whereas quantum selective unforgeability can be achieved by a broad family of unitary QPUFs [1065]. Later measurement-based and non-unitary constructions showed that existential unforgeability can be recovered under different QPUF models [1067]. Pseudorandom quantum states and pseudorandom unitaries can also relax the impractical requirement for ideal Haar-random resources in some constructions [1068].

Several experimental approaches coexist. Photonic QR-PUFs use multiple-scattering media, while a 2026 silicon-photonics proposal experimentally implements the physical PUF with a programmable silicon-nitride interferometer mesh and numerically studies a single-photon quantum-readout protocol [1069]. Another approach fingerprints a cloud QPU from device-specific noise and calibration properties. Phalak et al. demonstrated two such QPU fingerprints on IBM hardware, reporting an inter-device Hamming distance of 55% and an intra-device distance as low as 4%, compared with the idealized targets of 50% and 0% for balanced binary responses [1070]. These targets express uniqueness and repeatability and do not by themselves establish security, which also depends on entropy and attack resistance. Smith and Gokhale later studied intrinsic fingerprinting of fixed-frequency transmon processors and key extraction in the presence of noise [1071]. Such QPU fingerprints can help verify that a cloud job was executed on the expected physical processor, but temporal drift and recalibration also change the fingerprint and must be handled by the authentication protocol. More generally, practical QPUFs still face difficult requirements involving quantum-state preparation and storage, efficient generation of sufficiently pseudorandom transformations, noise tolerance and resistance to tomography or emulation attacks [1062].

Quantum Base

UK, 2013, $8M

Quantum Base commercializes Q-ID, a printable authentication technology based on quantum-active materials whose microscopic disorder produces a device-specific optical emission fingerprint that can be read with a smartphone. A 2022 peer-reviewed Lancaster University and Quantum Base paper gives a much closer scientific

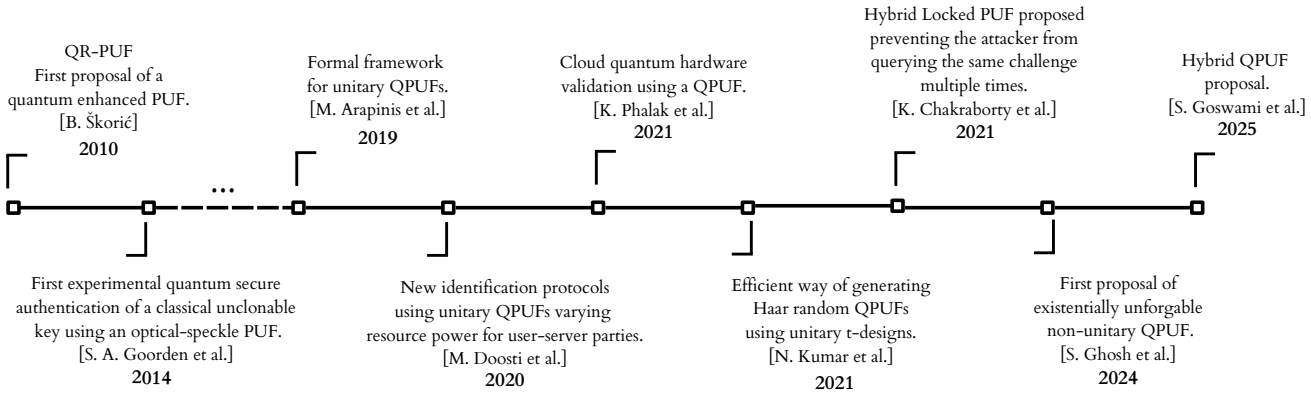


Figure 91: A timeline of academic developments in the QPUF domain. Source: the 2026 review paper [1062].

description of this approach: randomly deposited quantum dots embedded in a transparent polymer form a tag whose spatial photoluminescence pattern and nonlinear response to excitation power provide the fingerprint, which can be interrogated with an unmodified smartphone flash and camera [1072]. This is best described as an optical PUF exploiting quantum-material properties rather than a formal QPUF with quantum challenge and response states. Earlier Lancaster work demonstrated a different quantum-confinement PUF using fluctuations in the tunneling spectrum of resonant-tunneling diodes (RTDs) [1073]. The company also commercializes Q-RAND, a separate QRNG product. Q-ID and Q-RAND are independent products rather than one being integrated into the other.

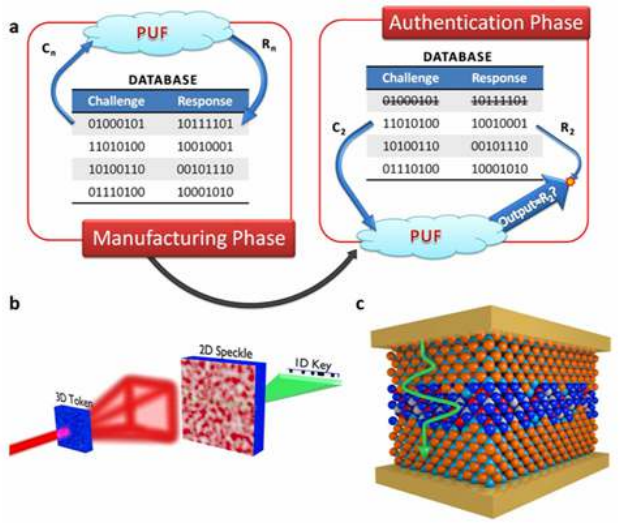


Figure 92: Schematic and working principles: (a) challenge-response enrollment and authentication, (b) a classical optical scattering PUF, and (c) a conceptual quantum-confinement PUF based on tunneling through a quantum well. The third panel is a quantum-material device, not a formal QPUF with quantum challenge and response states. Adapted from [1073].

In the RTD implementation, the identity is encoded in the positions and shapes of resonant peaks in the current-voltage characteristic. The 2015 experiment estimated about 10^3 distinguishable identities for the measured single-device structure and noted that arrays of devices or higher-dimensional quantum confinement could greatly enlarge this space [1073]. A later study on 130 RTDs showed how their current-voltage spectra could be converted into robust digital PUF responses [1074].

Quanta Infinitum Data

USA, 2024

Quanta Infinitum Data advertises quantum-dot-based tracking, certification and supply-chain services. However, the available public material does not describe a challenge-response PUF architecture, a quantum interrogation protocol, or a QPUF security model. I would therefore not classify this offering as a QPUF without additional technical evidence.

Infleqtion (USA) is developing QPUF techniques with the Australian Army and Diraq using its Superstaq software platform. In this class of approach, the "physical" part is the device-specific behavior of the quantum processor, such as gate, readout, decoherence and calibration characteristics, while the "quantum" part is that the fingerprint is generated by circuits executed on the QPU itself [1070, 1071]. Infleqtion describes both intrinsic and logical QPUFs and is exploring several hardware platforms.

1.6.1 Bibliography and notes

These are the bibliographical references and notes for the **Quantum Physical Unclonable Functions** subsection.

[1062] Secure Authentication via Quantum Physical Unclonable Functions: A Review, by Pol Julià Farré, Vladlen Galetsky, Mohamed Belhassen, Gregor Pieplow, Kumar Nilesh, Holger Boche, Tim Schröder, Janis Nötzel, and Christian Deppe, Advanced Quantum Technologies, January 2026 (19 pages).

[1063] Physical One-Way Functions, by Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld, Science, September 2002 (5 pages) 🔓 (preprint on hdl.handle.net).

[1064] Physical Unclonable Functions and Applications: A Tutorial, by Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas, Proceedings of the IEEE, August 2014 (16 pages).

[1065] Quantum Physical Unclonable Functions: Possibilities and Impossibilities, by Myrto Arapinis, Mahshid Delavar, Mina Doosti, and Elham Kashefi, Quantum, June 2021 (32 pages).

[1066] Quantum-Secure Authentication of a Physical Unclonable Key, by Sebastianus A. Goorden, Marcel Horstmann, Allard P. Mosk, Boris Škorić, and Pepijn W. H. Pinkse, Optica, December 2014 (4 pages).

[1067] Existential Unforgeability in Quantum Authentication from Quantum Physical Unclonable Functions Based on Random von Neumann Measurement, by Soham Ghosh, Vladlen Galetsky, Pol Julià Farré, Christian Deppe, Roberto Ferrara, and Holger Boche, Physical Review Research, December 2024.

[1068] On the Connection Between Quantum Pseudorandomness and Quantum Hardware Assumptions, by Mina Doosti, Niraj Kumar, Elham Kashefi, and Kaushik Chakraborty, Quantum Science and Technology, April 2022.

[1069] Quantum-Secure Physical Unclonable Function enabled by Silicon Photonics Integrated Circuits, by G. Sarantoglou, N. Tzekas, G. Moustakas, G.A. Karydis, V. Kaminski, E. Protsenko, K. Gradkowski, A. Bazin, C. Vigliar, A. Bogris, and C. Mesaritakis, arXiv, May 2026 (12 pages).

[1070] Quantum PUF for Security and Trust in Quantum Computing, by Koustubh Phalak, Abdullah Ash Saki, Mahabubul Alam, Rasit Onur Topaloglu, and Swaroop Ghosh, IEEE Journal on Emerging and Selected Topics in Circuits and Systems, June 2021 (10 pages) 🔓 (preprint on arXiv).

[1071] Trustworthy Quantum Computation through Quantum Physical Unclonable Functions, by Kaitlin N. Smith and Pranav Gokhale, arXiv, November 2023 (11 pages).

[1072] Using Intrinsic Properties of Quantum Dots to Provide Additional Security When Uniquely Identifying Devices, by Matthew J. Fong, Christopher S. Woodhead, Nema M. Abdelazim, Daniel C. Abreu, Angelo Lamantia, Elliott M. Ball, Kieran Longmate, David Howarth, Benjamin J. Robinson, Phillip Speed, and Robert J. Young, Scientific Reports, October 2022 (8 pages).

[1073] Using Quantum Confinement to Uniquely Identify Devices, by J. Roberts, I. E. Bagci, M. A. M. Zawawi, J. Sexton, N. Hulbert, Y. J. Noori, M. P. Young, C. S. Woodhead, M. Missous, M. A. Migliorato, U. Roedig, and R. J. Young, Scientific Reports, November 2015 (8 pages).

[1074] Resonant-Tunnelling Diodes as PUF Building Blocks, by Ibrahim Ethem Bagci, Thomas McGrath, Christine Barthelmes, Scott Dean, Ramon Bernardo Gavito, Robert James Young, and Utz Roedig, IEEE Transactions on Emerging Topics in Computing, April 2021 (8 pages).

This **Quantum Physical Unclonable Functions** subsection contains 13 bibliographical references and notes containing at least 133 pages.

1.7 QKD and PQC vendors

We review selected technology vendors in the PQC and QKD markets and describe their offerings and differentiation where public evidence is available (Figure 93 and Figure 94). I have only kept startups offering technology solutions and not integrated consulting and integration companies. I also skip most of the cybersecurity companies that are now embedding PQC in their offering.

The market for quantum and post-quantum cryptography remains modest compared with mainstream cybersecurity. A 2017 report estimated it at $2.5B by 2022 [1075]. The standardization landscape has now materially changed. NIST finalized FIPS 203 (ML-KEM, derived from CRYSTALS-Kyber), FIPS 204 (ML-DSA, derived from CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, derived from SPHINCS+) in August 2024. HQC was selected in March 2025 as an additional key-encapsulation mechanism for future standardization. The market is therefore increasingly shifting from algorithm selection to cryptographic inventory, migration, hybrid deployment, and crypto-agility.

In addition to startups, commercial offers in quantum and post-quantum cryptography are also proposed or about to be proposed by various large IT players such as **Battelle**, **Infineon**, **Raytheon**, **IBM** [1076], **Eviden/Atos**, **Gemalto** (part of Thales group), **Cisco**, **Infineon** with its OPTIGA TPM SLB 9672, a hardware trust module supporting symmetric and hash primitives such as AES and SHA-384, which are distinct from post-quantum public-key algorithms and do not by themselves make the product a PQC implementation, **Intel** [1077], **NEC**, **Huawei** [1078], **KT** and **Samsung**.

Amazon announced in 2022 the creation of its own quantum networking center in Boston and a partnership with Harvard University [1079].

NordVPN supports PQC in its VPN professional and consumer VPN offering since May 2025, including in its mobile versions.

Google integrated NIST-compliant PQC in its cloud Key Management Service (Cloud KMS) in 2025.

HP added quantum crypto-resistance to its color laser 8000 Series business printers in 2025, embedded in the printer ASIC chips [1080].

STMicroelectronics integrated PQC in hardware cryptographic accelerators and associated software libraries for their STM32 microcontrollers, in the X-CUBE-PQC software library, and for Stellar automotive microcontrollers that contain the SHA-3 hardware accelerator.

IBM was a major contributor to the NIST PQC process. CRYSTALS-Kyber and CRYSTALS-Dilithium, developed by international teams including IBM researchers, were standardized by NIST in 2024 as ML-KEM (FIPS 203) and ML-DSA (FIPS 204). IBM has progressively integrated quantum-safe cryptography into its software, cloud, infrastructure, and storage security offerings, generally using hybrid migration paths that combine existing cryptography with standardized PQC. Earlier IBM demonstrations included modified tape-drive firmware combining PQC key establishment with AES-256 for long-term data protection.

Microsoft historically researched several PQC candidates, including FrodoKEM and SIKE. Its production platform has now converged on the NIST standards. ML-KEM and ML-DSA became generally available through Windows Cryptography API: Next Generation (CNG) and certificate functions for Windows Server 2025 and Windows 11, after the initial Windows Insider support in 2025. Microsoft is also adding PQC support to certificate services and hybrid protocol stacks. In December 2022, Microsoft acquired Lumenisity, a UK startup developing hollow-core fiber (HCF), which can also be useful for quantum communications and QKD experiments [1081]. HCF links were tested by British Telecom [1082] and later for TF-QKD [1083].

Let's also mention **Toshiba**, one of the most mature commercial QKD suppliers. Its current portfolio includes the Multiplexed QKD System MU, the Long-Distance QKD System LD, the Flexible QKD System LE, and a quantum key-management system. The MU system multiplexes an O-band quantum channel with C-band classical traffic on existing fiber and specifies a secure key rate of 300 kb/s at 10 dB channel loss, a 30 dB loss budget, and a range of 90 km or more. The LD system uses a dedicated C-band quantum channel, requires two fibers, specifies the same 300 kb/s secure key rate at 10 dB loss, and reaches 150 km or more with a 30 dB loss budget. Both use Toshiba's efficient decoy-state BB84 implementation and standard 19" rack-mount hardware. Toshiba also continues research on chip-based, satellite, and twin-field QKD [1084].

01 Quantum

Canada, 1992

01 Quantum, formerly 01 Communique and marketed for years under the IronCAP brand, develops PQC software. Its IronCAP cryptographic engine and toolkits support the NIST-standardized ML-KEM, ML-DSA and SLH-DSA families, together with additional post-quantum algorithms. The product line includes IronCAP X for end-to-end file and email protection and application-oriented products such as XMail, OnCall and InTouch.

ABCMint Foundation

Switzerland, 2017

Created by Jin Liu and Jintai Ding, ABCMint Foundation proposed a quantum-resistant Blockchain based on the Rainbow multivariate signature scheme. This description is now historical. Rainbow was practically cryptanalyzed in 2022, including a key-recovery attack on its NIST security-level-1 parameters [135], and it

Figure 93: Map of QKD and QPU interconnect vendors in alphabetical order. Olivier Ezratty, 2023-September 2026.

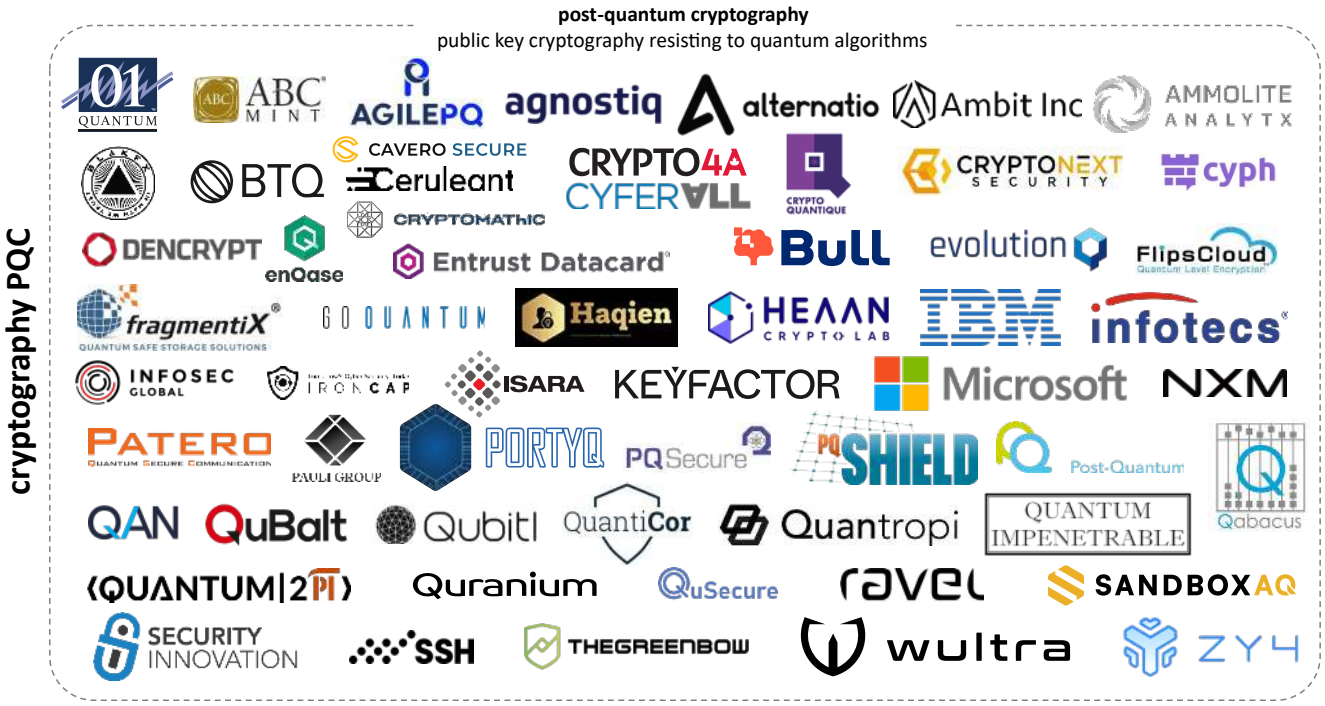


Figure 94: Map of PQC vendors in alphabetical order. Olivier Ezratty, 2023-September 2026.

was not standardized by NIST. ABCMint material still refers to Rainbow and to an upgrade path, but I did not find evidence of a completed migration to a standardized PQC signature scheme. It should therefore not be presented as a currently validated quantum-resistant Blockchain unless such a migration is documented.

Abelian

USA, 2018

Abelian develops a privacy-oriented, post-quantum Layer-1 Blockchain whose mainnet has operated since 2022. Its cryptography is lattice based and its current

positioning emphasizes quantum-resistant digital assets, privacy-preserving transactions, wallets and interoperability with Web3 applications. The project traces its development to 2018, rather than 2022. The earlier "gold 2.0" description no longer captures the scope of its offering. [1085]

AegiQ

UK, 2019, $4.3M

AegiQ is a University of Sheffield spin-off created by Max Sich, Scott Dufferwiel and Andrii Iamshanov. Its 2026 offering is broader than QKD. It sells deterministic C-band single-photon and entangled-state sources based on epitaxial quantum dots, available as fiber-packaged chips or turn-key 19" rack systems. It also offers QLAS, a Quantum Link Assurance System for real-time detection of tampering on optical fiber, the LightWorks SDK, and a first-generation reconfigurable photonic quantum computer. The same deterministic telecom-band light-source technology targets quantum networking and quantum-communication links.

AgilePQ

USA, 2014

AgilePQ developed lightweight cryptographic software for embedded and connected systems, including its DEFEND technology. Its public material historically emphasized proprietary adaptive key-generation and constrained-device deployments. DEFEND is not one of the NIST FIPS 203, 204 or 205 standards, and nominal key-space comparisons such as "429 orders of magnitude stronger than AES-256" are not meaningful measures of cryptographic security. The company is therefore better presented as a proprietary quantum-resistant security vendor rather than as a standardized PQC supplier.

Aliro Quantum

USA, 2018, $31M

Aliro Quantum, cofounded by Prineha Narang and Jim Ricotta, develops software to design, operate and manage entanglement-based quantum networks. Its current stack contains Aliro Simulator for network design and validation, AlirOS as the control plane and software/gateware stack that turns heterogeneous quantum-network hardware into network nodes, and Aliro Orchestrator for configuration, monitoring and automation. AlirOS currently implements BBM92 key distribution and abstracts vendor-specific sources, detectors and optical components, while being designed as a foundation for more general entanglement networks and future quantum-internet applications.

Ambit

USA, 2019, $1M

American Binary, now marketed as Ambit, develops post-quantum network-security software. Its flagship Ambit Client is an enterprise VPN designed around CNSA 2.0 requirements and crypto-agility, with standardized PQC rather than a proprietary "quantum" transport. The company emphasizes high-throughput VPN deployment and automatic cryptographic upgrades as standards evolve.

Anametric

USA, 2017, $5.2M

Anametric develops room-temperature, chip-scale quantum photonics for cybersecurity. Its current work emphasizes photonic quantum-random-number generation and quantum-communication components rather than information storage in room-temperature qubits. The company is one of the contributors to the QRNG Open API initiative led by Palo Alto Networks, and its recent development work includes integrated photonic entropy-generation architectures intended for secure communications and PQC systems. It raised an additional $3.3M seed round in 2024.

Alternatio

Poland, 2016-2022

Alternatio developed a post-quantum cryptography IP core to be integrated in chips for the industry and connected objects.

Ammolite Analytx

Canada, 2004

Ammolite Analytx is a cybersecurity company that provides an AI-based analytics tool to assess the risks with quantum computing on cybersecurity.

Arobs Polska

Poland, 2023

Arobs Polska is developing a high-rate photon detector for QKD for the ESA with Polytechnique de Milano and the University of Torun. It was also selected by ESA to embed PQC cryptography in satellite telecommunication applications as part of the PQC ASTrAL project. It is providing hardware, firmware, and cryptographic IP core (in FPGAs).

Arq Quantum Technologies

Spain, 2025, $1.4M

Arq Quantum Technologies is a spin-out from Hugues de Riedmatten's team at ICFO (Barcelona) that is developing rare-earth-based quantum repeater technology, creating telecom wavelengths entangled photon sources [925]. The company was created by Samuele Grandi, a former post-doc from this team.

Arqit

UK, 2016, $99.8M

Arqit is now a software cryptography company rather than a satellite-QKD vendor. After abandoning its own satellite-QKD program in 2022, it centered its offering on SKA-Platform, which creates synchronized symmetric keys at endpoints without transporting the keys themselves. Its current portfolio also includes NetworkSecure for applying these keys to network encryption and Encryption Intelligence for cryptographic visibility and policy. Arqit positions the system as crypto-agile and complementary to PQC, rather than as a replacement for the NIST PQC standards.

The company's earlier claim that terrestrial QKD could be implemented without trusted nodes or repeaters was challenged in the scientific literature [1086]. The historical satellite strategy and QuantumCloud branding should therefore not be confused with the current commercial offering.

Astrolight

Lithuania, 2019

Astrolight develops secure telecommunication systems for aerospace, defense and governmental applications including laser sources and optical ground stations which can be used for satellite QKD distribution.

Beyond Semiconductor

Slovenia, 2005

Beyond Semiconductor develops secure semiconductor IP and hardware and participated in the SiQUID EuroQCI project, completed in 2026, to develop compact QKD equipment and optical/security subsystems for European quantum-communication infrastructure. Its role is better described as QKD hardware and cryptographic-IP engineering than as a mature full-stack QKD-system vendor. Public product information remains much more limited than for the larger QKD suppliers.

BLAKFX

USA, 2017

BLAKFX develop quantum resistant software solutions around their Helix22 SDK that provides five layers of symmetric keys protections for end-user to end-user communications (AES1, TwoFish, AES2, ThreeFish, Snow3G). With sufficiently long keys, symmetric keys are quantum resistant.

BraneCell Systems

USA-Germany, 2015, $1.8M

BraneCell Systems is a startup launched by Wassim Estephan and Christopher Papile. It started to develop a cold atom based QPU [1087, 1088]! They have filed a few patents, including USPTO patent 9607271, validated in March 2017. It later pivoted to developing an atom-based repeater. It subsequently pivoted again to quantum neural networks for AI and to decentralized AI chip fabrication.

BTQ Technologies

Canada, 2021

BTQ Technologies develops post-quantum security technology for hardware and digital assets. Its QCIM, Quantum Compute-In-Memory, is a synthesizable crypto-agile accelerator IP intended for ASIC or FPGA integration and supporting both classical cryptography and standardized PQC including ML-KEM and ML-DSA. BTQ is also developing the Quantum Secure Stablecoin Network (QSSN) for quantum-safe privileged operations in payment and stablecoin systems, and Bitcoin Quantum, a migration architecture for Bitcoin. The earlier Sonora Gold and Silver Corp entry reflected a historical corporate transaction and is no longer the appropriate identity for this business.

CAS QuantumNet

China, 2017, $230M

CAS QuantumNet aka Guoke Quantum is a quantum key operation services company that offers its Q-NET BOX quantum security mobile private network communication equipment. It secures the backbone of LTE telecom networks with QKD.

Cavero Quantum

UK, 2024, £2.2M

Cavero Quantum is a University of Leeds spin-out created by Ben Varcoe and Frey Wilson. It develops software-only symmetric-key establishment and authentication. Its Symmetrikey product creates shared keys without conventional public-key exchange and is designed for constrained endpoints including SIM cards and embedded devices. Authentikey provides continuous mutual authentication. The company also provides a cryptographic library for integration. This is proprietary quantum-safe cryptography rather than QKD[1089, 1090]

Celare Quantum Communications

Denmark, 2024, €0.5M + €2.5M EIC grant

Celare Quantum Communications is a DTU spin-out created to commercialize room-temperature continuous-variable QKD. It develops compact network appliances designed to operate on existing telecommunications fiber. In 2026, Celare systems were installed in a Danish government quantum-secure network connecting four ministries and a government agency, and in the Danish Ministry of Defence. The company is also involved

in AccessQKD, a 2025-2028 project on scalable access-network CV-QKD, and received a €2.5M EIC Transition grant for further development and scaling. The earlier $582M funding figure was erroneous.

Ceruleant Systems

USA, 2019

Ceruleant Systems provides a PQC-ready encryption solution marketed around reduced computing and energy overhead.

CEW Systems (2020, Canada) provides an encryption wrapper around symmetric cryptography and markets it as quantum-resistant. Public technical information remains limited, so I do not classify it as a standardized PQC implementation without stronger documentation.

Ciena

USA, 1992

Ciena is an optical-network equipment vendor. Its current quantum-safe positioning combines high-speed optical-layer encryption with standardized PQC and interoperability with external QKD systems. Its WaveLogic 6 Extreme platform supports up to 1.6 Tb/s encrypted optical transport and has been demonstrated in hybrid PQC/QKD configurations, including with Toshiba on the Quantum Corridor network in 2026. Ciena has also demonstrated quantum-secured communications with QCi, integrating QKD, quantum authentication, classical authentication and AES-256-GCM optical encryption. It is therefore no longer accurate to describe Ciena as lacking a structured quantum-safe offering.

Cisco Systems

USA, 1984

Cisco is developing quantum-networking technology rather than a conventional commercial QKD appliance. In 2025, it unveiled with UC Santa Barbara a low-power integrated entangled-photon source prototype operating at telecom wavelengths and generating up to about 200 million entangled photon pairs per second [1091]. This device is intended as a building block for entanglement distribution and future quantum networks. Cisco has also published architectures for scalable quantum networks, optical switching between QPUs, circuit partitioning and quantum data-center infrastructures [1092, 1093].

Craft Prospect

UK, 2017

Craft Prospect is a space engineering company that is providing satellite CubeSat based QKD technology as part of the Amplified Quantum Key Distribution (AQKD) project funded by Innovate UK.

Crypta Labs

UK, 2013, $1.75M

Crypta Labs develops post-quantum encryption solutions adapted to connected objects. In particular, they propose quantum random number generators labelled Quantum Optics Module (QOM) that can be integrated into a cell phone (such as IDQ) and also work in space. The QRNG uses a LED or laser light source and a camera sensor. They are working with the University of Bristol as well as with Blueshift Memory.

Crypto4A Technologies

Canada, 2016

Crypto4A develops quantum-safe hardware security platforms rather than only entropy appliances. Its current portfolio includes QxHSM, QxEDGE and QxVault, built around the QASM cryptographic module. QxHSM supports the NIST-standardized ML-KEM, ML-DSA and SLH-DSA algorithms, as well as LMS/HSS and XMSS/XMSS-MT, with crypto-agile firmware updates for additional algorithms. In August 2026, Crypto4A announced FIPS 140-3 Level 3 certification of QASM, extending to the QxHSM, QxEDGE and QxVault product families. QxEDGE combines the quantum-safe HSM with confidential/general-purpose compute for edge and data-center deployments.

Figure 95: Crypto4A hardware-security appliances. The current product families are QxHSM, QxEDGE and QxVault.

CryptoExperts

France, 2008

CryptoExperts develops homomorphic encryption and post-quantum cryptography, and also offers services based on these technologies.

Cryptolab

USA-Italy, 2013, $800K

Cryptolab is a startup created by Massimo Bertaccini (CEO), Alessandro Passerini and Tiziana Landi (software engineers) that develops cryptographic solutions supporting AES-256 bit to secure data, particularly medical data. They are testing a new solution that "*allows transmitting a message directly via quantum channel*" which may mean a lot of things like being a QSDC. They are also working on a way to unlock a device using brain waves signatures.

CryptoNext Security

France, 2019, €11M

CryptoNext Security is a PQC software vendor founded from research at Inria, CNRS and Sorbonne University, with Florent Grosmaitre as CEO. Its current positioning is crypto-agility and migration rather than a proprietary multivariate algorithm. The 2026 product suite covers PQC evaluation, cryptographic discovery with CryptoNext COMPASS, remediation through a Quantum-Safe Library and SDKs, and centralized cryptographic-policy management with CAPTAIN. Its software supports the standardized NIST algorithms and hybrid deployments for applications, PKI, HSMs and embedded systems. The earlier GeMSS work is historically relevant but is no longer the basis of the commercial offering.

enQase

USA, 2024

enQase develops a crypto-agile quantum-safe security platform covering cryptographic discovery, migration, secure communications and integration of quantum entropy. In July 2026, its cryptographic module obtained FIPS 140-3 validation, providing independently validated cryptographic functionality for enterprise, government, critical infrastructure, IoT and edge deployments. The company also partners with other vendors to combine PQC, quantum entropy and deployable secure communications. The former "digital-QKD" terminology is too ambiguous to characterize the core offering.

Crypto Quantique

UK, 2016, $8M

Crypto Quantique secures IoT devices through a silicon hardware root of trust and a device-security management platform. QDID generates unique cryptographic identities and keys from device-level physical variability in silicon. It is a physical unclonable function rather than a photonic processor or an ID Quantique-like QRNG. QuarkLink is the associated IoT security platform for zero-touch provisioning, onboarding, certificate and fleet management, secure boot, over-the-air updates and service onboarding. The company also offers analog and digital PUF IP, lightweight root-of-trust IP, cryptographic cores, fault-injection detection and TRNG IP.

CUbiQ Technologies

the Netherlands, 2021

CUbiQ Technologies is a spin-out of Eindhoven University of Technology which develops a low-power quantum optical receiver for QKD infrastructures and a CV-QKD modem.

CyferAll

France, 2021

CyferAll is selling a messaging and communication platform embedding CRYSTALS-Dilithium and CRYSTALS-Kyber PQC end-to-end cryptography, working in memory. The offer contains D8Alock (for SaaS) and D8Ashield (to encrypt local mass storage).

Cyph

USA, 2014, $1M

Cyph sells PQC solutions. The company was created by Ryan Lester and Joshua Boehm, two engineers from SpaceX.

Dencrypt

Denmark, 2013

Dencrypt is a cybersecurity software provider protecting smartphone communications. They are working on creating PQC based solutions in partnership with the Technical University of Denmark (DTU).

EigenQ

USA, 2025, $45M

EigenQ develops a hardware-anchored "PQC+" security platform combining post-quantum cryptography, hardware-derived entropy, device identity, attestation and trusted-execution functions. Its announced product formats include PCIe and M.2 modules, embedded modules and software integration for servers, endpoints and zero-trust networks. In 2026 it announced compatibility work around Intel Xeon and AMD server platforms and a proposed business combination with Spring Valley Acquisition Corp.

evolutionQ

Canada, 2015, $5.5M

evolutionQ was cofounded by Michele Mosca and develops quantum-safe cybersecurity software and services. Its most distinctive product is BasejumpQDN, a vendor-neutral software layer for deploying and managing quantum key-exchange networks. It provides key routing, monitoring and interoperability across heterogeneous QKD devices and is described by the company as being in deployment today. BasejumpSIM complements it with cloud simulation of fiber, satellite, topology and traffic scenarios. evolutionQ also develops MultimodalKES, a cryptographic key-establishment approach intended to combine multiple primitives and integrate with existing protocols such as TLS, IPsec and MACsec. The company still provides quantum-risk assessment and migration services.

Falqon Systems

the Netherlands, 2022, €11M

Falqon Systems, formerly Q*Bird, is a QuTech spin-out created by Remon Berrevoets, Ingrid Romijn, Joshua

Slater and Joël Abrahams. The company supports Quantum Secure Networks (QSN), with combining MDI-QKD infrastructure, key management and network orchestration. It develops the Falqon family of measurement-device-independent QKD systems for multi-user networks, including user nodes, central measurement hubs and quantum switching. In June 2026, the startup introduced the Falqon Key Manager to integrate QKD-generated keys with encryption infrastructure, and its broader Quantum Domain Controller coordinates multi-node deployments. The company has moved beyond its initial Port of Rotterdam installation to additional European deployments, including multi-node networks in Ireland and Spain. In 2026 it also received EIC Accelerator support consisting of a grant and planned equity investment.

Fortaegis Technologies

the Netherlands, 2022, $65M

Fortaegis develops a hardware-rooted secure-computing and communications platform around a custom Secure Processing Unit and physically unclonable device identity. The company markets the architecture as quantum-resistant and as a full-stack security platform for governments and enterprises. It is not, however, a QKD technology and its differentiation is primarily proprietary silicon security rather than implementation of the NIST PQC standards.

Flipscloud

Taiwan, 2013

Flipscloud creates "quantum level" encryption software targeting IoT, cloud services and the big data market. It seems it is using some unspecified PQC and AES 256 bits keys. Software runs on embedded systems using Arm cores and Imagination CPUs.

fragmentiX

Austria, 2018

fragmentiX offers a secure data storage management system that uses the technique of fragmentation and distribution of data on different physical media. All this is supplied in the form of appliances.

The distributed data is of course encrypted, but in a classical way. This is another way to create data protection that is resistant to Shor's algorithm. It is not the only company positioned in this niche.

They combined their appliances with QKD equipment from IDQ and Toshiba that was available at AIT. The theoretical proposal comes from researchers of TU Darmstadt in Germany and it has already been implemented a couple of years ago in Tokyo.

GoQuantum

Chile, 2018

GoQuantum develops hardware and software for quantum-safe network security. Its current portfolio includes LS4 post-quantum secure communications terminals, PCIe and M.2 QRNG accelerators, QuantumVPN software, eSIM-oriented secure provisioning and integration of PQC with hardware quantum entropy. The company therefore combines standardized/post-quantum cryptography with QRNG hardware rather than relying on a vaguely defined "quantum radio-link encryption" scheme. Its highest-end QRNG accelerator is marketed with multi-Gbit/s effective random-bit throughput.

HEaaN CryptoLab

South Korea, 2017

HEaaN CryptoLab is specialized in the development of homomorphic encryption technology. They have their own PQC solution supporting algorithms selected during NIST's PQC standardization process, which was a standardization process and not a competition, and which produced the standardized ML-KEM and ML-DSA on top of supporting Korean's RLizard key encapsulating mechanism to embed PQC in devices and HiMQ, a PQC NIST candidate that was not selected in the 2020 round. They helped LG U+ develop its own PQC for its optical transmission equipment. Their CSO Damien Stehlé, formerly from ENS Lyon, was a key contributor to the development of CRYSTALS-Dilithium and CRYSTALS-Kyber, two of the 4 finalists of the PQC NIST competition in July 2022.

HEQA Security

Israel, 2018

HEQA Security, formerly QuantLR, develops the Sceptre quantum-safe networking platform. Its current appliances combine QKD, post-quantum cryptography and key-management functions in telecom-oriented 1U systems, with architectures for point-to-point and point-to-multipoint networks and edge deployments. The technology originated in work by Hagai Eisenberg's group at the Hebrew University of Jerusalem, including high-dimensional/time-bin QKD approaches [1094]. The former LoQomo 1 name describes an earlier generation of the company's hardware. HEQA also works with optical-transport vendors such as **PacketLight Networks** to integrate quantum-key delivery with WDM infrastructure.

Hub Security

Israel, 2017, $55M

Hub Security sells quantum secure FPGA based Hardware Security Module (HSM). These HSM modules contain QRNGs and support quantum-resistant algorithms acceleration in hardware (PQC).

IDQ

Switzerland, 2001-2025, $74.6M

ID Quantique, cofounded by Nicolas Gisin and colleagues from the University of Geneva, became an IonQ subsidiary in 2025 after IonQ acquired a controlling stake from SK Telecom. IDQ remains one of the broadest commercial quantum-communications suppliers, spanning QKD, quantum random-number generation and single-photon detection.

Its current QKD hardware is centered on the Clavis XG family. Clavis XG provides enterprise QKD, while Clavis XGR is oriented toward research and interoperability. In June 2026, IDQ launched Clavis XG Multiplex, designed to coexist with classical data channels on the same optical fiber. On the key-management side, Clarion KX is a crypto-agile platform that can ingest keys from discrete-variable QKD, continuous-variable QKD, entanglement-based QKD, PQC and other entropy/key sources. IDQ also introduced Solteris as a PQC-oriented crypto plane for integrating post-quantum key establishment into network-security infrastructure.

The QRNG portfolio continues under the Quantis family, from integrated chips to high-throughput appliances. IDQ also sells single-photon detection systems based on SPAD and SNSPD technologies, with system detection efficiencies above 90% in relevant telecom configurations and active development of photon-number-resolving SNSPD arrays [582, 1095]. IDQ also participates in satellite and quantum-network projects, including EAGLE-1. The older Cerberis and Centauris names shown in previous editions are therefore historical rather than the best representation of the 2026 portfolio.

Figure 96: Historical IDQ QKD offering from an earlier product generation. The 2026 portfolio is centered on Clavis XG, Clarion KX, Solteris and Quantis.

Icarus Quantum

USA, 2023

Icarus Quantum, founded by Poolad Imany and colleagues in Colorado, develops deterministic quantum-dot single-photon and entangled-photon sources for quantum networking. Its active US government programs in 2025-2026 target compact, high-rate entangled-photon generators for terrestrial and space-based quantum networks, using semiconductor quantum dots coupled to optical cavities. The core approach is cavity-enhanced semiconductor quantum-dot emission.

Infotecs

Russia, 1991

Infotecs is a cybersecurity and VPN supplier whose quantum-security offering now includes ViPNet QTS, a QKD system designed for integration into arbitrary-topology protected networks and for centralized key distribution to compatible encryptors. In July 2026, Infotecs announced Russian FSB certification of ViPNet QTS. The 2018 "ViPNet Quantum Phone" was an early demonstration built around a PC/VPN endpoint and external QKD equipment [1096], and should no longer be presented as the company's main QKD product.

IonQ

USA, 2016, $736M and SPAC IPO

IonQ is now showing up here on top of being a key player in the trapped-ion QPU space after a spree of acquisitions made since 2024:

- **Qubitekk**, whose acquisition of substantially all assets was completed in January 2025 after being announced in late 2024, adding entanglement-based network hardware including photon sources, detectors, optical switching and timing technology.
- **ID Quantique** with an announcement in February 2025 and completion in May 2025, for $250M, mostly with SK Telecom getting IonQ stocks for the deal. It was weird given the three product assets from IDQ are BB84 prepare-and-measure (read: no entanglement) based QKD, SNSPDs (single photon detectors) and QRNG.
- **Lightsynq** in May 2025 for $493M stock shares, who develops a NV center-based memory to be used in QPU interconnect. It led IonQ to partner in 2025 with Element Six for the manufacturing of synthetic diamond films where NV centers can be implanted.
- **Capella Space**, also in May 2025, an American aerospace company selling data and satellite solutions for government and commercial applications and using SAR (synthetic-aperture radar) satellites, using the Doppler effect to create 2D or 3D images of objects, such as landscapes or other points of interest. Supposedly, for the development of satellite-based QKD, which has not much connection with SAR technology.
- **Skyloom**, whose acquisition closed on January 28, 2026, adding free-space optical communication terminals, photonic systems engineering and secure high-

performance optical links for space and terrestrial networking.

These acquisitions, on top of Entangled Networks, acquired in 2023, were supposedly done for two reasons: one, to diversify IonQ's revenue source in quantum communications as its QPU revenue growth was not that stellar, and two, to acquire the technology needed to interconnect their QPU. This became secondary since Oxford Ionics plans to scale to thousands of logical qubits without requiring any photonic-based interconnect technology. Another reason mentioned by IonQ is the consolidation of a large pool of patents (961 granted and pending patents including 298 coming from IDQ, 118 from Qubitekk and 298 from Lightsynq).

In April, before Capella Space's acquisition, IonQ signed an MOI with Intellian Technologies (South Korea) to explore how secure quantum networking can enhance satellite communications, including satellite-to-satellite and ground-to-satellite links.

ISARA

Canada, 2015, $27M

ISARA develops post-quantum encryption software solutions and PQC implementation consulting with "ISARA Radiate Security Solution Suite" which provides public keys and encryption algorithms. They are visibly based on hash trees and combine PQC (post-quantum crypto) and traditional PKI (public-key infrastructure) [1097]. One of their investors is the Quantum Valley Investments fund, managed by Mike Lazaridis, cofounder of BlackBerry. He reinvested his BlackBerry-related fortune in the development of the Canadian scientific and entrepreneurial ecosystem, particularly in quantum, where he has invested a total of $450M [1098].

KEEQuant

Germany, 2020, $1.7M

KEEQuant, formerly InfiniQuant and spun out of the Max Planck Institute for the Science of Light, develops continuous-variable QKD for telecom networks. Its current Andariel product family uses coherent detection and Gaussian-modulated coherent states, together with the KMS1 key-management system for lifecycle management and distribution across network topologies. The 2026 Andariel Testbed specification gives a maximum tolerated channel loss of about 16 dB, corresponding to roughly 80 km of standard 0.2 dB/km fiber, with an indicative secret-key rate around 10 kbit/s under the stated test conditions.

KETS Quantum Security

UK, 2016, £8.2M

KETS Quantum Security is a University of Bristol spin-off developing integrated-photonic QKD and QRNG products. Its KETS Kore family spans packaged QKD transmitter/receiver chips, modules and full-system products, while its QRNG line ranges from packaged 5 mm × 5 mm chips and entropy boards to a PCIe card delivering up to 5 Gbit/s of post-processed quantum randomness. In 2026, KETS delivered its QKD v2.0 unit for integration into Nokia's mobile quantum-safe demonstration platform. Its differentiation remains miniaturization, low power and manufacturability through integrated photonics rather than conventional rack-scale discrete optics.

Keyfactor

USA, 2001

Keyfactor is a digital-trust, PKI and certificate-lifecycle vendor whose 2026 quantum-safe offering is centered on crypto-agility rather than QKD hardware. Its platform combines EJBCA PKI, SignServer signing, Keyfactor Command certificate lifecycle management and AgileSec cryptographic discovery/posture management. Current EJBCA and SignServer releases support post-quantum and composite certificate/signature workflows, including ML-DSA-based composite certificates, while AgileSec inventories deployed cryptography and prioritizes PQC migration.

Ki3 Photonics

Canada

Ki3 Photonics is a spin-off of the National Institute of Scientific Research on energy, materials and telecommunications from Montreal created by Yoann Jestin (CEO) and Piotr Rozgtocki (CTO). It develops compact and energy efficient QKD hardware solutions to ease its deployment over standard telecommunications links by multiplexing signals with frequency combs.

Lastwall

Canada, 2023, $27.5M

Lastwall was founded by Karl Holmqvist (CEO), Andrew McKenzie (COO), and Ian Rutherford (CTO). Its main product is IDCommand, a security hardware which integrates a PQC-ready PKI.

levelQuantum

Italy, 2023

levelQuantum was created by Magdalena Stobińska (CEO, a researcher specialized in DI-QKD [1099]), also a professor of quantum information at the University of Warsaw and Adam Buraczewski (CTO).

The company creates a QKD operating over satellite connections using a new DI-QKD (device independent, entanglement based) protocol protecting communication over long distance using twin-field light encoding and scaling, using SPDC based photon sources [1099]. It works on long distance in terrestrial and satellite mode with good key rates of 10^3 to 10^4 bits/sec for satellite and 10^7 bits per second on ground communication [1100].

The company is focused on satellite QKD, having created a communication terminal coupled to a small telescope. It operates in daylight using infrared in the 600 nm to 800 nm range. They target all satellite orbits (LEO, MEO and GEO for low, middle, and geostationary). The satellite part is developed by **Beyond Gravity** (Switzerland) handling photon swapping without the need for some quantum memory [1101, 1102].

LQUOM

Japan, 2020, $3M

LQUOM is creating and selling various MDI-QKD quantum communication systems and quantum repeaters. It supports entanglement based BBM92 QKD on dual-bands telecom on a range of 50 km [1103].

LuxQuanta

Spain, 2021, €8 M

LuxQuanta is an ICFO spin-off led by Vanesa Diaz that develops continuous-variable QKD for deployment over conventional telecom infrastructure. Its second-generation NOVA LQ system is a 2U CV-QKD appliance designed for coexistence with wavelength-division-multiplexed classical traffic and now specifies operation up to 100 km under appropriate link conditions, substantially beyond the roughly 40 km figure of the earlier generation. In 2026, LuxQuanta reported a 100 km field demonstration with live DWDM coexistence in the MADQuantum network. The company remains active in EuroQCI-related projects and integrations with cloud and edge infrastructure.

MagiQ

USA, 1999, $7.5M

MagiQ Technologies remains active in quantum cryptography alongside its defense, telecommunications and sensing businesses. Its current QPN product is a BB84-based Quantum Private Network system for QKD-protected network links. The company also sells AIMS adaptive interference-mitigation systems, CSR spectrum-recovery technology and GeoLite photonic seismic sensors. It is therefore inaccurate to present MagiQ as having effectively exited QKD, although QKD is now only one part of a broader photonics portfolio.

MtPellerin

Switzerland, 2018

MtPellerin is a startup specialized in the management of crypto assets via a dedicated mobile application ("Bridge Wallet"). They have created a quantum safe with IDQ, "The Quantum Vault", which is based on IDC's random number generator and QKD system.

NodeQ

UK, 2021

NodeQ is a software and service company dedicated to the deployment of quantum cryptography and telecommunications solutions. It was created by Stefano Pirandola and Samuel L. Braunstein. Stefano Pirandola pioneered continuous variable quantum cryptography, routing strategies on quantum networks using arbitrary topology, quantum repeaters, entanglement distillation and quantum computing optimization [1104]. After working as a MIT researcher, he became a professor of quantum computing at the University of York (UK) [1100]. With Samuel L. Braunstein, he created the hybrid quantum Internet concept, association direct and continuous variables [1105].

NuCrypt

USA, 2003-2026

NuCrypt developed optical technologies for quantum communications and metrology, including entangled-photon sources, optical pulse generators, single-photon detectors, polarization analyzers and associated software. Quantum Computing Inc acquired NuCrypt in March 2026 for approximately $5M.

NXM Labs

USA, 2016, $8.4M

NXM Labs provides PQC solutions and services for embedded systems.

Origone

UK, 2014

Origone develops cryptography solutions based on D-Wave computers. It targets the defense market as well as the railway industry. Their quantitative/post-quantum cryptography activity is an evolution of a traditional cybersecurity business.

Pauli Group

Canada, 2021

Pauli Group is a company protecting the Blockchain with PQC cryptography.

Patero

Germany, 2018

Patero develops crypto-agile network security for government, critical-infrastructure, cloud and edge deployments. Its CryptoQoR software module provides hybrid and post-quantum key establishment and is designed to let products migrate algorithms without replacing the surrounding application stack. PateroGo! and PateroGo! Plus are secure gateway products for point-to-point and multi-topology networks.

Portyq

France, 2024

PORTYQ specializes in post-quantum cryptography migration and implementation. In addition to consulting and training, it provides a PQC software library/API for integration into servers and HSM-oriented architectures, together with cryptographic assessment and hybrid-migration work. The company also follows QKD and QRNG as complementary key-distribution technologies. It therefore now has a software component offering and is not purely a consulting company, although integration services remain a significant part of its activity.

pQCee

Singapore, 2022, $6.7M

pQCee develops a broad PQC migration and secure-communications stack. Its products include inoQulate for post-quantum PKI and certificate workflows, QKDLite for key-management and QKD integration, SafeQuard for secure communications, AStablish for crypto-agility and QuICScript for quantum-computing education and emulation. It also develops quantum-safe Web3 infrastructure. In 2026, pQCee released a Windows Cryptography API: Next Generation provider supporting ML-DSA and SLH-DSA certificate operations, extending its offering from standalone applications to integration with enterprise operating-system cryptography.

PQ Solutions

UK, 2009, $10.4M

Post-Quantum, aka PQ Solutions, is a startup initially created under the name SRD Wireless that created the secure PQ Chat messaging using the random linear codes invented by Robert McEliece. The company was renamed as Post-Quantum or PQ Solutions Limited in 2014, or PQ Group. They offer a line of security products integrating post-quantum crypto algorithms. One of the cofounders, Martin Tomlinson, has developed the Tomlinson-Harashima pre-encoding, which corrects interference in telecommunication signals and various error correction codes. Their products also include PQ Guard, a post-quantum encryption system. Their CEO, Andersen Cheng is also the CEO of **Nomidio** (2020, UK), a provider of quantum-proof identity solutions, the Nomidio Private Identity Cloud.

PQSecure Technologies

USA, 2017

PQSecure Technologies, founded by Reza Azarderakhsh, develops software and silicon-ready cryptographic IP with side-channel protection. Its current hardware portfolio supports NIST-standardized ML-KEM (FIPS 203), ML-DSA (FIPS 204) and SLH-DSA (FIPS 205), together with stateful hash-based signatures, classical public-key primitives and symmetric cryptography for FPGA, ASIC and SoC integration.

PQShield

UK, 2018, $63.9M

PQShield is an Oxford University spin-off specializing in production-grade PQC software and hardware IP with side-channel protection. Its current software portfolio includes PQMicroLib-Core for constrained systems and PQCryptoLib-Core/PQCryptoLib-SDK for general-purpose software and OpenSSL integration. Its hardware portfolio includes PQPlatform-CoPro and PQPlatform-TrustSys, plus the high-performance PQPerform-Flare, Inferno and Flex accelerators. These products support NIST-standardized ML-KEM and ML-DSA, with crypto-agile support for additional algorithms and hybrid classical/PQC schemes.

Project Eleven

USA, 2024, $20M Series A

Project Eleven develops post-quantum infrastructure for digital assets, with particular emphasis on Bitcoin and other public blockchains. Its current tools include the Bitcoin Risq List, which inventories coins exposed through published public keys, Quantum Vault for post-quantum custody/key protection, and the open-source libqc cryptographic library. The company also works with blockchain ecosystems including XRP Ledger on migration to quantum-resistant signatures. It raised a $20M Series A in January 2026.

The company's Q-Day Prize produced a highly publicized 15-bit elliptic-curve demonstration in April 2026. The demonstrated key space was tiny, and the circuit did not establish scalable quantum cryptanalysis of real-world elliptic-curve keys. The interpretation of the result was criticized by Craig Gidney [89].

Qaisec

Bulgaria, 2019

Qaisec develops cryptographic solutions targeting the AI, finance and telecommunications sectors. They seem to offer first a security audit service and then cryptography solutions that use quantum random number generators for keys. They are also creating a PQC-based blockchain.

QANPlatform

Estonia, 2019, $15M

QANPlatform was cofounded by Johann Polecsak (CTO) and is providing a quantum-proof Blockchain relying on a Lattice-based PQC (CRYSTALS-Dilithium) implemented in the RUST programming language.

Qabacus

USA, 2019

Qabacus is developing quantum computing and cryptography technologies and a complete cyber-security software stack.

Qasky

China, 2016, $7.6M

Qasky, also known as Wentian Quantum, commercializes quantum-security technology originating from the Chinese Academy of Sciences ecosystem. Its 2026 catalog includes long-distance and card-format QKD terminals, local QKD equipment, key-management and network-management systems, QRNGs, single-photon/photonic components, quantum-safe gateways and switches, and tools for assessing cryptographic assets and quantum vulnerability. The company therefore spans QKD hardware, quantum entropy and PQC/crypto-migration products.

Figure 97: The Falqon MQS4000 Quantum Switch.

QCi

USA

QCi, aka Quantum Computing Inc, is primarily a photonic quantum-computing and integrated-photonics company but now also owns a quantum-communications product line. In March 2026 it acquired NuCrypt for approximately $5M, bringing entangled-photon sources, pulse-generation equipment, single-photon detection, polarization-analysis hardware and associated quantum-optics software into QCi. This is a more concrete current quantum-communications offering than the company's older patent-licensing activity around QKD.

QEYnet

Canada, 2016, $7M

QEYnet is developing a QKD quantum cryptography satellite network. Funding for the startup comes from the Canadian government.

QLocked

Turkey, 2022

QLocked is a spin-off of the İzmir Institute of Technology (IZTECH) by Serkan Ateş (CEO) and Ömer S. Tapşın (CTO). The company develops solid-state quantum-dots and color center based single-photon and entan-gled-photon-pair sources, with a bet on hexagonal boron nitride (hBN) for the creation of room-temperature sources [1106, 1107]. They also de-velop QKD subsystems built on those emitters, targeting fiber, free-space, and underwater channels [1108], along with an autonomous fiber coupling system for quantum sources. The third activity is consulting and training covering quantum computing, communication, imaging and sensing.

QNu Labs

India, 2016, $40M

QNu Labs develops an integrated quantum-safe security platform branded QShield. Its hardware products include Armos for QKD and Tropos for quantum random-number generation, while Hodos provides post-quantum cryptography. The broader stack includes Q-ORE orchestration/key-management, QConnect secure file exchange, QVerse secure messaging and Entropy-as-a-Service. QNu therefore combines QKD, QRNG, PQC and key-management software.

Qrate Quantum Communications

Russia, 2015

Qrate Quantum Communications sells QRate Key Distributor, a BB84 protocol-based QKD quantum key distribution solution in a 4U rack with a range of up to 100 km [1109].

They also market a single-photon avalanche diode detector (SPAD) operating at 1,550 nm and a quantum random number generator (QRNG).

QSpace Technologies

Russia, 2017, $1M

QSpace Technologies originated as a Russian Quantum Center/QRate spin-off working on CubeSat-based QKD. Earlier material announced a QKD-transmitter CubeSat for a 2023 launch, but I did not find sufficiently current public evidence confirming a 2026 commercial satellite-QKD product or the completion of that launch plan.

QTI

Italy, 2020

QTI, Quantum Telecommunications Italy, develops and manufactures reconfigurable discrete-variable QKD systems. Its Quell-X family consists of Alice and Bob units using decoy-state BB84 and operating in the optical C-band or O-band, not in a microwave C-band. Quell-X, Quell-XC and Quell-XR respectively target standard QKD, integrated encryption and research use. The company also offers a Key Management Entity, a QSDN software-defined networking layer aligned with ETSI GS QKD 015, and Ekate, introduced for scalable

QKD/PQC crypto-agility. In 2026, QTI demonstrated a Rome-Naples hybrid architecture in which local Quell-X QKD networks were interconnected through a PQC backbone.

Qtlabs

Austria, 2013

Qtlabs is a company providing ground stations for satellite QKD distribution, the Optical Ground Station 400 and 800 as well as prepare and satellite measure and entanglement based photon sources.

Qtonic Quantum

Israel, 2024

Qtonic Quantum Corp, formerly Qryptonic, is an Israeli company with headquarters in the USA that provides security testing, cryptographic risk assessment and PQC migration planning. Its product line contains three services: QScout for cryptographic risk and vulnerability intelligence, QStrike for quantum penetration testing, and QSolve for PQC migration advisory. They use LLM26, a 70-billion-parameter LLM specialized in quantum physics, cryptography, and cybersecurity, which designs QStrike test campaigns and interprets QScout findings. They launched in 2026 the Qtonic Quantum Lab, a vendor-neutral quantitative scoring platform for PQC implementations, evaluating 215 PQC implementations across 12 categories including cryptographic libraries, HSMs, certificate management platforms, browsers, VPNs, and silicon providers.

QuantiCor Security

Germany, 2017

QuantiCor Security develops PQC solutions, particularly for Blockchain applications and connected objects, via offerings with Quantum-Multisign and Quantum IDEncrypt, which are supposed to be cheaper than traditional PKIs. They come from TU Darmstadt and target the healthcare market in particular.

Quantum Bridge

Canada, 2019, $600K

Quantum Bridge is a startup created by Mattia Montagna (CEO) and Hoi-Kwong Lo (CTO) that provides a proprietary symmetric key distribution solution labelled DSKE (Distribution of symmetric key exchange) based on QKD. The offer contains Quantum Bridge KME, Security Hub, Black Phone (a mobile application that uses pre-shared symmetric keys) and a Client SDK. They are also working on the creation of photonic graph states which could be potentially used in quantum repeaters [1110].

Quantum Collective

the Netherlands, 2021

Quantum Collective is a European company created by Fabien Bouhier, Sebastien Le Goff and Floris Drupsteen that provides post-quantum security solutions. They name this "Quantum Security Solutions" but it's classical quantum-resilient security covering PKI, VPN and eMail security.

Quantum Corridor

USA, 2023, $10M

Quantum Corridor is a for-profit company that deployed a quantum communication network in the USA, from Chicago to nearby Indiana state over 172 miles, to be extended to Indianapolis.

Quantum2Pi

Italy, 2024

Quantum2Pi is a company created by Ugo Chirico (CEO and CTO) and Salvatore Cuomo (CSO) which proposes various PQC and QKD solutions, but also quantum machine learning. Their PQC offering contains Kylerlib and Dilithiumlib to deploy the eponymous PQC NIST standards, and QGram, a PQC-based emailing solution.

Quantum B

Poland, 2020

Quantum B, formerly Quantum Blockchains, was founded by Mirek Sopek, Xin Sun and Piotr Kulicki [1111, 1112]. The company officially adopted the Quantum B name on May 29, 2026 as its scope broadened from blockchain security to quantum-safe cybersecurity for communications, identity, critical infrastructure and digital assets. It continues to develop its Quantum Secured Blockchain (QSB), combining QKD, QRNG and PQC, and has demonstrated QSB integration with QNu Labs QKD equipment. Its broader work includes quantum-safe migration tooling, identity infrastructure and QKD simulation, while retaining blockchain as one application domain.

QuantumCTek

China, 2009

QuantumCTek is a provider of end-to-end quantum cryptography solutions: QKD, QKD repeaters, optical routers. The company is a spin-off of Hefei National Laboratory for Physical Science at Micro-scale (HFNL) and the University of Science and Technology of China (USTC).

It lived or lives with many other names: Anhui Quantum Communication Technology, National Shield Quantum, Guodun Quantum, Anhui GuoDun quantum Cloud Data

Technology, Xinjiang GuoDun Quantum Information Technology, on top of its holding subsidiary Shandong Guoxun quantum core technology Co. The company was created by Peng Chengzhi and Zhao Yong with the help from Jian-Wei Pan. They are behind the creation in 2014 of the "Quantum-Safe Security Working Group" with ID Quantique and Battelle, which promotes PQC. They deployed the 2000 km QKD-protected link between Shanghai and Beijing. They also develop their homegrown QRNG solution that seems to fit into a SIM card.

The company also manufactures control electronics, thermometers and dilution refrigerators. They ran an IPO (Initial Public Offering) in China in July 2020 and in March 2024, China Telecom invested in the company for $265M and obtained a 41.36% voting rights in the company.

Quantum Impenetrable

UK, 2018

Quantum Impenetrable is a Scottish startup that develops a security module (HSM) using a quantum random number generator and resistant to quantum key-breaking algorithms.

Quantum eMotion

Canada, 2007, $12.75M

Quantum eMotion, formerly Quantum Numbers Corp, develops QRNG technology based on the stochastic timing/noise of electron tunneling through a potential barrier. Its current portfolio is organized around the eQ family, including eCore-Q quantum-entropy IP, eFlux-Q and eCrypto-Q security modules and the eHot-Q hardware-security product, with additional eCMOS-Q, eSOC-Q and eVault-Q integration targets. The company reports gigabit-scale entropy generation for eCore-Q and is working with semiconductor partners to combine its QRNG with hardware roots of trust and physically unclonable functions. The technology is a licensable/integrable quantum entropy IP and security hardware than as a USB-key QRNG or a blockchain product [1113].

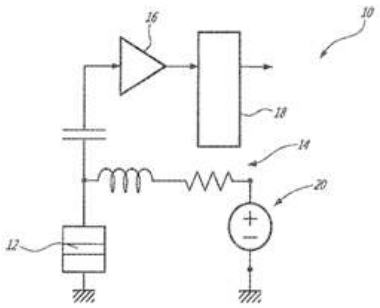


Figure 98: Electron-tunneling QRNG concept used by Quantum eMotion.

Quantum Optics Jena

Germany, 2020, €8.5M

Quantum Optics Jena develops entanglement-based quantum-communication hardware. Its product families include Elvis QKD systems, HD entangled-photon-pair sources at several wavelength bands, PAM polarization-analysis modules and associated control/software components. It also develops subsystems for fiber and free-space/satellite quantum links, including compact payload-oriented photon sources and receiver components.

QuantumPrime

Germany, 2024

QuantumPrime is an engineering company created by Anna Beata Kalisz Hedegaard that provides services for the development of space-based Entanglement as a Service (EaaS).

Quantum Trilogy

USA, 2016

Quantum Trilogy created a secure communications solution based on applications (including for mail and voice communication) protected by an unspecified encryption, a QRNG to create real entropy in generated keys and servers that are protected at some level by a QKD.

Quantum Xchange

USA, 2016, $23.5M

Quantum Xchange develops Phio TX, a crypto-agile key-delivery and network-encryption platform that can combine standardized PQC, conventional cryptography and externally supplied QKD keys. Current deployment formats include software/cloud, appliance and embedded/containerized implementations, with centralized management introduced in 2026. The platform supports FIPS 203 ML-KEM and hybrid operating modes, allowing customers to migrate existing links without requiring a dedicated QKD network.

Quantum Xchange's earlier 1,000-km Boston-Washington QKD backbone and partnerships with Zayo, Cisco and Thales remain relevant deployment history [1114, 1115], but the current product positioning is broader and primarily crypto-agile network protection rather than operation of a single QKD corridor.

QuBalt

Germany, 2015

QuBalt is a startup established between Germany and Latvia that develops solutions for post-quantum cryptography (PQC) and quantum algorithms.

Qubit Reset

USA, 2018

Qubit Reset develops proprietary cryptographic and quantum-communication protocols rather than a clearly documented commercial quantum-repeater appliance. Its current site presents protocols for quantum repeaters, dynamic symmetric cryptography, cloud key generation/storage, secure mobile communications and AI-assisted emulation of quantum processes, together with its "Crypto Capsule on the Cloud" concept. The company remains early stage and public technical validation is limited, so its offering should be described as protocol/IP development rather than deployed repeater hardware.

Qubitrium

Turkey, 2020

Qubitrium provides entangled photon sources, SPAD photon detectors and a CubeSat bundle for QKD experiments. It also works on distributed quantum time measurement [1116].

QUBO Technology

Austria, 2023

QUBO Technology is a spin-off from the University of Vienna created by Borivoje Dakic, Philip Walther and Stefan Fürnsinn. Their stated mission is "*to bring Quantum for EveryBody by introducing innovations that address real-world problems, grounded in quantum technologies*" which is kind of imprecise.

They seem to have a two-pronged product strategy. One is with PayTech, a quantum tokenization securing their payment system, seemingly using some sort of QKD [1117]. The other is BrainTech, which "*enables computers to work like the human brain*".

It is based on their homemade photonic quantum memristors to implement quantum reservoir computing for image classification and sequential data analysis [1118]. It remains a small-scale prototype.

QuDef

USA, 2024

QuDef is a quantum-security company created by Michal Krelina and Bo Dirks. Its SQOUT platform entered commercial availability in June 2026 and provides quantum-communication threat intelligence, QKD security assessment and implementation testing. SQOUT is offered as SaaS, on-premises software and expert service. QuDef is primarily a verification, threat-modeling and security-assessment vendor for quantum communications.

QuDoor

China, 2016, $7.8M

QuDoor, *aka* Qike Quantum or Guokai Quantum Technology, sells a broad quantum-communications hardware catalog. It includes QKD terminals, QRNGs, single-photon detectors, WDM/optical networking equipment, quantum optical switches, key-injection/key-management equipment and integrated QKD photonic chips. Its QOIC-280 silicon-photonics device integrates a decoy-state BB84 time-phase transmitter in a millimeter-scale die and supports clock rates up to the GHz range. QuDoor also works on trapped-ion computing and quantum sensing, but those activities are outside this QKD/PQC vendor inventory.

QIZ Security

USA and Israel, 2025, $17M

QIZ Security is a PQC migration platform vendor created by Ben Volkow, Itan Barmes and Lenny Ridel. They provide a SaaS platform to plan for PQC deployment.

QuintessenceLabs

Australia, 2006, $49.3M

QuintessenceLabs provides a broad quantum-enhanced cybersecurity portfolio. It includes the qStream 100/200 quantum random-number generators, with the qStream 100 providing up to 1 Gbit/s of conditioned quantum entropy, qRand entropy-management software, the Trusted Security Foundation key and policy-management platform, TSF Sentry for cryptographic asset discovery and crypto-agility, qOptica 100 for continuous-variable QKD, qConnect for PQC/QKD key distribution, qClient SDKs and qProtect secure-data protection. The portfolio now spans QRNG, key management, CV-QKD, standardized PQC integration, cryptographic discovery and remediation.

Qulabs

India, 2018

Qulabs is a jack-of-all-trade typical startup in India, created by Nixon Patel (CEO). It works in many fields like with the development of quantum inspired machine learning algorithms, building quantum memory storage (using their own software simulation tools) and finally, quantum secure direct communication (QSDC) sending quantum data without encryption or keys and quantum conference protocols (QCKA). They also developed a blind quantum computing simulator.

Qunnect

USA, 2017, $12.4M

Qunnect is a Stony Brook University spin-off created by Noel Goddard, Mael Flament, Mehdi Namazi and Eden Figueroa. It develops room-temperature hardware and control systems for distributing photonic entanglement over metropolitan telecom fiber. Its current commercial offering is centered on the Carina turnkey entanglement-

distribution system, which packages sources, stabilization, synchronization, networking and verification functions needed for deployed quantum links.

Qunnect has operated metropolitan test networks including GothamQ in New York and has moved toward multi-vendor network integration. In February 2026, Qunnect and Cisco reported deployed entanglement swapping over 17.6 km of fiber, with roughly 5,400 successfully heralded entangled pairs per hour in the reported configuration. The company's earlier QU-SOURCE, QU-MEM, QU-SWAP and related component names describe the technology building blocks behind this more integrated network product. [1119, 1120]

In May 2022, the company got two SBIR awards from the US DoE for $1.85M to fund the development and commercialization of their quantum repeater product suite. In October 2022, the startup got a series A funding of $8M led by Airbus Ventures Qunnect officially announces its Series A financing of over $8 million. The round was led by Airbus Ventures with Quantonation, SandboxAQ, NY Ventures, Impact Science Ventures and Motus Ventures as other investors.

In April 2025, Deutsche Telekom's T-Labs and Qunnect announced having achieved "a fidelity of 99% for the transmission of polarization-entangled photons over 30 km of commercial fiber for 17 consecutive days" [1121]. This was documented in details in two arXiv preprints [1122, 1123]. So, did they obtain sustained fidelities of 99%? It seems that these fidelities had a range from 85% to 99% and that 99% was the maximum and not the average. These are still excellent results according to their own comparison with other similar testbeds (Table I in [1122]).

The company partners with various technology vendors like Exail, Toptica, Q-CTRL, ColdQuanta and Single Quantum. It announced in 2023 the deployment of a new fiber loop expanding its existing quantum networking testbed GothamQ, from Brooklyn to Manhattan, connecting New York University to the Navy Yard. It was operational in 2024.

QuNETT

USA, 2022

QuNETT, aka Quantum Network Technologies, is developing quantum repeaters operating on existing telecom infrastructures.

Quranium

UAE, 2024

Quranium develops a "quantum-native" Layer 1 blockchain embedding PQC. The goal is to create a "Decentralized Quantum-Uncrackable Infrastructure Protocol" (DeQUIP) to secure digital transactions and "Web3" infrastructure from future quantum computing threats. The CEO is based in India and his two cofounders in Dubai.

QuSecure

USA, 2019, $42M

QuSecure develops QuProtect R3, a software-only post-quantum cryptography and crypto-agility platform. It inventories deployed cryptography, produces cryptographic bills of materials, and can protect traffic at the network layer without rewriting applications. The platform supports ML-KEM, ML-DSA and SLH-DSA, hybrid X25519MLKEM768, TLS 1.3, IPsec and related enterprise protocols, with cloud, on-premises and air-gapped deployment models. QuSecure also works with US government and defense customers.

SandboxAQ

USA, 2022, $975M

SandboxAQ is an Alphabet spin-out active in AI, sensing and cybersecurity. Its current cybersecurity platform is AQtive Guard, which covers cryptographic discovery, inventory, risk analysis, policy enforcement, crypto-agility and PQC migration. Its remediation layer is designed to replace or reconfigure cryptography without wholesale application or operating-system re-engineering. SandboxAQ also maintains the open-source Sandwich cryptographic API layer [1124]. Beyond cybersecurity, the company develops Large Quantitative Models for scientific and industrial applications and acquired Good Chemistry in 2024. The product formerly described simply as the "Security Suite" is now better identified by the AQtive Guard brand.

Secure-IC

France, 2010-2025

Secure-IC, now a subsidiary of Cadence, develops embedded security IP, secure elements and cryptographic accelerators. Its current PQC portfolio includes hardware/software implementations of ML-KEM and ML-DSA together with hash-based signature families such as LMS/XMSS and SLH-DSA, integrated into its Securyzr secure-element/IP architecture. The Analyzr platform supports evaluation of side-channel and fault-attack resistance.

SECQAI

UK, 2021

SECQAI is a quantum cybersecurity and applications company created by Rahul Tyagi, Dave Worrall and Martin Rudd with a broad goal to "*provide world leading technologies to organisations of all sizes*". Rahul Tyagi developed a patented room temperature QRNG when he was the CEO of LyfGen. The patent USPTO 10606561 was filed in August 2018 and validated in March 2020. It is based on using slits-based diffraction and scattering entropy. The company develops and integrates a PQC accelerator in silicon IP cores that are provided to SoC (system-on-chip) designers targeting the embedded and IoT space. Applications wise,

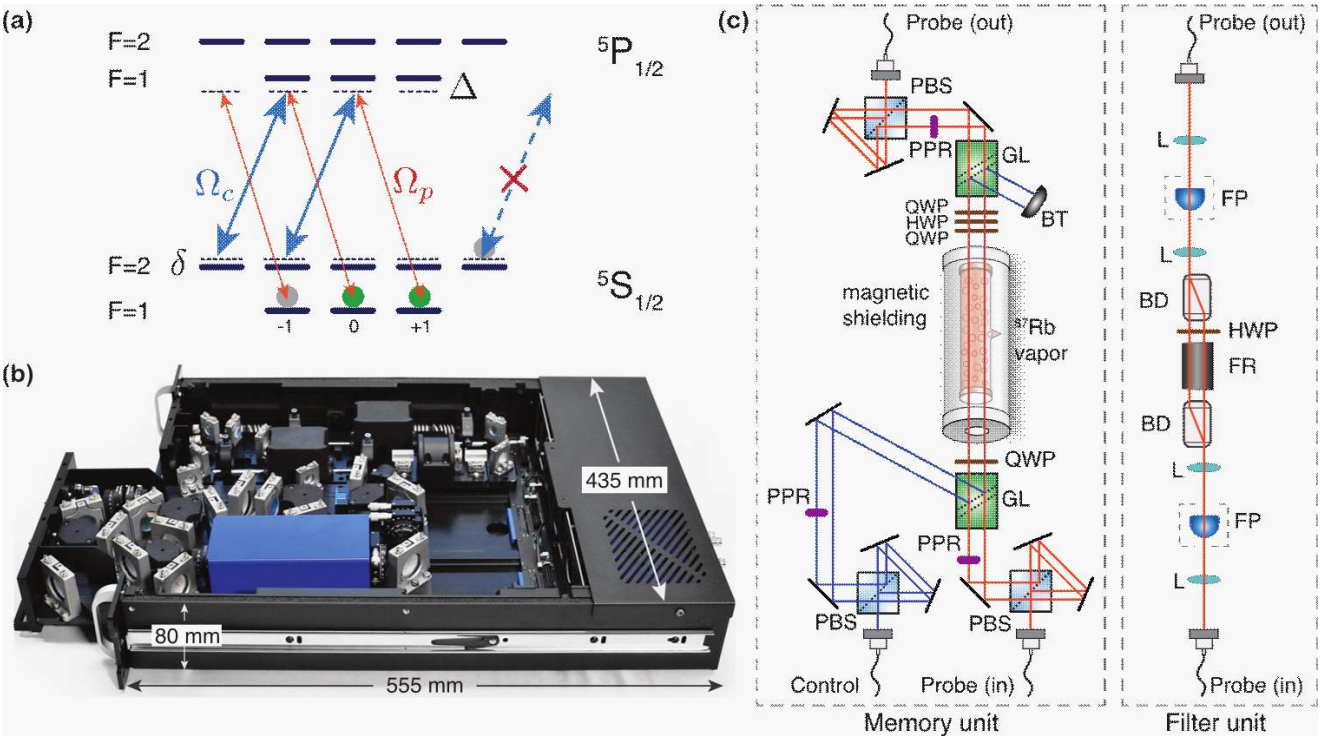


Figure 99: Qunnect repeater architecture. Source: [1119].

they developed quantum and machine learning solutions on logistics optimization, multidimensional intelligence data analysis and hyperspectral image data analysis.

In February 2025, the company launched the "first" hybrid Quantum Large Language Model (QLLM). There's no public information on how itleverages quantum computing.

Smarts Quanttelecom

Russia, 1991

Smarts Quanttelecom proposes a quantum cryptography solution based on CV-QKD which exploits standard fibers of telecom operators. Smarts was until 2015 a Russian mobile telecom operator. It has since become a telecom services operator with an offer of secure telecom links and data center and cloud services. Their QKD solution comes from Quanttelecom, a subsidiary of Smarts, developed jointly with the ITMO University of Saint Petersburg.

SpeQtral Quantum Technologies

Singapore, 2017, $10M

SpeQtral Quantum Technologies, formerly S-Fifteen Space Systems, develops both terrestrial and satellite quantum-secure communications. Its SpeQtre satellite was launched in November 2025 and entered quantum-communications experimentation in 2026. SpeQtral-1 is the follow-on commercial technology-demonstration program. The company also deploys fiber QKD and combines satellite QKD, terrestrial QKD and PQC in architectures intended to provide quantum-safe connectivity across long geographic distances.

SSH Communications Security

Finland, 1995, €14.1M

SSH Communications Security sells NQX, a Layer-2/Layer-3 network encryptor designed for quantum-safe high-speed links up to 100 Gbit/s. Current versions support hybrid post-quantum key establishment, including ML-KEM and FrodoKEM-based modes, and NQX has obtained Finnish security certification for classified use. The older Tectia Quantum Safe Edition was an early PQC-protected SSH product, but NQX is now the more representative commercial offering for this section.

STMicroelectronics

Switzerland

STMicroelectronics has a broad quantum-ready hardware and software portfolio. In June 2026, it introduced ST54M, a single-die secure mobile chip combining NFC, embedded secure element, eSIM and a hardware accelerator for ML-KEM and ML-DSA. ST also supports PQC through STM32 and STM32MP general-purpose devices, Stellar automotive microcontrollers, STSAFE-TPM products, the X-CUBE-CRYPTOLIB software library and NesLib-PQML libraries for secure microcontrollers. These products use hardware SHA-2/SHA-3 or dedicated PQC acceleration depending on the family.

Synergy Quantum

Switzerland, 2019

Synergy Quantum is a post-quantum encryption product and service startup that also supports data storage in a facility located in a former military bunker in the Swiss Alps.

They target the government, financial services, healthcare, smart city, energy and telecom sectors. The company is run by Jay Oberai (CEO), Arun K. Pati (Chief Scientific Officer), Mayank Sharma (VP Engineering), Vipin Kumar Rathi (VP Technology Architecture) and Manu Khullar (Chief Operating Officer). The leadership team also includes John Paukulis (CMO), Sasha Lazarevic (Head of Government Partnerships) and Jake Hwang (Head of Business Development and Investor Relations). It launched in 2022 a joint venture with the Quantum Technology Hub of the Indian Government. They seem to also offer some services in the QKD realm, including some that are provided as part of this deal in India.

Taqbit Labs (2018, India) sell solutions for QKD. Their website and communication are so vague that it's impossible to understand whether they sell third party QKD products with some integration service of develop QKD hardware products of their own, and if so, in what category given most vendors don't reinvent the wheel to become full-stack vendors.

Terra Quantum (Switzerland) is also working on QKD. In 2023, it announced a world record for long-distance QKD operating with optical-fiber cables over 1,032 kilometers at a (relatively) high key rate of 34 bits per second [1125].

Thales

France

Thales launched Luna 8 in August 2026, its next-generation Hardware Security Module with an architecture designed for crypto-agility and post-quantum deployment. Thales also provides High-Speed Encryptors, PQC migration services and hybrid classical/PQC protection for network and web-security products, including TLS 1.3 configurations combining classical key exchange with ML-KEM. On the quantum-cryptography side, Thales commercializes QKD-compatible network encryptors and integrates quantum random-number generation in parts of its security portfolio.

TheGreenBow

France, 1998

TheGreenBow is an old VPN cybersecurity company. Its MinInt now supports a PQC. They partner with CryptoNext Security. They are part of a consortium created with Thales for the creation of end-to-end PQC solutions.

ThinkQuantum

Italy, 2021

ThinkQuantum is a University of Padua spin-off developing QKD, QRNG and free-space/satellite quantum-communication systems. Its QUKY product is a polarization-encoded BB84 QKD platform for fiber links, complemented by QRNG devices and optical subsystems for terrestrial and space quantum links. The company therefore spans deployable fiber QKD and satellite-oriented quantum communications rather than only research prototypes.

Transilvania Quantum (2023, Romania) provides PQC and quantum-technology advisory services.

Utimaco

Germany, 1983

Utimaco offers Quantum Protect as an in-field upgrade for its u.trust General Purpose HSM Se-Series. The package supports ML-KEM (FIPS 203), ML-DSA (FIPS 204), LMS/HSS and XMSS/XMSS-MT, with SLH-DSA on the roadmap. Implementations of ML-KEM, ML-DSA and LMS passed NIST CAVP testing in 2025. A downloadable simulator is available for integration testing before deployment. The former emphasis on Picnic, an alternate NIST candidate, no longer represents the product line.

Vergence

USA, 2024

Vergence is a stealth startup cofounded by William Dean (CEO) in Boston doing cybersecurity consulting for the deployment of PQC. They also plan to create a semi-quantum system supporting 192 logical qubits and bringing superpolynomial time speedup, which looks like a classical emulator supporting tensor network compression.

VeriQloud

France, 2017

VeriQloud is a startup created by Elham Kashefi, and Marc Kaplan (France) and Joshua Nunn (UK). It is specialized in the creation of quantum software solutions adapted to quantum telecommunications for both QKD and distributed quantum processing.

Their offer is based on Qline, a software solution that enables the deployment of a multi-point quantum network with a lower cost in hardware infrastructure (Figure 100).

With this architecture, nodes that are very expensive can be replaced by simple modulators that are much more affordable. The operation is based on a kind of "time-sharing" of the line [1126]. This lowers the hardware addition by about two thirds on a typical installation below with two intermediate stations in the network.

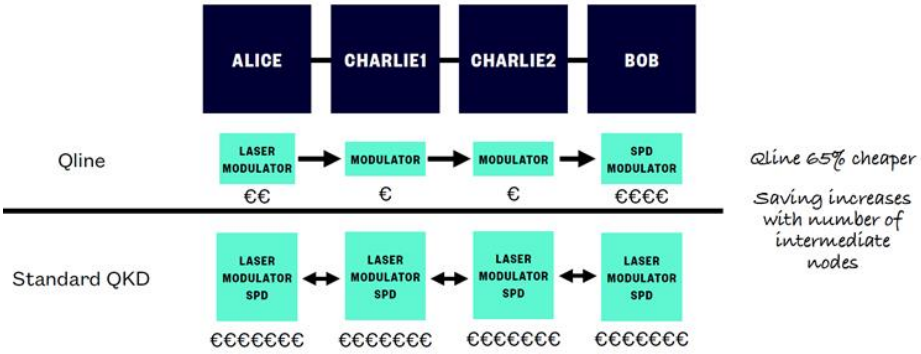


Figure 100: VeriQloud qline architecture. Source: VeriQloud.

At both ends of the line there is on one side a laser and modulator-based photon generator and on the other side a single photon detector, the most expensive part of the equipment ranging from €20K to €100K. The solution is deployable on networks totaling 100 to 200 km.

The first application is QKD quantum key distribution. They can interoperate with classical QKD networks. Initially, secure file transfer and instant messaging are targeted as applications associated with QKD. The system can also be used to generate disposable masks [1127].

The VeriQloud solution is also relevant for securing data storage. It has also been tested at a small scale for blind computing architecture [1128, 1129].

WISeKey Semiconductor

Switzerland, 1999, $256M

WISeKey Semiconductor is a cybersecurity, AI, Blockchain, and IoT company that developed QUASARS (QUAntum resistant Secure ARchitecures project), a RISC V platform base security solution supporting PQC cryptography.

SEALSQ

Switzerland, public company, $125M 2026 offering

SEALSQ, spun out of WISeKey, develops secure semiconductors, PKI and post-quantum hardware. Its 2026 portfolio is centered on the QS7001 post-quantum secure element and the QVault TPM family. QS7001 is a secure RISC-V platform designed for ML-KEM and ML-DSA, obtained NIST SP 800-90B Entropy Source Validation in May 2026, and passed major fault-injection and side-channel testing milestones toward Common Criteria EAL5+ certification. QVault is positioned as a post-quantum-capable hardware root of trust for hybrid and crypto-agile systems.

Wultra

Czechia, 2014, €6.8M Series A

Wultra develops authentication and digital-identity security for banks and fintech companies, with a strong focus on phishing resistance and post-quantum migration. In June 2026 it raised a €6.8M Series A to accelerate the international expansion of its post-quantum digital-identity products. Its offering is primarily software for mobile authentication and identity rather than PQC hardware.

Xiphera

Finland, 2017, €480K

Xiphera is providing hardware-based security solutions, including their PQC based xQlave product family IP cores that can be used in FPGA and ASIC circuit designs. It supports the standardized descendants of CRYSTALS-Kyber and CRYSTALS-Dilithium, namely ML-KEM and ML-DSA, in hardware IP for FPGA and ASIC integration.

XT Quantech

China, 2017

XT Quantech specializes in CV-QKD distribution equipment after initially focusing on DV-QKD solutions. The CV-QKD is essential because it can coexist in the fiber links of telecom operators.

They offer server appliances for QKD key encoding and decoding gateways. Its full name is Shanghai Xuntai Information Technology Co. The company also sells a QRNG, their XT-QRNG100 that is certified in …China.

XunTai Quantum Technology Co (China) is a QKD company for which I could not identify a public technical website as of September 2026. They contribute to securing CV-QKD infrastructures [1130].

ZeroRISC

Austria, 2023, $15M

ZeroRISC is a company created by Dominic Rizzo, who led the original OpenTitan project launched at Google in 2019 to create an open-source silicon root of trust. Their product is a com-mercial cloud security service built around the OpenTitan Earl Grey discrete chip design, delivered jointly with Nuvoton Technology Cor-

poration and Winbond Electronics. The chip is a hardware root of trust (RoT) for motherboards, network cards, laptops, phones, and IoT devices. It is brought together with the Integrity Management Platform (IMP) which provides an end-to-end security from fabrication to field deployment across silicon supply chain partners. ZeroRISC's Cryptolib includes hardware-accelerated implementations of the three NIST PQC algorithm families (ML-KEM, ML-DSA, and SLH-DSA aka SPHINCS+).

zerothird

Austria, 2023, €10M

zerothird, formerly Quantum Industries, develops entanglement-based QKD infrastructure and offers quantum keys as a managed service. Its architecture combines entangled-photon sources, high-efficiency single-photon detection, network-control software and integration with conventional encryption systems. In 2026 the company reported pilots and network deployments with telecommunications, banking and networking partners, including links extending beyond Austria. The former statement of a generic "300 km" product range is removed because achievable secure-key distance depends strongly on fiber loss, detector configuration and network architecture.

Figure 101: zerothird QKD endpoint from an earlier product generation.

ZeroTier

USA, 2013, $15M

ZeroTier provides a software-defined peer-to-peer networking platform. Its ZeroTier Quantum branch adds hybrid post-quantum cryptography to the ZeroTier Transport Protocol so that quantum-safe protection is applied at the overlay-network transport layer. As of June 2026 the company had released ZeroTier Quantum RC2, positioning the product for CNSA 2.0/NIST-aligned deployments and approaching general availability. It should therefore be described as a 2026 release-candidate product rather than as a mature platform already generally launched in March 2026.

1.7.1 Bibliography and notes

These are the bibliographical references and notes for the **QKD and PQC vendors** subsection.

[89] The predictable failure of the QDay Prize, by Craig Gidney, Craig Gidney's blog, April 2026.

[135] Breaking Rainbow Takes a Weekend on a Laptop, by Ward Beullens, Advances in Cryptology - CRYPTO 2022, August 2022 (16 pages).

[582] GHz detection rates and dynamic photon-number resolution with superconducting nanowire arrays, by Giovanni V. Resta, Félix Bussières, et al., arXiv, June 2023 (28 pages).

[925] Telecom-heralded entanglement between remote multimode solid-state quantum memories, by Dario Lago-Rivera, Samuele Grandi, Hugues de Riedmatten, et al., Nature, June 2021.

[1075] New CIR Report States Quantum Encryption Market To Reach $2.5 Billion Revenues By 2022: Mobile Systems Will Ultimately Dominate, by Robert Nolan, June 2017.

[1076] IBM's Cryptography Bill of Materials to speed up quantum-safe assessment, by Alessandro Curioni et al., December 2022.

[1077] Intel Labs Establishes Crypto Frontiers Research Center, by Intel, 2021.

[1078] Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations, by Fabian Laudenbach, Philip Walther, Hannes Hübel, et al., arXiv, May 2018 (71 pages).

[1079] Announcing the AWS Center for Quantum Networking, by Denis Sukachev et al., June 2022.

[1080] HP Launches World's First Printers to Protect Against Quantum Computer Attacks , by HP, HP, March 2025.

[1081] Quantum Communication with Quantum Dots Beyond Telecom Wavelengths via Hollow-Core Fibers, by Lorenzo Carosini, Christopher Hilweg, et al., arXiv, September 2025 (8 pages).

[1082] Distribution of Telecom Entangled Photons through a 7.7 km Antiresonant Hollow-Core Fiber, by Michael Antesberger, Philip Walther, Lee A. Rozema, et al., arXiv, June 2024 (11 pages).

[1083] Phase noise characterisation of a 2-km Hollow-Core Nested Antiresonant Nodeless Fibre for Twin-Field Quantum Key Distribution, by Mariella Minder, Marco Lucamarini, et al., arXiv, December 2025 (8 pages).

[1084] A Hybrid Integrated Quantum Key Distribution Transceiver Chip, by Joseph A. Dolphin, Taofiq K. Paraiso, Han Du, Robert I. Woodward, Davide G. Marangon, and Andrew J. Shields, arXiv, August 2023 (13 pages).

[1085] Abelian (ABEL) – A Quantum-Resistant Cryptocurrency Balancing Privacy and Accountability, by Alice et al., February 2022 (140 pages).

[1086] Long-range QKD without trusted nodes is not possible with current technology, by Bruno Huttner, Romain Alléaume, Eleni Diamanti, Florian Fröwis, Philippe Grangier, Hannes Hübel, Vicente Martin, Andreas Poppe, Joshua A. Slater, Tim Spiller, Wolfgang Tittel, Benoit Tranier, Adrian Wonfor, and Hugo Zbinden, npj Quantum Information, September 2022.

[1087] BraneCell Systems Presents Distributed Quantum Information Processing for Future Cities, by BraneCell Systems, April 2018.

[1088] AST and BraneCell Announce Their Partnership to Improve Critical Government Functions Through the Power of Quantum Computing, by BraneCell, July 2018.

[1089] Thermal state quantum key distribution, by Adam Walton, Anne Ghesquière, George Brumpton, David Jennings, and Ben Varcoe, arXiv, July 2021 (15 pages).

[1090] Universal Statistical Simulator, by Mark Carney and Ben Varcoe, arXiv, February 2022 (20 pages).

[1091] Quantum Networking: How Cisco is Accelerating Practical Quantum Computing, by Vijoy Pandey, Cisco Blogs, May 2025.

[1092] Quantum Data Center Infrastructures: A Scalable Architectural Design Perspective, by Hassan Shapourian, Eneet Kaur, Troy Sewell, Jiapeng Zhao, Michael Kilzer, Ramana Kompella, and Reza Nejabati, arXiv, January 2025 (22 pages).

[1093] Optimized Quantum Circuit Partitioning Across Multiple Quantum Processors, by Eneet Kaur, Reza Nejabati, et al., arXiv, January 2025 (12 pages).

[1094] High-dimensional coherent one-way quantum key distribution, by Kfir Sulimany, Michael Ben-Or, et al., arXiv, July 2023 (20 pages).

[1095] Enhanced Detection Rate and High Photon-Number Efficiencies with a Scalable Parallel SNSPD, by Lorenzo Stasi, Félix Bussières, et al., arXiv, December 2024 (29 pages).

[1096] Infotecs has presented its ViPNet Quantum Phone, by Infotecs, January 2018.

[1097] Enabling Quantum-Safe Migration with Crypto-Agile Certificates, by ISARA, 2018 (7 pages).

[1098] The Co-Inventor of BlackBerry Is Building Canada's Quantum Brain Trust, by Bloomberg, Bloomberg, 2018.

[1099] Long-range photonic device-independent quantum key distribution using SPDC sources and linear optics, by Morteza Moradi, Maryam Afsary, Piotr Mironowicz, Enky Oudot, and Magdalena Stobińska, arXiv, July 2025 (20 pages).

[1100] Proposal for the distribution of multiphoton entanglement with optimal rate-distance scaling, by Monika E. Mycroft, Magdalena Stobińska, et al., Physical Review A, January 2023 🔓 (preprint on arXiv).

[1101] Quantum-enhanced interferometry with large heralded photon-number states, by G. S. Thekkadath, I. A. Walmsley, et al., npj Quantum Information, October 2020.

[1102] Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, by M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature, May 2018 🔓 (preprint on orcid.org).

[1103] Nonlinear improvement of measurement-device-independent quantum key distribution using multimode quantum memory, by Yusuke Mizutani and Tomoyuki Horikiri, arXiv, June 2023 (18 pages).

[1104] Practical Routing and Criticality in Large-Scale Quantum Communication Networks, by Cillian Harney and Stefano Pirandola, arXiv, September 2025 (19 pages).

[1105] Physics: Unite to build a quantum Internet, by Stefano Pirandola and Samuel L. Braunstein, Nature, April 2016.

[1106] Free-Space Quantum Key Distribution with Single Photons from Defects in Hexagonal Boron Nitride, by Çağlar Samaner, Serkan Paçal, Görkem Mutlu, Kıvanç Uyanık, and Serkan Ateş, arXiv, April 2022 (6 pages).

[1107] Time-Resolved Stokes Analysis of Single Photon Emitters in Hexagonal Boron Nitride, by Çağlar Samaner and Serkan Ateş, arXiv, April 2025 (8 pages).

[1108] Secure Quantum Key Distribution Using a Room-Temperature Quantum Emitter, by Ömer S. Tapşın, Furkan Ağlarcı, Roberto G. Pousa, Daniel K. L. Oi, Mustafa Gündoğan, and Serkan Ateş, arXiv, April 2025 (11 pages).

[1109] Preparing a commercial quantum key distribution system for certification against implementation loopholes, by Vadim Makarov, Konstantin Zaitsev, et al., arXiv, October 2024 (34 pages).

[1110] Cost-aware Photonic Graph State Generation: A Graphical Framework, by Sobhan Ghanbari and Hoi-Kwong Lo, arXiv, September 2025 (38 pages).

[1111] Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic, by Xin Sun, Mirek Sopek, Quanlong Wang, and Piotr Kulicki, Entropy, September 2019 (15 pages).

[1112] Logic Programming with Post-Quantum Cryptographic Primitives for Smart Contract on Quantum-Secured Blockchain, by Xin Sun, Piotr Kulicki, and Mirek Sopek, Entropy, August 2021 (14 pages).

[1113] Qaas: hybrid cryptocurrency wallet-as-a-service based on Quantum RNG, by Muhammad Muneem Shabir, Kaiwen Zhang, Bertrand Reulet, and Ghyslain Gagnon, Cluster Computing, January 2025 🔓.

[1114] Quantum Xchange Breaks Final Barriers to Make Quantum Key Distribution (QKD) Commercially Viable with the Launch of Phio TX, by Quantum Xchange, September 2019.

[1115] Quantum Xchange Collaborates with Thales to Enable Quantum-Safe Key Delivery Across Any Distance, Over Any Network Media, by Quantum Xchange, November 2021.

[1116] Quantum Protocols for Time Synchronisation and Distribution: A Critical Assessment, by Michal Krelina, Utku Tefek, Zeki C. Seskir, and Kadir Durak, arXiv, April 2026 (24 pages).

[1117] Towards an All-Silicon QKD Transmitter Sourced by a Ge-on-Si Light Emitter, by Florian Honz and Bernhard Schrenk et al), arXiv, April 2024 (9 pages).

[1118] Experimental photonic quantum memristor, by Michele Spagnolo, Philip Walther, et al., Nature Photonics, March 2022.

[1119] Field-deployable Quantum Memory for Quantum Networking, by Yang Wang, Alexander N. Craddock, Rourke Sekelsky, Mael Flament, and Mehdi Namazi, arXiv, September 2022 (16 pages).

[1120] High-rate subgigahertz-linewidth bichromatic entanglement source for quantum networking, by Alexander N. Craddock et al., Physical Review Applied, March 2024 🔓 (preprint on arXiv).

[1121] Breakthrough for the quantum internet - from the laboratory to the real world, by Verena Fulde, Deutsche Telekom, April 2025.

[1122] Robust High-Fidelity Quantum Entanglement Distribution over Large-Scale Metropolitan Fiber Networks with Co-propagating Classical Signals, by Matheus Sena, Mehdi Namazi, et al., arXiv, April 2025 (11 pages).

[1123] High-fidelity entanglement between a telecom photon and a room-temperature quantum memory, by Yang Wang, Alexander N. Craddock, Jaeda M. Mendoza, Rourke Sekelsky, Mael Flament, and Mehdi Namazi, arXiv, March 2025 (10 pages).

[1124] Introducing Sandwich and the Journey Toward Modern Cryptography Management, by SandboxAQ, August 2023.

[1125] Forty Thousand Kilometers Under Quantum Protection, by N. S. Kirsanov, V. M. Vinokur, et al., arXiv, May 2023 (27 pages).

[1126] Establishing shared secret keys on quantum line networks: protocol and security, by Mina Doosti, Lucas Hanouz, Anne Marin, Elham Kashefi, and Marc Kaplan, arXiv, April 2023 (23 pages).

[1127] How to build quantum communication networks at a small scale, by Marc Kaplan from VeriQloud, May 2020.

[1128] Multi-client distributed blind quantum computation with the Qline architecture, by Beatrice Polacchi, Marc Kaplan, Fabio Sciarrino, Elham Kashefi, et al., Nature Communications, November 2023.

[1129] Experimental verifiable multi-client blind quantum computing on a Qline architecture, by Beatrice Polacchi, Marc Kaplan, Elham Kashefi, Fabio Sciarrino, et al., arXiv, July 2024 (14 pages).

[1130] Security Loophole Induced by Photorefractive Effect in Continous-variable Quantum Key Distribution System, by Zehao Zhou, Peng Huang, Tao Wang, and Guihua Zeng, arXiv, August 2024 (10 pages).

This **QKD and PQC vendors** subsection contains 60 bibliographical references and notes containing at least 747 pages.

1.8 Quantum telecommunications and cryptography key takeaways

- Quantum computing poses a theoretical threat to widely used public-key cryptography based on integer factoring or discrete logarithms. Shor's algorithm could, on a sufficiently large fault-tolerant quantum computer, recover the private information underlying schemes such as RSA from public data. Symmetric cryptography is affected differently, most notably through the quadratic search speedup provided by Grover's algorithm rather than through public-key distribution. The migration urgency is partly driven by the "store now, decrypt later" threat and by planning rules such as Mosca's inequality, which motivate deployment of quantum-resistant protections before cryptographically relevant quantum computers exist.
- Two broad families of countermeasures are commonly discussed: post-quantum cryptography (PQC), based on classical cryptographic algorithms believed to resist known quantum attacks, and quantum-communication techniques such as QKD. NIST launched its PQC standardization process in 2016 and selected algorithms for standardization in July 2022. In August 2024 it finalized FIPS 203, FIPS 204 and FIPS 205, covering ML-KEM, ML-DSA and SLH-DSA. FN-DSA, derived from FALCON, is planned for FIPS 206 and remains in development. PQC security must still be assessed against cryptanalysis, implementation flaws and side-channel attacks.
- Quantum key distribution (QKD) uses a quantum communication channel, together with an authenticated classical channel, to establish shared symmetric key material between remote parties. Protocols can use prepare-and-measure schemes or entanglement-based schemes, including architectures relevant to future quantum networks connecting computers and sensors. QKD does not transmit or protect public keys, and it does not require a general-purpose quantum computer. The generated key material is normally used with conventional symmetric cryptographic mechanisms for subsequent data protection.
- Quantum random-number generation (QRNG) can provide entropy for classical and quantum-communication cryptographic systems, including key generation, nonces and other protocol randomness. A QRNG does not by itself guarantee the security of a public or private key, which also depends on the cryptographic algorithm, implementation and threat model. QRNGs also have applications wherever high-quality randomness is useful in classical computing, including lotteries and Monte Carlo simulations.
- Quantum telecommunications can also use quantum entanglement to enable communications between quantum computers and/or quantum sensors. Distributed quantum computing has two potential benefits: scaling quantum computing beyond the capacity of individual quantum computers and enabling safe communications between quantum computers. There is a huge technology challenge with interconnecting quantum computers. It is about creating entanglement resources between distant qubits, sometimes using transduction between different wavelengths, and then, gate teleportation protocols to enable two-qubit gates between distant quantum processors. Distributed quantum sensing can also enable more accuracy sensing.
- Quantum Physical Unclonable Functions (qPUFs) are proposed authentication primitives whose security claims must be stated under a defined threat model, including assumptions about enrollment, verification and resistance to attacks. No physical authentication method is literally unfalsifiable, and qPUF technology remains immature.
- There are already many startups in the QKD and PQC scene. Deployments have already started worldwide, particularly in China with both landline fiber and satellite links. Europe is also experimenting quantum communication networks. PQC deployment is a priority for most governments and sensitive verticals (defense industry, financial services, healthcare, automotive).

2 Quantum sensing

Quantum sensing uses quantum systems, quantum properties and quantum effects to estimate physical quantities. Some implementations offer advantages over the best classical alternatives, under specified metrics and operating conditions, and many enable minimally invasive or noncontact measurements on solid or organic materials. The main physical values measured are time, distances, gravity, magnetism, temperature, and electromagnetic spectrum analysis.

2.1 Quantum sensing use-cases and market

Many applications can use quantum sensing technologies like radars, sonars, high-sensitivity acoustic sensors or the field of imaging in general and particularly in medical imaging and sensing [1131, 1132] (Figure 102).

Some of these technologies have commonalities with the various qubit types we have already explored in detail. This is particularly the case for cold atoms, NV centers and superconducting qubits. Precision magnetometers use NV centers as well as SQUIDs (superconducting quantum interference devices), which measure magnetic flux and can therefore be used to infer the direction of the circulating current in superconducting flux-type qubits, as D-Wave does in its quantum annealers. Besides a couple exceptions like Infleqtion, most quantum sensor vendors are specialist vendors in the sensing space (Figure 105) or classical sensors vendors who extend their product range with quantum sensors.

Many of these quantum measurement technologies make extensive use of photonic tools, either directly based on photons (lasers, frequency combs, entangled photons) or exploiting cold atoms and even NV centers, whose quantum state of interest is then evaluated by measuring their fluorescence.

Some of these technologies are already commercially viable and continue to progress steadily. It is still a niche market made up of many sub-niche markets, evaluated at around $1B and expected to double in a decade. The two largest applications markets are transportation and medical imaging and analysis (Figure 103, Figure 104). However, the growth forecasted in these charts from 2019 didn't happen. According to several analysts sources (Precedence Research, Fortune Business Insights, IDTechEx, McKinsey, Roots Analysis, Fact.MR, Grand View Research, Hyperion Research [1133]), published 2025 estimates span roughly $400M to $900M, and individual long-term forecasts reach $1.2B by 2032 and up to $2.5B by 2045. These sources do not share a common market definition, scope, currency, base year or forecast method, so their figures should be read side by side rather than merged into a single precise range.

But these forecasts may become wrong since some use cases might at some point become mainstream and drive more market growth. This is the case of GPS without satellite links using micro-magnetometers. It could for example someday equip many classical and autonomous vehicles.

Viewed from the bridge, the quantum sensing market seems more mature than quantum computing, with higher TRLs. It does not account for the fact that many advertised quantum sensors have not yet reached the industrialization phase.

The reasons may be linked to various engineering, miniaturization and cost problems that remain to be fixed. Sometimes, it is also because many of these sensors do not yet work as advertised [1144]. When selecting a technology and a vendor, some operational elements can be considered like the operating temperature of the sensor, has it got 3-axis vector sensing, its bandwidth, self-calibration, its form factor (size, weight, mobility), its robustness, ease of use and of integration.

Various other markets are relevant for quantum sensing: the energy and utilities sector [1145], telecoms, space, and astrophysics research [1146], high-energy particles physics research [1147, 1148], civil engineering, manufacturing industries using many sensors like for quality control and non-destructive testing and control, and of course the aerospace and defense sectors.

2.2 International System of Measurement

Sensing cannot be discussed without being connected to the **International System of Units** (SI). The 26th General Conference on Weights and Measures (CGPM), meeting in Versailles in November 2018 under the Metre Convention of 1875, unanimously adopted the revised definitions of the base units [1149]. They took effect on May 20, 2019.

The new 2019 SI updates the definition of the kilogram, ampere, kelvin and mole. It is built around seven fixed defining constants: the cesium-133 hyperfine transition frequency $\Delta\nu_{Cs}$, the speed of light in vacuum c, the Planck constant h, the elementary charge e, the Boltzmann constant k, the Avogadro constant N_A and the luminous efficacy K_{cd}. From these constants are derived the seven base units of the system: kilogram, meter, second, ampere, kelvin, mole and candela (Figure 106). Since 1967, the second has been defined from exactly 9 192 631 770 periods of the radiation corresponding to

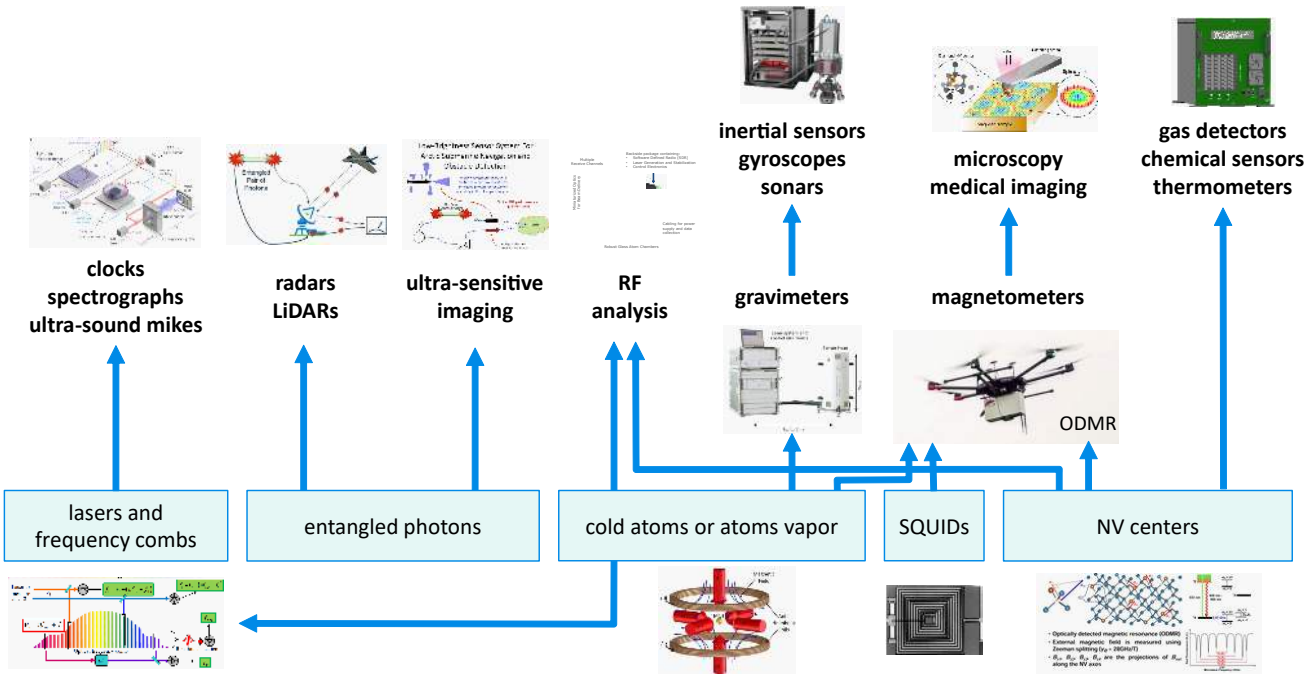


Figure 102: A (partial) map of various quantum sensing basic technologies and use cases. © Olivier Ezratty, 2021-2024.

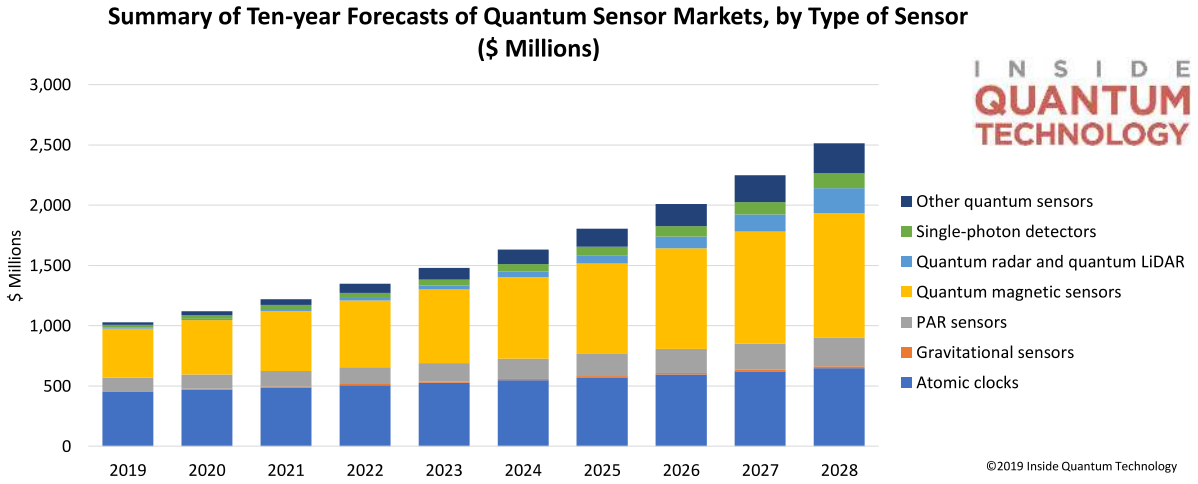


Figure 103: We are now more than halfway in this forecast of quantum sensing revenue. Actual market size estimates range from $435.5M [1134] to $700.8M [1135] and nears $892M [1136] in 2025, with between $502.1M [1137] and $860M [1138] in 2026. Long-term forecasts predictions reach $1,564M by 2034 at a 15.3% CAGR [1139], $1,700M by 2033 at a 7.6% CAGR [1140], $3,904.6M by 2035 at a 15.9% CAGR [1141], and up to $4,523.5M by 2035 at a 20.5% CAGR [1142]. Chart source: [1143].

the transition between the two hyperfine levels of the ground state of cesium-133. The 2019 SI reformulated this in terms of the fixed numerical value of $\Delta\nu_{Cs}$.

It no longer relies on material artifacts that can change over time, such as the international prototype kilogram formerly kept at the BIPM, nor on a fixed thermodynamic state of a particular material such as the triple point of water for defining the kelvin.

The mole was previously tied to 0.012 kg of ^{12}C. Since 2019, one mole contains exactly $N_A = 6.022\,140\,76 \times 10^{23}$ specified elementary entities, such as atoms, molecules, ions or electrons. The definition is a count of entities and does not involve multiplying N_A by their number of nucleons.

The standard meter, which is kept in the Archives in Paris, was no longer the reference since 1960. All other units of measurement such as hertz, joule, coulomb, lumen or watt are derived from constants and base units. This measurement system is branded as being "quantum" because it is based on the measurement of fundamental phenomena that bring us back to quanta, in particular for the definition of the second, which uses quantized energy transitions in the cesium atom, and that of the kilogram, which uses the Planck constant, itself a foundation of quantum physics.

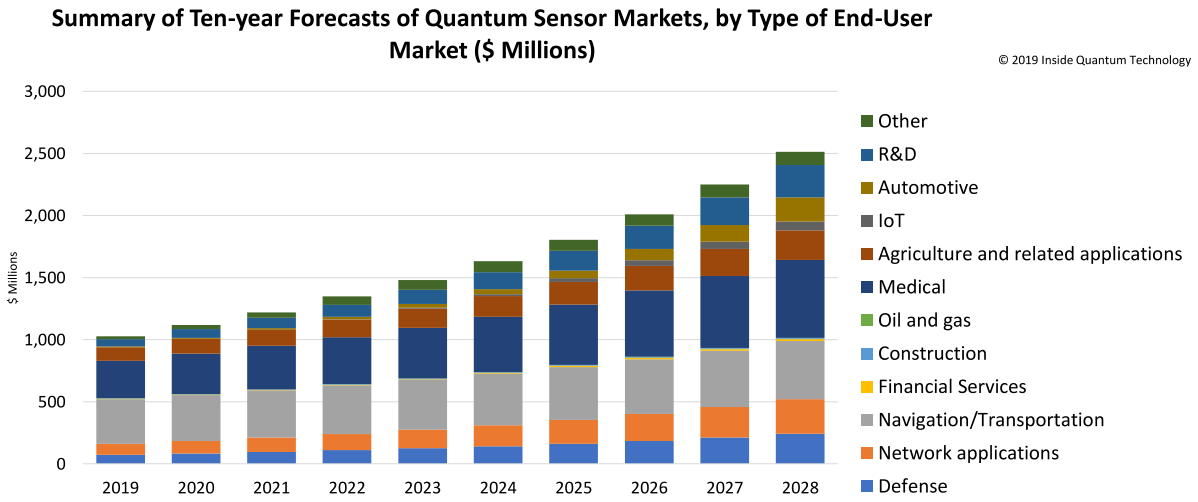


Figure 104: An old prediction, from 2019, for the quantum sensing global market. Source: [1143].

Numerous quantum physics works related to these evolutions of the international measurement system, notably at NIST, have a link with the commercial devices discussed in this section.

2.3 Quantum sensing taxonomy

Reusing a definition found on C.L. Degen et al's 2017 review paper [1150], quantum sensing describes the use of quantum systems, quantum properties and phenomena to measure physical quantities. The first quantum sensors were SQUID magnetometers, atomic vapors, and atomic clocks. Then, the field was expanded to cover magnetic and electric fields, time and electromagnetic-wave frequencies, mechanical rotations, temperature and pressure quantum measurement.

New "second generation" sensors work at the single-atom and spin level and may use quantum entanglement as a resource for increasing sensitivity [1151, 1152].

Quantum sensing can exploit one or more of the following phenomena, corresponding to type I, II and III quantum sensors:

- **Type I**: using a quantum object to measure a physical quantity, characterized by quantized energy levels and a non-classical state, like a squeezed state, that is not entangled with the receiver.
- **Type II**: transmits a classical state that is not entangled with the receiver and uses a quantum-enhanced detection technique in the receiver using, for example, quantum coherence, wave-like spatial or temporal superposition states to measure a physical quantity.
- **Type III**: using quantum entanglement to improve the sensitivity or precision of measurement. It is sometimes labelled "quantum metrology", "quantum-enhanced sensing" or "second generation quantum sensing".

The difference between quantum sensing and quantum metrology is not that clear in the scientific literature. Quantum metrology is used for devices measuring units or fundamental constants such as an atomic clock or an atom interferometer measuring the fine structure constant, or constants that were used to create the last SI. It can relate to the study of quantum-based precision measurements and quantum sensing using entanglement as seen in the above type I/II/III taxonomy. It can use the creation of photonic Schrödinger's cats [1153].

The table in Figure 107 lists several types of known quantum sensors with their type, the physical nature of the measuring object ("qubit nature") and the measured physical quantities. For example, charged systems like trapped ions are sensitive to electrical fields while spin-based systems mainly respond to magnetic fields. Some quantum sensors may respond to several physical parameters or measure indirectly some physical quantity, which is the case for quantum thermometry with NV centers [1154]. Most of the time, quantum sensing exploits changes in the transition frequency or the transition rate in response to an external signal [1155].

The rest of this quantum sensing part is mostly organized along the first row and its green/blue measured values: gravity, time, magnetism, temperature, radiofrequencies and then to higher-level applications like imaging, radars and LiDARs and chemical sensors.

Quantum sensors are a bit paradoxical: a single projective measurement on a sensing qubit returns a discrete outcome, often just one bit. So how do you get a floating-point number with a large precision? In the most basic cases, you make many measurements and average their results. In practice, sensors also infer a continuous parameter from photon counts, ensemble fluorescence, analog signals, multilevel readout, generalized measurements or continuous-variable detection, so a single readout is not restricted to one bit [1156, 1157]. There are other subtleties. With NV center sensors, you build a spin resonance spectrum from repeated measurements and the shape of the resulting curve lets

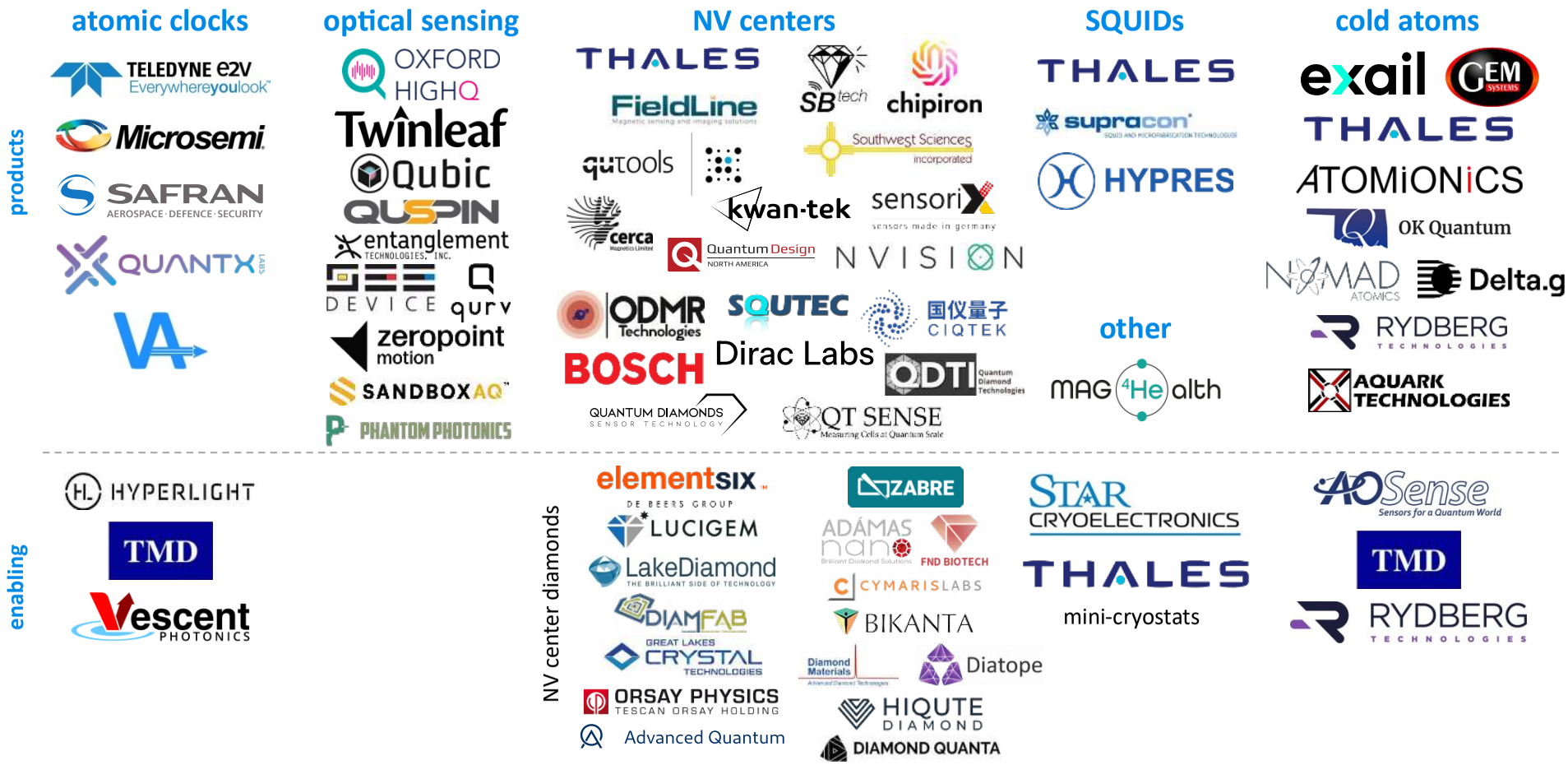


Figure 105: Market map for quantum sensing, including some of their enabling technologies. © Olivier Ezratty, 2023-September 2026.

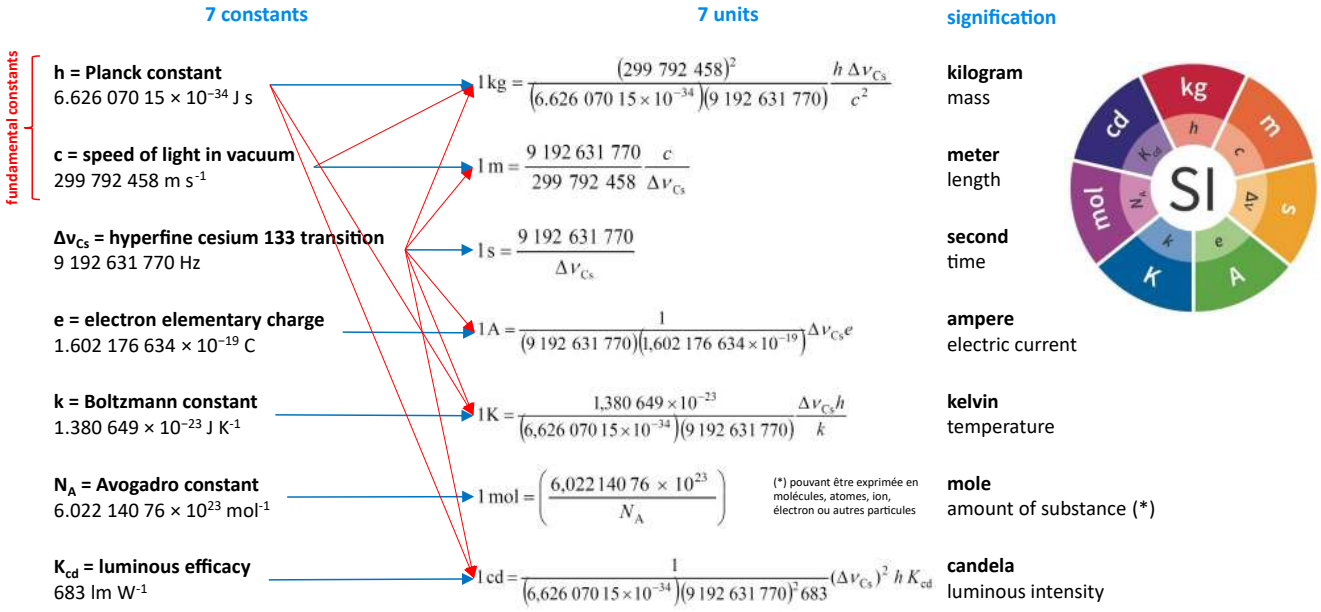


Figure 106: Reconstruction of the SI constants, units and their signification. Sources: Ⓒ Olivier Ezratty, 2021-September 2026, and [1149].

		sensor type	qubit nature	type I	type II	type III	rotation	acceleration	force	pressure	displacement	time	frequency	refractive index	magnetifield	electric field	voltage	temperature	mass
neutral atoms		atomic vapor	atomic spin		X	X	X					X	X		X				
		cold atom clouds	atomic spin		X	X		X				X	X		X				
Rydberg atoms			Rydberg states		X	X										X			
trapped ions			electronic state		X	X	X			X		X	X						
			vibrational mode		X				X							X			
solid state	spin ensembles	NMR	nuclear spins		X										X				
		NV/SiC center ensembles	electron spins		X		X			X					X	X		X	
	single spins	P donor in Si	electron spins		X										X				
		quantum dot	electron spins	X	X										X	X			
		single NV center	electron spins		X		X			X					X	X		X	
superconducting circuits		SQUIDs	supercurrent	X	X										X				
		flux qubits	circulating current		X										X				
		charge qubits	charge eigenstates		X											X			
single electron transistor			charge eigenstates	X												X			
optomechanics			phonons	X				X	X						X		X		
interferometer			photons, atoms		X	X	X				X			X					

Figure 107: Quantum sensing taxonomy. Source: table reconstructed and updated from [1150]. Added in 2022. Corrected in 2024.

you determine the detected magnetic field by computing the distance between two peaks. It is an indirect measurement. In some cases, the "qubit" doing the measurement contains some quantum data that could potentially be used by a quantum computer, thus avoiding a costly data encoding process [1158]. It can even lead to improved measurement sensitivity [1159, 1160].

A quantum sensor measurement precision will depend on several parameters: the sampling rate (how many measurements are made with the same sensors or similar sensors in parallel), the sensor noise and the sensor sensitivity [1161].

Which brings us to define some key concepts related to quantum measurement precision with more details (see the tutorial from Marco Barbieri published in 2025 in [1162] for more details, focusing on photonic based metrology). Quantum sensing has its own semantic zoology with measurements, estimators, estimations, precisions, variances, statistics, limits, bounds and the like. The following text clarifies some of the quantum

sensing lingua, given there are many inconsistencies in the related literature.

Precision vs accuracy. These are basic concepts, measurement accuracy corresponding to how close a result is to the true value, and precision which is about the consistency of repeated measurements [1163].

Quantum Fisher Information (QFI) quantifies how sensitively a parameterized quantum state changes with the parameter to be estimated. It is not itself a precision limit. For an unbiased estimator based on ν independent repetitions, it sets the quantum Cramér–Rao bound $\mathrm{Var}(\hat{\theta}) \geq 1/(\nu F_Q)$ under the usual regularity conditions. QFI can also serve as an entanglement witness for particular generators and multipartite states, but it is not a universal scalar measure of multipartite entanglement [1164, 1165]. Quantum error mitigation or quantum error correction can help a practical protocol approach the precision allowed by its noisy dynamics [1166, 1167].

Cramér–Rao bound (CRB) is the lower bound on the variance of an unbiased estimator. The terms Cramér–Rao bound and Cramér–Rao limit are commonly used for the same inequality, rather than for two different quantities. In a single-parameter classical estimation problem, $\mathrm{Var}(\hat{\theta}) \geq 1/(\nu F)$, where F is the Fisher information per repetition. The quantum Cramér–Rao bound replaces F by the QFI optimized over quantum measurements. In multiparameter estimation, the QFI becomes a matrix, but its inverse is not always jointly attainable because optimal measurements for different parameters may be incompatible.

Shot-noise limit (SNL) describes fluctuations associated with counting independent discrete events such as photons. For independent probes it typically gives a standard-deviation scaling $\delta\theta \propto 1/\sqrt{N\nu}$, with N probes per interrogation and ν repetitions. Depending on the physical problem, this scaling is also called the **standard quantum limit (SQL)**. The SQL is therefore not generally a direct consequence of simultaneously measuring complementary observables. It is the characteristic scaling obtained with independent, uncorrelated resources, subject to the resource definition used in the experiment.

Heisenberg limit (HL) conventionally denotes the best ideal scaling $\delta\theta \propto 1/N$ for many unitary metrology problems when the relevant resource is counted consistently. Entanglement, spin squeezing, NOON states, multipass strategies or other coherent protocols can provide the correlations needed to improve on the independent-probe $1/\sqrt{N}$ scaling. Noise and loss can remove this asymptotic advantage, and the precise form of the Heisenberg limit depends on what is counted as a resource [1165, 1168–1170]. Quantum error correction can restore Heisenberg-like scaling for some noise models [1171, 1172].

Beyond-Heisenberg or super-Heisenberg scaling is sometimes reported for nonlinear parameter-dependent Hamiltonians or when only a subset of the physical resources is counted. Formal scalings such as $1/N^2$ can occur in such models [1173, 1174], but they do not deliver universal precision limit beyond the Heisenberg limit. When interaction strength, evolution time, generator norm and other consumed resources are counted consistently, apparent super-Heisenberg scaling can disappear [1165]. Squeezing can beat the shot-noise or SQL scaling in suitable interferometric measurements, although loss, decoherence and technical noise limit the practical gain.

Sensor noise. The noise acting on the quantum system may be modeled as Markovian (no memory effect, leading to irreversible decoherence and limiting precision to the SQL unless some error correction is implemented [1175, 1176]) or non-Markovian (with some memory effect, which can be leveraged to surpass the SQL [1177]). Practical sensors also face technical noise that neither category describes: drift, vibration, laser intensity and frequency noise, imperfect magnetic shielding and readout electronics noise.

Let's also mention the developing field of quantumly networked sensors, distributed quantum sensing (DQS) which has several benefits like connecting ensembles of quantum sensors to collectively improve their sensitivity beyond classical limits, but mostly relying on long-distance interferometry [1178–1181], to connect them to some quantum computers to help these directly capture some quantum data and accelerate the processing of sensed data like optical pixels in astrophysics imaging [1182], and, to separate in a trusted way the state preparation, parameter encoding, measurement and data collection tasks [1163, 1183]. DQS can also be used for dark matter detection using networked superconducting qubits [1184].

Secure quantum remote sensing (SQRS) which uses quantum states to ensure secure data transmission against eavesdropping from a quantum sensor remotely connected to a readout optical device [1185, 1186]. There are even protocol proposals to make sure that the collected quantum data remains anonymous [1187, 1188].

Time-reverse metrology uses time-reversal protocols to improve measurement precision. [1189] groups four strategies: mirror metrology, which brackets the parameter encoding between a preparatory unitary and its inverse to amplify the visibility of a small parameter, weak-value amplification, which enhances the detectability of a weak coupling, the simulation of closed timelike curves, and indefinite causal order, where a channel is applied in a superposition of orderings. None of these reverses time. The retrocausal language used to describe the statistics of the first strategy is an interpretive model, not a physical claim, and the protocol itself is just a unitary transformation followed by its inverse.

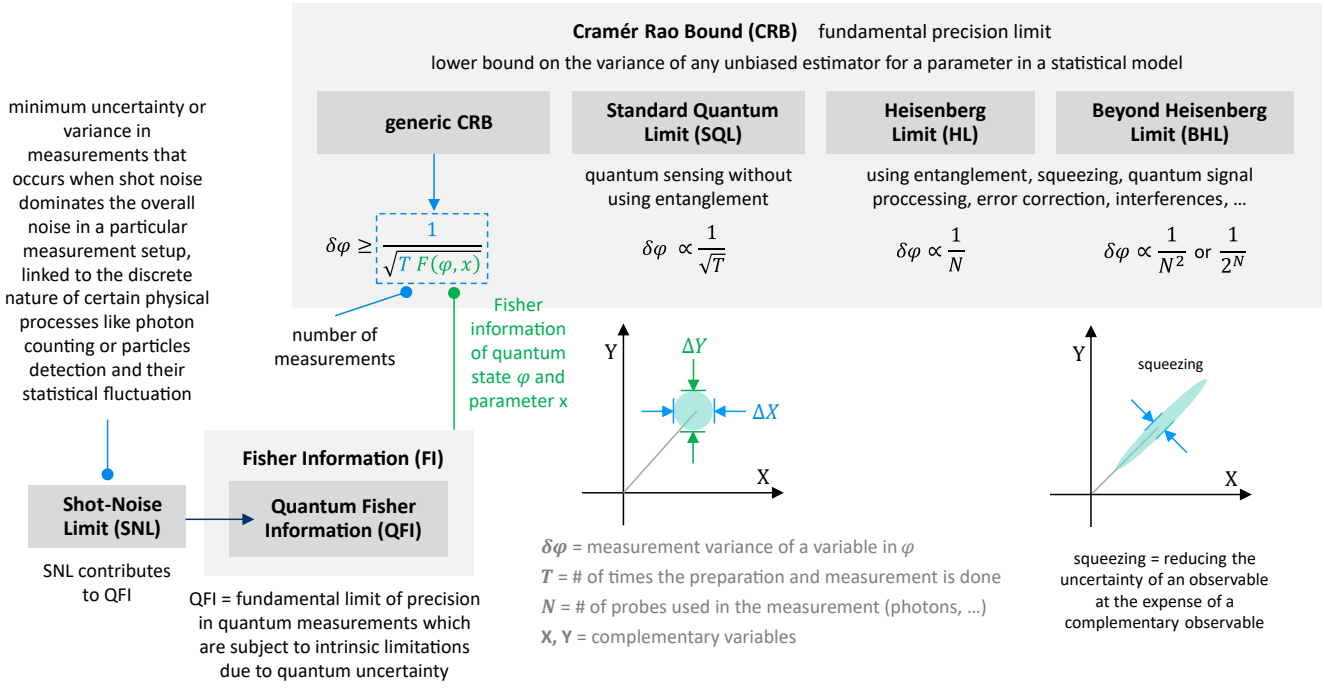


Figure 108: Mapping of the various quantum measurement limits. © Olivier Ezratty, 2023.

2.4 Quantum gravimeters, gyroscopes and accelerometers

Quantum gravimeters measure gravity with a very high accuracy. Usually based on matter-wave interferometry with cold atoms, these are useful in many scenarios: in seismic detectors and volcano monitoring, for inertial sensing and quantum position systems complementing or replacing GPS in airplanes, ships, submarines and drones, for gravity field mapping, for detecting subsurface voids before construction, for detecting groundwater and ice mass change, for oil and mineral exploration (with some caution) and for the detection of gravitational waves and even dark matter [1190]. A frequently mentioned use case is the detection of nuclear submarines, which would destabilize or neutralize the nuclear deterrence of the countries operating them, but its practicality is still questioned. An airborne array of SQUID magnetometers for submarine detection was reportedly prototyped in China in 2017. It requires cooling, but that is not a big deal for such a use case.

2.4.1 Quantum gravimeters

There are two categories of gravimeters. Absolute gravimeters measure the gravity per se measuring the free trajectory of a test mass in vacuum, and now, with cold atoms, their interferences. Relative gravimeters measure the variation of gravity over space and time. They are usually calibrated using absolute gravimeters. The most precise relative gravimeters are superconducting based but are not considered as quantum gravimeters.

The quantum measurement of gravity is generally performed with cold atom interferometers (CAI), taking advantage of the wave-particle duality of cold atoms [1191, 1192]. The technique has been developed since 1991 and perfected since then [1193, 1194]. The principle consists of creating a source of cold atoms free falling in suspension, generally rubidium, preparing their state with lasers, passing them through a three-stage laser-controlled atom interferometer and then analyzing the results [1195].

In the USA, NIST, NOAA and geodesy laboratories used FG5 absolute gravimeters from the 1990s onward. The FG5 tracks the free fall of a corner-cube retroreflector in a vacuum chamber with a laser interferometer. A rubidium frequency standard can provide the time reference, but rubidium atoms are not the falling test mass. Stanford created a cold atom gyroscope in 2006 which led to the creation of AOSense. In France, SYRTE developed a six-axis inertial sensor using two magneto-optical traps (MOTs), also in 2006.

The figures of merit of quantum gravimeters are their **sensitivity** (smallest detectable change in gravity, usually quoted as an amplitude spectral density in m s^{-2} $Hz^{-1/2}$ or in Gal $Hz^{-1/2}$, the gal belonging to the centimeter-gram-second system and named after Galileo), **accuracy** (closeness of agreement with a reference standard, expressed as an uncertainty in the unit of the measure and or as a relative uncertainty, and not inherently as a percentage) and **stability**. The sensitivity of such an atom interferometer scales with its free-fall time [1196]. The operational figures of merit are weight, size and warm-up time (which can last one hour).

Best-in-class movable cold atom absolute gravimeters like the ones from Exail/Muquans have a sensitivity of the order of 10^{-9} m s^{-2} Hz$^{-1/2}$. Interesting miniaturization designs are also proposed, although they lead to a lower sensitivity. [1197] uses a compact titanium vacuum package with a grating chip inside a tetrahedral grating magneto-optical trap (GMOT) using a single cooling beam, with a reported sensitivity of 2×10^{-6} m s^{-2} Hz$^{-1/2}$. On the other end of the spectrum, projects like the UK AION-10 ten meter interferometer target a projected sensitivity of 10^{-10} m s^{-2} Hz$^{-1/2}$, with applications in gravitational wave and dark matter detection [1198].

Quantum absolute gravimeters are often used alongside classical gravimeters. They complement each other, atom interferometers having high sensitivity, stability and accuracy but have a low data rate and dynamic range, while classical gravimeters have a larger bandwidth but exhibit bias and drift.

Figure 109: Exail/Muquans absolute gravimeter. Source: Muquans.

Quantum gravimetry could also be based on a SQUID, a transmon and a nanomechanical resonator [1199]. Its **projected** sensitivity is 10^2 to 10^3 nGal Hz$^{-1/2}$, equivalently 1 to 10 nm s^{-2} Hz$^{-1/2}$. For comparison, **measured** cold-atom absolute quantum gravimeters like the Exail AQG achieve 3×10^4 to 5×10^4 nGal Hz$^{-1/2}$, that is 300 to 500 nm s^{-2} Hz$^{-1/2}$, in field or quiet laboratory conditions. On paper the SQUID-based design would therefore be at least 30 times more sensitive, comparing a projection with a measurement. It also requires millikelvin cryogenics, which is not very practical, on top of adding vibration noise detrimental to the sensing task.

One last thing here. At CERN's Antimatter Factory, the ALPHA-g experiment reported in 2023 the first direct observation of the effect of gravity on neutral antihydrogen. Its best-fit downward acceleration was $0.75\,g$ with sizeable statistical, systematic and simulation uncertainties, consistent with ordinary attractive gravity and excluding a repulsive acceleration of $1\,g$ [1200]. GBAR is a separate experiment pursuing precision free-fall measurements of ultracold antihydrogen. Separately, coherent control of a single antiproton spin has been demonstrated and can be described as an antimatter-based qubit [1201, 1202].

2.4.2 Quantum gradiometry

A related field is gradiometry, which measures horizontal or vertical gravity gradients. It is used for the measurement of the variations or anomalies in the Earth's gravity field by creating gravity maps over the earth to either improve geopositioning or to detect changing underground features over time. It requires specific settings and techniques to reduce noise and vibrations within the gravimeter [1204–1206]. ONERA launched gravimetry experiments in 2009 (GIRAFE project) and in 2014-2016 (GIRAFE2) [1207]. It was tested by the French Navy in a surface vessel in 2025 and 2026. The goal is to create a map of underneath the oceans.

2.4.3 Quantum inertial sensors

Quantum inertial sensors are being developed to complement GNSS and to provide navigation during GNSS denial or jamming. They are particularly interesting for military and space applications.

They can be created with various technologies:

- **Cold-atom gravimeters** which measure rotation and can be embedded in gyroscopes [1208] which in turn create quantum inertial sensors for navigation [1209]. It can also operate in space, as China successfully experimented in 2024 [1210].
- Many of these systems are initialized or periodically aided by a global navigation satellite system (GNSS) such as the US GPS, the EU Galileo, Russia's GLONASS or China's BeiDou, then run autonomously or in an interleaved manner. Whether an external reference is needed, and how often, is architecture-dependent rather than universal.
- In June 2023, the **UK Royal Navy** conducted a trial of a cold atom quantum navigation system avoiding the use of GPS to determine a vessel's location anywhere on earth. The system that was tested in a Qinetiq NavyPOD container placed on deck of the 500 tons experimental ship XV Patrick Blackett was designed by physicists from the Centre for Centre for Quantum Engineering, Science and Technology (QuEST) at the Imperial College in London. It could also potentially be used by submarines.
- In May 2024, the UK minister of defense completed flight trials of quantum-based navigation systems developed by a consortium led by Infleqtion, BAE Systems and QinetiQ, with the participation from Fraunhofer Centre for Applied Photonics, Alter Technology UK, Caledonian Photonics, Redwave Labs and PA Consulting. The Quantum Enhanced Inertial Navigation Systems (Q-NAV) system uses the Tiqker

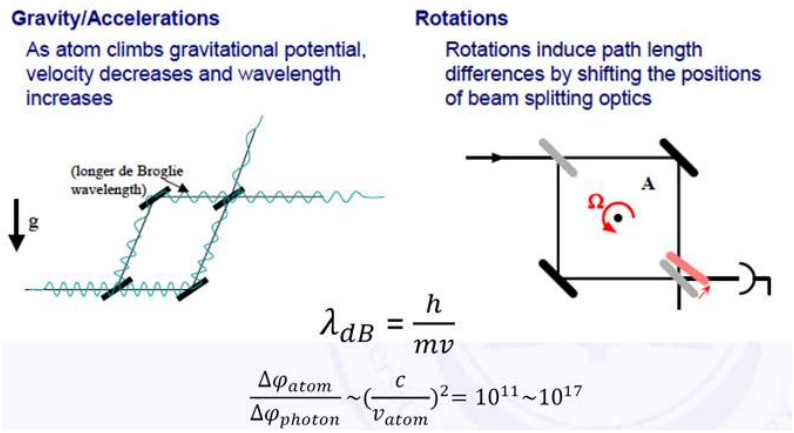


Figure 110: How cold atom interferometry works to measure both gravity, accelerations and rotations. Source: [1203].

optical atomic clock and an ultra-cold-atom-based quantum system, both from Infleqtion, installed in QinetiQ's RJ100 Airborne Technology Demonstrator, a modified aircraft. It got UK public funding of £8M.

- **Optical interferometry** [1211, 1212], as with the use of the effects of rotation on the polarization of light, which induces a differential phase shift in the propagation of left and right circularly polarized light, this phase shift being measured with interferometry [1213]. **Quantum fiber optic gyroscope** (QFOG) that utilizes optical quantum squeezing, quantum entanglement, and the non-Gaussianity of quantum states, as tested in China [1214].
- **Surface-acoustic-wave** (SAW) cavities working in the microwave band, also tested in China [1215] and Japan [1216].
- **NV centers**, by replacing nitrogen-14 with nitrogen-15 nuclear spins to improve sensitivity [1217].
- **Quantum magnetometry**, for example **SandboxAQ**'s AQNav system announced in June 2024, a quantum positioning system tested airborne that uses a sensitive quantum magnetometer to measure the Earth's crustal magnetic field, which exhibits geographically unique patterns. An AI algorithm is then used to compare this data against known magnetic maps, enabling the system to find its position. It also improves the signal-to-noise ratio and removes ambient noise acquired by the sensor.
- **Cavity magnomechanical** systems as experimented in China in 2025 [1218].

Other cold atom applications include magnetic field measurement in Earth monitoring and temperature measurement. Hybrid sensors can associate electrostatic and cold atom acceleration sensors. Cold atom interferometry will even be used for gravitational waves detection in the MIGA experiment being set up in France [1219, 1220].

2.4.4 Quantum rotation sensing

There are also quantum sensors just for measuring rotations, mostly photonic based [1221, 1222], or using atom interferometry [1223].

2.4.5 Vendors

Here are the various vendors also positioned in this market, given many are still in the product development phase and don't have yet a commercial offering.

Advanced Navigation

Australia, 2012

Advanced Navigation is a company specialized in navigation systems. It is creating a hybrid classical-quantum inertial sensor using their digital fiber-optic gyroscope (DFOG) with atom-interferometry-based quantum accelerometer. They work with Q-CTRL for the development of this sensor for future NASA lunar exploration. Q-CTRL also works on its side on magnetic-anomaly navigation (MagNav) [1224] as well as on gravity-anomaly mapping navigation [1225].

AOSense

USA, 2004

AOSense creates and sells quantum gyroscopes, commercial optical clocks and develops a quantum gravimeter. It also provides instrumentation equipment with cold atom generators and laser frequency comb generators

They collaborate with IonQ for their quantum computers based on trapped ions. It is a spin-out from Stanford and a pioneer in the sector who is now highly diversified. It created a quantum inertial measurement unit (IMU) for Boeing that was successfully tested in August 2024 [1226]. They also work along with Q-CTRL and Lockheed-Martin on a quantum-enabled Inertial Navigation System (QuINS) for the US DoD.

aQuark Technologies

UK, 2020, $5M

aQuark Technologies is a spin-off from the University of Southampton created by Andrei Dragomir (CEO). It develops small vacuum chambers and simpler atoms trap systems named supermolasses that avoid the use of a MOT (magneto-optical trap) thanks to coupling several lasers with slightly different frequencies. In October 2023, they demonstrated a lightweight 10 kg airborne solution of their system. In 2024, they also announced that they were working on the creation of an atomic clock using their technology, with a grant of £3.4M from the UK government. In June 2025, the startup completed a sea trial of its cold atom-based AQlock aboard HMS Pursuer from the Royal Navy. It showcased operation in rough offshore conditions over three days. In 2026, the experiment was extended using two AQlock 2.0 atomic clocks to demonstrate that quantum-based atomic clocks can synchronize networked military radars and maintain an accurate operational picture. aQuark also tested its aQuest cold atom sensor undersea using the UK National Oceanography Centre's Boaty McBoatface submersible in April 2025, in a gravity and magnetic field sensing configuration whose exact target quantity has not been publicly documented.

Atomionics

Singapore, 2018, $14.6M

Atomionics is currently developing Gravio, a cold atoms interferometry based sensor measuring acceleration, rotations and gravity variations. It can be used for navigation and resource exploration. It can also be used as an underground GPS and also undersea. Other laboratories are working on the same technology, such as the **Leibniz University** of Hannover [1227]. China is also playing in this field, but without having gone so far in miniaturization [1203].

CAS Cold Atom

China, 2020

CAS Cold Atoms develops miniaturized quantum gravimeters. The company is based in Wuhan.

Delta G

UK, 2023, £1.5M

Delta G is a spinout from the UK Quantum Technology Hub Sensors and Timing at the University of Birmingham. Created by Peter Stirling (CEO), Andrew Lamb (CTO) and Michael Holynski (CSO). It develops cold atom sensors applied to gravity gradiometry, targeting use cases in construction, archaeology and for the discovery of hidden natural resources [1204].

Exail

France, 2000

exail, formerly **iXblue Photonics** is a small business specialized in the design and manufacture of inertial and sonar systems, lithium niobate optical modulators, microwave amplifiers and modulator bias controllers for the control of Mach-Zehnder interferometers.

Their components are manufactured at their site in Lannion, Brittany and at Besancon. They are involved with the LP2N of Bordeaux in the creation of Ixatom, a quantum inertial sensor based on cold rubidium atoms. iXblue Photonics was the result of the acquisition of two companies: **iXFiber** in 2011, a specialist in passive optical components (FBG fiber grating filters, Fiber Bragg Gratings) and then, **Photline Technologies** in 2013, a spin-off from Femto-ST created in 2000 in Besancon. In May 2021, iXblue then acquired **Muquans** (quantum absolute gravimeters, created in 2011 in Bordeaux, France) and **Kylia** (a photonic equipment specialist, with its polarizers, delay line interferometers and multiplexers/multiplexers). In March 2022, Groupe Gorgé made the acquisition of iXblue Photonics to merge it with its subsidiary of **ECA Group**, a security, defense, and industry security technologies provider. It became **exail** in November 2022.

Muquans is based at the Institut d'Optique in Bordeaux. Their absolute quantum gravimeters are commercial products targeting, for example, the detection of cavities in construction, oil exploration and the monitoring of volcanoes such as Etna in Italy [1228].

Here is how their absolute quantum gravimeter and other similar neutral atom-based quantum gravimeters work. The usual description looks like the image in Figure 111 from Muquans.

We can decompose the quantum gravimetry steps in six parts.

Heating source: a heated source at the top of the system prepares a small cloud of about 10^6 atoms of rubidium (^{87}Rb). The source of the atoms also contains an accelerometer that corrects the phase of the lasers in real time. It is prepared with a 2D MOT.

Magneto-optical trap: a 3D MOT as shown in Figure 112919 is used to confine and cool the prepared source of atoms at 1 μK using three pairs of counter-propagating laser beams in three orthogonal directions, applying the Doppler effect, and two anti-Helmholtz coils which magnetically trap the atoms [1229, 1230].

Inverted pyramid retroreflection: an inverted mirrors-based pyramid sits around the MOT and orients the prepared atom cloud downward in the instrument as shown in Figure 113.

State preparation: a laser beam coming from the bottom controls the atom cloud position. It is switched off and the cloud starts to freefall.

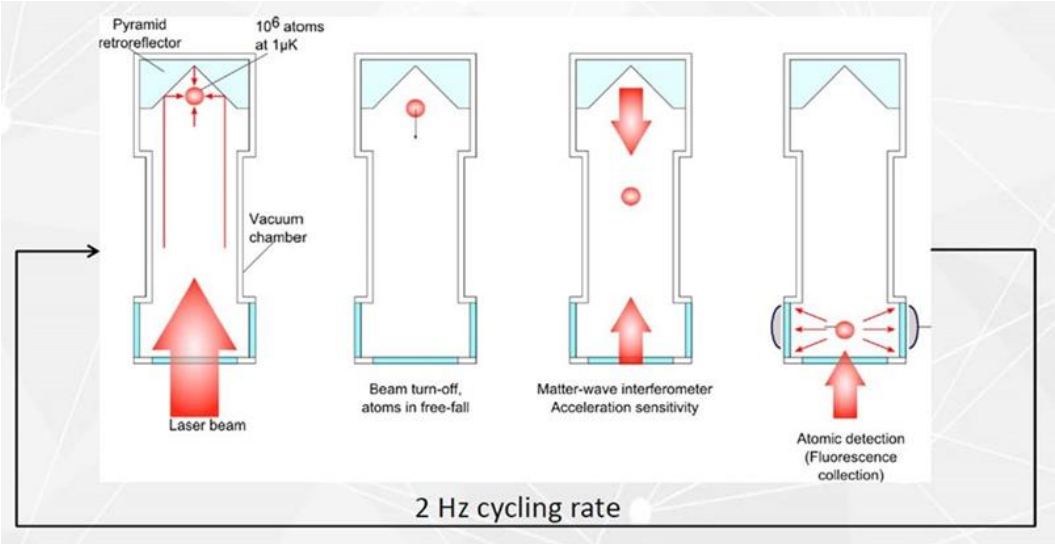


Figure 111: How atom interferometry works. All laser beams come from the bottom of the device. Source: Muquans.

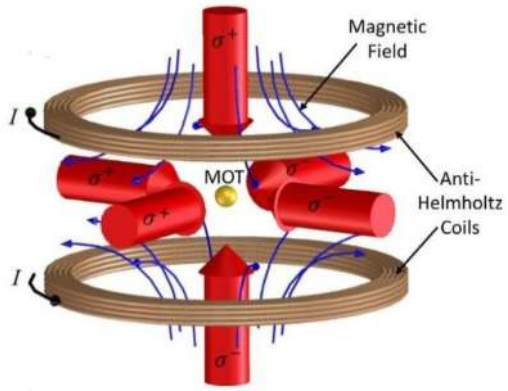


Figure 112: Typical Magneto-Optical Trap used to cool and confine neutral atoms. Source: [1231].

Atom interferometer: during its free fall, the atom cloud is exposed to two counter-propagating vertical laser pulses in three successive steps forming the standard $\pi/2$, π, $\pi/2$ sequence. Each pulse drives a stimulated two-photon Raman transition between the two hyperfine levels of the rubidium ground state, through a far-detuned excited state that is only virtually populated and never actually occupied. The two-photon process transfers a momentum $\hbar k_{eff}$ to the atoms, so that the internal state and the momentum state are coupled, which is what makes the interferometer work. The first $\pi/2$ pulse acts as a coherent beam splitter and creates a balanced superposition of the two paths. The π pulse acts as a mirror, inverting the internal populations and redirecting the two paths towards each other. The final $\pi/2$ pulse recombines them. Gravity does not set the splitting ratio, which is fixed by the pulse area. It appears in the phase $\Delta\phi = k_{eff}\, g\, T^2$ accumulated between the two paths over the pulse separation T, read out as a population imbalance at the output. These pulses are interferometer optics, not a cooling stage, the cooling having taken place earlier in the MOT and in the optical molasses. One alternative design is the Zacharias fountain, where the atoms are launched upward [1232].

Detection: one or two other high precision lasers excite the two streams of atoms exiting the interferometer, generating a fluorescence effect that is detected by two sets of four broadband photodiodes using different frequencies. These diodes enable the measurement of the proportion of atoms in each interferometer output (excited/non excited). Their proportion will help compute the phase difference accumulated by the two atom streams, which itself will help calculate the ambient gravity. The process is repeated twice per second and a classical computer averages the results. Their gravimeters have a precision of 10^{-9} m/s^2.

Exail is involved in the ESA's **NAVISP** program which plans to provide a supplementary navigation solution using gradiometry. The company is also developing a 3-axis quantum inertial sensor which was demonstrated in July 2024 [1233]. The control of cold atoms has other applications [1234, 1235]. For example, Muquans participates in the European flagship project **Quantum Internet Alliance** to create hardware to extend the reach of QKD systems and with the French startup **Pasqal** which creates quantum processors based on cold atoms.

Figure 113 describes the three steps of cold atoms interferometry used in a gravimeter. The figure is somewhat confusing since the position axis (Z) goes up as the atom falls. So, it is inverted. Otherwise, how would you measure atoms at the bottom of the gravimeter? Two counterpropagating lasers are used, one coming from the top at frequency $\omega_1$and a wave vector k_1 and one from the bottom at ω_2 and a wave vector k_2 to create a double-photon Raman transition that will modify displacement for a share of the atoms that depends on the gravity.

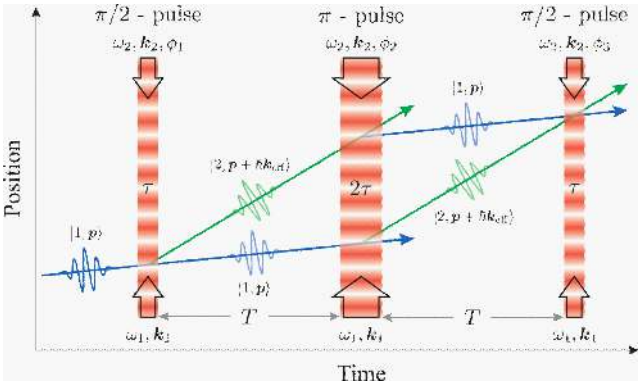


Figure 113: The three steps of cold atoms interferometry used in a gravimeter. Sources: [1236].

Figure 114 shows the Raman transitions created by lasers with pulses ω_1 and ω_2. f corresponds to the fundamental or ground state, e to the excited state. p is the atom momentum and its difference in the excited state is $\hbar k_{eff} = \hbar(k_1 - k_2)$. The width of the laser pulse τ (about 10 ms) corresponds to its duration which generates a superposition like a Hadamard gate in gate-based computing in step 1 and 3, and a population inversion in step 2 with a duration of 2τ. Meaning, the excited atoms (green lines) are turned in ground state atoms (blue line) and vice-versa, and also inverting their vertical velocity. If the lasers were used continuously, they would create a Rabi oscillation creating a continuous change in the populations of the ground and excited states over a couple ms.

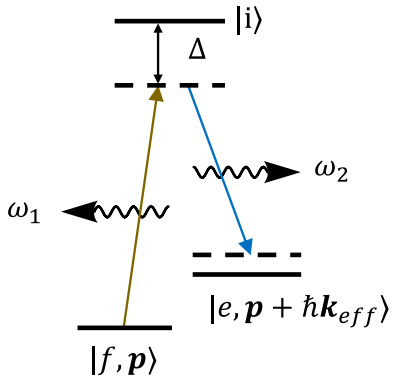


Figure 114: Atomic states of a ^{87}Rb atom and stimulated Raman transitions induced by counter propagating laser beams. [1237].

In October 2024, Exail and various partners announced the launch of the EU funded €17M CARIOQA-PMP project (Cold Atom Rubidium Interferometer in Orbit for Quantum Accelerometry – Pathfinder Mission Preparation) with a consortium (CNES, DLR, Airbus Defence and Space, TELETEL, Leonardo, GMV, etc.) for the creation of cold atom-based interferometry sensors to detect environmental changes on Earth from satellites (glaciers, sea level, variations in groundwater levels).

Innoseis

the Netherlands, 2020, $6.9M

Innoseis was created by Mark Beker and Johannes van den Brand (who worked on gravitational waves detections instruments like those from LIGO), from Maastricht University. They develop MEMS based quantum gravimeters targeting seismic surveying.

Leidos

USA, 2013

Leidos is a US defense contractor that has a quantum unit specializing in quantum sensing for resilient navigation in GPS-denied environments and quantum networking for robust cybersecurity, including some interest for distributed quantum computing. They develop PICs (Photonic Integrated Circuits). The quantum unit is led by Elizabeth Iwasawa.

M Squared

UK, 2006-2025, $56M

M Squared has been developing a cold atom quantum gravimeter for a long time but withdrew from this market and focused back on its original lasers business covering the spectrum from 200 nm to 4,000 nm. These lasers are used in industry and in optical clocks. In November 2022, M Squared announced it was entering the neutral atoms quantum computing market with its Maxwell system as part of a collaborative UK government funded project. Maxwell was supposed to become a "state of the art breakthrough system" but with undisclosed characteristics. In August 2025, the company entered insolvency proceedings.

Hangzhou Weijia Quantum Technology (2018, China) is a company partnering with Lin Qiang from the Zhejiang Technology University which develops since 2020 a quantum gravimeter used in geological and oceanography exploration. In June 2024, they reported probing the ground to a depth of 300 meters.

Nomad Atomics

Australia, 2018, $10M

Nomad Atomics develops compact cold atom-based quantum gravimeters and accelerometers. The company was launched by Kyle Hardman, Christian Freier and Paul Wigley, respectively researcher and post-docs at the Australian National University.

Qooda

Germany, 2026

The company created by Björn Pötter (CEO, formerly from IQM) develops geolocalization systems based on the analysis of the magnetic field. It seems that the precision is of about a km [1238].

Thales

France

Thales Research & Technology is developing miniaturized cold atom accelerometer, gyrometer and clock designed to be embedded. The whole with a "BEC on chip" component (for "Bose-Einstein condensates on chip") in collaboration with the Charles Fabry laboratory of the Institut d'Optique (LCFIO). Atoms are vaporized in a glass cage glued to the chip, in which a good vacuum has been created. They are laser-cooled and trapped by a magnetic field and controlled by electromagnetic fields. This research project started around 2014 (Figure 115).

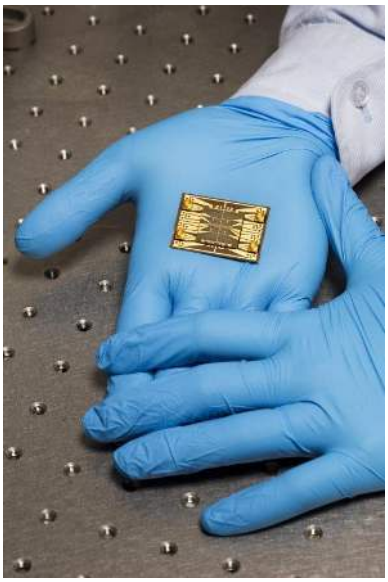


Figure 115: A Thales BEC on chip. Photo credit: Ecliptique - Laurent Thion.

Vector Atomic

USA, 2021-2025

Vector Atomic was a startup created by Jamil Abo-Shaeer (CEO), a former project manager at DARPA. It is developing with Honeywell Aerospace an atomic clock based navigation sensor that avoids the use of GPS. It was funded by Defense Innovation Unit of the US DoD. The company was acquired by IonQ in 2025.

Zero Point Motion

UK, 2020, £4M

Zero Point Motion is a quantum optical inertial sensors company created by Ying Lia Li (Imperial College and University College London). Their hybrid sensors use quantum photonics and cavity opto-mechanics to read the motion of MEMS masses. The product is being developed at the Quantum Technologies Innovation Centre at Bristol University with commercialization to start in 2024.

And...

Rafael Advanced Defense Systems (Israel) also has a department creating quantum sensing solutions, mainly gravitation sensors, with the Weizmann Institute of Science.

Microg LaCoste (1939, USA) develops falling-corner-cube absolute gravimeters.

Draper Labs (1932, USA) also designs cold atoms sensors, mostly, gravimeters and accelerometers for navigation systems.

Trumpf (Germany) develops cold-atoms and VCSEL (lasers) based gyroscopes for satellites as part of the QYRO project funded by the German government and along with its subsidiary Q.ANT.

Wideblue (2006, UK) creates MEMS gravimeters. It is a consulting and engineering company.

Quantum accelerometers are also investigated to equip autonomous or assisted drive vehicles. German equipment manufacturer **Bosch** announced in February 2022 the creation its own quantum gyroscope for this purpose, aka IMU for inertial measurement unit as part of its new Bosch Quantum Sensing Unit, an internal startup led by Katrin Kobe and with a team of 15 people, which launched a joint venture with Element Six in April 2025.

Finally, let's also mention a very special category of microgravimeters: the LIGO microgravimeters that are used to evaluate gravitational waves. They are based on optical interferometers of very high precision but of a size incompatible with all other imaginable uses [1239–1241].

2.5 Quantum clocks

Atomic clocks used in GPS provide resilience for navigation systems when standard satellite GPS signals are unavailable. They are also used in telecommunication infrastructure for the Internet and mobile communications, particularly with high-speed broadband landline and mobile infrastructures. Many industry sectors also rely on precision time measurement, like the financial sector and utilities power grids. Fundamental research and astrophysics also heavily rely on precision clocks.

2.5.1 Science

Time measurement steadily progressed since the first mechanical clocks used between the 14^{th} and 19^{th} centuries. Quartz clocks, developed between the two World Wars, exploit the piezoelectric effect discovered by Pierre and Jacques Curie in 1880. A common watch crystal oscillates at $2^{15} = 32\,768$ Hz so that binary frequency division produces a 1 Hz tick. Other quartz oscillators operate at many different frequencies. Consumer quartz watches typically drift by roughly seconds to tens of seconds per month, depending on oscillator quality and temperature compensation.

The first cesium atomic clocks came out in the 1950s. Using a frequency around 9 GHz, they provide a time measurement accuracy ranging from 10^{-13} up to 10^{-16} with recent generations. The second is defined since 1967 as the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two "hyperfine" levels of the fundamental electronic state of cesium 133. The recent variants of these clocks are "fountain clocks". They operate at very low temperature, with laser cooling bringing the atoms at 1 μK, way much colder than superconducting qubits that are at 15 mK but is however easier to obtain than with a dilution refrigerator. A frequency oscillator generates a transition between two levels of cesium energy. The frequency is locked with a servo loop.

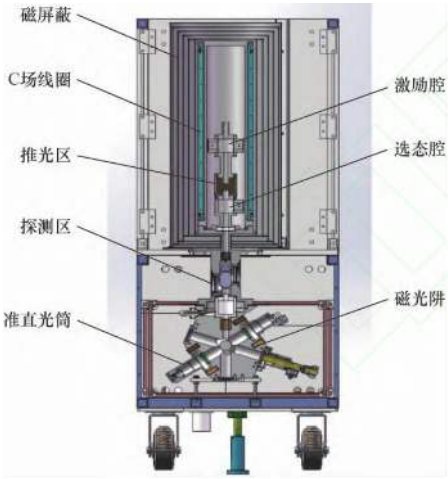


Figure 116: NIM-TF3's atomic clock from the National Institute of Metrology of China is 1.5 meter tall. Source: [1242].

The National Institute of Metrology of China created in 2024 such an atomic clock, the NIM-TF3 using laser-cooled cesium atoms [1242]. These atoms emit fluorescence as they fall under gravity through a microwave energy field. The clock is 1.5 meters high and may have some military applications (Figure 116).

The precise measurement of frequencies has many applications: time measurement, synchronization of various devices on the Internet, even if only servers or scientific instruments, synchronization of moving objects to measure their position, astronomy (as with exoplanets and gravitational waves detection), absorption or emission precision spectroscopy, fiber optic transmissions and the generation of radio waves of arbitrary shape (Figure 117) [1243]. However, a better accuracy may be needed, thus the need for quantum clocks [1244, 1245].

For about 20 years, time measurement was implemented with optical measurement of frequencies and time [1246] (Figure 119).

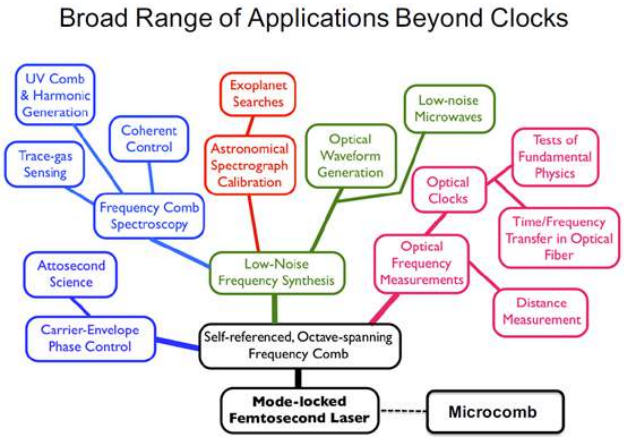


Figure 117: Femto lasers use cases in quantum sensing.

Optical clocks interrogate atomic transitions at frequencies of order 10^{14} to 10^{15} Hz, much higher than the approximately 9.2 GHz cesium microwave transition. Their higher carrier frequency can support substantially smaller fractional frequency uncertainty. Around 1999–2000, self-referenced optical frequency combs made it practical to coherently link optical frequencies to microwave frequency standards. This optical frequency-comb technique was a central reason why John L. Hall and Theodor W. Hänsch shared half of the 2005 Nobel Prize in Physics.

Figure 118: A CSAC chip.

In the USA, the **Chip Scale Atomic Clock** (CSAC) program funded by DARPA with NIST participation [1249] led to the creation of highly compact vapor-cells cesium based atomic clocks manufactured by Microchip (mentioned later, with a size of 40.6 mm × 35.6 mm × 11.4 mm) after a decade of work starting in 2000 and $100M spent. It generates pulses of 4,596.3 MHz with a frequency tuning resolution of $1x10^{-12}$s [1250] (Figure 118).

Atomic clocks used microwave frequency transitions while the new generation of quantum clocks are based on higher electromagnetic wave frequencies in the optical spectrum. They use the technique of frequency combs. Since these frequencies are higher, these clocks can have a better precision, with three orders of magnitude gain compared to classical atomic clocks. Quantum atomic clocks also have accuracy limitations [1251].

Frequency combs arise naturally from mode-locked lasers, whose development dates to the 1960s, but modern optical frequency-comb metrology emerged around 1999–2000 with octave-spanning spectra and

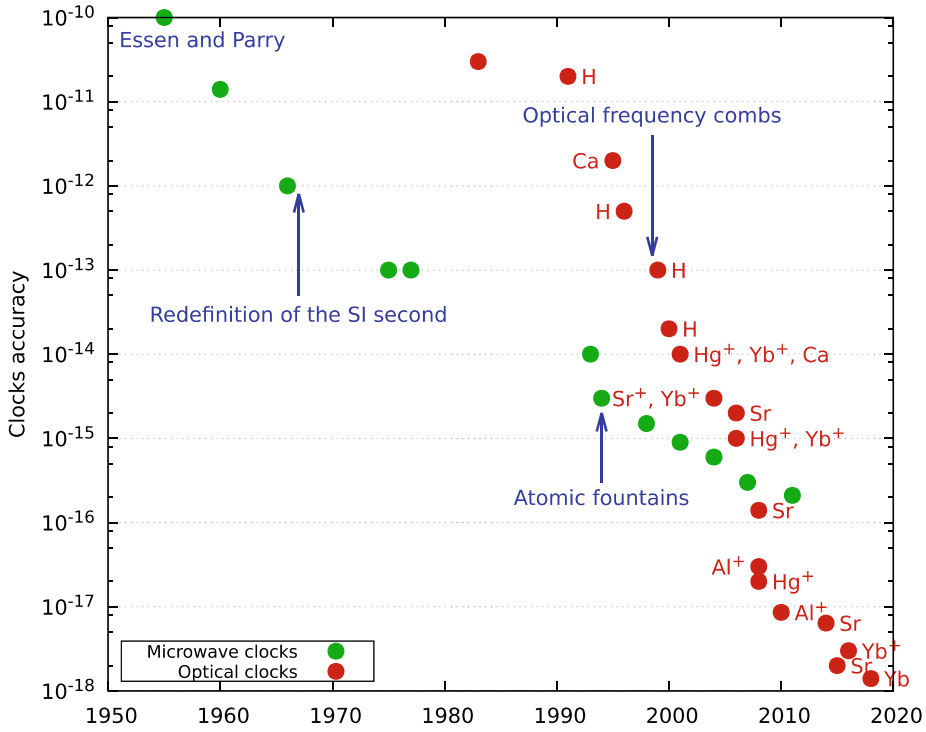


Figure 119: How quantum clock accuracy evolved over time. A recent multi-ion clock reached a systematic fractional frequency uncertainty of about 5×10^{-19} in 2026 [1247]. Chart source: [1248].

self-referencing [1252]. John Hall describes frequency combs as the intersection of four initially independent fields of research: ultra-stable lasers, fast-pulse lasers, nonlinear optical materials and precision laser spectroscopy. Optical frequency combs coherently connect optical frequencies to radio or microwave references, allowing optical frequencies to be counted electronically. They commonly use mode-locked lasers that generate trains of ultrashort pulses, which can be only a few femtoseconds long.

The frequency decomposition of this kind of signal gives a Gaussian-shaped frequency comb with each tooth regularly spaced at a frequency equivalent to that of the laser pulse. This is related to the fact that the length of the laser cavity is a multiple of the length of the electromagnetic waves emitted by the laser. Adjacent comb teeth correspond to longitudinal cavity modes separated approximately by the pulse repetition frequency. The optical carrier frequency is set by the laser transition and cavity dynamics.

The frequency spectrum resembles a Gaussian curve. Its envelope is equal to the envelope of the spectrum of an isolated pulse, which is continuous. The width of the frequency spectrum covered can be narrow, a few nm in wavelength, or cover the entire visible spectrum, thus a few hundred nm.

Some computing determines the very high frequencies of the frequency comb (f_n). It uses several parameters: the reference frequency f_{rep} of the laser pulses which is of the order of 250 MHz to 1GHz, n, the number of frequencies detected via spectroscopy (there can be hundreds of thousands) and the carrier-envelope phase evolution of the mode-locked laser which is added to each pulse and generates the frequency offset f_0, which is evaluated with a method described below and which is also of a lower order than GHz (Figure 120).

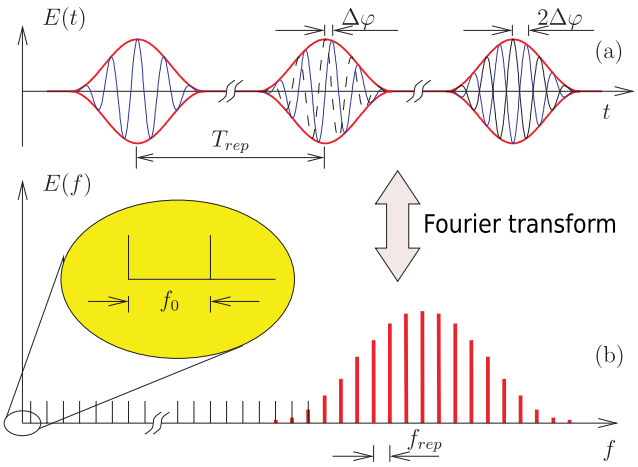


Figure 120: How a frequency comb works. Source: Ultrashort light pulses for frequency metrology, CNRS (6 pages).

The measurement of radio frequencies in the MHz/GHz wave range results in the measurement of frequencies in 10s and 100s of THz to the nearest Hz. The system thus acts as a frequency multiplier. The measurement of light frequencies is impossible with traditional electronics because of the frequencies used, which are several tens or hundreds of tera-Hertz. These calibrated frequency combs are also used to measure a frequency difference with this standard [1253–1257].

The frequency comb covers an octave, from one frequency (n) up to its double (2n) (Figure 121).

The evaluation of f_0 is done by extracting the frequency f_n and doubling it with a crystal. By beating the frequency-doubled component $2f_n$ against the comb component f_{2n}, their difference yields the carrier-envelope offset frequency f_0.

$$2\left(f_0 + n \times f_{rep}\right) - \left(f_0 + 2n \times f_{rep}\right) = f_0$$

This is called **heterodyne detection**. The frequency comb becomes a kind of graduated ruler which is then used to position a frequency to be measured relative to the ruler. With that, you can build a new generation atomic clock [1258]!

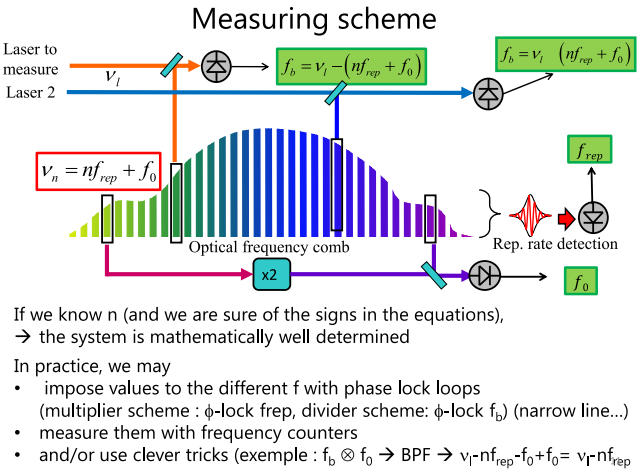


Figure 121: Frequency comb and heterodyne detection. Source: [1256].

The readout of spectroscopy results using frequency combs can use CCD or CMOS cameras depending on the frequencies used in or around visible light. [1259] describes the many methods and use cases of frequency comb based spectroscopy. This measurement accuracy evolves with the use of lasers using a high pulse frequency.

To date, the record for the accuracy of an atomic clock using spectroscopy is that of NIST. It is built with some aluminum ion associated with a magnesium ion. The aluminum ion is excited by two ytterbium lasers. Measurement is carried out using a quantum logic spectroscopy which is using the frequency combs, shown in Figure 122 [1260]. The clock reaches a fractional systematic uncertainty of order 10^{-18}. Expressing this as an equivalent accumulated timing error gives the often quoted order of one second over tens of billions of years, assuming that fractional offset remained constant [1261].

In this market for optical quantum clocks, many research laboratories produce their own equipment. These are usually based on titanium-sapphire with pulses of a few femtoseconds (10^{-15} to 10^{-14} seconds).

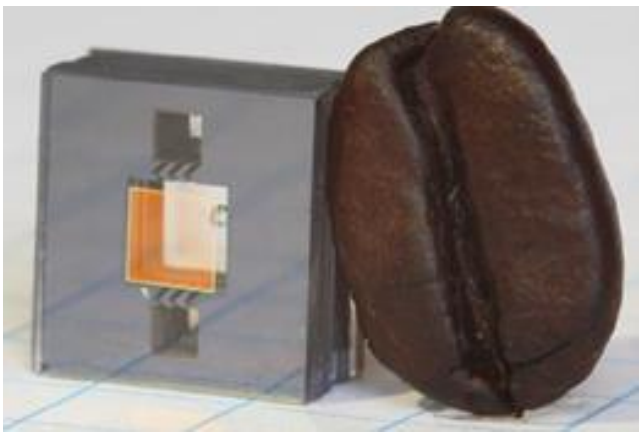


Figure 122: A NIST atomic clock based on aluminum and magnesium ions. Source: [1261].

NIST is also working on an atomic clock that would fit into a component the size of a coffee bean, using a double frequency comb and rubidium gas (in Figure 123). The whole thing consumes only 275 mW. This project was co-funded by DARPA [1262, 1263]. However, for the moment, the precision obtained is not yet satisfactory for any industrialization.

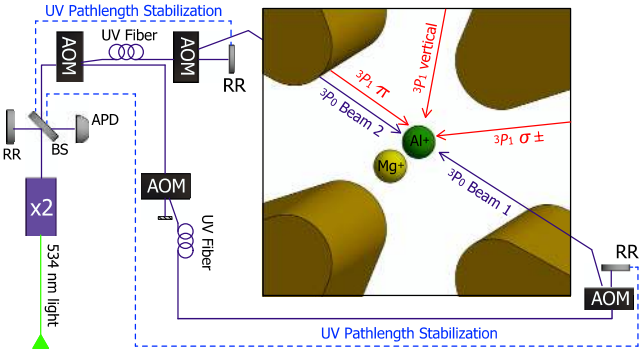


Figure 123: A NIST atomic clock the size of a coffee bean. Sources: [1262, 1263].

One of the projects of the European Quantum Flagship, **iqClock** (the Netherlands, €10M), also aims to create very high-precision, portable quantum clocks. The consortium brings together six universities and six private partners including Teledyne EV (USA), Toptica (Germany), NKT Photonics (Denmark, part of Hamamatsu since May 2024), AckTar (Israel) and Chronos (UK).

Optical lattice clocks trap atoms with laser tweezers in an optical lattice, after Doppler cooling. They use strontium and ytterbium elements thanks to their narrow spectral line widths for optical transitions, which help them have very good precision. These clocks are also less sensitive to external magnetic and electric fields. They are still complex to setup [1264]. They can also use entanglement to improve their accuracy, and the technique of the tweezer clock, which prepares atoms entanglement with high precision two-qubit gates [1265, 1266]. It reported clock performance at the 10^{-18} level in fractional frequency instability or uncertainty, de-

pending on the metric used in the cited experiment [1267].

Optical clocks can be used for time synchronization between distant parties. In 2022, China physicists led by Jian-Wei Pan (USTC) transferred time and frequency information over a 113 km in free space. They were using an optical clock having three components: atom samples with energy transitions operating at a stable reference frequency in optical frequencies, a feedback system that "locks" the output of the local oscillator laser to this reference frequency and a very precise measurement of the frequency of the laser using optical frequency comb (OFC). The researchers demonstrated time-frequency dissemination between such a feedback system and an OFC separated by 113 km using two ground optical telescopes [1268].

After 10,000 seconds, the clock's frequency instability was less than 4×10^{-19}, representing one second for 100 billion years. It opens the path for satellite-to-ground time-frequency dissemination. The China team now plans to extend this test to synchronize satellites at medium and geostationary orbits, and low Earth orbit satellites with ground stations. It could have various applications in metrology, navigation and positioning and in the search for dark matter, redefining fundamental constants and testing relativity. These synchronization systems could even benefit from entanglement, which can yield a quantum advantage in atomic clock synchronization over lossy satellite-to-satellite channels [1269].

Quantum dots can also be used to create quantum clocks. It was experimentally tested by using a charge sensor to count charges tunneling through a double quantum dot (DQD) in a cryostat at 180 mK [1270]. The results suggest that the entropy produced by the amplification and measurement of a clock's ticks corresponds to the bulk of the thermodynamic cost of timekeeping at the quantum scale, leading to potential optimizations.

Nuclear clocks is another option, using laser accessible transition in atom nuclei like with ^{229}Th (thorium). But its stability and precision is a couple of orders of magnitude lower than state of the art optical clocks [1271, 1272].

2.5.2 Vendors

Let's now look at some vendors in high-precision quantum time measurement.

Adamant Quanta

Sweden, 2022, €1M

Adamant Quanta develops chip scale NV-center based quantum sensors for timing, navigation, and communication applications. Its QDi.AC is an NV-center frequency reference. It is a small through-hole component that can be soldered into system electronics. It generates a pre-configured 10 or 20 MHz LVCMOS or sine wave reference signal.

HyperLight Corp

USA, 2018, $117M

HyperLight Corp, based in Cambridge, near Boston, develops nanophotonic integrated circuits such as frequency combs or resonators that are used in quantum sensing.

Mesa Quantum

USA, 2023, $16M

Mesa Quantum is a Boston-based startup launched by Sristy Agrawal (CEO) and Wale Lawal (CTO). It develops a position, navigation, and timing (PNT) chip-scale quantum sensor avoiding the use of GPS, seemingly based initially on an atomic clock.

MicroSemi

USA, 1960

MicroSemi sells its Quantum SA.45s, a miniaturized chip-scale atomic clock (CSAC). Among other use cases, it can be used in portable IED (improvised explosive devices) jammers. The company is a subsidiary of MicroChip Technology (1989, USA).

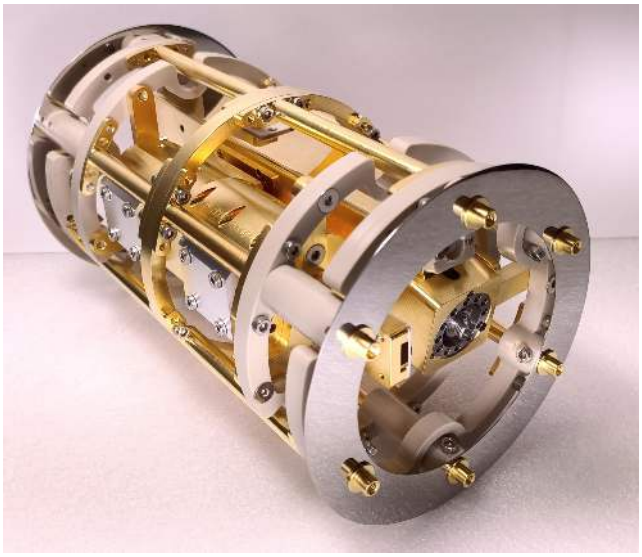


Figure 124: QuantX Labs TEMPO atomic clock that was launched in space late 2026.

QuantX Labs

Australia, 2016

QuantX Lab, formerly Cryoclock, develops sapphire-based cryogenic oscillators. The company was co-founded by John Hartnett.

Cryoclock produces extremely stable signals from HF to X-band and can be used as a local oscillator for atomic clocks and for trapped ion quantum computers. In 2024, to sold its clock to the Australian Defence Force (ADF). And late 2025, it will launch its lighter TEMPO atomic clock in space on a SpaceX mission for the Australian Space Agency (Figure 124). They also offer SENTIO, a

compact quantum magnetometer and SYNCHRO, Time Transfer Synchronisation tool.

QuPrayog

India, 2024

QuPrayog is offering optical atomic clocks, Ti-sapphire lasers and optical frequency combs.

Safran

France

Safran acquired Orolia (2005, France) in July 2022 and Syrlinks (2011, France) in November 2022. Orolia creates atomic clocks with cesium, or based on rubidium oscillators. They mainly target the aerospace industry and provide the Galileo GNSS service. Syrlinks develops miniature atomic clocks based on MEMS and cesium for embedded applications. Their MMAC is 40 x 35 x 22 mm and consumes less than 0.3 W. With Thales, and with the help of CNRS (SYRTE lab) Syrlinks is developing Chronos, new quantum clocks for civil and military applications with an error below 1 second over tens of thousands of years. It will enable geolocalization when GNSS like GPS and Galileo are not available.

Shanghai Quantum Sensing Intelligence

China, 2023, $4.6M

Shanghai Quantum Sensing Intelligence has two businesses: miniaturized photonic quantum gyroscopes and industrial gas monitoring. The company spun out from Shanghai's Jiao Tong University.

Teledyne

USA

Teledyne sells Minac (cesium atomic clock), T-CSAC (also cesium, integrated in a chip) and Synchronicity (ytterbium-based). UK aircraft carrier HMS Prince of Wales has been fitted with the world's first atomic clock of its kind to help ensure pinpoint accuracy wherever she goes provided by BP and Teledyne e2v.

TMD

UK, 1969

TMD sells microwave amplifiers. They also develop atomic clocks and instrumentation for the manipulation of cold atoms.

Vector Atomic

USA, 2018-2025

VectorAtomic markets rubidium atomic clocks for quantum inertial navigation systems that can then avoid using GPS. They were acquired by IonQ in September 2025.

Figure 125: Vescent RUBRIComb optical frequency comb. Source: Vescent web site.

Xairos

USA, 2019, $1.45M

Xairos is a space and technology startup created by David Mitlyng, in the field of position, navigation, and timing. They are creating a quantum photonics-based clock synchronization system [1273].

Zhongkeqidi Optoelectronic Technology is a company based in Guangzhou, China, *aka* Tus-China Optoelectronic Technology, that develops various optoelectronic components used in atomic clocks.

In June 2022, **Infleqtion** announced that it was working for the US Navy with **LocatorX** (USA) to create an atomic clock using the Solid-state Miniature Atomic Clock (SMAC) technology created by LocatorX under license of Oxford University. The system is using fullerene molecules (C60) doped with nitrogen. It is not relying on cold atoms, the core technology mastered by Infleqtion. It seems the two vendors are combining lightweight atomic clocks and more precise ones using cold atoms.

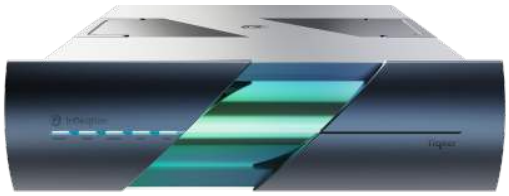


Figure 126: Infleqtion 2U Tiqker optical clock. Source: Infleqtion.

Infleqtion received in December 2024 $11M in funding from the DoD under the Accelerate the Procurement and Fielding of Innovative Technologies (APFIT) program, for the Rack Mounted Optical Clocks project, using Infleqtion's Tiqker clock (Figure 126).

In April 2026, Infleqtion established a partnership with Safran Electronics & Defense for the creation of a quantum-based timing solution integrating its Tiqker optical clock with Safran's White Rabbit time synchronization and SecureSync time server.

In January 2023, **GLOphotonics** (France) got a CES Innovation award for its Photonic Microcell Atomic Clock (PMCAC), a stylus form-factor atomic clock. I am not sure what the consumer use case for such a product would be (Figure 127).

Figure 127: GLOphotonics Photonic Microcell Atomic Clock (PMCAC) that fits into a relatively large stylus form factor package. Source: GLOphotonics. January 2023.

Muquans also uses its cold atoms expertise to sell an atomic clock, the MuClock, designed in partnership with the LP2N laboratory in Bordeaux and the LNE-SYRTE. It is positioned as an alternative to cesium atomic clocks. The instrument weighs 135 kg and consumes 200W.

2.6 Quantum magnetometers

Quantum magnetometers are used to detect small variations or levels of magnetism with high spatial accuracy. There are many uses cases: navigation, mineral exploration, current detection, magnetocardiography, magnetoencephalography, materials inspection, orientation of drones and autonomous vehicles in tunnels where GPS does not work, sonar, detection of moving metal objects such as vehicles and cellular imaging [1274].

Quantum magnetometry has some other interesting use cases. One is for astrophysics and the search for dark matter of the dark photons variant using atomic magnetometers. For example, [1276] is using 15 atomic magnetometers, which are synchronized with the Global Positioning System (GPS) and are situated on the edges of two meter-scale shielded rooms, serving as a powerful tool to search for dark photons. The magnetic precision is 15 $fT/\sqrt{Hz}$.

A variant is proposed for the detection of the same dark-photons with energies as low as 10^{-22} eV with cold-atoms trapped in MOT and in tweezer arrays. Rydberg atoms are extremely sensitive to external electric fields. A dark photon field, a hypothetical low energy dark matter candidate, could induce a tiny oscillating electric field which would cause transitions or excitations in the energy levels of the trapped Rydberg atoms. The measurement could detect Zeeman shifts (magnetic field-induced energy level changes) or diamagnetic shifts (changes due to magnetic susceptibility) to tune the energy levels of the atoms. This would enable scanning across a range of dark photon masses [1277]. This requires some miniaturization for the MOT and there are multiple options for this [1278].

There are also NV center magnetometers [1279] and even transmon qubits magnetometers [1280, 1281]. Other amazing use cases for NV center magnetometry are the precise measurement of battery charge and discharge [1282], and scanning NV magnetometry (SNVM) to inspect MRAM [1283].

A last one relates to submarine detection. Wang Xuefeng and his team from China Aerospace Science and Technology Corporation (CASC) announced in April 2025 the creation and test of a drone-mounted quantum sensor to detect submarines and map the seabed [1284]. The corresponding study was published on April 16 in the Chinese Journal of Scientific Instrument but is not available online. The proposed system uses a rubidium-based magnetometer to detect variations of the magnetic field, generating seven distinct microwave resonance signals. By measuring these resonances, the sensor can obtain the strength and direction of a magnetic field. This type of sensor would be useful in low-latitude regions, such as the South China Sea, where the Earth's magnetic field is almost parallel to the surface, creating shadow areas where conventional sensors lose effectiveness. During sea trials near Weihai, Shandong Province and western North Korea, the system mapped a 400-meter by 300-meter underwater grid with a magnetic anomaly detection accuracy of 2.517 nT, improved to 0.849 nT after correction. The drone must be within a km of the submarine to detect it reliably, which presupposes knowing where it is in advance. The proposed system would have a sensitivity similar to NATO's existing multi-probe MAD-XR but would be more affordable. The tests need to be carried out in real conditions [1285].

2.6.1 Science

As shown in Figure 128, there are many techniques available for high precision magnetometry, their difference being presented in a double scale with the magnetic noise corresponding to their precision and their effective linear dimension, which is their geometrical accuracy. NV centers are more adapted to short range and mid-precision while SQUIDs and OPMs are useful for longer range and much better precision applications including imaging applications described in a later part.

NV centers

NV centers is the main quantum sensing technology used for detecting both static and oscillating magnetic fields [1286].

Combined with optically detected magnetic resonance (ODMR), it has a sensitivity (or noise) usually ranging from 10^{-9} to 10^{-15} $T/\sqrt{Hz}$ and decreasing as the signal frequency increases [1287, 1288].

It exploits the variation of the NV spin resonance spectrum in the diamond, which depends on the ambient magnetic field (see Figure 130 on spin resonance spectrum and the review [1289]). The distance between the two fluorescent light pulses (Y) generated is measured as a function of the electromagnetic excitation frequency

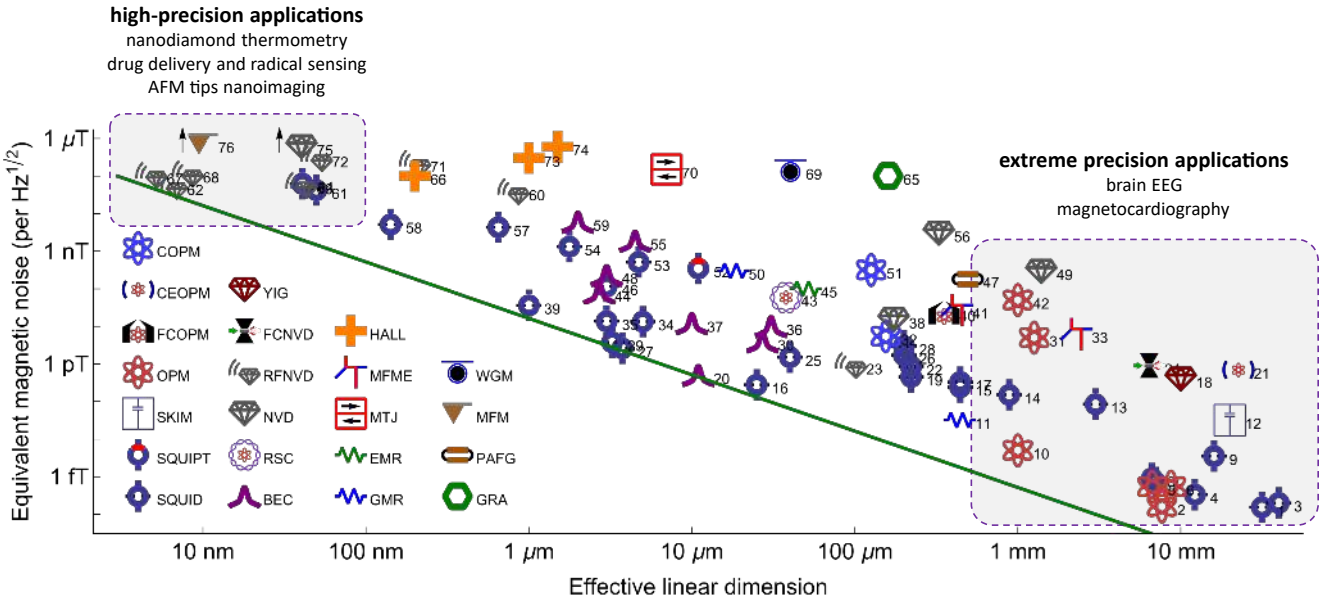


Figure 128: Acronyms meaning: SQUID = superconducting quantum interference device, SQUIPT = superconducting quantum interference proximity transistor, SKIM = superconducting kinetic impedance magnetometer, OPM = optically-pumped magnetometer, FCOPM = OPM with flux concentrators, CEOPM = cavity-enhanced OPM, COPM = OPM with cold thermal atoms, BEC = Bose-Einstein condensate, RSC = Rydberg Schrödinger cat, NVD = nitrogen-vacancy center in diamond, RFNVD = radio-frequency NVD, FCNVD = NVD with flux concentrators, YIG = yttrium-aluminum-garnet, GMR = giant magneto-resistance, EMR = extraordinary magneto-resistance, MTJ = magnetic tunnel junction, MEMF = magnetoelectric multiferroic, HALL = Hall effect sensor, GRA = graphene, PAFG = parallel gating fluxgate, MFM = magnetic force microscope and WGM = whispering-gallery mode. Sources: [1275] and Commercializing Quantum Sensors by Stefan Bogdanovic, SandBoxAQ, QED-C Workshop, June 2024.

used (X). After optical magnification, fluorescence can be analyzed by a CCD image sensor. The spins preparation is performed with a laser and its modification with 3 GHz microwave pulses. NV-center based magnetometers can use large unordered ensembles of NV centers [1290] or individual NV centers [1291].

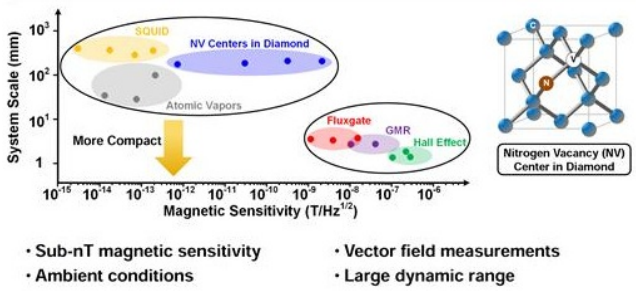


Figure 129: Magnetometers comparison. Source: [1292].

Quantum magnetometers reach picotesla levels and below, billions of times smaller than the Earth's field of about 50 μT. The relevant figure of merit is the noise-equivalent sensitivity, quoted as an amplitude spectral density in T $\mathrm{Hz}^{-1/2}$, and not the accuracy, which is the agreement with a reference standard. Reported NV-center sensitivities span a wide range depending on the device and the bandwidth: single-NV scanning probes sit in the μT $\mathrm{Hz}^{-1/2}$ range [1290], while large NV ensembles reach the pT $\mathrm{Hz}^{-1/2}$ range. NV centers provide a lesser sensitivity than alkali-vapor magnetometers, but their use is more practical because the instrument is easier to miniaturize and most of them work at ambient temperature [1292] (Figure 129). Scanning-probe magnetometers use a diamond nanocrystal hosting a single NV center, that is a substitutional nitrogen atom adjacent to a lattice vacancy. The probe can be moved in space and used to analyze the magnetism of a material in 2D (Figure 130).

NV center sensors could also be used to measure static magnetic fields with being attached to a soft ferromagnetic microwire [1293].

NV, SiV and GeV color centers can measure magnetism under ultra-high pressure up to 240 GPa [1294–1297].

NV centers can be used in quantum magnetic field cameras based on infrared absorption optically detected magnetic resonance (IRA-ODMR) mediated by perpendicularly intersecting infrared and pump laser beams forming a pixel matrix of 3 × 3 pixels for a starter [1298]. It could be useful to detect neural signals.

At last, NV centers help detect transient magnetic signals with a time resolution down to the nanosecond and even picosecond, which could be useful for spintronics and semiconductor characterization [1299].

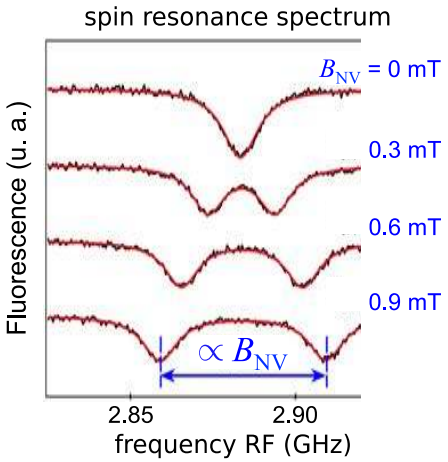


Figure 130: NV center static magnetometry principle using spin resonance spectrum analysis. The two energy gaps which depend on the ambient magnetic field enable the evaluation its current value. Source: [1300].

ODMR and NV centers can probe Oersted fields (long-range magnetic fields) of nano circuits, using three components (directions) of the magnetic field, based on the multiple orientations of defects in NV center diamonds. It is used to reconstruct a 3D view of a chip and detect anomalous current flow in semiconductors or various other heterostructures [1301]. It operates at room temperature [1302]. ODMR widefield imaging can also have high temporal resolution [1303].

NV center readout is usually based on optical single photon counting modules (SPCM) to collect the red NV center fluorescence. It can be replaced by the photoelectric detection of magnetic resonance (PDMR) using a CMOS-based photo-current detector (IPCD) [1304, 1305]. It can reach precision of $1.6\,\mu T/\sqrt{Hz}$ in smaller sensor form factors [1306]. Measurement can be done with spin-to-charge conversion using an SLM with better parallelization [1307].

The NV-centers technique appeared in 2009. It is notably developed in France by **Thales**. ASTERIQS (France, €9.7M) or "Advancing Science and Technology through diamond Quantum Sensing" was a European Quantum Flagship project launched in 2018 and led by Thales, to advance techniques for measuring magnetic, electric, temperature and pressure fields. There are many applications, such as sensors for vehicle battery monitoring, high-resolution sensors for nuclear medical imaging (NMR, nuclear magnetic resonance) or for creating radio frequency spectrum analyzers. The Swiss startup Qnami was involved in the project and provides artificial diamonds. The project was then continued by the 3-year project Amadeus in 2022. It also involved Thales, Diatope, Bosch, SQUTEC, Fraunhofer IAF, University of Stuttgart and IMEC.

Laboratories in Bristol, the University of Ulm in Germany and Microsoft are working on the use of NV Centers techniques coupled with machine learning and Bayesian inference methods to correct the noise found at higher temperatures [1308].

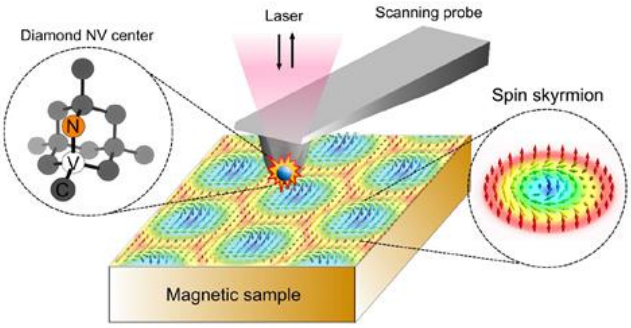


Figure 132: NV centers used in ODMR for medical imaging of materials inspection. Source: [1309].

Different technical approaches are developed to improve NV magnetometry, like using the nuclear spin of the NV center nitrogen atom to drive sensing with an optical control, which can enable compact sensing in magnetometry and gyroscopic applications [1310], using ultrathin NV center layers less than 20 nm below the surface of an ultrapure diamond [1311] and using graphitic electrodes without the need of any metallic deposition on the diamond surface, thereby simplify the sensor fabrication [1312].

In fundamental research, NV centers-based DC magnetometry and SQUIDs can also detect dark microwave photons linked to dark matter [1279, 1313, 1314], including a variant including cat-states in superconducting microwave cavity developed in China [1315].

Other quantum magnetic sensors

NV centers are not the only basis for magnetic field quantum sensing. We also can count on...

- **SQUIDs**, superconducting effect with a Josephson junction as in superconducting qubits [1313, 1316].
- **Cold atoms** with Bose-Einstein condensates (BEC), atomic spins in vapors [1317–1320] and Ramsey interferometry [1321].
- **Surface trapped ions** which can measure both static magnetic fields (DC) or oscillating fields up to range in 100s of MHz [1322].
- **Molecular spins ensembles** can probe AC magnetic fields, using oxovanadium tetraphenyl porphyrin (VO(TPP)) and α, γ-bisdiphenylene-β-phenylally (BDPA). It can study biological systems and topological 2D materials or superconductors [1323].
- **Optomechanics-photonics systems**, like in a 2022 proposal from a China research team. It couples a thin SiN mechanical membrane to Terfenol-D rods with a height that is sensitive to a static magnetic field. The membrane position modifies the phase of a laser-originated photon that is reflected in a cavity containing the membrane. The magnetic field

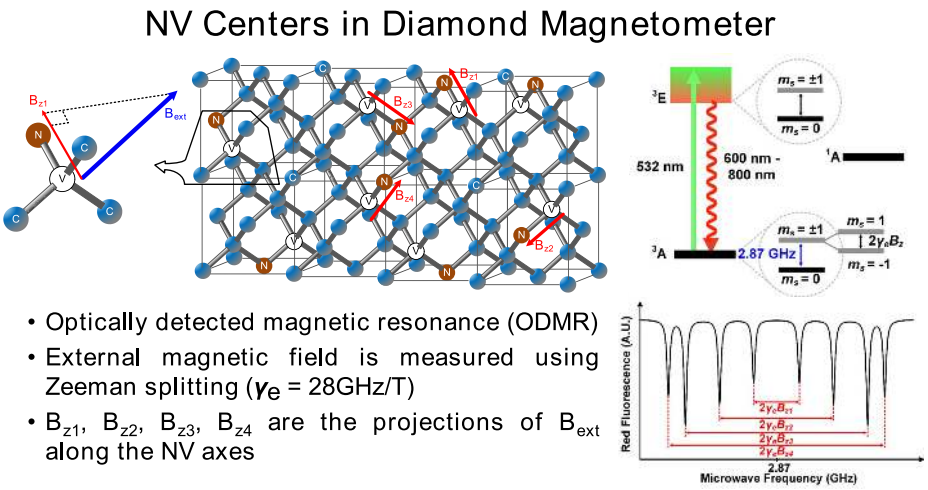


Figure 131: The principle of using NV centers in magnetometers. Source: [1292].

is converted into the photon phase which is measured with homodyne detection using a local oscillator. The sensitivity of this sensor could be excellent, reaching 10^{-15} to 10^{-17} $T/\sqrt{Hz}$ [1324] (Figure 133). Terfenol-D is a magnetostrictive material made from an $Tb_xDy_{1-x}Fe_2$ ($x \approx 0.3$) alloy. Its name comes from terbium, iron (Fe), Naval Ordnance Laboratory (NOL, who developed the material in the 1970s), and D for dysprosium. The material is used to produce sonar systems. Another magnetometry technique, adapted to microwave sensing, is using a p-terphenyl crystal housed within a hollow cylinder of crystalline strontium titanate (STO) and singlet/triplet spin detection with a solid-state maser technology [1325].

- **ESR** (electron spin resonance) microscopy, which can measure magnetism at the individual atom level when coupled with a scanning tunneling microscope (STM) [1326, 1327].

- **Boron-nitride** (hBN) sensors which are nanotubes with spin defects placed on an AFM (atomic force microscope) tip [1328] or 2D hBN structures [1329], both able to measure a directional magnetic field with an ODMR variant which can be multidirectional using bias driving fields [1330] (Figure 134). These operate at ambient temperature.

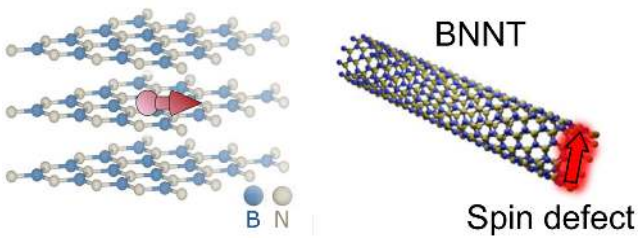


Figure 134: Two types of hBN defects to build directional quantum magnetometers, with 2D structures and nanotubes. Sources: [1328, 1330].

- **SiC-vacancies** (silicon vacancies in silicon carbide) [1331–1336] (Figure 129) as well as **boron nitride** (hBN) vacancies are also used [1337–1340]. They may be preferred to NV centers since they are easier to manufacture.

2.6.2 Vendors

Let's now look at some vendors in the quantum magnetometry space.

Advanced Quantum

Germany, 2023

Advanced Quantum is a spin-off from the University of Stuttgart. It sells NV-center-based sensors, which include characterization tools for spin qubits. The company also sells quantum physics experiments for education and training purposes in universities and companies.

Cerca Magnetics

UK, 2018, £3.8m

Cerca Magnetics is a spin-out from the UK Sensors and Timing Quantum Technology Hub at the University of Nottingham. It develops a wearable magnetoencephalography (MEG) system that avoids the cryogenic cooling required by SQUID-based MEG. It uses optically pumped magnetometers measuring weak magnetic fields. These are made with a laser illuminating a small alkali-metal vapor cell containing rubidium or cesium. A photodiode detects the transmitted light, which depends on the local magnetic field perpendicular to the laser beam [1341]. The technology competes with SQUID-based MEG, not with MRI.

CIQTEK

China, 2016, $18.45M

Figure 133: A SiN-based optomechanics-photonics magnetometry quantum sensor developed in China in 2022. Source: [1324].

CIQTEK manufactures quantum sensors targeting quantum computation, healthcare, food safety, chemistry, and material science markets. These sensors are NV center magnetometers. The company based in Hefei is also named Guoyi Quantum. It was created with the support of Jiangfeng Du (1969) and is led by Yu He, a student of his at the USTC. As of 2024, it had 700 employees. It made its IPO in the Shanghai Stock Exchange in August 2026.

At last, the **Ivar Giæver Geomagnetic Laboratory** (IGGL) in Norway also uses SQUIDs to detect underground magnetism for paleomagnetic applications, to measure the magnetic remanence of ancient rocks. Using SQUIDs, their magnetometer must be cooled to 4K with a pulsed tube [1342].

Deteqt

Australia, 2023, $750K

DeteQt is a spin-off from the University of Sydney Nano Institute that develops NV-center based quantum magnetometers for navigation (including a contract with the Australian Defence Force), critical mineral detection, and medical imaging (with a partnership with OneScan on portable MRI). It uses standard silicon chip fabrication with Global Foundries.

Dirac Labs

USA, 2023, $1.8M

Dirac Labs was co-founded by Sanket Deshpande (CEO) and Aishwarya Das (COO) and is a spinout of UW-Madison. Their product is an NV-center-based positioning system, fusing magnetometry and NVIDIA Jetson Orin Nano-based AI, and using magnetic anomaly maps. Its optical head is packaged in an injection-molded assembly integrated with the diamond into roughly a 5 × 5 cm cube operating at room temperature.

Elta Systems

Israel, 1967

Elta Systems is a subsidiary from the IAI consortium. The company develops various electromagnetic sensors and radars for defense and intelligence.

FieldLine Inc

USA, 2018

FieldLine Inc develops optically pumped magnetometers based on alkali-metal vapor cells, particularly for medical brain imaging (HEDscan) and non-destructive materials testing. The company was created by Orang Alem (CEO), Svenja Knappe and Jeramy Hughes.

GEM Systems

Canada, 1980

GEM Systems is selling quantum magnetometers using optically pumped potassium (K-Mag).

Great Lakes Crystal Technologies

USA, 2019, $20M

Great Lakes Crystal Technologies is a supplier of diamonds for use in NV center applications, especially for quantum magnetometers. It is a spin-off from the University of Michigan and Fraunhofer USA.

kwan-tek

France, 2020, €3.8M

kwan-tek, formerly Wainvam-E, is providing a set of NV centers magnetometry solutions for materials non-destructive inspection (corrosion and cracks detection), and for objects detection and navigation in the industry and defense markets.

They propose MAG-ST an NV-center magnetometer for the stabilisation of high magnetic fields and MAG-NAV, a 3 axis magnetometer for autonomous navigation, and WAINTEACH, a practical work kit in quantum engineering, to contribute to the training of students, launched in 2023 (Figure 135). Its basic modules enable the optical detection of magnetic resonance (ODMR), analyzing the Zeeman effect and hyperfine levels. The

toolkit contains a control unit, 3-axis Helmholtz coils, a photodetector, a laser, NV center diamond and RF antenna, some optomechanical components and software. It can be extended with a pulse generator, an acquisition control board, an AOM (acoustic optical modulator), and an RF switch.

The company partners since March 2026 with Metrolab Technology (Switzerland) for the commercialization of their NV based sensors.

Figure 135: Kwan-Tek's KWANTEACH toolkit for learning how to use NV centers in students training. Source: Kwan-Tek, 2025.

ODMR Technologies

USA, 2015

ODMR Technologies is a stealth spin-off from Berkeley which designs a magnetic resonance spectroscopic analysis system based on NV centers.

QDM.IO

USA, 2021

QDM.IO is creating an NV center based microscope. It comes from the Quantum Catalyzer from the University of Maryland.

Phasor Innovation

Australia, 2021

Phasor Innovation is a company specialized in RF and microwave engineering. They are working on a Quantum Diamond Magnetometer (QDM) with the University of Melbourne and RMIT University. They develop quantum magnetic sensors in collaboration with Israeli research groups and industry partners. These sensors can help detect IEDs (improvised explosive devices, unexploded ordnance, geophysical structures, vehicles and ships). They also work on quantum optical magnetometry and sub-pico-Tesla atomic magnetometers which can be used in medical imaging (MEG).

Q.ANT

Germany

Q.ANT sells a handheld NV-center magnetometer with a vendor-reported sensitivity of 20 pT $Hz^{-1/2}$, operating at room temperature (Figure 136). This is a noise-equivalent field sensitivity and not a spatial or field resolution.

Figure 136: Q.ANT handheld magnetic sensor. Source: Q.ANT.

Qubic Technologies

Canada, 2019, $2.5M

Qubic Technologies is a startup from the Institut Quantique from the University of Sherbrooke in Quebec led by Jérôme Bourassa. The company is working on microwave-based quantum sensing tools for sensing, imaging and communications. It is mainly developing quantum radars along with Christopher Wilson from the University of Waterloo, Sreeraman Rajan from Carleton University and Zero Point Cryogenics.

Qsensato

Italy, 2024, €500K

Qsensato is a spinoff from the University of Bari which develops atomic-photonic chips for OPM-based quantum sensing and metrology applications using femtosecond laser-written vapor cells (LWVCs), achieving picotesla sensitivity [1343]. It targets biomedical and lab-on-chip, space and defense, remote sensing, and automotive applications. The company has collaboration with ICFO and CNR-IFN in Milan.

QuantX Labs

Australia, 2016

QuantX Labs is working on NV-center magnetometer arrays and their application to detect subterranean structures and materials in the field.

Quantum Technologies

Germany, 2020

x Quantum Technologies is a spin-off of the Jan Berend Meijer group at Leipzig University. It is industrializing NV center based technology including diamond material and sensing related optics and electronics. They sell optical fiber-based magnetic field sensors utilizing diamond powder with a high NV-center density. These sensors have a small footprint, are non-magnetic and non-conductive. They can be used for current sensing and in various medical applications. What a company name! It is impossible to do a search on it!

Qutools

Germany, 2005

Qutools offers its quNV quantum magnetometer kit, based on diamond NV-centers as its name suggests. It fits in a 3U rack (Figure 137). They also sell an interferometer for interferometric displacement measurement.

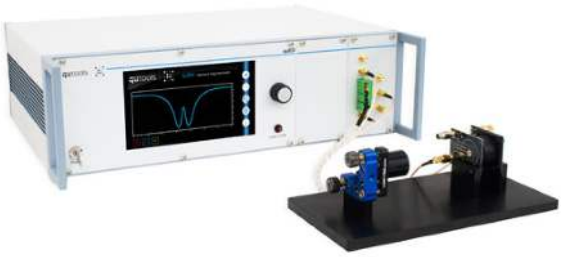


Figure 137: A quantum magnetometer from qutools.

The company also developed quTAG, a time-to-digital converter that records timing events and provides a timestamp with picosecond precision for each event. It is used for time-correlated single photon counting (TCSPC), coincidence measurements, start-stop measurements, auto- and cross-correlations measurements and other applications.

Also, in Germany, the University of Stuttgart is working with the Fraunhofer Institute to transfer NV-centered magnetometry technology as part of the **QMag** [1344] project.

Q-Sensorix

USA, 2019

Q-Sensorix develops NV centers magnetometer-based gyroscopes, launched by Alexey Akimov, Vladimir Shalaev and Yuri Lebedev. These are alumni of the University of Buffalo in New York State.

SandboxAQ

USA, 2022, $975M

SandboxAQ tested in May 2023 its airborne quantum sensor-based magnetic anomaly navigation system with the US Air Force aboard a C-17 GlobeMaster III transport aircraft. This Assured Positioning, Navigation, and Timing (APNT) solution is designed to complement classical GPS to provide uninterrupted navigation when GPS is unavailable or intentionally denied or spoofed by enemies. The system collects data from NV sensors and uses machine learning to filter out the ambient noise generated by the airplane. The benefits of the system are manyfold. The Earth's magnetic field cannot be jammed. It can be detected in any weather condition, and it works passively.

SQUTEC

Germany, 2018

SQUTEC produces diamonds with vacancies and NV center based quantum sensors for magnetometry, electrometry and thermometry. They are also developing a NV center-based quantum computer.

Supracon

Germany, 2001

Supracon manufactures magnetometers based on SQUIDs (Superconducting Quantum Interference Devices). It is a spin-off of the Leibnitz Institute of Photonics in Jena. It sells its sensors to astrophysics research laboratories and for geophysics prospection.

Twinleaf

USA, 2007

Twinleaf develops optically pumped atomic magnetometers based on alkali-metal vapor cells, the laser being used to pump and probe the vapor. The company is headed by Elisabeth Foley, a specialist in the field, and Thomas Kornack (CSO), both Princeton alumni.

2.7 Quantum electric field sensing

Quantum electric field sensing is a lesser known quantum sensing domain. It can make use of trapped ions ensembles [1346, 1347], cold atoms [1348–1350], NV centers [1351, 1352] and SiC centers [1353, 1354]. I have not identified any company proposing such a technological solution.

2.8 Quantum RF sensing

Radio-frequency measurement is well established, but it is still progressing thanks to quantum technologies often associating optronics with cold atoms. Wideband frequency quantum sensing can be implemented with neutral atoms and NV centers.

2.8.1 Science

There are various types of quantum radio frequencies sensors.

Cold atom-based sensors paired with optical readout using coherent spectroscopy can analyze electromagnetic-wave frequencies from direct current (0 Hz) to the THz range. This is due to their so-called high-energy Rydberg states which can help measure high-frequency electro-magnetic waves thanks to their strong dipole [1355]. It can help reduce the size of various antennas, improve radio frequency filtering, extend the range between mobile communications cellular towers and improve sensitivity [1356]. This sort of broadband

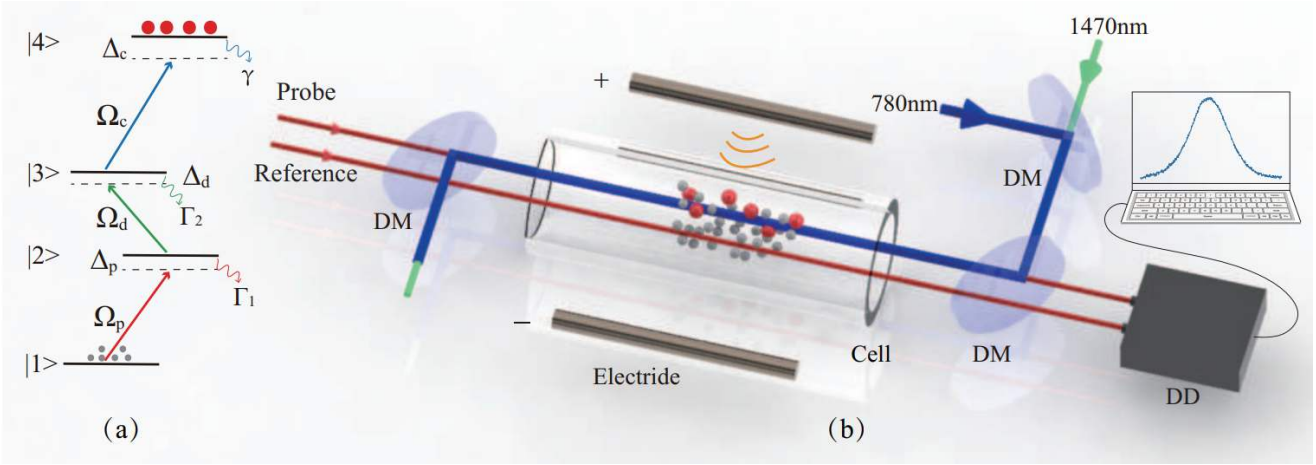


Figure 138: How neutral atoms are used to measure the electromagnetic-wave frequency spectrum in a highly sensitive solution developed in China, using a hot vapor cell of cesium atoms excited by lasers in their Rydberg states. The grey electrodes are connected to an RF antenna. Source: [1345].

How do we probe the transverse electric and magnetic fields of electromagnetic wave?

It requires specialized sensors and setups to measure each field component separately and confirm their orientation relative to the direction of wave propagation.

Measuring the electric field is commonly done with dipole antennas. They respond to the electric field component aligned with their axis, so by rotating the dipole, one can map the direction of the electric field. Other techniques include electro-optical sensors, which rely on materials whose optical properties change in response to electric fields. With optical photons, this is done by probing the polarization of light passing through these materials. In microwave and radio-frequency setups, near-field scanning probes can also be used to map the electric field distribution close to the source.

Measuring the magnetic field is more difficult due to its weaker interaction with sensors. Loop antennas offer a practical solution. A small conducting loop responds to the magnetic flux through its area. By orienting the loop in different directions, one can isolate the magnetic field component perpendicular to the loop. Magneto-optic sensors use the Faraday effect to detect changes in light polarization caused by magnetic fields and can measure high-frequency or pulsed fields. Superconducting quantum interference devices (SQUIDs) can detect minute magnetic fields for low-frequency or static fields.

Some sensors measure simultaneously the electric and magnetic fields. Dual-mode sensors developed for electromagnetic compatibility testing combine orthogonal dipole and loop antennas to capture both field components in the near-field region. These setups are often used in antenna characterization and waveguide analysis.

The time varying sinusoidal shape of electromagnetic waves can be measured with radio waves thanks to their long wavelengths that are compatible with the capabilities of electronic sensors. However, you don't detect individual photons but measure the collective effect of many photons. Radio transmitters generate coherent sources with well-defined phase, which maintains the sinusoidal form of the electric and magnetic fields. At optical frequencies, direct photodetection measures intensity or photon arrivals rather than the carrier oscillation, which is far too fast for any detector. Phase-sensitive information is still accessible through interferometry, homodyne or heterodyne detection against a local oscillator.

spectrum analysis can have multiple use cases, particularly in the military and intelligence sectors. These systems do not necessarily provide high spectral resolution and can be used as "heads-up" spectrum analysis tools before more specialized tools are used for specific parts of the electromagnetic spectrum. Such sensors have been tested by British Telecom to create more sensitive 5G base antennas [1357].

Recent work has improved these neutral-atom electromagnetic spectrography systems, notably in the MHz bands [1345, 1358] (Figure 138) and for creating isotropic (covering all directions) antennas [1359].

A quantum sensor based on alkali atoms excited to Rydberg states can cover the radio spectrum from 1 kHz to 100 GHz [1345, 1358, 1360–1368]. That span is an aggregate coverage obtained by changing the addressed

atomic transitions and the laser frequencies, not a continuous instantaneous bandwidth, which stays narrow around each transition. Other quantum sensors can analyze radiation in the 1 THz band, the terahertz region lying between microwave and infrared, with potential applications in the measurement of the thickness of thin layers of heterogeneous materials. Rydberg atom radiofrequency sensors can also be used to build three-dimensional polarimeters [1369]. They are also very efficient at capturing weak microwave signals [1370–1372] like the ones emitted by satellites [1373]. These sensors have a wealth of applications in space [1374].

NV-center sensors can help run RF spectral analysis, from 0 to 40 GHz, with the advantage of being lighter than most neutral-atom sensors [1375, 1376]. RF electrometry with NV centers relies on optically detected magnetic resonance (ODMR) and on the NV spin transitions. Nuclear magnetic resonance is a distinct configuration, in which the NV center detects the fields produced by the nuclear spins of a nearby sample [1377]. NV-center sensors can even be arranged in sensor arrays enabling both a wideband spectrum coverage and a high-precision analysis of a target band [1378]. ODMR-based NV-center ensembles can implement high-resolution spectroscopy down to the Hz from 10 MHz to 4 GHz [1379]. Improvements enable RF sensing with single-shot measurements [1380].

Pure optical techniques can be used to implement frequency sensing in the THz range [1381]. And surprisingly, it can also work, in a different fashion, to create quantum optical microphones with the benefit of improving the quality of AI-based speech recognition [1382].

Optical sensors using spectral hole burning (SHB) are a technology developed by Thales that relies on a "rainbow architecture". An RF signal is first converted to optical wavelengths using a Mach-Zehnder electro-optical modulator driven by a laser, the resulting optical beam is then diffracted by a rare-earth-ion-doped crystal cooled to 3 K, and the result is finally detected by an array of photodetectors. It supports a 20 GHz bandwidth with sub-MHz resolution (Figure 139). Thales also works on RF quantum receivers based on Rydberg atoms [1383].

Quantum antennas. Research on quantum-enhanced antennas explores nonclassical resources, including squeezed states, for specified sensing or communication tasks [1384]. It is an emerging field that can address other needs, like field shaping, quantum radars, quantum imaging and creating antennas for THz electromagnetic fields using quantum dots [1385]. Since 2022, **BAE Systems** (UK) is developing quantum antennas on behalf of DARPA.

Superconducting qubits can act as electrometers or as microwave single-photon detectors, detecting the quantized electric field of a microwave photon. This capability underpins a **proposal** to detect high-frequency gravitational waves through the inverse Gertsenshtein effect, in which gravitational waves crossing a strong static magnetic field are resonantly converted into electromagnetic waves [1387]. The proposal assumes a very high quality factor cavity, a strong magnetic field and a noise budget that no experiment has demonstrated so far.

2.8.2 Vendors

Infleqtion

USA, 2007

Infleqtion develops SqyWire, an atom-based wide spectrum Quantum Radio Frequency (QRF) aperture and receiver system that is tested by the US Army (Figure 140). It uses a three-laser scheme to excite atoms to Rydberg states in a room-temperature vapor cell. The atom states are then captured by photon detectors.

It covers many RF bands: HF/VHF/UHF (radio), L/S-band (some airborne radars), C-band (used in telecommunications, aka microwaves and 5G), X-band (weather radars), Ku/K band (used in satellite communications), all in one. It uses RF splitting of EIT/EIA lines (electromagnetically induced transparency or absorption) using the AC Stark effect discovered in 1955 by Stanley Autler and Charles Townes.

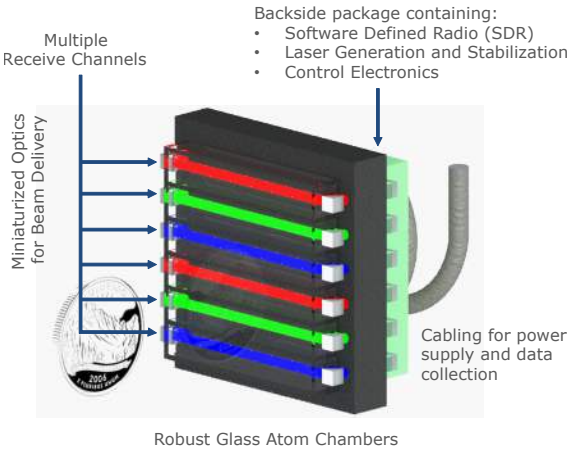


Figure 140: Infleqtion's SqyWire vapor atom-based RF sensor. Source: [1388].

In that effect, an oscillating electric field is tuned in resonance or close to the transition frequency of a given spectral line and results in a change of the shape of the absorption/emission spectra of that spectral line.

Thales

France

Thales is developing a real-time radiofrequency spectral analyzer *aka* a Quantum Diamond Signal Analyzer (Q-DiSA) with a bandwidth of 10 MHz to 25 GHz and a frequency resolution of 1 MHz, based on NV centers [1389]. The frequency adjustment is done by controlling

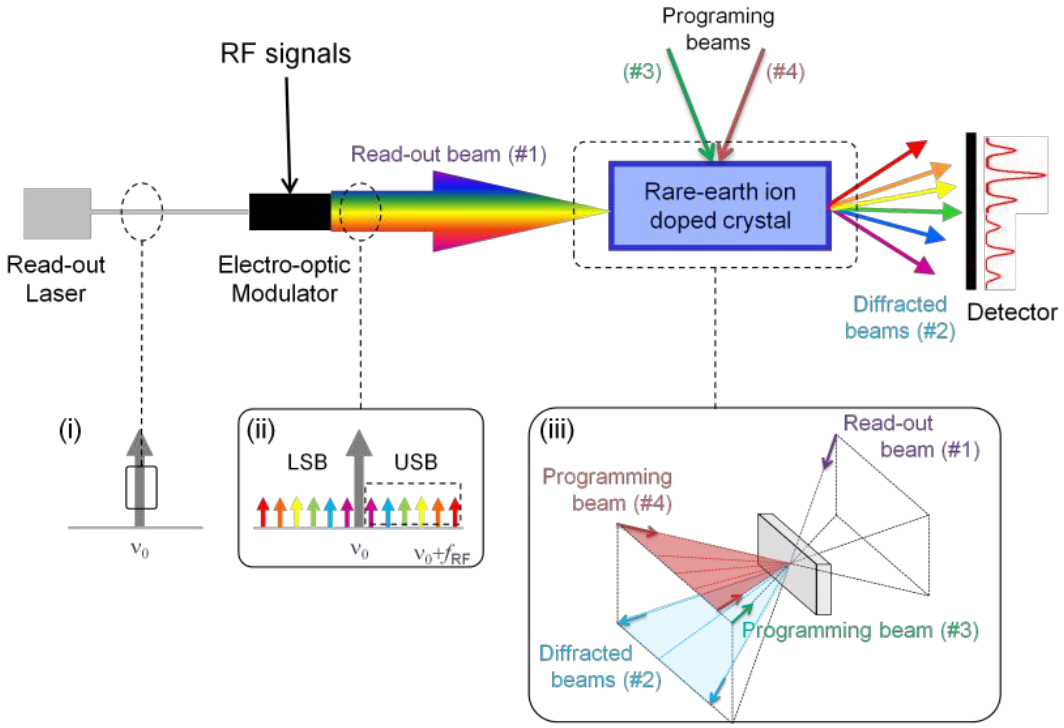


Figure 139: Spectral hole burning (SHB) RF sensing technique developed by Thales. It uses a "rainbow architecture" that starts with a RF signal conversion to optical wavelengths using a Mach-Zehnder electro-optical modulator driven by a laser and then, diffraction of the resulting optical beam by a rare-earth-ion-doped crystal cooled to 3 K, followed by detection with an array of photodetectors. It supports 20 GHz bandwidth with sub-MHz resolution. Source: [1386].

the distance of the NV center with a small 1.3 cm magnetic sphere. The system is using a 532 nm laser and a CMOS sensor.

Rydberg Technologies

USA, 2015

Rydberg Technologies provides cesium or rubidium specimens for cold atom-based radio frequency sensing solutions.

They sell Rydberg lasers, a Rydberg atoms-based radio-frequency probe, a RFMS (Rydberg Field Measurement System) covering the 1MHz-100 GHz frequency range, and Rydberg vapor cells [1390]. Their technology is also integrated in AM and FM radio-frequency receivers as well as in radars.

It enables long range radio communication. Their roadmap shows how far they are going with miniaturizing their device and reducing its power consumption (Figure 141).

2.9 Quantum imaging

Potential benefits of some quantum-imaging methods include super-resolution beyond the Rayleigh diffraction limit, noise reduction obtained by keeping only the events coincident in two independent detection systems, and an improved signal-to-noise ratio in transmission imaging at ultra-low light levels through signal-idler coincidence counting, known as sub-shot-noise imaging [1391, 1392] (see some quantum imaging methods in Figure 144). Each of these holds for a specific protocol, resource count and classical baseline rather than for quantum imaging in general. Quantum sensing is enlarging the scope of what is possible to do in imaging, at both the nanoscale (atoms), microscale (biological cells [1393] and biomedical imaging [1394, 1395] Figure 142, including neuronal electrical activity imaging [1396]) and larger scale levels [1397, 1398], non-destructive material inspection and also telescope imaging [1399].

2.9.1 Science

These new tools are based on various techniques that we will cover here. The list mixes modalities, so each item is best read with its status in mind: **quantum-enhanced** when a nonclassical state or correlation improves the measurement, **single-photon** when the detector counts individual photons without a nonclassical probe, **quantum-enabled** when the device exploits quantum material properties without coherent control, and **classical comparison** when an item is included as a benchmark:

- **SQUIDs** are superconducting interference devices used as extremely sensitive magnetometers and as readout elements for some cryogenic detector arrays [1400]. They are not synonymous with superconducting qubits, although both technologies use Josephson junctions. SQUIDs are widely used in biomag-

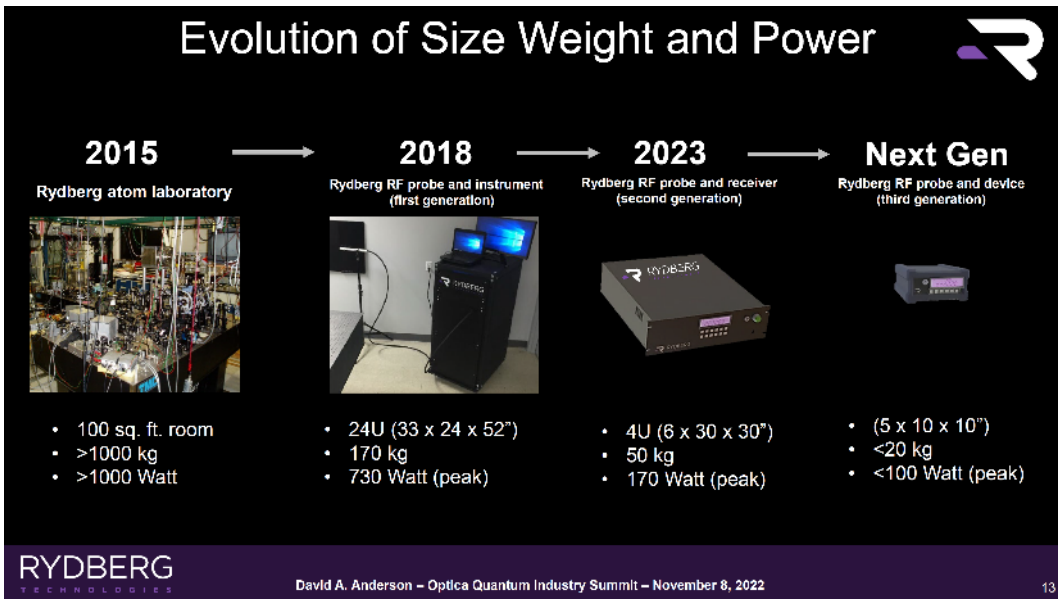


Figure 141: Rydberg Technologies miniaturization roadmap as presented at the Optica Conference in November 2022. Source: Rydberg Technologies. Added in 2023.

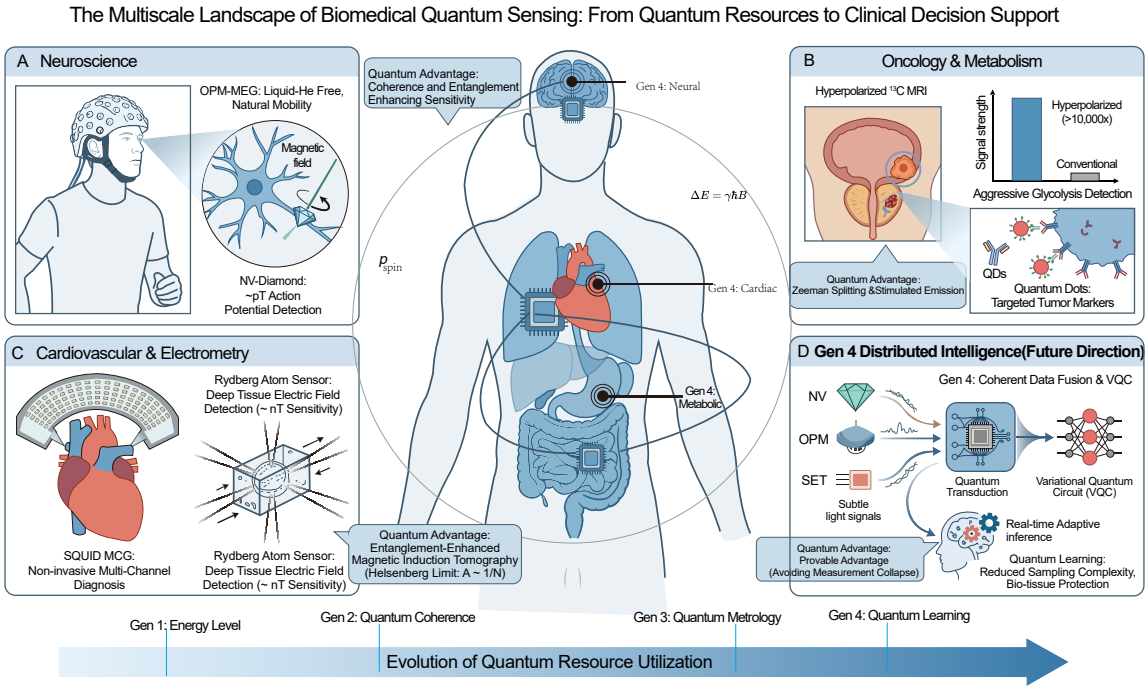


Figure 142: Evolution of biomedical quantum sensing across neuroscience, oncology and cardiovascular medicine, and emerging solutions using coherent data fusion via quantum transduction and adaptive inference through variational quantum circuits. Source: [1395].

netism, including MEG, and in cryogenic instrumentation. Some superconducting detector architectures for millimeter, submillimeter and X-ray astronomy use SQUID-based readout, but JWST/NIRSpec is not an example because its focal-plane detectors are semiconductor HgCdTe arrays. Superconducting radio-frequency cavities are a different technology and can be used in searches for dark photons [1401].

- **SNSPD cameras** [1402, 1403], which can be arranged in 1D and 2D arrays [1402, 1404, 1405]. The largest reported to date is a 400,000-pixel camera published by NIST in 2023 [1406]. It can be used for example in astrophysics (Figure 143).

- **Quantum-enhanced Raman microscopy** using a bright squeezed single-beam, enabling operation at the optimal efficiency of the SRS (Stimulated Raman scattering) process. It can be used to gener-

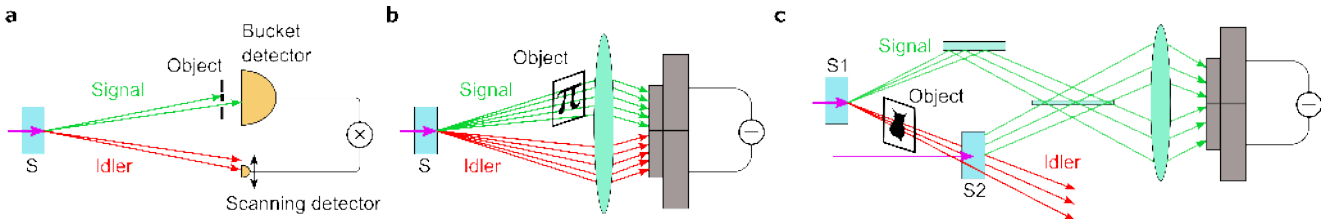


Figure 144: Examples of quantum imaging methods. a) **Ghost imaging** with a source S emitting pairs of spatially entangled photons. The signal photons pass through an absorptive object and are then collected by a 'bucket' detector. The object shape is recovered by scanning a spatially-resolving detector in the idler channel and registering signal-idler correlations. b) **Sub-shot-noise imaging** with twin beams where a weakly absorbing object is placed in the signal beam and the images of both beams are detected by cameras and subtracted. The image noise is then reduced due to the signal-idler photon-number correlations. c) **Imaging with undetected photons** where coherently pumped sources S1 and S2 generate photon pairs, so that idler photons from S1 pass through S2. Signal photons from both sources are overlapped on a beam splitter and they interfere if their idler partners are indistinguishable. An object placed in the idler channel between the two sources breaks this indistinguishability, allowing a camera in the signal channel to reveal the shape of the object. Image and caption from [1392].

ate quantum-enhanced multispectral images of living cells of 100×100 pixels [1407].

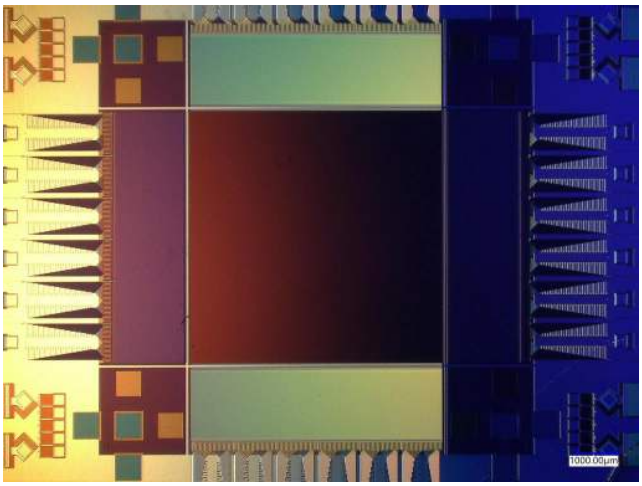


Figure 143: The 400,000-pixel SNSPD camera chip from NIST, developed in 2023. Source: NIST.

- **NV-center** magnetometry used to implement nanoscale NMR spectroscopy, valued for its spatial resolution and readout precision. NV-center image sensing is often used in confocal microscopy due to its small range [1408]. Variants use other point defects, such as color centers in hexagonal boron nitride, which enable standoff distances down to 1 nm [1409]. NV-center and other defect-based imaging at the nanoscale is often done with a scanning quantum microscope (SQM) which moves a tiny diamond over the surface to analyze [1410]. NV centers can even image the photonic spin texture (PST) of a material, meaning the spatial distribution of the spin angular momentum (SAM) of light [1411].
- **OPMs**, that is optically pumped magnetometers based on alkali-metal vapor ensembles, which can be used in material science and chemistry [1412] and for neural imaging in magnetoencephalography (MEG) [1413].
- **Entanglement-based imaging** with scanning quantum microscopy by coincidence (QMC) or imaging by coincidence from entanglement (ICE), reported to reach Heisenberg-like resolution scaling for the specific protocol and resource count used, with better contrast-to-noise ratios (CNRs) than the wide-field quantum imaging methods it was compared against [1414, 1415]. Entanglement-based imaging is also applicable to X-rays [1391]. On larger scales, entanglement-assisted telescope arrays are **proposed** to improve the spatial resolution of optical telescopes. They rely on long-baseline interferometry and approach the quantum Cramer-Rao bound for the estimation task considered, under idealized loss and noise assumptions [1416–1418].
- **Super-resolution imaging** using interferometry in the microwave regime for passive remote sensing [1419], for example satellite measurements of soil moisture, ocean salinity and ground temperature [1420].
- **Laser interferometry** makes it possible to examine molecules under ambient or operando conditions rather than only under vacuum at cryogenic temperature, at the spatial resolution allowed by the specific optical technique used [1421].
- **Thermal light based quantum sensing** using a sub-threshold diode laser with a spectral density exceeding that of SPDC sources by approximately 10 orders of magnitude [1422].
- **Light-field microscopy** (LFM), where volumetric information is captured in a single shot by recording both the spatial position and the propagation angle of the rays reaching the sensor, and not the optical angular momentum. It has a depth of field of ∼500 μm, 3 times better than the latest LFM designs or >100 times what can be obtained with conventional microscopes [1423].

- **Single-pixel cameras**. Single-pixel imaging reconstructs an image from a sequence of structured illumination patterns measured by one non-imaging detector, the photon flux per pattern depending entirely on the implementation and not implying one photon per image pixel. Jian-Wei Pan's Hefei laboratory developed a photon-counting version operating at very low light levels, associated with algorithms filtering out the noise. Imaging is done in the infrared at 1,550 nm and with polarized photons. This could be integrated in observation satellites [1424]. Single-pixel cameras implement spectrography in the infrared spectrum, using colloidal semiconductor quantum dots [1425, 1426].
- **Giant magnetoresistance** (GMR) microscopes, listed here as a **classical comparison**, GMR being a spintronic transport effect used without coherent control or a nonclassical probe. They provide excellent nanoscale spatial resolution but come at the expense of much lower field sensitivities [1427]. These are based on a magnetoresistance effect observed in thin film structures composed of alternating ferromagnetic and non-magnetic conductive layers. It creates significant changes in electrical resistance depending on the relative alignment of the magnetization in the ferromagnetic layers when an external magnetic field is applied. The sensor is made with these films, which may be scanned over the examined sample with piezoelectric actuators. The electrical resistance changes in the GMR film sensor are measured and converted into voltage signals and processed classically to create a map of the magnetic field distribution in the sample. GMR microscopes are used to examine magnetic storage media, thin films, nanostructures, magnetic sensors, actuators, and other advanced materials. They can detect and image magnetic nanoparticles used in biological imaging. The shortcomings of GMR microscopes are that the film sensor is hard to manufacture. They are also sensitive to temperature variations and external magnetic noise.
- **Nanoscale magnetic resonance imaging** (NanoMRI), which can itself be based on NV center, Electron spin resonance (ESR) combined with scanning tunneling microscopy (STM), and superconducting resonators [1428].
- **Quantum Fourier transform infrared** (QFTIR) spectroscopy for the detection of organic gases [1429] (Figure 145).
- **Underwater LiDAR** using single-photon CMOS detection arrays (SPADs) directly interfaced to a GPU for real-time image reconstruction, but with a range of only 3 meters [1430].
- **Transmission electron microscopes** (TEM) which can deliver atomic resolution thanks to the short (de Broglie) wavelength, mostly implemented in cryo-EM for cryogenic electron microscopes, and which can be improved with electron spin squeezing [1431].
- **Free electrons illumination** and nanophotonics, but it is at best in type I quantum sensors [1432, 1433].
- **Quantum-light-enhanced stimulated Brillouin scattering** (SBS) can enable nanomechanical observations at the cellular and subcellular levels, like the study of viscoelastic property changes over time. SBS is a nonlinear optical process occurring when light interacts with acoustic waves or phonons within a medium, such as an optical fiber or a crystal. It can be quantum-enhanced with improved signal-to-noise ratio using a quantum squeezed light source generated with a four-wave mixing (FWM) process in an atomic ^{85}Rb vapor cell [1434].

We will also look at "ghost imaging" systems, which take pictures of objects with a single-pixel sensor, and at other special quantum sensors.

2.9.2 NV centers imagers

NV-centers imagers can be used to analyze organic molecules with excellent spatial resolution [1412] as well as various materials, as well as 3D semiconductor chips [1435] and even improve X-ray telescopes imaging [1436].

These are different configurations. In NV ODMR, a green laser initializes the NV spin and microwaves drive its own spin resonance, the fluorescence contrast reporting the local field. This works at room temperature. In nanoscale NMR, the NV center detects the weak magnetic fields produced by the nuclear spins of a nearby sample [1437]. Driving the spins of the examined material with microwaves, and operating at cryogenic temperature, apply only to specific protocols such as scanning-tunneling-microscope ESR, where the technique is integrated into an STM or an atomic force microscope (AFM). There are many variants of quantum diamond microscopes (QDM) [1438–1440]. NV-center imaging has many other variations like QDMTM (quantum-enhanced diamond molecular tension microscopy) which could quantify integrin-based cell adhesive forces [1441].

The NV-center technique also enables the examination of a hard disk and semiconductor defects with a probe equipped with a single NV-center as shown in Figure 149 and Figure 148. It is also used for the characterization and inspection of integrated circuits working with millimeter frequencies such as in 5G [1442] and even materials under heavy pressure [1443].

Others are working on NV centers-based microscopy of living cells [1444]. There is even an application to qualify malaria patients by analyzing hemozoin nanocrystals appearing in red blood cells affected by the disease parasite [1445].

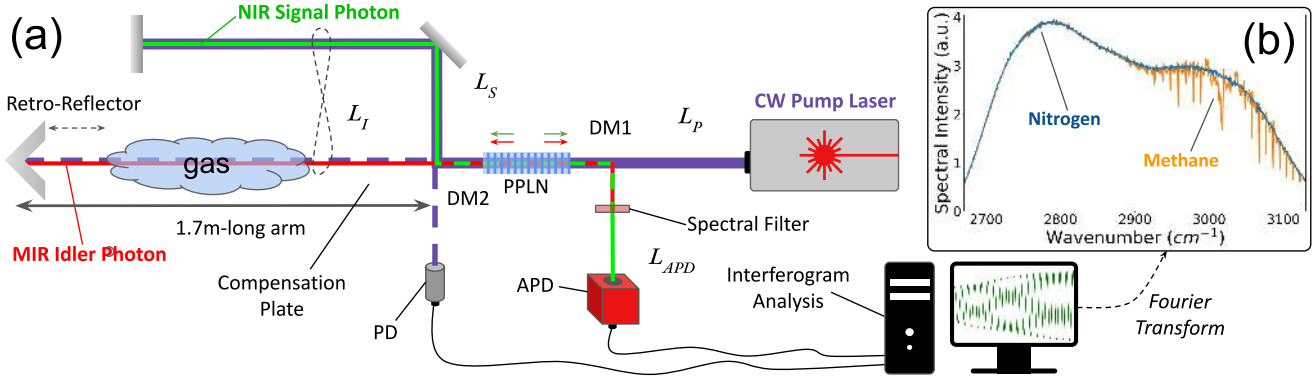


Figure 145: Quantum Fourier transform infrared (QFTIR) spectrometer uses a nonlinear Michelson interferometer. A periodically poled nonlinear crystal (PPLN) is pumped by a narrow-line CW pump laser, generating spectrally entangled signal and idler photons via SPDC (spontaneous parametric down-conversion). This conversion process occurs with low probability, either on the pump's first passage or its second passage, after all modes have traveled through the interferometer and have been reflected back into the crystal. The overlap of all beams in the interferometer erases the which-way information, making it impossible to know whether the photons were emitted on the first or second passage. By induced coherence, interference appears in the signal channel when the idler path length changes. A classical Fourier transform of the resulting interferogram obtained by the APD (avalanche photodiode) readout gives the spectral intensity of the idler photon, including the absorption of a sample placed on its path. Source: [1429].

These techniques are used with confocal microscopy. This generates images with a very shallow depth of field of about 400 nm, creating optical sections of the sample to analyze. By modifying the position of the depth focal plane, a series of images are created which are then assembled to generate a 3D view of the analyzed sample. The light source is reflected or obtained by fluorescence in reaction to a laser beam.

The result is a Confocal Laser Scanning Microscope (CLSM). NV-centers also improve the accuracy of adaptive optics, which are used in astronomy [1446]. NV-center-based microscopy also analyzes the time evolution of magnetic fields [1447]. The fluorescence light can be detected with SPAD (single photon avalanche diodes) as described in [1448]. It can help accelerate the image acquisition which is otherwise usually slow [1449].

Another application detects faulty hemoglobin in several forms of anemia (methemoglobin or MetHb) with NV center imaging combined with X-ray photoelectron spectroscopy (XPS) and atomic force microscopy (AFM) [1450]. Imaging also exploits an array of small NV centers that provide much better resolution than imaging systems based on SQUIDs magnetometers and can do magnetometry imaging [1451].

The example in Figure 146 shows its architecture [1452]. The NV-center arrays are 100 μm wide. [1453–1455]. The second was made to study bacteria that contain magnetic microelements. In other cases, magnetic markers can be used to attach themselves to the cells to be detected, typically in oncology. NV centers could also be used in heart monitoring using magnetocardiography [1456]. It was tested on rats in Japan, as shown in Figure 147 [1457].

The European Quantum Flagship includes **MetaboliQs** (Germany, €6.7M), a diamond-based nuclear magnetic resonance cardiac medical imaging project.

It also detects atrial fibrillation, a common cardiac pathology, with a rubidium-based atomic magnetometer [1458]. Another Flagship project, **PhoG** (United Kingdom, €2.6M) or Sub-Poissonian Photon Gun by Coherent Diffusive Photonics, is about creating stable light sources for various applications, particularly in quantum sensing. It involves researchers from Belarus, Germany and Switzerland.

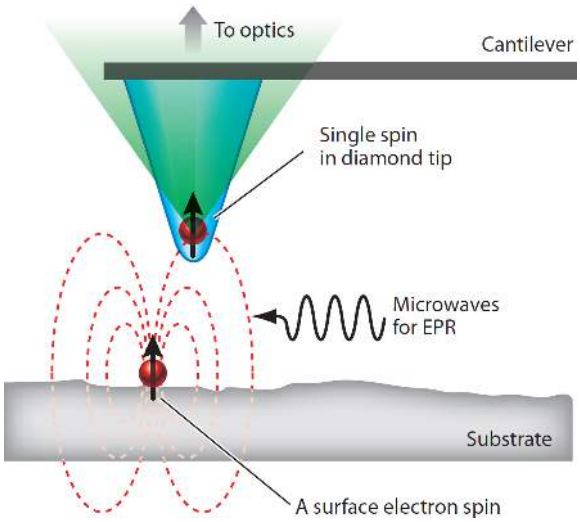


Figure 149: Typical NV center in a diamond tip for various imaging applications. Source: [1460].

Other vacancies like color centers in hexagonal boron nitride (hBN) in 2D layered structure have a similar broad spectrum of applications to measure static magnetic fields, magnetic noise, temperature, strain, nuclear

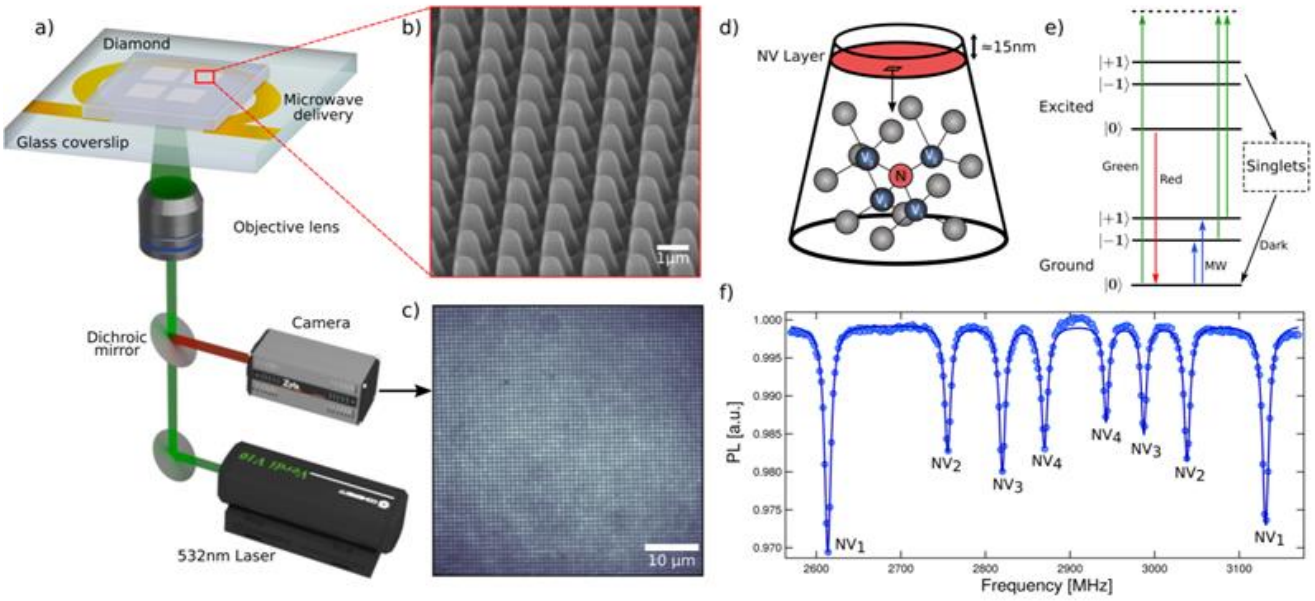


Figure 146: Widefield array of NV centers to improve their sensitivity, developed in Australia. Source: [1452].

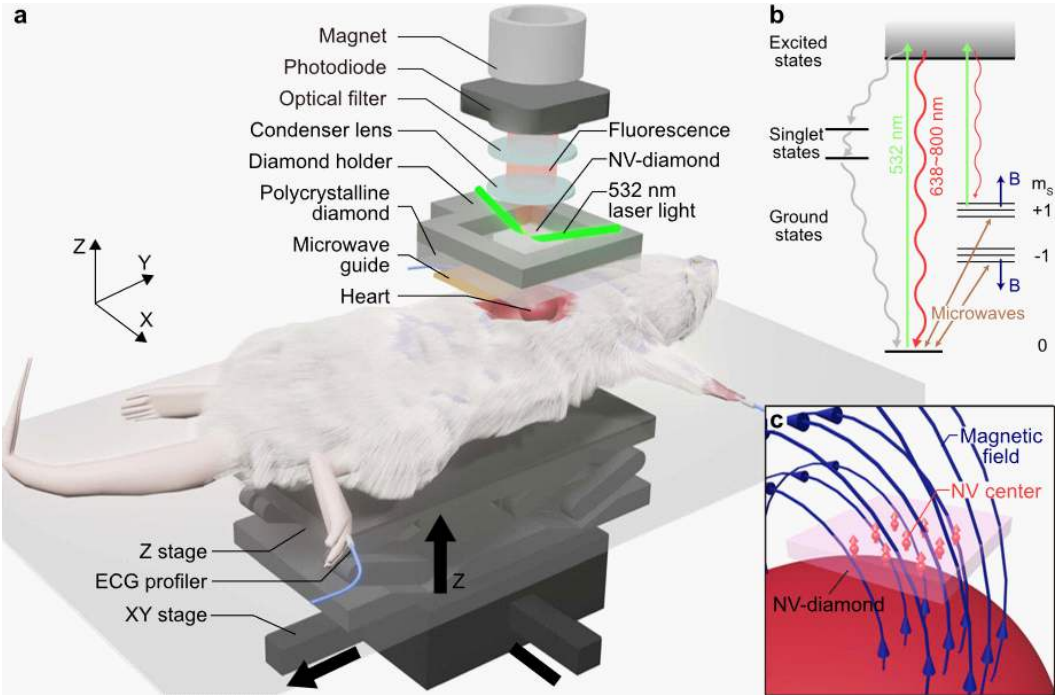


Figure 147: NV center based magnetocardiography experiment on rats. Source: [1457].

spins, paramagnetic spins in liquids and RF signals [1461, 1462].

2.9.3 OPMs

Optically pumped magnetometers (OPMs) enable the measurement of very weak magnetic fields and are based on the Zeeman effect [1463]. They can be configured as scalar sensors, measuring the field magnitude, or as vector sensors, depending on the pumping and modulation scheme. These sensors emerged in the 1970s and expanded since the 2000s thanks to a better sensitivity, on par with SQUIDs.

One of their main use cases is MEG (magnetoencephalography) to examine brain activity [1464] but they can also be used for materials inspection [1465]. OPM-MEG is an alternative to conventional SQUID-MEG and complements structural or functional MRI rather than competing with it. Clinical MRI uses superconducting magnets and RF coils, not SQUID detection, and MRI and MEG provide complementary information. OPM sensors are lighter, can be wearable, and do

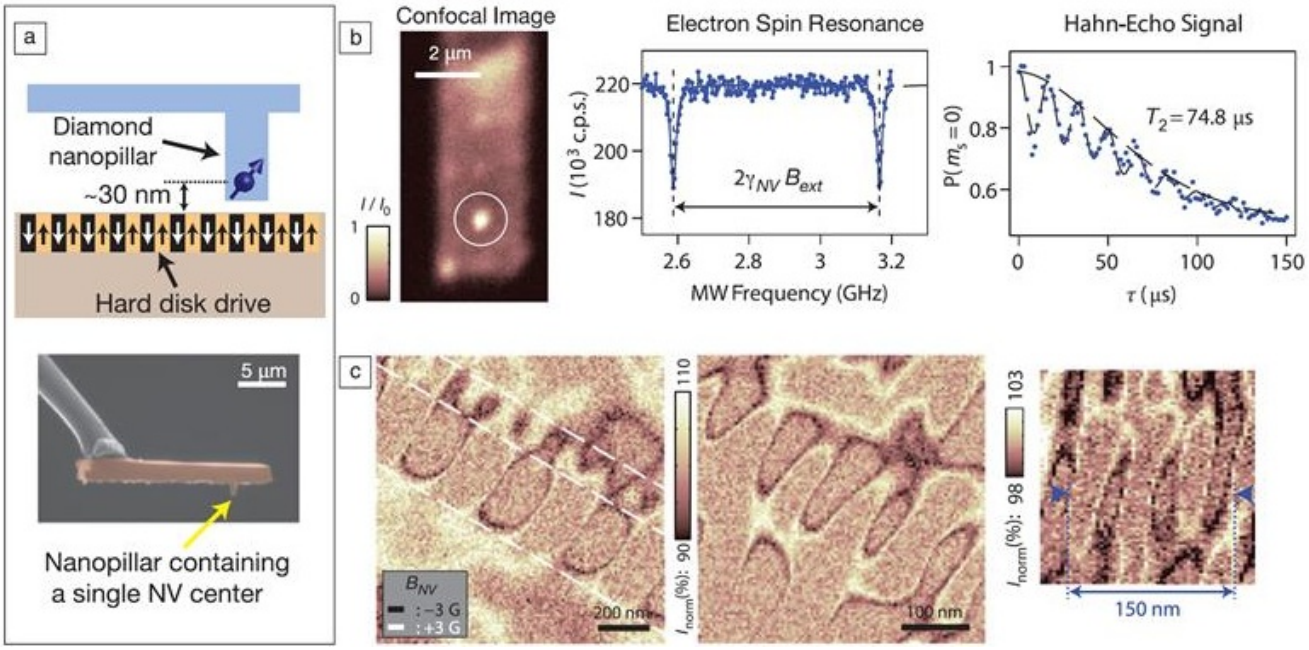


Figure 148: Schematic of a monolithic diamond nanopillar probe (top) and representative SEM image of the nanopillar probe (bottom). (b) Characteristics of a nanopillar probe device. Confocal image of the device (left) clearly shows a localized fluorescence spot from a single NV center at the position of the nanopillar. Electron spin resonance (middle) was acquired with an enhanced fluorescence of 220,000 photons/sec. The coherence time of the measured Hahn-echo signal (right) is 74.8 μs, an order of magnitude longer than a typical Hahn-echo coherence time of commercial diamond nanocrystals ($\sim 5\ \mu s$). (c) Magnetic images of a hard disk drive acquired by the nanopillar probe. Alternating magnetic bits were imaged with varying sizes down to 25 nm (right), indicating the distance between a single NV center at the probe and the hard disk sample is roughly within 25 nm. Source: [1459].

not require cryogenic cooling at the sensor. They can for example help track neurodegenerative diseases such as dementia, Alzheimer's and Parkinson's by tracking patients' brain activity and how it changes over time [1466]. The principle of operation of an OPM is rather simple. A small laser beam, which can come from a vertical-cavity surface emitting laser (VCSEL), illuminates a heated alkali-metal vapor (rubidium, cesium or potassium) trapped in a millimeter-scale glass cell. The effective spatial resolution depends on the cell and beam dimensions, on the sensor-to-source distance, on the channel spacing in an array and on the source reconstruction, not on cell size alone. The electron spin polarization of the alkali atoms, hyperfine-coupled to the nuclear spin, precesses in the ambient magnetic field, which changes the optical properties of the vapor and therefore its absorption of the probe light. Light is then measured by a photodetector after traversing a polarizing beam splitter [1467] (Figure 152).

OPMs can also be used for magnetocardiography as shown in Figure 151. A similar technique is studied by SandboxAQ. The human body is not transparent for electric fields but is for magnetic fields. Magnetocardiography helps study how electricity operates the heart. Damaged heart fibers have different signals than dead fibers creating distorted fields which can be detected with a panel of OPM magnetometers.

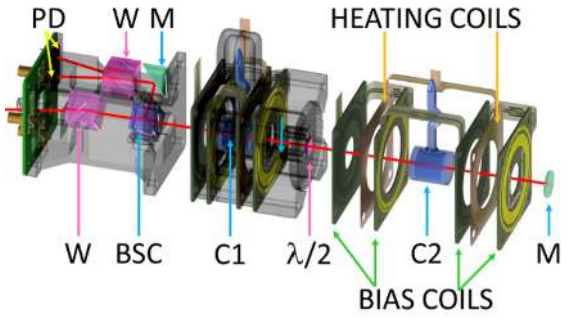


Figure 150: OPM based Magnetocardiography Sensor layout. The laser beam (red line) is delivered with an optical fiber and collimated using a GRIN lens (not shown). The beam is deflected on a Wollaston prism (W), 10% of the beam passes through the beam splitting cube (BSC), cell 1 (C1), half-wave plate ($\lambda/2$), cell 2 (C2) and is retroreflected with a mirror (M). After passing through the cells the second time, 90% of the beam is reflected by the BSC and then a right-angle mirror to the polarimeter formed by a second Wollaston prism and two PDs. The coils surrounding both cells are identical but are expanded around C2 for better visualization. Source: [1468].

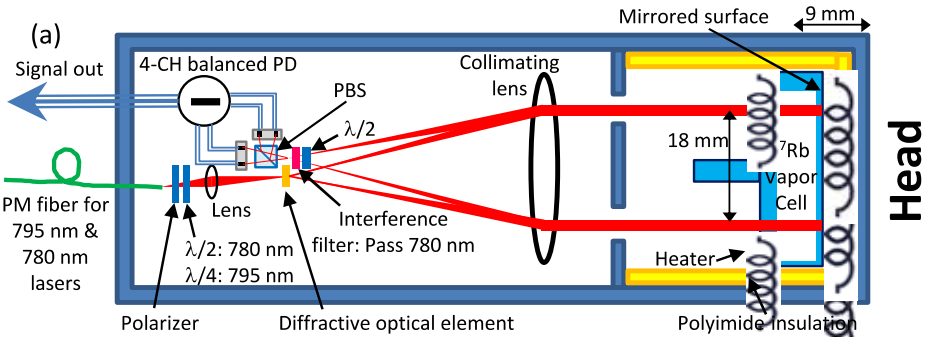


Figure 152: The principle of an OPM-based magnetoencephalography sensor. Source: [1467].

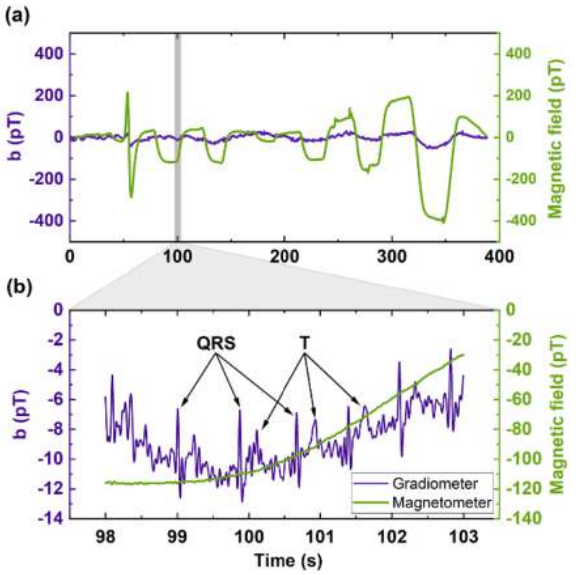


Figure 151: The signal output of the OPM based Magnetocardiography Sensor with the difference between the magnetic field and the more precise magnetic gradiometer field. The chart in (a) covers the full duration of the recording while (b) zooms on a specific period. The purple trace is the gradiometer signal and the green trace is the reference magnetometer showing the magnetic field component in the gradiometer's sensitive axis direction. At 50 s, the impact of a magnetic door lock as a door is opened and closed is visible. After 70 s, the operation of the building's lifts started. The arrows indicate the QRS complex and T wave of the measured heartbeat. Source: [1468].

2.9.4 Quantum photometry

Some photometric measurement applications require high precision. In 2026, an early bacterial detection was proposed using a bright squeezed-light probe created with a doubly resonant optical parametric amplifier (OPA) [1469] (Figure 153). Squeezed-light quantum imaging can also generate 2D images [1470].

2.9.5 Ghost imaging

Quantum imaging could also use **ghost imaging** or quantum phantom imaging (Figure 154). It exists in many variations. The first one used a generator of infrared photons in 1995 [1471, 1472]. One half of the photons illuminates the object and the other half a photo sensor, by crossing an optical delay line [1473, 1474]. The photons illuminating the object are entangled with those illuminating the camera, which has not seen the object at all! The obtained image is very noisy and requires some appropriate processing. What is the purpose of this? Mainly to analyze objects with a very low photon number to avoid modifying the object to be analyzed. This can be interesting in microbiology [1475].

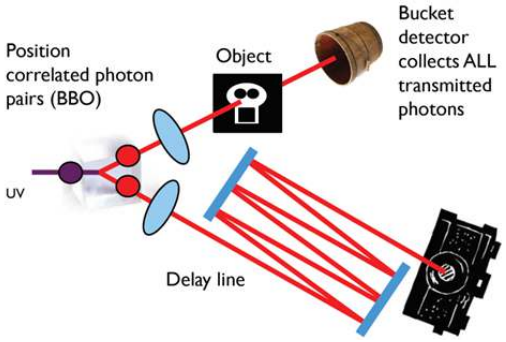


Figure 154: Ghost imaging principle. Source: [1473].

Demonstrations have mostly used small objects, which reflects the available sources and detectors rather than a fundamental scale limit. There is also an explicitly theoretical interaction-free proposal in which no photon reaches the object and only the time bins with no photon arrival carry the information [1476]. It should be kept separate from conventional correlation-based ghost imaging and from imaging with undetected photons.

Another proposed technique uses free electron-photon pairs generated inside a transmission electron microscope (TEM) to allow spatial information about a sample to be reconstructed from photons that are correlated with the probing electrons rather than probing the sample themselves. It brings a less invasive method of imaging that is valuable for delicate biological or nanostructured materials. The spatial resolution is 2 μm. [1477] introduces correlated particle detection which enables multi-modal imaging that combines structural and optical data.

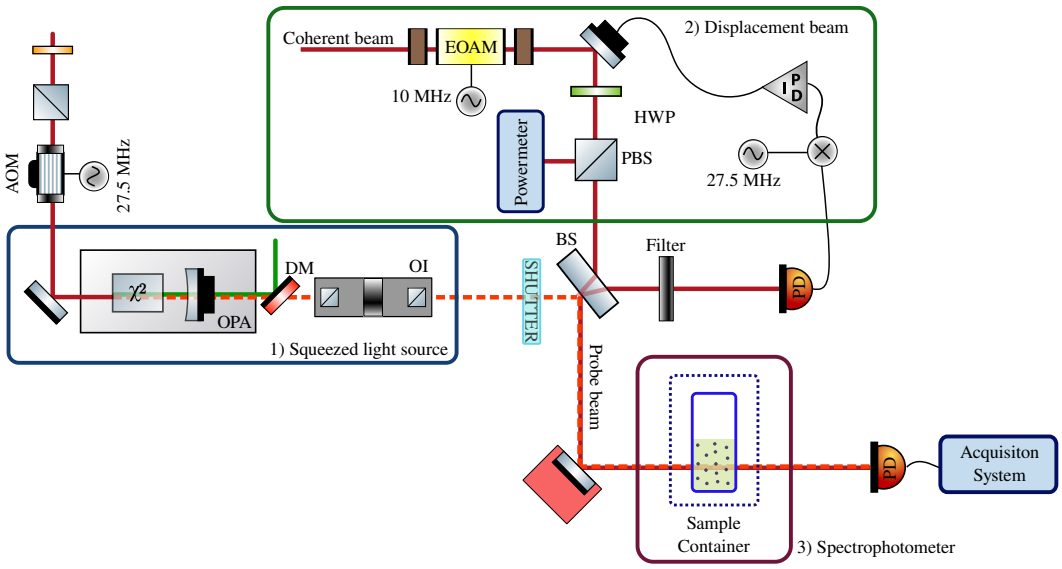


Figure 153: A quantum photometry experimental setup for an early bacterial detection. The three parts are a squeezed light source, a displacement beam module and a photometer. OPA: Optical Parametric Amplifier, DM: Dichroich mirror, OI: Optical isolator, HWP: Half-wave plate, PBS: Polarizing beam-splitter, BS: Beam-splitter, PD: Photodetector, EOAM: Electro-optic modulator, AOM: Acoustic optical modulator. Source: [1469].

Other non-quantum techniques use a single-pixel color imager that uses 1,300 structured lights per second to illuminate the object for a few seconds, with up to one million iterations. The sensor prototyped at the University of Glasgow in 2013 contains four photodiodes positioned at different locations [1478–1481]. This makes it possible to generate a 3D view of the object (Figure 155).

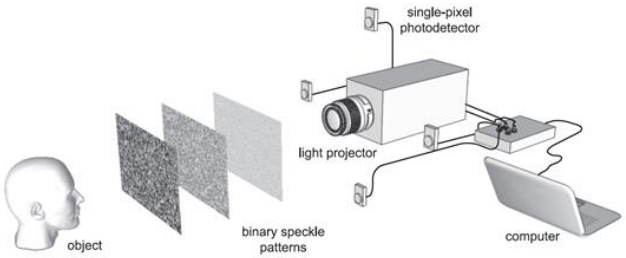


Fig. 1. Experimental setup used for 3D surface reconstructions. The light projector illuminates the object (head) with computer-generated random binary speckle patterns. The light reflected from the object is collected on four spatially separated single-pixel photodetectors. The signals from the photodetectors are measured and used to reconstruct a computational image for each photodetector.

Figure 155: A single-pixel color imager from the University of Glasgow developed in 2013. Source: [1479].

Finally, quantum imaging can also rely on the illumination of the object by entangled microwaves, using the principle of quantum radar that we will see in a following section. It is **proposed** for analyzing objects with low reflectivity, with possible applications in medical imaging and in short-range radar. Published work remains at the laboratory demonstration stage, at GHz frequencies with the entanglement source held at millikelvin temperatures, over ranges of the order of a meter, and the relevant comparison is with the best classical transmitter allowed the same energy and bandwidth [1482] (Figure 156). It can also work with infrared light [1483].

Entangled photons can also be used to create holograms, as discovered in 2021 by a team of physicists from the University of Glasgow [1484].

Quantum imaging with undetected photons is a variant relying on the indistinguishability of the two sources emitting the photons that illuminate the object, those photons being precisely the ones that are not detected [1485]. It uses photon pair creation in two separate down-conversion crystals. The photons passing through the object are not detected. The image is created with their sister photons, which do not interact with the object (Figure 157). The imaged object can be either opaque or invisible to the detected photons. This technique's advantage is to probe the object at a wavelength that is difficult to detect, while detection happens at a more convenient wavelength. This can implement terahertz quantum imaging, in the terahertz and far-infrared region lying between infrared and microwaves [1486].

Another technique couples a camera that does not see the object to be captured and a single pixel sensor that sees the object. It can be based on the entanglement of photons or of twisted pairs of photons in the visible spectrum, between the two sensors [1487, 1488].

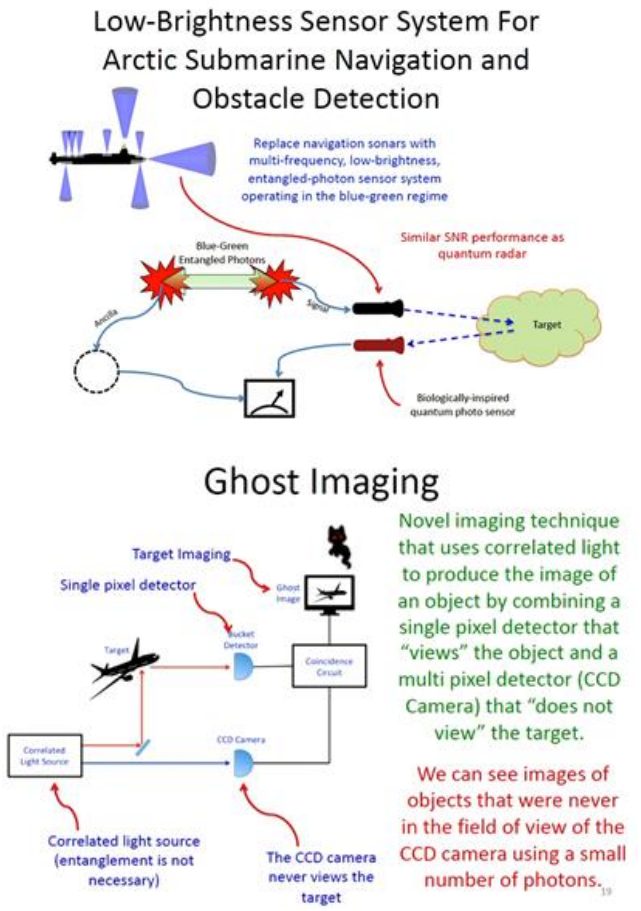


Figure 156: Another ghost imaging concept. Source: [1489].

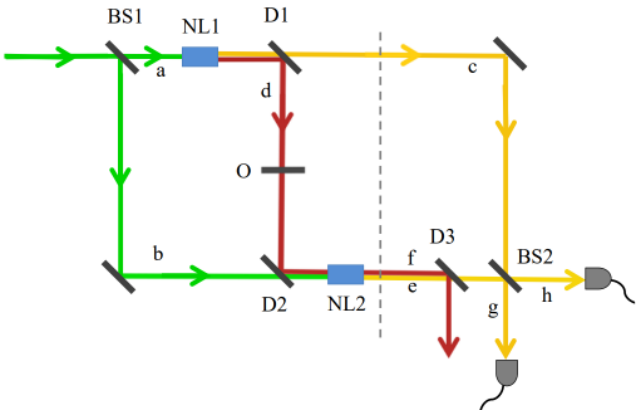


Figure 157: A description of quantum imaging with undetected photons with a laser exposing a non linear crystal (NL1) creating yellow and red photons, the red photon illuminates the observed object O with a result being transformed with another non linear crystal, the two yellow streams are converging in the beam splitter BS2 and detected. Source: [1485].

Finally, Quantum Ghost Spectroscopy (QGS) is a sort of counterpart in the frequency domain of Quantum Ghost Imaging (QGI). It can detect gas threats [1490].

2.9.6 Vendors

Vendor funding, acquisitions, staffing, product availability, performance figures and clinical-use statements below are as of September 2026 and come from company releases or official filings unless stated otherwise. Specifications are vendor-reported.

Chipiron

France, 2020, €19M

Chipiron develops a portable and helium-free 2D and 3D MRI system using stacked SQUIDs quantum detectors (superconducting / Josephson effect based). The startup created by Dimitri Labat and Evan Kervella is first targeting osteoporosis and brain diagnosis. In 2025, the company published a white paper describing its technology [1491].

Damavan Imaging

France, 2014

Damavan Imaging provides imaging solutions to visualize ionizing radiation with cameras using Compton's effect. They are also developing gamma ray imaging solutions.

Diasense

Denmark, 2024

Diasense is developing a NV center based microscope to run contactless chip failure analysis at the microscopic level or biological samples analysis. The company is a spin-out from DTU created by Christian D. Nielsen (CEO), Marvin Holten (CTO), Alexander Huck (CSO) and Ulrik Lund Andersen.

Diffraqtion

USA, 2024, $1.5M

Diffraqtion was created by Johannes Galatsanos, Saikat Guha and Christine Yi-Ting Wang from MIT, Harvard, University of Maryland, and the University of Arizona. They develop quantum imaging sensors coupled with energy-efficient AI for autonomous vehicles, robotics, cellphones, and space applications. They won a $1.5M SBIR award to develop and commercialize their technology.

EuQlid

USA, 2023, $3M

EuQlid is a startup coming out of the Quantum Catalyzer (Q-Cat) in Maryland. They are combining a large-field-of-view quantum diamond microscope (QDM) and some neural network image analysis to enable non-invasive imaging of integrated circuits.

Mag4Health

France, 2021

Mag4Health is a spin-off from CEA-Leti who develops a helium optically pumped magnetometer-based magnetoencephalography (MEG) system, working at room temperature [1492]. It uses quantum sensors that were developed at CEA-Leti [1493]. These record the brain's electromagnetic activity in real time, helping with the diagnosis of neurological disorders. Mag4Health MEGs are much lighter (about 150 kg) than classical systems using large superconducting magnets (5 tons).

Magnolia Quantum Sensing

Denmark, 2025

Magnolia Quantum Sensing was created by Hans Stærkind (CEO), Kristin Engel (applications) and Asger Pedersen (CTO) as a spin-off from Niels Bohr Institute.

It develops a magnetic resonance imaging (MRI) imaging solution, the EXAAQ sensor, a quantum optical magnetometer. It uses room-temperature cesium atoms which are stored in a small glass cell. The cesium atoms have particular resonances and laser light absorption at specific frequencies which depend on the magnetic field. One particular cesium resonance occurs between the quantum states of maximum total projected spin, *aka* the extreme angular-momentum states, thus the method named, EXtreme Angular-momentum Absorption-spectroscopy Quantum (EXAAQ) magnetometry.

Nvision

Germany, 2015, €103M

Nvision Imaging is a spin-off from the Institutes of Quantum Optics and Theoretical Physics at Ulm University created by Sella Brosh (CEO), Ilai Schwartz (CTO), Alex Retzker, Fedor Jelezko, and Martin Plenio. It is developing POLARIS, a spin-based MRI medical imaging solution using parahydrogen-based polarization. It amplifies the magnetic resonance signals by hyperpolarization of key metabolites for medical imaging and analytical chemistry. With PIQC, it also plans to develop a molecular spin based quantum computer based on the same technology.

Phantom Photonics

Canada, 2023

Phantom Photonics is a spinout from the University of Waterloo by Alex Maierean, Shihan Sajeed, and Thomas Jennewein. They develop a quantum 3D photonic remote imaging sensor [1494].

QDTI

USA, 2012

QDTI is the only known startup initially engaged in the development of a quantum computer based on NV Centers. Created by a team from Harvard University, it is logically based in Boston.

QLM Technology

UK, £16.1M

QLM Technology developed a "Quantum Gas Imaging Lidar", a single-photon lidar and spectroscopy system that detects methane leaks in pipelines up to 100 meters away. It is not a magnetometer. The measuring system, weighing a few kg, can be carried by a large drone flying at 50 km/h. It uses a laser that illuminates a gaseous medium of variable opacity and a photodetector.

IDQ is involved in the creation of the solution at the lidar level, supplying the single-photon detection. The system is embedded in "Schlumberger End-to-end Emissions Solutions" (SEES), a product line that detects and eliminates the oil and gas industry's methane and flaring emissions (Figure 158).

Figure 158: An airborne LiDAR to detect gas leaks.

QT Sense

the Netherlands, 2024, €6M

QT Sense is a spin off company from Romana Schirhagl's group in the University Medical Center Groningen. The idea behind the company emerged from an ERC starting grant in 2022 which led to a NV center based biological measurement system proof of concept. The portable equipment measures oxidative stress in biological cells.

Quantum Computing Inc

USA

Quantum Computing Inc, *aka* QCi, announced in July 2023 its Quantum Photonic Vibrometer (QCi QPV-1.0), a photonic based remote vibration detection, sensing, and inspection instrument. It can detect highly obscured and non-line-of-sight objects like landmines, implement non-destructive material control and also detect voices in noisy environments. It measures surface vibrations

by counting the number of individual photons that are reflected as the surface slightly moves or tilts.

Figure 159: QCI quantum vibrometer.

Qnami

Switzerland, 2017, $7.3M

Qnami is a spin-off from the Quantum Metrology Research Laboratory at the University of Basel.

Among other things, they produce artificial diamonds for various photonics applications. They targeted first the quantum sensing market with their Quantilever MX nano-diamonds probes (Figure 160). They then launched in 2019 the ProteusQ range of NV center confocal microscopes, used to analyze ferromagnetic materials, based on the Quantilever probe. Quantonation and Runa capital are among their investors. And one of the cofounders and the CEO, Mathieu Munsch, came from Grenoble Phelma and worked at the CEA in Grenoble and did his PhD at CNRS Institut Néel.

Founded in 2017, the startup was acquired in June 2026 by Quantum Design (USA), a company specialized in scientific instrumentation which also had acquired Oxford Instruments NanoScience in January 2026, and their cryogenic business.

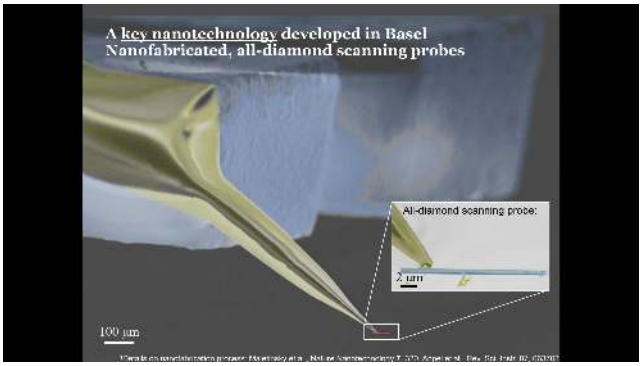


Figure 160: Qnami NV center based imaging system. Source: Patrick Maletinsky, University of Basel.

Quantum Scopes AB

Sweden, 2024

Quantum Scopes AB is a company created by Val Zwiller, a spin-out from the Quantum Nano Photonics Group at the Applied Physics Department of KTH.

It designs and manufactures single photon generation and detection solutions. Their first product is SignaQ, a bright source of photon pairs generated at telecom wavelength, a quantum spectrometer used for photon counting spectroscopy over a large wavelength range while recording the arrival time of every single photon with 10 ps accuracy, a quantum Lidar operating at the single photon level and generating live 3D maps of various atmospheric pollutants, and a confocal fluorescence microscope for non-invasive bio-imaging using quantum dots and superconducting nanowire single photon detectors.

Qurv

Spain, 2020

Qurv is a spin-off of ICFO that offers wide-spectrum quantum dots based image sensors covering the visible and short-wave infrared range.

QuSpin

USA, 2012

QuSpin is proposing an optical magnetometer (OPM) for neuro-imagery.

QuantumDiamonds

Germany, 2022, €98 M

QuantumDiamonds (*aka* QD) is a spin-off from TUM (Technical University of Munich) that produces NV center based non-destructive inspection tools, QDM, used in particular in semiconductor manufacturing. The €98 M shown above aggregates equity and grants, of which €76 M is EU Chips Act funding, as announced by the company. In December 2025, they announced a €152M plan to build a quantum-based chip inspection facility in Munich, also supported by the EU Chips Act.

RobQuant

UK-Sweden, 2023

RobQuant develops solid-state quantum sensors targeting disease detection, particularly with non-invasive brain scans. Their first product, RQ-1, integrates a vector magnetic field into a 6-degree-of-freedom robotic arm. The sensor is a heterogeneous NV center spin sensor and CMOS silicon chip integrating control electronics [1495–1497].

SBQuantum

Canada, 2019

SBQuantum is a startup coming from Institut Quantique (University of Sherbrooke), also known as SBTech and Shine Bright Technologies. It develops NV centers-based quantum magnetometers [1498]. They target various markets the automotive market, agriculture (partnering with John Deere since 2024), mining and exploration (partnering with Silicon Microgravity in Canada to com-

bine magnetic and inertial sensors in a drone), medical imaging, and CubeSat-type satellites. They also developed a tri-axial version of their system that measures magnetism along the x-, y- and z-axes. Research on this product was funded by the NIH (National Institutes of Health). The product is mainly targeting magnetoencephalography (MEG) brain imaging. In 2024, the company got a contract from ESA and the Canadian Space Agency to test their magnetometers in space, with the long-term goal of creating a potential GPS backup solution.

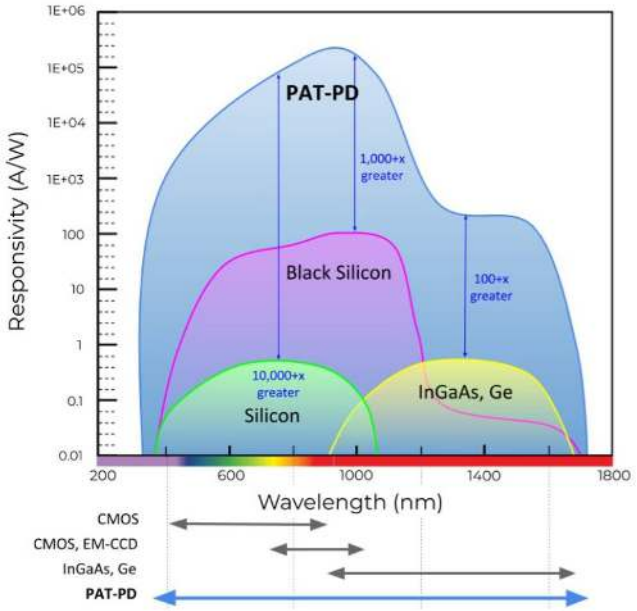


Figure 161: SeeDevice covered wavelengths.

SeeDevices

USA, 2017, $4.85M

SeeDevices develops a quantum imaging system, the PAT-PD (Photon Assisted Tunneling Photo Detector), which exceeds the performance of traditional CMOS imagers. This imager contains photosites using the tunneling effect that can detect single photons in a wide range of wavelengths from near infrared (1,800 nm) to ultraviolet (up to UVA1, at 350 nm). This can be used for seeing in the dark and for medical imaging, like for detecting blood vessels in the infrared range (Figure 161). The startup is now focused mainly on medical imaging systems also using these NV centers, with the creation of precision magnetometers combined with MRI and immunological tests.

Serino

Germany, 2023

Serino develops quantum dots based NIR sensors.

Siloton

UK, 2020, £1.7M

Siloton is developing optical coherence tomography (OCT) solutions for the assessment of age-related macular degeneration. The company is the first investment from the Quantum Exponential Group launched by Steven Metcalfe. Their chip devices are designed by VLC Photonics in Spain and manufactured by Ligentec in Switzerland. OCT uses low-coherence light to capture micrometer-resolution, 2- and 3-dimensional images from within optical scattering media like the retina. It is also used in nondestructive testing (NDT) in the industry. It makes use of low-coherence interferometry with near-infrared light that easily penetrates the inspected medium. It probably belongs to Type I quantum sensing.

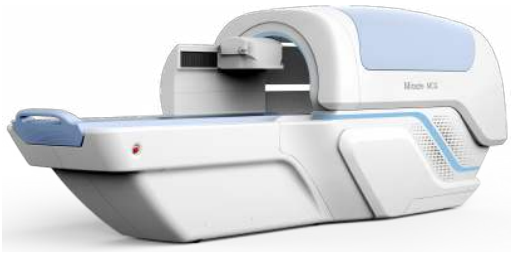


Figure 162: Xmagtech magnetic sensors for magnetocardiography and magnetoencephalography.

Xmagtech

China, 2018, $28M

Xmagtech *aka* Beijing Weimag Technology, develops weak-field magnetic sensors for medical applications. It includes magnetocardiography and magnetoencephalography. Their sensors use optically pumped magnetometer (OPM) based on rubidium 87 spins in small vapor cells. Their SERF magnetometer is advertised in the femtotesla range. Sensitivity for such devices should be quoted as a noise-equivalent field in T $Hz^{-1/2}$ together with the bandwidth and the shielding conditions.

2.10 Distance measurement

A team from Jian-Wei Pan in China demonstrated dual-comb ranging over a 113 km free-space path, with a reported precision at the micron level under the atmospheric conditions and link availability described in [1499]. It uses two optical frequency combs and interferometry in the telecom band (1545 nm and 1563 nm) (Figure 164). The applications are more in the scientific field, such as in geodesy to measure the effects of plate tectonics or for the creation of new gravitational wave sensors.

Distance measurement can be combined with a quantum position verification (QPV) protocol, designed to test a claimant's reported location under explicit trust and adversary assumptions [1500]. QPV does not authenticate the identity of a detected object and does not make ranging inherently spoof-proof.

2.11 Quantum radars and LiDARs

Quantum radars are very slowly emerging from research [1501]. It is of course of great interest for the military in many countries. This is a special case of "hype" since there are many claims of the existence of quantum radars able to detect stealth aircraft while several groups, mostly in Europe, argue that it cannot work or that it offers only marginal improvements over classical radars [1502–1504].

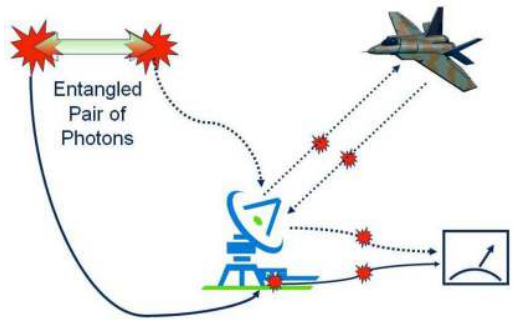


Figure 163: The principle of an entanglement-based quantum radar. Source: [1505].

Technology

The idea initially came from Seth Lloyd at MIT in 2008 when he devised the concept of quantum illumination [1506–1509]. Classical radar operates in the radio and microwave bands to begin with, so a useful taxonomy separates the quantum resource from the carrier frequency:

- **Quantum illumination and correlation receivers**. The transmitter emits one half of an entangled pair, retains the idler, and a joint measurement is performed on the noisy return and the retained idler (Figure 163 and Figure 165). The relevant classical benchmark is the best coherent-state transmitter and receiver allowed the same transmitted energy, bandwidth and detection resources.
- **Quantum-enhanced receiver components** used with classical illumination, such as single-photon detectors or squeezed-light front ends. Nothing about the transmitted waveform is nonclassical here, and the reported gains are modest and depend on the loss and noise regime.
- **Rydberg-atom RF receivers**, where a vapor cell replaces the antenna and the front end of a conventional radar, the transmitter staying entirely classical.

Early proposals in the visible spectrum are a special case of the first category. They work poorly because of clouds, atmospheric scattering and background light, and because quantum illumination is not defined by operating in the visible in the first place. Converting optical photons into microwave photons while preserving the quantum state, and doing the same for the retained idler, is a separate and difficult transduction subsystem rather than a free step, and it is where much of the practical difficulty sits.

In the high-loss, high-noise regime the transmitted signal-idler entanglement is generally destroyed. The advantage, when achievable, comes from a joint statistical measurement of the noisy return and the retained idler that exploits correlations stronger than those available to an appropriately constrained classical transmitter [1510].

The microwave variant of the first category is the one more seriously studied, like using microwave entanglement and a dual-receptor scheme to improve the angular detection of a target [1511]. Microwaves traverse bad weather, which photons in the visible spectrum cannot do. However, noise-induced decoherence is hard to fight [1512].

Microwaves could also be directly generated without being converted from visible entangled photons, using for example JPAs (Josephson Parametric Amplifiers) or TWPAs (traveling wave parametric amplifiers) [1513]. This last solution was experimented by a French team from ENS Lyon in 2022/2023, as shown in Figure 165, using direct microwaves photon counting and reporting a signal-to-noise ratio improvement of about 20% over the classical benchmark considered in that work, at matched transmitted energy and bandwidth and in the specific loss and noise regime tested [1514]. It is using two entangled microwave modes with a delay line to detect targets with an improved signal to noise ratio.

Without playing with entanglement, a team from NIST and Raytheon tested a Rydberg atom based sensor in 2025 used as subwavelength sensor that down converts a classical frequency modulated continuous wave (FMCW) radar echoes [1515]. The radar itself remains classical in that case. These techniques are expected to improve the accuracy of traditional radars and to improve their resistance to noise, interference and jamming. This kind of radar could theoretically detect stealth aircraft, modulo the fact that their flat reflective surfaces reduce their radar signature whatever the radar frequency [1516, 1517]. The first concepts saw the light of day in 2015 [1518–1520]. It is also studied in South-Korea [1521].

Another method consists of using Rydberg atoms to analyze microwaves received by a conventional radar, as proposed in [1522]. The received microwave field couples two Rydberg states in a cesium vapor cell while probe and coupling lasers establish electromagnetically induced transparency. A sufficiently strong resonant microwave field produces **Autler–Townes splitting** of the EIT resonance. The splitting is proportional to the microwave Rabi frequency and therefore to the electric-field amplitude. Measuring the optical transmission spectrum with a photodetector provides a calibrated microwave-field measurement. The atom-based receiver can be much smaller than a resonant conventional an-

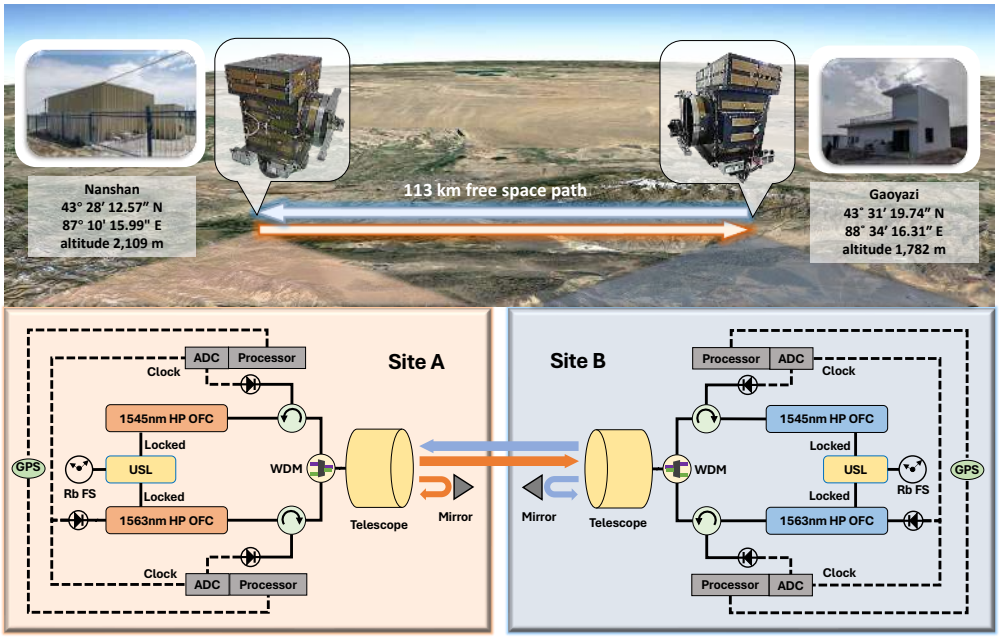


Figure 164: 113 km distance sensing implemented in China in 2024 with dual optical frequency combs. Source: [1499].

tenna and can be tuned over a broad frequency range by selecting atomic transitions and laser frequencies.

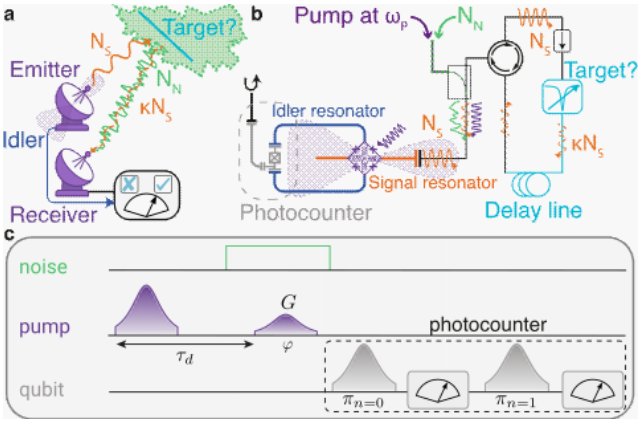


Figure 165: The superconducting circuitry based microwave quantum radar proposed by ENS Lyon in 2023, using a delay line. Source: [1514].

The claimed benefit is a better signal-to-noise ratio than a conventional receiver of comparable aperture, particularly for detecting targets moving at specific speeds. Such a comparison only means something once the classical receiver, its aperture, its noise figure and the detection bandwidth allowed are specified. The caveat is that the gas cell has a small cross-section and the radar is relevant for detecting very accurate signals at close range. Also, Rydberg atoms are very sensitive but they are tuned to a specific transition. If the radar carrier or an interfering signal changes frequency rapidly, the atomic receiver and its lasers may need retuning, which is technically difficult compared to a wideband electronic circuit. In addition, the system requires the use of two frequency-stabilized lasers, which are very expensive and sensitive to vibrations, and a precision optical alignment system (Figure 166).

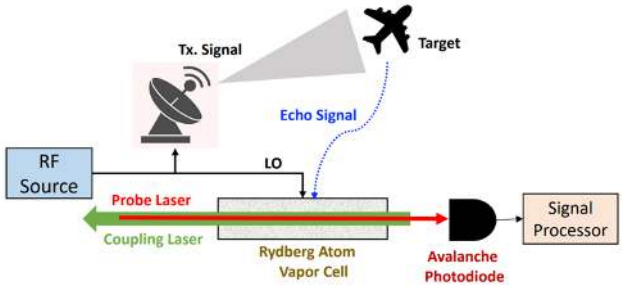


Figure 166: A Rydberg atom glass cell could help better amplify the incoming microwaves received by a classical radar. Source: [1522].

Trials

China Electronics Technology Group, a state-owned company, announced a successful test of a quantum radar in 2016 and a prototype in 2018, with a claimed range exceeding 100 km [1523, 1524]. Detection of low-observable aircraft is the motivation stated in the press coverage. These are reported demonstrations rather than independently verified performance, and no measurement methodology, waveform or target description has been published. More recent papers show the limitations of this technology and how researchers in China are trying to improve it [1525].

Other labs and companies are developing such radars:

- In **Canada**, as the Institute for Quantum Computing from the University of Waterloo in Canada [1526]. This project is funded by the Canadian Department of Defense for $2.7M. Iran is also on it [1527].

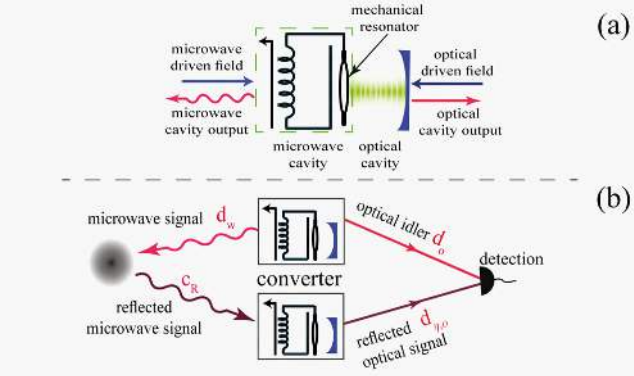


Figure 167: Converting radar RF waves to/from photons. Source: [1528].

- In **Austria** at the Institute of Science and Technology in Klosterneuburg.
- In **Germany**, the QUARATE project is about improving microwave radars with quantum sensing [1529].
- In **Italy**, some researchers are even working with researchers in China on quantum Doppler radars [1530].
- In **Europe**, the Quantum Flagship **QMiCS** is dedicated to creating quantum microwave technologies operating at the single photon level that could help build quantum radars.
- In the **USA**, Lockheed Martin is also invested in this emerging field. Specialists such as Marco Lanzagorta of the US Naval Research Laboratory believe that QKD satellites launched by the Chinese like Micius would have military applications of this type [1489]. A new technique to slightly improve the efficiency of quantum radars was proposed by a researcher from the Los Alamos National Laboratory in 2024, which consists of using unreflected photons [1505, 1531]. And a team from the US Army worked on how an entanglement-based quantum radar could detect spoofing [1532].

Quantum radars are still very theoretical devices [1533] that are currently plagued by photon losses, noise and various detection issues, whether they operate in the visible or microwave domains [1534–1537]. They have fundamental limitations that could limit their range drastically [1538].

Quantum technologies can also be used for other tasks like analyzing classical radar data [1539] or revealing spoofing of classical radars thanks to the analysis of quantum noise [1540].

Quantum LiDARs

Quantum illumination could however be used in LiDARs to verify that the inbound photons correspond to those emitted by its own laser, avoiding unwanted optical interference from other LiDARs [1541, 1542] and avoiding jamming [1543]. LiDARs can measure the range and velocity of target objects [1544].

Without malicious interferences, this may be very useful when many autonomous vehicles equipped with LiDARs will have to coexist on the road [1545]. Quantum LiDARs can also have an improved resolution [1546], be used in meteorologic monitoring [1547] or specialized in ranging detection [1548]. They could also be turbulence resistant [1549].

Single-photon LiDARs could be used for remote wind detection at high resolution. It has been developed in China since 2014 and is used in transportable radars, including UAVs [1424, 1550–1552] (Figure 168 and Figure 169). The variant Temporal single-photon (TSP-) LiDAR studied in China could support long-range target detection [1553].

European researchers are also working on quantum-enhanced Doppler LiDARs [1554].

Quantum-enhanced LiDAR architectures can be limited by source brightness, collection efficiency and detector loss, motivating "quantum-inspired" approaches [1555]. Single-photon LiDAR itself is not limited to meter-scale ranges and can operate over tens of kilometers or more. Much shorter ranges reported in some experiments apply to particular entanglement-based, interference-based or quantum-illumination demonstrations [1556].

Underwater quantum lidar and optical ranging

In a domain close to radar, quantum-enhanced underwater ranging could use blue-green photons, where seawater transmission is comparatively favorable. Such a system would be better described as underwater quantum LiDAR or quantum optical ranging rather than "quantum sonar", since sonar uses acoustic waves. Related blue-green optical links are also studied for communication with submerged platforms. These concepts remain constrained by absorption, scattering, background light and the severe link budget of underwater optical propagation.

Vendors

HENSOLDT

Germany

HENSOLDT is working on quantum radars. It got a contract from the DLR Quantum Computing Initiative (DLR QCI) for the QUASAR research project. HENSOLDT is working with the Microwaves and Radar Institute of DLR and Tensor AI Solutions (Germany). QUASAR addresses the unfavorable geometric scaling of radar, the received power falling as $1/R^4$ for a monostatic system, by studying whether quantum correlations can improve detection at a given received energy.

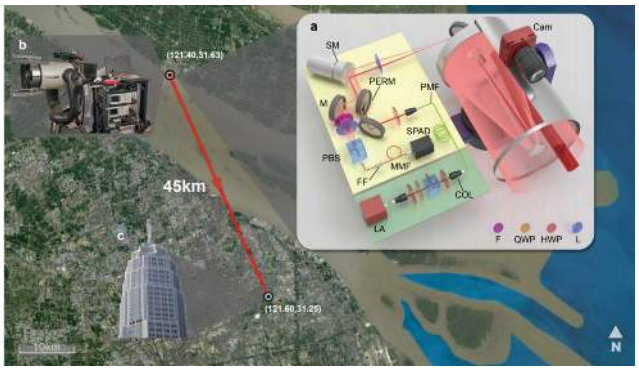


Figure 168: A test of quantum LiDAR with a range of 45 km in China in 2019. Sources: [1424, 1550].

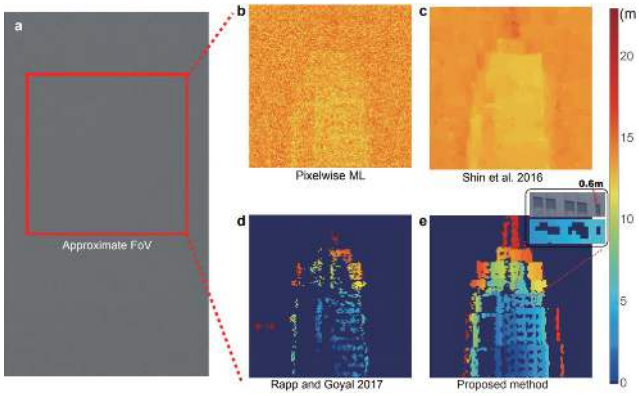


Figure 169: The simulated result of the 2019 quantum LiDAR. Sources: [1424, 1550].

Shandong Guoyao Quantum Radar Technology

China, 2017

Shandong Guoyao Quantum Radar Technology is developing quantum radars and LiDARs. Based in Jinan (Shandong). Their quantum detectors are used in the defense domain, for weather observations like wind speed, cloud mass, and atmospheric pollution [1557].

2.12 Quantum thermometers

2.12.1 Science

NV centers can be used for nanoscale and microscale thermometry with very high spatial resolution. Reported temperature performance depends strongly on integration time, collection efficiency, diamond quality and calibration, with millikelvin-scale sensitivity achievable in suitable ensemble or optimized measurements [1154, 1558, 1559]. This makes NV thermometry particularly attractive when spatial resolution and local, minimally invasive probing matter.

Quantum thermometry also has applications at very low temperatures, including cryostats and fundamental-physics experiments. Noise-equivalent temperature sensitivity is commonly quoted in $\mathrm{K}/\sqrt{\mathrm{Hz}}$. This is distinct from absolute accuracy. For approximately white uncorrelated noise, averaging for a longer time improves the statistical uncertainty roughly as $1/\sqrt{t}$ until drift or other systematic noise dominates.

How do NV-center thermometers work? Several methods are used, such as spin-based thermometry with ODMR (optically detected magnetic resonance) spectrum measurement using microwave excitement. Some classical machine learning postprocessing may be necessary to improve the robustness of the result, particularly with a small number of measurements [1560].

The diamond containing NV centers can be attached to a fiber [1561]. There are even hybrid thermometers associating NV centers and more classical magnetic nanoparticle thermometers [1562, 1563] (Figure 171). It uses the fact that the zero-field splitting frequency shifts with the ambient temperature. That dependence is close to linear over a limited calibrated range, typically around room temperature, and becomes markedly nonlinear at cryogenic temperatures. All-optical methods use the correlation between the NV center ZPL (zero-phonon lines) and temperature [1564].

There are solutions for temperature measurement in biological matter by fluorescence that are based on quantum dots [1565]. Other ODMR based sensors can measure both pressure and temperature [1566].

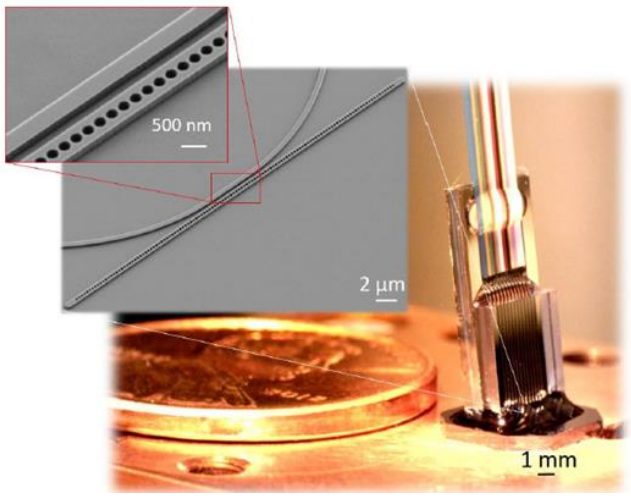


Figure 170: Quantum photonic thermometer from NIST.

In 2017, NIST produced a quantum photonics thermometer of very small size for optically measuring the surface temperature of metals. However, the picture does not show the control electronics associated with the sensor [1567] (Figure 170).

Quantum thermometry can also use another defect, with negatively charged boron-vacancy centers (V_B^-) in hexag-

onal boron nitride (hBN), as experimented in the USA [1568].

Other quantum thermometry methods are using an optomechanical system with an optical field coupled to a mechanical resonator, superconducting microwave resonators [1569], superconducting qubits [1570] or superconducting transition edge sensors (TES) [1571].

2.12.2 Vendors

Southwest Sciences

USA, 1985

Southwest Sciences develops optical temperature sensors based on NV centers for use in cryogenic systems. The company was founded by Alan C. Stanton and Joel A. Silver.

QuantumCTek

China

QuantumCTek created a ruthenium oxide resistance thermometer operating down to 6 mK, used to monitor the temperature of superconducting qubit chips. It is a cryogenic resistive sensor rather than a quantum thermometer in the sense used elsewhere in this chapter, since no coherently controlled quantum degree of freedom takes part in the sensing protocol.

2.13 Quantum chemical sensors

Quantum sensing is also applicable with chemical sensors used to analyze the chemical composition of various materials and substances. It is commonly used with optical interferometers [1572, 1573].

2.13.1 Science

Many such solutions could use NV centers, like:

- The detection of paramagnetic species in biological samples using a fiber equipped with an NV center detection probe [1574].
- Concentration sensors using NV center to detect electrochemical signals emerging from an electrolyte solution and using the inhomogeneous dephasing rate of the electron spin of the NV center ($1/T_2^*$) as a signal [1575]. It is still theoretical work.
- Another theoretical NV center sensor, dedicated to the fast and cheap detection of SARS-CoV-2 in biological samples, with a projected false-negative rate below 1%. The NV sensor would be coated with cationic polymers such as polyethyleneimine (PEI), which can form reversible complexes with viral complementary DNA sequences. The detection is indirect. A complicated biological reaction creates an RNA compound which diffuses in the solution, increasing the distance between magnetic molecules and the nanodiamond. The NV centers then sense less magnetic noise and have a longer T_1 time, which turns into a larger fluorescence intensity [1576].
- Various quantum sensing techniques, again, including NV centers, could help detect various types of organic molecules [1577, 1578] and biomolecular interactions [1579].

Quantum sensors can be used for individual atom nuclear magnetic resonance (NMR) spectroscopy. In [1580], a CEA team used in 2026 an individual Er^{3+} paramagnetic center embedded in a $CaWO_4$ crystal, operating at 10 mK using a superconducting thin-film niobium resonator and a transmon-based Single Microwave Photon Detector (SMPD) to measure the nuclear magnetic resonance (NMR) spectrum of a proximal individual nuclear-spin-9/2 ^{93}Nb impurity with Hertz-level spectral resolution. It measures the ^{93}Nb insertion site, its relative position to the Er^{3+} ion, and its complete quadrupolar tensor. Applications include obtaining non-invasive structural and chemical information at the level of individual atoms or molecules.

Also, **superconducting nanowire single-photon detectors** (SNSPDs), whose nanowire architecture can be adapted to the detection of impinging massive particles, can detect macromolecules in the gas phase [1581].

The University of Glasgow has developed and sells under license **IndiPIX**, listed here as a **classical comparison** rather than as quantum-enhanced sensing, an improved and simplified ambient temperature mid-wave infrared (MWIR) imager using indium antimonide (InSb) photodiodes on gallium arsenide (GaAs) transistors. It can detect outdoor gas leaks and plumes, mitigating explosion risks and reduce environmental impact [1582].

Ultracold chemical reactions could be used in cold atom sensors to detect very weak signals like in dark matter detection [1583].

2.13.2 Vendors

Aeris Technologies

USA, 2013

Aeris Technologies is a subsidiary of Project Canary (2019, USA) that develops a quantum cascade laser based compact mid-infrared (MIR) quantum gas sensing technology.

Entanglement Technologies

USA, 2010

Entanglement Technologies is a spin-off of Stanford and Caltech. It sells AROMA (Autonomous Rugged Optical

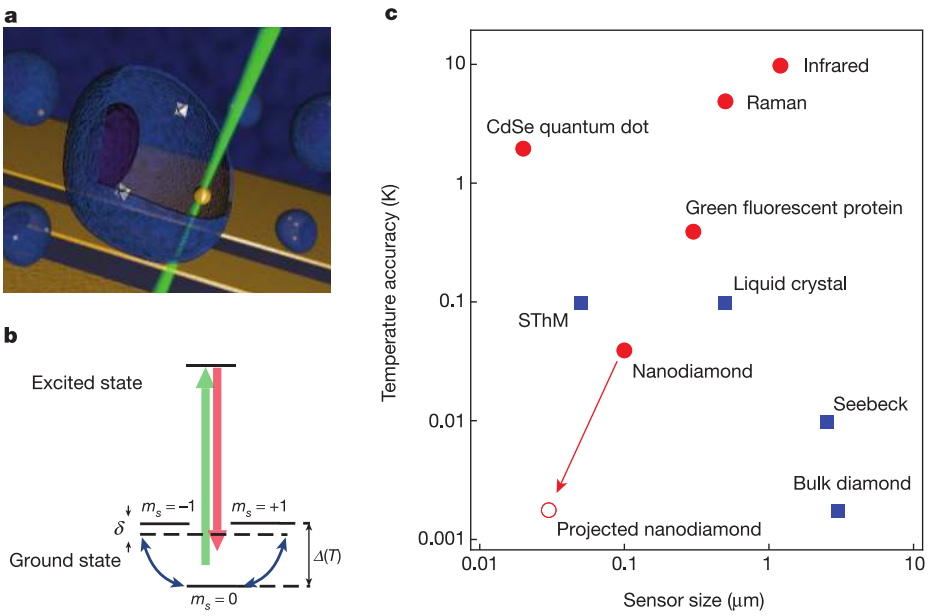


Figure 171: Hybrid thermometers associating NV centers and classical magnetic nanoparticle thermometers can be used to measure temperature within biological cells. Source: [1563].

Multigas Analyzer), a cavity ring-down spectroscopy (CRDS) absorption spectrometer using lasers and high-finesse optical resonators similar to those used to detect gravitational waves in LIGO.

Figure 172: Entanglement Technologies AROMA.

Conventional CRDS is not inherently quantum-enhanced, so any genuinely nonclassical resource used in the product would have to be stated separately. It allows the detection of dangerous gases in industry, especially in the extraction of fossil fuels (Figure 172). The work was supported by the Environmental Defense Fund (EDF), a US nonprofit that should not be confused with the French utility sharing the same acronym.

Flari Tech

USA, 2024

Flari Tech is a company created by Eva Yao (CEO), Jun Ye (JILA) and Qizhong Liang (JILA) in Colorado which develops a portable breath analyzer using an optical frequency comb.

Florence Quantum Labs

USA, 2024

Based in Los Angeles, Florence Quantum Labs is integrating ultraweak photon emission (UPE) spectroscopy, quantum-enhanced sensing, and machine learning to understand arbuscular mycorrhizal fungal (AMF) symbiosis. Their biosensors leverage NV center quantum detection, hyperbolic plasmonic metasurfaces, and optically resonant microcavities to extract single-photon-level spectral signatures of AMF viability, metabolic flux, and stress response in real time. They capture biophoton-mediated redox dynamics, mitochondrial electron transport fluctuations, and metabolic perturbations as a high-fidelity signature of AMF functionality.

Oxford HighQ

UK, 2017

Oxford HighQ is a spin-off from the University of Oxford developing chemical and nanoparticles sensors using optical microcavities.

2.14 Quantum pressure sensors

Quantum techniques can also be applied to pressure measurement, for example through pressure-dependent shifts of defect-spin or optical transitions. However, not every highly sensitive nanoscale, optical or semiconductor pressure sensor is a quantum sensor in the second-generation sense used elsewhere in this chapter. The classification should depend on whether a coherently prepared quantum degree of freedom or a specifically

quantum measurement resource is part of the sensing protocol.

We have for example:

- **Classical comparison**: thin high-sensitivity pressure sensors used in medical monitoring, such as carbon-sphere/polydimethylsiloxane composites [1584], illustrate the performance that a quantum-pressure sensor should be compared against.
- **Quantum-based metrology**: measurement of low pressures using light interacting with helium gas and pressure dependent refractive index of helium [1585].
- **Quantum-limited or electromechanical proposals**: various optomechanical quantum sensors [1586, 1587].
- **Quantum-enabled material sensors**: high-pressure measurement up to 4 GPa using the shift of the optical spectra of quantum-wells made of III/V GaAs/AlGaAs materials [1588]. A 2026 experiment was implemented on some superconducting microcrystal also under a pressure of 4 GPa [1589].
- **Coherently controlled defect-spin sensors**: high pressure and magnetism measurement with sheets of boron nitride less than 100 nanometers thick [1590].
- **Quantum-enabled material sensors**: quantum dots used to measure pressure in liquids [1591].
- **Quantum electromechanics**: superconducting qubits coupled to a seven-mode surface acoustic wave resonator (SAWR) [1592].

These sensors can be placed either in the diamond anvil tip or in nano-diamonds embedded in the analyzed medium [1593].

2.15 Quantum NEMS and MEMS

Nano- and micro-electromechanical structures are widely used in accelerometers and other sensors, but most MEMS and NEMS operate entirely in the classical regime. Quantum electromechanics or optomechanics arises when a mechanical resonator is coupled strongly enough to an optical cavity, microwave cavity or qubit for quantum states, zero-point motion or quantum-limited readout to matter [1594, 1595]. Such platforms are investigated for pressure, motion, mass and force sensing [1596–1600]. Three-dimensional mechanical sensor arrays have also been **proposed**, rather than demonstrated, for searches for ultraheavy dark matter near the Planck-mass scale [1601].

Let's also mention the European Quantum Flagship project **macQsimal** (Switzerland, €10.2M) or "Miniature Atomic vapor-Cells Quantum devices for SensIng and Metrology Applications", for the creation of quantum sensors aimed at the market of autonomous vehicle piloting and for medical imaging.

Figure 173: Quantum pressure sensors and quantum motion sensors. Source: [1596]. Copyright MKS Instruments.

This includes the creation of atomic clocks, gyroscopes, magnetometers, imaging systems using microwaves and electromagnetic fields in the terahertz range as well as gas detectors. In short, a fairly generalist approach. It is based on the use of cold atom vapor integrated in MEMS, a technique that Thales is also using.

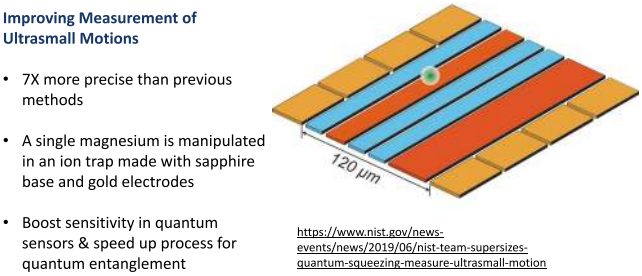


Figure 174: Quantum motion sensors. Source: [1597].

2.16 Dark matter sensing

Dark matter is the name given to a non-luminous gravitating component whose microscopic nature has not been identified. No confirmed electromagnetic interaction of dark matter has been observed, so its presence is inferred primarily from gravitational effects rather than from emitted or reflected light. Examples include galaxy rotation curves, gravitational lensing, galaxy-cluster dynamics and cosmological observations.

Evidence for dark matter comes from several independent scales. Cosmic microwave background measurements by WMAP and Planck, large-scale structure formation, gravitational lensing and systems such as the Bullet Cluster are jointly well described by the ΛCDM model. ΛCDM combines general relativity, a cosmological-constant-like dark-energy component Λ, cold dark matter and ordinary baryonic matter, and successfully describes a wide range of observations from the early Universe to the distribution of galaxies.

Dark-matter candidates span an enormous mass and interaction range. They include primordial black holes, axions and axion-like particles, dark photons in some models, weakly interacting massive particles (WIMPs) and sterile-neutrino candidates. Sterile neutrinos are

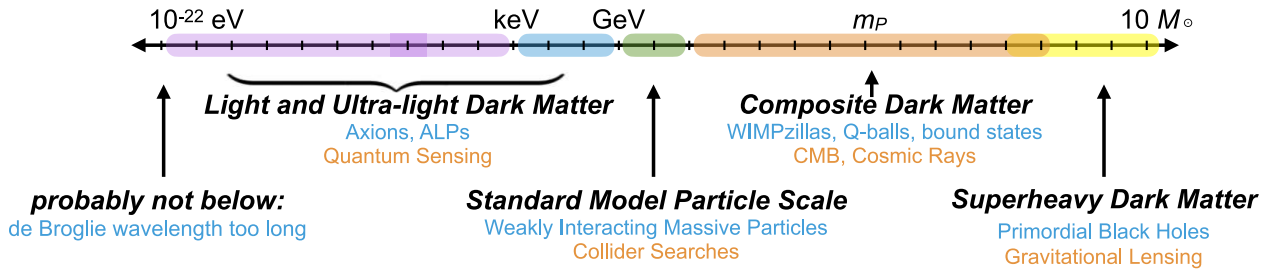


Figure 175: The energy levels of dark matter candidates. Source: [1602] which also positions very well the different quantum sensing techniques used in high-energy particle physics.

Standard-Model gauge singlets, but if they mix with active neutrinos they can acquire indirect weak-interaction signatures. It is therefore too strong to say that they interact only through gravity.

Scientists are looking for these first through indirect methods like the analysis of galaxy rotation curves, gravitational lensing, and cosmic microwave background measurements. Then, there are ongoing efforts in high-energy particle physics experiments to detect dark matter directly, via underground detectors and collider experiments (mostly at the CERN LHC), and astrophysical observations. An incredible number of experiments is conducted or planned to detect these various candidates [1603, 1604].

This part is not about turning you (and me) into a specialist of dark matter which is a very broad scientific field but to discover how quantum sensing and quantum computing may help find trails of various forms of dark matter candidates (Table 1). At the end, we also discuss laboratory tests of dark-energy and modified-gravity models, some of which already use atom interferometry.

2.16.1 Ultralight bosonic dark matter

According to the ultralight bosonic dark matter (UBDM) hypothesis, dark matter consists of extremely light bosons with masses ranging from approximately 10^{-22} eV (e.g., fuzzy dark matter, light axions, hidden photons, and scalar fields) up to 10^{-6} eV or higher in some models (e.g., axion-like particles, dark photons, and hidden sector scalars). Fermionic candidates like sterile or massive neutrinos are not part of the UBDM framework [1606] (Figure 177).

UBDM includes axions and axion-like bosons whose enormous occupation number can make the local dark-matter field behave approximately as a coherent classical wave rather than as individually resolved particles. Describing cosmological axion dark matter as a Bose–Einstein condensate can be useful in some models but is not a model-independent statement. Bao et al. argue that *intrinsically quantum* signatures of axion dark matter are not observable in realistic searches, not that axion dark matter itself is undetectable [1607].

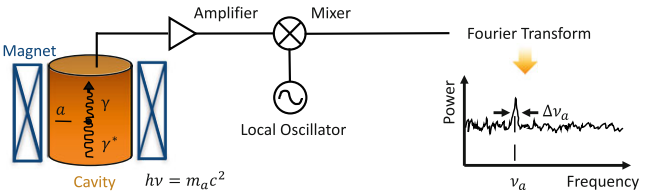


Figure 177: Simplified axion detection schematic of microwave cavity searches. Much like an AM radio, the high frequency axion signal is mixed down to audio frequencies by mixing with a local oscillator maintained at a fixed offset frequency from the cavity frequency. This allows for much lower digitization rates. The cartoon power spectrum shows a sample axion signal above the noise. Caption and schema source: [1606].

Here are various quantum sensing methods to detect axions, most of them being at the proposal stage [1608]:

- **Cold atom based interferometry**, *aka* matter-waves interferometers, which splits and recombines atomic wavefunctions and detects minute phase shifts caused by passing dark matter waves. This is ideal for ultralight bosonic fields. Key experiments are the AEDGE (Atomic Experiment for Dark Matter and Gravity Exploration in Space) proposal to detect scalar and vector fields [1612], MAGIS-100 at Fermilab that uses strontium atoms in a vertical interferometer to detect ultralight dark matter and gravitational waves. It is a prototype for future kilometer-scale sensors [1613]. AION is a UK initiative to deploy a network of vertical interferometers across multiple sites, starting with a 10-meter prototype and scaling up to 100 meters and beyond. It uses rubidium and strontium atoms [1198]. Finally, an international team is proposing the installation of a 100 m interferometer against a wall of the PX46 access shaft to the LHC at CERN. It would "*probe unexplored ranges of the possible couplings of bosonic ultralight dark matter (ULDM) to atomic constituents and undertake a pioneering search for gravitational waves (GWs) at frequencies intermediate between those to which existing and planned experiments are sensitive*" [1609] (Figure 178). The project was technically detailed in a long paper published in 2026, with the experiment getting its name as the Atom Interferometer CERN Experiment (AICE) Facility [1610].

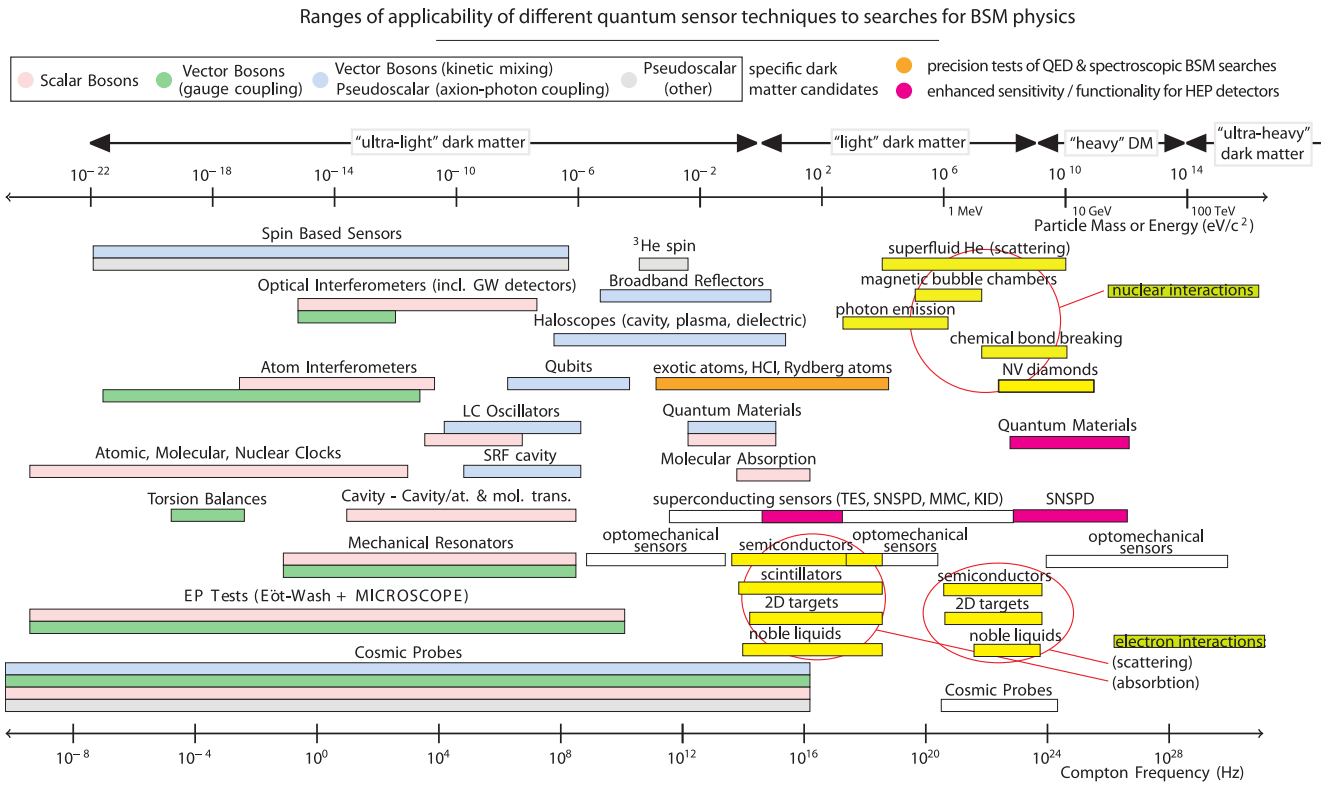


Figure 176: The various quantum sensors used for the seach of dark matter. Source: [1605].

- **Cold atoms sensing** with the SATIN (Signal Amplification Through Time Reversal) experiment that is developed at MIT [1614]. It uses an ensemble of ytterbium-171 ultracold atoms, and leverages quantum entanglement and time-reversed dynamics to amplify signals. It doesn't mean the experiment goes back in time. It applies a reverse transformation to recover the initial state. SATIN could sharpen quantum sensors used to detect gravitational waves and dark matter. There are other proposals for cold atom axion sensing [1615, 1616].

- **Trapped-ions** in linear Paul traps and using a Rabi-type protocol which detects the transition of the qubit from the ground to the excited state [1617].

- **Axion-photon coupling** is used to convert axions or ALPs (axion like particles) into photons in the presence of strong magnetic fields. It is based on microwave photon counters [1618]. This is the technique used in microwave cavity haloscopes like the ADMX (Axion Dark Matter Experiment based at the University of Washington that uses a tunable microwave cavity inside a superconducting magnet [1619] and the QUAX experiment in Italy [1620]. It detects a few single GHz photons via Quantum Non-Demolition measurement (QND) [1621, 1622].

- **Superfluid helium ultralight dark matter detector** with the HeLIOS and HeRALD prototypes. HeLIOS uses the acoustic modes of superfluid helium-4 to detect oscillating forces induced by ultralight dark matter fields. These forces are coherent over millions of cycles, allowing the helium's high-Q mechanical resonances to amplify the signal. A superconducting microwave cavity reads out the motion with extreme sensitivity. By pressurizing the helium, researchers can tune the mechanical frequency, effectively broadening the detection bandwidth [1623]. HeRALD uses superfluid helium as a target for detecting sub-GeV dark matter via quantum evaporation, a process where quasiparticles like phonons and rotons escape the liquid and are detected by transition-edge sensors (TES) which capture scintillation light and quasiparticle excitations. It uses unoxidized cesium films to block superfluid film flow, enabling clean calorimetric measurements [1624]. The experiment can benefit from innovations in cryogenics with the use of a secondary GHS (gas handling system) to cool and helium based experiment within a dilution-based cryostat [1625] (Figure 179).

- **Laser magnetometry** with the GNOME network global array of laser magnetometers using optically pumped cesium atoms to detect disturbances possibly caused by axions. The sensors are sensitive to changes in atomic spin states, which could be triggered by dark matter fields.

- **Superconducting qubit-based sensors** with specific quantum circuits that could enhance signal rates for dark matter detection [1626]. They could help detect wave-like dark matter through phase evolution in qubits [1627–1631]. Superconducting qubits can also detect gamma rays which are outside the field of dark matter [1632].

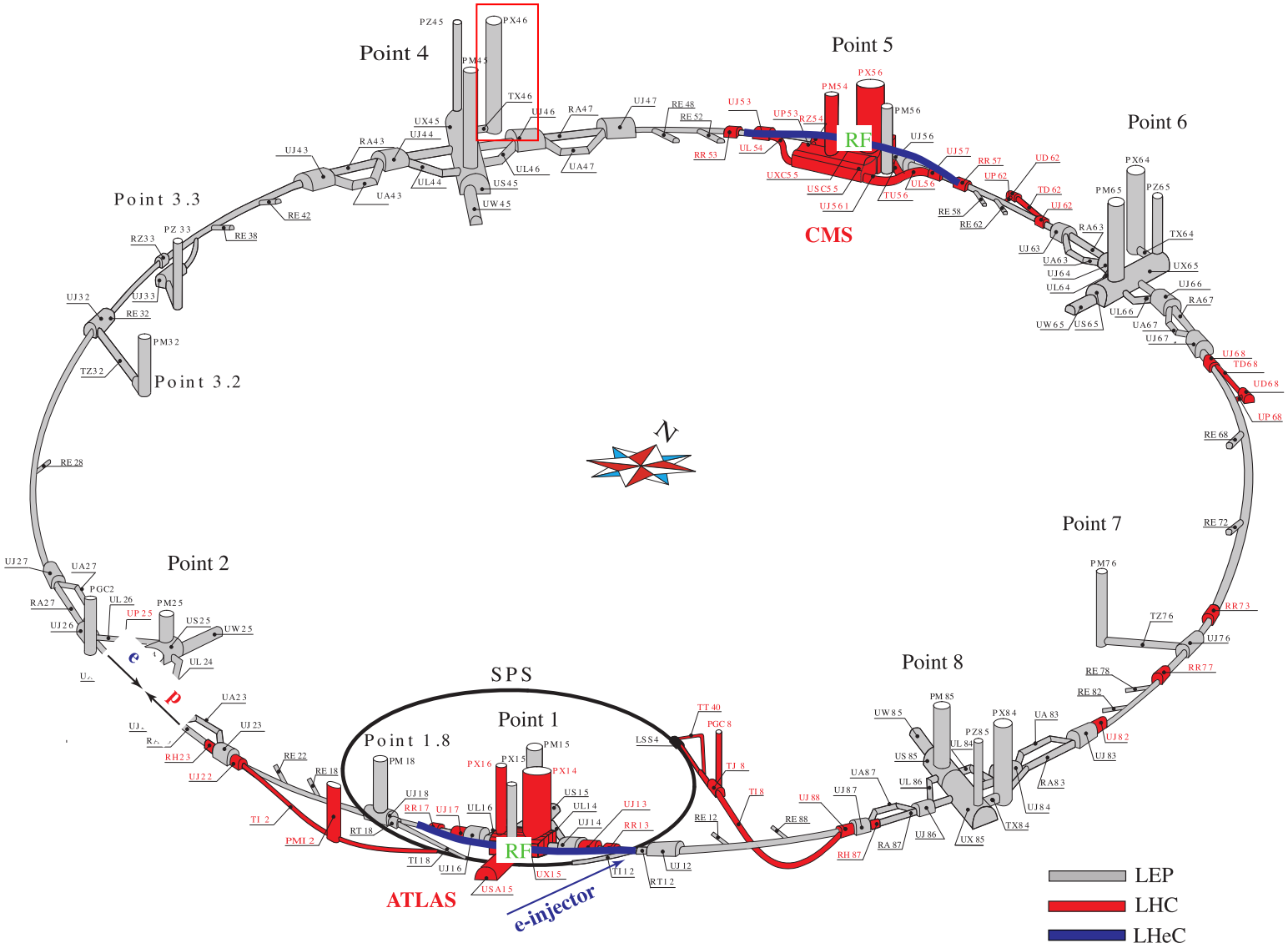


Figure 178: The location in the red rectangle a the top of the proposed 100-m cold atom interferometer in the PX46 access shaft of the CERN LHC at point 4, not far from the CMS experiment [1609]. It is the largest shaft with a height of 146 m. This is good "infrastructure leverage" in a well protected environment. The experiment got its name, Atom Interferometer CERN Experiment (AICE) Facility, in a 2026 preprint [1610]. The LHC has a diameter of 9 km and a length of 27 km. Image source. The two largest experiments in the LHC are Atlas and CMS, which helped discover the Higgs boson in 2012. See my visit report of these experiments in January 2025 in [1611].

- **Nuclear spin sensing** using identical nuclear spins that are coupled to a superconducting circuit [1633].
- **Quantum magnetometry** with variants of atomic magnetometers. For example, [1276] is using 15 atomic magnetometers, which are synchronized with the Global Positioning System (GPS) and are situated on the edges of two meter-scale shielded rooms, serving as a powerful tool to search for dark photons. The magnetic precision is 15 $fT/\sqrt{Hz}$.
- **Optomechanical accelerator** to search for ultralight dark matter at low acoustic frequencies near 39 kHz, the sensor prototype being cooled at 3.5K, with the target one requiring cooling at 10 mK like a superconducting qubit [1634].
- **NV-centers** qutrits [1635] or qubits [1636].
- **CMOS spin qubit arrays** [1637].
- **Quantum dots** coupled to CCDs [1638]

2.16.2 Dark photons

Dark photons can behave like ultralight bosonic dark matter if their mass is extremely low, or they can act as mediators between dark matter and ordinary matter if heavier. Their detection often relies on observing tiny oscillations or shifts in atomic transitions due to kinetic mixing with regular photons. They're not axions or WIMPs but part of the same effort to uncover the nature of dark matter with a different theoretical angle. Among the quantum sensing tools to detect these dark photons, we have superconducting radio frequency cavities [1401].

Quantum Calorimetry Quantum calorimeters (e.g., transition-edge sensors, microwave kinetic inductance detectors) are used in several dark matter experiments and could be highlighted as a cross-cutting technology.

In October 2025, a Fermilab team led by Anna Grasselino proposed to use an array of N entangled superconducting cavities initialized in an m-photon Fock state. Its protocol combines entanglement, photon counting, and stimulated emission to detect dark photons [1639].

2.16.3 Weakly Interacting Massive Particles

At the other end of the dark matter candidate spectrum are WIMPs, which are massive in comparison with axions (Figure 180). Most established direct searches use large conventional rare-event detectors. LZ provides a useful example before we consider quantum-sensing proposals.

Here are a couple related quantum sensors:

- **NV centers** to build a direction-sensitive WIMP detector, with WIMPs scattering off a nucleus in the diamond and creating a nanometer-scale track of vacancies which alter the crystal strain. It can be measured using quantum sensors embedded in the diamond. This allows the reconstruction of the recoil direction which helps distinguish WIMP signals from isotropic backgrounds. At this point, this technique is highly speculative.

- **3D MEMS quantum sensor arrays** to detect ultraheavy dark matter at the mass Planck scale [1601].

The September 2026 LUX-ZEPLIN (LZ) analysis provides a useful boundary case between particle detection and quantum sensing. Its central detector is a dual-phase time projection chamber containing about 7 tonnes of active liquid xenon. A particle recoil creates prompt vacuum-ultraviolet scintillation light, S1, and ionization electrons. Electric fields drift these electrons to the liquid surface and extract them into xenon gas, where electroluminescence produces delayed S2 light. Photomultiplier-tube arrays detect both signals. The S2 light pattern and the S1-S2 delay reconstruct the three-dimensional interaction position, while the S2-to-S1 ratio helps distinguish electron recoils from nuclear recoils. In an exposure of 2.84 tonne-years, LZ observed one event consistent with a nuclear recoil energy of $248 \pm 23\,(\text{stat}) \pm 23\,(\text{sys})$ keV in a low-background region. Across the tested models, the maximum local significance was 3.4σ and the global significance after look-elsewhere effects was 2.6σ [1640]. The event was recorded on June 16, 2023. It is therefore interesting but far below discovery significance and is does not yet an evidence for dark matter detection.

One proposal interprets the event as absorption of fermionic dark matter with a mass near 247 MeV/c^2, but its benchmark coupling is already in strong tension with a recast of KamLAND data [1641]. More LZ data and independent tests will be needed to determine whether the event is a statistical fluctuation, an unidentified background, or a first indication of nonstandard dark matter interactions.

Can LZ itself be called a quantum detector? In the broad sense, yes. A microscopic recoil is converted through quantized excitations, ionization electrons, scintillation photons, and photoelectric detection into classical electrical signals. However, LZ is not a quantum sensor. It does not prepare and coherently control a quantum probe or use interference, squeezing, entanglement, or QND readout to improve its sensitivity [1642]. Its performance primarily comes from target mass, radiopurity, shielding, veto detectors, calibration, spatial reconstruction, and statistical background rejection. LZ should therefore be described as a conventional rare-event particle detector with quantum transduction, rather than as a quantum-enhanced sensor.

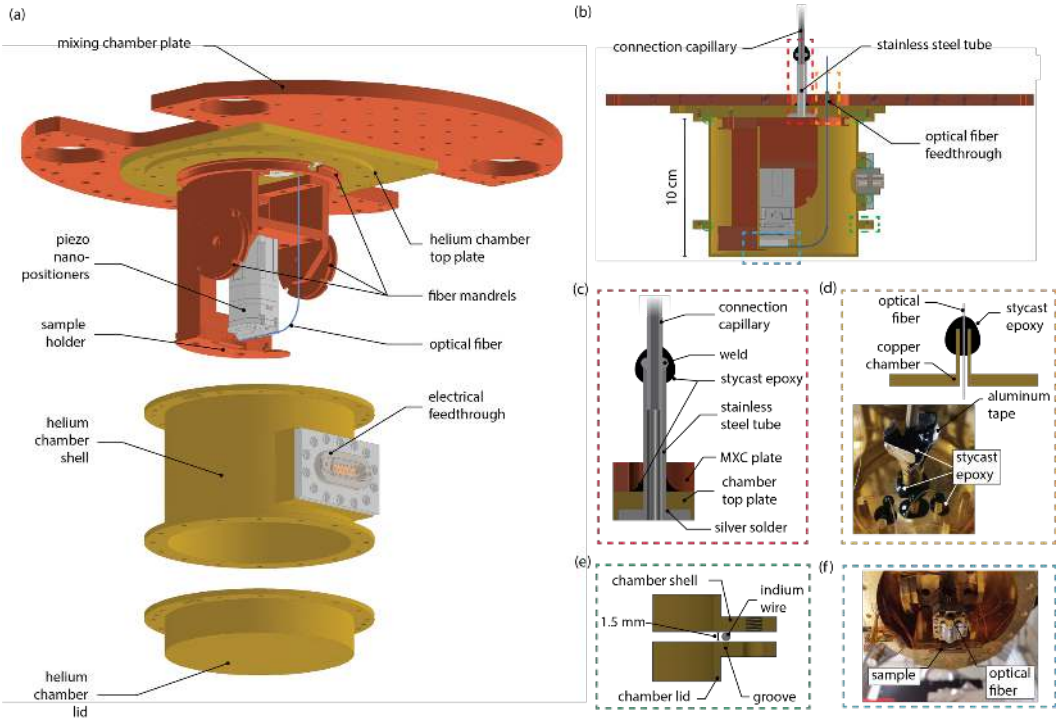


Figure 179: Superfluid helium experiment device within a cryostat. It has its own gas handling system (GHS on top of the one cooling the cryostat. Source: [1625].

Quantum Sensor Type	Used For	Key Experiments / Concepts
Atomic Interferometry	UBDM (scalar/vector fields)	MAGIS-100, AEDGE, AION
Microwave Cavities	Axions, Dark Photons	ADMX, QUAX, SRF cavity experiments
NV Centers in Diamond	WIMPs (directional detection)	Conceptual proposals, strain-based recoil tracking
Superfluid Helium Detectors	UBDM, sub-GeV DM	HeLIOS, HeRALD
Laser Magnetometers	Axions, Dark Photons	GNOME network
Qubit-Based Sensors	UBDM, Dark Photons	Quantum circuits, QND readout
MEMS Arrays	Ultraheavy DM (Planck scale)	Qin et al. (2025)

Table 1: Summary of quantum sensor types used for different dark matter candidates and associated experiments.

2.16.4 Dark energy detection

We've dealt so far with dark matter which is estimated to make up about 27% of the total energy content of the universe. Dark energy is even bigger, accounting for 68% of the energy of the Universe according to models.

Dark matter clusters gravitationally around galaxies and galaxy clusters. Dark energy is not established as a new force. In the standard ΛCDM description it is represented by a cosmological constant with approximately uniform energy density and negative pressure, which drives accelerated cosmic expansion. More general models replace this with a dynamical field or a modification of gravity. Its microscopic nature is unknown.

While dark matter inspires a host of quantum sensor experiments, dark energy is typically studied through large-scale cosmological observations rather than direct detection.

The most widely accepted explanation for dark energy is the cosmological constant (Λ), a concept introduced by Albert Einstein in 1917 [1643] which makes the hypothesis of a constant energy density that fills space uniformly and exerts negative pressure, causing the universe to expand faster over time. It has an extremely small value. An alternative to this static model is quintessence, a dynamic scalar field that evolves over time and could vary across space. It might leave subtle imprints on the cosmic microwave background or the distribution of galaxies.

Other speculative candidates include phantom energy, which has even more negative pressure than quintessence and could lead to a hypothetical "Big Rip" scenario where the universe tears itself apart (after a long time,

lucky you are). Chameleon fields is another option. It changes properties depending on the local matter density, potentially evading detection in dense environments. Some researchers also propose that dark energy might not be a new substance at all, but rather a sign that our understanding of gravity needs revision. Modified gravity theories, such as f(R) gravity or the DGP model, suggest that the laws of gravity evolve on cosmic scales.

Quantum sensors are already involved in laboratory tests of some dark-energy and modified-gravity models. Atom-interferometry experiments have searched for anomalous accelerations produced by screened scalar fields and have placed constraints on chameleon and symmetron parameter spaces [1644]. These experiments do not directly detect the cosmological dark-energy density. Rather, they test specific scalar-field or modified-gravity mechanisms motivated in part by cosmic acceleration. Precision clocks, accelerometers, Casimir-force measurements and optomechanical systems can provide complementary constraints on related new-force models.

Dark energy research currently relies on astronomical observations as with the observation of Type Ia supernovae to measure cosmic distances, while baryon acoustic oscillations and weak gravitational lensing help map the large-scale structure of the universe. The cosmic microwave background (CMB) provides a snapshot of the early universe that can be used to infer the influence of dark energy over time. Future space missions such as the ESA's Euclid telescope [1645] which uses a large array of CCD imagers and a Near-Infrared Spectrometer and Photometer, NASA's Nancy Grace Roman Space Telescope (using infrared imagers) and the Vera Rubin Observatory's LSST (a 8.5m terrestrial telescope located in Chile using a donut shaped mirror and a 64 cm wide CCD array-based 3.2-gigapixel camera Figure 181) may help refine scientists' understanding of dark energy's equation of state and its evolution.

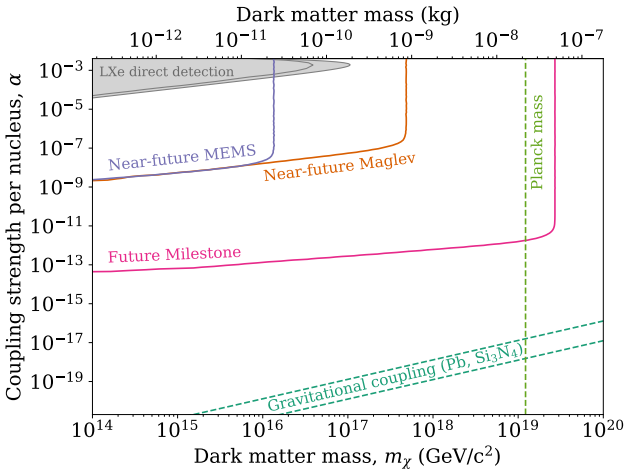


Figure 180: Dark matter sensitivity of the different sensor configurations investigated in [1601].

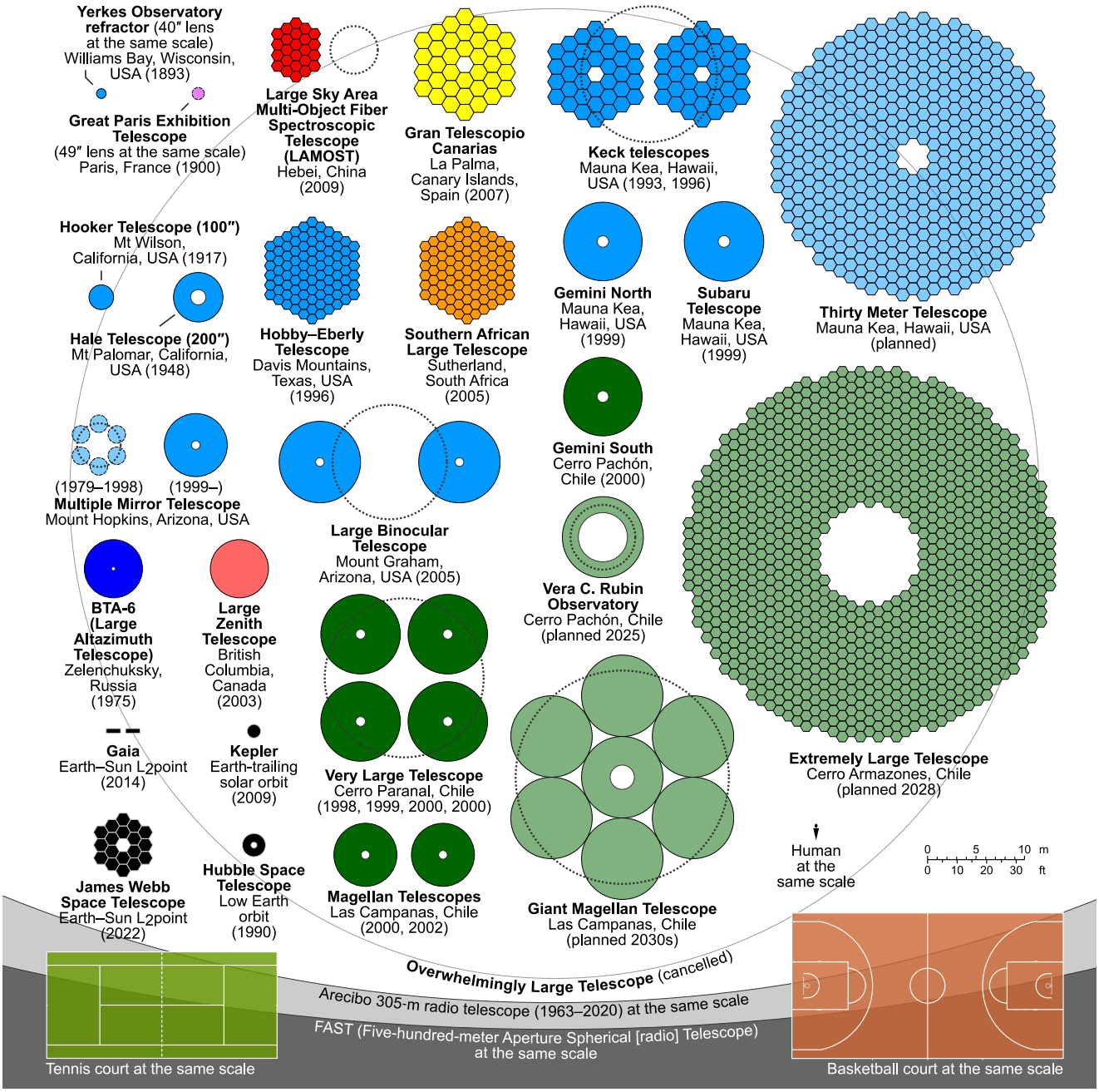


Figure 181: Comparison of space and ground telescopes mirror sizes with the Vera Rubin in green in the middle with its donut shape mirror. Source: Wikipedia.

2.17 Quantum sensing key takeaways

- Quantum sensing is a slightly more mature and overlooked market in quantum technologies, one potential reason being its fragmentation and currently limited large-scale use cases. It is perceived as having a higher technology readiness level (TRL) than quantum computing. But these sensors are still not easy to design from an industrial point of view and their actual accuracy and sensitivity do not always match expectations.
- Quantum sensing enables more precise measurement of nearly any physical parameter: time, distance, temperature, movement, acceleration, pressure, gravity, magnetism, light frequency, radio spectrum and the chemical composition of matter.
- The 2019 revision of the International System of Units (SI) fixed exact numerical values for several defining physical constants. Quantum electrical standards, atomic clocks and other precision-measurement techniques are central to the realization and dissemination of several SI units, but it is more accurate to describe them as part of precision metrology than to say that quantum sensing itself "updated" the SI.
- Lasers and optical frequency combs are used for extremely precise frequency and time metrology, including comparisons involving optical atomic clocks that can outperform cesium microwave clocks in stability and accuracy. Frequency combs are commonly generated with mode-locked lasers producing trains of ultrashort, often femtosecond, pulses.
- Nitrogen-vacancy (NV) centers in diamond are one of the most widely studied solid-state quantum-sensing platforms. They can measure magnetic fields and, through adapted protocols, other parameters such as temperature, pressure or electric fields, with applications ranging from materials characterization to biomedical research. Their practical performance depends on trade-offs among sensitivity, spatial resolution, bandwidth, stand-off distance and form factor. Many implementations are still moving from laboratory demonstrations toward robust products.
- Another important approach is cold-atom interferometry, implemented in gravimeters, accelerometers and inertial sensors relevant to PNT, meaning "positioning, navigation, and timing". Atomic systems can also be used for radio-frequency sensing and are being investigated for searches for some forms of dark matter.
- China supposedly built some quantum radars using photon entanglement and up/down converters between visible photons and radar frequencies, but the real performance of these devices is questionable, particularly their range, and is driving a lot of skepticism in the Western world. But the related research is still going on and quantum LiDARs seem to make progress. Quantum sensing can also potentially improve the sensitivity of classical radars.

2.18 Bibliography and notes

These are the bibliographical references and notes for the **Quantum sensing** section.

[1131] Quantum Sensing Use Cases 2022, by SRI, QED-C, September 2022 (36 pages).

[1132] Nitrogen Vacancy Centers in Diamond for Quantum Biosensing: Magnetometry Techniques, Platforms and Applications, by Sirsendu Ghosal, Umakant Prajapati, Sachin Negi, Saifian Farooq Bhat, Thejas B, and Vibhav Bharadwaj, arXiv, September 2026 (50 pages).

[1133] 2025 Market Forecast: Quantum Sensing, by Bob Sorensen, QED-C, March 2025 (14 slides).

[1134] Quantum Sensors Market Size, Share, and Industry Analysis, by Fortune Business Insights et al., June 2025 (150 pages).

[1135] Global Quantum Sensors Market Outlook, by Astute Analytica et al., April 2025 (180 pages).

[1136] Quantum Sensors Market Size and Trends, by DataM Intelligence et al., February 2025 (120 pages).

[1137] Quantum Sensors Market 2026 Report, by Fortune Business Insights et al., January 2026 (160 pages).

[1138] Quantum Sensors Market Share Analysis, by Mordor Intelligence et al., March 2026 (140 pages).

[1139] Quantum Sensors Market Growth Forecast, by Fortune Business Insights et al., September 2024 (155 pages).

[1140] Quantum Sensors Market Size Report, by Grand View Research et al., May 2024 (110 pages).

[1141] Quantum Sensors Market Forecast to 2035, by DataM Intelligence et al., August 2025 (130 pages).

[1142] Quantum Sensors Market Growth to 2035, by Astute Analytica et al., November 2025 (190 pages).

[1143] Quantum Sensors: Ten Year Market Projections, by Lawrence Gasman, Inside Quantum Technology, March 2019 (7 slides).

[1144] A Perspective on Quantum Sensors from Basic Research to Commercial Applications, by Eun Oh, Charles A. Sackett, et al., arXiv, June 2024 (96 pages).

[1145] Quantum Sensing for Energy Applications: Review and Perspective, by Scott E Crawford et al., June 2021 (33 pages).

[1146] Quantum Communication, Sensing and Measurement in Space, by Baris I. Erkmen, 2012 (136 pages).

[1147] Quantum Sensors for High Energy Physics, by Aaron Chou, Kathryn M. Zurek, et al., arXiv, November 2023 (63 pages).

[1148] Snowmass 2021: Quantum Sensors for HEP Science - Interferometers, Mechanics, Traps, and Clocks, by Oliver Buchmueller, Marianna S. Safronova, et al., arXiv, September 2022 (18 pages).

[1149] The International System of Units (SI), by NIST, 2019 (138 pages).

[1150] Quantum sensing, by C. L. Degen, F. Reinhard, and P. Cappellaro, arXiv, June 2017 (45 pages).

[1151] A Framework for Spatial Quantum Sensing, by Luís Bugalho, Yasser Omar, and Damian Markham, arXiv, May 2026 (32 pages).

[1152] Qutrit entanglement and joint multi-parameter estimation in an optical clock platform, by Ohad Lib, Shuheng Liu, Maximilian Ammenwerth, Hendrik Timme, Shijia Sun, Qiongyi He, Marcus Huber, Giuseppe Vitagliano, Immanuel Bloch, and Johannes Zeiher, arXiv, August 2026 (17 pages).

[1153] Minutes-scale Schrödinger-cat state of spin-5/2 atoms, by Y. A. Yang, W.-T. Luo, J.-L. Zhang, S.-Z. Wang, Chang-Ling Zou, T. Xia, and Z.-T. Lu, arXiv, October 2024 (20 pages).

[1154] Microkelvin resolution thermometry at the nanometre scale, by Jack W. Hart, Soham Pal, Julien R. E. Roth, Katie Ninham, Abbie H. Aleksandrova, Xander Peetroons, Soumen Mandal, Oliver A. Williams, Gavin W. Morley, Mete Atature, and Helena S. Knowles, arXiv, September 2026 (8 pages).

[1155] Current Trends in Global Quantum Metrology, by Chiranjib Mukhopadhyay, Victor Montenegro, and Abolfazl Bayat, arXiv, February 2025 (16 pages).

[1156] Fundamental Limits of Continuous Gaussian Quantum Metrology, by Kazuki Yokomizo, Aashish A. Clerk, and Yuto Ashida, arXiv, January 2026 (31 pages).

[1157] Quantum Metrology under Coarse-Grained Measurement, by Byeong-Yoon Go, Geunhee Gwak, Young-Do Yoon, Sungho Lee, Nicolas Treps, Jiyong Park, and Young-Sik Ra, arXiv, January 2026.

[1158] Quantum Analog-to-Digital Converter for Phase Estimation, by Eugenio Caruccio, Fabio Sciarrino, et al., arXiv, February 2025 (5 pages).

[1159] Universal quantum operations and ancilla-based read-out for tweezer clocks, by Ran Finkelstein, Adam L. Shaw, Manuel Endres, et al., Nature, October 2024.

[1160] Quantum Computing Enhanced Sensing, by Richard R. Allen, Francisco Machado, Isaac L. Chuang, Hsin-Yuan Huang, and Soonwon Choi, arXiv, January 2025 (9 pages).

[1161] Journey in quantum metrology and sensing from foundations to applications: a review, by Priya Ghosh, Tanoy Kanti Konar, Debraj Rakshit, Aditi Sen De, and Ujjwal Sen, arXiv, May 2026 (93 pages).

[1162] Tutorial: Optical quantum metrology, by Marco Barbieri, arXiv, July 2025 (24 pages).

[1163] Noise-Resilient Quantum Metrology with Quantum Computing, by Xiangyu Wang, Chenrong Liu, Xinqing Wang, Dawei Lu, and Ying Dong, arXiv, August 2025 (10 pages).

[1164] Robust estimation of the Quantum Fisher Information on a quantum processor, by Vittorio Vitale, Cyril Branciard, Benoît Vermersch, et al., arXiv, July 2024 (24 pages).

[1165] Ultimate limits to quantum metrology and the meaning of the Heisenberg limit, by Marcin Zwierz, Carlos A. Pérez-Delgado, and Pieter Kok, Physical Review A, April 2012.

[1166] Quantum-Error-Mitigation Circuit Groups for Noisy Quantum Metrology, by Yusuke Hama and Hirofumi Nishi, arXiv, April 2023 (42 pages).

[1167] Autonomous Quantum Error Correction and Application to Quantum Sensing with Trapped Ions, by F. Reiter, A. S. Sørensen, P. Zoller, and C. A. Muschik, arXiv, February 2017 (6 pages).

[1168] General Optimality of the Heisenberg Limit for Quantum Metrology, by Marcin Zwierz, Carlos A. Pérez-Delgado, and Pieter Kok, Physical Review Letters, October 2010 (preprint on arXiv).

[1169] Quantum metrology in the noisy intermediate-scale quantum era, by Lin Jiao, Wei Wu, Si-Yuan Bai, and Jun-Hong An, arXiv, November 2023 (23 pages).

[1170] Heisenberg Limit beyond Quantum Fisher Information, by Wojciech Górecki, arXiv, April 2023 (103 pages).

[1171] Achieving the Heisenberg limit using fault-tolerant quantum error correction, by Himanshu Sahu, Qian Xu, and Sisi Zhou, arXiv, January 2026 (18 pages).

[1172] Rare-Event Quantum Sensing using Logical Qubits, by Robert Ott, Torsten V. Zache, Soonwon Choi, Adam M. Kaufman, and Hannes Pichler, arXiv, January 2026 (12 pages).

[1173] Generalized Limits for Single-Parameter Quantum Estimation, by Sergio Boixo, Physical Review Letters, February 2007 🔓 (preprint on arXiv).

[1174] Exponentially Enhanced Quantum Metrology, by S. M. Roy, Physical Review Letters, June 2008 🔓 (preprint on arXiv).

[1175] Adaptive Quantum Metrology under General Markovian Noise, by Rafał Demkowicz-Dobrzański, Physical Review X, October 2017.

[1176] Entanglement-enhanced optimal quantum metrology, by Muhammad Talha Rahim, Saif Al-Kuwari, and Asad Ali, arXiv, November 2024 (10 pages).

[1177] Non-Markovian noise mitigation in quantum teleportation: enhancing fidelity and entanglement, by Haiyang Zhang, Caijuan Xia, et al., Scientific Reports, October 2024.

[1178] Distributed quantum sensing with a mode-entangled network of spin-squeezed atomic states, by Benjamin K. Malia, Mark A. Kasevich, et al., arXiv, May 2022 (8 pages).

[1179] Parallel Quantum-Enhanced Sensing, by Mohammadjavad Dowran, Alberto M. Marino, et al., arXiv, November 2023 (12 pages).

[1180] Quantum Logic Enhanced Sensing in Solid-State Spin Ensembles, by Nithya Arunkumar, Ronald L. Walsworth, et al., arXiv, March 2022 (7 pages).

[1181] All-optical Loss-tolerant Distributed Quantum Sensing, by Rajveer Nehra, Changhun Oh, Liang Jiang, and Alireza Marandi, arXiv, July 2024 (15 pages).

[1182] Enhancing Optical Imaging via Quantum Computation, by Aleksandr Mokeev, Babak Saif, Mikhail D. Lukin, and Johannes Borregaard, PRX Quantum, January 2026 (18 pages).

[1183] Quantum Metrology with Delegated Tasks, by Nathan Shettell and Damian Markham, arXiv, November 2022 (21 pages).

[1184] Optimized quantum sensor networks for ultralight dark matter detection, by Adriel I. Santoso and Le Bin Ho, arXiv, May 2025 (7 pages).

[1185] Experimental secure entanglement-free quantum remote sensing over 50 km of optical fiber, by Wenjie He, Chunfeng Huang, Rui Guan, Ye Chen, Zhenrong Zhang, and Kejin Wei, arXiv, December 2024 (7 pages).

[1186] Optimal scheme for distributed quantum metrology, by Zhiyao Hu, Allen Zang, Jianwei Wang, Tian Zhong, Haidong Yuan, Liang Jiang, and Zain H. Saleem, arXiv, September 2025 (11 pages).

[1187] Anonymous and private parameter estimation in networks of quantum sensors, by Jarn de Jong, Anna Pappa, et al., arXiv, July 2025 (20 pages).

[1188] Correlation Geometry of Quantum Sensor Networks: Local-Global Information Flow and Local Privacy, by Gong-Chu Li, Lei Chen, Xu-Song Hong, Hua-Qing Xu, Yuancheng Liu, Si-Qi Zhang, Jia-Hao Zhao, Geng Chen, Chuan-Feng Li, and Guang-Can Guo, arXiv, August 2026 (5 pages).

[1189] Quantum metrology enhanced by effective time reversal, by Yu-Xin Wang, Flavio Salvati, David R. M. Arvidsson-Shukur, William F. Braasch Jr., Kater Murch, and Nicole Yunger Halpern, arXiv, February 2026 (11 pages).

[1190] Atom Interferometer Tests of Dark Matter, by Yufeng Du, Clara Murgui, Kris Pardo, Yikun Wang, and Kathryn M. Zurek, arXiv, September 2024 (26 pages).

[1191] Experimental gravitation and geophysics with matter wave sensors, by Philippe Bouyer, LP2N, 2018 (234 slides).

[1192] Ultracold Quantum Gravimeters: An Introduction for Geophysicists, by Ivaldevingles Rodrigues De Souza Junior, Andrea Trombettoni, and Carla Braitenberg, arXiv, January 2026 (43 pages).

[1193] Atomic Interferometry Using Stimulated Raman Transitions, by Mark Kasevich et al., PRL, July 1991 (4 pages).

[1194] Young double-slit experiment with atoms: A simple atom interferometer, by Olivier Carnal and Jürgen Mlynek, 1991 (6 pages).

[1195] INTENTAS – An entanglement-enhanced atomic sensor for microgravity, by O. Anton, L. Wörner, et al., arXiv, September 2024 (30 pages).

[1196] Free-Falling Interferometry, by Markus Arndt, Physics, February 2013.

[1197] A Compact Cold-Atom Interferometer with a High Data-Rate Grating Magneto-Optical Trap and a Photonic-Integrated-Circuit-Compatible Laser System, by Jongmin Lee, Peter D. D. Schwindt, et al., arXiv, September 2022 (21 pages).

[1198] AION-10: Technical Design Report for a 10m Atom Interferometer in Oxford, by Kai Bongs, I. Wilmut, et al., arXiv, August 2025 (53 pages).

[1199] Chip-scale superconducting quantum gravimeter combining a SQUID, a transmon, and a nanomechanical resonator, by Salman Sajad Wani, Mughees Ahmed Khan, Abrar Ahmed Naqash, and Saif Al-Kuwari, arXiv, May 2026 (17 pages).

[1200] Observation of the effect of gravity on the motion of antimatter, by E. K. Anderson, C. J. Baker, W. Bertsche, et al., Nature, September 2023 (7 pages).

[1201] A quantum leap for antimatter measurements, by CERN, CERN, July 2025.

[1202] Coherent spectroscopy with a single antiproton spin, by B. M. Latacz, S. Ulmer, et al., Nature, July 2025.

[1203] Compact and Portable Atom Gravimeter, by Shuai Chen, ITU, June 2019 (22 slides).

[1204] Quantum sensing for gravity cartography, by Ben Stray, Kai Bongs, Michael Holynski, et al., Nature, February 2022.

[1205] Position fixing with cold atom gravity gradiometers, by Alexander M. Phillips, Jason F. Ralph, et al., arXiv, April 2022 (10 pages).

[1206] Circulating pulse cavity enhancement as a method for extreme momentum transfer atom interferometry, by Rustin Nourshargh, Michael Holynski, et al., Communications Physics, December 2021.

[1207] ONERA invents with SHOM the "atomic" precision gravity mapping, by ONERA, February 2016.

[1208] Quantum sensing of acceleration and rotation by interfering magnetically-launched atoms, by Clément Salducci, Alexandre Bresson, et al., arXiv, September 2024 (20 pages).

[1209] A Short Introduction to Basic Principles of Quantum Navigation Based-on Rb Cold Atom Interferometry, by Narges Kafaei and Ali Motazedifard, arXiv, May 2024 (7 pages).

[1210] Realization of a cold atom gyroscope in space, by Jinting Li et al., National Science Review, January 2025 (10 pages).

[1211] Noisy quantum gyroscope, by Lin Jiao and Jun-Hong An, arXiv, January 2023 (9 pages).

[1212] Nonlinear Multi-Resonant Cavity Quantum Photonics Gyroscopes Quantum Light Navigation, by Mengdi Sun, Marko Lončar, Vassilios Kovanis, and Zin Lin, arXiv, October 2023 (18 pages).

[1213] A Precision Gyroscope from the Helicity of Light, by Michael A. Fedderke, Vyacheslav P. Yakovlev, et al., arXiv, April 2025 (16 pages).

[1214] Enhancing the sensitivity of quantum fiber-optical gyroscopes via a non-Gaussian-state probe, by Wen-Xun Zhang, Rui Zhang, Yunlan Zuo, and Le-Man Kuang, arXiv, June 2024 (10 pages).

[1215] Quantum gyroscopes based on double-mode surface-acoustic-wave cavities, by Yuting Zhu, Shibei Xue, Fangfang Ju, and Haidong Yuan, arXiv, January 2024 (12 pages).

[1216] Focusing Surface-Acoustic-Wave Resonators on Thin-Film Lithium Niobate with Transverse-Mode Suppression, by Ryo Sasaki, Ryusuke Hisatomi, Rekishu Yamazaki, Yuya Yamaguchi, Yasunobu Nakamura, and Atsushi Noguchi, arXiv, July 2026 (10 pages).

[1217] Emulated nuclear spin gyroscope with ^{15}NV centers in diamond, by Guoqing Wang, Paola Cappellaro, et al., arXiv, January 2024 (11 pages).

[1218] Quantum gyroscope based on the cavity magnomechanical system, by Zhe-Qi Yang, Lei Chen, Yu-Rong Lin, Wei Qin, and Zhi-Rong Zhong, arXiv, May 2025 (13 pages).

[1219] Exploring gravity with the MIGA large scale atom interferometer, by B. Canuel, Philippe Bouyer, et al., Scientific Reports, September 2018.

[1220] A gravity antenna based on quantum technologies: MIGA, by B. Canuel, Philippe Bouyer, et al., arXiv, April 2022 (4 pages).

[1221] Quantum metrology of rotations with mixed spin states, by Eduardo Serrano-Ensástiga, Chryssomalis Chryssomalakos, and John Martin, arXiv, February 2025 (15 pages).

[1222] Quantum enhanced mechanical rotation sensing using wavefront photonic gears, by Ofir Yesharim, Guy Tshuva, and Ady Arie, arXiv, April 2024 (8 pages).

[1223] Rotation sensing using tractor atom interferometry, by Bineet Dash, Georg Raithel, et al., AVS Quantum Science, March 2024.

[1224] Quantum-assured magnetic navigation achieves positioning accuracy better than a strategic-grade INS in airborne and ground-based field trials, by Murat Muradoglu, Michael J. Biercuk, et al., arXiv, April 2025 (10 pages).

[1225] GNSS-free quantum gravity-aided navigation and fine-scale marine surveying with a strapdown quantum gravimeter, by Patrick J. Everitt, Donald H. White, Todd Lyon, Murat Muradoglu, Alessandro D'Ortenzio, Aaron J. Canciani, Malo Cadoret, Daniel D. Brown, David Adams, Yosri Ben-Aïcha, Suraj Bijjahalli, Mojtaba K. Farsani, Alexander Rischka, Karandeep S. Gill, Magdalena Meyer, Henry W. Orton, Nicholas P. Robins, Reuben Symon, Michael J. Biercuk, Michael R. Hush, Stuart S. Szigeti, and Russell P. Anderson, arXiv, August 2026 (14 pages).

[1226] Boeing completes world's 1st quantum navigation flight test, by Boeing, August 2024.

[1227] Atom interferometry and its applications, by Sven Abend, Wolfgang P. Schleich, et al., arXiv, January 2020 (48 pages).

[1228] Detecting Volcano-Related Underground Mass Changes With a Quantum Gravimeter, by Laura Antoni-Micollier, June 2022 (9 pages).

[1229] Gravity measurements below 10-9 g with a transportable absolute quantum gravimeter, by Vincent Ménoret, Bruno Desruelle, et al., Scientific Reports, August 2018.

[1230] Digging Into Quantum Sensors, by Stewart Wills in Optics & Photonics, September 2019.

[1231] Cold atom interferometry sensors: physics and technologies, by Martino Travagnin, July 2020 (47 pages).

[1232] Ramsey Resonance in a Zacharias Fountain, by A. Clairon, Christophe Salomon, S. Guellati, and William D. Phillips, Europhysics Letters, 1991.

[1233] A leap towards quantum inertial sensing for onboard applications with atom interferometry, by Simon Jumel, July 2024.

[1234] Fifteen Years of Cold Matter on the Atom Chip: Promise, Realizations, and Prospects, by Mark Keil, Ron Folman, et al., arXiv, May 2016 (44 pages).

[1235] Micro-fabricated components for cold atom sensors, by J. P. McGilligan, September 2022 (28 pages).

[1236] Mobile and remote inertial sensing with atom interferometers, by B. Barrett, Arnaud Landragin, et al., arXiv, August 2014 (63 pages).

[1237] Cold atom interferometry sensors: physics and technologies, by Martino Travagnin, JRC Publications Repository, July 2020 (47 pages).

[1238] Distributed Quantum Magnetic Sensing for Infrastructure-free Geo-localization, by Thinh Le, Shiqian Guo, and Jianqing Liu, arXiv, December 2025 (13 pages).

[1239] Advanced LIGO Just Got More Advanced Thanks To An All-New Quantum Enhancement, by Ethan Siegel, December 2019.

[1240] NIST Team Supersizes 'Quantum Squeezing'to Measure Ultrasmall Motion, by NIST, 2019.

[1241] Squeezing the quantum noise of a gravitational-wave detector below the standard quantum limit, by Wenxuan Jia et al., arXiv, October 2024 (17 pages).

[1242] Small Cesium Atomic Fountain Clock for Time Keeping System, by JIN Shuanghao et al., Acta Metrologica Sinica, December 2024 (18 pages).

[1243] Quantum Sensing with Atomic, Molecular, and Optical Platforms for Fundamental Physics, by Jun Ye et al., PRL, May 2024 (11 pages).

[1244] Time and Quantum Clocks: a review of recent developments, by M. Basil Altaie, Daniel Hodgson, and Almut Beige, arXiv, May 2022 (39 pages).

[1245] Quantum clocks are more precise than classical ones, by Mischa P. Woods, Ralph Silva, Gilles Pütz, Sandra Stupar, and Renato Renner, arXiv, February 2022 (60 pages).

[1246] Basics of atomic clocks, by Andrei Derevianko, 2021 (77 slides).

[1247] A multi-ion optical clock with $\mathbf{5 \times 10^{-19}}$ uncertainty, by Melina Filzinger, Martin R. Steinel, Jian Jiang, Daniel Bennett, Tanja E. Mehlstäubler, Ekkehard Peik, and Nils Huntemann, arXiv, March 2026 (11 pages).

[1248] Chronometric Geodesy: Methods and Applications, by Pacome Delva, Heiner Denker, and Guillaume Lion, Rigetti, January 2019 (161 pages) 🔓 (preprint on arXiv).

[1249] MEMS Atomic Clocks, by Svenja Knappe, 2008 (45 pages).

[1250] Fifteen Years of Cold Matter on the Atom Chip: Promise, Realizations, and Prospects, by Mark Keil et al., 2016 (44 pages).

[1251] Fundamental accuracy-resolution trade-off for timekeeping devices, by Florian Meier, Emanuel Schwarzhans, Paul Erker, and Marcus Huber, arXiv, November 2023 (7 pages).

[1252] Nobel Lecture: Defining and measuring optical frequencies, by John L. Hall, Reviews of Modern Physics, November 2006 (17 pages).

[1253] Phase Coherent Vacuum-Ultraviolet to Radio Frequency Comparison with a Mode-Locked Laser, by J. Reichert, T. W. Hänsch, et al., Physical Review Letters, April 2000 🔓.

[1254] Direct Link between Microwave and Optical Frequencies with a 300 THz Femtosecond Laser Comb, by Scott Diddams, 2000 (4 pages).

[1255] Fundamentals of frequency combs What they are and how they work, by Scott Diddams, NIST, 2015 (46 slides).

[1256] Optical frequency combs and optical frequency measurements, by Yann Le Coq, LNE-SYRTE, April 2014 (38 slides).

[1257] Chip-scale Optical Atomic Clocks and Integrated Photonics, by Matthew Hummon, 2018 (35 slides).

[1258] Optical Atomic Clocks, by Andrew Ludlow et al., 2015 (65 pages).

[1259] Frequency comb spectroscopy, by Nathalie Picqué and Theodor W. Hänsch, arXiv, February 2019 (27 pages).

[1260] Quantum Logic for Precision Spectroscopy, by Piet Schmidt, 2009 (6 pages).

[1261] $^{27}Al^{+}$ Quantum-Logic Clock with a Systematic Uncertainty below 10^{-18}, by S. M. Brewer, D. R. Leibrandt, et al., Physical Review Letters, July 2019 🔓 (preprint on arXiv).

[1262] Optical atomic clocks, by N. Poli, C. W. Oates, P. Gill, and G. M. Tino, arXiv, January 2014 (69 pages).

[1263] Architecture for the photonic integration of an optical atomic clock, by Zachary L. Newman, Optica, May 2019 (6 pages).

[1264] An optical lattice clock, by Masao Takamoto, Feng-Lei Hong, Ryoichi Higashi, and Hidetoshi Katori, Nature, May 2005 (4 pages) 🔓.

[1265] Universal quantum operations and ancilla-based readout for tweezer clocks, by Ran Finkelstein, Manuel Endres, et al., arXiv, October 2024 (24 pages).

[1266] Usefulness of Quantum Entanglement for Enhancing Precision in Frequency Estimation, by Marco A. Rodríguez-García, Ruynet L. de Matos Filho, and Pablo Barberis-Blostein, arXiv, December 2024 (16 pages).

[1267] Clock precision beyond the Standard Quantum Limit at 10^{-18} level, by Y. A. Yang, Maya Miklos, Yee Ming Tso, Stella Kraus, Joonseok Hur, and Jun Ye, arXiv, May 2025 (6 pages).

[1268] Free-space dissemination of time and frequency with 10^{-19} instability over 113 km, by Qi Shen, Jian-Wei Pan, et al., Nature, October 2022 🔓 (preprint on arXiv).

[1269] LEO Clock Synchronization with Entangled Light, by Ronakraj Gosalia, Robert Malaney, Ryan Aguinaldo, Jonathan Green, and Peter Brereton, arXiv, February 2024 (6 pages).

[1270] Entropic costs of the quantum-to-classical transition in a microscopic clock, by Vivek Wadhia, Florian Meier, Natalia Ares, et al., arXiv, January 2025 (16 pages).

[1271] A nuclear clock based on ^{229}Th, by Beichen Huang, Gaowei Yan, Qi Xiao, Wenhao Bu, Zhen Zhang, Chengchun Zhao, Chao Yan, Zhi-Ang Chen, Peixiong Zhang, Gleb Penyazkov, Zhenhai Zhan, Lingfeng Yan, Yuefei Wang, Lin Li, Shanming Li, Xiaobo Qian, Xuegang Liu, Qiange He, Taoxiang Sun, Haochen Tian, Binkun Lu, Ningyuan Ma, Juxian Li, Yanzhang Wu, Qiaorui Gong, Yuxiang Li, Haoyu Shi, Xiangliang Li, Longsheng Ma, Shining Zhu, Yuxiang Mo, Jun Lin, Li You, Yige Lin, Xibo Zhang, Yin Hang, Liangbi Su, and Shiqian Ding, arXiv, June 2026 (8 pages).

[1272] Toward nanophotonic platforms for solid-state ^{229}Th nuclear clocks, by Sandro Kraemer, Karen Mamian, Toby Bi, Shun Fujii, Jan de Haan, Harshith Babu, Arno Claessens, Rafael Ferrer Garcia, Fedor Ivandikov, Piet Van Duppen, Andreas Dragoun, Christoph E. Düllmann, Christoph Marquardt, Ulrich Wahl, Bart Kuyken, Thorsten Schumm, Pascal Del'Haye, Lino M. C. Pereira, Georgy A. Kazakov, Kasper Van Gasse, and Charles Roques-Carmes, arXiv, April 2026 (30 pages).

[1273] Towards global time distribution via satellite-based sources of entangled photons, by Stav Haldar, Physical Review A, February 2023 🔓 (preprint on repository.lsu.edu).

[1274] Nitrogen-vacancy centers in diamond for nanoscale magnetic resonance imaging applications, by Alberto Boretti, 2019 (24 pages).

[1275] Colloquium: Quantum limits to the energy resolution of magnetic field sensors, by Morgan W. Mitchell et al., Reviews of Modern Physics, April 2020 🔓 (preprint on arXiv).

[1276] Long-baseline quantum sensor network as dark matter haloscope, by Min Jiang, Jiangfeng Du, et al., Nature Communications, April 2024.

[1277] Dark matter detection using optically trapped Rydberg atom tweezer arrays, by So Chigusa, Taiyo Kasamaki, Toshi Kusano, Takeo Moroi, Kazunori Nakayama, Naoya Ozawa, Yoshiro Takahashi, Atsuhiro Umemoto, and Amar Vutha, arXiv, July 2025 (9 pages).

[1278] Enabling photonic integrated 3D magneto-optical traps for quantum sciences and applications, by Daniel J. Blumenthal, Andrei Isichenko, and Nitesh Chauhan, Optica Quantum, December 2024 (14 pages).

[1279] Light Dark Matter Search with Nitrogen-Vacancy Centers in Diamonds, by So Chigusa, Kazunori Nakayama, et al., arXiv, March 2025 (7 pages).

[1280] Detection of hidden photon dark matter using the direct excitation of transmon qubits, by Shion Chen, Thanaporn Sichanugrist, et al., arXiv, November 2023 (7 pages).

[1281] Transmon qubit modeling and characterization for Dark Matter search, by R. Moretti, A. Giachero, et al., arXiv, December 2024 (23 pages).

[1282] High-precision robust monitoring of charge/discharge current over a wide dynamic range for electric vehicle batteries using diamond quantum sensors, by Yuji Hatano, Mutsuko Hatano, et al., Scientific Reports, September 2022.

[1283] A quantum sensing metrology for magnetic memories, by Vicent J. Borràs, Peter Rickhaus, et al., npj Spintronics, June 2024.

[1284] China unveils drone-mounted quantum device for submarine detection in South China Sea, by Stephen Chen, South China Morning Post, April 2025.

[1285] MAD-XR - Magnetic Anomaly Detector-Extended Role, by Ministère des Armées, Ministère des Armées, October 2024.

[1286] Scalar and Vector Airborne Platform Calibration Using Quantum and Classical Magnetometers and Inertial Sensors, by Antonia Hager, Torleiv H. Bryne, and Mia Jukić, arXiv, May 2026 (11 pages).

[1287] The impact of microwave phase noise on diamond quantum sensing, by Andris Berzins, Victor M. Acosta, et al., arXiv, October 2024 (8 pages).

[1288] Enhanced quantum magnetometry with a laser-written integrated photonic diamond chip, by Yanzhao Guo, Shane M. Eaton, et al., arXiv, February 2025 (9 pages).

[1289] Engineering Nanodiamonds for Quantum Sensing: Material Constraints at the Nanoscale, by Ashutosh Rathi, Keisuke Oshimi, Kento Sasaki, Kensuke Kobayashi, Yutaka Shikano, Oliver Benson, Tim Schröder, Shery L. Y. Chang, and Masazumi Fujiwara, arXiv, August 2026 (20 pages).

[1290] Picotesla magnetometry of microwave fields with diamond sensors, by Zhecheng Wang, Jiangfeng Du, et al., arXiv, August 2022 (7 pages).

[1291] Scanning gradiometry with a single spin quantum magnetometer, by W. S. Huxter, C. L. Degen, et al., Nature Communications, June 2022.

[1292] A Scalable Quantum Magnetometer in 65nm CMOS with Vector-Field Detection Capability, by Mohamed Ibrahim et al., March 2019 (51 slides).

[1293] Single-Spin Nitrogen-Vacancy Magnetometer with Enhanced Static Field Sensitivity, by Vinaya K. Kavatamane, Gopalakrishnan Balasubramanian, et al., arXiv, October 2025 (33 pages).

[1294] Optical properties of SiV and GeV color centers in nanodiamonds under hydrostatic pressures up to 180 GPa, by Baptiste Vindolet, Jean-François Roch, et al., arXiv, November 2022 (7 pages).

[1295] NV center magnetometry up to 130 GPa as if at ambient pressure, by Antoine Hilberer, Jean-François Roch, et al., arXiv, January 2023 (5 pages).

[1296] Diamond quantum sensing at record high pressure up to 240 GPa, by Qingtao Hao, Yanming Ma, et al., arXiv, October 2025 (16 pages).

[1297] Optical Stability and Photophysics of NV Centers in Diamond up to 120 GPa, by Kin On Ho, Jean-François Roch, et al., arXiv, June 2026 (7 pages).

[1298] Diamond-on-chip infrared absorption magnetic field camera, by Julian M. Bopp, Tim Schröder, et al., arXiv, December 2023 (14 pages).

[1299] Quantum magnetometry of transient signals with a time resolution of 1.1 nanoseconds, by Konstantin Herb, Christian L. Degen, et al., arXiv, November 2024 (11 pages).

[1300] NV Diamond Centers from Material to Applications, by Jean-François Roch, Collège de France, 2015 (52 slides).

[1301] Imaging nanomagnetism and magnetic phase transitions in atomically thin CrSBr, by Märta A. Tschudin, Patrick Maletinsky, et al., Nature Communications, July 2024.

[1302] Three-dimensional imaging of integrated-circuit activity using quantum defects in diamond, by Marwa Garsi, Jörg Wrachtrup, et al., arXiv, June 2024 (38 pages).

[1303] Widefield Diamond Quantum Sensing with Neuromorphic Vision Sensors, by Zhiyuan Du, November 2023 (12 pages).

[1304] High PDMR contrast in single NV centres and related photocurrent properties, by Michael Petrov, Boo Carmans, Josef Soucek, Akhil Kuriakose, Ottavia Jedrkiewicz, Emilie Bourgeois, and Milos Nesladek, arXiv, March 2026 (13 pages).

[1305] Real-Time Magnetic Field Sensing based on Microwave Frequency Modulated Photocurrent of Nitrogen-Vacancy Centers in Diamond, by Xuan-Ming Shen, Qilong Wu, Huihui Yu, Pei-Nan Ni, Qing Lou, Chao-Nan Lin, Xun Yang, Chong-Xin Shan, and Yuan Zhang, arXiv, February 2026 (14 pages).

[1306] Microelectronic readout of a diamond quantum sensor, by Daniel Wirtitsch, Michael Trupke, et al., arXiv, March 2024 (10 pages).

[1307] Massively multiplexed nanoscale magnetometry with diamond quantum sensors, by Kai-Hung Cheng, Nathalie P. de Leon, et al., arXiv, August 2024 (19 pages).

[1308] Magnetic-field-learning using a single electronic spin in diamond with one-photon-readout at room temperature, by Raffaele Santagati, Anthony Laing, et al., arXiv, July 2018 (18 pages).

[1309] Probing and imaging nanoscale magnetism with scanning magnetometers based on diamond quantum defects, 2016 (35 slides).

[1310] All-Optical Nuclear Quantum Sensing using Nitrogen-Vacancy Centers in Diamond, by Beat Bürgler, Patrick Maletinsky, et al., arXiv, December 2022 (6 pages).

[1311] Diamond-based optical vector magnetometer, by Charlie Oncebay Segura and Sérgio Ricardo Muniz, arXiv, September 2022 (13 pages).

[1312] Efficient and all-carbon electrical readout of a NV based quantum sensor, by Guillaume Villaret, Thierry Debuisschert, et al., arXiv, December 2022 (11 pages).

[1313] SQUIDs for detection of potential dark matter candidates, by Siddarth Sivakumar, Manan Agarwal, and Hannah Rana, arXiv, July 2024 (5 pages).

[1314] A Flux-Tunable cavity for Dark matter detection, by Fang Zhao, David I. Schuster, Aaron Chou, et al., arXiv, January 2025 (15 pages).

[1315] Quantum-enhanced dark matter detection using Schrödinger cat states, by Pan Zheng, Dapeng Yu, et al., arXiv, July 2025 (20 pages).

[1316] Superconducting Sensor Development in Support of the Superconducting Sensor Development in Support of the Search for the Neutron Electric Dipole Moment, by Robin Cantor, 2017 (17 slides).

[1317] Quantum sensing using circular Rydberg states, by Rémi Richaud, November 2018 (41 slides).

[1318] Rubidium vapors in high magnetic fields, by Stefano Scotto, November 2017 (168 pages).

[1319] Brief Review of Quantum Magnetometers, by Ivan Hrvoic et al., January 2009 (15 pages).

[1320] Atomic magnetometers and their application in industry, by Xuanyao Bai, June 2023 (20 pages).

[1321] Adaptive cold-atom magnetometry mitigating the trade-off between sensitivity and dynamic range, by Zhu Ma, Chaohong Lee, et al., arXiv, March 2025 (30 pages).

[1322] Scalable surface ion trap design for magnetic quantum sensing and gradiometry, by Qirat Iqbal and Altaf Hussain Nizamani, arXiv, April 2026 (6 pages).

[1323] Quantum Sensing of Magnetic Fields with Molecular Spins, by Claudio Bonizzoni, Alberto Ghirri, Fabio Santanni, and Marco Affronte, arXiv, November 2023 (11 pages).

[1324] Quantum Magnetometer with Dual-Coupling Optomechanics, by Gui-Lei Zhu, Jing Liu, Ying Wu, and Xin-You Lü, arXiv, September 2022 (7 pages).

[1325] Ultra-sensitive solid-state organic molecular microwave quantum receiver, by Bo Zhang, Jun Zhang, et al., arXiv, May 2024 (10 pages).

[1326] A quantum sensor for atomic-scale electric and magnetic fields, by Taner Esat, Ruslan Temirov, et al., Nature Nanotechnology, July 2024.

[1327] A single optically detectable tumbling spin in silicon, by Félix Cache, Yoann Baron, Baptiste Lefaucher, Jean-Baptiste Jager, Frédéric Mazen, Frédéric Milési, Sébastien Kerdilès, Isabelle Robert-Philip, Jean-Michel Gérard, Guillaume Cassabois, Vincent Jacques, and Anaïs Dréau, arXiv, January 2026 (6 pages).

[1328] Nanotube spin defects for omnidirectional magnetic field sensing, by Xingyu Gao, Tongcang Li, et al., Nature Communications, September 2024.

[1329] Non-radiative energy transfer between boron vacancies in hexagonal boron nitride and other 2D materials, by Fraunié Jules, Vincent Jacques, Cedric Robert, et al., arXiv, December 2025 (14 pages).

[1330] A single spin in hexagonal boron nitride for vectorial quantum magnetometry, by Carmem M. Gilardoni, Hannah L. Stern, et al., Nature Communications, May 2025 (9 pages).

[1331] Fiber-integrated silicon carbide silicon vacancy-based magnetometer, by Wei-Ke Quan, Lin Liu, Qin-Yue Luo, Xiao-Di Liu, and Jun-Feng Wang, arXiv, August 2022 (13 pages).

[1332] Quantum sensing with duplex qubits of silicon vacancy centers in SiC at room temperature, by Kosuke Tahara, Takeshi Ohshima, et al., arXiv, April 2025 (20 pages).

[1333] Demonstration Of A Quantum Magnetometer Chip Based On Proprietary And Scalable 4H-Silicon Carbide Technology, by P. A. Stuermer, Joerg Wrachtrup, et al., arXiv, January 2026 (8 pages).

[1334] Localization and coherent control of 25 nuclear spins in Silicon Carbide, by Pierre Kuna, Erik Hesselmeier-Hüttmann, Phillip Schillinger, Felix Gloistein, István Takács, Viktor Ivády, Wolfgang Knolle, Jawad Ul-Hassan, Jörg Wrachtrup, and Vadim Vorobyov, arXiv, December 2025 (25 pages).

[1335] Waveguide-integrated colour centres in silicon carbide with broadband photonic crystal reflectors for efficient readout, by Marcel Krumrein, Julian M. Bopp, Timo Steidl, Wolfgang Knolle, Jawad Ul-Hassan, Vadim Vorobyov, Tim Schröder, and Jörg Wrachtrup, arXiv, December 2025 (13 pages).

[1336] Nanoscale graphitization and defect evolution in silicon-vacancy center-containing nanodiamonds under high-pressure high-temperature annealing, by M. De Feudis, B. Yavkin, L. Henry, K.O. Ho, M.-P. Adam, P. Goldner, F. Benedic, S. Desgreniers, and J.-F. Roch, arXiv, August 2026 (12 pages).

[1337] Continuous drive heterodyne microwave sensing with spin qubits in hexagonal boron nitride, by Charlie J. Patrickson, Isaac J. Luxmoore, et al., arXiv, June 2024 (33 pages).

[1338] Hexagonal boron nitride based photonic quantum technologies, by Madhava Krishna Prasad, Ying-Lung Daniel Ho, et al., arXiv, July 2024 (20 pages).

[1339] Multi-species optically addressable spin defects in a van der Waals material, by Sam C. Scholten, Jean-Philippe Tetienne, et al., Nature Communications, August 2024.

[1340] A quantum coherent spin in hexagonal boron nitride at ambient conditions, by Hannah L. Stern, Mete Atatüre, et al., Nature Materials, May 2024.

[1341] Optically pumped magnetometers: From quantum origins to multi-channel magnetoencephalography, by Tim M. Tierney, 2019 (12 pages).

[1342] The Ivar Giæver Geomagnetic Laboratory, by IGGL, 2019.

[1343] Picotesla optically pumped magnetometer using a laser-written vapor cell with sub-mm cross section, by Andrea Zanoni et al., Journal of Applied Physics, October 2024 (7 pages).

[1344] Quantum Magnetometers for Industrial Applications, by IAF, April 2019.

[1345] Highly sensitive measurement of a megahertz rf electric field with a Rydberg-atom sensor, by Bang Liu, Bao-Sen Shi, et al., arXiv, July 2022 (6 pages).

[1346] Quantum-enhanced sensing of displacements and electric fields with two-dimensional trapped-ion crystals, by Kevin A. Gilmore, John J. Bollinger, et al., Science, August 2021 🔓 (preprint on arXiv).

[1347] Quantum sensing of oscillating electric fields with trapped ions, by Fabian Wolf et al., Measurement: Sensors, December 2021 (3 pages).

[1348] Electric Field Sensing via Rydberg Electromagnetically Induced Transparency Using Zeeman and Stark Effects, by Yu-Chi Chen, Shao-Cheng Fang, Hsuan-Jui Su, and Yi-Hsin Chen, arXiv, June 2025 (7 pages).

[1349] Quantum sensing of microwave electric fields based on Rydberg atoms, by Jinpeng Yuan, Suotang Jia, et al., arXiv, January 2024 (28 pages).

[1350] Sensing electric fields through Rydberg atom networks, by Philip Kitson, Wayne J. Chetcuti, Gerhard Birkl, Luigi Amico, and Juan Polo, arXiv, September 2025 (10 pages).

[1351] Quantum sensing of electric field distributions of liquid electrolytes with NV-centers in nanodiamonds, by M Hollendonner, September 2023 (8 pages).

[1352] High-resolution electric field imaging based on intermittent-contact mode scanning NV center electrometry, by Zhi Cheng, Zhiwei Yu, Mengqi Wang, Lingfeng Yang, Zihao Cui, Ya Wang, and Pengfei Wang, arXiv, September 2025 (11 pages).

[1353] Imaging of electrical signals in a quantum SiC microscope, by A. Suhana, T. A. U. Svetikova, C. Schneider, M. Helm, A. N. Anisimov, and G. V. Astakhov, arXiv, September 2025 (9 pages).

[1354] Quantum electrometry in a silicon carbide power device, by Yuichi Yamazaki, Takeshi Ohshima, et al., arXiv, March 2026 (19 pages).

[1355] High sensitivity measurement of ULF, VLF and LF fields with Rydberg-atom sensor, by Mingwei Lei and Meng Shi, arXiv, May 2024 (6 pages).

[1356] Doppler sensitivity and resonant tuning of Rydberg atom-based antennas, by Peter B. Weichman, arXiv, February 2024 (22 pages).

[1357] BT trials a new quantum radio to boost next-generation 5G & IoT Networks, by BT, May 2022.

[1358] Quantum sensing of weak radio-frequency signals by pulsed Mollow absorption spectroscopy, by T. Joas, A. M. Waeber, G. Braunbeck, and F. Reinhard, Nature Communications, October 2017.

[1359] An isotropic antenna based on Rydberg atoms, by Shaoxin Yuan, Suotang Jia, et al., arXiv, September 2023 (13 pages).

[1360] Assessment of Rydberg Atoms for Wideband Electric Field Sensing, by David H. Meyer, Zachary A. Castillo, Kevin C. Cox, and Paul D. Kunz, arXiv, January 2020 (16 pages).

[1361] Waveguide-coupled Rydberg spectrum analyzer from 0 to 20 GHz, by David H. Meyer, Paul D. Kunz, and Kevin C. Cox, arXiv, May 2021 (10 pages).

[1362] Doppler-enhanced superheterodyne Rydberg microwave receiver, by Yuwen Yin, Ruimin Chen, Shibing Ji, Jinlian Hu, Shaofeng Wang, Yunhui He, Jingxu Bai, Xiao-Qiang Shao, Yuechun Jiao, and Jianming Zhao, arXiv, June 2026 (6 pages).

[1363] Hybrid Six-Level Rydberg Atomic Quantum Receiver for Multi-Band Wireless Communications, by Lahiru Shyamal, Harini Hapuarachchi, Saman Atapattu, and Jared H. Cole, arXiv, July 2026 (14 pages).

[1364] Electrometry of extremely-low frequencies from kHz to sub-Hz with a Rydberg-atom sensor, by Aveek Chandra, Narongrit Paensin, and Rainer Dumke, arXiv, March 2026 (10 pages).

[1365] Sensing Low-Frequency Field with Rydberg Atoms via Quantum Weak Measurement, by Ding Wang, Shenchao Jin, Xiayang Fan, Hongjing Li, Jiatian Liu, Jingzheng Huang, Guihua Zeng, and Yuan Sun, arXiv, March 2026 (6 pages).

[1366] Multi-Shot Quantum Sensing for RF Signal Detection with MIMO Rydberg-Atom Receivers, by Saman Atapattu, Harini Hapuarachchi, and Nathan Ross, arXiv, March 2026 (8 pages).

[1367] Bridging gaps in Rydberg RF receivers using modulation transfer bandwidth enhancement, by Mickael Branco, K V Adwaith, Gabriel Boccara, Duc-Anh Trinh, Sacha Welinski, Perrine Berger, Fabienne Goldfarb, and Fabien Bretenaker, arXiv, May 2026 (11 pages).

[1368] Broadband Heterodyne Microwave Detection using Rydberg Atoms with High Sensitivity, by Hsuan-Jui Su, Shao-Cheng Fang, Ting-An Li, Chen-Hao Chang, Yu-Chi Chen, and Yi-Hsin Chen, arXiv, January 2026 (8 pages).

[1369] Complete three-dimensional vector polarimetry with a Rydberg atom rf electrometer, by Peter K. Elgee, Kevin C. Cox, Joshua C. Hill, Paul D. Kunz, and David H. Meyer, arXiv, July 2024 (10 pages).

[1370] High-precision measurement of microwave electric field by cavity-enhanced critical behavior in a many-body Rydberg atomic system, by Qinxia Wang, Tiancai Zhang, et al., arXiv, March 2025 (5 pages).

[1371] Cavity-Enhanced Rydberg Atomic Superheterodyne Receiver, by Yukang Liang, Tiancai Zhang, et al., arXiv, February 2025 (7 pages).

[1372] Rydberg Atomic Quantum Receivers for Classical Wireless Communications and Sensing: Their Models and Performance, by Tierui Gong, Lajos Hanzo, et al., arXiv, May 2025 (16 pages).

[1373] Satellite Signal Detection via Rydberg-Atom Receiver, by Mignwei Lei, Jianquan Zhang, Qun Luo, Zhentao Zhang, Ming Wang, and Meng Shi, arXiv, June 2025 (8 pages).

[1374] Rydberg Receivers for Space Applications, by Gianluca Allinson, Sylvain Schwartz, Aaron Strangfeld, et al., arXiv, January 2026 (72 pages).

[1375] Power sensitivity of broadband radiofrequency detectors based on quantum diamond spins, by Nicholas Gillespie, Christopher T.-K. Lew, Ryan Kinsella, Andy Sayers, Brant Gibson, David A. Broadway, and Jean-Philippe Tetienne, arXiv, May 2026 (14 pages).

[1376] Using NV centers in diamond to detect DC to very-low frequency magnetic fields, by Valts Krumins, Ivars Krastins, Oskars Rudzitis, Reinis Lazda, Florian Gahbauer, and Marcis Auzinsh, arXiv, December 2025 (8 pages).

[1377] Efficient Detection of Statistical RF Fields at High Magnetic Field with a Quantum Sensor, by Rouven Maier, Jörg Wrachtrup, et al., arXiv, June 2025 (21 pages).

[1378] Sensing of Arbitrary-Frequency Fields Using a Quantum Mixer, by Guoqing Wang et al., Physical Review X, June 2022.

[1379] High-resolution, Wide-frequency-range Magnetic Spectroscopy with Solid-state Spin Ensembles, by Zechuan Yin, Justin J. Welter, Connor A. Hart, Paul V. Petruzzi, and Ronald L. Walsworth, arXiv, December 2024 (9 pages).

[1380] Efficient Radiofrequency Sensing with Fluorescence Encoding, by Nicole Voce and Paul Stevenson, arXiv, October 2025 (11 pages).

[1381] Terahertz quantum sensing, by Mirco Kutas, March 2020 (8 pages).

[1382] A Quantum Optical Microphone in the Audio Band, by Raphael Nold, Jörg Wrachtrup, et al., arXiv, April 2022 (8 pages).

[1383] Long-Lived Mechanically-Detected Molecular Spins for Quantum Sensing, by Sahand Tabatabaei, Pritam Priyadarsi, Daniel Tay, Namanish Singh, Pardis Sahafi,

Andrew Jordan, and Raffi Budakian, arXiv, July 2026 (15 pages).

[1384] Quantum Antennas, by Gregory Ya. Slepyan, Svetlana Vlasenko, and Dmitri Mogilevtsev, arXiv, June 2022 (70 pages).

[1385] Generating tunable terahertz radiation with a novel quantum dot photoconductive antenna, by Andrei Gorodetsky, Ksenia A. Fedorova, Natalia Bazieva, and Edik U. Rafailov, 2016 🔓.

[1386] RF Spectrum Analyzer for Pulsed Signals: Ultra-Wide Instantaneous Bandwidth, High Sensitivity, and High Time-Resolution, by Perrine Berger, Thierry Chanelière, Daniel Dolfi, Loïc Morvan, et al., Journal of Lightwave Technology, May 2016 (6 pages) 🔓.

[1387] High-Frequency Gravitational Wave Detection with Superconducting Qubits, by Heechan Yi, Seong Chan Park, Kyoungchul Kong, and Myeonghun Park, arXiv, August 2026 (21 pages).

[1388] Quantum Radio Frequency Sensing, by William Clark, Q2B Santa Clara, December 2023 (14 slides).

[1389] A quantum radio frequency signal analyzer based on nitrogen vacancy centers in diamond, by Simone Magaletti, Ludovic Mayer, Jean-François Roch, and Thierry Debuisschert, Communications Engineering, July 2022.

[1390] A vapor-cell atomic sensor for radio-frequency field detection using a polarization-selective field enhancement resonator, by D. A. Anderson et al., Applied Physics Letters, October 2018 (11 pages) 🔓 (preprint on arXiv).

[1391] Quantum Imaging with X-rays, by Justin C. Goodrich, Sean McSweeney, et al., arXiv, December 2024 (12 pages).

[1392] Advances in quantum imaging, by Hugo Defienne, Warwick P. Bowen, Maria Chekhova, Gabriela Barreto Lemos, Dan Oron, Sven Ramelow, Nicolas Treps, and Daniele Faccio, arXiv, November 2024 (18 pages).

[1393] High resolution quantum enhanced phase imaging of cells, by Alberto Paniate, Giuseppe Ortolano, Sarika Soman, Marco Genovese, and Ivano Ruo Berchera, arXiv, June 2025 (13 pages).

[1394] Quantum Optical Techniques for Biomedical Imaging, by Vahid Salari, Christoph Simon, Daniel Oblak, et al., arXiv, November 2025 (20 pages).

[1395] Four Generations of Quantum Biomedical Sensors, by Xin Jin, Priyam Srivastava, Ronghe Wang, Yuqing Li, Jonathan Beaumariage, Tom Purdy, M. V. Gurudev Dutt, Kang Kim, Kaushik Seshadreesan, and Junyu Liu, arXiv, April 2026 (22 pages).

[1396] Quantum Sensing MRI for Noninvasive Detection of Neuronal Electrical Activity in Human Brains, by Yongxian Qian, Fernando E. Boada, et al., arXiv, March 2026 (26 pages).

[1397] 2024 Roadmap on Magnetic Microscopy Techniques and Their Applications in Materials Science, by D. V. Christensen, M. Poggio, et al., arXiv, January 2024 (111 pages).

[1398] Quantum sensors for biomedical applications, by Nabeel Aslam, Hongkun Park, et al., Nature Reviews Physics, February 2023.

[1399] Investigation of Widefield NV-Center Magnetic Imaging for Non-Destructive Materials Testing, by Niklas Mathesa, Marvin Feuerhelm, Simon Philipp, Ivan Soldatov, Philipp DÁstolfo, Peter Knittel, Thomas Straubb, Jan Jeske, Rüdiger Quay, and Xavier Vidal, arXiv, September 2026 (15 pages).

[1400] Magnetometry of neurons using a superconducting qubit, by Hiraku Toida, Shiro Saito, et al., arXiv, June 2022 (6 pages).

[1401] Search for Dark Photons with Superconducting Radio Frequency Cavities, by A. Romanenko, Physical Review Letters, June 2023.

[1402] A 64-pixel mid-infrared single-photon imager based on superconducting nanowire detectors, by Benedikt Hampel, Richard P. Mirin, Sae Woo Nam, and Varun B. Verma, arXiv, September 2023 (7 pages).

[1403] From Pixels to Camera: Scaling Superconducting Nanowire Single-Photon Detectors for Imaging at the Quantum-Limit, by Jun Gao, Ali W. Elshaari, et al., arXiv, May 2025 (13 pages).

[1404] A compact multi-pixel superconducting nanowire single-photon detector array supporting gigabit space-to-ground communications, by Hao Hao, Qing-Yuan Zhao, Yang-Hui Huang, Jie Deng, Fan Yang, Sai-Ying Ru, Zhen Liu, Chao Wan, Hao Liu, Zhi-Jian Li, Hua-Bing Wang, Xue-Cou Tu, La-Bao Zhang, Xiao-Qing Jia, Xing-Long Wu, Jian Chen, Lin Kang, and Pei-Heng Wu, Light: Science & Applications, January 2024.

[1405] Arrays of single photon detectors for quantum optics, by Valery Zwiller, Quantum Sensing and Nano Electronics and Photonics, March 2025.

[1406] A superconducting-nanowire single-photon camera with 400,000 pixels, by Bakhrom G. Oripov, Adam N. McCaughan, et al., arXiv, June 2023 (19 pages).

[1407] Fast biological imaging with quantum-enhanced Raman microscopy, by Alex Terrasson, W. P. Bowen, et al., arXiv, March 2024 (14 pages).

[1408] Design of a quantum diamond microscope with efficient scanning confocal readout, by Daniel G. Ang, Jiashen Tang, and Ronald L. Walsworth, arXiv, March 2025 (13 pages).

[1409] Prospects for Ultralow-Mass Nuclear Magnetic Resonance using Spin Defects in Hexagonal Boron Nitride, by Declan M. Daly, Ronald L. Walsworth, et al., arXiv, May 2025 (25 pages).

[1410] Probing Vortex Dynamics in 2D Superconductors with Scanning Quantum Microscope, by Sreehari Jayaram, Jörg Wrachtrup, et al., arXiv, May 2025 (7 pages).

[1411] Quantum Imaging of Photonic Spin Texture in an OAM Beam with NV Centers in Diamond, by Shoaib Mahmud, Wei Zhang, Farid Kalhor, Pronoy Das, and Zubin Jacob, arXiv, February 2025 (16 pages).

[1412] Quantum Sensors for Chemistry and Materials Science, by Piotr Put, Arjun Pillai, Xuan Hoang Le, Mikhail D. Lukin, and Hongkun Park, arXiv, July 2026 (22 pages).

[1413] Kernel Flux: a whole-head 432-magnetometer optically-pumped magnetoencephalography (OP-MEG) system for brain activity imaging during natural human experiences, by Ethan J. Pratt et al., Optical and Quantum Sensing and Precision Metrology, November 2021 (18 pages).

[1414] Quantum microscopy of cells at the Heisenberg limit, by Zhe He, Yide Zhang, Xin Tong, Lei Li, and Lihong V. Wang, Nature Communications, April 2023.

[1415] Experimental realization of scanning quantum microscopy, by V. F. Gili, F. Setzpfandt, et al., arXiv, January 2025 (13 pages).

[1416] Large baseline quantum telescopes assisted by partially distinguishable photons, by Subhrajit Modak and Pieter Kok, arXiv, December 2024 (9 pages).

[1417] Superresolution imaging with entanglement-enhanced telescopy, by Isack Padilla, Aqil Sajjad, Babak N. Saif, and Saikat Guha, arXiv, April 2025 (6 pages).

[1418] Progress in quantum telescopes, by David R. Gozzard, Fiona H. Panther, and Andrew G. White, arXiv, September 2026 (23 pages).

[1419] Super-resolution imaging based on active optical intensity interferometry, by Lu-Chuan Liu, Jian-Wei Pan, et al., arXiv, April 2024 (42 pages).

[1420] Super-Resolution Imaging with Multiparameter Quantum Metrology in Passive Remote Sensing, by Emre Köse and Daniel Braun, arXiv, January 2023 (12 pages).

[1421] An Entanglement Enhanced Microscope, by Takafumi Ono et al., arXiv, January 2014 (8 pages).

[1422] Practical Quantum Sensing with Thermal Light, by Peng Kian Tan, Xi Jie Yeo, Alvin Zhen Wei Leow, Lijiong Shen, and Christian Kurtsiefer, arXiv, March 2023 (5 pages).

[1423] Quantum correlation light-field microscope with extreme depth of field, by Yingwen Zhang et al., arXiv, March 2023 (16 pages).

[1424] Single-photon computational 3D imaging at 45 km, by Zheng-Ping Li, Jian-Wei Pan, et al., arXiv, April 2019 (22 pages).

[1425] Quantum dot-enabled infrared hyperspectral imaging with single-pixel detection, by Heyan Meng et al., Light: Science & Applications, May 2024.

[1426] Very long wave infrared quantum dot photodetector up to 18 μm, by Xiaomeng Xue, Menglu Chen, et al., Light: Science & Applications, April 2024.

[1427] Giant Magnetoresistance: Basic Concepts, Microstructure, Magnetic Interactions and Applications, by Inga Ennen, 2016 (24 pages).

[1428] Roadmap on Nanoscale Magnetic Resonance Imaging, by Raffi Budakian, Erik Gauger, et al., arXiv, December 2023 (81 pages).

[1429] Open-Path Detection of Organic Vapors via Quantum Infrared Spectroscopy, by Simon Neves, Adimulya Kartiyasa, Shayantani Ghosh, Geoffrey Gaulier, Luca La Volpe, and Jean-Pierre Wolf, arXiv, May 2024 (8 pages).

[1430] Submerged single-photon LiDAR imaging sensor used for real-time 3D scene reconstruction in scattering underwater environments, by Aurora Maccarone, 2023 (19 pages).

[1431] Spin Squeezing in Electron Microscopy, by Shiran Even-Haim, Ido Kaminer, et al., arXiv, July 2025 (21 pages).

[1432] Free-electron-light interactions in nanophotonics, by Charles Roques-Carmes, Marin Soljačić, et al., arXiv, August 2022 (34 pages).

[1433] A general framework for scintillation in nanophotonics, by Charles Roques-Carmes, Marin Soljačić, et al., arXiv, October 2021 (14 pages).

[1434] Harnessing quantum light for microscopic biomechanical imaging of cells and tissues, by Tian Li, Marlan O. Scully, et al., arXiv, August 2024 (14 pages).

[1435] Quantum Diamond Microscopy for Non-Destructive Failure Analysis of an Integrated Fan-Out Package-on-Package iPhone Chip, by Bartu Bisgin, Marwa Garsi, Andreas Welscher, Michael Hanke, and Fleming Bruckmaier, arXiv, December 2025 (12 pages).

[1436] Improving the Energy and Angular Resolutions of X-ray Telescopes with Nitrogen-Vacancy Centers in Diamond, by Ephraim Gau, Zhongyuan Liu, Henric Krawczynski, and Chong Zu, arXiv, November 2025 (15 pages).

[1437] Advances in nano- and microscale NMR spectroscopy using diamond quantum sensors, by Robin D. Allert, May 2022 (42 pages).

[1438] Quantum Diamond Microscope for Narrowband Magnetic Imaging with High Spatial and Spectral Resolution, by Zechuan Yin, Ronald L. Walsworth, et al., arXiv, October 2024 (16 pages).

[1439] Diamond Micro-Chip for Quantum Microscopy, by Shahidul Asif, Mark J.H. Ku, et al., arXiv, March 2024 (45 pages).

[1440] Quantum Frequency Mixing using an N-V Diamond Microscope, by Samuel J. Karlson, Danielle A. Braje, et al., arXiv, December 2024 (8 pages).

[1441] Quantum-Enhanced Diamond Molecular Tension Microscopy for Quantifying Cellular Forces, by Feng Xu, Zhiqin Chu, et al., arXiv, June 2023 (51 pages).

[1442] Microwave device characterisation using a widefield diamond microscope, by Andrew Horsley, Philipp Treutlein, et al., arXiv, October 2018 (10 pages).

[1443] Imaging the Meissner Effect and Flux Trapping of Superconductors under High Pressure using N-V Centers, by Cassandra Dailledouze, Antoine Hilberer, Martin Schmidt, Marie-Pierre Adam, Loïc Toraille, Kin On Ho, Anne Forget, Dorothée Colson, Paul Loubeyre, and Jean-François Roch, arXiv, January 2025 (10 pages).

[1444] A fluorescent nanodiamond foundation for quantum sensing in cells, by Simon Robert Hemelaar, 2018 (147 pages).

[1445] Diamond magnetic microscopy of malarial hemozoin nanocrystals, by Ilja Fescenko, September 2018 (17 pages).

[1446] Nanodiamonds enable adaptive-optics enhanced, super-resolution, two-photon excitation microscopy, by Graeme E. Johnstone et al., Royal Society of Open Science, July 2019 (7 pages).

[1447] Quantum Diamond Microscope for Dynamic Imaging of Magnetic Fields, by Jiashen Tang, Ronald L. Walsworth, et al., arXiv, September 2023 (18 pages).

[1448] Toward a CMOS-integrated quantum diamond biosensor based on NV centers, by Ioannis Varveris, Gianni D. Aliberti, Felix J. Barzilaij, Zhi Jin, Samantha A. van Rijs, Qiangrui Dong, Daan Brinks, Salahuddin Nur, and Ryoichi Ishihara, arXiv, February 2026 (19 pages).

[1449] High-resolution wide-field magnetic imaging with sparse sampling using nitrogen-vacancy centers, by Keqing Liu, Jiazhao Tian, Bokun Duan, Hao Zhang, Kangze Li, Guofeng Zhang, Fedor Jelezko, Ressa S. Said, Jianming Cai, and Liantuan Xiao, arXiv, January 2026 (15 pages).

[1450] Magnetic Relaxometry of Methemoglobin by Widefield Nitrogen-Vacancy Microscopy, by Suvechhya Lamichhane, Abdelghani Laraoui, et al., arXiv, October 2024 (13 pages).

[1451] Diamond-on-chip magnetic field camera for mobile imaging, by Julian M. Bopp, Physical Review Applied, March 2025.

[1452] Enhanced widefield quantum sensing with nitrogen-vacancy ensembles using diamond nanopillar arrays, by D. J. McCloskey, D. A. Simpson, et al., arXiv, February 2019 (7 pages).

[1453] Optical magnetic imaging of living cells, by Le Sage et al., Nature, 2013 (11 pages).

[1454] Principles and Techniques of the Quantum Diamond Microscope, by Edlyn V. Levine, Ronald L. Walsworth, et al., arXiv, September 2019 (47 pages).

[1455] Atomic Scale Magnetic Sensing and Imaging Based on Diamond NV Centers, by Myeongwon Lee, 2019 (17 pages).

[1456] Human Cardiac Measurements with Diamond Magnetometers, by Muhib Omar, Joerg Wrachtrup, Arne Wickenbrock, et al., arXiv, January 2026 (21 pages).

[1457] Millimetre-scale magnetocardiography of living rats with thoracotomy, by Keigo Arai, Takayuki Iwasaki, et al., Communications Physics, August 2022.

[1458] Sub-Sm–1 electromagnetic induction imaging with an unshielded atomic magnetometer, by Cameron Deans, Luca Marmugi, and Ferruccio Renzoni, Applied Physics Letters, March 2020 (preprint on arXiv).

[1459] A robust scanning diamond sensor for nanoscale imaging with single nitrogen-vacancy centres, by P. Maletinsky, A. Yacoby, et al., Nature Nanotechnology, April 2012 (preprint on arXiv).

[1460] Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology, by Romana Schirhagl, Kevin Chang, Michael Loretz, and Christian L. Degen, Annual Review on Physics Chemistry, April 2014 (27 pages) (preprint on ResearchGate).

[1461] Quantum sensing and imaging with spin defects in hexagonal boron nitride, by Sumukh Vaidya, Tongcang Li, et al., arXiv, April 2023 (21 pages).

[1462] Quantum sensing with a spin ensemble in a two-dimensional material, by Souvik Biswas, Jelena Vučković, Joonhee Choi, et al., arXiv, September 2025 (25 pages).

[1463] Optical magnetometry, by Dmitry Budker and Michael Romalis, Nature Physics, April 2007 (preprint on arXiv).

[1464] Optically pumped magnetometers: From quantum origins to multi-channel magnetoencephalography, by Tim M. Tierney, 2019 (11 pages).

[1465] Optically Pumped Magnetometer Measuring Fatigue-Induced Damage in Steel, by Peter A. Koss, 2022 (11 pages).

[1466] Improved spatio-temporal measurements of visually evoked fields using optically-pumped magnetometers, by Aikaterini Gialopsou, Peter Krüger, et al., Scientific Reports, November 2021.

[1467] Four-channel optically pumped atomic magnetometer for magnetoencephalography, by Anthony P. Colombo, 2016 (15 pages).

[1468] An optically pumped magnetic gradiometer for the detection of human biomagnetism, by Harry Cook, Anna U Kowalczyk, et al., Quantum Science and Technology, April 2024.

[1469] Quantum-enhanced biosensing enables earlier detection of bacterial growth, by Rayssa B. de Andrade, Anne Egholm Høgh, Gaetana Spedalieri, Stefano Pirandola, Kirstine Berg-Sørensen, Tobias Gehring, and Ulrik L. Andersen, arXiv, December 2025 (12 pages).

[1470] Quantum Squeezing Enhanced Photothermal Microscopy, by Pengcheng Fu, Xiao Liu, Siming Wang, Nan Li, Chenran Xu, Han Cai, Huizhu Hu, Vladislav V. Yakovlev, Xu Liu, Shi-Yao Zhu, Xingqi Xu, Delong Zhang, and Da-Wei Wang, arXiv, January 2026 (34 pages).

[1471] Optical imaging by means of two-photon quantum entanglement, by T. B. Pittman et al., Physical Review A, November 1995 🔒.

[1472] Observation of Two-Photon "Ghost" Interference and Diffraction, by D. V. Strekalov, Physical Review Letters, May 1995 🔒.

[1473] An introduction to ghost imaging: quantum and classical, by Miles Padgett et al., 2016 (10 pages).

[1474] Quantum Ghost Image Identification with Correlated Photon Pairs, by Mehul Malik, Robert W. Boyd, et al., Physical Review Letters, April 2010 🔒.

[1475] The Dawn of Quantum Biophotonics, by Dmitri Voronine, 2016 (30 pages).

[1476] Ghost imaging with zero photons, by Meixue Chen, Yiqi Song, Yu Gu, Huafan Zhang, Huaibin Zheng, Yuchen He, Hui Chen, Yu Zhou, Fuli Li, Zhuo Xu, and Jianbin Liu, arXiv, April 2026 (6 pages).

[1477] Ghost Imaging with Free Electron-Photon Pairs, by Sergei Bogdanov, Philipp Haslinger, et al., arXiv, September 2025 (10 pages).

[1478] Fast full-color computational imaging with single-pixel detectors, by Stephen Welsh, 2013 (7 pages).

[1479] 3D Computational Imaging with Single-Pixel Detectors, by B. Sun et al., Science, May 2013 (4 pages) 🔒.

[1480] Imaging with a small number of photons, by Peter A. Morris, Reuben S. Aspden, Jessica Bell, Robert W. Boyd, and Miles J. Padgett, arXiv, August 2014 (9 pages).

[1481] Quantum-inspired computational imaging, by Yoann Altmann et al., Science, 2019 (9 pages).

[1482] Microwave quantum illumination using a digital receiver, by S. Barzanjeh, S. Pirandola, D. Vitali, and J. M. Fink, arXiv, January 2020 (12 pages).

[1483] Quantum optical induced-coherence tomography by a hybrid interferometer, by Eun Mi Kim et al., December 2023 (10 pages).

[1484] Polarization entanglement-enabled quantum holography, by Hugo Defienne, Bienvenu Ndagano, Ashley Lyons, and Daniele Faccio, arXiv, January 2021 (31 pages).

[1485] Quantum imaging with undetected photons, by Gabriela Barreto Lemos, Anton Zeilinger, et al., Nature, August 2014 🔒 (preprint on arXiv).

[1486] Terahertz Quantum Imaging, by Mirco Kutas, Felix Riexinger, Jens Klier, Daniel Molter, and Georg von Freymann, arXiv, August 2024 (20 pages).

[1487] An introduction to ghost imaging, by Miles John Padgett et al., 2017 (11 pages).

[1488] Quantum imaging exploiting twisted photon pairs, by Dianzhen Cui, X. X. Yi, and Li-Ping Yang, arXiv, January 2023 (7 pages).

[1489] The Future of Quantum Sensing & Communications, by Marco Lanzagorta of the US Naval Research Laboratory, September 2018.

[1490] Near Infrared Quantum Ghost Spectroscopy for Threats Detection, by Andrea Chiuri, Federico Angelini, Ilaria Gianani, Simone Santoro, and Marco Barbieri, arXiv, September 2024 (20 pages).

[1491] High quality 1 mT MRI, by Dimitri Labat Zineb Belkacemi et al., Chipiron, March 2025 (35 pages).

[1492] Performance Analysis of Optically Pumped 4He Magnetometers vs. Conventional SQUIDs: From Adult to Infant Head Models, by Saeed Zahran et al., Sensors, April 2022 (18 pages).

[1493] Helium-4 magnetometers for room-temperature biomedical imaging: toward collective operation and photon-noise limited sensitivity, by William Fourcault, May 2021 (9 pages).

[1494] Observing quantum coherence from photons scattered in free-space, by Shihan Sajeed and Thomas Jennewein, arXiv, February 2021 (5 pages).

[1495] Crosstalk-mitigated microelectronic control for optically-active spins, by Hao-Cheng Weng, John G. Rarity, Krishna C. Balram, and Joe A. Smith, arXiv, July 2025 (11 pages).

[1496] Heterogeneous Integration of Solid-State Quantum Systems with a Foundry Photonics Platform, by Hao-Cheng Weng, August 2023 (8 pages).

[1497] Robotic Vectorial Field Alignment for Spin-Based Quantum Sensors, by Joe A. Smith, November 2023 (10 pages).

[1498] Who Let the Diamonds Out?, by Vincent Halde, David Roy-Guay, et al., arXiv, September 2025 (8 pages).

[1499] 113 km absolute ranging with nanometer precision, by Yan-Wei Chen, Jian-Wei Pan, et al., arXiv, December 2024 (21 pages).

[1500] Secure quantum ranging, by Yunkai Wang, Graeme Smith, and Alex May, arXiv, May 2025 (21 pages).

[1501] Quantum-optical sensing and target detection, by Guo Yao Tham, arXiv, October 2024 (156 pages).

[1502] Lesson learnt from the rise and fall of quantum radar research, by Gapare Galati et al., Academia Quantum, March 2025.

[1503] Quantum Computing for Partition Function Estimation of a Markov Random Field in a Radar Anomaly Detection Problem, by Timothe Presles, Cyrille Enderli, Gilles Burel, and El Houssain Baghious, arXiv, January 2025 (6 pages).

[1504] Quantum Information Processing, Sensing and Communications: Their Myths, Realities and Futures, by Lajos Hanzo, Osvaldo Simeone, et al., arXiv, December 2024 (52 pages).

[1505] Quantum Radar, by Marco Lanzagorta, 2012 (141 pages).

[1506] A Study on Quantum Radar Technology Developments and Design Consideration for its integration, by Manoj Mathews, arXiv, May 2022 (8 pages).

[1507] Quantum illumination networks, by Xiaobin Zhao, Zheshen Zhang, and Quntao Zhuang, arXiv, June 2024 (29 pages).

[1508] Quantum Illumination Advantage for Classification Among an Arbitrary Library of Targets, by Ali Cox, Quntao Zhuang, Jeffrey H. Shapiro, and Saikat Guha, arXiv, August 2024 (6 pages).

[1509] Quantum illumination networks, by Xiaobin Zhao, Zheshen Zhang, and Quntao Zhuang, Communications Physics, February 2025 🔒 (preprint on arXiv).

[1510] Gaussian beam quantum radar protocol, by Lorenzo Maccone, Yi Zheng, and Changliang Ren, arXiv, September 2023 (6 pages).

[1511] Entanglement-assisted multi-aperture pulse-compression radar for angle resolving detection, by Bo-Han Wu, Saikat Guha, and Quntao Zhuang, arXiv, July 2022 (18 pages).

[1512] Restoring Quantum Superiority of Noisy Quantum Illumination, by Wei Wu and Jun-Hong An, arXiv, October 2025 (7 pages).

[1513] Microwave quantum illumination using a digital receiver, by S. Barzanjeh, S. Pirandola, D. Vitali, and J. M. Fink, Science, May 2020.

[1514] Quantum advantage in microwave quantum radar, by R. Assouly, R. Dassonneville, T. Peronnin, A. Bienfait, and B. Huard, Nature Physics, June 2023 (preprint on HAL).

[1515] An Imaging Radar Using a Rydberg Atom Receiver, by William J. Watterson, Matthew T. Simons, et al., arXiv, June 2025 (6 pages).

[1516] Can quantum mechanics improve radar technology?, by Giacomo Sorelli et al., November 2020.

[1517] Quantum Flashlight Pierces the Darkness With a Few Percent as Many Photons, by Adrian Cho, 2020.

[1518] Focus: Quantum Mechanics Could Improve Radar, by Physics, February 2015.

[1519] Microwave Quantum Illumination, by Shabir Barzanjeh, Saikat Guha, Christian Weedbrook, David Vitali, Jeffrey H. Shapiro, and Stefano Pirandola, arXiv, February 2015 (5 pages).

[1520] Enhanced Sensitivity of Photodetection via Quantum Illumination, by Seth Lloyd, 2018 (4 pages).

[1521] Digital twins for compact hybrid quantum classical learning in FMCW radar detection, by Sebastian Ratto Valderrama, Ahmed N. Sayed, Arien Sligar, Jose R. Rosas-Bustos, Omar M. Ramahi, and George Shaker, arXiv, May 2026 (12 pages).

[1522] Rydberg Atomic RF Sensor-based Quantum Radar, by Sourav Banerjee and Neel Kanth Kundu, arXiv, January 2026 (5 pages).

[1523] China's claim of developing "quantum radar" for detecting stealth planes: beyond skepticism, by Ashish Gupta, 2016 (4 pages).

[1524] The US and China are in a quantum arms race that will transform warfare, by Martin Giles, January 2019.

[1525] Quantum illumination via frequency-mode-based correlation-to-displacement conversion, by Xin Chen and Zhibin Ye, arXiv, February 2025 (11 pages).

[1526] Quantum radar will expose stealth aircraft, by Waterloo University, April 2018.

[1527] Long-Range Entangled Quantum Noise Radar Over Order of Kilometer, by H. Allahverdi and Ali Motazedifard, arXiv, December 2024 (21 pages).

[1528] Advances in Quantum Radar and Quantum LiDAR, by Ricardo Gallego Torrome and Shabir Barzanjeh, arXiv, October 2023 (19 pages).

[1529] Engineering Constraints and Application Regimes of Quantum Radar, by Florian Bischeltsrieder et al., IEEE, January 2025 (18 pages).

[1530] Quantum illumination advantage in quantum Doppler radar, by Rongyu Wei, Francesco Albarelli, Jun Li, and Vittorio Giovannetti, arXiv, November 2024 (14 pages).

[1531] Quantum radar with unreflected photons, by T.J. Volkoff, arXiv, August 2024 (9 pages).

[1532] Revealing spoofing of quantum illumination using entanglement, by Jonathan N. Blakely, Shawn D. Pethel, Kenneth R. Stewart, and Kurt Jacobs, arXiv, October 2024 (23 pages).

[1533] Quantum-enhanced Doppler lidar, by Maximilian Reichert, Roberto Di Candia, Moe Z. Win, and Mikel Sanz, arXiv, December 2022 (28 pages).

[1534] Detecting a target with quantum entanglement, by Giacomo Sorelli, Nicolas Treps, Frederic Grosshans, and Fabrice Boust, arXiv, July 2021 (24 pages).

[1535] The short weird life—and potential afterlife—of quantum radar, by Adrian Cho, Science, September 2020.

[1536] Quantum Illumination and Quantum Radar: A Brief Overview, by Athena Karsa, Alasdair Fletcher, Gaetana Spedalieri, and Stefano Pirandola, arXiv, July 2024 (14 pages).

[1537] On Target Detection by Quantum Radar (Preprint), by Gaspare Galati and Gabriele Pavan, arXiv, February 2024 (12 pages).

[1538] Range Limitations in Microwave Quantum Radar, by Gabriele Pavan et al., Remote Sensing, July 2024.

[1539] Synthetic Aperture Radar Image Segmentation with Quantum Annealing, by Timothe Presles, Cyrille Enderli, Gilles Burel, and El Houssain Baghious, arXiv, January 2024 (15 pages).

[1540] Revealing spoofing of classical radar using quantum noise, by Jonathan N. Blakely, Shawn D. Pethel, and Kurt Jacobs, arXiv, July 2023 (24 pages).

[1541] Super-resolution and super-sensitivity of quantum LiDAR with multi-photonic state and binary outcome photon counting measurement, by Priyanka Sharma, Manoj K. Mishra, and Devendra Kumar Mishra, arXiv, April 2024 (20 pages).

[1542] Heisenberg-Limited Quantum Lidar for Joint Range and Velocity Estimation, by Maximilian Reichert, Quntao Zhuang, and Mikel Sanz, arXiv, January 2025 (21 pages).

[1543] Spoofing resilience for simple-detection quantum illumination LIDAR, by Richard J. Murchie and John Jeffers, arXiv, October 2025 (23 pages).

[1544] Heisenberg-Limited Quantum Lidar for Joint Range and Velocity Estimation, by Maximilian Reichert, Physical Review Letters, September 2024 (preprint on hdl.handle.net).

[1545] Quantum Lidar - Remote Sensing at the Ultimate Limit, by Jonathan Dowling, 2009 (97 pages).

[1546] Two-photon interference LiDAR imaging, by Robbie Murray et al., 2022 (7 pages).

[1547] Analysis of Observation Performance of a Mobile Coherent Doppler Wind Lidar Using DBS Scanning Mode, by Debao Dong, 2020 (7 pages).

[1548] Quantum Target Ranging for LiDAR, by Giuseppe Ortolano and Ivano Ruo-Berchera, arXiv, August 2024 (11 pages).

[1549] Experimental Demonstration of Turbulence-resistant Lidar via Quantum Entanglement, by Binod Joshi, Michael M. Fitelson, and Yanhua Shih, arXiv, May 2024 (5 pages).

[1550] Single Photon LiDAR, by Feihu Xu, ITU, June 2019 (25 slides).

[1551] Quantum LiDAR with Frequency Modulated Continuous Wave, by Ming-Da Huang, Zhan-Feng Jiang, Hong-Yi Chen, Ying Zuo, Xiao-Peng Hu, Hai-Dong Yuan, Li-Jian Zhang, and Qi Qin, arXiv, July 2023 (29 pages).

[1552] Quantum secured LiDAR with Gaussian modulated coherent states, by Dong Wang, Juan-Ying Zhao, Ya-Chao Wang, Liang-Jiang Zhou, and Yi-Bo Zhao, arXiv, August 2023 (10 pages).

[1553] Semantic Temporal Single-photon LiDAR, by Fang Li, Tonglin Mu, Shuling Li, Junran Guo, Keyuan Li, Jianing Li, Ziyang Luo, Xiaodong Fan, Ye Chen, Yunfeng Liu, Hong Cai, Lip Ket Chin, Jinbei Zhang, and Shihai Sun, arXiv, December 2025 (14 pages).

[1554] Quantum-enhanced Doppler lidar, by Maximilian Reichert, Roberto Di Candia, Moe Z. Win, and Mikel Sanz, npj Quantum Information, December 2022.

[1555] Compact All-Fiber Quantum-Inspired LiDAR with > 100dB Noise Rejection and Single Photon Sensitivity, by Han Liu, Changhao Qin, Georgios Papangelakis, Meng Lon Iu, and Amr S Helmy, arXiv, August 2023 (10 pages).

[1556] Quantum LiDAR with non-local modulation, by Xiao-Dong Fan, Qiang Zhou, et al., arXiv, June 2026 (32 pages).

[1557] Differential absorption ozone Lidar with 4H-SiC single-photon detectors, by Xian-Song Zhao, Jian-Wei Pan, et al., arXiv, March 2025 (6 pages).

[1558] High sensitivity silicon carbide divacancy-based thermometer, by Qin-Yue Luo, Jun-Feng Wang, et al., arXiv, January 2023 (13 pages).

[1559] Temperature sensing using nitrogen-vacancy centers with multiple-poly crystal directions based on Zeeman splitting, by Li Xing, Xiaojuan Feng, Jintao Zhang, and Zheng Wang, arXiv, December 2022 (13 pages).

[1560] Nanodiamond quantum thermometry assisted with machine learning, by Kouki Yamamoto, Kensuke Kobayashi, et al., arXiv, April 2025 (5 pages).

[1561] Temperature dependence of nitrogen-vacancy center ensembles in diamond based on an optical fiber, by Ke-Chen Ouyang, Xing-Tuan Yang, et al., arXiv, November 2021 (17 pages).

[1562] Ultra-sensitive hybrid diamond nanothermometer, by Chu-Feng Liu, Ren-Bao Liu, et al., arXiv, December 2019 (20 pages).

[1563] Nanometre-scale thermometry in a living cell, by G. Kucsko, M. D. Lukin, et al., Nature, July 2013.

[1564] Diamond quantum thermometry from foundations to applications, by Masazumi Fujiwara et al., September 2021 (24 pages).

[1565] Intracellular thermometry with fluorescent sensors for thermal biology, by Kohki Okabe, 2018 (15 pages).

[1566] High sensitivity pressure and temperature quantum sensing in organic crystals, by Harpreet Singh, Ashok Ajoy, et al., arXiv, October 2024 (7 pages).

[1567] Thermodynamic miniaturized sensors and standards and the quantum SI, by Gregory F. Strouse, 2016 (39 slides).

[1568] Temperature dependent spin-phonon coupling of boron-vacancy centers in hexagonal boron nitride, by Zhongyuan Liu, Chong Zu, et al., arXiv, December 2024 (7 pages).

[1569] Enhancing low-temperature quantum thermometry and magnetometry via quadratic interactions in optomechanical-like systems, by Asghar Ullah and Özgür E. Müstecaplıoğlu, arXiv, February 2026 (14 pages).

[1570] Thermometry Based on a Superconducting Qubit, by Dmitrii S. Lvov, Sergei A. Lemziakov, Elias Ankerhold, Joonas T. Peltonen, and Jukka P. Pekola, arXiv, February 2025 (20 pages).

[1571] Bolometric Superconducting Optical Nanoscopy (BOSON), by Ran Jing, Mengkun Liu, et al., arXiv, April 2025 (13 pages).

[1572] Quantum optical technologies for metrology, sensing and imaging, by Jonathan P. Dowling and Kaushik P. Seshadreesan, arXiv, February 2015 (12 pages).

[1573] Advanced Micro- and Nano-Gas Sensor Technology: A Review, by Haleh Nazemi et al., Sensors, March 2019 (23 pages).

[1574] Nanodiamonds based optical-fiber quantum probe for magnetic field and biological sensing, by Yaofei Chen, Zhe Chen, et al., arXiv, February 2022 (21 pages).

[1575] Sensing electrochemical signals using a nitrogen-vacancy center in diamond, by Hossein T. Dinani, Enrique Muñoz, and Jeronimo R. Maze, arXiv, February 2021 (17 pages).

[1576] SARS-CoV-2 quantum sensor based on nitrogen-vacancy centers in diamond, by Changhao Li, Rouhollah Soleyman, Mohammad Kohandel, and Paola Cappellaro, arXiv, November 2021 (14 pages).

[1577] A molecular approach to quantum sensing, by Chung-Jui Yu, April 2021 (12 pages).

[1578] Amplified nanoscale detection of labeled molecules via surface electrons on diamond, by Ainitze Biteri-Uribarren, Jorge Casanova, et al., Communications Physics, December 2023.

[1579] Quantum relaxometry for detecting biomolecular interactions with single NV centers, by Min Li, Qi Zhang, Xi Kong, Sheng Zhao, Bin-Bin Pan, Ziting Sun, Pei Yu, Zhecheng Wang, Mengqi Wang, Wentao Ji, Fei Kong, Guanglei Cheng, Si Wu, Ya Wang, Sanyou Chen, Xun-Cheng Su, and Fazhan Shi, arXiv, December 2025 (37 pages).

[1580] Precision hyperfine spectroscopy of an individual nuclear-spin-9/2, by J. Travesedo, Z. W. Huang, L. Mykolyshyn, N. Thill, L. Pallegoix, P. Goldner, T. Chaneliere, S. Bertaina, T. Charpentier, D. Esteve, P. Abgrall, D. Vion, J. OSullivan, E. Flurin, and P. Bertet, arXiv, May 2026 (39 pages).

[1581] Highly sensitive single-molecule detection of macromolecule ion beams, by Marcel Strauß, Markus Arndt, et al., Science, December 2023.

[1582] IndiPIX: Paving the way towards compact, portable, and cost-effective mid-wave infrared systems imaging systems, by University of Glasgow, University of Glasgow, 2024 (7 pages).

[1583] Quantum metrology with ultracold chemical reactions, by Seong-Ho Shinn, Uwe R. Fischer, and Daniel Braun, arXiv, August 2022 (21 pages).

[1584] Quantum effect-based flexible and transparent pressure sensors with ultrahigh sensitivity and sensing density, by Lan Shi, Zhuo Li, Min Chen, Yajie Qin, Yizhou Jiang, and Limin Wu, Nature Communications, July 2020.

[1585] Quantum-Based Photonic Sensors for Pressure, Vacuum, and Temperature Measurements: A Vison of the Future with NIST on a Chip, by J Hendricks, 2021 (4 pages).

[1586] Adventures in quantumland, by Oscar Costa Hamido, 2021 (142 pages).

[1587] Quantum Advantage of One-Way Squeezing in Enhancing Weak-Force Sensing, by Jie Wang, Hui Jing, et al., arXiv, March 2024 (7 pages).

[1588] Quantum-well pressure sensors, by Witold Trzeciakowski, Sensors and Actuators A: Physical, April 1994 🔒.

[1589] Widefield NV Magnetic Field Reconstruction for Probing the Meissner Effect and Critical Current Density under Pressure, by Kin On Ho, Cassandra Dailledouze, Martin Schmidt, Loïc Toraille, Marie-Pierre Adam, and Jean-François Roch, arXiv, May 2026 (6 pages).

[1590] Probing stress and magnetism at high pressures with two-dimensional quantum sensors, by Guanghui He, Chong Zu, et al., Nature Communications, September 2025 (8 pages).

[1591] Quantum dots to probe temperature and pressure in highly confined liquids, by Sayed M. B. Albahrani, 2018 (12 pages).

[1592] Quantum Acoustics with Superconducting Qubits in the Multimode Transition-Coupling Regime, by Li Li, Dongning Zheng, et al., arXiv, May 2025 (14 pages).

[1593] Spectroscopy Study on NV Sensors in Diamond-based High-pressure Devices, by Kin On Ho, Jörg Wrachtrup, Sen Yang, et al., arXiv, January 2023 (15 pages).

[1594] Controlling complex dynamics with synthetic magnetism in optomechanical systems: A route to enhanced sensor performance, by Deivasundari Muthukumar, Serge Guy Nana Engo, et al., arXiv, July 2025 (26 pages).

[1595] Probing the quantum motion of a macroscopic mechanical oscillator with a radio-frequency superconducting qubit, by Kyrylo Gerashchenko, Samuel Deléglise, et al., arXiv, May 2025 (27 pages).

[1596] FLOC Takes Flight: First Portable Prototype of Photonic Pressure Sensor, by NIST, February 2019.

[1597] Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact, by NIST, 2019 (39 slides).

[1598] Quantum electro-mechanics: a new quantum technology, by Konrad Lehnert, 2012 (47 slides).

[1599] From micro to nano-optomechanical systems: light interacting with mechanical resonators, by Ivan Favero, 2021 (45 slides).

[1600] Progress of optomechanical micro-nano sensors a review, by Xinmiao Liu, 2021 (40 pages).

[1601] Mechanical Sensors for Ultraheavy Dark Matter Searches via Long-range Forces, by Juehang Qin, Christopher Tunnell, et al., arXiv, March 2025 (11 pages).

[1602] Quantum Sensing for Particle Physics, by Steven Worm, INFIERI Summer School, September 2025 (29 pages).

[1603] Dark Matter Candidates and Searches, by Nassim Bozorgnia, Joseph Bramante, James M. Cline, David Curtin, David McKeen, David E. Morrissey, Adam Ritz, Simon Viel, Aaron C. Vincent, and Yue Zhang, arXiv, June 2025 (40 pages).

[1604] Direct Detection of Dark Matter – APPEC Committee Report, by Julien Billard, Marc Schumann, et al., arXiv, April 2021 (106 pages).

[1605] Quantum sensing for particle physics, by Steven D. Bass and Michael Doser, Nature Reviews Physics, April 2024 🔓 (preprint on cds.cern.ch).

[1606] The search for ultralight bosonic dark matter, by Derek F. Jackson Kimball, Karl van Bibbers, et al., Springer Open Access, 2021 (375 pages).

[1607] Intrinsically Quantum Effects of Axion Dark Matter are Undetectable, by Yunjia Bao, Dhong Yeon Cheong, Nicholas L. Rodd, Joey Takach, Lian-Tao Wang, and Kevin Zhou, arXiv, October 2025 (10 pages).

[1608] Quantum sensing and dark matter searches, by Alex Sushkov, Boston University, 2022 (40 slides).

[1609] Letter of Intent: 100m Atom Interferometer Experiment at CERN, by Charles Baynham, Wolf von Klitzing, et al., arXiv, September 2025 (16 pages).

[1610] Technical Proposal for the Atom Interferometer CERN Experiment (AICE) Facility, by Gianluigi Arduini, Wolf von Klitzing, Michael Werner, et al., arXiv, August 2026 (170 pages).

[1611] CERN QT4HEP, LHC, Atlas, CMS and antimatter factory, by Olivier Ezratty, Opinions Libres, January 2025.

[1612] AEDGE: Atomic Experiment for Dark Matter and Gravity Exploration in Space - EPJ Quantum Technology, by Yousef Abou El-Neaj, Jure Zupan, et al., EPJ Quantum Technology, March 2020.

[1613] Matter-wave Atomic Gradiometer Interferometric Sensor (MAGIS-100), by Mahiro Abe, Thomas Wilkason, et al., arXiv, April 2021 (65 pages).

[1614] Time-reversal-based quantum metrology with many-body entangled states, by Simone Colombo, Vladan Vuletić, et al., Nature Physics, July 2022 🔓 (preprint on arXiv).

[1615] Dark Matter Detection through Rydberg Atom Transducer, by J. F. Chen, Haokun Fu, Christina Gao, Jing Shu, Geng-Bo Wu, Peiran Yin, Yi-Ming Zhong, and Ying Zuo, arXiv, March 2026 (12 pages).

[1616] Rydberg Single Photon Detection for Probing 0.1-10 meV Dark Matter with BREAD, by Abhishek Banerjee, Reza Ebadi, and Surjeet Rajendran, arXiv, October 2025 (6 pages).

[1617] Coherent collective response in many-qubit systems for dark matter detection, by Ryuichiro Kitano and Ryoto Takai, arXiv, July 2026 (21 pages).

[1618] Quantum-Enhanced Sensing of Axion Dark Matter with a Transmon-Based Single Microwave Photon Counter, by C. Braggio, Physical Review X, April 2025.

[1619] Axion Dark Matter eXperiment: Detailed Design and Operations, by R. Khatiwada, G. C. Hilton, et al., arXiv, October 2020 (23 pages).

[1620] Search for post-inflationary QCD axions with a quantum-limited tunable microwave receiver, by Giosuè Sardo Infirri, Giuseppe Ruoso, et al., arXiv, June 2025 (5 pages).

[1621] Design and simulation of a transmon qubit chip for Axion detection, by Roberto Moretti, Guido Torrioli, Andrea Vinante, et al., arXiv, January 2024 (5 pages).

[1622] Exploring dark matter with quantum-enhanced haloscopes and time projection chambers, by David Díez-Ibáñez, arXiv, September 2025 (248 pages thesis).

[1623] Superfluid helium ultralight dark matter detector, by M. Hirschel, Physical Review D, May 2024 🔓 (preprint on arXiv).

[1624] First Demonstration of the HeRALD Superfluid Helium Detector Concept, by R. Anthony-Petersen, M.R. Williams, et al., arXiv, November 2024 (14 pages).

[1625] A cryogenic chamber setup for superfluid helium experiments with optical fiber and electrical access, by Alexander R. Korsch, Niccolò Fiaschi, and Simon Gröblacher, arXiv, August 2025 (10 pages).

[1626] Achieving speedup in Dark Matter search experiments with a transmon-based NISQ algorithm, by Roberto Moretti, Andrea Giachero, et al., arXiv, March 2026.

[1627] Dark Matter Detection with Qubits, by Meeri Mäkitalo, VTT, August 2025.

[1628] Quantum Enhancement in Dark Matter Detection with Quantum Computation, by Shion Chen, Hajime Fukuda, Toshiaki Inada, Takeo Moroi, Tatsumi Nitta, and Thanaporn Sichanugrist, arXiv, July 2024 (8 pages).

[1629] Quantum Computers as Dark Matter Detectors, by Aaron S. Chou, Fermilab, August 2022 (57 slides).

[1630] Wide-mass-scanning-range setup and phase-resolved protocol for axion dark matter detection, by Audrey Cottet and Takis Kontos, New Journal of Physics, February 2026 (19 pages).

[1631] Time domain non-linear quantum interferometry, by C. Fruy, A. Théry, B. Hue, W. Legrand, L. Jarjat, J. Craquelin, M.R. Delbecq, A. Cottet, and T. Kontos, arXiv, September 2026 (24 pages).

[1632] Evaluating radiation impact on transmon qubits in above and underground facilities, by Francesco De Dominicis, Anna Grassellino, Laura Cardani, et al., arXiv, July 2025 (7 pages).

[1633] Toward 48 dB Spin Squeezing and 96 dB Signal Magnification for Cosmic Relic Searches with Nuclear Spins, by Marios Galanis, Onur Hosten, Asimina Arvanitaki, and Savas Dimopoulos, arXiv, August 2025 (20 pages).

[1634] An Optomechanical Accelerometer Search for Ultralight Dark Matter, by M. Dey Chowdhury, J. P. Manley, C. A. Condos, A. R. Agrawal, and D. J. Wilson, arXiv, September 2025 (17 pages).

[1635] Beyond Qubits: Multilevel Quantum Sensing for Dark Matter, by Xiaolin Ma, Volodymyr Takhistov, Norikazu Mizuochi, and Ernst David Herbschleb, arXiv, October 2025 (14 pages).

[1636] Simulation of Axion-Induced Electromagnetic Signal Detection Using Plasmonic Metasurfaces and Diamond NV Centers, by James L. Webb, arXiv, June 2026 (15 pages).

[1637] Quantum Error Correction Assisted Axion Search in CMOS Spin Qubit Arrays, by Xiangjun Tan and Zhanning Wang, arXiv, May 2026.

[1638] Towards Quantum-Dot Detectors as Barcodes for Dark Matter Interactions, by Marek Matas, Andrea Gallo Rosso, Antonio Cammarata, Nora Hoch, Carlos Blanco, Jan Conrad, Rouven Essig, Tim Linden, and Lindley Winslow, arXiv, August 2026 (24 pages).

[1639] Quantum Enhanced Dark-Matter Search with Entangled Fock States in High-Quality Cavities, by Benjamin Freiman, Yao Lu, et al., arXiv, October 2025 (8 pages).

[1640] Search for dark matter particle interactions in an extended nuclear recoil energy window with the LUX-ZEPLIN (LZ) experiment, by D. S. Akerib, A. K. Al Musalhi, B. J. Almquist, et al., LUX-ZEPLIN Collaboration preprint, submitted to Physical Review Letters, September 2026 (25 pages).

[1641] Fermionic Dark Matter Absorption and the High-Energy Event in LUX-ZEPLIN, by Yuanchao Lou and Chih-Ting Lu, arXiv, September 2026 (11 pages).

[1642] Quantum sensing, by Christian L. Degen, Friedemann Reinhard, and Paola Cappellaro, Reviews of Modern Physics, July 2017 (46 pages) 🔓 (preprint on arXiv).

[1643] Einstein's 1917 Static Model of the Universe: A Centennial Review, by Cormac O'Raifeartaigh, Michael O'Keeffe, Werner Nahm, and Simon Mitton, arXiv, May 2017 (60 pages).

[1644] Experiment to Detect Dark Energy Forces Using Atom Interferometry, by D. O. Sabulsky, I. Dutta, E. A. Hinds, B. Elder, C. Burrage, and Edmund J. Copeland, Physical Review Letters, August 2019 (6 pages).

[1645] The revolution in strong lensing discoveries from Euclid, by Natalie E. P. Lines, Mike Walmsley, et al., arXiv, August 2025 (16 pages).

This **Quantum sensing** section contains 515 bibliographical references and notes containing at least 10,412 pages.

Page intentionally left blank.

Page intentionally left blank.

Page intentionally left blank.

⟨ 137 | 1WQC | 3D NAND | 2DEG | Abelian | ABRC | Active space | Active Volume | ADAPT-VQE | Adaptive quantum circuits | ADC | AC Stark shift | Adiabatic | Adiabatic theorem | ADR | Advantage | aka | AKLT state | Algorithm | Algorithmic qubit | Amdahl's law | AFC | Amplitude | Amplitude amplification | Anharmonic oscillator | Angular momentum | Anomalous heating | Ansatz | Antibunching | Anyon | arXiv | Antisymmetry | AOD | Approximate Amplitude Encoding | Artificial atoms | ASIC | Assumptions | Atoms | Auger effect | Autonomous quantum error correction | AWG | Axion | BB84 | Back action | Backside power delivery | Balmer series | Band gap | Balanced beam splitter | Barren plateaus | Baryon | Base temperature | BCS theory | Beam splitter | Bell inequalities | Bell states | Bell test statistic | Bernstein-Vazirani | Basis encoding | Betti number | Bichromatic field | Bright/dark fluorescence readout | Bias-preserving gate | Biphoton | Black body | Blind Quantum Computing | Angle encoding | Amplitude encoding | Bloch states | Bloch sphere | Brightness | Bucket brigade | Block-encoding | Bond dimension | Born rule | Born-Oppenheimer approximation | Bose-Einstein Condensate | Bose-Hubbard model | Boson sampling | Boson | Bosonic codes | BQP | Bra-ket | Brane | Bravais lattice | Break-even | Brillouin scattering | BSM | cADR | Cap table | Capex | Carleman linearization | Carnot efficiency | Casimir effect | Cavity | Cavity quantum electrodynamics | CFD | CFET | Chandelier | Chern number | Chi | Chip | Chipset | Chiplet | CHSH inequality | CIM | Circuit quantum electrodynamics | Circuit synthesis | Classical shadows | Clifford group | Circulators | Circuit | Clock qubit | Cluster state | CLOPS | CMOS | CNOT | Coarse graining | Coaxmon | Code distance | Coherence | Coherence fraction | Coherence length | Cold atoms | Cold plate | Cold trap | Compatible properties | Commutativity | Commutator or commutation operator | Complementarity | Complementary variables | Complex number | Complexity | Compton effect | Computational basis | Concatenated codes | Condensed matter physics | Conjugate variables | Concurrence | Consistent histories | Constructor theory | Contextuality | Continuous variables quantum computing | Cooper pair | COP | Copenhagen interpretation | Coplanar waveguide (CPW) | CPLEX | Cryo-CMOS | Correspondence principle | Coulomb blockade | Coulomb force | Counterfactuals | Counterfactual models | CPTP map | Crosstalk | Cryocooler | Cryogenics | Cryopumping | Cryostat | CSCO | CSM | Butterfly velocity | Cuprate | CV-QKD | CVaR | CVD | DAC | DAQC | Data re-uploading | Dark count | Dark energy | Dark matter | Dark silicon | Dark state | Dark state protocols | DCE | DCQO | DDS | DQC | De Broglie wavelength | Decoherence | Degenerate | Delayed-choice experiment | Dennard scaling | Density matrix | Dequantization | Determinism | Deutsch-Jozsa | DFT | Dimon | DI-QKD | Dicke state | $k=0$: | $k=1$: | $k=2$: | $k=3$: | $k=4$: | Diffraction | Dilution refrigerator | Dirac's notation | Dirac constant | Discrete log problem | Dissipation engineering | Distillation | DLA | DMRG | Domain specific architecture | Doppler cooling | Doppler effect | DV-QKD | D-Wave | DQI | DRAG | DRAM | Dressed state | Dual-rail encoding | Dual-species | E91 | EBL | EDSR | Eigenstate | Eigenvalue | Eigenvector | Einselection | Electromagnetic spectrum | EIT | Electron | Electron gas | Elliptic Curves Cryptography | Energetics of quantum technology | Engineering | Entanglement | Entropy | EPLG | EPDA | Epistemology | EPR paradox | EQA | Erasure error | ERC Grants | Ergodicity | Ergotropy | Error Correction Codes | Errors | ESR | Eta letter | EUV | Exchange-only qubit | Exciton | Exclusion principle | Expectation value | Euclidean networks | Extended Church-Turing thesis | Fabry-Pérot cavities | FBQC | FD-SOI | Feedforward | Fermi's golden rule | Fermi sea | Fermi-Hubbard model | Fermions | Fine structure | FinFET | First quantization | First quantum revolution | Floquet code | Fine-structure constant | FOFI | Fluxonium | Flying qubits | Fock space | Fock state | Flux biasing | Foliation | Fourier Transform | FPGA | Fredkin gate | Free Electron Laser (FEL) | FTQC | GAA | GAN | GAS | Gatemon | Gate-based quantum computing | Gate teleportation | Gaussian Boson Sampling (GBS) | Gaussian state | GBS | GGSA | GHS | GHZ | Gibbs state | Gifford-McMahon | Ginzburg-Landau theory | GKP qubits | Gleason's theorem | GPGPU | GQE | Graviton | Green's function | Grotrian diagram | Ground state | Grover | GSA | Gurobi | H-bar | Hadamard | Hafnian | Hall effect | Hamiltonian | Hamiltonian simulation | Hamming distance | Harmonic oscillator | Hartree-Fock | HBM | Heisenberg | Heisenberg cut | Heisenberg limit | Helium 3 | Helium 4 | HEMT | Hermitian matrix | Heterostructures | Heuristic algorithm | Heralded single-photons | Helicity | Heterodyne measurement | HHL | High-NA | Hilbert | Holevo bound | Hong-Ou-Mandel effect | Hidden variables | HOBO | Homodyne | Hoplon | HPC | HPQC | HSP | HTS | Hubbard model | HUBO | Hybrid bonding | Hyperentanglement | Hybrid quantum algorithms | Hyperfine qubit | Iceberg code | IDR | In-memory computing | Indeterminacy principle | Indistinguishability | Indistinguishable photons | Integrated Photonics | Interference | Interposer | Intersubjectivity | Invertible computation | Irreversible | Ion | Ion shuttling | Ion traps | Ion trap I/Q mixer | Isotopes | IT | Jaynes-Cummings Hamiltonian | Jevons paradox | JJ | Josephson | JPA | Kapitza resistance | Kerr effect | Ket | Klein-Gordon equation | Kochen-Specker theorem | Koomey's law | Koopman–von Neumann | Lamb shift | Lamb-Dicke regime | Landauer limit | Larmor frequency | Larmor precession | Laser | Lattice surgery | LCHS | LCU | Leakage errors | Learning | Leggett-Garg inequality | Leggett-Garg inequalities | Kraus operators | Lie group | Lindblad equation | Linear algebra | Linear optics | Lieb-Robinson bound | Light cone | LNOI | Local Friendliness | Loophole-free Bell test | Lorentz factor | LPPT | LQG | M-theory | Many-worlds interpretation | max-LINSAT max-k-XORSAT | Locality | LOCC | Logical Qubit | Loophole | LRU | LSTM | MAGIC | Magic states distillation | Magic state cultivation | Magneto-Optical Trap | Magnon | Majorana fermion | Manifold | Markovian process | Matchgate circuits | Matrix | Matter wave | MAXCUT | Maxwell's demon | MBE | MBQC | MCMC | MCMR | MDI-QKD | MegaQuop | Meissner effect | MERA | Mesoscopic | Metaheuristic algorithm | Metal layers | Metasurface | Microring resonator | Mid-circuit measurement | MIS | Microwave-to-optical transduction | Mixing chamber | Moore's law | More than Moore | MRAM | MZI | Mølmer–Sørensen | Mode | Mode option | MNR | Mode-locked laser | Mott insulator | Mott transition | MPO | MPS | MVP | MINLP | Multi-qubit state | Momentum | Optimode | Muonic atoms | Mutually unbiased bases | Nanosheet | NDR | NEMS | NFQC | NISQ | No-go theorem | No-cloning theorem | No-signaling | Nonlinear optics | Nonlocality | Non-Markovian process | NMR | Non-classical light | Non-demolition measurement | Non-selective measurement | NOON state | Noether's theorem | Normalization | NP | NP-complete | NP-difficult | NV center | Oracle | OMR | OFHC | On-premise | Ontology | OPA | Opex | Operator norm | OPO | OTOC | Optical molasses | Optical pumping | Optical qubit | Optical tweezer | Oracle | Orbital angular momentum | Oscillator | Overhauser field | P | Paramp | Paul trap | Pauli | Pauli blockade | Pauli string | PBR theorem | PCA | PDE | PDK | Penning trap | PEPS | Permanent | Phase Estimation Algorithm | Phase | Phase class | Phase space | Phasor diagram | Phonon | Photoelectric effect | Photoionization | Photolithography | PIC | PIM | Photon | Photonic | Photonic qubit | PKI | Planck constant | Planck length | Planck units | Plasmon | PMT | PNRD | Pockels effect | Poincaré sphere | Pointer states | Polarized Beam Splitter | Polaritons | Postselection | POVM | PQC | PQE | PQS | Prefactors | Prepare-and-measure | Private Key | Process Design Kit | Property | Psi-ontic and psi-epistemic | Public key | PUBO | PUE | Pulse tube | Purcell effect | Purcell filter | Pure state | Purification | PVD | PVM | Q factor | Q-Score | QAA | QAE | QAI | QACM | QAQM | QAOA | QAOA | QBER | QBism | QCCD | QCKA | QCaaS | QCNN | QCV | QFC | QFT | QFHE | QFT | QGLM | QIP | QHO | QIR | QITE | QKD | QLBM | qLDPC | QLM | QLSA | QLSP | QMA | QML | QND | QNLP | QPE | QPINN | QPU | qRAM | QRC | QRNG | QROM | QSA | QSCI | QSP | QSDC | QSS | QST | QSVD | QROAM | QSVT | Quantics representation | Quantization | Quantronium | Quasi-locality | Quantum accelerator | Quadrature | Quantum advantage | Quantum algorithm | Quantum annealing | Quantum batteries | Quantum channel | Quantum Chaos | Quantum chromodynamics | Quantum circuit | Quantum cognition | Quantum computer | Quantum Conference Key Agreement | Quantum Darwinism | Quantum data center | Quantum dots | Quantum Electro-Dynamic | Pauli propagation | Quantum emulator | Quantum energetics | Quantum engineering | Quantum Field Theory | Quantum Fisher Information | Quantum foundations | Quantum gates | Quantum Hall effect | Quantum hydrodynamics | Quantum Internet | Quantum jump | Quantum kernel | Quantum capability learning | Quantum logic | Quantum matter | Quantum medicine | Quantum Non Demolition measurement | Quantum numbers | Quantum postulates | Quantum Physical Unclonable Functions | Quantum repeater | Quantum reservoir computing | Quantum reservoir engineering | Quantum resource estimator | Quantum simulator | Quantum speed limit | Quantum spin liquid | Quantum state | Quantum state tomography | Quantum Steering | Quantum supremacy | Quantum switch | Quantum teleportation | Quantum thermodynamics | Quantum transduction | Quantum trajectories | Quantum utility | Quantum variational circuits | Quantum volume | Quantum walk | Quantum Zeno Effect | Quasiparticles | Qubit | Qubyte | Qubench | Qumode | Qunit | Ouquart | Outrit | QWOA | Rabi | Racetrack | Raman cooling | Raman effect or Raman scattering | Random circuit | Rare earth ion | Rayleigh scattering | RBM | Realism | Rebound effect | Reduced Planck constant | Register | Relativistic Quantum Mechanics | Relaxation | ReLU | Renormalization | Renyi entropy | Repumping | Reticle limit | Retrodiction | Reversible computing | RIE | RSA | RUS | RSG | Rydberg state | Rydberg blockade | Sapphire | SAT | Scrambling | Scale-out | Scattering | Schrödinger | Schrödingerization | Schrödinger wave function collapse | SDP | LP | MIP | ILP | Second quantization | Second quantum revolution | SED | Semiclassical QFT | Semi-classical light | SFQ | Shelving | Shor | Shortcuts to Adiabaticity | Sideband | Silicon 28 | SIMD | Simon | Single mode | SKR | Singlet-triplet qubit | Sign problem | Sisyphus cooling | Skyrmion | SLM | SNAQ | SNSPD | SoC | SOI | SPAC | SPAD | SPAM | Spectral lines | Spectral decomposition | Spin | SpinBus | Spin-to-charge conversion | Spin-boson model | Spin glass | Spinor | Spintronics | Spontaneous emission | Spontaneous Four-Wave Mixing | Spontaneous Parametric Down-Conversion | SPOQC | Squeezed states of light | Squeezing | SQUID | SRAM | Stabilizer gates | Standard model | Standard quantum limit | Stark shift or Stark effect | State reduction | Retargetability | Strong simulation | State vector | Stationary qubits: stationary | Stern-Gerlach experiment | Still | Stimulated emission | String theory | Sturm–Liouville problem | Superabsorption | Superatom | Superconductivity | Superdense coding | Superdeterminism | Superfluidity | Supersonic propagation of correlations | Superoperator | Superposition | Superradiance | Superselection | Supersolid | Surface codes | Surface trap | SVD | SVM | SWAP | s-wave, p-wave and d-wave | SWSPD | SYK | Symmetry | Sympathetic cooling | Szilard engine | T gate | T-count | T-depth | Tachyon | Tau scaling law | TCI | TCO | TDA | TDP | Technology node | Tensor network | TF-QKD | TFLN | TES | THC | Theory of everything | TSP | T_1 | T_2 | Tabu search | TDSE | Tensor | TeraQuop | Thermodynamics first law | Thermodynamics second law | Time crystal | Time domain | Time reversal | Toffoli | Topological | Topological insulator | Time-bin entanglement | Tsirelson bound | Transmon | Transpiler | Transpilation | Transversal gates | Trapped ions | Trotterization | Trusted node | TSV | TTN | TTSB | Tunnel effect | Twistronics | Two-Level Systems | TWPA | Type I and type II superconductors | UCC | UHV | Ultraviolet catastrophe | Unary iteration | Unary gates | Uncompute trick | Unconventional Computing | Unitary operation | Universal quantum computer | Universal quantum gates | Unruh effect | Vacuum fluctuation | Vacuum polarization | Value migration | Variational algorithm | von Klitzing constant | VQA | VQC | VQE | VQLS | Wafer-scale engine | Warm start | Weak simulation | Wave packets | Wave-particle duality | Wavicle | Weyl fermion | Wien's displacement law | Wigner crystal | Wigner function | Wigner's friend | WIMP | X | XY gates | Y | Z | Zeeman effect | Zeeman

le lab quantique