cybersecurity in the quantum age

myths and legends, real problems and real solutions

olivier ezratty

olivier@oezratty.net www.oezratty.net

DTU, Kongens Lyngby, December 7th, 2023

the quantum fear

TechCrunch

The quantum computing apocalypse is imminent

Shlomi Dolev January 2018

Connectivity

Quantum Computing Paranoia Creates a New Industry

Even though quantum computers don't exist yet, security companies are preparing to protect against them.

by Tom Simonite January 30, 2017

MIT Technology Review

F **ear sells in the computer security business. And in late 2015** Massachusetts-based Security Innovation got an unexpected boost from one of the scariest organizations around—the National Security Agency.

MIT Technology Review

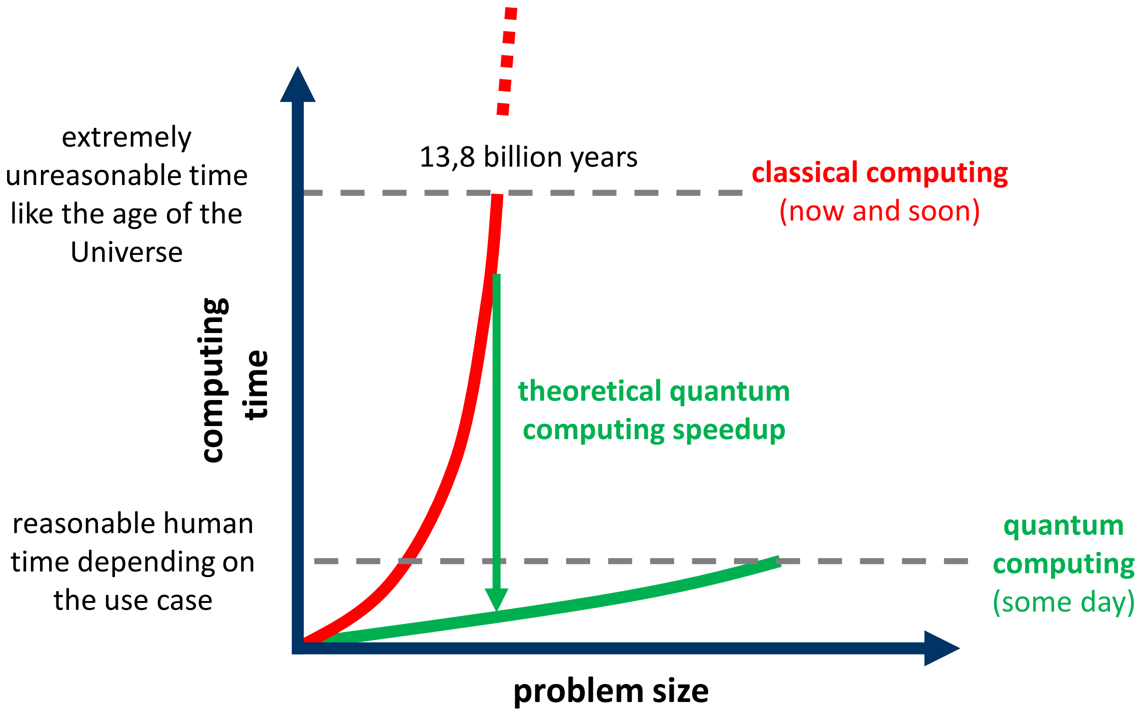
Business Impact

Quantum Computers Pose Imminent Threat to Bitcoin Security

The massive calculating power of quantum computers will be able to break Bitcoin security within 10 years, say security experts.

by Emerging Technology from the arXiv November 8, 2017

the quantum computing threat



solve so-called intractable exponential problems like …

breaking public PKI asymmetric keys and even symmetric cryptography keys

emitter — RSA cryptography — receiver

determines **p and q**, two large random prime numbers
computes **N = pq** which is a very large integer (preferably >=2048 bits)
evaluate **e**: a prime number with O(N) given
O(N) = number of prime integers between 1 and N, and since p and q are prime, **O(N) = (p-1)(q-1)**
d is a large integer coprime of O(N) that is chosen according to :
e^d = 1 mod (O(N))

original information

use public key **(N, e)** to encode the data

sends public key

sends the public key with **(N, e)** to the sender of the data

encoded data

sends encoded data with public key

use private key **d**, kept by the receiver, and the public key to decode the data

a pirate could guess **d** with using **e** and factoring **N** in (p,q), and decode the intercepted message

threatened cryptography systems

Peter Shor factoring algorithm - 1994
integer factoring
exponential acceleration

$$O(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}) \Rightarrow O((\log N)^2\,(\log \mathit{log}\, N))$$

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

$$O(e^{(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}) \Rightarrow O((\log N)^2\,(\log \mathit{log}\, N))$$

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

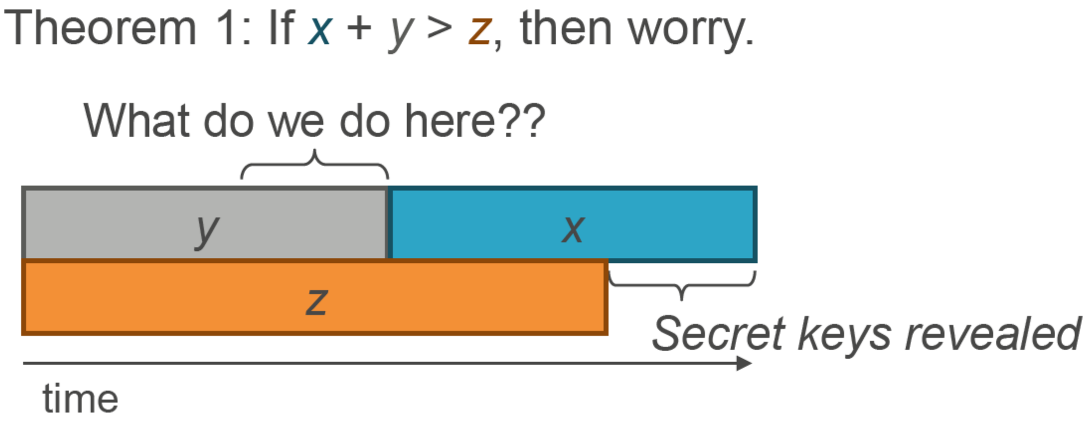
The Quantum Countdown
Quantum Computing And The Future Of Smart Ledger Encryption

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

potential long term quantum threats on cryptos. Source: The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption by Long Finance, 2018 (60 pages)

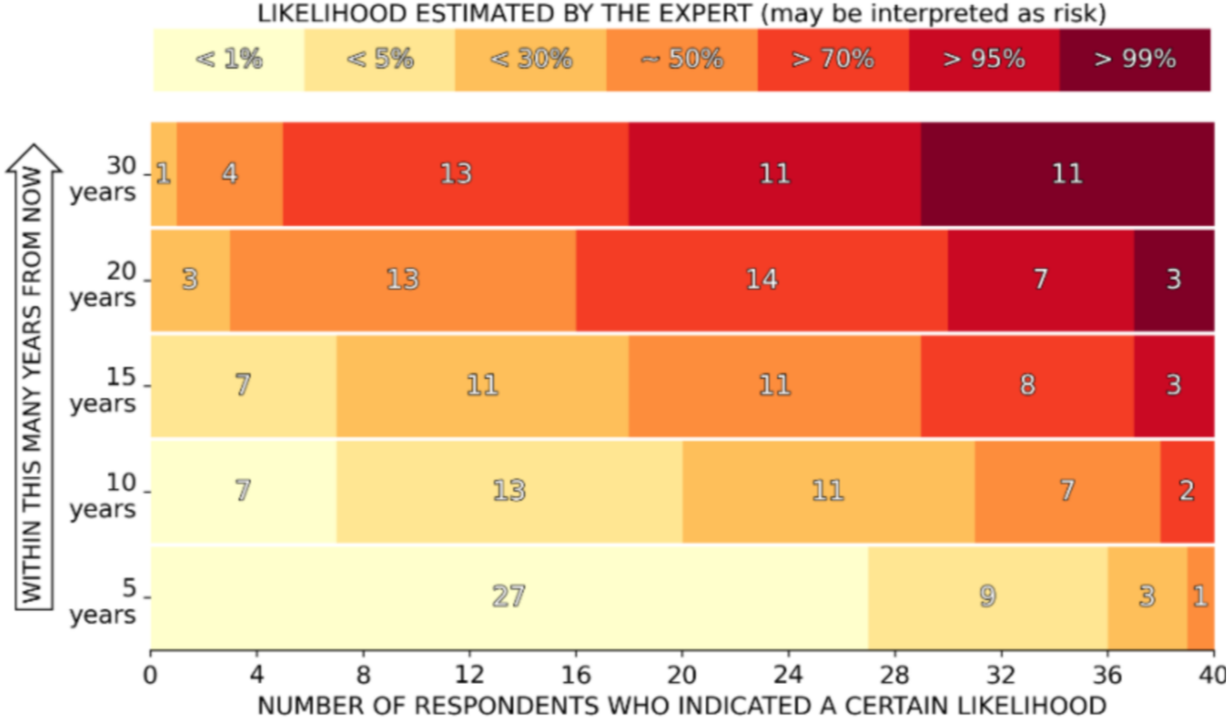
Mosca « XYZ risk model » or theorem



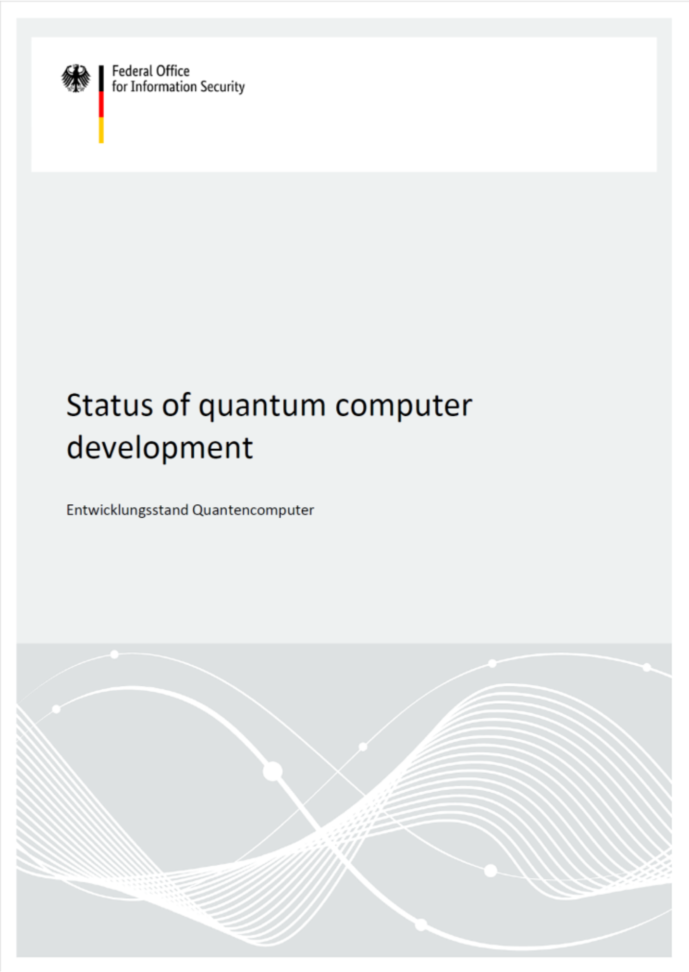
	definition	estimation	uncertainty
x	time that you need encryption to be secure	≈ 10-20 years	none: regulatory
y	time to re-tool the existing infrastructure with PQC	≈ 5-10 years	average: operational
z	time to build a FTQC computer breaking RSA-2048	≈ 15-30 years	total

2022 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

The experts indicated their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 quickly—for various time frames, from a short term of 5 years all the way to 30 years.



https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/


Federal Office for Information Security

Status of quantum computer development

Entwicklungsstand Quantencomputer

the quantum threat

Shor integer factoring

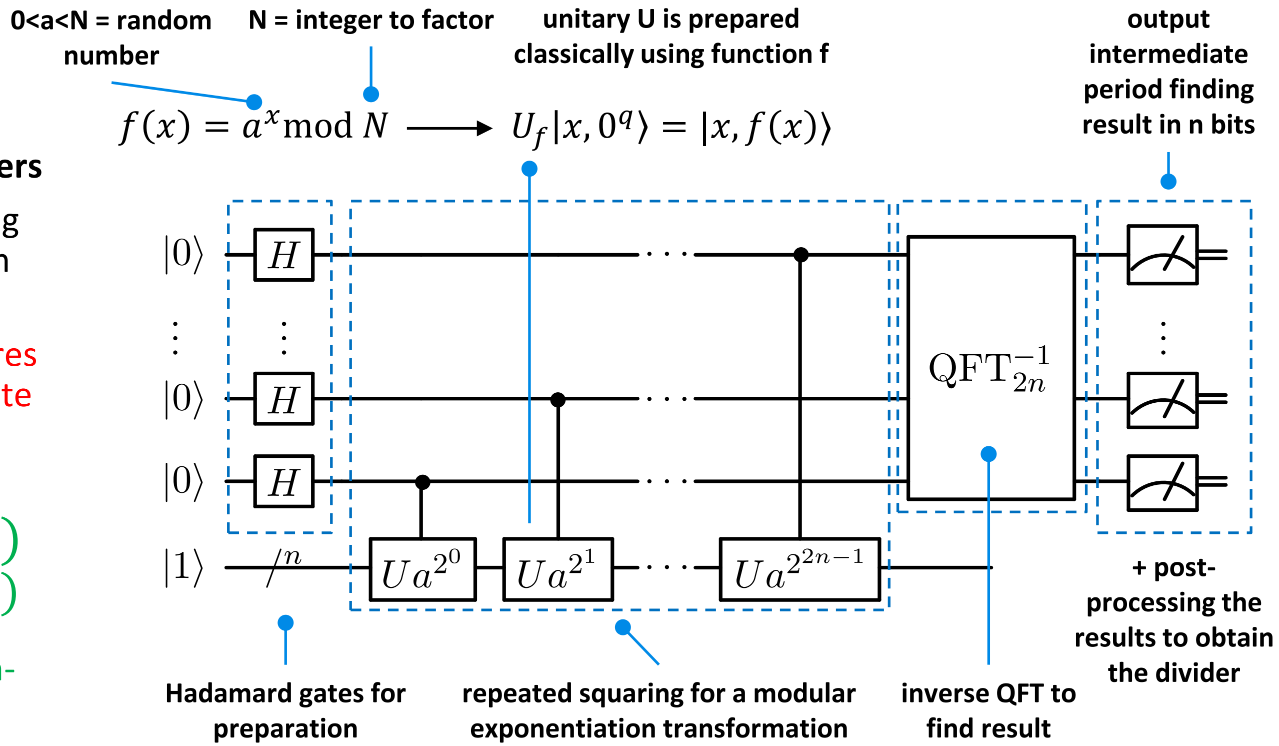
factors an integer in prime numbers

algorithm relies on a period finding algorithm and an inverse quantum Fourier transform

breaking RSA 2048 bits key requires 20 millions qubits with an error rate of 0.1% and 8 compute hours.

$$O\left(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}\right)$$
$$\Rightarrow O\left((\log N)^2\,(\log\log N)\right)$$

exponential speed gain vs best in-class GNFS classical algorithm



Shor algorithm requirements

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

99.9% gate fidelities

surface code cycle time of 1 μs

reaction time of 10 μs

Factoring 2 048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory

Élie Gouzien* and Nicolas Sangouard†
Université Paris–Saclay, CEA, CNRS, Institut de Physique Théorique, 91 191 Gif-sur-Yvette, France
(Dated: September 29, 2021)

memory storing 28 million spatial modes and 45 temporal modes with 2 hours storage time.

doi:10.1103/PhysRevLett.131.040602

Performance Analysis of a Repetition Cat Code Architecture: Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits

Élie Gouzien[1,*] Diego Ruiz[2,3] Francois-Marie Le Régent[2,3] Jérémie Guillaud[2] and Nicolas Sangouard[1,†]
[1]*Université Paris–Saclay, CNRS, CEA, Institut de physique théorique, 91 191 Gif-sur-Yvette, France*
[2]*Alice&Bob, 53 boulevard du Général Martial Valin, 75 015 Paris, France*
[3]*Laboratoire de Physique de l'École normale supérieure, École normale supérieure, Mines Paris, Université PSL, Sorbonne Université, CNRS, Inria, 75 005 Paris, France*
(Dated: August 7, 2023)

350,000 cat-qubits

4 days

full architecture proposal

Schnorr schneller than Shor?

FINANCIAL TIMES

US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

Quantum technologies + Add to myFT

Chinese researchers claim to find way to break encryption using quantum computers

Experts assess whether method outlined in scientific paper could be a sooner-than-expected turning point in the technology

- **hybrid QAOA based algorithm using classical "Schnorr" algorithm.**
- **would require 372 NISQ physical qubits and 1139-1490 gate depth.**
- **QAOA does not scale well.**
- **classical and quantum part speedup and time were not provided.**
- **NISQ qubit noise would require some QEC and a much larger number of physical qubits.**

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan,[1,2,*] Ziqi Tan,[3,*] Shijie Wei,[4,*] Haocong Jiang,[5] Weilong Wang,[1] Hong Wang,[1] Lan Luo,[1] Qianheng Duan,[1] Yiting Liu,[1] Wenhao Shi,[1] Yangyang Fei,[1] Xiangdong Meng,[1] Yu Han,[1] Zheng Shan,[1] Jiachen Chen,[3] Xuhao Zhu,[3] Chuanyu Zhang,[3] Feitong Jin,[3] Hekang Li,[3] Chao Song,[3] Zhen Wang,[3,†] Zhi Ma,[1,‡] H. Wang,[3] and Gui-Lu Long[2,4,6,7,§]

[1] *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2] *State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[3] *School of Physics, ZJU-Hangzhou Global Scientific and Technological Innovation Center, Interdisciplinary Center for Quantum Information, and Zhejiang Province Key Laboratory of Quantum Technology and Device, Zhejiang University, Hangzhou 310000, China*
[4] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[5] *Institute of Information Technology, Information Engineering University, Zhengzhou 450001, China*
[6] *Beijing National Research Center for Information Science and Technology and School of Information Tsinghua University, Beijing 100084, China*
[7] *Frontier Science Center for Quantum Information, Beijing 100084, China*

https://arxiv.org/abs/2212.12372, December 23rd, 2022

« Happy 40th Birthday Dana!

Cargo Cult Quantum Factoring

For those who don't care to read further, here is my 3-word review:

No. Just No.

And here's my slightly longer review:

Ed Gerck, PhD, PhD • 2nd
Founder Planalto Research, Chief Scientist, ZSentry architect.
1mo • Edited •

+ Follow •••

Today, we could announce it. Quantum computing (QC) has become a reality. We broke the RSA -2048 key. Ron Rivest is a dear friend, but that was needed to advance.

The QC version used here has simultaneous multiple-states logic (following ‘all states at once’), with more than a googol of possible states.

We show that the equivalence of QC techniques (with IBM, Google and others compared with our version of QC) has been hidden for about 2,500 years – since Pythagoras.

All our QC computations were done in a commercial cellphone, or a commercial Linux desktop, as our QC devices -- opening the user market to many industries. No cryogenics or special materials were used.

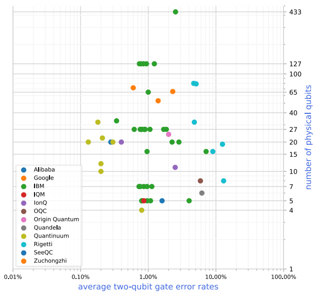
A post-quantum, HIPAA compliant, end-to-end, patent-free, export-free, secure online solution, is being created, based on ZSentry as used from 2004 to 2014, to replace RSA. One needs a quantum-resistant algorithm, because all existing public-key encryption can be broken.

“Quantum computing (QC) has become a reality. We broke the RSA -2048 key.”

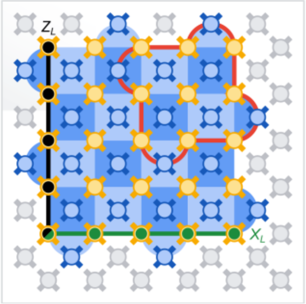
“The QC version used here has simultaneous multiple-states logic (following ‘all states at once’), with more than a googol of possible states.”

“All our QC computations were done in a commercial cellphone, or a commercial Linux desktop”.

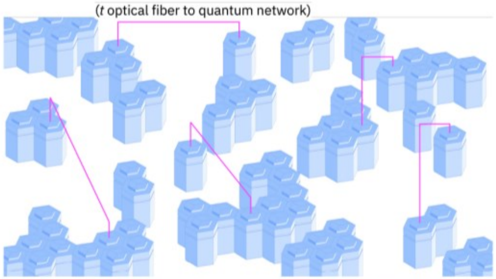
key scientific and engineering challenges



improve qubits fidelities

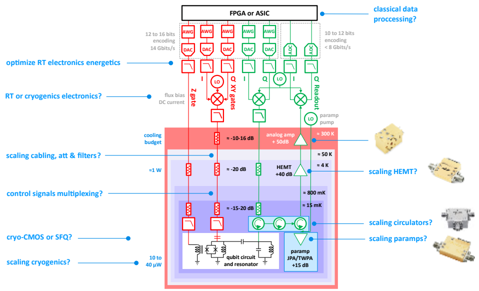


errors mitigation and correction



(e) t type modularity involves microwave-to-optical transduction to link QPUs in different dilution refrigerators.

quantum interconnect



electronics, cabling and/or cryogeny scalability

#QEI

the quantum energy initiative

energy consumption containment or advantage

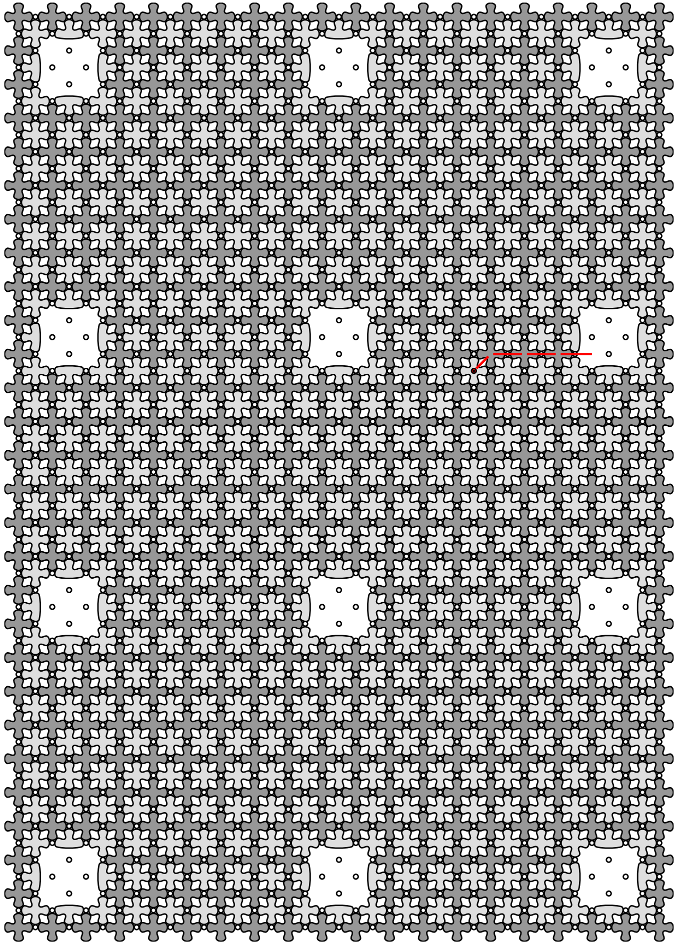
logical qubits

physical qubit

error rates ≈0.1%

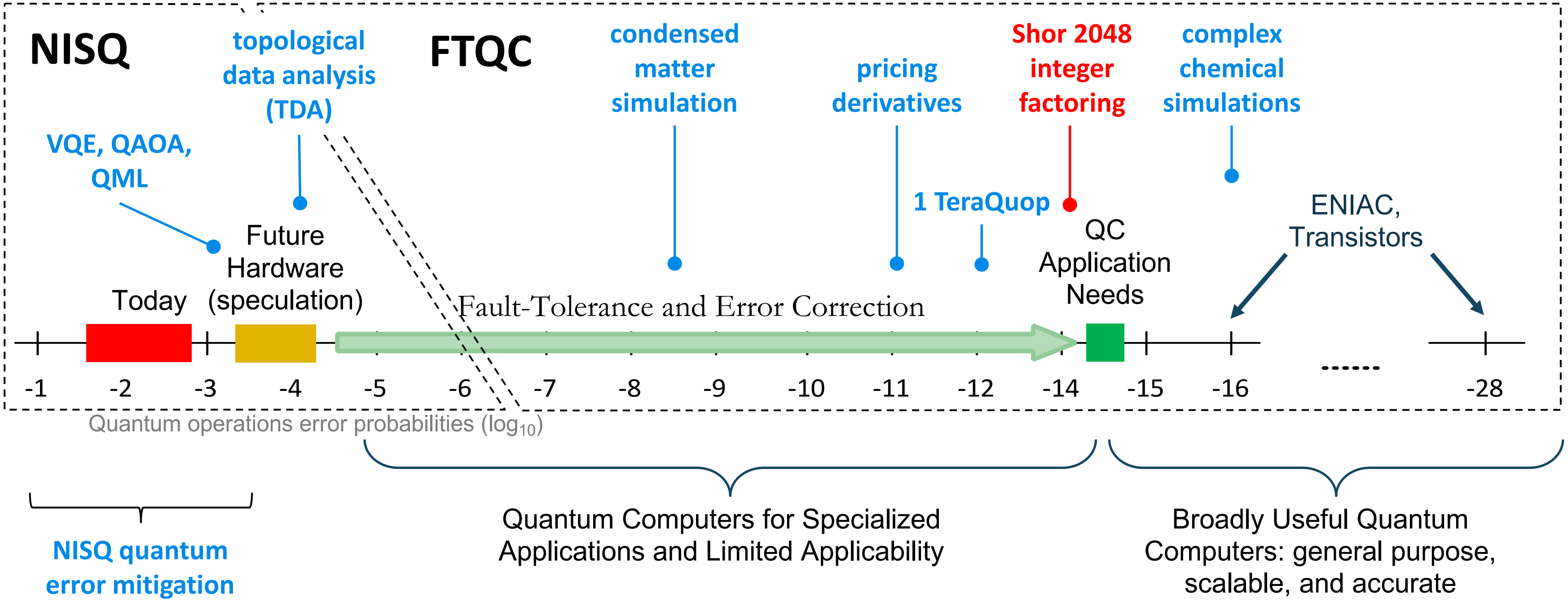
logical qubit

error rate $<10^{-8}$ to $<10^{-15}$

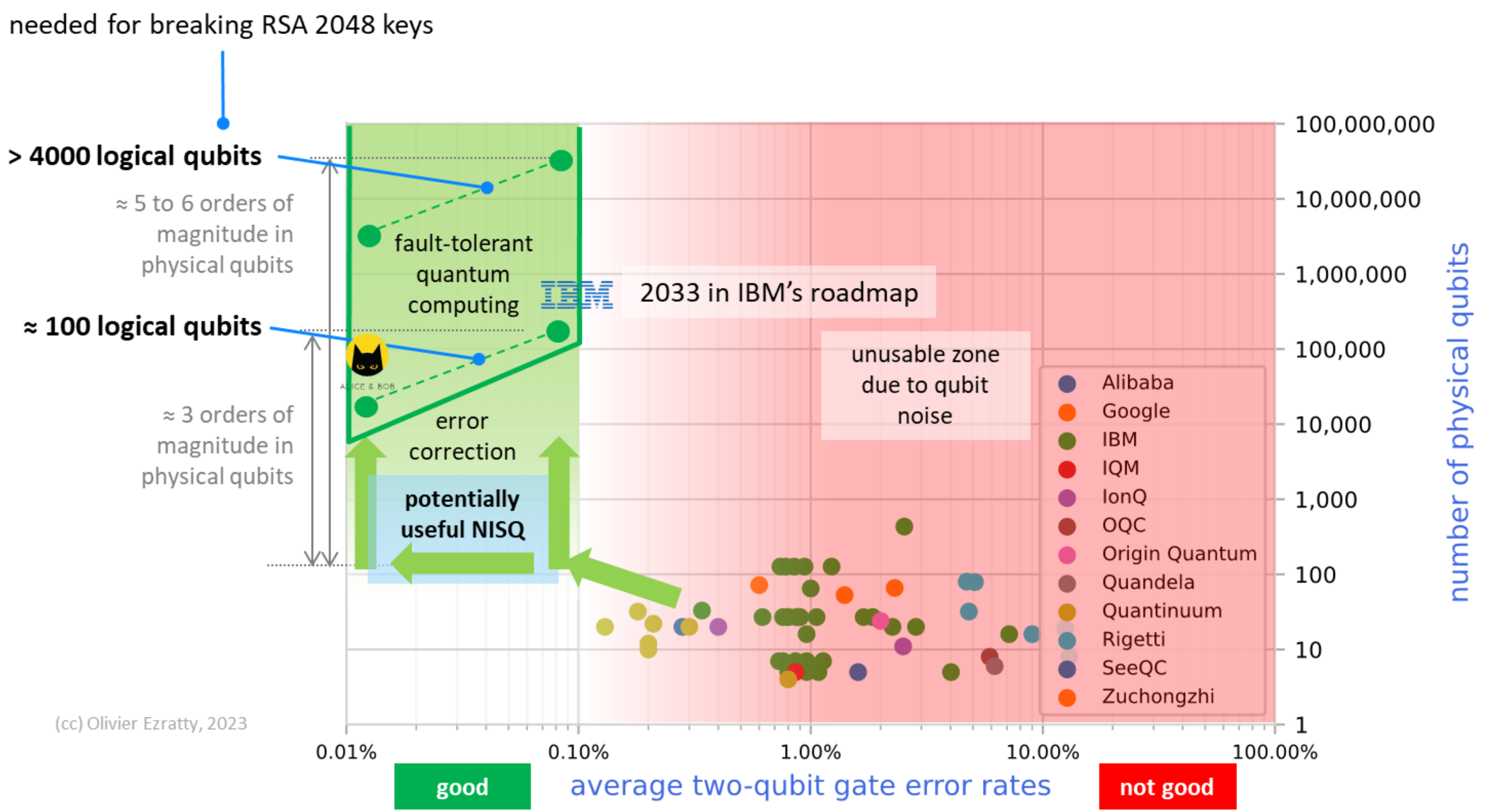


https://arxiv.org/abs/1202.2639

from NISQ to FTQC



source: How about quantum computing? by Bert de Jong, DoE Berkeley Labs, June 2019 (47 slides) + Olivier Ezratty additions.



needed for breaking RSA 2048 keys
> 4000 logical qubits
≈ 5 to 6 orders of magnitude in physical qubits
≈ 100 logical qubits
≈ 3 orders of magnitude in physical qubits
fault-tolerant quantum computing
IBM
2033 in IBM's roadmap
error correction
potentially useful NISQ
unusable zone due to qubit noise
Alibaba
Google
IBM
IQM
IonQ
OQC
Origin Quantum
Quandela
Quantinuum
Rigetti
SeeQC
Zuchongzhi
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
10
1
number of physical qubits
0.01%
0.10%
1.00%
10.00%
100.00%
good
average two-qubit gate error rates
not good
(cc) Olivier Ezratty, 2023

Article | Published: 06 December 2023

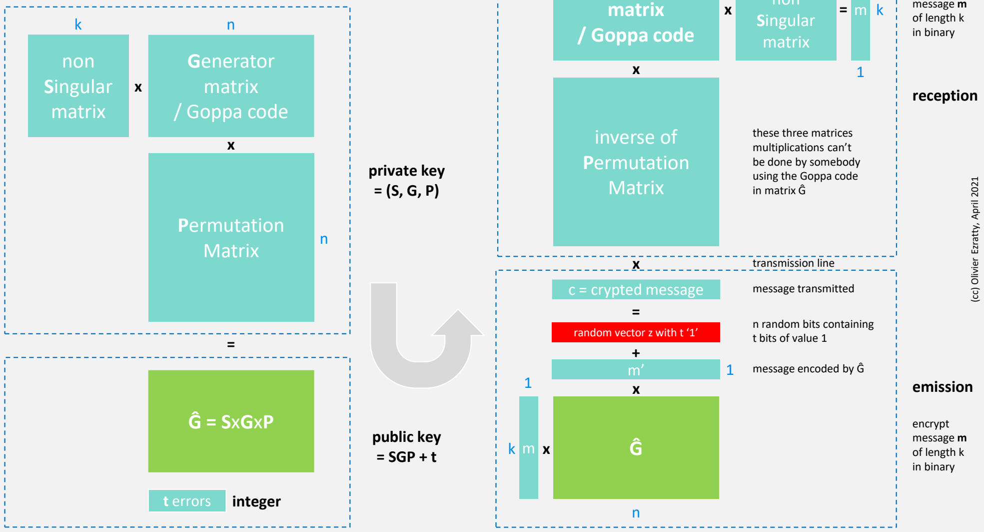
Logical quantum processor based on reconfigurable atom arrays

Dolev Bluvstein, Simon J. Evered, Alexandra A. Geim, Sophie H. Li, Hengyun Zhou, Tom Manovitz, Sepehr Ebadi, Madelyn Cain, Marcin Kalinowski, Dominik Hangleiter, J. Pablo Bonilla Ataides, Nishad Maskara, Iris Cong, Xun Gao, Pedro Sales Rodriguez, Thomas Karolyshyn, Giulia Semeghini, Michael J. Gullans, Markus Greiner, Vladan Vuletić & Mikhail D. Lukin ✉

Nature (2023) | Cite this article

cybersecurity solutions

code-based cryptography



classical technologies

QRA
quantum resistant cryptography
classical cryptography resisting to quantum algorithms

PQC
post-quantum cryptography
new classical asymmetric keys and signatures resisting to quantum algorithms

symmetric keys
classical cryptography already resistant to quantum algorithms (AES, …)

mathematical protection

quantum technologies

Quantum Key Distribution (QKD)

first generation
prepare-and measure based,
protects public keys sent through optical links, use trusted nodes as repeaters

second generation
entanglement based, protects public keys sent through optical links, use memory based repeaters

Quantum Conference Key Agreement
entangled quantum keys shared with more than 2 parties.

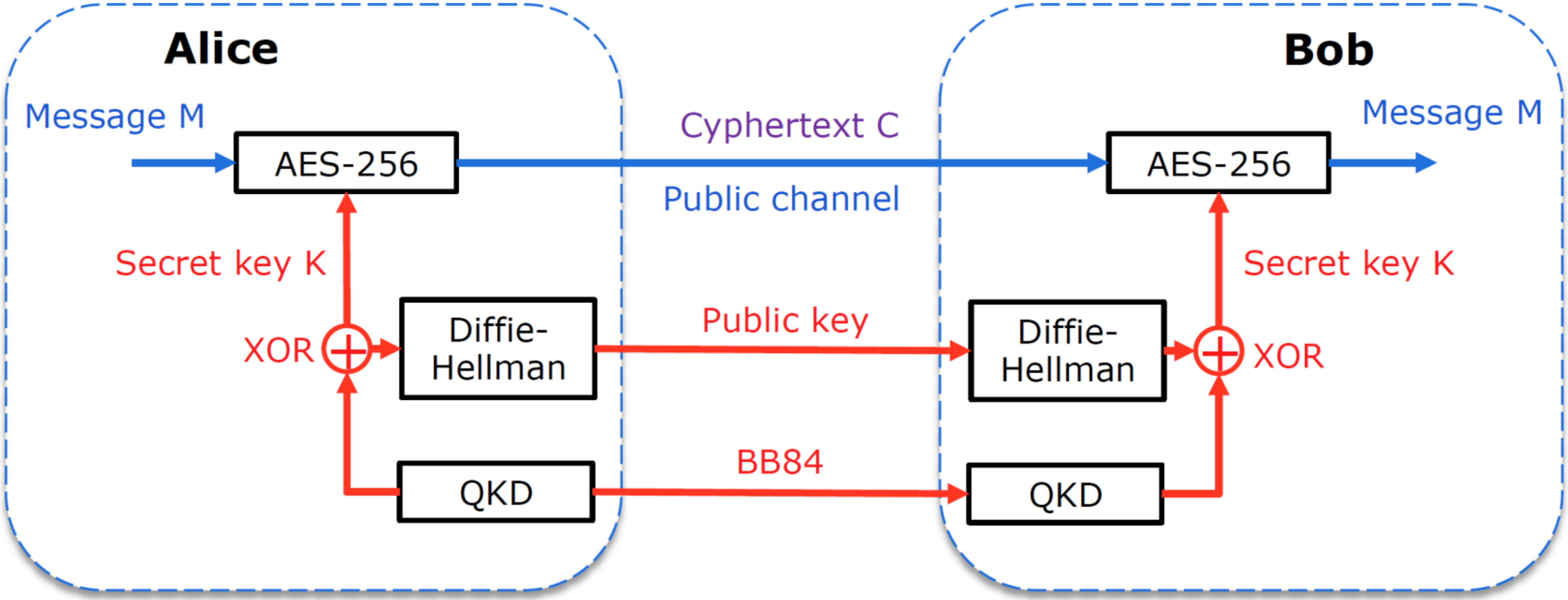
entanglement distribution
entangled photons distribution to multiple parties

QRNG
quantum random key generators
ensure the quality of public keys in classical and quantum cryptography

quantum repeaters
with quantum memory and entanglement swapping, enable entanglement sharing over long distances

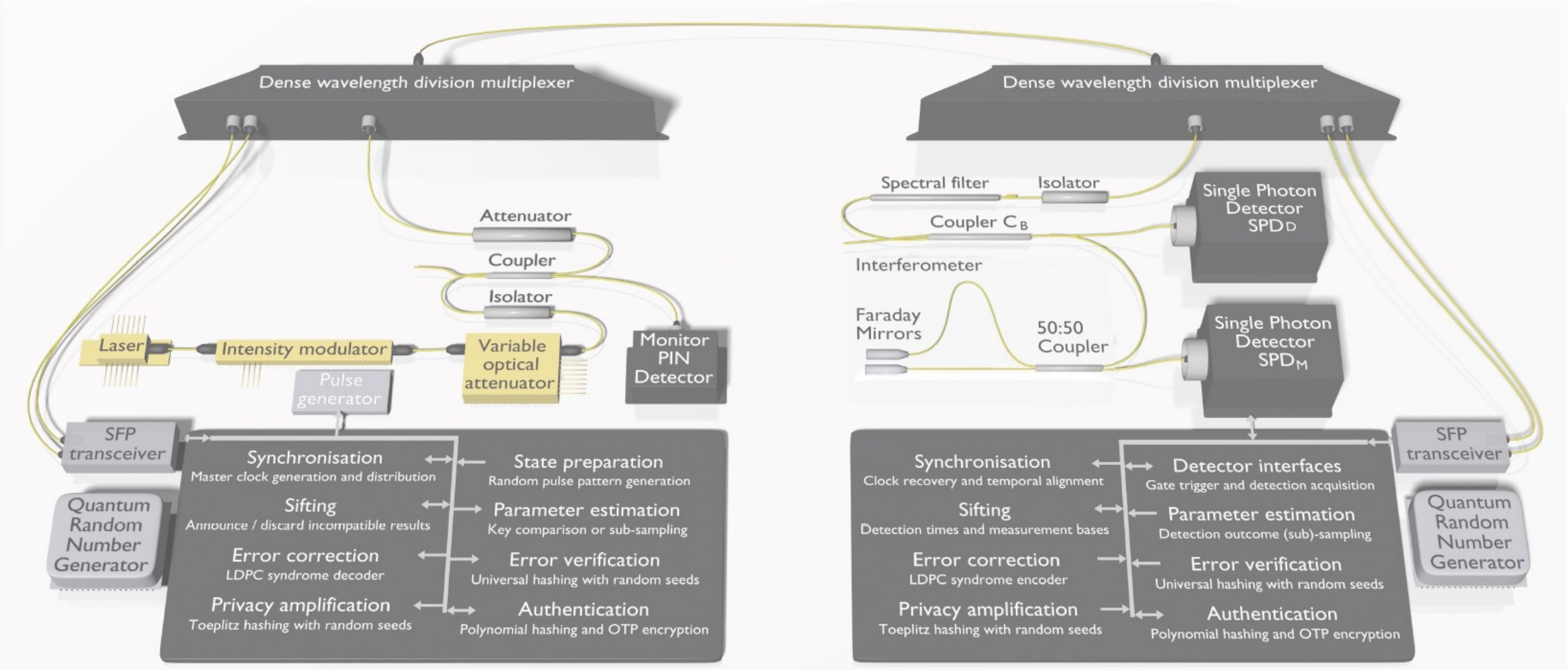
physical protection

QKD principle



source: How to Quantum-Secure Optical Networks? by Helmut Griesser, ADVA Optical Networking SE, 2016 (31 slides).

typical QKD hardware settings

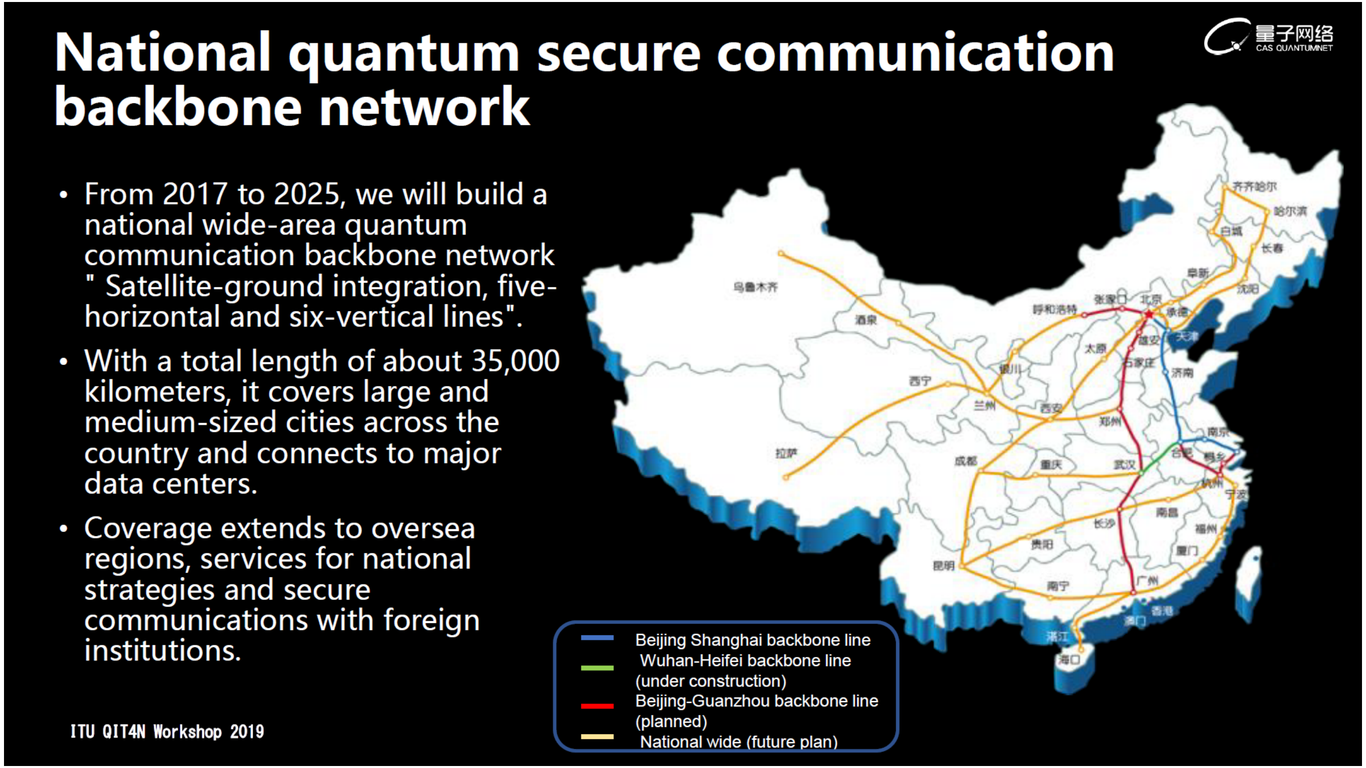


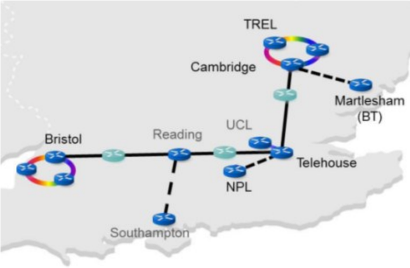
QKD in China

Beijing-Shanghaï Network
2013-2016, 32 nodes, 2,000 km of QKD secured fiber link, 20 kbits/s

31,000 km extension, 2017-2025

10,000 km deployed as of 2023





Netherlands
Delft, Leiden, Amsterdam, The Hague OpenQKD project 2019

Germany
QKD project, 165M€
2019-*

Tchekia
OpenQKD project
2019

Poznan
2021

Denmark
Dantze Bank
DTU
2022

Ireland
2022

Cambridge – London - Bristol 2018

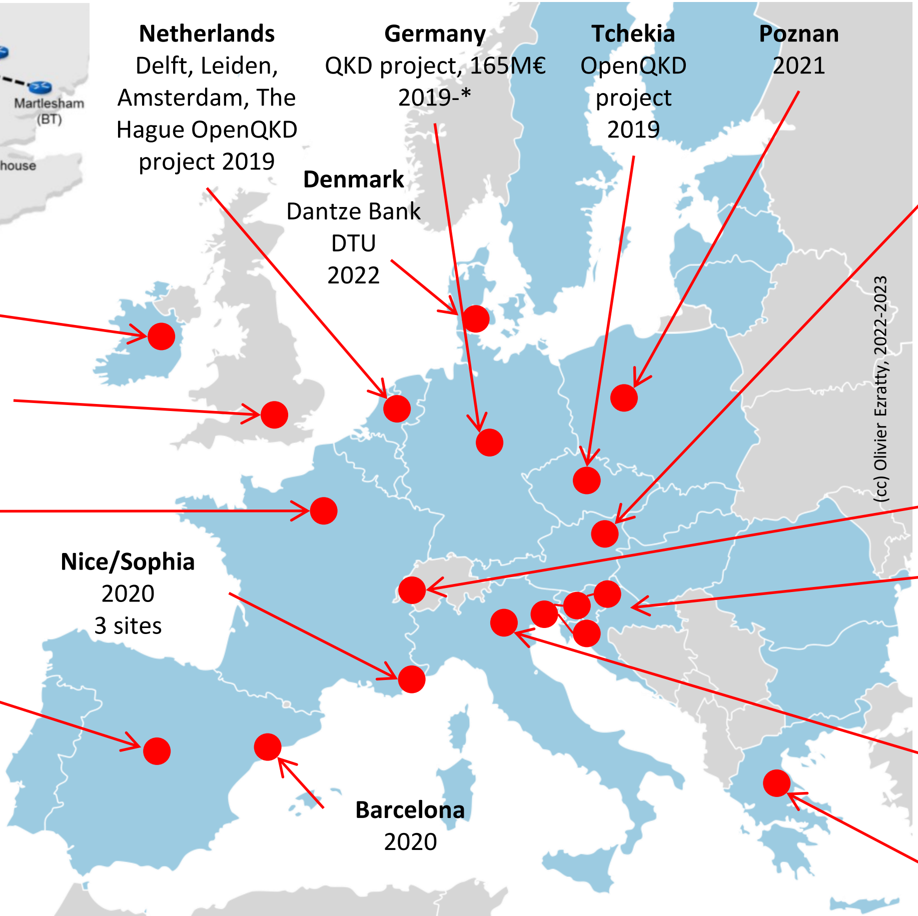
Ile de France
2020-*
OpenQKD project

Nice/Sophia
2020
3 sites

Madrid
2018
Telefonica & Huawei

Canaries
2007/2010
144 km free to air

Barcelona
2020



Vienna
2008
SECOQC, 5 nodes, 20/25 km

Geneva
1993, 1995, 2007, 2018 (400 km)

Italy-Slovenia-Croatia network

Italian Quantum Backbone (IQB) 1,850 km QKD link connects Turin, Milan, Bologna, …, a 150 km fiber reaches Modane in France, and connects to Grenoble, Lyon and Paris, then Europe + Padua satellite/ground QKD experiment

Athens
2019
OpenQKD project DataCom

satellite based QKD

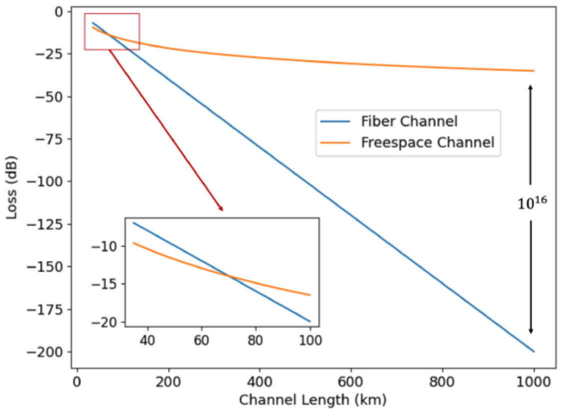


FIG. 10 Typical losses in fiber and free-space channels. The attenuation parameter of fiber is $\sim 0.2\ dB/km$. The parameters of free-space channel are based on the design of Micius satellite. The free-space channel shows advantage for a distance over $\sim$ 70 km

how photon losses compare between fiber and freespace channel using satellite. Source: Micius quantum experiments in space by Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng and Jian-Wei Pan, August 2022 (53 pages).

quantum random number generators

photons counting

photons arrival time

vacuum fluctuations

phase noise

radioactive decay

self-certified SDI QRNG

qubit Bell states measurements

other

TECH / SAMSUNG / MOBILE

Samsung’s Galaxy Quantum 2 has quantum cryptography built in

/ Featuring the world’s smallest quantum random number generator

By Sam Byford

Apr 13, 2021, 8:35 AM GMT+2 | 0 Comments / 0 New

Samsung Galaxy Quantum 2

- Released 2021, April 23
- 176g, 8.1mm thickness
- Android 11, One UI 3.1
- 128GB storage, microSDXC

1.8% 1,084,743 HITS

190 BECOME A FAN

6.7"	64MP	6GB RAM	4500mAh
1440x3200 pixels	2160p	Snapdragon 855+,	Li-Po

OPINIONS COMPARE PICTURES

2.5 mm

GSMArena

Peter 14 November 2023 Huawei HarmonyOS

At the 2023 Digital Technology Ecology Conference carrier China Telecom presented a modified version of the Huawei Mate 60 Pro with quantum security. This builds on work from last year when it unveiled a Mate 40E with Quantum SIM support.

The new Mate 60 Pro can secure voice calls (VoLTE), messages as well as file transfers. The way it works is that a Quantum Key Distribution algorithm generates a new key before you start a new secure call, then this key is shared with the recipient so that their phone can decode the call (or message or file, etc.). The users must use secure authentication first to verify their identity.

Security is ensured not just by the Quantum SIM card, there is also a custom chipset and the algorithm, which is a closely-guarded secret. The recipient must have similar hardware before the call/message/file goes through.

what the quantum SiM could embed:

- **PQC cryptography logic.**
- **some QRNG to create the PQC keys.**

国盾量子 QuantumCTek

there is no such thing as a QKD for smartphones! It requires some photonic link.

and QKD is not an « algorithm »

post-quantum cryptography

Name of Cryptographic Algorithm	Type	Purpose	Resilience against Quantum Computer
AES-256	Symmetric Key	Encryption	Ok but larger key sizes needed
SHA-256, SHA-3		Hash function	Ok but larger output needed
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed
Code-based (Mc Eliece)	Public Key	Encryption	Believed
Multivariate polynomials	Public Key	Encryption; signature	Believed
Supersingular elliptic curve isogenies (SIDH)		Encryption; possibly signature	Believed
ECDSA, ECDH (Elliptic Curve Crypto)	Public Key	Signatures, Key exchange	No longer secure
RSA	Public Key	Signatures, Key establishment	No Longer secure
DSA (Finite Field Crypto)	Public Key	Signatures	No Longer secure

High level of confidence

Under investigation

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

threatened by quantum algorithms

NIST Search CSRC CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

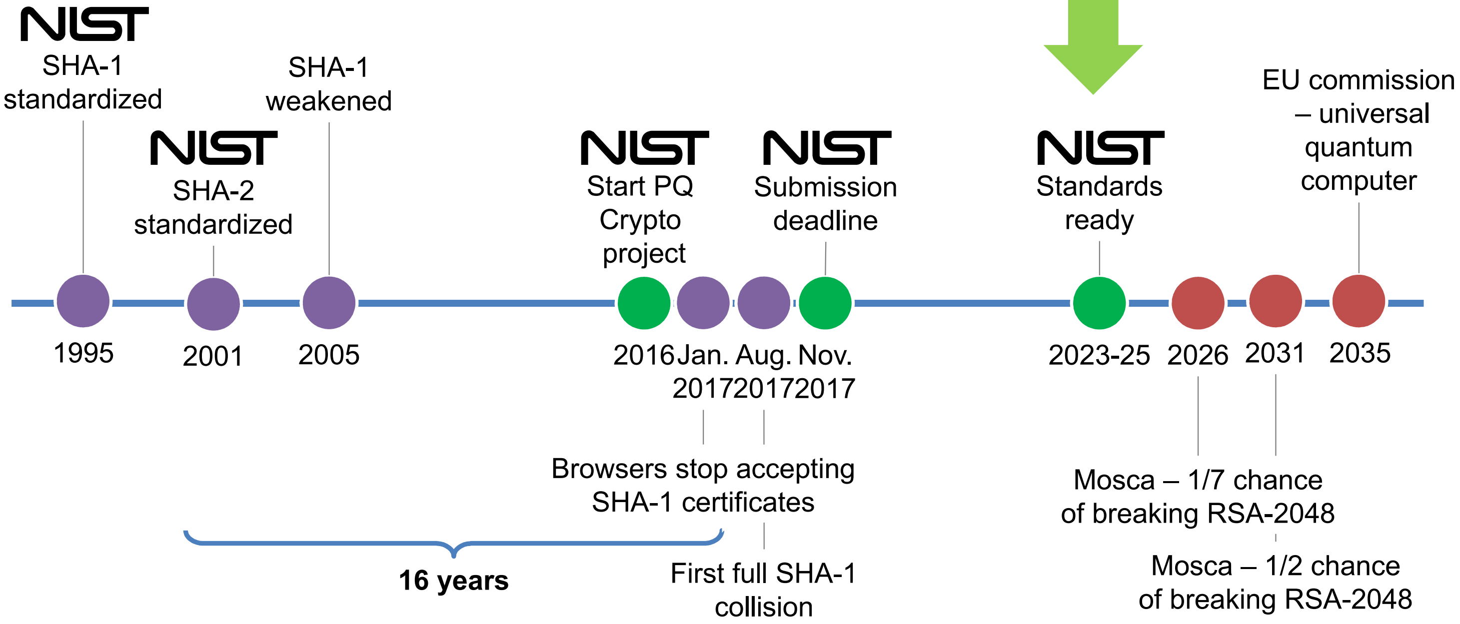
UPDATES 2023

Comments Requested on Three Draft FIPS for Post-Quantum Cryptography

August 24, 2023

NIST requests comments on the initial public drafts of three Federal Information Processing Standards (FIPS):

1. FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
2. FIPS 204, *Module-Lattice-Based Digital Signature Standard*
3. FIPS 205, *Stateless Hash-Based Digital Signature Standard*



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
	CRYSTALS-KYBER	**USA**: SRI. **Canada**: U. Waterloo. **Europe**: Radboud U. Netherlands, Ruhr U. 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	CRYSTALS-DILITHIUM	**USA**: Florida Atlantic U. **Switzerland**: ETH Zurich. **Europe**: CWI Netherlands, Ruhr U. Bochum, MPI, ENS Lyon.	IBM Research Europe Google, PQShield
	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

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
	SPINCS+	**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

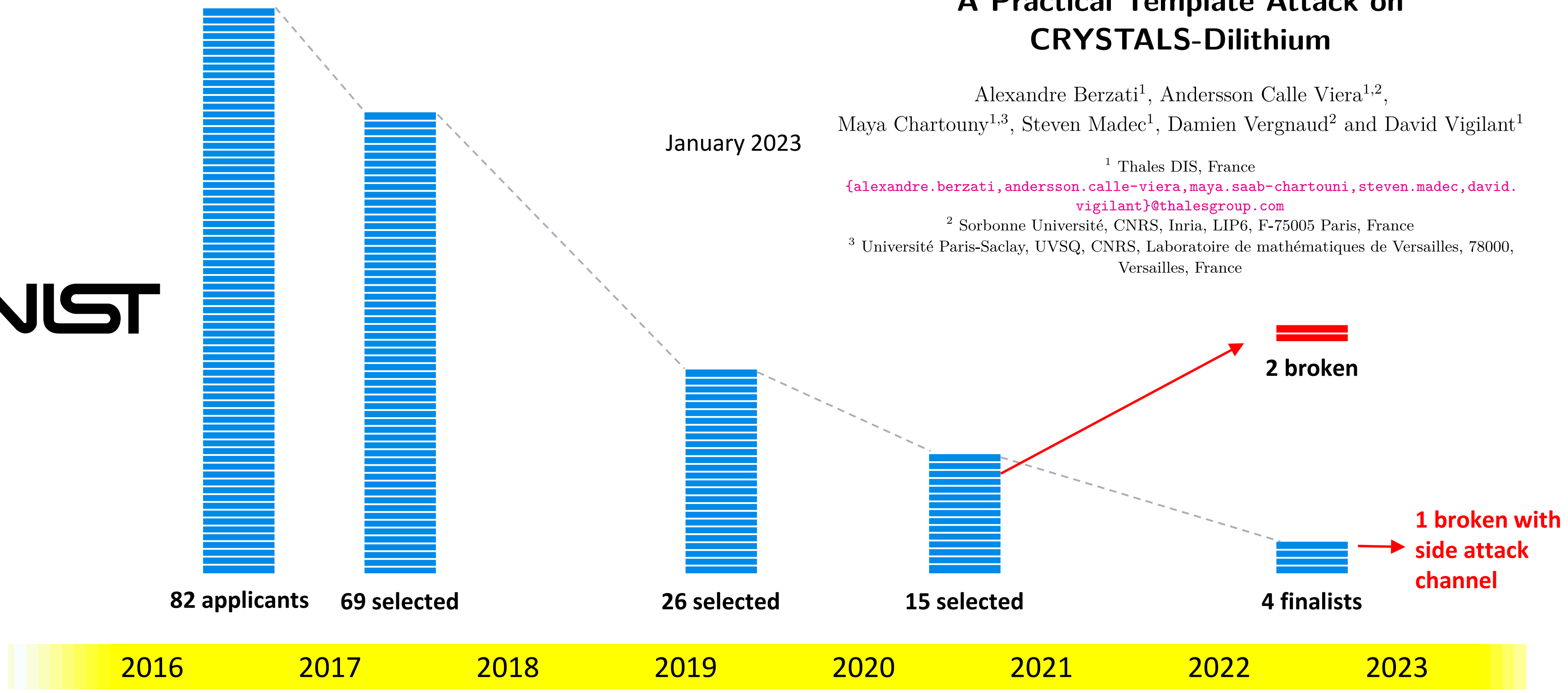
PQC NIST competition

January 2023

A Practical Template Attack on CRYSTALS-Dilithium

Alexandre Berzati[1], Andersson Calle Viera[1,2], Maya Chartouny[1,3], Steven Madec[1], Damien Vergnaud[2] and David Vigilant[1]

[1] Thales DIS, France
{alexandre.berzati,andersson.calle-viera,maya.saab-chartouni,steven.madec,david.vigilant}@thalesgroup.com
[2] Sorbonne Université, CNRS, Inria, LIP6, F-75005 Paris, France
[3] Université Paris-Saclay, UVSQ, CNRS, Laboratoire de mathématiques de Versailles, 78000, Versailles, France



cryptography PQC

post-quantum cryptography

public key cryptography resisting to quantum algorithms

CRYPTONEXT SECURITY
Post-Quantum
PQSecure
QuBalt
ISARA
PQSHIELD

CRYPTOMATHIC
evolution
Qubitl
QAN
ZY4
Ambit Inc

AGILEPQ
Quantropi
QUANTUM IMPENETRABLE
PATERO QUANTUM SECURE COMMUNICATION
HEAAN CRYPTO LAB
Haqien

FlipsCloud Quantum Level Encryption
alternatio
QuantiCor
BLAKFX IN MATH WE TRUST
Qabacus
CRYPTO QUANTIQUE
SECURITY INNOVATION

Entrust Datacard®
agnostiq
cyph
CRYPTO4A
CYFERALL
infotecs®

DENCRYPT
GO QUANTUM
QuSecure
SSH
ravel
fragmentiX® QUANTUM SAFE STORAGE SOLUTIONS

EVIDEN an atos business
Microsoft
IBM
SANDBOXAQ

quantum keys QKD / BB84

protects symmetric keys with optical link (fiber or sat)

cryptography QKD

Quintessence Labs Data Uncompromised
NANO-META TECHNOLOGIES, INC.
Q→NU
Qubitekk
QuantLR
循态量子 XT Quantech

KEEQUANT
nu QUANTUM
KETS
国盾量子 QuantumCTek
QRATE QUANTUM COMMUNICATIONS
asky

ciena
S-FIFTEEN SPACE SYSTEMS QUANTUM-SAFE COMMUNICATION
MagiQ
ANAMETRIC
nodeQ
QEYnet

Ki3PHOTONICS Technologies
QSIM+
Qunnect
QUANTUMXCHANGE
Mt Pelerin
SMARTS
AegiQ

Crypta Labs
QUSIDE
Q*bird quantum connectivity
Qubit Reset
LUXQUANTA
QTI Quantum Telecommunications Italy

ArQit
infotecs
LUXQUANTA
ICARUS QUANTUM
LQUOM Quantum Communication
Cryptolab
QULABS

SAMSUNG
TOSHIBA
amazon
IDQ
qtlabs
CRAFT PROSPECT

key takeaways

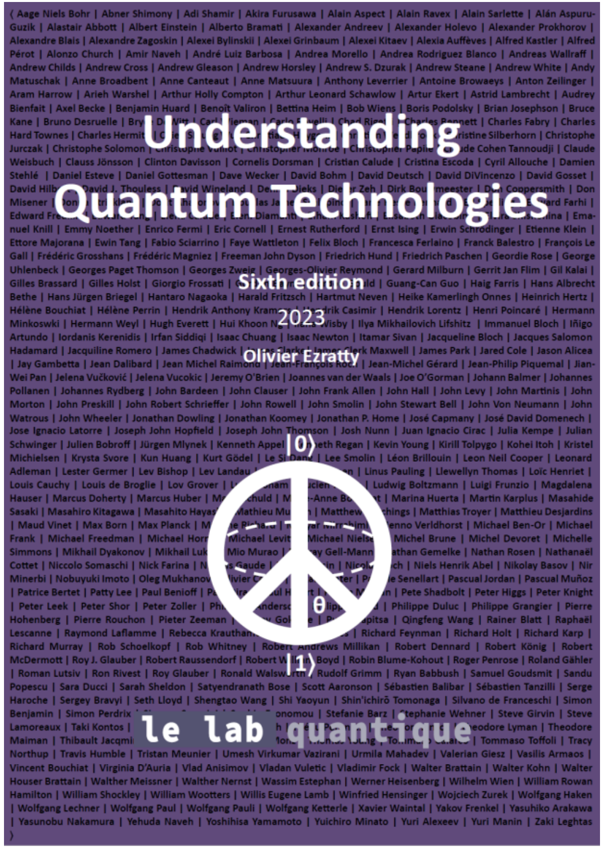
the cure (PQC) may be more dangerous than the ill (Shor)

new classical threats also loom around

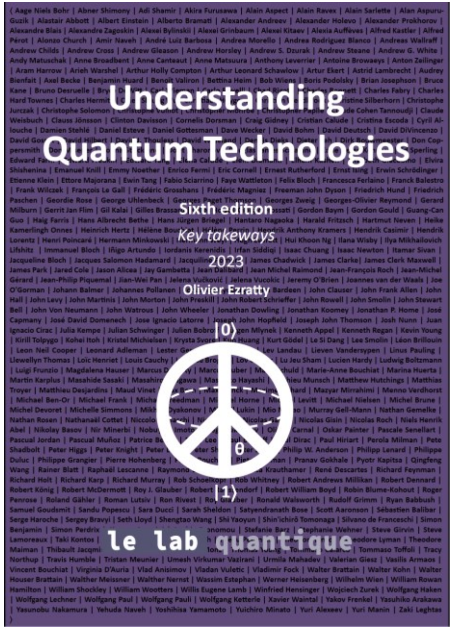
PQC will be deployed but it requires some care

QKD is interesting for « strategic » applications

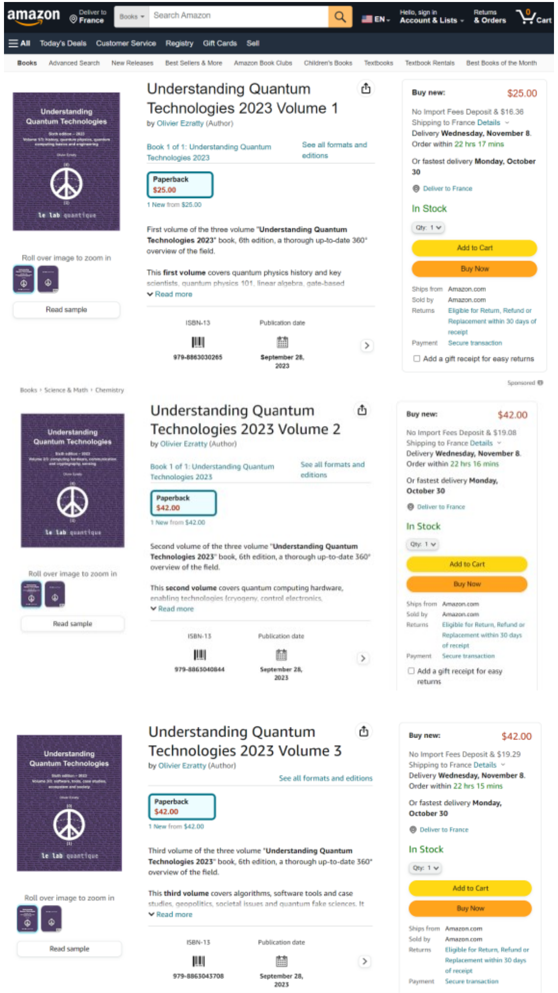
entangled based QKD is the way to build a quantum Internet



2023, 1,366 pages
free PDF download



2023, 24 pages
free PDF download



discussion

various QKD protocols

Protocol	Type	Approach	Year
BB84	DV	Prepare-and-measure	1984
E91	DV	Entanglement-based	1991
BBM92	DV	Entanglement-based	1992
GG02	CV	Prepare-and-measure	2002
DPS	DV	Prepare-and-measure	2002
Decoy-state	DV	Prepare-and-measure	2003–2005
SARG04	DV	Prepare-and-measure	2004
COW	DV	Prepare-and-measure	2005
MDI	DV/CV	Prepare-and-measure	2012
TF	DV	Prepare-and-measure	2018
PM	DV	Prepare-and-measure	2018