Opinions Libres
le blog d'Olivier Ezratty

Decode Quantum avec Romain Alléaume de Telecom Paris

Dans ce **41e épisode** des entretiens **Decode Quantum**, toujours avec **Fanny Bouton** et en partenariat avec Frenchweb, nous accueillons **Romain Alleaume** (crédit portrait : Aurore Drucbert).

Romain est enseignant-chercheur à **Telecom Paris**, maintenant installée à Palaiseau en face du centre de recherche C2N du CNRS et de l'Université Paris-Saclay. Diplômé de l'ENS Paris, il a fait une thèse de doctorat en 2004 à l'ENS Cachan et à l'Université Paris VI. Il a alors rejoint Telecom Paris pour y coordonner la recherche en QKD dans le cadre du projet européen SECOQC ainsi que de nombreux projets nationaux et internationaux. Ses recherches visent à permettre l'industrialisation des communications quantiques à base de QKD dans le cadre du pilier communication du quantum flagship européen (CIVIQ, OpenQKD et EuroQCI). Il a aussi cofondé la start-up **SeQureNet** (2008-2017) dont il nous racontera les péripéties. Enfin, Romain est aussi responsable d'une option quantique de dernière année à Telecom Paris sur l'information quantique.

Voici les principaux éléments de discussion de cet entretien et les éventuels liens associés :

- Comment il est tombé dans la marmite du quantique pendant tes études ? Il aimait les mathématiques, la physique et la philosophie. Il était aussi influencé par son père qui était physicien spécialisé en cristallographie à Bordeaux. Il était abonné à "La Recherche". Il avait réalisé un projet TIPE sur l'intrication quantique en classe préparatoire aux grandes écoles. Il a alors choisi la physique quantique comme option à l'ENS avec **Jean-Michel Raymond** comme enseignant. À cette occasion, il a découvert **Jean-François Roch** et **Alain Aspect**.

- Le sujet précis de ta thèse soutenue en 2004 portait sur la cryptographie quantique exploitant des sources de

photons uniques utilisant deux types de sources : des centres colorés de diamants (NV centers) et des molécules. Voir **Réalisation expérimentale de sources de photons uniques, caractérisation et application à la cryptographie quantique** (198 pages) sous la direction de **Jean-François Roch** que nous avons reçu dans le **32e épisode** de Decode Quantum en 2021. Dans le jury de thèse, il y avait notamment **Philippe Grangier** comme examinateur ainsi que **Jean-Michel Raymond**.

- Comment se positionnent les nombreuses sources de photons, par exemple vis à vis des quantum dots créés par **Pascale Senellart**, qui avait bouclé sa thèse en 2001. Les méthodes utilisant des lasers à impulsion et la génération de moins d'un photon par impulsion par atténuation. Les lasers semiconducteurs. La génération d'états cohérents semi-classiques. Les lois de distribution des photons (loi de Poisson). Les "mitraillettes à photons" utilisant des émetteurs uniques comme les quantum dots de Quandela, les molécules comme dans sa thèse, les atomes de Rydberg, les centres NV. La qualité de la source est caractérisée par la statistique d'émission des photons et la qualité des états cohérents. Les sources cohérentes de Quandela sont notamment adaptées au calcul quantique.

- Les sources qui produisent des paires de photons intriquées comme celles de **Sara Ducci** au MPQ. Utilisent le "heralding", qui consiste à détecter l'un des deux photons pour annoncer l'autre. Les expériences d'échantillonnage de bosons réalisées en Chine utilisent cela.

- La distribution de clés quantiques (QKD) n'a pas besoin de photons uniques. Les capteurs quantiques en ont besoin.

- Lors de sa thèse, Romain a travaillé quatre mois dans le laboratoire de l'entreprise **MagiQ**. Il décrit son activité.

- Son activité de chercheur à Telecom ParisTech dans de nombreux projets (PROSPIQ (2006-2009), SEQURE (2007-2010) et le projet franco-canadien FREQUENCY puis le projet FP7 Q-CERT (2008-2012) et un projet de QKD dans des réseaux télécoms (ANR Quantum-WDM, 2012-2015). Le projet européen SECOCQ mené avec **Philippe Grangier**. Il s'agissait de projets de QKD et de leur sécurité d'ensemble.

- Il a aussi travaillé avec **Eleni Diamanti** lorsqu'elle était chercheuse à Telecom Paris avant de passer au CNRS LIP6.

- Nous évoquons l'aventure de la startup **SeQureNet** à laquelle il a participé entre 2008 et 2017 avec **Sébastien Kunz-Jacques** (ex ANSSI et qui y est revenu) et **Paul Jouguet**. Sur la base d'un système développé à l'IOGS et chez Thales dans des thèses, l'ambition était de créer de bons correcteurs d'erreurs, sur la base du travail d'**Anthony Leverrier** (maintenant Inria) qui avait fait sa thèse à Télécom Paris. La percée dans sa thèse a été mise en œuvre par la startup. Elle permettait de gagner en distance pour la distribution de clés quantiques, passant de 20 km à 100 km. La mise au point a duré 3 à 4 ans. Leur CV-QKD, Cygnus, a été alors lancée en 2012. Mais le projet n'a pas vraiment abouti à cause, notamment, d'oppositions en France mais aussi aux USA, notamment des agences étatiques qui voulaient éviter que la cryptographie dépende de la couche physique. La maturité était trop faible et les systèmes étaient et ne sont toujours pas certifiables.

- Les projets chinois de QKD n'ont pas influencé le marché du reste du monde. Mais le satellite Micius a marqué les opérateurs télécoms et motivé le lancement du projet EuroQCI dans le flagship quantique européen. Orange et Nokia sont devenus des acteurs importants.

- Romain explique comment s'y retrouver dans les projets CIVIQ (2018-2021), OpenQKD et EuroQCI. CIVIQ est le projet phare. OpenQKD vise à déployer des testbeds (Madrid, Berlin et Paris). EuroQCI porte une ambition plus futuriste d'Internet quantique constitué de réseaux quantiques avec des répéteurs.

- Romain évoque aussi sa participation à la normalisation de la QKD comme à l'ETSI. C'est un verrou pour l'industrialisation et pour l'évaluation. L'agence de sécurité allemande BSI est impliquée et associée à un groupe d'expert international. La standardisation porte aussi sur les questions d'interopérabilité.

- Nous passons à son activité d'enseignement à Telecom Paris et à l'option qu'il anime, ses élèves et son évolution dans le temps. L'enseignement quantique démarre par des cours de physique quantique en première et seconde années, ne serait-ce que pour comprendre le fonctionnement des semi-conducteurs. Les algorithmes quantiques et Qiskit sont couverts en première année. La seconde comprend une filière d'information quantique QuEng-3A qui dure 6 mois et est complétée par 6 mois de stage en entreprise ou dans un laboratoire de recherche. Elle couvre l'informatique quantique, l'algorithmique et la cryptographie quantique. On n'y trouve qu'environ 5 élèves par an sur 150 élèves par promotion. Ils s'appuient aussi sur les masters QPCS et ARTEQ du plateau de Saclay. Deux tiers des élèves vont ensuite faire des thèses fondamentales ou plus industrielles (CIFRE) et le reste deviennent ingénieurs dans l'industrie.

https://synapses.telecom-paris.fr/catalogue/2020-2021/parcours/1390/QENG-3A-option-quantum-engineering-s1

Cet article a été publié le 16 mars 2022 et édité en PDF le 17 mars 2022.