Opinions Libres
le blog d'Olivier Ezratty

Decode Quantum avec Grégoire Ribordy d'IDQ

Dans ce 67e épisode des entretiens Decode Quantum, **Grégoire Ribordy** qui dirige la société IDQ évoque la thématique de la cryptographie quantique. Je suis toujours avec ma comparse **Fanny Bouton** d'OVHcloud.

Grégoire Ribordy est cofondateur et PDG d'IDQ, ou ID quantique, l'une des sociétés les plus anciennes des technologies quantiques avec D-Wave, créée en 2001. Avant cette création, il était chercheur dans le Groupe de Physique Appliquée de l'Université de Genève entre 1997 et 2001 où il a développé la technologie de cryptographie quantique (QKD) avec plusieurs brevets à la clé dans le domaine. Auparavant, entre 1995 et 1996, il avait travaillé dans la division R&D de Nikon à Tokyo. Avec lui nous allons faire un grand tour historique, technologique et mondial sur l'histoire de la QRNG et de la QKD.

Voici le synopsis et les liens utiles de cette discussion :

Comment notre invité a découvert le quantique ? Cela tient du hasard en 1997 au moment du démarrage de sa thèse avec Nicolas Gisin. Il était tombé sur son groupe de recherche par hasard. Auparavant, il avait suivi des cours de physique quantique lors de ses études. Il était intéressé par la proximité entre la recherche

fondamentale et les premières applications de la QKD.

Sa rencontre avec Nicolas Gisin qui est une grande personnalité scientifique du domaine de la QKD et est devenu un cofondateur d'IDQ. Ce grand chercheur avait (et a toujours) la capacité de mélanger théorie, application et expérience. C'est un physicien qui avait fait de la théorie et s'intéressait aux expériences et applications. Il travaillait initialement pour Swisscom sur les fibres optiques télécoms. La QKD lui a permis de mélanger la théorie et la pratique.

Sa thèse : "Experimental quantum key distribution" qui portait notamment sur les détecteurs de photons uniques. Il était le second thésard sur le sujet dans l'équipe de Nicolas Gisin. Elle faisait suite à la publication de l'article **Quantum Cryptography** par Charles Bennet, Gilles Brassard et Artur Ekert dans Scientific American en 1992. Le comptage de photons uniques opérait d'abord dans le visible puis a été appliqué à l'infrarouge qui est utilisé dans les fibres optiques des opérateurs télécoms, notamment en 1550 nm, qui remplaçait le 1310 nm qui était généré par le germanium. Il fallait simplifier le refroidissement avec un effet thermoélectrique. En liaison avec sa thèse, il a alors publié **Performance of InGaAs/InP Avalanche Photodiodes as Gated-Mode Photon Counters** par G. Ribordy, J. D. Gautier, H. Zbinden, and N. Gisin, 1998 (16 pages).

Les principes et l'histoire de la cryptographie quantique. Elle démarre avec Bennet et Brassard avec leur protocole BB84 de 1984 dont les dérivés sont toujours d'actualité et sont au cœur de l'offre d'IDQ. L'idée était restée en veille pendant pas mal de temps.

Le protocole BB84 consiste à préparer des photons dans deux bases différentes, puis à effectuer une mesure. La mesure perturbe les photons. Grégoire utilise l'analogie de la partie de tennis. Le message est écrit sur une balle de tennis. Si quelqu'un intercepte la balle de tennis et la ré-envoie, on peut récupérer le message. Ici, on utilise des bulles de savon fragiles qui sont impossibles à intercepter.

La QKD s'appuie sur l'émission de photons uniques. C'est ce qui rend le protocole quantique, en plus de la mesure des photons dans des bases de polarisation différentes à 0° et à 45°. On peut aussi utiliser la phase des photons, qui est plus facile à préserver dans les fibres optiques. Le transfert des informations sur les bases est réalisé de manière classique. Les mesures sont faites au hasard puis l'échange des bases permet de faire le tri a posteriori dans les mesures effectuées.

Dans le protocole d'Artur Ekert, il n'y a pas d'envoi d'information. La source des photons est entre Alice et Bob, avec deux récepteurs, un de chaque côté. La clé est générée de manière totalement aléatoire grâce à la mesure d'états intriqués. La source pourrait cependant être placée à côté d'un des récepteurs. L'écrasement du paquet d'ondes est considéré comme étant équivalent entre les modèles prepare-and-measure et à base d'intrication.

Le choix de l'aléatoire est actif (dans BB84, avec des bases de photons déterminées par un générateur de nombres aléatoires qui peut être lui-même quantique) ou passif (Ekert, E91). On peut aussi avoir des choix passifs dans BB84. Le récepteur de Bob peut avoir un séparateur de faisceaux avec deux polariseurs.

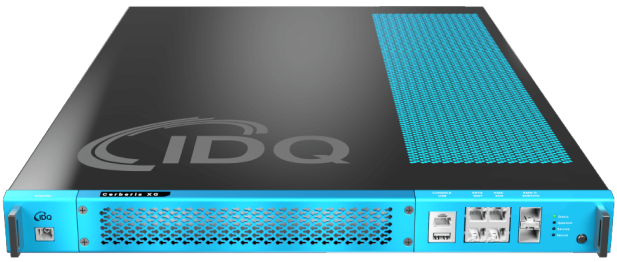
L'histoire de la création d'IDQ. En 1998, la société Magic Technologies était lancée par un investisseur américain. Il avait engagé des physiciens théoriciens et envisageait de créer un ordinateur quantique. C'était un peu tôt ! Puis il est allé voir du côté de la distribution quantique de clés et fait le tour des laboratoires. L'investisseur a alors visité le groupe de recherche de Nicolas Gisin. Grégoire a manifesté son intérêt pour la création d'une entreprise. Finalement, avec Nicolas Gisin et Hugo Zbinden, ils ont décidé de créer l'entreprise tous seuls et sans investissement extérieur. C'était une société anonyme avec un investissement de départ de l'équivalent de 100K€.

IDQ s'est-elle construit et développé avec trois gammes de produits : générateurs de nombres aléatoires, détecteurs de photons et modulateurs/démodulateurs de QKD « prepare and measure ».

Détecteurs de photons : c'est le premier business historique de la société. En octobre 2001, ils avaient reçu une commande de 6 détecteurs par l'Université de Boston, alors que l'entreprise n'était pas encore lancée. Ils ont accepté la commande avant même de créer la société. Il s'agit de détecteurs III/V de type InGaAs. Cette activité existe toujours et représente environ 30% du chiffre d'affaires d'IDQ. La technologie a évolué et utilise maintenant des nanofils supraconducteurs (SNSPD). Ils ne détectent pas de "dark photons" (photons thermiques parasites) et ont une très bonne résolution temporelle. Ils fonctionnent à environ 4K. Ce produit leur permet de rester en contact de la recherche.

Générateurs quantiques de nombres aléatoires (QRNG). Le premier client intéressé était Swisscom, qui à l'époque s'appelait Telecom PTT avant sa privatisation. La société avait coupé les crédits de recherche à l'Université de Genève. Mais ils avaient besoin de produire des clés classiques. IDQ a alors lancé un premier produit de la taille d'une brique de lait qui était vendu 10K€ à l'époque. Il générait de l'intérêt mais il y avait un fort besoin de miniaturisation et de baisse de prix. Puis via une collaboration avec EPFL, ils lançaient en 2004, un produit tenant dans une boite d'allumettes et commercialisé autour de 1000€. Il couvre les marchés de la sécurité et celui des casinos en ligne et des loteries qui se dématérialisaient. Cela fonctionne avec l'émission de photons qui traversent un miroir semi-réfléchissant et réfléchissent les photons de manière aléatoire à 50%/50%. La source de lumière est un laser atténué qui émet de temps en temps un photon. Les doubles photons sont automatiquement éliminés. Ce produit a été commercialisé pendant 10 ans. L'étape suivante en 2018 a été la création d'un chip de 2,5mm de côté. Il est intégré dans des smartphones Samsung Galaxy commercialisés en Corée et avec le partenariat avec SK Telecom qui est un de leurs actionnaire. C'est utilisé pour de la cryptographie qui a besoin de clés aléatoires. Le hasard lié aux photons est meilleur que les techniques habituelles qui exploitent des paramètres systèmes divers (thermiques, utilisation du réseau, …). Avec la QRNG photonique, il n'y a pas de préchauffe nécessaire. Leur QRNG n'est pas « device independant » qui certifie la confiance dans l'aléatoire et le non déterminisme, qui reste peu pratique et trop cher. Cette activité représente environ 20% du CA d'IDQ.

Infrastructure de QKD, qui représente une grosse partie de leurs revenus. Leur premier système a été vendu en 2004 à l'Université de Genève, sans logiciel au départ. Puis, ils ont développé les logiciels traitant les résultats en temps réel. L'idée était de produire des clés secrètes et "fraiches" à deux endroits, et de vérifier qu'elles ne sont pas interceptées. C'est de la cryptographie symétrique. Elle s'affranchit d'hypothèses computationnelles sur la protection des clés (publiques). La sécurité est basée sur la physique. Ils en sont aujourd'hui à leur quatrième génération de systèmes. La première application commerciale date de 2007. Elle a servi au dépouillement d'élections dans le Canton de Genève. L'application était quelque peu artificielle mais permettait d'illustrer la protection de l'intégrité des données. Puis ils ont commercialisé leur offre à des banques et des gouvernements pour des liaisons point à point. Cela les protège contre les attaques d'interception des données « store now – decrypt later » (SNDL). Un gros changement est intervenu autour de 2015-2016 lorsque Google a commencé à parler d'ordinateurs quantiques (avec D-Wave). Puis est venu un papier de la NSA indiquant l'émergence d'un risque sur la cryptographie classique à clés publiques, validant le risque quantique puis la compétition PQC lancée par le NIST en 2016. En pratique, il y a une hybridation entre PQC (génération de clés asymétriques protégées contre le cassage par ordinateurs quantiques) et QKD (clés symétriques). SK Telecom associe de la QKD qui protège le cœur des réseaux et la PQC et la QRNG qui protège les liaisons hertziennes (5G).



Nous évoquons le **récent rapport** de l'ANSSI et de leurs collègues UK/Allemagne/Suède qui est clairement réticent à la QKD. Le rapport est bien écrit et sans erreurs de sens, ce qui permet de discuter de manière objective. Il met en avant un point valide concernant la certification. Mais les choses bougent, notamment via l'Asie (Chine, Japon, Singapour et en Corée). La Corée a lancé le premier processus de certification en avril 2023. D'autres problèmes mentionnés sont liés à une incompréhension sur la clé d'authentification des parties prenantes établie pour une première session. En fait, il est facile d'établir ce secret initial. On devrait parler de « Quantum secret expansion ».

Nous évoquons ensuite la manière dont les USA et l'Europe s'intéressent aux communications quantiques. Les USA se focalisent sur les usages futurs qui auront besoin de génération d'intrication et de répéteurs quantiques. L'Europe doit faire attention à ne pas se faire déborder et à bien financer la recherche dans ces domaines.

Puis nous passons à la roadmap industrielle d'IDQ et ses partenariats. La société est dans un mode "IT" avec des versions nouvelles par trimestres. Elle apporte des améliorations graduelles à ses systèmes. En parallèle, elle collabore avec les fabricants d'autres composants, comme les mémoires quantiques. Ils continuent de travailler avec l'Université de Genève. Ils ont aussi des partenariats technologiques avec des "consommateurs de clés" comme Nokia qui produit des équipements de transport optique avec des interfaces entre boitiers de

chiffrement et de QKD. Le tout vise en à en baisser les barrières d'adoption.

Cet article a été publié le 8 mars 2024 et édité en PDF le 15 mars 2024.