CRYPTOGRAPHIE QUANTIQUE - Mémo

C'est l'histoire de Alice, Bob et Eve. Alice envoie un message à Bob, ils ont chacun une clé, identique ou pas, qui permet à Alice de crypter le message et à Bob de le déchiffrer.
Lors du transfert de ce message, Eve l'intercepte et, parvient à le décrypter avant de le laisser filer vers Bob qui pense, en le déchiffrant, être la seule à le connaitre.

C'est ainsi, qu'avec le génie d'Allan Turing, les anglais arrivèrent à déchiffrer les messages d'Enigma durant la seconde guerre mondiale sans que les allemands le sachent. Nous reconnaissons aujourd'hui que Turing a joué un rôle essentiel dans la victoire de 1945.

Depuis 1945, la cyber sécurité a toujours été le wagon qui s'est « accroché » à la locomotive nommée « hackers ». Avec la cryptologie quantique, nous entrons dans le monde de la cybersécurité inviolable.

1. La cryptographie quantique

Si l'informatique quantique n'est pas encore, et pour de nombreuses années, amenée à remplacer les ordinateurs d'aujourd'hui, il n'en va pas de même de la cryptographie quantique. Elle est utilisée pour transmettre les clés de données de codage et de décodage.
C'est dans les années 70 qu'un physicien anglais eu l'idée d'appliquer les propriétés de la physique quantique à la cryptographie. **Transmettre la clé sous forme de photons polarisés**.
En 1984, Bennet et brassard ont réalisé le premier protocole de polarisation des photons : BB84 .

Les trois propriétés dont il s'agit sont :

a- La modification des propriétés d'un photon par l'observation. Si Eve observe l'information envoyée par Bob, Alice saura non seulement que le message a été espionné mais connaitra également la partie du message espionnée.
b- Il est impossible de dupliquer un photon à l'identique.
c- L'intrication. Terme barbare pour un néophyte et encore mystérieux pour les spécialistes de la physique quantique. L'intrication, démontrée mais pas expliquée par les physiciens c'est la relation entre deux électrons (photons) qui ont été créés en même temps puis séparés l'un de l'autre. Lorsque l'on polarise l'un d'eux, l'autre est simultanément polarisé quelque soit la distance qui les sépare.
La clé de déchiffrage d'un message peut ainsi être créée par Bob, elle sera simultanément en possession d'Alice sans qu'un transfert d'information ait eu lieu.
Donc, sans possibilité de violation de cette clé.

La cryptographie quantique, c'est l'histoire du passage de l'ère industrielle à l'ère algorithmique.

2. Etat des lieux

Il existe un grand nombre de produits liés à la cryptographie quantique. Du hardware au logiciel, en passant par les capteurs, les fibres, les répétiteurs, etc.

D'après Orbis Research©: "2017 Market Research Report on Global Quantum Cryptography Industry", en 2017, le Marché représente 300M USD en 2017 et connaitra une croissance annuelle de 30% pour atteindre 1.8MD en 2024.

A ce jour, les clients équipés de cette technologie sont très logiquement les acteurs les plus concernés et les plus piratés de la planète : la NSA, les ministères de la défense dans de nombreux pays, etc.

Dès demain, ce seront les grandes entreprises et l'ensemble des administrations.

Du coté des fournisseurs, les métiers sont très diverses :

- Encryption solution providers, Quantum cryptography vendors, Application security service providers,System integrators/network security service providers, Consultancy firms/advisory firms,Training and education service providers, Data integration service providers, Managed service providers, Quantum computing and quantum cryptography R&D firms

Si les géants de l'industrie sont déjà présents – Toshiba, IBM, Thalès - , ils ne semblent pas les plus actifs sur ce segment. Le leader du Marché, bien que nous ne possédions pas de données serait ID Quantique (Suisse) .
En Europe, Cube et Post quantum (en) ou encore Physec et Idee GmbH (D) sont présents mais leur taille et leur activité restent à la dimension du photon.

En France, une start up – Sequrenet – communique sur sa capacité à fournir du codage quantique encrypté mais elle ne semble pas très active.

Aux Etats unis, les start up sont plus nombreuses et plus actives. D'une part parce que les fonds disponibles et dédiés à cette activité sont plus importants mais également parce que les clients ayant fait le pas sont plus nombreux. Parmi celles qui communiquent le plus, on peut citer PQsecure ou encore Nano Meta Technologies.

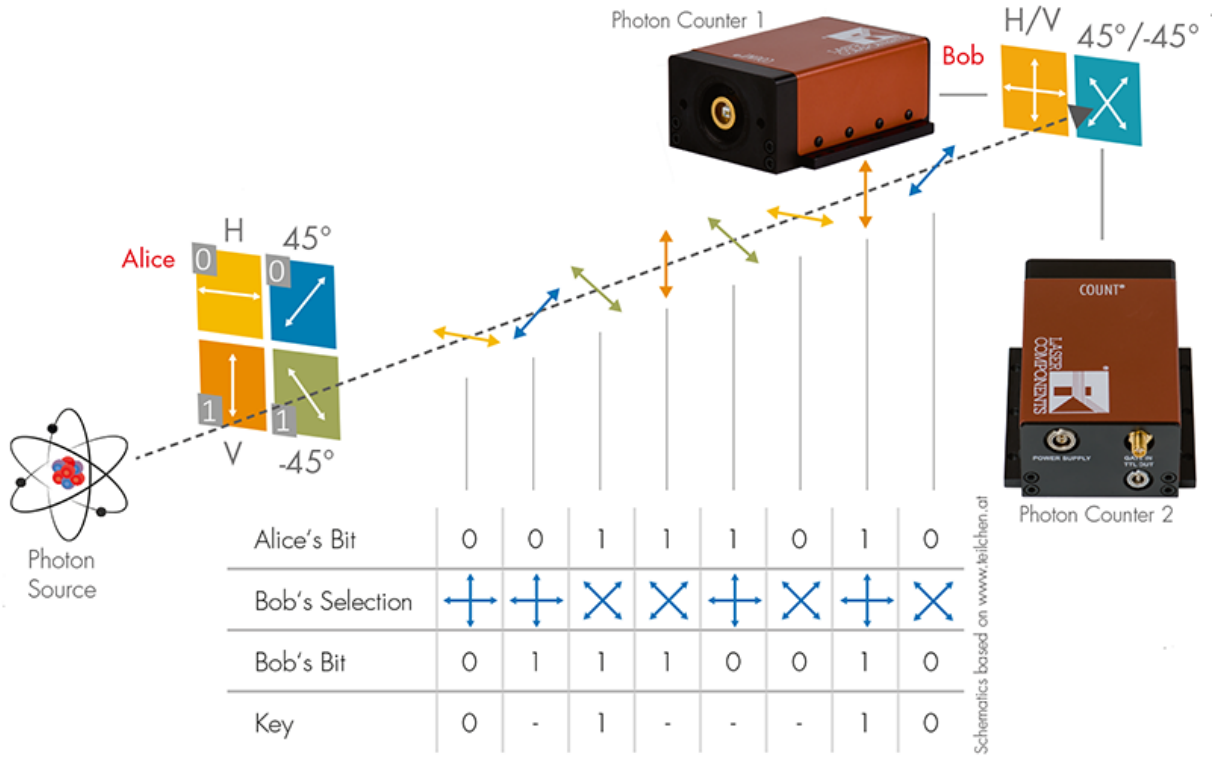
3. <u>Le projet</u>

Le porteur :

J'ai créé et dirigé 6 entreprises en 30 ans. Mon savoir-faire couvre l'industrie en PME, la start up des années 2000 sur Internet, la start up technologique des années 2010, l'imagerie médicale ou encore le conseil et la formation.

Ma motivation : foncer sur un Marché disruptif.

La start up aura comme objectif la création et la vente de solutions cryptées selon les protocoles quantiques – Quantum Key Distribution -.



La réalisation de ce projet s'articule autour de 3 périodes :

- Lancement du projet, recherche du product market fit
  - Durée : 18 mois -2 ans
  - Enveloppe :

- Positionnement sur le Marché
  - Durée : 2 ans
  - Enveloppe

- Croissance et sortie
  - Durée : 3 ans
  - Enveloppe :

Start FY1 FY2 FY3 FY4 FY5