Ordinateurs quantiques et futur de la sécurité, conférence le 15 avril 2019
par **Renaud Lifchitz**

Présentation par **Gérard Peliks**

La physique quantique révèle de bien étranges choses. Raisonner avec notre vécu quotidien ne permet pas de comprendre les phénomènes qui se passent au niveau des particules subatomiques : neutrons, photons et plus petits encore. Par exemple un électron peut être partout à la fois, au même moment, et si on connait sa position à un instant, il n'est pas possible de connaître sa vitesse, et inversement. Plus étrange encore, si vous essayez d'observer les caractéristiques d'une particule, il y a décorrélation et elle perd ses propriétés quantiques. Par exemple deux photons intriqués l'un à Paris, l'autre en orbite autour de Mars, réagissent en même temps quand l'un ou l'autre change de configuration, ce qui contrarie la théorie de la relativité mais s'explique d'une autre manière.
Un bit prend la valeur 0 ou 1, mais dans la physique quantique, son équivalent, le qubit, prend à la fois l'état 0 et l'état 1, ce qui lui offre quatre possibilités (00, 01, 10 et 11). Incroyable mais vrai ! et c'est à la base des calculs que réaliseront les ordinateurs quantiques qui seront infiniment plus rapides, quand ils pourront exploiter ces fonctionnalités.

Une des applications de ces étranges phénomènes est donc l'ordinateur quantique qui par sa puissance de calcul, quand (si ?) il sera opérationnel de manière industrielle et à grande échelle, résoudra les problèmes mathématiques trop complexes, trop coûteux en temps, sinon impossibles à résoudre avec les calculateurs classiques. Ceci rendra-t-il obsolète la cryptologie asymétrique qui profite du fait que certains problèmes sont très difficiles à résoudre comme la factorisation d'un grand nombre ou le logarithme discret ? Le calculateur quantique marquera-t-il ainsi la fin de la cryptologie ? Non car des algorithmes dit « post quantiques » sont en cours de développement.

Pour bien comprendre cette théorie quantique, pensée par de grands chercheurs, Einstein, Bohr, Planck et d'autres dont plusieurs ont été récompensés par le prix Nobel, seul quelqu'un qui a l'habitude de la vulgarisation scientifique et qui maîtrise autant le sujet que la pédagogie, peut nous faire entrer dans ce monde merveilleux pour nous faire comprendre l'incompréhensible.

Et ce sera le thème de notre Lundi de la Cybersécurité du mois d'avril, le 15 avril à 18h30, qu'animera Renaud Lifchitz.

Je donne la plume à l'intervenant :

« Cette présentation introduira sans prérequis techniques et pour le plus grand nombre :

* L'état de l'art des ordinateurs quantiques ;
* les principes du calcul quantique ;
* l'inversion quantique d'une fonction ;
* les puces quantiques et simulateurs accessibles au grand public ;
* les progrès et records des technologies quantiques ces dernières années et dans les années à venir ;

* les menaces sur les dispositifs de sécurité existants ;
* les apports sécuritaires des technologies quantiques ;
* la cryptographie post-quantique.

Elle permettra donc à tout un chacun d'y voir plus clair et de démythifier les nombreuses rumeurs et approximations colportées par les médias, et de se faire son propre avis sur cette technologie prometteuse ».

L'intervenant : Renaud Lifchitz

Renaud Lifchitz, expert chez Digital.Security, est un expert sécurité français reconnu en sécurité informatique ayant une longue expérience d'auditeur et de formateur, principalement dans les secteurs bancaire et télécom. Il s'intéresse tout particulièrement au développement sécurisé, aux protocoles de communication sans fil et à la cryptographie. Il a été intervenant dans de nombreuses conférences internationales : CCC 2010, Hackito Ergo Sum 2010 & 2012, DeepSec 2012, Shakacon 2012, 8dot8 2013 et a formé plus de 1800 personnes. Ses travaux de sécurité les plus significatifs portent sur les thèmes : cartes bancaires sans contact, géolocalisation GSM, blockchain, signatures RSA, ZigBee, Sigfox, LoRaWAN, Vigik et calcul quantique.