Compte-rendu du lundi de la cybersécurité du mois d'avril 2019

Thème : Ordinateurs quantiques et futur de la sécurité

Ce lundi de la cybersécurité visait à nous présenter :

- Un exposé technique, les ordinateurs quantiques ;
- Les Simulateurs quantiques d'une part et d'autre part les vraies puces quantiques qui existent et qui sont en plus gratuitement accessible à tout le monde, depuis le web ;
- Les algorithmes quantiques.

Intervenant : Renaud Lifchitz, expert sécurité chez Econocom Digital Security

Date et Lieu : 15 avril 2019 à Telecom ParisTech

Longtemps resté une simple idée de physicien, l'ordinateur quantique, qui promet de révolutionner le calcul, devient une réalité de plus en plus tangible. D'après **Renaud Lifchitz** dans quelques années (4ans environ), les premières machines capables de surpasser les ordinateurs classiques devraient faire leur apparition tout en offrant des capacités de calcul phénoménales.

Qu'est-ce qu'on entend par ordinateur quantique ?

Un ordinateur quantique est l'équivalent des ordinateurs classiques mais qui effectuerait ses calculs en utilisant directement les lois de la physique quantique et, à la base, celle dite de superposition des états quantiques. Alors qu'un ordinateur classique manipule des bits d'information, qui sont soit des 0 soit des 1, un ordinateur quantique utilise des qubits. Ceux-ci sont des généralisations des bits classiques, qui sont en quelque sorte une superposition simultanée de ces deux états 0 et 1, comme peut l'être, par exemple une polarisation pour un photon ou un spin pour un électron.

Principe de calcul des ordinateurs quantiques

On distingue quatre (4) grands principes à la base des ordinateurs quantiques

- **La dualité** : ondes / particules ;
- **Le principe de superposition quantique / principe d'incertitude d'Heisenberg** : les caractéristiques physiques ne sont pas prédictibles et au moment de la mesure la particule perd cette superposition ;

- **Une décohérence quantique** : Une interaction ou mesure va faire s'effondrer cette superposition d'états et laisser un état stable ;
- **Le principe de théorème de non-clonage :** on ne peut reproduire à l'identique un état quantique.

NB : les 3 premiers principes conditionnent les algorithmes quantiques.

Renaud Lifchitz nous a parlé de deux expériences effectuées par la même équipe à quelques années d'intervalle et illustrant les propriétés de l'intrication quantique.

1ère expérience

Interaction instantanée de qubits intriqués : en été 2008, Université de Genève, Nicolas Gisin et ses collègues déterminent que la vitesse d'une interaction quantique est d'au moins 10000 fois la vitesse de la lumière en utilisant des photons corrélés à 18 kms de distance.

Pour en savoir plus (http://arxiv.org/abs/0808.3316)

Quantum téléportation : en septembre 2014, la même équipe réussit une téléportation quantique de 25 kilomètres (qui consiste à agir sur un élément et vérifier que l'action se répercute à distance sur le même élément intriqué).

2ième expérience

Expérience du chat de Schrödinger (c'est une « expérience de pensée » pour prouver le principe de la superposition de plusieurs états quantiques, pas une manipulation réelle) : permet de montrer la frontière qui existe entre le monde de infiniment petit et le monde macroscopique.

Distinction entre états superposés et intriqués

Un ordinateur quantique utilise les lois de la mécanique quantique, une théorie qui décrit les phénomènes physiques à l'échelle sub-atomique. Une molécule peut se trouver dans différents états en même temps : on parle **d'états superposés**.

Alors que dans un ordinateur ordinaire, les informations sont codées sous la forme de bits qui ne peuvent prendre que deux valeurs, 0 ou 1, selon le passage ou non de courant électrique à travers un transistor, les bits quantiques (ou qubits) peuvent simultanément prendre les valeurs 0 et 1. Qui plus est, lorsque deux qubits interagissent, leurs états physiques « s'enchevêtrent », si bien que les deux systèmes ne peuvent plus être décrits de façon indépendante : on parle **d'états intriqués**.

Les portes quantiques

En informatique quantique, et plus précisément dans le modèle de circuit quantique de calcul, une porte quantique (ou porte logique quantique) est un circuit quantique élémentaire opérant sur un petit nombre de qubits.

Ces portes nous ont été présentées comme ci-dessous.

Portes	Nombres des qubits	Descriptions
Pauli-X	1	Equivalent quantique d'une porte logique "NON". Tourne le qubit autour de son axe X de 180 degrés. X.X = I
Hadamard	1	Transforme un qubit constant dans une superposition équiprobable de |0| et |1| **Remarque** : Pour cette raison, elle est beaucoup utilisée comme première étape d'un algorithme pour travailler en parallèle sur toutes les valeurs possibles des entrées.
CNOT	2	Porte "NON" contrôlée. Le premier qubit est le qubit de contrôle, le second est le qubit cible. Ne change pas le qubit de contrôle et change le qubit cible uniquement si le contrôle vaut |1|
SWAP	2	Echange les 2 qubits d'entrée

NB : On a autant de qubits en entrée qu'en sortie parce que les portes quantiques sont **réversibles** contrairement aux portes logiques classiques qui sont non réversibles. Elles peuvent être vues comme des matrices, ou comme des vecteurs.

Simulateurs quantiques et puces quantiques accessibles sur le cloud

- **Simulateurs quantiques**

Quantum inspire

Pour aller plus loin : https://www.quantum-inspire.com

Quirk qui est intéressant et peut-être visuel sur le net

http://algassert.com/quirk

Quantum circuit simulator (androïd)

Une liste plus exhaustive : https://quantiki.org/wiki/list-qc-simulators

La simulation quantique a déjà abouti à des résultats mais avec l'augmentation du nombre de qubits, elle promet des avancées plus spectaculaires encore. Précisons qu'à chaque Qubit rajouté, la puissance de calcul est doublée. L'avantage de la simulation, est que la décohérence n'est finalement plus une contrainte puisque les systèmes qu'on simule sont eux-mêmes soumis à ce phénomène.

- **Puces quantiques accessibles sur le cloud**

Public quantum cloud computing services. Leur technique de fabrication est plutôt simple, ce qui permet de les dupliquer facilement et d'envisager d'en intégrer un grand nombre sur une même puce (IBM, Google...)

Quelques sites expérimentation, d'accès gratuits et accessibles à tous

Alibaba Quantum Computing Cloud Service (http://quantumcomputer.ac.cn) : jusqu'à 11 qubits

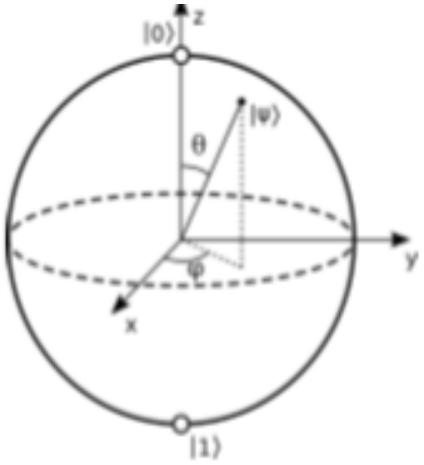
IBM "Q Experience" (https://www.research.ibm.com/ibm-q/technology/devices/) : jusqu'à 14 qubits, 20 qubits pour les clients privés

Rigetti "Quantum Cloud Services" (https://www.rigetti.com/qpu) : jusqu'à 19 qubits, 128 qubits à venir

D-Wave "Leap" (https://cloud.dwavesys.com/leap/) : jusqu'à 1000 qubits, puce quantique adiabatique, ordinateur quantique simulé, non universel, principalement utilisé pour des problèmes d'optimisation.

Comment représenter des qubits ?

L'exemple pris par M. Renaud Lifchitz est une sphère dite « sphère de Bloch » qui voit un qubit comme un vecteur unitaire dans une sphère, avec deux paramètres, les angles phi et théta.



Sphère de Bloch

Calculs quantiques et cryptographie

- **Calculs quantiques : comment s'y prendre ?**

En appliquant le calcul quantique à la cryptographie, une des approches consiste à essayer d'inverser des fonctions classiquement difficilement inversibles. Pour ce faire, deux approches sont possibles :

- Créer un circuit correspondant à la fonction et l'exécuter en sens inverse. La fonction visée est souvent non réversible et on doit compliquer la procédure pour qu'elle soit efficace. Le cas présenté est celui de CRC-8
- Implémenter la fonction à inverser et utiliser l'oracle de Grover pour parvenir au résultat. Le cas présenté est celui de l'inversion d'un chiffrement XOR par l'Oracle.

- **Cryptographie**

Qu'est-ce que s'est ?

La cryptographie : c'est l'art de chiffrer et de déchiffrer.
La cryptographie quantique : c'est une méthode de protection évoluées pour lutter contre une menace toujours croissante de découverte, par des personnes non autorisées, des clés secrètes de chiffrement.

Quelles sont les menaces qui peuvent être rencontrées ?

Cette étape, est assez importante, permet de distinguer les menaces quantiques selon le type de cryptographie.

Menaces des ordinateurs quantiques pesant sur la cryptographie symétrique

La principale menace est l'algorithme de Grover :

- ✓ Algorithme purement quantique pour chercher parmi N valeurs non triées
- ✓ Complexité : O(√N) opérations et O(logN) en stockage
- ✓ Algorithme probabiliste, itératif et optimal

Défense : doubler toutes les tailles de clés symétriques est suffisant pour échapper à toutes les attaques quantiques futures, donc pas une grosse menace.

Menaces des ordinateurs quantiques contre la cryptographie asymétrique

La principale menace est l'algorithme de Shor :

- ✓ Algorithme quantique pour la recherche de période formulé en 1994 ;
- ✓ Complexité : O((logN)3) opérations et espace de stockage ;
- ✓ Algorithme probabiliste qui trouve la période de la séquence ak mod N puis des racines de l'unité ;
- ✓ Utilise une QFT, quelques étapes effectuées sur un ordinateur classique ;
- ✓ Casse RSA, DSA, ECDSA, ECDLP de façon efficace ;
- ✓ La factorisation d'un grand nombre en deux nombres premiers dont il est le produit, base du RSA, devient faisable dans un temps acceptable. La cryptographie asymétrique est ainsi très menacée ;
- ✓ Le chiffrement par courbes elliptiques est également menacé.

Défense : utiliser de la cryptographie post-quantique

➢ La cryptographie post-quantique

La cryptographie post-quantique est une cryptographie résistante aux algorithmes quantiques.

Algorithmes post-quantique symétrique

Toutefois, les approches résistantes aux attaques par des algorithmes quantiques ne manquent pas. Actuellement six (6) principales approches ont été répertoriées :

- ✓ Lattice-based cryptography
- ✓ Multivariate cryptography
- ✓ Hash-based cryptography
- ✓ Code-based cryptography
- ✓ Supersingular Elliptic Curve Isogeny cryptography
- ✓ Symmetric Key Quantum Resistance

Algorithmes post-quantiques asymétriques

Peu d'algorithmes post-quantiques asymétriques, le plus connu est NTRU, a lattice-based shortest vector problem :

- ✓ NTRUEncrypt pour le chiffrement (1996)
- ✓ NTRUSign pour la signature électronique

Pour plus d'informations :

Evénement annuel à propos de la cryptographie quantique : PQCrypto conférence (https://twitter.com/pqcryptoconf, 10th edition in 2019)

https://www.onboardsecurity.com/products/ntru-crypto

Cryptographie post-quantique expérimentée dans Google Chrome

Article MISC HS n°13 "Le grand defi du post-quantique » : https://connect.ed-diamond.com/MISC/MISCHS-013/ Le-grand-defi-du-post-quantique (Ludovic Perret & Jean-Charles Faugère)

Conclusion

Les ordinateurs quantiques restent un véritable challenge. Pour faire de l'ordinateur quantique une réalité il faudra :

- Être capable de corriger les erreurs de calcul liées à la décohérence qui obligent aujourd'hui à utiliser de nombreux qubits physiques correcteurs d'erreurs pour donner des qubits logiques réellement utilisables ;
- Améliorer les performances du nombre de qubits.

Néanmoins on a essentiellement deux approches permettant de fabriquer des qubits :

- Les circuits « solides », comme des circuits supraconducteurs ou des boîtes quantiques ;
- Des systèmes plus « exotiques », comme des ions piégés, les centres colorés du diamant, etc.

L'ordinateur quantique peut être utilisé de manière offensive et défensive.

Mes remerciements vont à l'endroit de :

- **RENAUD LIFCHITZ** pour la présentation et la qualité des échanges avec la salle ;
- L'école **TELECOM PARISTECH** et **Télécom ParisTech Entrepreneurs** de nous avoir accueillis dans leurs locaux ;
- Le MEDEF Hauts-de-Seine, **Béatrice Laurent** et **Gérard PELIKS** pour l'organisation des « Lundi de la cybersécurité ».

TILEUK Reine Raïssa
MBA Management de la sécurité des données numériques, Institut Léonard de Vinci
Contact : reinetilk@gmail.com