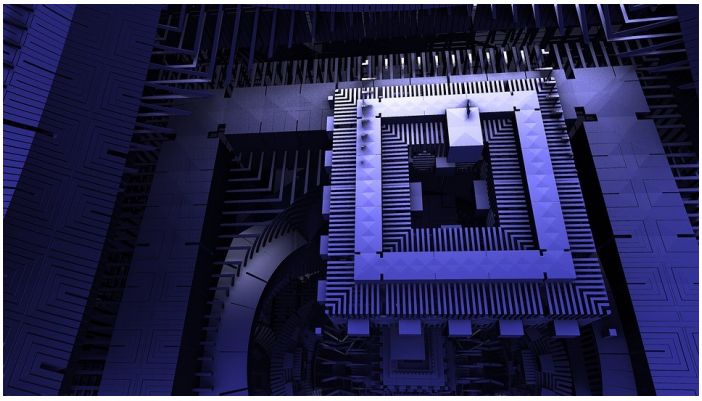
NOTE DU CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Numéro 46 – Février 2020

ASPIRANT Axel LEMOINE

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE



SUPRÉMATIE QUANTIQUE : LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES ÉCHANGES SUR INTERNET SONT-ELLES CONDAMNÉES ?

De ses premiers pas guidés par Alan Turing[1] jusqu'au triomphe d'AlphaGo[2] face au légendaire joueur de Go, Lee Sedol, l'informatique s'est bâtie une réputation de science en ébullition permanente. Les techniques actuelles ne cessent de s'améliorer pendant que d'autres apparaissent et constituent chacune une petite révolution dans le domaine, imposant aux professionnels d'être constamment à jour sur l'état de l'art.

Depuis les années 90, une nouvelle théorie se développe : celle de l'informatique quantique. Les composants électroniques des ordinateurs sont alors conçus pour être particulièrement soumis aux lois de la mécanique quantique, cette théorie physique de l'infiniment petit. Les visionnaires Peter Shor et Lov Grover ont élaboré, durant les années 90, des algorithmes exploitant ces phénomènes.

L'apport de l'informatique quantique n'est encore en bonne partie que théorique à ce jour. Le calculateur quantique est bien loin de proposer les mêmes fonctionnalités qu'un ordinateur classique, mais il a la capacité d'apporter des solutions à des problèmes auparavant insolubles en pratique. Parmi eux, un problème mathématique en apparence anodin, mais dont la complexité de résolution incarne un pilier fondamental de la sécurité des transactions sur Interne : la factorisation de très grands nombres entiers en facteurs premiers.

I) Pourquoi un ordinateur quantique ?

L'idée fondamentale en informatique, toujours d'actualité, est de traiter l'information sous forme binaire. Les composants de l'ordinateur (fabriqués à partir de transistors) construisent, stockent et manipulent des *bits*, c'est-à-dire des éléments pouvant avoir exactement deux états : 0 ou 1 (selon si le dispositif est traversé par un courant électrique ou non). La force de cette technique est d'assimiler la paire d'états (0 ou 1) au couple logique (faux ou vrai). En agençant judicieusement les composants de la machine, on peut ainsi créer des portes logiques[3] puis les instructions des programmes.

La puissance de l'ordinateur par rapport au cerveau humain réside dans sa capacité à effectuer une quantité astronomique d'opérations simples dans un laps de temps infinitésimal. Pourtant les processeurs classiques ne

1 Mathématicien et cryptologue britannique, considéré comme le père de l'informatique.
2 Intelligence artificielle de l'entreprise britannique Google Deepmind célèbre pour avoir vaincu Lee Sedol au jeu de go.
3 Ces petits dispositifs permettent d'associer entre eux des *bits* pour simuler les opérateurs logiques tels que (en anglais) AND, OR, NOT ou encore XOR (le fameux « ou exclusif »).

peuvent effectuer les tâches que les unes après les autres. C'est de ce point précis dont s'est affranchi le calculateur quantique.

Le processeur quantique manipule pour sa part non pas des *bits*, mais des *qu-bits*. Un *qu-bit* peut, tout comme un *bit*, être dans l'état 0 ou dans l'état 1 : ce sont ses *états propres*. Mais en règle générale, le *qu-bit* est dans une superposition de ces états[4]. Un ordinateur quantique peut donc avoir accès à tous les résultats possibles d'un calcul à la fois, tandis qu'un ordinateur classique délivre un résultat après l'autre. C'est de cette particularité théorique que naît la puissance de l'ordinateur quantique. L'exemple le plus parlant reste l'algorithme pour effectuer une recherche dans une liste non ordonnée de données. La méthode classique consiste à parcourir la liste du début à la fin jusqu'à tomber sur l'élément recherché. Avec un ordinateur quantique, on peut vérifier plusieurs items de la liste en même temps (algorithme de Grover)[5].

La performance du processeur quantique provient d'une subtilité apparaissant lorsque l'on considère un processeur à plusieurs *qu-bits*. Si un processeur possède, disons 3 *qu-bits*, ceux-ci ne seront pas indépendants mais *intriqués* : ils ne représentent qu'un seul objet quantique. Le processeur est donc dans une superposition des 8 états propres possibles[6], et peut ainsi réaliser 8 calculs en parallèle, donc en quelque sorte aller 8 fois plus vite. De manière générale, la rapidité d'un calculateur quantique augmente exponentiellement avec la quantité de *qu-bits*. Plus précisément, gagner ne serait-ce qu'un seul *qu-bit* doublera le nombre d'états propres, et par conséquent la puissance de l'appareil. L'intérêt de faire croître le nombre de *qu-bits* en découle naturellement.

Cette puissance potentielle de l'ordinateur quantique inquiète certains experts, qui imaginent qu'il pourrait casser le système de cryptage dont l'usage est universel : le chiffrement RSA[7].

II) Un danger pour l'algorithme RSA ?

Tout l'enjeu du chiffrement est de transmettre un message qui ne sera lisible que de ses seuls destinataires possédant la clé pour le décrypter. Depuis les premières méthodes de chiffrement (telles que le chiffrement de César), de nombreuses sophistications ont vu le jour. L'idée est d'utiliser des clés (c'est-à-dire des protocoles) pour coder et décoder des messages.

Aujourd'hui, la majeure partie des communications sur Internet sont chiffrées selon l'algorithme RSA. Celui-ci repose sur un chiffrement dit *asymétrique* : la clé pour chiffrer est différente de celle servant à déchiffrer. Chaque utilisateur possède une clé dite *privée* qui lui sert à déchiffrer les messages qu'on lui envoie. Il met à disposition de tous une clé publique permettant de chiffrer des messages pour ensuite les lui envoyer[8].

Concrètement, ces clés sont des nombres entiers de très grande taille et judicieusement choisis. Interviennent en particulier les module[9] et exposant de chiffrement (qui constituent la clé publique) et l'exposant de déchiffrement (qui donne la clé privée). Une relation mathématique déterministe lie les deux exposants, de sorte que la connaissance de la clé publique permet théoriquement d'en déduire à coup sûr la clé privée. Toute la sécurité du chiffrement RSA vient du fait que cette dernière opération est beaucoup trop difficile à mettre en œuvre en pratique.

4 Un objet quantique est, en fait, dans une superposition d'états propres, un état étant une liste de propriétés. Il y a par ailleurs des proportions : il peut être « à 60 % dans l'état X et 40 % dans l'état Y ». Cette superposition est levée lors de la mesure (on trouve soit X soit Y), et les chiffres s'interprètent comme la probabilité de trouver X ou Y.

5 Si la liste contient *N* éléments, le temps moyen que mettra la méthode classique est proportionnel à *N*. L'algorithme de Grover offre un temps moyen de l'ordre de la racine carrée de *N*, ce qui est considérablement mieux :https://arxiv.org/abs/quant-ph/9605043

6 Ces états propres sont les combinaisons des états propres de chaque *qu-bit* : (0,0,0), (0,0,1), (0,1,0), … , (1,1,1).

7 Ce nom représente les initiales de ses inventeurs : Ronald Rivest, Adi Shamir et Leonard Adleman. Il s'agit du mode de chiffrement le plus utilisé sur Internet.

8 L'explication la plus traditionnelle est la suivante : « Bob souhaite transmettre un message secret à Alice. Pour garantir que ce message ne soit lu par personne d'autre, le message doit être chiffré par Bob avant la transmission, puis déchiffré par Alice après réception. Pour cela, Alice génère deux clés : une clé publique qu'elle envoie à Bob, puis une clé privée qu'elle conserve précieusement. Bob chiffre son message secret avec la clé publique, puis transmet le message chiffré à Alice. Après réception, Alice déchiffre le message grâce à sa clé privée. ». Source : http://linor.fr/tutoriaux/tuto-423-cryptage-rsa-en.php

9 Cet entier est impérativement choisi *semi-premier*. Autrement dit, il s'écrit comme le produit de deux nombres premiers. Pour que le chiffrement RSA soit difficile (voire impossible) à casser, le but est de choisir le module de chiffrement le plus grand possible.

Pour comprendre en quoi l'ordinateur quantique pourrait compromettre cette sécurité, il convient de se pencher sur quelques détails de l'algorithme RSA. Le module de chiffrement s'écrit comme le produit de deux nombres premiers p et q. L'obtention de l'exposant de déchiffrement (et par conséquent de la clé privée) peut se faire à partir de l'exposant de chiffrement et d'une valeur obtenue à partie du module[10]. Ceci n'est possible en pratique que si l'on connaît la décomposition du module en la multiplication de p par q. En conclusion, la sécurité de nos transactions et communications sur Internet provient simplement de la difficulté de décomposer le module de chiffrement en facteurs premiers. Ce système semblait ne présenter aucune faille crédible. En effet, le temps que prendrait le meilleur algorithme actuel pour factoriser un nombre de 600 chiffres (soit la longueur de clés RSA de taille moyenne) serait plus de 100 fois supérieur à l'âge de l'Univers[11].

Les complications arrivèrent alors que Peter Shor travaillait aux Bell Labs (célèbres laboratoires du New Jersey). Il développe à cette époque l'algorithme qui porte son nom[12], ce qui lui vaudra d'être lauréat du prix Nevanlinna récompensant les mathématiques liées à l'informatique. Ce programme fonctionne précisément sur les ordinateurs quantiques et a vocation à factoriser les nombres entiers. Il est dit « exponentiellement meilleur » que le meilleur algorithme classique actuel, et réaliserait en quelques minutes ce qu'un processeur conventionnel prendrait des billions d'années à effectuer.

III) L'informatique quantique en pratique

Les algorithmes quantiques semblent incarner des solutions miracles à certains problèmes fastidieux. Encore faut-il réaliser une machine capable de mettre en œuvre ces algorithmes. Dès 2001, IBM réalisait l'exploit de faire tourner l'algorithme de Shor sur un calculateur quantique à 7 *qu-bits*[13], mettant ainsi le monde scientifique en effervescence devant leur prouesse : l'algorithme a réussi à factoriser 15=3×5. La question germait alors dans les esprits : finira-t-on par construire un ordinateur quantique *meilleur* qu'un ordinateur classique pour ce type de problème ?

La course à la suprématie quantique[14] était lancée, Google et IBM en tête. Intel frôlera cet objectif en 2018 avec 49 *qu-bits*[15]. C'est finalement Google qui annoncera en premier avoir franchi le seuil, en octobre 2019 dans la revue *Nature*[16]. L'équipe de Google est parvenue à faire fonctionner 53 *qu-bits* et affirme avoir exécuté en 600 secondes ce qu'un superordinateur d'un million de cœurs aurait mis plusieurs dizaines de milliers d'années à réaliser selon elle : la suprématie quantique a bien été atteinte. Toutefois, une équipe d'IBM conteste le véritable exploit de Google et prétend pouvoir réduire ces « dizaines de milliers d'années » à seulement trois jours en utilisant un autre algorithme[17]. Cependant, les ressources énergétiques nécessaires pour alimenter ledit ordinateur classique restent effroyablement supérieures à celles requises par le calculateur quantique de Google, et IBM n'est pas parvenu à réduire le temps d'exécution à l'ordre de la centaine de secondes.

10 Pour le lecteur curieux, l'exposant de déchiffrement est l'inverse de l'exposant de chiffrement modulo l'indicatrice d'Euler du module. La mutuelle primalité des quantités mises en jeu (pour assurer l'existence de l'inverse) est une consigne à respecter lors de la création des clés.

11 CHAILLOUX, André, L'algorithme quantique de Shor, *Interstices,* 30 mars 2018 . Disponible sur : https://interstices.info/lalgorithme-quantique-de-shor/

12 La publication récapitulative de Peter W. SHOR : *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, du 25 janvier 1996 : https://arxiv.org/pdf/quant-ph/9508027.pdf

13 JORRAND, Philippe, Vers l'ordinateur quantique, un défi scientifique majeur pour les prochaines décennies, *Interstices*, 18 novembre 2005. Disponible sur : https://interstices.info/vers-lordinateur-quantique-un-defi-scientifique-majeur-pour-les-prochaines-decennies/

14 Cette appellation désigne le fait d'avoir un ordinateur quantique capable de résoudre un problème qu'un ordinateur classique ne peut pas résoudre en temps raisonnable. Ceci correspond à un processeur quantique de 50 *qu-bits* environ.

15 FONTAINE, Pierre, CES 2018 : Intel frôle la suprématie quantique avec un processeur de 49 qubits, *01net*, 10 janvier 2018. Disponible sur : https://www.01net.com/actualites/ces-2018-intel-frole-la-suprematie-quantique-avec-un-processeur-49-qubits-1346276.html

16 « Quantum supremacy using a programmable superconductingprocessor », *Nature*, 23 octobre 2019. Disponible sur : https://www.nature.com/articles/s41586-019-1666-5

17 « Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore CircuitsPublication », 22 octobre 2019. Disponible sur : https://arxiv.org/pdf/1910.09534.pdf

Les technologies concernant le domaine quantique sont donc en pleine effervescence. La NSA aurait même investi plus de 80 millions de dollars dans un processeur quantique via un programme intitulé *Penetrating Hard Target* et un projet du nom de *Owning the Net*[18]. Mis en place par l'administration américaine en 2019, le National Quantum Initiative Act représenterait un investissement d'1,3 Md$. De son côté, la Chine consacrerait 2 Md$ au secteur de l'informatique quantique. L'Union européenne est également vue comme une concurrente sérieuse dans cette course et réunira 1 Md$ sur 10 ans pour les technologies quantiques [19]. En France, 60 M€ ont déjà été investis. Le rapport Forteza suggère qu'il faut tripler cet effort et répartir 1,4 Md€ sur 5 ans. Pour l'heure, le ministre de l'Économie et des Finances envisage une stratégie économique de protection du patrimoine scientifique français[20].

Tout le domaine pourrait connaître une avancée remarquable d'un jour à l'autre grâce aux prouesses toujours plus spectaculaires des entreprises du numérique. Gardons cependant à l'esprit que personne n'est encore capable de casser un chiffrement RSA (la plus grande factorisation par un ordinateur quantique connue étant 4088459=2017×2027 en 2018, des quantités bien inférieures aux nombres cryptographiques qui sont codés sur au moins 1024 *bits* pour RSA, soit un peu plus de 300 chiffres)[21], ce qui pourrait prendre encore du temps. Pourtant, la question des dangers que représente l'informatique quantique est posée aujourd'hui.

IV) Vers la cryptographie post-quantique ?

Pour pallier ce potentiel défaut de fiabilité du chiffrement, la solution la plus évidente serait d'utiliser des clés RSA plus longues, donc plus difficiles à casser. Ceci imposerait une génération des clés plus lente et plus coûteuse (doubler la longueur d'une clé RSA multiplierait le temps de génération par 16), qui ne saurait être une solution à long terme. L'enjeu est de taille pour les forces de l'ordre : auront-elles une capacité d'écoute décuplée ou seront-elles aussi vulnérables que tout autre utilisateur ? La nécessité de s'orienter vers un autre type de cryptographie dans le futur paraît ainsi de plus en plus crédible.

Bien que le chiffrement RSA soit loin d'être en danger à l'heure actuelle, la recherche autour d'un mode de cryptographie résistant aux attaques par ordinateur quantique (dit *post-quantique*) est en cours dès à présent. En particulier, le NIST[22] cherche à promouvoir des standards de cryptographie post-quantique via un concours qu'il organise. Des laboratoires du monde entier travaillent sur des nouvelles technologies de cryptage. 26 technologies finalistes issues de 69 propositions préalablement étudiées seront examinées jusqu'à ce que ressorte un unique vainqueur[23]. Ce concours est pris très au sérieux par la communauté spécialiste de la cryptographie, à tel point que la messagerie française Olvid[24] se dit prête à intégrer la technologie développée par le futur vainqueur.

18 RICH, Steven, GELLMAN, Barton, « NSA seeks to build quantum computer that could crack most types of encryption », *The Washington Post*, 2 janvier 2014. Disponible sur : https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html

19 Ce projet est pris au sérieux par le MIT Technology Review : https://www.technologyreview.com/f/612679/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/
Pour en savoir plus sur le projet européen Quantum Flagship : https://qt.eu/about/

20 FORTEZA Paula, HERTEMAN, Jean-Paul, KERENIDIS, Iordanis, *Quantique, le virage, technologique que la France ne ratera pas,* janvier 2020. Disponible sur : https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf

21 La méthode était différente de l'algorithme de Shor et ne présentait aucun avantage par rapport aux techniques classiques : https://blog.d2si.io/2019/06/20/ordinateur-quantique-rsa/

22 National Institute of Standards and Technology, agence du département du Commerce des États-Unis.

23 DUCAS, Léo, Propos recueillis par PAJOT, Philippe, Le NIST a annoncé les protocoles qui seront examinés pour devenir les nouveaux standards de cryptographie post-quantique, *La Recherche,* 5 février 2019. Disponible sur : https://www.larecherche.fr/informatique-cryptographie/le-nist-annonc%C3%A9-les-protocoles-qui-seront-examin%C3%A9s-pour-devenir-les

24 Ladite messagerie a d'ailleurs remporté le prix de la startup FIC 2020. *Cf.* POIREAULT, Kevin, En amont du FIC 2020, la cryptographie prête au post-quantique de la messagerie Olvid récompensée, *Industrie et Technologies*, 10 décembre 2019. Disponible sur : https://www.industrie-techno.com/article/fic-2020-en-s-affranchissant-des-serveurs-la-messagerie-olvid-est-prete-pour-la-cryptographie-post-quantique.58449