Vers de nouveaux concepts cryptographiques 2/2

Revue militaire générale n°54

le chef de bataillon Mathieu MORALES

Publié le 22/03/2019

Sciences & technologies

L' ordinateur quantique

La célèbre loi de Moore prévoyait que le nombre de transistors sur un microprocesseur doublerait tous les dix-huit mois. En se basant sur ces calculs, en 2020, la taille d'un transistor approchera celle d'un atome, ce qui marquera la fin de la loi de Moore alors que les besoins en capacité de calcul continuent d'augmenter. Il fallait donc imaginer un nouveau type d'ordinateur utilisant les propriétés quantiques de l'atome.

Trois notions de physique quantique intéressent particulièrement les chercheurs dans le domaine.

Premièrement, la superposition quantique. On admet en physique quantique qu'une particule peut être dans un état indéterminé ou plutôt dans plusieurs états à la fois. À l'instar d'un ticket de loterie qui, tant que le tirage n'a pas eu lieu, n'est ni gagnant ni perdant, mais une superposition de ces deux états pondérés d'une certaine probabilité.

Deuxièmement, l'intrication quantique. Bien que ce sujet soit encore soumis à de nombreuses recherches, il est possible de lier plusieurs particules entre elles pour qu'elles continuent à ne former qu'un système unique indépendamment de la distance qui les sépare. Une opération sur l'une d'elle se répercutera sur toutes les autres.

Enfin, la décohérence quantique. Les propriétés quantiques sont conservées tant que le système est isolé et qu'il n'a pas de contact avec l'extérieur. Or, pour exploiter les résultats, une mesure est nécessaire. Ainsi, pour reprendre l'analogie avec le ticket de loterie, ce dernier est dans un état de superposition (à la fois gagnant ou perdant) jusqu'au tirage. Une fois cette mesure effectuée, le ticket devient soit gagnant soit perdant et retrouve des propriétés de la physique classique.

C'est sur cette base que les chercheurs imaginent le fonctionnement de l'ordinateur quantique. Ainsi, alors que l'informatique classique manipule de façon séquentielle des bits qui peuvent valoir soit 0 soit 1, l'informatique quantique utilise en simultané des bits quantiques ou qbits, qui prennent comme valeur une superposition de 0 et de 1. Les gains de temps sont considérables car un ordinateur quantique de dix qbits pourra tester en un seul calcul toutes les combinaisons de dix bits là où un ordinateur classique nécessitera 1024 opérations (soit 210 opérations). Des algorithmes existent déjà mais ne sont pas encore suffisamment efficaces sur les machines actuelles. Le plus connu est l'algorithme de SHOR, de décomposition en nombres premiers en des temps opérationnels qui rendraient obsolètes les crypto-systèmes comme le RSA.

En pratique, la recherche se heurte à plusieurs complications puisque la manipulation d'éléments quantiques nécessite des conditions physiques très particulières, notamment l'isolement des particules à des températures proches du zéro absolu et le maintien de la cohérence quantique suffisamment longtemps pour effectuer tous les calculs. Toutefois, la recherche progresse et la question n'est plus de savoir si l'ordinateur quantique, tel qu'on l'imagine, existera, mais quand il existera. De grandes entreprises comme IBM, Microsoft, Google ou encore le français ATOS se sont engagés dans les recherches sur l'ordinateur

quantique et les annonces se multiplient. IBM permet depuis l'année dernière aux chercheurs d'essayer leurs algorithmes sur un ordinateur de cinq qbits et promet un processeur de 50 qbits[58] dans les années à venir. La NSA, quant à elle, a investi 80 millions de dollars au travers du programme « Penetrating hard targets » pour se doter d'un ordinateur suffisamment puissant pour déchiffrer toutes les connexions sécurisées d'Internet.

La cryptographie moderne

Devant ces avancées technologiques et face à la menace que font peser les calculateurs quantiques sur la sécurisation des communications, deux domaines de la cryptographie ont vu récemment le jour.

La cryptographie quantique permet de se protéger des attaques quantiques par des moyens quantiques, en particulier dans les modes de transmission. Dans ce domaine, la Chine a une longueur d'avance puisqu'elle est parvenue, l'été dernier, à réaliser la première communication intercontinentale avec un système cryptographique inviolable entre Vienne et Pékin. La communication se fait par des moyens classiques, mais la clé de cryptage est transmise par des moyens quantiques. Jusqu'à présent, ce genre de transmission se faisait par fibre optique, ce qui limitait la distance de transmission à 200 km. Ce bond technologique a pu être réalisé grâce au satellite Micius, mis en orbite le 16 août 2016. Capable de fabriquer et d'émettre des paires de photons intriqués, il permet de s'assurer que les deux communicants ont bien la même clé. La décohérence quantique, quant à elle, permet de s'assurer que la clé n'a pas été interceptée, car si tel était le cas, le système perdrait son caractère quantique et les destinataires, s'apercevant de l'attaque, n'utiliseraient pas la clé. L'essai de communication quantique devrait être répété prochainement entre Pékin et Singapour, puis avec l'Italie, l'Allemagne et la Russie, et pourrait ouvrir la voie à un réseau Internet quantique mondial.

Le deuxième domaine d'étude est la cryptographie post quantique. En raison de leur coût et de leurs conditions particulières d'utilisation, les moyens quantiques n'ont pas vocation à se populariser et à remplacer tous les systèmes d'information actuels. L'enjeu de cette

branche de la cryptographie est de concevoir, pour les systèmes d'informations classiques, de nouveaux protocoles qui résisteraient à une attaque quantique. Les conférences PQ-Crypto rassemblent chaque année les chercheurs du domaine pour exposer et confronter les nouveaux algorithmes et concepts mathématiques susceptibles de constituer la base des échanges de demain.

Le « prix de l'innovation Jean-Claude Cassaing » a été attribué, le 14 avril 2017, à Jean-Christophe Deneuville pour ses travaux sur les « Contributions à la cryptographie post-quantique ». Dans sa thèse[59], il propose différents protocoles basés sur des outils mathématiques alternatifs (les réseaux euclidiens et les codes correcteurs d'erreurs) a priori résistants à ces nouveaux ordinateurs. Ces protocoles sont, à terme, voués à remplacer ceux existants afin de fournir les mêmes garanties de sécurité. Certains des travaux de cette thèse seront proposés prochainement à l'agence américaine des standards (NIST) en vue de leur utilisation à grande échelle.

Conclusion

Alors que les attaques massives se multiplient et que sont mises en exergue de plus en plus de failles sur la sécurité et la transmission des données, les avancées en matière de calculateur quantique viennent remettre en question les fondements même de tous les protocoles de sécurité actuels. Certains états investissent des sommes considérables pour être les premiers à se doter de ces technologies et avoir ainsi la maîtrise des communications. Certes, ces supercalculateurs ne sont pas encore pleinement opérationnels, mais la course est lancée et les performances augmentent de plus en plus rapidement. Compte tenu des délais nécessaires à la mise à jour et la normalisation des protocoles d'échanges, les mesures palliatives doivent être pensées, voire éprouvées dès maintenant.

Ainsi, les années à venir seront dédiées à la redéfinition des concepts cryptographiques et des protocoles de transmissions sécurisées pour faire face aux menaces d'interceptions qui pèsent sur la confidentialité des informations.

Officier du génie, le chef de bataillon Morales a effectué sa première partie de carrière dans le génie aéronautique à la 1re compagnie opérationnelle du génie de l'air. Dans le cadre du diplôme technique, il a effectué un mastère spécialisé en management des systèmes d'information à Centrale-Supélec.

57 Pretty Good Privacy : logiciel libre de cryptographie.

58 Il existe des imprécisions sur les définitions des qbits et des ordinateurs quantiques. La société D-Wave annonce par exemple la commercialisation d'un ordinateur quantique à 2 000 qbits, mais il s'agit en réalité d'un simulateur quantique capable uniquement de résoudre des problèmes d'optimisation bien précis. À l'heure actuelle, il semblerait que les meilleurs ordinateurs quantiques aient une puissance avoisinant les 17 qbits.

59 Thèse disponible sur le site : http://www.unilim.fr/pages_perso/deneuville/files/phd_thesis.pdf

Titre : Vers de nouveaux concepts cryptographiques 2/2

Auteur(s) : le chef de bataillon Mathieu MORALES

Date de parution : 14/03/2019