LES NOTES SCIENTIFIQUES DE L'OFFICE
OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Note n° 18 — Juillet 2019

Technologies quantiques : cryptographies quantiques et post-quantiques

Résumé

- *Les communications, terrestres ou satellitaires, tiennent une place centrale dans notre société et des outils efficaces ont été mis au point ces dernières décennies afin de sécuriser les données échangées et de se prémunir des attaques.*
- *Cependant, l'ordinateur quantique et sa puissance de calcul potentielle constituent une menace pour les données chiffrées avec ces méthodes, qu'ils pourraient décrypter en un temps record.*
- *Pour répondre à cette menace, deux axes principaux et complémentaires se développent : d'une part, la cryptographie post-quantique, qui se base sur de nouveaux concepts mathématiques pour chiffrer les protocoles de communication, d'autre part, la cryptographie quantique, qui utilise les propriétés de la physique quantique pour sécuriser le transport de l'information.*
- *Même si l'avènement de l'ordinateur quantique ne se pose qu'à moyen, voire à long terme, les différents acteurs doivent anticiper cette transition vers de nouveaux protocoles de chiffrement, notamment pour répondre à des enjeux stratégiques et de souveraineté.*

Source :Nmedia/AdobeStock

M. Cédric Villani, Député, Premier vice-président

Notre société repose de plus en plus sur les communications, c'est-à-dire l'échange d'informations[1]. Les technologies actuelles permettent d'échanger sur des grandes distances et à très haut débit via des liaisons terrestres, sous-marines ou satellitaires. Si deux personnes souhaitent communiquer de manière confidentielle, il est nécessaire, d'une part, de **chiffrer les données échangées sur leur trajet** pour éviter qu'un tiers ne s'en empare, d'autre part, que l'expéditeur utilise une **signature numérique**[2] (à l'instar de la signature physique) afin de garantir l'authenticité d'un message et d'empêcher sa falsification. Dans de nombreux cas, qu'il s'agisse de données sensibles pour l'État (défense, diplomatie), pour des entreprises (finance, spatial, etc.) ou des particuliers (mots de passe, codes de cartes bancaires, etc.), une faille de sécurité peut avoir des conséquences graves. **La puissance de l'ordinateur quantique est perçue comme une menace en la matière, car elle permettra à terme de nouvelles attaques contre certains de ces protocoles sécurisés.**

Méthodes de chiffrement actuelles

Les premières techniques de cryptographie remontent à l'Antiquité. Jusqu'au XX^{e} siècle, elles reposent en général sur un encodage astucieux des lettres de l'alphabet. Les protocoles gagnent progressivement en complexité, jusqu'à la machine allemande « Enigma »[3] dont la cryptanalyse[4] devient un enjeu majeur pendant la Seconde guerre mondiale. Dans les années 1940, les travaux de Claude Shannon posent les fondements de la théorie de l'information[5] et créent un cadre rigoureux pour étudier les attaques possibles contre les chiffrements. Dans les années 1970, le *National Institute of Standards and Technologies* (NIST) américain propose le premier standard de chiffrement, appelé *Data Encryption Standard* (DES)[6], qui sera utilisé dans des administrations américaines. Puis, dans les années 1980, l'utilisation de problèmes issus de l'arithmétique ouvre la voie à des nouvelles méthodes de cryptographie. Aujourd'hui, le chiffrement (et le déchiffrement) de données s'appuie sur des techniques mathématiques complexes, **qui doivent continuellement s'adapter à mesure que la puissance des ordinateurs, ainsi que leur vitesse de calcul, augmentent**. Deux grands types de méthodes sont employés.

Tout d'abord, la **cryptographie symétrique**, similaire aux techniques « historiques » et pour laquelle une **clef secrète** (par exemple le nombre 5) **est utilisée pour chiffrer et déchiffrer les messages**. Cette clef est connue au préalable des deux participants (appelés traditionnellement Alice et Bob[7]). Concrètement, et de manière simplifiée, si Alice veut envoyer le nombre 4 à Bob, elle peut le chiffrer avec la clef 5 sous la forme de 9 = 4+5 et Bob devra calculer 9-5 pour retrouver le message[8].

Avant toute communication utilisant un chiffrement symétrique, il est nécessaire qu'Alice et Bob se « mettent d'accord » sur la clef secrète qu'ils vont utiliser.

Néanmoins, ils ne peuvent pas l'échanger en clair sur le réseau, sinon n'importe quel observateur pourra décrypter leurs conversations. Le **chiffrement asymétrique** résout ce problème puisqu'il permet de communiquer sans avoir un secret commun au préalable. Pour ce faire, Alice construit **deux clefs distinctes** (d'où l'asymétrie) : une **clef de chiffrement publique**, accessible par tout le monde sur le réseau (par exemple un nombre), et une **clef de déchiffrement privée**, connue seulement par elle (par exemple une méthode mathématique unique pour calculer ce nombre). Si Bob veut envoyer un message à Alice, il utilise la clef publique d'Alice pour le chiffrer, de sorte que seule Alice peut déchiffrer le message avec sa clef privée[9].

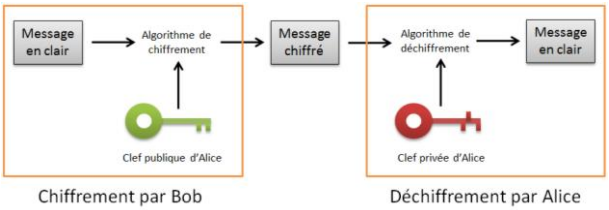

FIGURE 1. PRINCIPE DES PROTOCOLES DE CHIFFREMENT ASYMETRIQUES ENTRE DEUX UTILISATEURS ALICE ET BOB

En pratique, de nombreuses méthodes de chiffrement sont employées, avec le plus souvent une utilisation hybride des techniques symétriques et asymétriques. La cryptographie symétrique, qui peut chiffrer plusieurs giga-octets de données par seconde, est utilisée pour sécuriser les données numériques et les communications quotidiennes[10]. Les algorithmes asymétriques, plus lents (quelques méga-octets par seconde), servent principalement pour échanger les clefs secrètes en amont de ces communications symétriques. Ces derniers sont basés sur des problèmes mathématiques complexes pour un ordinateur, comme le logarithme discret[11]. Historiquement, le plus connu d'entre eux est le **chiffrement RSA, dont le décryptage repose sur la factorisation en nombres premiers** (voir encadré). En effet, ce problème est **particulièrement difficile à résoudre pour les ordinateurs classiques** : en 2010, dans une expérience[12] mise au point pour factoriser un nombre à 232 chiffres, plusieurs centaines d'ordinateurs ont dû fonctionner pendant 2 ans. Le standard de clef utilisé aujourd'hui comporte 617 chiffres décimaux codés sur 2 048 bits (RSA 2048). Il faudrait un temps « supérieur à l'âge de l'Univers » (soit 13,8 milliards d'années) aux meilleurs ordinateurs pour réussir à trouver les facteurs premiers (clé secrète) qui le composent avec les algorithmes connus actuellement[13].

La menace de l'ordinateur quantique

Dès les années 1990, des chercheurs ont mis en évidence le fait qu'un **ordinateur quantique, potentiellement très puissant mais alors encore hypothétique, pourrait décrypter certains chiffrements en un temps record**. L'**algorithme de Shor**, inventé en 1994 pour fonctionner sur un ordinateur quantique, permet de factoriser des nombres entiers en un temps exponentiellement plus rapide[14] que tous les algorithmes classiques connus. **Il menacerait donc la sécurité du RSA actuel[15]**, permettant de retrouver la clef privée (et donc les messages) à partir de la clef publique en seulement quelques minutes. Une variante de l'algorithme permet également des attaques contre d'autres chiffrements asymétriques[16]. Si d'énormes progrès ont été réalisés depuis, les machines actuelles ne comptent que quelques dizaines de qubits[17] et sont donc loin d'être une menace imminente, puisque, **pour utiliser l'algorithme de Shor dans une attaque contre les clefs RSA 1024 ou 2048, il faudrait disposer de plusieurs milliers de qubits[18]**.

Le chiffrement RSA et la factorisation:

Introduit en 1978 par Ronald Rivest, Adi Shamir et Leonard Adleman(*), le chiffrement RSA (du nom de ses inventeurs) repose sur la **factorisation en nombres premiers.** Autant il est facile de calculer un produit de nombres (par exemple 3×5), autant l'opération inverse, dite de factorisation, qui consiste à retrouver 3 et 5 depuis 15 est bien plus difficile pour un ordinateur. L'idée générale du chiffrement est d'utiliser **l'écriture d'un produit de nombres premiers comme clef privée, et la valeur de ce produit comme clef publique**. Lorsque les entiers ont plusieurs centaines de chiffres, il devient impossible de retrouver la clef privée à partir de celle qui est publique.

(*) Ronald Rivest, Adi Shamir et Leonard Adleman, « A method for obtaining digital signatures and public-key cryptosystems », Communications of the ACM, vol. 21, no 2, 1978, p. 120–126

À l'aide d'un ordinateur quantique, des attaques contre les chiffrements symétriques peuvent également être envisagées, notamment grâce à l'algorithme de Grover[19]. Ce dernier permettrait de réduire considérablement le temps d'une recherche exhaustive de la clef secrète, mais en pratique, cette vulnérabilité peut être compensée par un doublement de la taille des clefs. **D'autres formes d'attaques quantiques contre les chiffrements symétriques ont récemment été découvertes[20], ce qui impose de modifier également ces derniers, mais la menace semble moins critique que pour la cryptographie asymétrique.**

Il est impossible de prédire si et quand un ordinateur quantique suffisamment puissant sera disponible pour réaliser des attaques. Néanmoins, certains experts estiment qu'il existe 50 % de chances qu'au moins une des méthodes de cryptographie existante soit brisée dans les quinze prochaines années[21]. Mettre au point de nouvelles méthodes de chiffrement prend du temps dans la mesure où leur solidité doit être minutieusement testée et mise à

l'épreuve. De cette manière, **un système est généralement considéré comme robuste après environ une dizaine d'années de tests concluants**. D'autre part, la **transition vers ces nouveaux systèmes s'étalera sur plusieurs années**, en fonction du temps nécessaire pour modifier tous les algorithmes déjà déployés dans des applications[22]. Enfin, **certaines données produites aujourd'hui doivent rester protégées pendant plusieurs décennies** - jusqu'à 60 ans pour les plus sensibles en matière de défense nationale. Il importe donc de les chiffrer avec un protocole qui ne pourra pas être décrypté dans les années à venir. En dépit du niveau d'incertitude qui entoure l'ordinateur quantique, **il semble prudent de développer dès à présent une cryptographie résistante à cette nouvelle menace qui reste future et non totalement déterminée.**

Vers une cryptographie post-quantique

Face à ce constat, le *National Institute of Standards and Technology* (NIST) américain a lancé en 2017 un appel à projets mondial[23] pour la définition de nouveaux **standards de cryptographie dits « post-quantiques », *i.e.* résistants aux attaques de l'ordinateur quantique**, à la fois pour le chiffrement, la signature numérique et l'échange de clé. Si des recherches étaient déjà menées dans le domaine, elles restaient principalement au stade de la théorie ; l'appel du NIST a permis de fédérer la communauté cryptographique mondiale vers un objectif concret[24]. Ces méthodes reposent à nouveau sur des problèmes mathématiques abstraits de différentes natures[25]. Au total, 82 algorithmes[26] de 26 pays différents ont été proposés. En janvier 2019, 26 candidats ont été retenus[27], dont une dizaine émane en partie de chercheurs français, notamment de l'INRIA et du CNRS, au terme d'une première phase de sélection menée par le NIST et s'appuyant sur les nombreux travaux des experts internationaux. Une ou deux phases supplémentaires sont prévues d'ici 2022, pour déterminer les algorithmes les plus résistants et les nouveaux standards de cryptographie. De son côté, la Chine a lancé sa propre compétition, officiellement ouverte à tous, mais sur une plateforme rédigée en mandarin, non traduite.

En France, le **projet RISQ[28], labellisé « Grand Défi du numérique »** dans le cadre du Programme d'Investissement d'Avenir, ambitionne de regrouper les compétences françaises en cryptographie post-quantique. Il fédère plusieurs acteurs industriels (Thalès, Secure-IC, CryptoExperts) et académiques (INRIA, CNRS), afin de donner à la filière cryptographique française un poids dans la définition de nouveaux standards[29]. **La France dispose de certains des meilleurs experts du post-quantique, et plus généralement d'un excellent tissu de recherche et d'enseignement en cryptographie, qu'il convient de mettre en valeur, notamment dans l'industrie.**

Néanmoins, la transition vers ces nouvelles méthodes comporte de nombreux obstacles : elles ne sont pas encore matures, que ce soit au niveau de la conception ou de l'implémentation, et ne le seront pas avant 5 à 10 ans d'études. La situation est similaire à celle du protocole RSA dans les années 1990 : dès sa découverte, il a suscité un fort engouement, pourtant les premières années de son utilisation ont révélé que de nombreuses précautions d'emploi devaient être prises[30] car la recherche manquait de recul. Dans ce cadre, il importe **d'éviter une régression vers des méthodes d'échange de clé asymétrique vulnérables à un ordinateur classique**. Pour maintenir au moins le niveau de sécurité qui existait jusqu'à présent, **l'ANSSI[31] recommande à court et moyen terme une solution hybride : combiner une méthode classique éprouvée à une méthode post-quantique[32]**.

L'intrication et la cryptographie quantique

En parallèle de la cryptographie post-quantique (qui repose, en réalité, sur des algorithmes de chiffrement classiques), et pour anticiper la nouvelle génération de protection des communications, se développe **la cryptographie quantique**[33]. Celle-ci utilise les principes de la mécanique quantique, à savoir la superposition et l'intrication (cf. encadré), et repose sur les propriétés physiques du milieu porteur de la communication. De manière très générale, la cryptographie quantique permet de générer des clefs, localement ou à distance[34] puis de les utiliser dans des protocoles de chiffrement (symétriques ou asymétriques) classiques, ou à terme, post-quantiques. Concrètement, il s'agit de coder l'information que l'on souhaite échanger sur l'état d'un système physique quantique (un état correspond à une information). La méthode la plus utilisée actuellement utilise la polarisation de la lumière[35], via les photons, particules vecteurs de lumière.

Cette méthode consiste à produire des photons uniques au moyen d'une source spécifique (le plus souvent une boîte quantique semiconductrice[36]). L'information est alors codée sur une caractéristique du photon, telle que sa fréquence ou sa polarisation. En application du principe de superposition, il existe alors une quasi-infinité d'états disponibles pour ce photon[37], contrairement au cas binaire classique où l'information ne peut prendre que les valeurs 0 et 1. L'utilisateur A peut alors envoyer, en clair, son information codée sur l'état d'un photon unique vers l'utilisateur B qui pourra la lire. Cette méthode permet, par exemple, de partager une clef publique.

De plus, au moyen d'une autre source de photons (un cristal non linéaire[38] par exemple), une paire de particules intriquées peut être produite pour coder l'information sur un objet quantique composé de deux « sous-systèmes » qui resteront intriqués de leur création jusqu'à leur détection. En mécanique quan-

tique, la mesure « perturbe » l'état du système. Préparés dans des états initiaux parfaitement prédéfinis (par exemple en termes de polarisation ou de fréquence), les deux photons sont envoyés aux utilisateurs munis de détecteurs calibrés. Les deux propriétés précédentes assurent **qu'une mesure chez l'utilisateur A a une incidence instantanée chez l'utilisateur B**. Très utile pour partager des clefs privées, cette méthode, appelée **Distribution quantique de clefs (QKD)**[39], permet aussi de détecter très efficacement les « intrusions » sur un réseau de communication.

La superposition et l'intrication quantiques:

En physique classique, un objet physique (un atome…) peut être modélisé par un point qui se trouve à une position précise à un temps donné. On les distingue des ondes, qui caractérisent une perturbation qui se propage dans l'espace.

En physique quantique, les deux concepts fusionnent pour expliquer le comportement des objets à l'échelle atomique : c'est la dualité onde-corpuscule. On ne peut alors plus prédire la position exacte d'un corps à un instant donné, mais seulement la probabilité de le trouver en un endroit donné. Ces phénomènes, assez contre-intuitifs, se trouvent à l'origine des deux principaux concepts utilisés par la majorité des technologies utilisant la mécanique quantique : la superposition d'états et l'intrication.

La **superposition** est la capacité d'un corps quantique à se trouver dans plusieurs états en même temps. L'état global d'un système à un instant donné devient donc une combinaison de tous les états possibles à cet instant.

L'**intrication** permet la connexion entre deux objets quantiques et leurs informations. Une modification d'état chez l'un entraine un changement chez l'autre de manière **instantanée**. Il faut alors considérer la paire comme un système unique, inséparable et global (les propriétés de la paire ne sont pas simplement égales à la réunion des propriétés des deux corps).

Ces méthodes ont été rendues possibles grâce aux récents progrès technologiques issus de la mécanique quantique[40] qui atteignent déjà des niveaux avancés allant jusqu'à la commercialisation. Ainsi, pour les élections du Canton de Genève, en Suisse, est utilisée depuis 2007[41] une liaison quantique terrestre offerte par la société suisse ID-Quantique[42] pour sécuriser l'envoi des relevés de vote en ligne sur 300 km[43]. **L'utilisation de photons comme support quantique de l'information permet notamment d'utiliser les réseaux de fibres optiques déjà installés et de réduire les coûts d'infrastructure.** Aujourd'hui, le coût de l'installation d'une ligne de communication quantique est estimé à 100 000 euros, avec un potentiel de réduction par un facteur 10 d'ici 5 ans[44]. Cependant, la décohérence[45] quantique constitue le principal verrou technologique car elle limite les distances sur lesquelles l'intrication peut être maintenue. Toute une R&D se met en place pour développer des répéteurs quantiques, qui permettraient de relayer, de façon synchronisée, l'information quantique à deux endroits distants sur la ligne de communication.

Les liaisons satellitaires sont aussi concernées : en 2016, un satellite chinois, avec à son bord une source quantique, a permis de distribuer des photons intriqués entre deux récepteurs séparés de 1 200 km[46] au lieu d'une centaine de km jusqu'alors. Le satellite Micius a été développé par la *Chinese Academy of Sciences* avec le soutien de *l'University of Vienna*. Cette expérience offre une alternative aux liaisons quantiques terrestres limitées et ouvre la voie à des communications quantiques à longue distance voire intercontinentales, **premières briques d'un éventuel futur réseau Internet quantique** ultra-sécurisé. Pour l'implémenter à l'échelle mondiale, ce réseau devra être multiforme, c'est-à-dire combiner des liaisons satellites (spatial), comme dans l'expérience chinoise, et le réseau de fibres optiques déjà existant (terrestre). Globalement, les puissances asiatiques semblent avoir fait le choix d'investir dans le déploiement de lignes de communications quantiques[47], tandis que l'Europe et les États-Unis se focalisent plutôt sur de nouvelles méthodes post-quantiques (via l'appel du NIST).

Reste que ces différents scénarios ne permettent pas aujourd'hui d'envisager le remplacement de l'échange de clé classique (actuel ou post-quantique) par la cryptographie quantique dans la plupart des situations (équipements mobiles, communications internet passant par de nombreux relais intermédiaires...).

Perspectives

Face à la menace de l'ordinateur quantique vis-à-vis des algorithmes actuels de sécurisation des données, deux grands axes de transition se mettent en place : d'une part, la **cryptographie post-quantique**, qui vise à étudier de nouveaux problèmes **mathématiques** sous-jacents aux protocoles de chiffrement, d'autre part, la **cryptographie quantique**, qui modifie le **support physique** de l'information et utilise les nouvelles technologies quantiques. Si cette menace s'inscrit plutôt à moyen, voire à long terme, ces deux techniques demandent de l'**anticipation** et des améliorations **à la hauteur des enjeux** ; notamment la sécurisation quasi-parfaite des données et des communications avec une qualité au moins équivalente à celle d'aujourd'hui[48]. Les deux axes de transition demanderont encore des années de R&D, mais **cette évolution, inévitable, requiert des choix stratégiques pour les États, dès maintenant**.

Sites Internet de l'OPECST :
http://www.assemblee-nationale.fr/commissions/opecst-index.asp
http://www.senat.fr/opecst/

Experts consultés

M. Alain Aspect, physicien à l'Institut d'Optique, membre du Conseil scientifique de l'Office.

Mme Astrid Lambrecht, directrice de recherche au CNRS, directrice de l'Institut de physique du CNRS (INP/CNRS), membre du conseil scientifique de l'Office.

ANSSI (M. Guillaume Poupard, directeur général ; M. Vincent Strubel, sous-directeur expertise ; M. Sébastien Kunz-Jacques, chef adjoint de la division scientifique et technique ; M. Henri Gilbert, chef du laboratoire de cryptographie ; M. Jérôme Plût, chercheur au laboratoire de cryptographie).

Mme Fanny Bouton, journaliste spécialisée dans les nouvelles technologies.

M. Antoine Browaeys, Directeur de Recherche au CNRS, laboratoire Charles Fabry de l'Institut d'Optique..

Mme Anne Canteaut, directrice de recherche à l'INRIA, équipe-projet SECRET.

M. Philippe Chomaz, directeur scientifique exécutif de la Direction de la recherche fondamentale au CEA.

M. Thierry Debuisschert, ingénieur de recherche, Thalès.

M. Bruno Desruelle, PDG de la start-up Muquans.

Mme Eleni Diamanti, chargée de recherche au Laboratoire d'Informatique de Paris 6 (LIP6).

M. Philippe Duluc, directeur technique big data & security d'Atos.

M. Daniel Estève, directeur de recherche et chef du groupe Quantronique au CEA.

M. Olivier Ezratty, consultant spécialisé en nouvelles technologies et auteur du blog "Opinion libres".

M. Adrien Facon, chef de file du Programme RISQ, Directeur de la Recherche et de l'Innovation chez Secure-IC.

M. Philippe Grangier, Directeur de Recherche CNRS et Responsable du Groupe Optique Quantique à l'Institut d'Optique.

M. Serge Haroche, professeur émérite au Collège de France, prix Nobel de physique 2012.

M. Christophe Jurczak, directeur général du fonds d'investissement Quantonation.

M. Anthony Leverrier, chargé de recherche à l'INRIA, équipe-projet SECRET.

M. Grégoire Ribordy, co-fondateur et PDG de la start-up ID Quantique.

Mme Pascale Senellart, directrice de recherche au Laboratoire de photonique et nanostructures (LPN) du CNRS. Co-fondatrice de la start-up Quandela.

M. Sébastien Tanzilli, Directeur de recherche et chargé de mission au CNRS sur les technologies quantiques.

M. Georges Uzbelger, AI/Advanced Analytics Solution chez IBM France.

M. Benoit Wintrebert, Conseiller en Innovation au Ministère des Armées.

Coordination scientifique de Mme Sarah Tigrine, conseillère scientifique (avec la participation de M. Gaëtan Douéneau).

Ouvrages de référence consultés :

- « Comprendre l'informatique quantique » O. Ezratty, novembre 2018 (e-book)

- Rapport des Académies américaines : National Academies of Sciences, Engineering, and Medicine. 2018. Quantum Computing : Progress and Prospects. The National Academies Press, Washington, DC. DOI : https ://doi.org/10.17226/25196.

- « Clefs du CEA » N° 66- juin 2018 « révolutions quantiques »

Nota : en accord avec la déontologue de l'Assemblée nationale, Cédric Villani s'est mis en retrait de sa participation au Conseil scientifique d'ATOS – organe non décisionnel – pour la durée de ses travaux pour l'Office portant sur les technologies quantiques.

Références

(1) Le concept de « communication » désigne toutes les étapes du protocole d'échange d'informations c'est à dire générer, distribuer, traiter et stocker les données.

(2) Aussi appelées « signature électronique », ces méthodes permettent de certifier qu'un message provient bien de l'expéditeur indiqué, et qu'il n'a pas été modifié pendant son acheminement. Sans elles, il devient possible pour un individu malintentionné de se faire passer pour une autre entité, par exemple pour envoyer des mails frauduleux (« hameçonnage »).

(*3*) La célèbre machine Enigma a été mise au point par l'allemand Arthur Scherbius en 1919 et a été largement reprise par l'armée allemande dès les années 1930. Via un procédé électromécanique, elle a servi à chiffrer et déchiffrer les messages militaires et était réputée inviolable. Pendant la Seconde guerre mondiale, les Alliés, notamment grâce aux travaux d'Alan Turing, ont fini par déchiffrer

une grande partie des messages interceptés, ce qui selon certains experts a permis d'écourter le conflit d'au moins deux ans (http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF).

(4) Le terme « cryptanalyse » désigne le processus d'attaque d'un système de cryptographie pour révéler le message chiffré, sans connaître la clef.

(5) Shannon, C. E. (1948). A mathematical theory of communication. Bell system technical journal*, 27(3), 379-423.*

(6) En 1973, le NIST lance un appel pour définir un nouveau standard de chiffrement. IBM propose alors son algorithme, dénommé Lucifer. Ce dernier, qui comporte quelques failles, sera retravaillé par la NSA et la version finale, appelée DES, sera finalement implémentée en 1976.

(7) Alice et Bob sont des figures couramment utilisées en cryptographie, depuis les années 1970, en remplacement de « utilisateur A » et « utilisateur B ».

(8) On peut également imaginer que les messages transitent dans un coffre-fort, dont seuls Alice et Bob ont la clef.

(9) Ici, il faut voir la clef publique comme un coffre-fort et la clef privée comme le code de ce coffre. Alice envoie le coffre-fort ouvert à Bob et en garde le code. Quand Bob veut envoyer un message à Alice, il le met dans le coffre et le referme, avant de l'envoyer. La seule personne à pouvoir l'ouvrir et lire le message est alors Alice.

(10) Le chiffrement symétrique, via le protocole AES, est notamment utilisé pour les transactions Web, les cartes de transport, le Wi-Fi… https://www.larecherche.fr/la-fragilit%C3%A9-inattendue-du-chiffrement-sym%C3%A9trique.

(11) En mathématiques, le logarithme d'un nombre Y est le nombre X tel que $2^x = Y$. Le problème du logarithme discret consiste, étant donnés deux éléments a et b, à trouver l'entier k tel que $a^k = b$. Un chiffrement asymétrique peut être construit à partir de ce problème, en utilisant k comme clef privée et le couple a,b comme clef publique. Sa sécurité (l'impossibilité de retrouver la clef privée depuis la clef publique) tient au fait que le logarithme discret est extrêmement difficile à calculer par les ordinateurs.

(12) Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., ... & Te Riele, H. (2010, August). Factorization of a 768-bit RSA modulus. In CRYPTO 2010 – 30th Annual Cryptology Conference (pp. 333-350). Springer, Berlin, Heidelberg.

(13) https://www.larecherche.fr/informatique-cryptographie/%C2%AB-la-meilleure-garantie-de-s%C3%A9curit%C3%A9-est-l%C3%A9preuve-du-temps-%C2%BB

(14) L'algorithme de Shor permet de factoriser des nombres en temps *polynomial* (i.e. dont le temps d'exécution est de la forme n^a, où n dépend de la taille du nombre fourni et a est une constante fixée). À l'opposé, les meilleurs algorithmes classiques pour le problème de factorisation ont un temps d'exécution quasiment exponentiel (de la forme 2^n), ce qui devient déraisonnablement plus long quand les données d'entrée sont grandes. À titre d'exemple, 2^{100} est supérieur à l'âge de l'univers, exprimé en secondes.

(15) En plus de RSA, de nombreux protocoles de sécurisation d'Internet sont menacés, avec par exemple : TLS/SSL qui protègent les sites web et les transferts de fichiers via FTP, le protocole SSH d'accès à distance à une machine, PGP qui est parfois utilisé pour chiffrer les emails... La menace s'étend aussi à la signature électronique de logiciels et donc leurs mises à jour automatiques, les VPN pour l'accès à distance aux réseaux d'entreprises protégés, la sécurisation des emails avec S/MIME, les systèmes de paiement, DSA (Digital Signature Algorithm, un protocole de signature électronique), Diffie-Hellman pour l'envoi de clés symétriques et la cryptographie à courbes elliptiques. Enfin, les protocoles de signature électronique du Bitcoin et de nombreuses blockchains sont aussi menacés (source : O. Ezratty).

(16) Une variante de l'algorithme de Shor pourrait notamment s'appliquer au problème du logarithme discret (voir note 10), utilisé dans de nombreux autres chiffrements asymétriques.

(17) Dans un ordinateur classique, la brique élémentaire d'information est le bit : il s'agit d'une unité qui peut prendre deux valeurs (états) possibles soit 0 soit 1. Dans le monde de l'informatique quantique, son équivalent s'appelle le qubit. Concrètement, il s'agit d'un système physique (atomes, ions…) dans un état quantique. Grâce au principe de superposition, l'état d'un qubit est une combinaison linéaire des états 0 et 1 ; et, grâce à l'intrication, différents qubits peuvent être liés entre eux. En physique classique, ajouter un bit supplémentaire permet de décrire seulement une valeur de plus ; en physique quantique, l'ajout d'un nouveau qubit double la puissance de calcul. Ainsi, une machine quantique de 10 qubits peut traiter simultanément 2^{10}=1024 valeurs (contre 10 pour une machine classique de 10 bits).

(18) Il faudrait disposer de quelques milliers de qubits « logiques », c'est-à-dire parfaits. En pratique cependant, les qubits physiques sont imparfaits et l'on obtient de bons qubits logiques en combinant un grand nombre de qubits physiques (voir la note de l'Office n 15 : « Les technologies quantiques : l'ordinateur quantique »). Pour l'algorithme de Shor, les estimations optimistes requièrent de la dizaine à la centaine de millions de qubits physiques.

(19) Pour retrouver une clef de n bits utilisée par un algorithme de chiffrement symétrique ne possédant pas de faiblesse particulière, un ordinateur classique doit essayer toutes les combinaisons possibles, ce qui requiert jusqu'à 2^n opérations. Ce nombre est généralement trop grand pour que l'attaque soit réalisable. Ainsi pour le standard AES, la clef est longue de 128 bits, et $2^{128} \approx 10^{39}$ est un nombre à 39 chiffres, alors que les meilleurs supercalculateurs savent traiter seulement 10^{15} opérations par seconde. L'algorithme de Grover, introduit en 1996, ne nécessite que $2^{n/2}$ opérations pour retrouver la clef. Dans l'exemple de l'AES, il suffirait donc de $2^{64} \approx 10^{20}$ opérations, ce qui est beaucoup plus proche du calculable. Pour revenir à un niveau de sécurité convenable, une solution possible serait d'utiliser une clef deux fois plus longue. L'AES peut effectivement fonctionner avec des clefs de $2 \times 128 = 256$ bits ; c'était d'ailleurs l'un des arguments qui ont conduit à le choisir comme standard.

(20) Le projet QUASYModo à l'INRIA s'intéresse à cette question : https://project.inria.fr/quasymodo/

(21) Selon Michele Mosca, chercheur à l'Université de Waterloo (Canada) : https://www.larecherche.fr/informatique-cryptographie/%C2%AB-la-meilleure-garantie-de-s%C3%A9curit%C3%A9-est-l%C3%A9preuve-du-temps-%C2%BB

(22) Historiquement, certains protocoles de chiffrement ont continué à être utilisés plusieurs années après avoir été cassés (par un ordinateur classique), parce que l'infrastructure réseau n'avait pas été modifiée.

(23) https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

(24) Ce mode de compétition scientifique n'est pas une nouveauté et historiquement, le NIST est déjà à l'origine de l'élaboration de plusieurs standards de cryptographie tels qu'AES (Advanced Encryption Standard, 2002) ou SHA-3 (2012).

(25) La plupart des problèmes mathématiques utilisés par les soumissions au NIST se regroupent en quatre grandes catégories en fonction des objets mathématiques qu'ils utilisent : les codes correcteurs d'erreurs, les réseaux euclidiens, les polynômes multivariés et les isogénies de courbes elliptiques.

Depuis plusieurs décennies, les codes correcteurs d'erreurs sont utilisés afin d'éviter que certaines données soient « perdues » lors de leur transmission, par exemple si le canal de communication introduit du bruit dans les messages. Ils sont également utilisés pour les CD ou DVD, afin qu'une petite imperfection ne rende pas un fichier illisible. En 1978, soit quelques mois après la découverte de RSA, R. J. McEliece a montré comment utiliser ces techniques pour construire un système de cryptographie asymétrique. Ce chiffrement a été amélioré depuis, mais son défaut majeur est d'avoir des clés publiques de grande taille.

Introduite en 1996, la cryptographie des réseaux euclidiens est fondée sur la résolution de systèmes d'équations diophantiennes linéaires (équations sur les nombres entiers). Sous certaines hypothèses, la résolution de ces systèmes est un problème très difficile du point de vue calculatoire. On peut alors utiliser un système d'équations comme clef publique, et une méthode de résolution comme clef privée.

Un polynôme à plusieurs variables (par exemple x, y et z) est une expression P faisant intervenir des sommes et des produits de ces variables (par exemple $P = xy + y^2+z^3x + z$). L'idée de la cryptographie multivariée, introduite en 1988, est d'utiliser plusieurs polynômes de cette forme (par exemple P, Q et R). Si l'on connaît les valeurs de x, y et z, il est très facile de calculer celles de P, Q et R ; en revanche, l'opération inverse est particulièrement ardue pour les ordinateurs. Pour le système de chiffrement, il est donc possible d'utiliser les polynômes comme clef publique, et une « méthode d'inversion » comme clef privée. Afin que l'inverse ne soit pas facilement calculable, il est nécessaire d'utiliser un très grand nombre de variables, ce qui limite la rapidité du chiffrement.

Les courbes elliptiques sont un objet mathématique bien connu en cryptographie, à l'origine de plusieurs protocoles de chiffrement actuels (voir avant). Dans le cadre des chiffrements post-quantiques, les chercheurs ne les utilisent pas directement, mais s'intéressent à certaines fonctions appelées isogénies, qui permettent de passer d'une courbe à une autre en préservant leur structure.

(26) Seule une minorité d'entre eux est soumise à un brevet, critère qui est également pris en compte négativement dans leur évaluation dans le cadre de cet appel à projets ouvert. Les modalités sont disponibles sur le site du NIST : https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

(27) https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

(28) https://risq.fr/?page_id=8&lang=fr

(29) Les entreprises financent une partie du projet sur leurs fonds propres. L'assiette prévisionnelle de dépenses de l'initiative RISQ s'élève à environ 8 millions d'euros.

(30) https://www.pourlascience.fr/sr/article/strategies-dattaques-4764.php

(31) Agence Nationale de la Sécurité des Systèmes d'Information (http://ssi.gouv.fr/).

(32) L'ajout de la « surcouche » constituée d'une méthode classique éprouvée n'alourdit les traitements que de quelques pourcents par rapport à l'emploi de méthodes post-quantiques seules car les méthodes classiques restent très légères après des années de développement. À titre d'exemple, voici les tailles des messages émis pour les mécanismes ECDH-256 (classique) et NewHope512 (l'un des candidats post-quantiques les plus compacts) : 32 octets pour ECDH contre 1120 octets pour NewHope. Ajouter une surcouche ECDH sur un échange NewHope entraîne donc un surcoût d'un peu moins de 3 %, et permet de garantir une non-régression de la sécurité par rapport aux techniques actuelles.

(33) Le terme « post-quantique » désigne toute méthode résistante à la puissance d'un ordinateur quantique, et se comprend comme « post-ordinateur quantique ». En parallèle, le terme « cryptographie quantique » désigne les méthodes d'échange de clé qui reposent sur une infrastructure utilisant des propriétés quantiques, mais qui ne correspondent pas à de la cryptographie au sens large. Pour ces deux axes, il est fort probable que les dénominations, peu précises et portantes à confusion, évoluent au fur et à mesure des développements technologiques dans les prochaines années.

(34) La cryptographie quantique ne peut être employée qu'entre correspondants disposant d'une liaison physiquement directe, comme une fibre optique ou une liaison à l'air libre.

(35) Plus généralement, la polarisation d'une onde décrit une orientation privilégiée dans la répartition des oscillations qui la composent. Une polarisation peut être unidirectionnelle (polarisation linéaire, verticale ou horizontale par rapport au sens de propagation). Dans le cas d'une onde électromagnétique, si les composantes électriques et magnétiques sont déphasées de 90°, la polarisation peut alors être circulaire ou elliptique.

(36) Souvent appelée par son nom anglais « quantum dot », une boite quantique (de taille nanométrique) consiste en une insertion d'un matériau semi-conducteur dans un autre, constituant un piège très efficace pour les électrons. Ces derniers émettront des photons un par un, avec des caractéristiques (longueur d'onde, flux) plus ou moins maitrisables. L'enjeu actuel de R&D pour une utilisation en communication est de ne pas générer trop d'impulsions contenant plus d'un photon, ce qui, en contrepartie, réduit le débit d'émission de photons et donc la qualité de la communication (https://www.photoniques.com/articles/photon/pdf/2015/04/photon201577p36.pdf). La société française Quandela s'est spécialisée dans cette technologie.

(37) En physique quantique, les échanges d'énergie se font de manière discontinue par paquets appelés « quantas ». Cf. la note n°13 « Technologies quantiques : introduction et enjeux » de l'Office : http://www2.assemblee-nationale.fr/content/download/79022/810034/version/2/file/Note_TechnologiesQuantiques_Introduction_versionFinale.pdf

(38) L'optique non linéaire s'intéresse aux milieux qui modifient, en sortie, les propriétés de la lumière qu'ils reçoivent. Plus particulièrement, les cristaux non linéaires permettent de produire une paire de photons à partir d'un photon unique en scindant son énergie en deux.

(39) Diamanti, Eleni, et al. "Practical challenges in quantum key distribution." npj Quantum Information 2 (2016): 16025.

(40) Notamment, le développement de méthodes pour produire des photons uniques ou des paires de photons intriqués a été un véritable levier pour mettre au point ces techniques.

(41) https://www.ge.ch/document/etat-geneve-mise-cryptographie-quantique

(42) https://www.idquantique.com/

(43) https://www.ge.ch/document/etat-geneve-mise-cryptographie-quantique

(44) Communication de la société ID Quantique.

(45) Le phénomène de décohérence traduit une perte de l'information quantique vers l'environnement du système. La fonction d'onde (l'état) du système est « brouillée » par les multiples interactions extérieures et finit par perdre son caractère ondulatoire et donc sa dimension quantique. La notion de décohérence a été mise en évidence en 1970 par le physicien Dieter Zeh et permet de mieux appréhender la frontière entre le monde quantique et classique : les objets classiques ne sont que des objets quantiques qui ont subi une décohérence par interaction avec leur environnement.

(46) https://science.sciencemag.org/content/356/6343/1140 pour l'article scientifique et pour une bonne analyse des enjeux : https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

(47) En complément, d'autres projets existent en Asie : depuis 2011, la ville de Tokyo a déployé un réseau de communication quantique permanent ; la Chine souhaite l'installation d'une ligne quantique entre Pékin et Shanghai (sur une distance d'environ 1 000 km). Enfin, la société Sud-coréenne SK Telecom est devenue actionnaire majoritaire d'ID Quantique, notamment afin de sécuriser au sol les prochains réseaux de 5G.

(48) En termes de sécurité, de débit, de portée et de vitesse.