LE GRAND DEFI DU POST-QUANTIQUE

MISC HS n° 013 | avril 2016 | Ludovic Perret - Jean-Charles Faugère

Sécurité

En août 2015, la NSA a surpris le monde de la cybersécurité en faisant une annonce très surprenante à l'intention des entreprises et administrations américaines. Elle recommande de préparer le basculement de la cryptographie à clef publique classique fondée sur la théorie des nombres vers des systèmes résistants à l'ordinateur quantique. Depuis, l'organisme de normalisation américain NIST a lancé la course post-quantique avec un appel international pour la création de standards à l'épreuve de l'ordinateur quantique.

Le prix Turing – équivalent du prix Nobel en informatique – a récompensé cette année les deux cryptologues W. Diffie et M. Hellman pour leur protocole d'échange de clefs et l'invention de la cryptographie à clef publique. Ces idées révolutionnent la cryptographie à la fin des années 80 et permettent aujourd'hui à des millions d'utilisateurs du Web de communiquer de manière confidentielle. La sécurité du protocole de Diffie-Hellman, et plus généralement la cryptographie à clef publique, repose sur des problèmes mathématiques réputés difficiles. Par exemple, le protocole Diffie-Hellman est basé sur la difficulté de trouver un logarithme discret (DLOG) dans des corps finis ou des courbes elliptiques. Le chiffrement à clef publique RSA – du nom de ses inventeurs R. Rivest, A. Shamir, L. Adelman eux aussi prix Turing en 2002 – repose sur la difficulté de décomposer des grands nombres en produits de facteurs premiers (problème FACT).

La plupart des protocoles utilisant la cryptographie à clef publique (https, IPSEC...) reposent uniquement sur la difficulté des problèmes FACT et DLOG. Ainsi, une percée technologique ou mathématique remettant en cause la difficulté de ces problèmes rendrait vulnérables toutes les communications, et paralyserait, par exemple, le commerce électronique. C'est le scénario de la « cryptocalypse » ; une défaillance simultanée dans la difficulté des deux problèmes mathématiques qui garantissent la sécurité des échanges électroniques mondiaux.

En l'état de nos connaissances et avec la technologie actuelle, nous sommes encore loin de cette situation. Avec des paramètres appropriés, RSA et Diffie-Hellman sont encore considérés comme sûrs. Toutefois, on sait depuis 20 ans déjà que la cryptographie à clef publique basée sur DLOG et FACT est menacée par une percée technologique : les ordinateurs quantiques.

Il existe déjà des machines quantiques qui sont commercialisées par la start-up canadienne D-WAVE **[DWAVE]**. La puissance véritable de ces machines reste encore aujourd'hui un sujet controversé. D'autre part, la machine D-WAVE n'est pas un calculateur quantique complet et permet « uniquement » de résoudre des problèmes de type optimisation.

À notre connaissance, il n'existe pas aujourd'hui d'ordinateur quantique (complet) suffisamment puissant pour factoriser des grands nombres. Le plus grand nombre jamais factorisé avec un processus quantique est 56153. Pour attaquer RSA, il faut factoriser un nombre 130 fois plus gros.

La construction d'un ordinateur quantique reste un risque difficile à mesurer en cryptographie. Certains spécialistes du domaine annoncent l'arrivée imminente d'une telle machine. D'après M. Mariantoni **[M14]**, on pourrait construire une machine quantique d'ici 15 ans pour un budget de un milliard de dollars et il faudrait alimenter cette machine avec une centrale nucléaire. À l'échelle d'un État, cela semble plausible. Inversement, d'autres spécialistes pensent que l'apparition de la machine quantique sera plus lente : au moins 50 ans.

Par conséquent, le pays capable de construire un ordinateur quantique posséderait un atout stratégique majeur. La course technologique pour cette machine est lancée avec des investissements massifs à travers le monde: Union européenne **[EUq]**, Google avec D-WAVE et la NASA **[AiQ]**, Chine **[Ali,XXZH16]** et d'autres. C'est une version moderne de la course pour marcher sur la Lune.

Cependant, il est possible de construire des cryptosystèmes à clef publique avec d'autres problèmes mathématiques et le risque quantique est aujourd'hui jugé suffisamment critique pour que le NIST, organisme de standardisation américain, annonce début 2016 son intention de standardiser des algorithmes à clefs publiques résistants à l'ordinateur quantique **[NISTpq]**. Avec le recul, nous savons qu'un algorithme standardisé par le NIST devient de facto un standard mondial. En cryptographie, un exemple de standard bien connu du NIST est le chiffrement à clef secrète AES. L'Europe n'est pas (trop) en retard sur le sujet puisque l'organisme de normalisation européen (ETSI) travaille sur la standardisation des algorithmes post-quantique **[ETSIpq]** depuis 2015.

Une mini-révolution en cryptographie à clef publique est en marche, et le défi s'annonce colossal **[Mo15]** : la transition de notre infrastructure à clef publique vers des algorithmes post-quantiques.

1. IMPACT DE L'ORDINATEUR QUANTIQUE EN CRYPTOGRAPHIE

L'ordinateur quantique est la promesse d'une machine qui utilise des phénomènes de physique quantique pour décupler sa puissance de calcul. L'ordinateur quantique permet ainsi de résoudre certains problèmes mathématiques beaucoup plus efficacement qu'une machine classique. S. Jordan, chercheur au NIST, tient à jour un « bestiaire » des algorithmes quantiques **[QZoo]** avec une liste quasiment exhaustive des problèmes pouvant se résoudre plus efficacement avec un ordinateur quantique.

L'exemple certainement le plus célèbre des capacités d'un ordinateur quantique est donné par P. Shor. Il propose un algorithme qui est capable de résoudre DLOG et FACT sur une machine quantique en un temps polynomial. Le choc est rude et la conséquence sans appel. Ainsi, dans le monde quantique, RSA et Diffie-Hellman offrent seulement le même niveau de sécurité que la méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes !

La cryptographie à clef secrète est également touchée par l'ordinateur quantique. L'algorithme de Grover permet une accélération quadratique de la recherche exhaustive. Prenons l'exemple de l'algorithme de chiffrement à clef symétrique AES avec une clef secrète de 128 bits. Sur une machine classique, la recherche exhaustive nécessite d'énumérer au plus 2128 clefs. Avec une machine quantique et l'algorithme de Grover, il faut parcourir au plus 264 candidats pour retrouver

la bonne clef. L'impact est ici moins important puisqu'il suffit de doubler la taille des clefs en cryptographie symétrique pour se prémunir de l'ordinateur quantique.

Récemment M. Kaplan, G. Leurent, A. Leverrier, et M. Naya-Plasencia ont montré que l'impact de l'ordinateur quantique sur la cryptographie symétrique ne se limitait pas forcément à l'algorithme de Grover. Les auteurs de cet article utilisent un algorithme quantique encore jamais utilisé en cryptanalyse – l'algorithme de Simon – pour attaquer certains *modes opératoires* des chiffrements symétriques. Un chiffrement symétrique comme l'AES opère sur des blocs de taille fixe, 128 bits. Un mode opératoire est une technique permettant de faire opérer un chiffrement symétrique sur des messages de taille quelconque. L'attaque nécessite toutefois de faire une hypothèse assez forte sur les moyens de l'attaquant. Ceci indique que l'impact de l'ordinateur quantique en cryptographie est une histoire qui n'est pas encore complètement écrite et nous réserve des rebondissements.

Il est important de souligner qu'il existe des problèmes qui sont difficiles à résoudre indépendamment de la machine (quantique ou classique). En théorie de la complexité, nous classifions les problèmes en fonction de leur difficulté intrinsèque. Les problèmes NP-difficiles sont des problèmes pour lesquels il n'existe pas a priori d'algorithme efficace pour les résoudre ; en quantique comme en classique. C'est la fameuse conjecture P différent de NP.

2. CRYPTOGRAPHIE POST-QUANTIQUE

En pratique, nous utilisons la cryptographie à clef publique essentiellement pour l'échange des clefs (en utilisant éventuellement un algorithme de chiffrement à clef publique) et pour l'authentification par certificats (signature). L'objectif de la *cryptographie post-quantique* est de construire des cryptosystèmes (échange de clef, chiffrement, signature...) résistants aux ordinateurs quantiques. Cette cryptographie post-quantique inclue typiquement **[ETSIpq,NISTpq,BBD09]** *la cryptographie multivariée, la cryptographie fondée sur codes correcteurs d'erreurs, la cryptographie fondée sur réseaux euclidiens, et la cryptographie fondée sur des arbres de hachages*.

Il existe d'autres alternatives post-quantiques que nous ne traiterons pas ici comme la cryptographie à base d'isogénies, celle-ci étant plus récente. Nous trouvons également des cryptosystèmes qui utilisent directement la physique quantique. Typiquement, il est possible de construire un protocole d'échange de clef dont la sécurité repose sur des lois physiques. La distribution quantique des clefs est aujourd'hui commercialisée, mais le coût reste trop élevé pour un déploiement à grande échelle.

2.1 CRYPTOGRAPHIE MULTIVARIEE

La cryptographie multivariée consiste à construire des cryptosystèmes dont la sécurité repose sur la difficulté du problème PoSSo : c'est-à-dire de trouver - s'il existe - un zéro commun d'un ensemble de polynômes non-linéaires. Le problème PoSSo est NP-difficile et sa difficulté n'est a priori pas remise en cause par l'émergence d'un ordinateur quantique.

Les bases de Gröbner sont un outil important pour évaluer la sécurité des cryptosystèmes multivariés. Ce concept peut également servir à analyser la sécurité d'autres primitives post-quantiques. Les bases de Gröbner permettent, notamment, de trouver les solutions d'un système d'équations non-linéaires. La complexité des meilleurs algorithmes de base de Gröbner sert souvent de référence pour spécifier en pratique les paramètres des cryptosystèmes multivariés.

En général, la clef publique d'un cryptosystème multivarié est donnée par un ensemble de polynômes non-linéaires. Pour chiffrer un message, il suffit d'évaluer le message sur les polynômes de la clef publique. On donne ci-dessous un exemple jouet de chiffrement en cryptographie multivariée. Nous avons utilisé un logiciel de calcul forme MAGMA pour réaliser cet exemple:

/* Le message à chiffrer est donné sous forme d'un vecteur de bits */

[0, 1, 1, 1, 1];

/* Petit exemple d'une clef publique; 5 polynômes en 5 variables.

[x1*x2 + x1 + x2*x3 + x2*x5 + x2 + x3*x5 + x3 + x4 + 1,

x1*x2 + x1*x3 + x1*x4 + x1 + x2*x3 + x2*x4 + x3 + x4*x5,

x1*x3 + x1*x4 + x1*x5 + x1 + x3 + x4*x5,

x1*x2 + x2*x5 + x2 + x3*x4 + x3*x5 + x3 + x4*x5 + x4 + x5 + 1,

x1*x3 + x1*x5 + x1 + x2*x3 + x2*x4 + x2 + x3 + x4]

/* Pour chiffrer, on évalue les polynômes de la clef publique pour le message x1=0, x2=1, x3=1, x4=1, x5=1, et obtient le message chiffré en prenant le reste modulo 2: */

[1, 0, 0, 1, 1]

La cryptographie multivariée permet aussi d'obtenir des schémas de signature. La clef publique sera toujours donnée par un ensemble de polynômes non-linéaires. La vérification d'une signature consiste simplement à évaluer les polynômes de la clef publique sur la signature.

Le domaine est très dynamique, et de nombreuses constructions sont présentées chaque année par différents auteurs à travers le monde. Certains ne résistent pas à l'analyse de la communauté. Parmi les schémas multivariés ayant résisté à l'analyse des cryptologues, on compte HFE- (*Hidden Field Equations*) **[HFE96]**, UOV (*Unbalanced Oil and Vinegar*) et QUARTZ. Ces schémas suivent tous le principe de chiffrement (ou de vérification d'une signature) que nous venons d'évoquer. Ils diffèrent ensuite sur la méthode de construction de la clef secrète, et donc de la trappe.

Dans HFE, la clef publique est un ensemble de n polynômes non-linéaires en n variables dont les coefficients sont sur F_2 le corps à deux éléments. L'idée est de construire la clef publique à partir d'un polynôme P particulier en une variable définie sur F_{2^n} ; une extension de degré n de F_2.

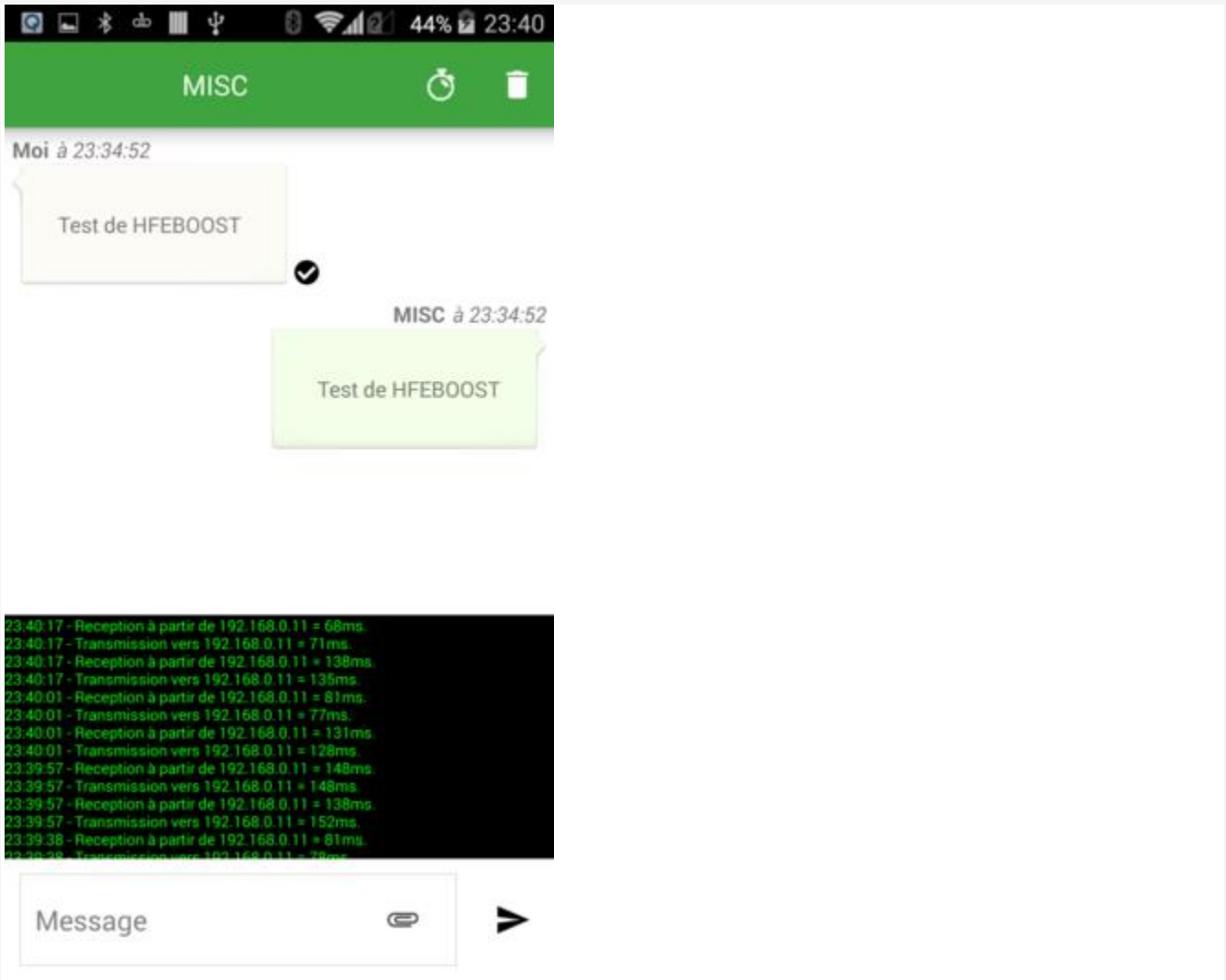
/* Exemple de polynôme de type HFE sur une extension de degré 5; w est un générateur du corps F_{2^5} et X est la variable */

w^7*X^17 + w^29*X^12 + w^11*X^10 + w^29*X^9 + w^26*X^6 + w^28*X^5 + w^6*X^3

Les polynômes de la clef publique sont une *version masquée* des composantes du polynôme P *déplié* sur F_2. Avec la clef secrète, le déchiffrement est alors équivalent à trouver les racines du polynôme en une variable P. Contrairement au problème de trouver les zéros d'un ensemble polynômes non-linéaires qui problème NP-difficile, le problème de trouver les racines est lui bien plus facile. On trouve les racines d'un polynôme en une variable très efficacement ; en un temps quasi-linéaire en son degré.

Le point fort de la cryptographie multivariée est de construire des schémas permettant de signer des messages avec des signatures très courtes. Par exemple, l'algorithme QUARTZ, une variante de HFE-, permet d'obtenir des signatures de l'ordre de 100 bits.

Un point longtemps bloquant était la taille des clefs publiques ; bien plus élevée que les cryptosystèmes classiques basés sur DLOG ou FACT. C'est une caractéristique commune à presque tous les cryptosystèmes post-quantiques.



MISC

Moi *à 23:34:52*

Test de HFEBOOST

Test de

Dans HFEBoost **[PolSys]**, une autre variante du schéma HFE-, que nous avons développé pour des tests de l'armée de terre, la clef publique était de 130 Ko. Typiquement, une clef publique RSA est de 2000 bits. Dans des infrastructures réseaux modernes, ce point n'est plus vraiment handicapant. Les tests terrains pour HFEBoost ont été réalisés sur un réseau 4G. Les clefs publiques transitaient entre des centaines de participants sans problème de latence.

2.2 CRYPTOGRAPHIE FONDEE SUR LES CODES CORRECTEURS

Le cryptosystème de McEliece est le chiffrement à clef publique post-quantique le plus ancien. Sa conception date de 1978 ; juste après l'invention de la clef publique par W. Diffie et M. Hellman. La sécurité du cryptosystème de McEliece repose sur la difficulté de décoder un code linéaire. Nous pouvons voir ce problème comme celui de trouver la solution d'un système linéaire dont une partie des équations est erronée. Il est très simple de résoudre un système d'équations linéaires, mais la tâche est bien plus complexe si les équations comportent des erreurs. Ce problème, dénommé BoundedDecoding, est notoirement difficile. Il a été prouvé NP-Dur et largement étudié. La complexité du meilleur algorithme pour résoudre BoundedDecoding sert de référence pour choisir les paramètres de McEliece.

La clef publique est ici donnée par une matrice à coefficients binaires. Cette matrice n'est pas aléatoire, mais est dérivée d'un *code correcteur d'erreur* particulier: *un code de Goppa binaire*. En résumé, un code correcteur d'erreurs (linéaire) est un espace vectoriel. Nous pouvons ainsi représenter un code linéaire par une matrice génératrice dont les lignes sont les vecteurs d'une base de cet espace vectoriel. Pour les codes de Goppa binaires, nous avons des méthodes efficaces permettant de résoudre le problème BoundedDecoding.

Dans McEliece, le message que l'on souhaite chiffrer est représenté sous la forme d'un vecteur. Pour chiffrer, il faut d'abord choisir un *vecteur d'erreurs*. On chiffre ensuite en multipliant notre message par la matrice publique, puis on ajoute au résultat le vecteur d'erreurs. Pour illustrer le principe, on donne ci-dessous un exemple jouet de chiffrement avec McEliece :

/* Le message à chiffrer est donné par un vecteur 5 bits */

[0, 1, 1, 1, 1];

/* Exemple d'une clef publique; matrice M à coefficients binaires de 5 lignes et 10 colonnes */

[1 0 0 0 0 0 1 1 1 1]

[0 1 0 0 0 1 0 1 0 0]

[0 0 1 0 0 1 0 1 1 1]

[0 0 0 1 0 0 0 0 1 1]

[0 0 0 0 1 1 0 1 1 1]

/* Pour chiffrer, il faut choisir un vecteur d'erreurs */

[1, 0, 0, 0, 0, 0, 0, 1, 0, 1]

/* Ensuite, il faut multiplier le message par la matrice publique M, et ensuite additionner le résultat avec le vecteur d'erreurs (les calculs se font modulo 2). */

/* Voici le message chiffré. */

[1 1 1 1 1 1 0 1 0 1]

Il est également possible d'obtenir un schéma de signature en utilisant l'idée de McEliece [CFS01]. Ce schéma est toutefois moins compétitif qu'une signature multivariée.

Le système de chiffrement proposé par McEliece a résisté à toutes les tentatives de cryptanalyse depuis 1978. C'est remarquable au regard de l'intense activité en cryptographie. En plus de sa résistance à l'ordinateur quantique, le schéma de McEliece présente plusieurs autres avantages vis-à-vis de la cryptographie classique, comme sa vitesse de chiffrement et de déchiffrement. Comme en cryptographie multivariée, un point bloquant pour McEliece était la taille des clés publiques, de l'ordre de 100 fois plus élevé qu'une clef RSA typique. Des tentatives ont été faites pour réduire ces tailles de clé en utilisant des codes plus structurés. Plusieurs travaux, dont **[FOPPT15]**, ont montré que cette approche donnait lieu à des attaques par bases de Gröbner qui se révèlent très dangereuses sur ces familles de codes structurés. La dernière tentative en date pour réduire la taille des clefs consiste à utiliser des codes MDPC.

En définitive, le schéma de chiffrement McEliece dans sa version avec des Goppa binaires reste une référence de sécurité pour cette cryptographie.

2.3 CRYPTOGRAPHIE REPOSANT SUR LES RESEAUX EUCLIDIENS

Cette cryptographie repose sur un autre objet mathématique bien étudié : *les réseaux euclidiens*. Pendant des années, les réseaux euclidiens étaient surtout réputés comme un outil de cryptanalyse. Leur utilisation cryptographique a connu un premier renouveau grâce aux travaux de J. Hoffstein, J. Pipher, et J. H. Silverman sur NTRU et une explosion avec les résultats de O. Regev **[Rev05]**.

O. Regev propose un schéma de chiffrement à clef publique similaire au chiffrement de McEliece. La clef publique est (essentiellement) donnée par une matrice *aléatoire* dont les coefficients sont des entiers modulo un nombre premier. Il s'agit d'une différence importante avec McEliece, puisque la matrice de la clef publique n'est pas aléatoire.

> /* Exemple de la matrice publique dans le schéma de O. Regev. */

[10 18 17 110 103 110 96 115 46 76]

[108 58 15 117 43 29 3 55 17 37]

[74 66 44 82 34 97 63 16 17 11]

[21 107 91 108 43 49 27 112 45 20]

[121 48 41 122 75 59 91 15 93 69]

Dans le schéma de Regev, le chiffrement consiste également à multiplier un vecteur par la matrice publique et tirer un vecteur d'erreurs. Les coefficients du vecteur d'erreurs sont choisis selon une loi de distribution particulière : *une loi Gaussienne discrète*. C'est une autre différence avec McEliece.

Le chiffrement de Regev est particulièrement séduisant, car il est possible de relier la sécurité du cryptosystème à la difficulté de résoudre l'instance la plus difficile d'un problème portant sur les réseaux euclidiens. Cette propriété permet de garantir un haut niveau de confiance.

Les réseaux *euclidiens* offrent aujourd'hui une grande flexibilité pour la conception de cryptosystèmes.

Nous trouvons des protocoles de chiffrement, de signature (BLISS) et bien d'autres ; dont la sécurité repose sur des problèmes difficiles liés aux réseaux *euclidiens.*

Un défi pour cette cryptographie est de réduire l'écart qui existe entre les constructions qui sont « prouvées sûres » et leurs variantes utilisables en pratique. En effet, la taille de certains paramètres nécessaire pour garantir une sécurité prouvée est trop élevée en pratique. Il est donc fréquent d'utiliser les meilleures attaques connues pour réduire la taille de ces paramètres en conservant une certaine sécurité.

2.4 CRYPTOGRAPHIE FONDEE SUR LES ARBRES DE HACHAGES

Le principe de la cryptographie fondée sur les arbres de hachages remonte à L. Lamport en 1979. L'idée est d'utiliser uniquement une fonction de hachage cryptographique. Cette technique permet de construire uniquement des schémas de signature dont la sécurité repose sur la fonction de hachage utilisée. Le schéma proposé par L. Lamport a toutefois un intérêt limité puisque nous pouvons seulement signer un seul message avec la même clef publique sans compromettre la sécurité. R. Merkel propose en 1989 une amélioration du schéma de L. Lamport permettant de signer un nombre plus important de messages en utilisant un arbre de hachage (ou arbre de Merkle). Le nombre de signatures que l'on autorise pour une même clef publique dépend de la profondeur de l'arbre et influence aussi les performances du schéma (taille de la signature). Dans **[XMSS,SPHINCS]**, les auteurs ont amélioré le principe de Merkle. Finalement, nous pouvons obtenir – pour cette famille post-quantique – des schémas de signature avec des performances acceptables. Typiquement, la clef publique dans SPHINCS est de 1Kb, la signature de 41 Kb et permet de signer 250 messages sans compromettre la sécurité.

3. LA COURSE AU POST-QUANTIQUE

Pour un spécialiste du domaine, le changement soudain du statut de la cryptographie post-quantique est impressionnant. En 2012, la conférence « Symbolic Computation and Cryptography », dédiée à l'analyse des systèmes post-quantiques, réunissait une quarantaine de chercheurs. L'année suivante, la conférence « Post-Quantum Cryptography (PQCrypto) », organisée à Limoges, réunissait une audience légèrement supérieure.

En 2016, c'est le boom du domaine. La conférence PQCrypto, qui se déroule au Japon, enregistre un record d'affluence : plus de 222 inscrits. Dans cette foule, nous trouvons des chercheurs, mais également de nombreux industriels (Cisco, Google, Gemalto, Intel, LG, Microsoft, NTT, Toshiba...) qui se pressent pour comprendre le phénomène et prendre le train post-quantique en route.

L'événement déclencheur est une annonce inattendue de la *National Security Agency* (NSA), en août 2015, qui conseille aux administrations américaines d'anticiper dès à présent le basculement vers une cryptographie post-quantique **[NSASuiteb]**. Cette annonce arrive dans une période où la cryptographie à base de courbes elliptiques devait envahir notre quotidien et enfin se substituer à l'utilisation de RSA. D'après la NSA, les courbes elliptiques ne sont pas une technologie d'avenir :

« Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many once hoped it would be. »

Au regard de la réputation de cette agence et des révélations de l'affaire Snowden, l'annonce ne manque pas de faire réagir : la NSA possède-t-elle un ordinateur quantique ? La NSA manipule-t-elle encore une fois les standards à son avantage ? La NSA sait-elle « casser » les courbes elliptiques ? La NSA pense-t-elle que d'autres pays sont en passe de construire un ordinateur quantique ? … Nous laissons le lecteur se forger une opinion sur la question. Une référence sur ce sujet est l'article de N. Koblitz et A. Menezes **[KM15]**.

Aujourd'hui, le risque de l'ordinateur quantique est perçu comme très élevé. Concernant les secrets ayant une longue durée de vie (typiquement les données gouvernementales et les données médicales) la menace est jugée crédible. Le PIDS, un équivalent hollandais de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), recommande dès aujourd'hui de « surchiffrer » ces données avec un chiffrement classique et un chiffrement post-quantique. D'autre part, le déploiement total d'un nouveau standard cryptographique nécessite au moins 20 ans. Le lecteur de *MISC* sait que ce déploiement est un parcours semé d'embûches. La solidité mathématique d'un algorithme n'est pas l'unique composante dans la chaîne de la sécurité. Il faut aussi prendre en compte les problèmes au niveau de l'implémentation et l'interaction de la brique post-quantique avec des protocoles de plus haut niveau comme TLS, SSH et IPSEC. Ces derniers aspects ont été très peu étudiés jusqu'à présent. Le NIST, l'ETSI et d'autres institutions, jugent ainsi qu'il est nécessaire d'agir dès maintenant.

Le NIST a ainsi lancé un appel international pour normaliser des algorithmes post-quantiques **[M16]**. En priorité, le NIST souhaite avoir des standards pour deux fonctionnalités : signature numérique et échange des clefs. Le NIST a appelé la communauté mondiale à soumettre ses meilleurs algorithmes post-quantiques d'ici la fin 2017. Il s'ensuivra une période d'étude des algorithmes d'environ trois ans au bout de laquelle le NIST sélectionnera un ou plusieurs algorithmes post-quantiques en fonction du niveau de confiance que la communauté scientifique accorde aux candidats. Ce n'est pas une compétition puisque le NIST s'autorise à sélectionner plusieurs vainqueurs. Les modalités de l'appel sont encore en discussion et seront fixées fin 2016.

L'appel du NIST est à la fois un risque et une opportunité pour la filière française de cybersécurité. Il faut prendre conscience de cette mini-révolution pour éviter une perte de compétitivité à moyen terme. De l'autre côté de l'Atlantique,

des entreprises comme Intel et Microsoft aiguisent déjà leur stratégie post-quantique **[Intelpq,Micrpq]**. Dans cette course, nous avons la chance de posséder en France un atout important. Une proportion substantielle des compétences mondiales sur le post-quantique se trouve dans les équipes académiques françaises (Paris, Lyon, Rennes, Limoges, Marseille, Saint-Étienne, Toulon…). Nos chercheurs sont donc en capacité d'avoir un impact important sur les standards post-quantiques. C'est une belle opportunité pour les industriels d'accompagner et d'appuyer l'effort des académiques dans cette course au post-quantique.

REMERCIEMENTS

Nous remercions l'équipe de *MISC*, et particulièrement Emilien Gaspar pour ses commentaires et sa relecture attentive de l'article.

REFERENCES

[Ali] Alibaba. « Alibaba's Cloud Unit Teams with Chinese Researchers on Quantum Computing », http://fortune.com/2015/07/30/alibaba-chinese-academy-team-on-quantum-computing/

[BBD09] D. J. Bernstein, J. Buchmann et E. Dahmen, editors. « Post-Quantum Cryptography », Mathematics and Statistics Springer-11649. 2009

[PolSys] http://www-polsys.lip6.fr/Links/index.html

[SPHINCS] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, et Z. Wilcox-O'Hearn. « SPHINCS: Practical Stateless Hash-Based Signatures », EUROCRYPT, LNCS 9056, pages 368-397, Springer, 2015

[Intelpq] E. Brickell, « The Intel Strategy for Post Quantum Cryptography », Invited talk, PQCrypto 2014

[XMSS] J. Buchmann, E. Dahmen, et A. Hülsing. « XMSS - a Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions », PQ Crypto, LNCS 7071, pages 117–129. Springer, 2011

[NISTpq] L. Chen, S. Jordan, Y-K. Liu, D. Moody, R. Peralta, R. Perlner, et D. Smith-Tone. « Report on Post-Quantum Cryptography », NISTIR 8105 DRAFT, 2016

[CFS01] N. Courtois, M. Finiasz, et N. Sendrier. « How to Achieve a McEliece-Based Digital Signature Scheme », ASIACRYPT, LNCS 2248, pages 157-174, Springer, 2001

[DWAVE] D-WAVE. «The Quantum Computing Compagny », **http://www.dwavesys.com/**

[ETSIpq] ETSI, « ETSI Launches Quantum Safe Cryptography Specification Group», **http://www.etsi.org/news-events/news/947-2015-03-news-etsi-launches-quantum-safe-cryptography-specification-group**, 2015

[FOPPT15] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc et J-P. Tillich. « Structural Cryptanalysis of McEliece Schemes with Compact Keys », Des. Codes Cryptogr., 2015

[AIQ] Google. « Launching the Quantum Artificial Intelligence Lab », **http://googleresearch.blogspot.fr/2013/05/launching-quantum-artificial.html**

[Qzoo] S. Jordan. « The Quantum Algorithm Zoo », **http://math.nist.gov/quantum/zoo/**

[KM15] N. Koblitz and A. Menezes, « A Riddle Wrapped in an Enigma », Cryptology ePrint Archive : Report 2015/1018, **https://eprint.iacr.org/2015/1018.pdf**

[Micrpq] Brian LaMacchia, **https://news.microsoft.com/features/from-ai-and-data-science-to-cryptography-microsoft-researchers-offer-16-predictions-for-16/**

[M14] M. Mariantoni. « Building a Superconducting Quantum Computer », Invited talk, PQ Crypto 2014

[M16] D. Moody. « Post-Quantum Cryptography: NIST's Plan for the Future », PQCrypto 2016, **https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf**

[Mo15] M. Mosca. « Cybersecurity in an Era with Quantum Computers : Will we be Ready ? », IACR Cryptology ePrint Archive 2015, 1075, 2015

[NSASuiteb] NSA. « Cryptography Today », **https://www.nsa.gov/ia/programs/suiteb_cryptography/** et **https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm**

[HFE] J. Patarin. « Hidden fields Equations (HFE) and Isomorphisms of Polynomials (IP) : Two New families of Asymmetric Algorithms », EUROCRYPT, LNCS 1070, pages 33–48. Springer, 1996

[Reg05] O. Regev. « On Lattices, Learning with Errors, Random Linear Codes, and Cryptography », STOC, pages 84-93. ACM, 2005

[EUQ] Union Européenne, « Call to accelerate Quantum Technologies across Europe », **https://ec.europa.eu/digital-single-market/en/news/call-accelerate-quantum-technologies-across-europe**

[XXZH16] H. Xiang, T. Xiang, Z.-F. Zhang et Z.-F. Han. « An Overview of PQC Workshops/Projects and Standardization Concerns in China », **https://pqcrypto2016.jp/data/10-An_Overview_of_PQC_in_China_by_Hong_Xiang.pdf**