Cryptographie post-quantique

La sécurité du futur

Arnaud Lebon
Lucas Brignoli
4 janvier 2021

Introduction

Un ordinateur tout puissant

Aujourd'hui, un ordinateur classique représente l'information sous forme de bits contenant soit des 0 soit des 1. Depuis quelques années, l'ordinateur quantique a vu le jour. Cette machine, contrairement à un ordinateur classique, utilise les bits quantiques ou qubits, qui peuvent être les deux états (0 ou 1) à la fois, on appelle cela la superposition.
Deux qubits permettent donc de superposer 4 états (2 puissance 2), 4 qubits, d'en superposer 16 (2 puissance 4) etc. La puissance de calcul de l'ordinateur quantique double à chaque fois qu'on lui ajoute un qubit.

Algorithmes quantiques

Un des algorithmes quantique les plus prometteurs est l'algorithme de Shor, capable de factoriser aussi vite que de multiplier, alors que dans un calcul classique, il y a une différence de temps de résolution entre les deux opérations. Pour le moment, le quantique arrive à factoriser uniquement des nombres de moins de 10 chiffres mais le jour où un ordinateur quantique réussira à exécuter l'algorithme de Shor à grande échelle, cela remettrait en cause toute la cryptographie régissant nos codes de sécurité (cartes de crédit, etc.), basée sur la longueur de la factorisation, l'algorithme RSA.

Un autre algorithme considérable est l'algorithme de Grover, qui permet d'inverser une fonction. Cet algorithme permet notamment de rechercher des éléments dans une liste non-ordonnée ou dans une base de données non-structurée de façon efficace. Il peut ainsi être utilisé pour accélérer la recherche d'une clé de chiffrement symétrique.

Une cryptographie remise en question

Cryptographie actuelle en danger

Un tel ordinateur est une menace dans le monde de la cryptographie, il rendrait obsolète la majorité des algorithmes de cryptographie.
En effet, la plupart des algorithmes qui permettent d'échanger une clé secrète entre deux entités afin d'obtenir une communication sécurisée, et la grande majorité des schémas de signature numérique, ont une sécurité qui repose essentiellement sur la difficulté de deux problèmes : le logarithme discret et la factorisation des entiers. Problèmes facilement résoluble par un ordinateur quantique.

Une urgence cryptographique

L'organisme de standardisation américain NIST (National Institute of Standards and Technology) a lancé un effort international pour la standardisation d'algorithmes cryptographiques dits post-quantiques, ce qui signifie qu'ils résisteraient également aux adversaires disposant d'un ordinateur quantique. Ce processus de standardisation se déroule sous la forme d'une compétition internationale à laquelle tous les volontaires sont invités à soumettre chaque années depuis 2016, de nouveaux algorithmes d'échange de clé et de nouveaux schémas de signature. 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

Une des idées envisagées par les scientifiques est d'augmenter la taille des clés numériques afin que le nombre de permutations devant être recherchées à l'aide de la puissance de calcul brute augmente de manière

significative. Mais pour le moment, quatre pistes de constructions mathématiques ont été retenues par la communauté de chercheurs comme les plus prometteuses pour concevoir des algorithmes cryptographiques incassables par des ordinateurs quantiques : les problèmes de vecteurs courts dans les réseaux euclidiens, la cryptographie à partir de codes correcteurs d'erreurs, celle qui s'appuie sur l'inversion des polynômes multivariés et une cryptographie basée sur les isogénies.

Cryptographie post-quantique

Algorithmes à résolution difficile

La *cryptographie post-quantique a pour objectif* de construire des cryptosystèmes (algorithmes de chiffrement, signature, échange de clés…) à l'épreuve des ordinateurs quantiques. Il faut savoir qu'il existe des problèmes qui, pour un ordinateur classique comme quantique, est difficile à résoudre. En théorie de la complexité, les problèmes sont classés en fonction de leur difficulté. Les problèmes NP-difficiles sont des problèmes pour lesquels il n'existe pas à priori d'algorithme efficace pour les résoudre. La cryptographie post-quantique inclue donc différents types de cryptographies essentiellement basées sur un problème NP-difficiles.

Cryptographie multivariée

La cryptographie multivariée est l'un des domaines les plus prometteur dans le post-quantique. Il permet de créer des cryptosystèmes basés sur la difficulté du problème PoSSo : trouver une racine commune d'un ensemble de polynômes non-linéaires, si elle existe. Le problème PoSSo

est NP-difficile et sa difficulté n'est a priori pas remise en cause par l'arrivé d'un ordinateur quantique.
La clé publique d'un cryptosystème multivarié est donnée par un ensemble de polynômes. Pour chiffrer un message, il suffit d'évaluer le message sur les polynômes de la clé publique. On donne ci-dessous un exemple de chiffrement en cryptographie multivariée.

```
/* Le message à chiffrer est donné sous forme d'un vecteur
de bits */
[0, 1, 1, 1, 1]

/* Exemple d'une clé 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 clé publique
pour le message x1=0, x2=1, x3=1, x4=1, x5=1, et on obtient
le message chiffré en prenant le reste modulo 2 */
[ 1, 0, 0, 1, 1]
```

Pour déchiffrer, il faut posséder comme clé secrète un moyen d'inverser la clé publique.

La cryptographie multivariée permet aussi d'obtenir des schémas de signature. La clé publique sera toujours donnée par un ensemble de polynômes non-linéaires. La vérification d'une signature consiste simplement à évaluer les polynômes de la clé publique sur la signature.
Le domaine est très dynamique, et de nombreuses constructions sont présentées chaque année par différents auteurs à travers le monde.

Une caractéristique commune à presque tous les cryptosystèmes post-quantiques est la taille des clés publiques qui est bien plus élevée que les cryptosystèmes classiques, ce qui risque d'engendrer des problèmes de latence lors de leurs transmissions.

Le point fort de la cryptographie multivariée est de construire des schémas permettant de signer des messages avec des signatures très courtes. Par exemple, un de ces algorithmes permet d'obtenir des signatures de l'ordre de 100 bits. Il n'existe aucun schéma post-quantique permettant d'obtenir une signature aussi courte, et aussi pratique, qu'un schéma multivarié. Le multivarié est donc un candidat très prometteur pour un standard post-quantique de signature courte.

Cryptographie des codes correcteurs

La résolution d'un système d'équations linéaires est simple, mais si les équations comportent des erreurs, cette tâche sera bien plus complexe. Le cryptosystème de McEliece est le chiffrement à clé publique post-quantique le plus ancien, elle date de 1978. Sa sécurité est basée sur la difficulté de décoder un code linéaire.

Pour représenter la clé publique, ce système utilise une matrice à coefficients binaires. Cette matrice n'est pas aléatoire, mais est dérivée d'un *code correcteur d'erreur (technique de correction d'information lors de sa transmission - ex. un pixel manquant -)*. 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 de chiffrement :

```
/* Le message à chiffrer est donné par un vecteur 5 bits */
[ 0, 1, 1, 1, 1 ]

/* Exemple d'une clé publique, matrice 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]
```

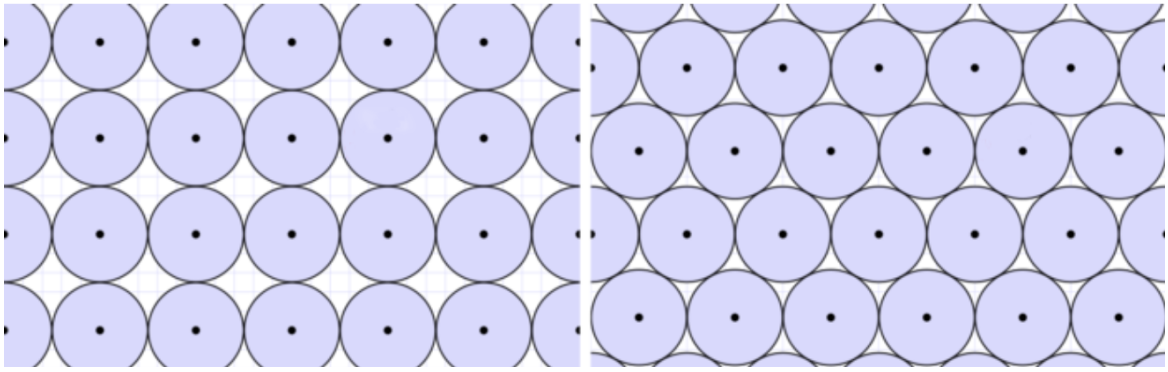
```
/* Pour chiffrer, il faut choisir un vecteur d'erreurs */
[ 1, 0, 0, 0, 0, 0, 0, 0, 1, 0 ]

/* Ensuite, il faut multiplier le message par la matrice
publique modulo 2 */
[ 0, 1, 1, 1, 1, 1, 0, 1, 1, 1 ]

/* Puis additionner le résultat avec le vecteur d'erreurs
modulo 2 */
/* Message chiffré */
[ 1, 1, 1, 1, 1, 1, 0, 1, 0, 1 ]
```

Pour le déchiffrement, il est nécéssaire de réaliser plusieurs calculs impliquant le message chiffré ainsi que deux matrices contenues dans la clé privée.

Ce système de chiffrement a résisté à toutes les tentatives de cryptanalyse depuis son apparition en 1978. Le schéma de McEliece présente plusieurs autres avantages, comme sa vitesse en matière de chiffrement et de déchiffrement. Comme pour la cryptographie multivariée, un point gênant pour ce cryptosystème est la taille des clés publiques, 100 fois plus élevé qu'une clé RSA.

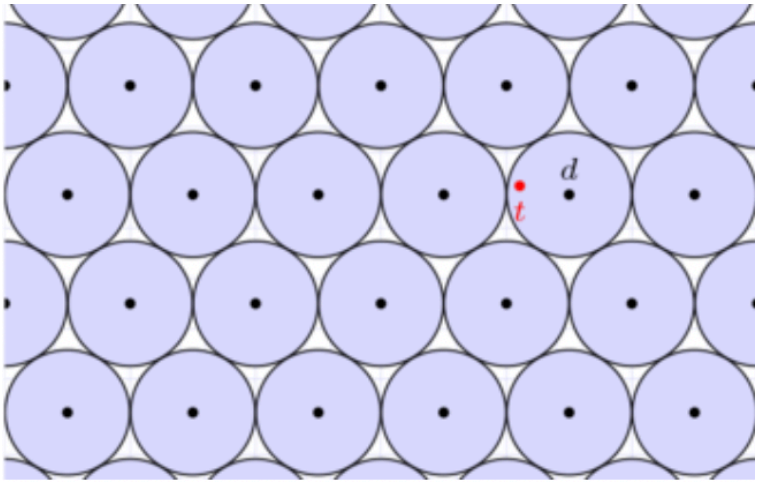
Cryptographie des réseaux euclidiens

Les réseaux euclidiens représentent des arrangements réguliers de points, comme le quadrillage d'un jeu d'échecs ou les alvéoles d'abeilles. La cryptographie des réseaux se base sur la difficulté à résoudre les problèmes géométriques des réseaux euclidiens ayant des milliers de dimensions.



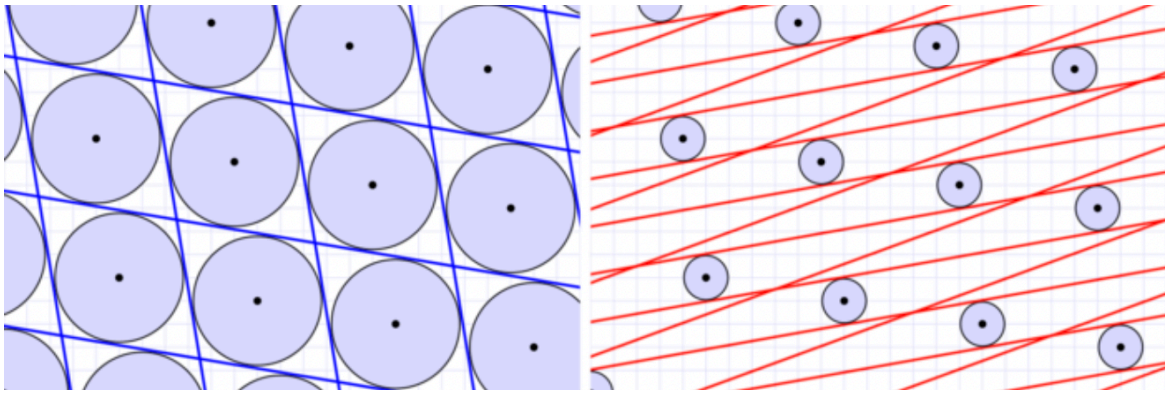
Le réseau carré (à gauche) laisse beaucoup d'espace inutilisé, seulement 78% de la surface est utile. À l'opposé, le réseau dit hexagonal (structure en nid d'abeille, à droite) est optimal avec une densité de plus de 90%.

Le message à chiffrer sera sous forme d'un petit vecteur, également interprété comme une "erreur", ce vecteur sera ajouté à un point aléatoire du réseau. De cette façon, quelqu'un connaissant une bonne base pourra retrouver cette "erreur" (message), mais sans une bonne base il sera difficile de la retrouver.



L'émetteur cherche à transmettre le point d, mais le point se transforment en t = d + e pour une erreur e. Le récepteur retrouvera le point d : c'est le point du réseau le plus proche de t.

Il existe des algorithmes pour retrouver rapidement un point proche, et ces algorithmes utilisent une base du réseau. Les bases servent à découper l'espace pour retrouver le point le plus proche.



Correction d'erreur avec bonne base (à gauche), et mauvaise base (à droite).

Ainsi on peut espérer se servir d'une bonne base comme d'une clef secrète.

Les réseaux montrés jusqu'alors, sont de dimension 2. La correction d'erreur est aisé en dessinant quelques cercles. Ce qui peut se traduire par un algorithme efficace. Mais si l'on se place dans un réseau avec plus de dimensions, on va devoir faire des compromis pour que l'algorithme reste efficace : on ne pourra pas corriger des erreurs trop grosses. Ainsi, on estime qu'avec 200 ou 250 dimensions, la réduction de réseau est impossible à moins de milliards d'années de calculs.

Conclusion

Des défis à surmonter

Avant de pouvoir proposer de véritables solutions cryptographiques pouvant faire face à la puissance des ordinateurs quantiques, les chercheurs du post-quantique se retrouvent confrontés à plusieurs problématiques.

Pour commencer, les algorithmes post-quantiques en développement ont des tailles de clé trop importantes, allant de plusieurs dizaines de kilo-octets jusqu'à un méga-octet parfois (contre quelques centaines ou milliers de bits pour les algorithmes actuels).

Ensuite, les besoins en bande passante ont également un impact sur le développement de solutions de cryptographie post-quantique, puisqu'ils augmenteront probablement massivement avec leur arrivée, tout comme les architectures et les infrastructures de réseaux existants, qui devront très probablement être mis à niveau voire remplacés pour supporter ces nouvelles solutions. Une opération qui pourrait prendre de nombreuses années.

Pour finir, l'urgence de la situation est une problématique en soi : les technologies cryptographiques sont ancrées dans de nombreux systèmes différents (objets connectés, véhicules, e-commerce, etc) et mettre en œuvre de nouvelles peut prendre beaucoup de temps. La cryptographie post-quantique doit devenir une réalité avant l'apparition d'un ordinateur quantique suffisamment puissant.

Une menace encore lointaine

Aujourd'hui, le risque de l'ordinateur quantique est perçu comme très élevé. Cependant, la venue d'un ordinateur quantique d'une capacité suffisante pour représenter une menace à la cryptographie classique n'est

pas pour demain. On peut penser que les recherches en matière de cryptographie post-quantique seront bien avancées avant l'arrivé d'une telle machine, et que le changement des constructions cryptographiques pourra être largement anticipé.
Il est donc très probable que la cryptographie post-quantique envahisse notre quotidien ces prochaines années, le type de cryptographie post-quantique reste encore lui à définir. On peut donc anticiper une très forte activité, dans le domaine ces prochaines années.