Les candidats post-quantiques

Quel sera le standard adopté pour la cryptographie du futur ? Les soumissions reposent sur des types de problèmes mathématiques parfois anciens qui reviennent sur le devant de la scène, ou plus nouveau. Petit tour d'horizon.

Contexte - Réseaux euclidiens, codes correcteurs d'erreurs, ou systèmes multivariables se disputent le privilège de devenir le standard cryptographique qui équipera nos ordinateurs et cartes à puces. La compétition est ouverte.

Introduction - À la fin du XIXe siècle, le cryptographe néerlandais Auguste Kerchoffs préconisait que dans un système cryptographique, tout doit être public, excepté une petite information – la clé – qui doit avoir assez d'"entropie" pour qu'on ne puisse pas la retrouver facilement. Ce principe dit de Kerchoffs permet qu'il y ait un audit public des systèmes, condition d'une réelle confiance. C'est cet audit public qui a commencé et qui va durer quelques années pour les protocoles cryptographiques qui devront résister à l'ordinateur quantique que l'on nous promet pour la prochaine décennie. Sur les 82 soumissions, provenant de 26 pays, 69 ont été considérées comme « complètes et valides » par le NIST. Cinq candidats se sont retirés de la compétition et il reste donc 64 soumissions examinées, qui concernent soit la signature de documents numériques soit des algorithmes de chiffrement.
Chaque soumission émane d'un groupe de plusieurs chercheurs, et inclut souvent des cryptographes travaillant dans des entreprises privées, qu'il s'agisse de grosses sociétés – Microsoft participe à 4 soumissions, mais on trouve également Amazon, Texas Instrument – ou de petites entreprises de sécurité. Parmi les 13 soumissions françaises, neuf sont regroupées sous l'égide du RISQ (Regroupement de l'industrie française pour la sécurité post-quantique). Ce projet, qui entre dans le cadre des projets d'investissements d'avenir (PIA), encourage les entreprises (Airbus, C&S, CryptoExperts, Orange, Secure IC, ou Thalès), les partenaires académiques (CNRS, CEA, ENS, INRIA, Sorbonne Université, Universités de Versailles Saint-Quentin et Rennes) et l'ANSSI à travailler ensemble pour les soumissions NIST. Son objectif est aussi de préparer le déploiement dans les industries françaises du post-quantique. Le projet RISQ prévoit ainsi de développer un premier prototype post–quantique de quelques produits des partenaires industriels.

Comment - La sécurité d'un système cryptographique repose le plus souvent sur ce que les mathématiciens nomment des « fonctions à sens unique ». Une opération qu'il est aisé de faire dans un sens, et difficile (pour un ordinateur) dans l'autre sens. L'exemple typique étant la multiplication de deux nombres, qui est facile, alors que retrouver les facteurs premiers d'un très grand nombre nécessite beaucoup trop de temps pour un ordinateur

classique. D'où la confiance que l'on pouvait avoir dans le protocole RSA, fondé sur cette difficulté à factoriser. Comme l'ordinateur quantique dans son principe factorise très rapidement, il faut trouver de nouveaux problèmes. Cet article décrit les idées sous-jacentes à ces problèmes mathématiques, les promesses de sécurité, mais aussi les difficultés. Le vainqueur – ou les vainqueurs – seront annoncés autour de 2022-2023.

La cryptographie multivariable

Invention : C'est une équipe Japonaise, composé de M. Matsumoto et H. Imai, qui a inventé le premier cryptosystème à clé publique utilisant des systèmes d'équations à plusieurs variables. Le domaine a été popularisé grâce aux travaux de J. Patarin, de l'université de Versailles Saint-Quentin.

Avantages : La cryptographie multivariable permet d'obtenir des schémas de signature ayant une taille de signature très courte (probablement, la plus courte des candidats pour le NIST). La vérification d'une signature est également très rapide.

Inconvénients : La taille de la clé publique.

Nombre de soumissions au NIST : 7 pour la signature, 2 pour le chiffrement

Les systèmes d'équations à plusieurs variables forment des outils de choix pour les systèmes cryptographiques.

En 1996, J. Patarin a mis au point un cryptosystème, baptisé HFE, qui est probablement le schéma le plus étudié de cette catégorie. « C'est en cherchant à attaquer ce système et en analysant ses faiblesses, que nous sommes parvenus à obtenir des propositions qui pourraient résister à l'ordinateur quantique, explique Jean-Charles Faugère, cryptographe dans une équipe commune entre Sorbonne Université et INRIA Paris. Nous avons fait trois propositions en collaboration avec Jacques Patarin, des chercheurs d'Orange et de C&S ainsi que des doctorants de mon équipe. »

Le principe de cette cryptographie est d'utiliser un système d'équations qui font intervenir le produit de plusieurs variables (par exemple x1, x2, x3, x4, x5) :

$$
\begin{aligned}
y1 &= f1(x1,x2,x3,x4,x5)\\
y2 &= f2(x1,x2,x3,x4,x5)\\
y3 &= f3(x1,x2,x3,x4,x5)\\
y4 &= f4(x1,x2,x3,x4,x5)\\
y5 &= f5(x1,x2,x3,x4,x5)
\end{aligned}
$$

où les fi sont des polynômes de degré deux en les xi.

S'il est facile et rapide de retrouver yi pour xi fixé, l'inverse n'est pas vrai. C'est le problème "difficile" sur lequel se fondent les systèmes multivariables. « L'enjeu a été de parvenir à renforcer la proposition d'origine en choisissant les paramètres de manière adéquates de

sorte que le problème soit résistant, mais pas trop, pour que cela reste efficace » précise Jean-Charles Faugère. « En pratique, nous avons fait en 2015 un test à grande échelle pour l'armée de terre en déployant une première version de nos propositions sur un téléphone portable de type Android, ce qui a aidé à estimer les paramètres de sécurité » reprend Ludovic Perret, maitre de conférences à Sorbonne Université.

Pourquoi ce type de système est-il plus facile pour la signature que pour le chiffrement, comme en témoigne la différence du nombre de soumissions? « C'est que vérifier la signature c'est très facile avec des systèmes polynomiaux : il suffit juste de vérifier que la solution donnée est bien solution du système. Historiquement, il a toujours été plus difficile de trouver les bons paramètres pour le chiffrement que pour la signature » précise Ludovic Perret qui démarre avec son collègue une start-up sur la cryptographie résistante à l'ordinateur quantique.