Le NIST a choisi ses algorithmes de cryptographie post-quantiques

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 juillet 2022. Dernière mise à jour le 16 août 2024

https://www.bortzmeyer.org/nist-pq.html

Ce mardi 5 juillet 2022, l'organisme de normalisation étatsunien NIST a annoncé <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptograph qu'il avait choisi les algorithmes de cryptographie post-quantiques qu'il allait maintenant normaliser. Ce sont Kyber <https://pq-crystals.org/kyber/index.shtml> pour l'échange de clés et Dilithium <https://pq-crystals.org/dilithium/index.shtml> pour les signatures.

L'annonce était prévue plus tôt mais a été retardée, selon certains par des problèmes liés aux nombreux brevets qui grèvent ces algorithmes (l'annonce du NIST prévoit des négociations), selon d'autres par la difficulté qu'avait la NSA à

attaquer les algorithmes proposés <https://www.bloomberg.com/news/articles/2022-05-13/nsa-says-no-backdoor-in-new-encryption-scheme-for-us-tech>. Il est difficile de le savoir puisque le NIST, même s'il avait fait un effort d'ouverture à cette occasion, reste assez opaque. En tout cas, désormais, c'est fait.

Pour comprendre l'importance de cette annonce <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>, il faut revenir sur celle de la cryptographie. On sait que cet ensemble de techniques est absolument indispensable à la sécurité de l'utilisateur sur l'Internet. Ne croyez pas les politiciens ou les éditorialistes qui vont vous expliquer que si vous ne faites rien de mal, vous n'avez rien à cacher et pas besoin de cryptographie. Cet argument a été réfuté d'innombrables fois depuis des années <https://www.bortzmeyer.org/crypto.html> mais continue à être parfois utilisé pour pousser les citoyen·nes à communiquer en public. Ignorez-le, et chiffrez l'intégralité de vos communications, c'est indispensable dans le monde d'aujourd'hui.

Mais aucune technique de sécurité n'est parfaite, que cela soit la cryptographie ou une autre. Il y a des questions non-techniques <https://www.bortzmeyer.org/concealing-for-freedom.html> mais aussi des limites techniques de la cryptographie. Notamment, dans l'ordre d'importance décroissante :

— La cryptographie protège contre des tiers qui écoutent et/ou modifient les communications, mais pas contre le destinataire.
— Les logiciels de cryptographie, comme les autres, ont des bogues.
— Et les algorithmes utilisés en cryptographie peuvent ne pas être aussi solides qu'on le pense ; la cryptanalyse peut parfois en venir à bout. (Voyez par exemple le RFC 7465 [1].)

Ce dernier risque est le plus spectaculaire et celui que les "*geeks*" préfèrent mentionner. Mais, en pratique, il est sans doute le moins sérieux. Vous avez bien plus de chances de voir vos secrets percés suite à une imprudence ou une maladresse de votre correspondant·e ou de vous-même que suite à une découverte mathématique fondamentale résolvant le problème du logarithme discret et cassant ainsi ECDSA. Certes, un problème mathématique comme la décomposition en facteurs premiers, qui est à la base de RSA, reste un problème ouvert et on n'a jamais démontré qu'il était insoluble. Néanmoins, vu le nombre de gens qui l'ont attaqué depuis des dizaines d'années, on peut être raisonnablement confiant : le problème est manifestement très difficile, et RSA reste donc sûr. La seule méthode connue pour attaquer des algorithmes comme ECDSA ou RSA reste donc la force brute, l'examen systématique de toutes les possibilités, ce qui prend quelques milliards d'années avec les machines existantes. (Je simplifie : on dispose en fait d'algorithmes meilleurs que la pure force brute mais ils ne font pas de miracles non plus.) En outre, la difficulté augmente exponentiellement avec la taille de la clé, et un progrès dans les processeurs ou bien certaines optimisations des programmes de cryptanalyse peuvent facilement être annulés en agrandissant la clé.

Mais les calculateurs quantiques pourraient changer les choses. Je ne vais pas détailler ici le fonctionnement de ces machines. Je dirais juste que, reposant directement sur la quantique, ils permettent de faire tourner des algorithmes radicalement différents (et pas évidents du tout à programmer !) de ceux qui sont utilisés actuellement, sur les ordinateurs classiques. Ainsi, l'algorithme de Shor permet de décomposer un nombre en ses facteurs premiers, en un temps linéaire, et donc de trouver une clé privée RSA à partir de la clé publique, tâche qui était impossible aux ordinateurs classiques. L'algorithme de Shor ne tournant que sur des calculateurs quantiques, si on dispose d'un tel calculateur, on a cassé RSA (et, avec un algorithme proche, ECDSA et les autres algorithmes à courbes elliptiques). Ce serait une catastrophe pour la sécurité de l'Internet, puisque les communications confidentielles pourraient toutes être décryptées, et les signatures toutes imitées. (Notez que cela serait pareil, même sans calculateur quantique, si un·e mathématicien·ne génial·e découvrait demain un moyen simple de décomposer un nombre en facteurs premiers. Comme indiqué plus haut, c'est peu probable mais pas impossible.)

Mais attention, le « si on dispose d'un calculateur quantique » est un gros « si ». De même qu'Euclide avait développé des algorithmes et qu'Ada Lovelace avait écrit des programmes longtemps avant qu'un ordinateur ne soit disponible pour les exécuter, Shor a développé son algorithme sans avoir de calculateur quantique. On a progressé depuis et des calculateurs quantiques existent, et on peut faire tourner l'algorithme de Shor dessus. Le problème est qu'ils sont très expérimentaux, très peu existent dans le monde et leurs plus grands exploits sont très loin de ce qui serait nécessaire pour casser les clés d'aujourd'hui. Les optimistes parient que ce n'est qu'une question de temps et que, dans quelques années, les calculateurs quantiques (dont les enthousiastes prédisent depuis des années qu'ils sont presque au point) s'attaqueront facilement à nos algorithmes cryptographiques. Les pessimistes font remarquer que les difficultés pratiques qui se présentent face aux calculateurs quantiques sont colossales et que les résoudre n'est pas un simple travail d'ingéniérie prévisible mais est souvent plus proche de la recherche fondamentale et de ses incertitudes. Bref, il n'y a pas actuellement de consensus sur le temps dont nous disposons encore face à la « menace quantique ».

Comme il faut s'y prendre à l'avance pour développer, tester et déployer de nouveaux algorithmes dits post-quantiques, les cryptographes n'ont pas attendu de voir les calculateurs quantiques en vente

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7465.txt`

chez Darty <https://www.darty.com/nav/recherche/quantique.html> pour réagir. Le travail sur des algorithmes post-quantiques a commencé il y a longtemps. Ces nouveaux algorithmes doivent résister aux calculateurs quantiques. Plus exactement, il faut qu'on ne connaisse pas d'algorithme quantique pour les attaquer. Mais il faut aussi qu'ils résistent à la cryptanalyse classique (voir par exemple cette attaque contre Rainbow, un des finalistes du concours <https://eprint.iacr.org/2022/214>). Et il faut aussi qu'ils soient réalistes en performance, en taille de clés <https://blog.cloudflare.com/sizing-up-post-quantum-signatures/>, etc. Plusieurs candidats prometteurs ont été développés, et les cryptanalystes se sont déjà fait les dents à essayer de les casser.

Sur l'Internet, mais aussi en général dans le monde numérique, la normalisation est essentielle. Avoir des protocoles et des algorithmes, notamment de cryptographie, communs, permet l'interopérabilité, qui garantit liberté de choix, et bon fonctionnement du réseau. Pour qu'Alice puisse envoyer un message à Bob, il faut bien qu'Alice chiffre avec un algorithme que Bob puisse déchiffrer. Le rôle des organisations de normalisation est donc crucial. C'est pour cela que le NIST étatsunien a lancé en 2016 un grand concours pour choisi le meilleur algorithme à normaliser. Plutôt que de faire travailler ensemble des cryptologues à développer en commun ce meilleur algorithme, ce qui risquait d'amener à un compromis qui ne satisferait personne, le NIST a choisi le concours : de nombreuses équipes proposent leur algorithme, chacun essaie de casser celui des concurrents et que le meilleur gagne. C'est ce concours qui vient de franchir une étape décisive, avec l'annonce du choix de :

— Kyber <https://pq-crystals.org/kyber/index.shtml> pour l'échange de clés (aussi nommé KEM pour "*key encapsulation mechanism*" cf. RFC 9180), préalable au chiffrement effectué ensuite avec un algorithme symétrique classique comme AES. Kyber utilise les réseaux euclidiens.
— Dilithium <https://pq-crystals.org/dilithium/index.shtml> (oui, ça vient de Star Trek <https://en.wikipedia.org/wiki/Dilithium_(Star_Trek)>) pour les signatures. Dilithium utilise également les réseaux euclidiens.
— Deux autres algorithmes de signature ont été également retenus, pour des usages spécifiques, Sphincs+ et Falcon, et plusieurs autres algorithmes seront examinés pour fournir un algorithme de secours, au cas où des problèmes apparaissent avec ceux sélectionnés (rappelons que, contrairement à, par exemple, RSA, ils n'ont pas bénéficié d'années de recherches de failles). Sphincs+ est le seul à ne pas utiliser les réseaux euclidiens, mais des fonctions de condensation.

Maintenant que ces algorithmes ont été choisis, verra-t-on dès demain TLS, SSH, DNSSEC et les autres utiliser des algorithmes post-quantiques ? Non, car il reste plusieurs étapes à franchir. D'abord, le NIST doit finir le travail de normalisation : il faut spécifier rigoureusement l'algorithme et publier la spécification officielle. (Cela a été fait deux ans après, le 14 août 2024, avec la parution de FIPS-203 <https://csrc.nist.gov/pubs/fips/203/final>, FIPS-204 <https://csrc.nist.gov/pubs/fips/204/final> et FIPS-205 <https://csrc.nist.gov/pubs/fips/205/final>.) Cela implique, comme le note l'annonce officielle, une négociation réussie sur les brevets qui plombent le champ de la cryptographie post-quantique (cf. par exemple le problème avec le CNRS <https://www.lemonde.fr/sciences/article/2021/11/16/quand-un-brevet-perturbe-l-innovation-postquantique
6102215_1650684.html> et l'accord ultérieur <https://www.cnrs.fr/fr/accord-de-licence-entre-le-ni
Ensuite, la plupart des utilisations de la cryptographie se fait au sein d'un protocole de cryptographie comme TLS <https://blog.cloudflare.com/securing-the-post-quantum-world/>. Les protocoles sérieux disposent tous de la propriété d'agilité (RFC 7696), ce qui veut dire qu'ils ne sont pas lié à un algorithme de cryptographie particulier. Mais il faudra quand même spécifier l'utilisation du nouvel algorithme pour ce protocole (par exemple, pour DNSSEC, il faudra l'ajouter au registre IANA <https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-1>, ce qui nécessitera la publication d'un RFC). (Cet article <https://sofiaceli.com/2022/07/05/pq-signatures.html> donne une première idée du travail à faire.) Ensuite, les programmeur·ses devront programmer ces algorithmes post-quantiques (une tâche à effectuer soigneusement ; on a vu que les bogues sont à l'origine de bien des problèmes de cryptographie). Même s'il existe déjà plusieurs mises en œuvre de ces algorithmes, des programmes dignes d'être utilisés en production sont une autre affaire. Et il faudra ensuite déployer ces programmes dans le monde réel.

Pour la partie de normalisation dans les protocoles TCP/IP, ce qui relève de l'IETF, on peut noter que quelques RFC parlent déjà de post-quantique. C'est le cas par exemple des RFC 8784, RFC 8696, RFC 8773 et RFC 8784, mais c'est exagéré, ils décrivent simplement des clés de cryptographie symétrique pré-partagées. Plus sérieusement, le RFC 8032 discute les risques que les calculateurs quantiques posent à l'algorithme EdDSA, et le RFC 8391 le fait pour XMSS, tandis que le RFC 9180 (section 9.1.3) a une vision plus générale. Même discussion pour les RFC 8240 et RFC 8576, dans le contexte de l'Internet des objets. Le RFC 9021 doit être un des rares qui repose déjà sur un algorithme post-quantique mais on voit que la prise de conscience était ancienne.

Il faudra donc compter de nombreuses années avant d'avoir les algorithmes post-quantiques massivement déployés. C'est d'ailleurs pour cela qu'il faut commencer tout de suite le processus, alors même que la menace des calculateurs quantiques est lointaine. (On peut aussi se rappeler que la cryptographie sert parfois à protéger des secrets de longue durée. Si les fichiers que vous chiffrez actuellement seront toujours sensibles dans trente ans, dites-vous bien que les calculateurs quantiques capables de casser les clés utilisées seront peut-être une réalité dans trente ans.)

Le mot « quantique » est parfois mis à toutes les sauces. Il faut notamment signaler que les questions discutées ici n'ont rien à voir avec ce qu'on nomme parfois la « cryptographie quantique » (et qui serait mieux appelée « distribution quantique de clés »), une technique dont l'intérêt n'est pas du tout évident <https://www.bortzmeyer.org/communication-quantique.html> (voir aussi le démontage de cette idée par Dan Bernstein <https://blog.cr.yp.to/20160516-quantum.html> et l'avis de l'ANSSI <https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-us>, en anglais seulement). De même, la question de la cryptographie post-quantique n'a pas de lien direct avec les projets d'« Internet quantique » (où les routeurs sont quantiques), sur lesquels travaille entre autres l'IRTF dans son groupe QIRG <https://datatracker.ietf.org/rg/qirg/>.

Sinon, question mises en œuvre, Kyber et Dilithium sont dans la bibliothèque de Cloudflare <https://github.com/cloudflare/circl> (écrite en Go). Elle n'a apparemment aucune documentation et son utilisation semble difficile. (La bibliothèque de Microsoft <https://github.com/microsoft/PQCrypto-SIDH> avait fait le choix d'autres algorithmes.)

Quelques bonnes lectures sur cette question des algorithmes de cryptographie post-quantiques :

— Les algorithmes post-quantiques ont été le sujet de la Journée du Conseil scientifique de l[Caractère Unicode non montré [2]]Afnic <https://www.afnic.fr/observatoire-ressources/actualites/jcsa19-retour-sur-ledition-2019-de-la-journee-du-conseil-scientifique> en 2019.
— Un bon article d'introduction au CNRS <https://lejournal.cnrs.fr/articles/vers-une-cryptog
— J'avais fait un exposé sur le post-quantique à Pas Sage En Seine en 2018 <https://www.bortzmeyer.org/pas-sage-en-seine-quantique.html>.
— L'ANSSI a produit un avis détaillé <https://www.ssi.gouv.fr/publication/migration-vers-la-c>. (Voir aussi l'article de l'ANSSI sur l'annonce du NIST <https://www.ssi.gouv.fr/actualite/selection-par-le-nist-de-futurs-standards-en-cryptographie-post-quantique/>.)
— Sur les conséquences du post-quantique sur le DNS, notamment DNSSEC, on peut regarder le rapport de l'ICANN de 2022 <https://www.icann.org/en/blogs/details/icann-publishes-pape> (en anglais).
— Un article en anglais d'Hilarie Orman, « "*Internet Security and Quantum Computing*" », faisait en 2021 le point sur les conséquences des calculateurs quantiques pour la sécurité de l'Internet.

2. Car trop difficile à faire afficher par LaTeX

— Il semble qu'il y ait eu un autre concours de sélection d'algorithmes post-quantiques, organisé en Chine, mais je n'ai pas beaucoup de détails <https://m.cacrnet.org.cn/site/content/854.html>.
— Sur la quantique en général (pas seulement sur la cryptographie post-quantique), la députée Paula Forteza a sorti le 10 janvier 2020 un intéressant rapport <https://www.bortzmeyer.org/rapport-forteza-quantique.html>.

Et merci à Manuel Pégourié-Gonnard et Damien Stehlé pour leur relecture attentive. Évidemment, les erreurs restantes sont de moi.