RFC 9794 : Terminology for Post-Quantum Traditional Hybrid Schemes

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 juin 2025

Date de publication du RFC : Juin 2025

https://www.bortzmeyer.org/9794.html

La cryptographie post-quantique vise à développer des algorithmes de cryptographie qui résistent à des ordinateurs quantiques. Mais ces algorithmes sont relativement récents et peuvent avoir des faiblesses, voire des failles, que la cryptanalyse classique pourra exploiter. La tendance actuelle est donc aux protocoles et formats **hybrides**, combinant algorithmes classiques et post-quantiques. Ce RFC spécifie la terminologie de ces protocoles hybrides.

On peut aussi dire AQ, pour après-quantique car le sigle anglophone PQ de "*post-quantum*" peut faire drôle en France. D'ailleurs, les termes à utiliser (post-quantique ? résistant au quantique ?) ont fait l'objet de chaudes discussions dans le groupe de travail IETF <https://datatracker.ietf.org/wg/pquip/>.

Le point de départ de tout le tintouin autour de l'après-quantique, c'est l'algorithme de Shor. Conçu pour les calculateurs quantiques, et donc inutilisable encore aujourd'hui, il permet de résoudre des problèmes mathématiques qu'on croyait difficiles, comme la décomposition en facteurs premiers (qui est derrière RSA) ou le logarithme discret (qui est derrière ECDSA). Le jour, qui n'est pas encore arrivé, où on aura des CRQC ("*Cryptographically-Relevant Quantum Computer*", un calculateur quantique qui puisse s'attaquer à des problèmes de taille réelle, et pas juste faire des démonstrations), ce jour-là, la cryptographie classique, ou traditionnelle, aura un problème.

Les CRQC sont loin dans le futur, un lointain dont il est très difficile d'estimer la distance. Comme on ne sait pas quand est-ce que les CRQC seront disponibles, et que certains secrets qu'on chiffre maintenant devront rester secrets pendant de nombreuses années, il est prudent de travailler dès maintenant aux algorithmes AQ, après-quantique, ceux pour lesquels on ne connait pas d'algorithme (quantique ou classique) pour les casser. Ce travail a effectivement commencé depuis des années <https://www.bortzmeyer.org/nist-pq.html> et on a déjà des algorithmes AQ normalisés comme ML-KEM (ex-Kyber). Notez toutefois qu'aucune norme IETF n'a encore été publiée en intégrant ces algorithmes,

mais le travail est en cours, entre autre au sein du groupe de travail pquip <https://datatracker.ietf.org/wg/pquip/>.

Mais remplacer complètement les algorithmes traditionnels par les algorithmes AQ n'est pas forcément satisfaisant. Au contraire de RSA et ECDSA, testés au feu depuis longtemps et qui ont toujours résisté, les algorithmes AQ peuvent sembler un peu jeunes. Que se passerait-il si un·e cryptanalyste cassait un de ces algorithmes ? Pour limiter les dégâts, on envisage d'utiliser des mécanismes **hybrides**, combinant cryptographie classique (pré-quantique) et après-quantique. Ainsi, un chiffrement hybride verrait le texte en clair chiffré par un mécanisme classique puis par un mécanisme après-quantique. Une signature hybride se ferait en mettant deux signatures et en vérifiant ensuite que les deux sont valides. Cette méthode « ceinture et bretelles » est utilisée par exemple dans le RFC 9370 [1] ou dans les "*Internet-Drafts*" draft-ietf-tls-hybrid-design, draft-ietf-lamps-pq-composite-kem ou draft-ietf-lamps-cert- On peut aussi consulter la FAQ du NIST <https://csrc.nist.gov/Projects/post-quantum-cryptography faqs> (« "*A hybrid key-establishment mode[Caractère Unicode non montré [2]]is defined here to be a key establishment scheme that is a combination of two or more components that are themselves cryptographic key-establishment schemes.*" ») ou bien le document ETSI TS 103 744 <https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf> nommé « "*Quantum-safe Hybrid Key Exchanges*" ». Attention toutefois avec cette terminologie car l'adjectif « hybride » est également souvent utilisé en cryptographie pour désigner la combinaison d'un algorithme de cryptographie asymétrique avec un algorithme de cryptographie symétrique (quand on crée une clé de session échangée via de la cryptographie asymétrique puis qu'on chiffre les données avec cette clé et de la cryptographie symétrique ; c'est ce que font TLS et OpenPGP, par exemple). C'est le sens qu'utilisent les RFC 4949 et RFC 9180, par exemple. Notre RFC 9794 note que ces deux usages du terme « hybride » vont certainement prêter à confusion mais qu'il n'y avait pas trop le choix : chaque usage était déjà solidement installé dans un milieu particulier. Essayer de promouvoir un autre terme pour la cryptographie après-quantique, comme « double algorithme » ou « multi algorithme » était sans doute voué à l'échec.

Passons maintenant aux définitions. Je ne vais pas les reprendre toutes mais donner quelques exemples. La section 2 du RFC commence par les mécanismes de base et d'abord, mécanisme hybride traditionnel / post-quantique ("*post-quantum traditional hybrid scheme*", ou PQ/T), un mécanisme qui combine la cryptographie existante et celle du futur. On peut aussi simplifier en disant juste mécanisme hybride. Il y a aussi :

— Multi-algorithme, qui est plus large qu'hybride puisqu'il inclut les mécanisme ayant deux algorithmes traditionnels ou deux algorithmes après-quantique.
— Composé ("*composite*"), qui désigne les mécanismes hybrides où le mécanisme est exposé aux couches supérieures sous forme d'une interface unique (ce qui est évidemment plus simple et plus sûr pour le ou la programmeur·se).

Ensuite, on grimpe d'un niveau (section 3 du RFC), avec les éléments, qui sont les données en entrée ou en sortie d'un processus cryptographique. Quand on dit « l'algorithme X prend en entrée un texte en clair et une clé secrète et produit un texte chiffré », le texte en clair, la clé et le texte chiffré sont des éléments. Dans le mécanisme hybride décrit dans draft-ietf-tls-hybrid-design, il y a deux clés publiques, qui sont deux éléments. Un élément peut à son tour être composé de plusieurs éléments.

On peut maintenant utiliser tout cela pour faire des protocoles (section 4). Un protocole hybride PQ/T est, comme vous vous en doutez, un protocole qui utilise au moins deux algorithmes, un classique et un après-quantique. C'est ce qui est proposé dans draft-ietf-tls-hybrid-design. Ce dernier est même composé (dans le mécanisme de désignation de la clé, le KEM). Alors que le mécanisme du RFC 9370 est hybride mais pas composé (on fait un échange de clés classique et un KEM après-quantique).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9370.txt
2. Car trop difficile à faire afficher par LaTeX

Les noms des services de sécurité qu'on souhaite utiliser vont de soi (section 5) : confidentialité hybride PQ/T (confidentialité assurée par un mécanisme hybride traditionnel/après-quantique) et authentification hybride PQ/T.

Idem pour les certificats (section 6). Un « certificat hybride PQ/T » contient au moins deux clés publiques, une pour un algorithme traditionnel et une pour un algorithme après-quantique (alors que le certificat traditionnel et le certificat après-quantique ne contiennent qu'un seul type de clés publique, comme c'est le cas du certificat décrit dans `draft-ietf-lamps-dilithium-certificates`).

Et merci à Magali Bardet pour sa relecture mais, bien sûr, les erreurs sont de moi et moi seul.