L’OTAN se signale sur la cryptographie post-quantique

Comment sécuriser les communications entre membres de l’OTAN ? Avec un VPN post-quantique*. Voilà un an, le NCSC (cellule cyber de l’organisation transatlantique) avait lancé une expérimentation dans ce sens. Il l’a finalisée en début d’année. Mais l’annonce publique vient seulement d’intervenir, dans un contexte opportun : le conflit russo-ukrainien.

On doit le VPN en question à PQ Solutions. Cette entreprise britannique a développé d’autres services (messagerie instantanée, identification biométrique…) qui ont un algorithme en commun. En l’occurrence, NST-KEM, codéveloppé avec des chercheurs de l’université de Londres.

Le projet a fini par fusionner avec un autre, dont le socle technologique remonte aux années 1970 : Classic McEliece. En toile de fond, une initiative du NIST (National Institute of Standards and Technology). L’institut américain a entrepris de mettre à jour trois standards dans le domaine de la cryptographie à clés publiques :

– FIPS 186-4 (signature électronique ; dernière version : 2013)
– SP 800-56A (cryptographie à logarithme discret ; 2018)
– SP 800-56B (cryptographie à factorisation d’entiers ; 2019)

Un premier appel à propositions avait été lancé fin 2016. Avec trois catégories :

– « Chiffrement à clés publiques » (création, chiffrement, déchiffrement)
– « Échange de clés » (création, encapsulation, décapsulation)
– « Signature électronique » (création, signature, vérification)

À la clé, 69 algorithmes. À l’issue d’un processus de sélection à plusieurs tours, il en reste aujourd’hui 15. Divisés en deux groupes. D’un côté, 7 algorithmes « généralistes » favoris pour faire l’objet d’une standardisation. De l’autre, 8 algorithmes plus spécialisés ou moins matures. Classic McEliece est dans le premier groupe, catégorie échange de clés. Il est candidat pour succéder à RSA et EC (cryptographie à courbes elliptiques).

** En l’état, le VPN mêle des algorithmes quantiques et des binaires. Il a récemment fait l’objet d’un partenariat avec un fournisseur de solutions de cybersécurité pour un déploiement sur des super-yachts.*

Photo d’illustration © Siarhei – Adobe Stock