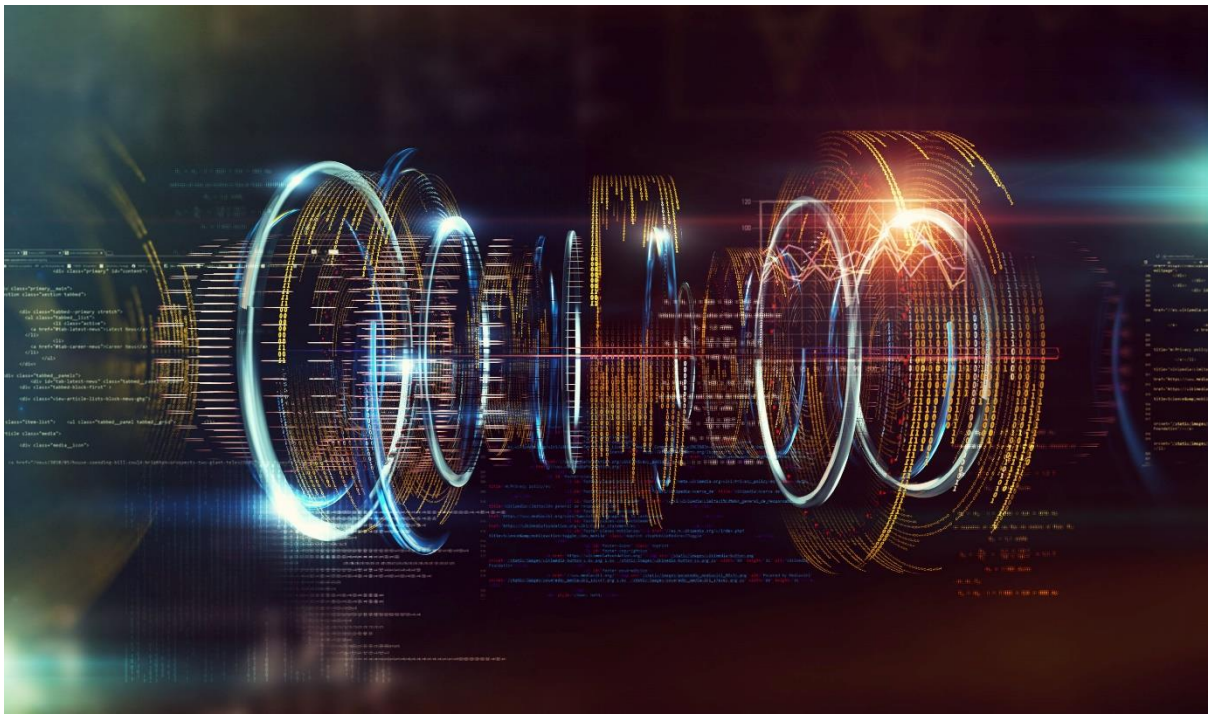
THALES
Building a future we can all trust

COMMUNIQUÉ DE PRESSE
12 juillet 2022
Paris La Défense

L'algorithme Falcon – co-développé avec Thales – sélectionné par le NIST comme nouvelle norme de cryptographie post-quantique

- **L'Institut américain des normes et de la technologie (NIST) du ministère du Commerce des États-Unis a sélectionné l'algorithme Falcon pour les signatures numériques. Co-développé pour devenir la norme de cryptographie post-quantique, il est capable de résister aux attaques des futurs ordinateurs quantiques, extrêmement puissants.**
- **Retenu pour son haut niveau de sécurité et sa remarquable efficacité spectrale, Falcon sera intégré dans les normes de cryptographie post-quantique du NIST, dont la définition devrait être finalisée d'ici deux ans.**
- **Le choix de Falcon, au bout de 5 années de compétition mondiale démontre le leadership de Thales dans les domaines de la cybersécurité, des technologies de pointe et de la recherche.**



© Carlos Castilla Jimenez

Dans le cadre du concours international lancé en 2017 par le NIST en vue d'établir les futures normes de cryptographie post-quantique pour les signatures numériques et le chiffrement par clé publique, concours auquel ont participé 82 candidats de 25 pays, l'algorithme Falcon a été sélectionné pour son niveau de sécurité extrêmement élevé et sa très grande efficacité spectrale.

Falcon a été co-développé par Thales avec des partenaires du monde académique et du secteur industriel de France (Université Rennes 1, PQShield SAS), de Suisse (IBM), du Canada (NCC Group) et des États-Unis (Brown University, Qualcomm). Il a été sélectionné par le NIST avec deux autres algorithmes comme norme pour les signatures numériques, tandis qu'un quatrième algorithme a été retenu comme norme pour le chiffrement par clé publique. Thales est le seul groupe de haute technologie présent sur les marchés de la défense, de l'aéronautique et de l'identité numérique à avoir participé au concours.

La cryptographique post-quantique permettra aux ordinateurs classiques de résister aux attaques des ordinateurs quantiques extrêmement puissants qui devraient, selon de nombreux spécialistes, faire leur apparition d'ici quelques années. Les machines quantiques conféreront aux ordinateurs une telle puissance de calcul qu'ils seront capables de briser en à peine quelques secondes les algorithmes cryptographiques actuels.

Ce « bond quantique » de la puissance de calcul pourrait ouvrir la voie à une « apocalypse cryptographique » et constituer une menace extrêmement sérieuse pour la sécurité des systèmes numériques utilisés au quotidien par les citoyens et les organisations du monde entier, comme les systèmes d'information critiques, les services bancaires en ligne, les cartes de paiement, l'e-commerce, les procédures de signature électronique ou le vote en ligne. Un hacker disposant d'un ordinateur quantique, par exemple, pourrait facilement avoir accès à des données confidentielles, usurper l'identité de quelqu'un ou falsifier des transactions et des contrats juridiques. De la même manière, une nation pourrait voir sa sécurité menacée, si ses systèmes de communication critiques étaient la cible d'une attaque quantique.

Ce qui permet aux nouveaux algorithmes, tels que Falcon, d'être résistants au quantique, ce sont les problèmes mathématiques sur lesquels ils sont basés et qui sont parmi les plus difficiles à résoudre, même pour un ordinateur quantique.

Les organisations qui souhaitent protéger leurs données dans un monde dit de « confiance zéro » (Zero Trust) doivent adopter une solide stratégie de crypto-agilité quantique. Les équipes Thales de conseil en cyber solutions ont développé une offre d'architecture cyber post-quantique pour aider leurs clients à se préparer au risque de cyber-attaques provenant d'ordinateurs quantiques. Thales utilise également des algorithmes résistants au quantique dans son réseau de chiffrement et son module HSM Luna.

« *Thales est à la pointe de la recherche sur la cryptographie post-quantique depuis 2013 ; la sélection de l'algorithme Falcon par le NIST est la reconnaissance de l'excellence du travail de co-développement et de l'expertise de nos équipes de chiffrement. Nous allons poursuivre les recherches en cours en France et en Europe pour développer des solutions post-quantiques innovantes de confiance, sans rien sacrifier en termes de performance. Nous accompagnons d'ores et déjà nos clients dans leur transition vers une nouvelle génération de solutions de sécurité afin d'éviter une future 'apocalypse cryptographique' »,* indique **Pierre-Yves Jolivet, Vice-président, Solutions de Cyber Défense chez Thales.**

À propos de Thales

Thales (Euronext Paris: HO) est un leader mondial des hautes technologies qui investit dans les innovations du numérique et de la « deep tech » – connectivité, big data, intelligence artificielle, cybersécurité et quantique – pour construire un avenir de confiance, essentiel au développement de nos sociétés. Le Groupe propose des solutions, services et produits qui aident ses clients –

entreprises, organisations, États - dans les domaines de la défense, de l'aéronautique, de l'espace, du transport et de l'identité et sécurité numériques, à remplir leurs missions critiques en plaçant l'humain au cœur des décisions.

Thales compte 81 000 collaborateurs dans 68 pays. En 2021, le Groupe a réalisé un chiffre d'affaires de 16,2 milliards d'euros.

CONTACT PRESSE

Thales, Relations médias
Sécurité
Marion Bonnet
+33 (0)6 60 38 48 92
marion.bonnet@thalesgroup.com

EN SAVOIR PLUS

Groupe Thales

@Thalesgroup