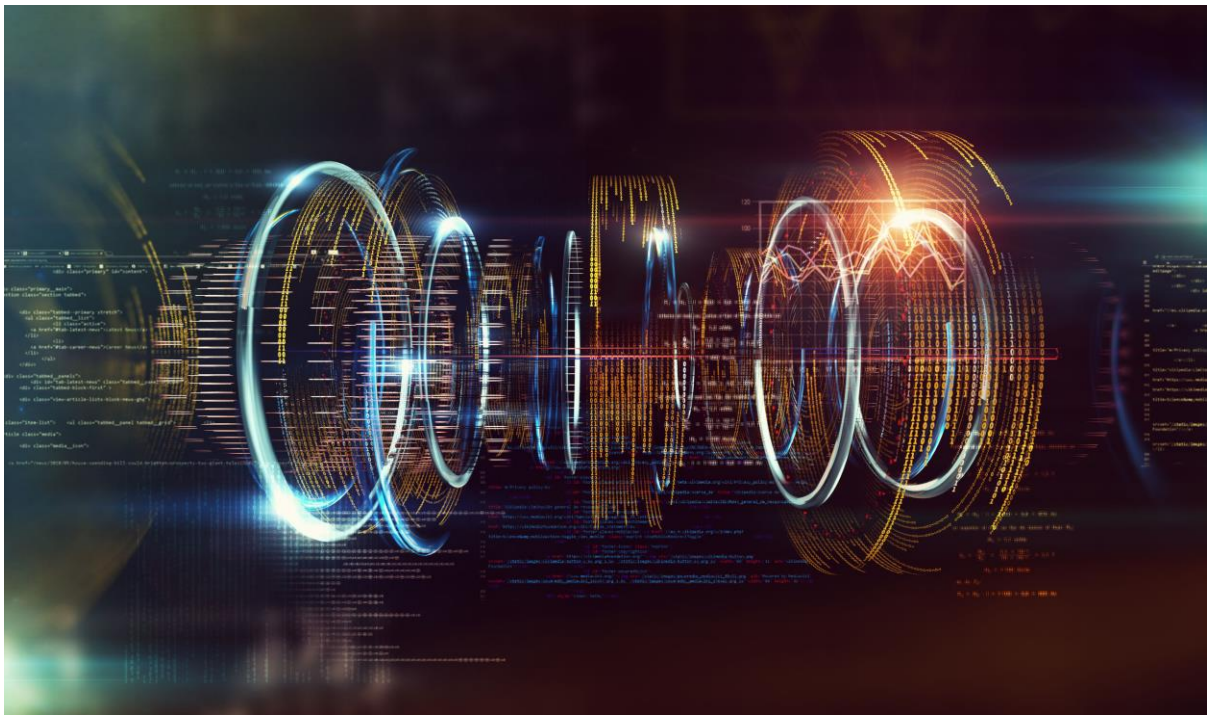
THALES
Building a future we can all trust

PRESS RELEASE
July 13th, 2022
Paris La Défense

Falcon algorithm co-developed with Thales selected by the NIST as a new standard in post-quantum cryptography

- **The US National Institute of Standards and Technology (NIST) has selected Falcon algorithm co-developed as a post-quantum cryptography standard for digital signatures, meaning it is able to withstand attacks from future large quantum computers.**
- **Falcon, selected for its extremely strong security and high bandwidth efficiency, will be included in the NIST's post-quantum cryptography standards expected to be fully defined within the next two years.**
- **The selection of Falcon, following a 5-year long global competition demonstrates Thales' leading position in cybersecurity, cutting-edge technology and research.**



© Carlos Castilla Jimenez

Following the launch in 2017 of a global challenge to set future post-quantum cryptography standards in digital signatures and public key encryption, which attracted 82 candidates from 25 countries, the NIST has selected Falcon algorithm co-developed for its extremely strong security and high bandwidth efficiency.

Falcon was co-developed by Thales together with academic and industrial partners from France (University of Rennes 1, PQShield SAS), Switzerland (IBM), Canada (NCC Group) and the US (Brown University, Qualcomm). It was selected by NIST alongside two other algorithms as standard for digital signatures, while a fourth algorithm was deemed standard for public key

encryption/KEM. Thales was the only technology group serving the defence, aerospace and digital identity markets, to take part in the NIST competition.

Post-quantum cryptography enables conventional computers to withstand attacks by large-scale quantum computers, which many specialists believe could appear in the next few years. Quantum machines are expected to increase today's computer processing power to such a degree that they could break current cryptographic algorithms in a matter of seconds.

This 'quantum leap' in computing power could usher in a "crypto-apocalyse" by posing very real and serious threats to the security of digital systems private citizens and organisations worldwide rely on day-to-day, such as critical information systems, on-line banking, payment cards, e-commerce, electronic signatures or on-line voting. A hacker with a quantum computer, for example, could easily gain access to confidential data, steal someone else's identity or falsify transactions and legal contracts. In the same way, a nation's security could be threatened if its critical communications systems were the target of a quantum attack.

New algorithms such as Falcon, are quantum-resistant because they are based on mathematical problems that are among the most difficult to solve, even for a quantum computer.

Organisations who are willing to protect their data in a Zero Trust world must adopt a strong quantum crypto agility strategy. Thales' Cyber Solutions consulting teams have developed a post-quantum cyber architecture offer to help their customers prepare for the threat of cyber-attacks by quantum-computers. Thales also provides quantum resistant network encryption and hardware security modules that are capable of protecting customer data against future quantum attacks, by already allowing customers to implement a number of Quantum Resistant algorithms.

"*Thales has been at the forefront of post-quantum cryptography research since 2013, and the selection of the Falcon algorithm by NIST is great recognition of the excellent co-development work and expertise of our crypto teams. We will pursue our on-going research in France and Europe to develop innovative, trusted solutions that will be quantic-resistant, without compromising performance, and are already helping our customers in their transition to a new generation of security solutions, to avert a future 'crypto-apocalypse'."* **said Pierre-Yves Jolivet, Vice-President, Cyber Defence Solutions at Thales.**

About Thales

Thales (Euronext Paris: HO) is a global leader in advanced technologies, investing in digital and "deep tech" innovations – connectivity, big data, artificial intelligence, cybersecurity and quantum technologies – to build a confident future crucial for the development of our societies. The Group provides its customers – businesses, organizations and governments – in the defense, aeronautics, space, transport, and digital identity and security domains with solutions, services and products that help them fulfil their critical role, consideration for the individual being the driving force behind all decisions.

Thales has 81,000 employees in 68 countries. In 2021, the Group generated sales of €16.2 billion.

PRESS CONTACT

GROUP COMMUNICATIONS – Thales - Tour Carpe Diem - 31 Place d
Cedex - France – Tel.: +33(0)1 57 77 86 26 - www.thalesgroup.com

PLEASE VISIT

Thales Group

PRESS RELEASE
July 13th, 2022
Paris La Défense

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

@Thalesgroup