PRESS RELEASE
Feb 24th, 2023
Paris La Défense

Thales pioneers Post Quantum Cryptography with a successful world-first pilot on phone calls

- Thales, leader in advanced technologies, successfully experimented end-to-end encrypted phone calls, tested to be resilient in the Post Quantum era.
- The pilot was performed with the Thales ‘Cryptosmart’ secure mobile app and 5G SIM cards installed in today's commercial smartphones, testing a mobile-to-mobile call, voice/data encryption, and user authentication.
- Any data exchanged during the call is set to be resistant to Post Quantum attacks thanks to a hybrid cryptography approach, combining pre-quantum and post-quantum defence mechanisms.

Thales, as a worldwide cybersecurity leader, has created the first real-world application of Post Quantum Cryptography (PQC) in its flagship secure ‘Cryptosmart’ mobile app, leveraging 5G SIM for PQC. In the pilot, hybrid cryptography (pre and post quantum crypto) was used in a phone call between two devices to protect the information exchanged during the call. Thales has invested and tested post-quantum cybersecurity technologies over the last decade in order to prepare for these emerging threats.

Even if today's quantum computer[1] prototypes are still far from posing a threat to public key cryptography, it is critical to begin investigating resilient solutions. For example, there is a variant of "store now, decrypt later" attacks that consists in storing today's exchanged data and messages in order to decrypt these messages once Quantum Computers are available. This means the majority of digital infrastructure security based on public key cryptography (PKC) may already be vulnerable to a quantum attack.

Such threats are relevant for scenarios involving highly sensitive information, such as classified information exchanged over an encrypted phone call. To address these threats, Thales created a proof of concept to test the scalability and quality of its solutions, which range from 5G SIM cards to secure communication software.

This first real-world quantum protected mobile solution, which combines Thales' 'Cryptosmart' application and its 5G SIM, employs hybrid cryptography, as recommended by the NIST (National Institute of Standards and Technology). 'CRYSTALS-Kyber', one of the four algorithms selected by the NIST[2], is the PQC algorithm natively implemented in the 5G SIM and used by Cryptosmart application to encrypt the communication.

"Building defences against threats that do not yet exist may appear to be a daunting task. That is exactly the prospect that the global cybersecurity community faces with the impending arrival of quantum computing. The post-quantum era is still years away, but as quantum computing becomes more prevalent, practicing crypto agility now with such pilots and trials are helping Thales and its customers get prepared" said **Philippe KERYER, Executive Vice President Strategy & Technology at Thales.**

[1] Computers that can perform certain tasks much faster than today's computers on a large scale.

[2] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

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 computing — to build a future we can all trust, which is vital to the development of our societies.

The company provides solutions, services and products that help its customers —businesses, organisations and states — in the defence, aeronautics, space, transportation and digital identity and security markets to fulfil their critical missions, by placing humans at the heart of the decision-making process.

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

PRESS CONTACT

Thales, Media Relations
Digital Identity and Security
Vanessa Viala
+33 (0)6 07 34 00 34
vanessa.viala@thalesgroup.com

PLEASE VISIT

Thales Digital Identity & Security
Thales unveils three quantum technologies set to revolutionise the world of tomorrow | Thales Group
Business Data Protection and Cybersecurity | Ercom

@Thalesgroup