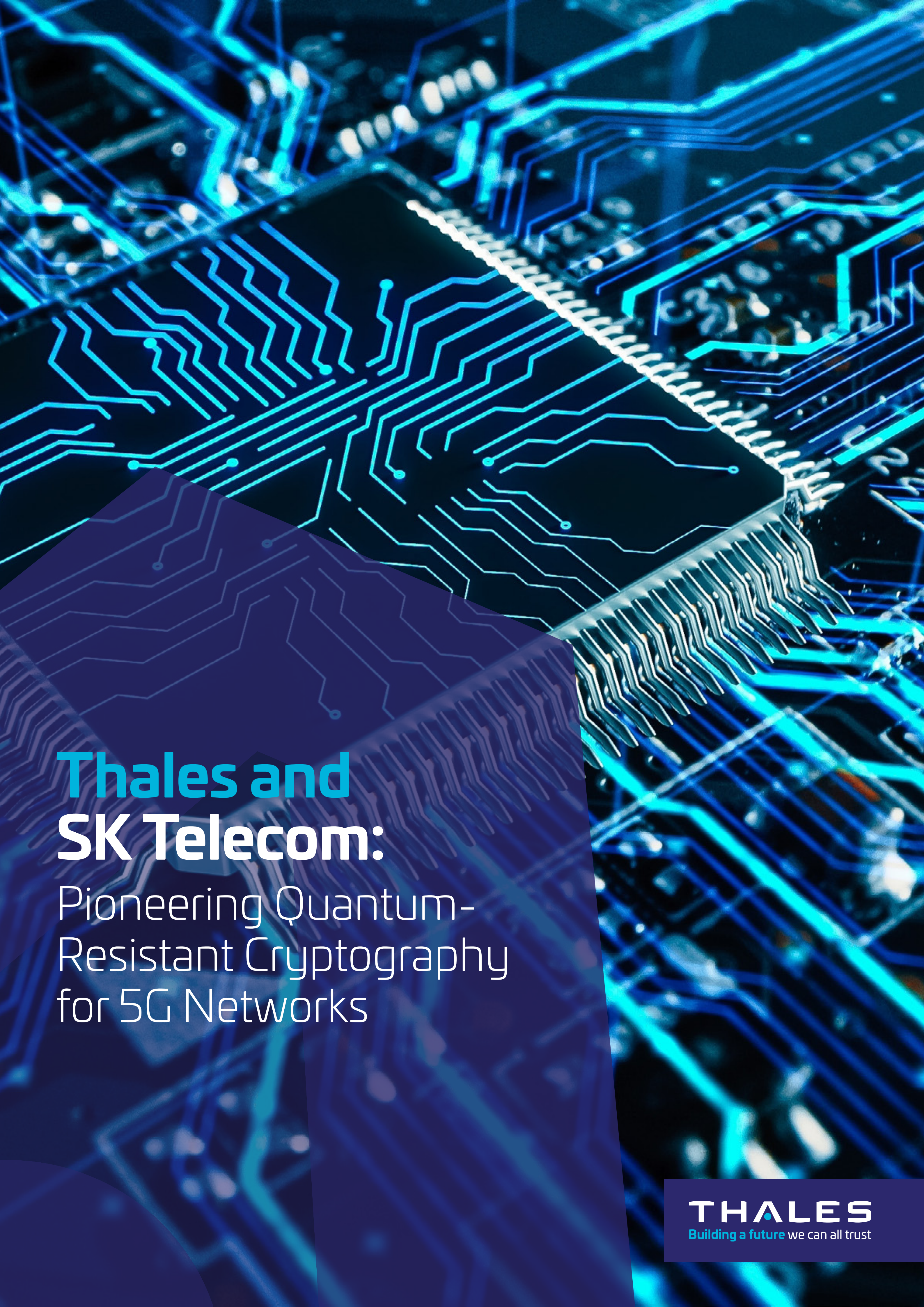
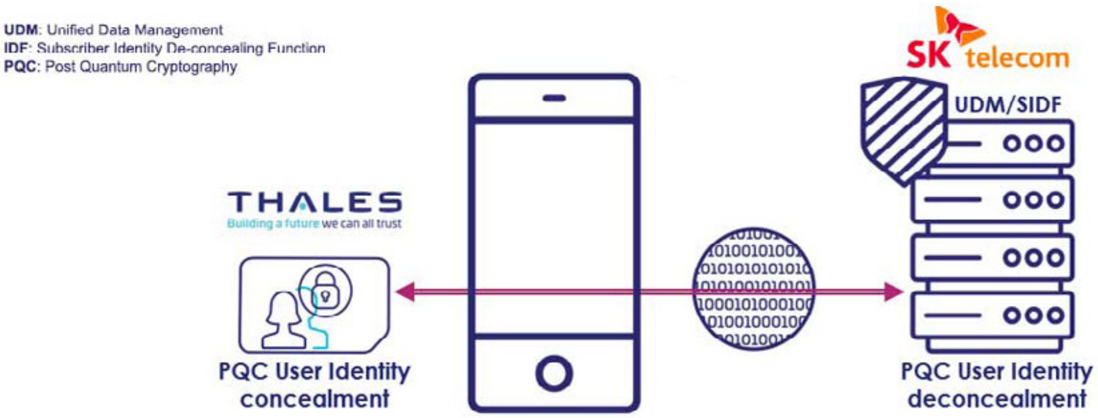


Thales and SK Telecom: Pioneering Quantum-Resistant Cryptography for 5G Networks

THALES
Building a future we can all trust

Thales and SK Telecom: Pioneering Quantum-Resistant Cryptography for 5G Networks

Mobile Connectivity Solutions


UDM: Unified Data Management
IDF: Subscriber Identity De-concealing Function
PQC: Post Quantum Cryptography
THALES
Building a future we can all trust
PQC User Identity concealment
SK telecom
UDM/SIDF
PQC User Identity deconcealment

SK Telecom and Thales have joined forces to advance post-quantum cryptography (PQC) within 5G networks.

Their collaboration has led to a successful end to end experiment to deploy PQC, utilising Thales 5G PQC SIM cards in SKT's standalone 5G real commercial environment.

This initiative is focused on protecting user identity and privacy against the threat posed by quantum computing.

Leveraging the Crystals-Kyber algorithm, which is anticipated to be secure against quantum attacks, the effort is in step with the National Institute of Standards and Technology's (NIST) goal to standardise such cryptographic measures.

This is relevant already today, in order to protect subscribers' identity, against "record now, decrypt later" tentatives. It is a step change versus previously demonstrated PQC encryption within secured applications, as it allows to encrypt and protect subscriber identity on a standard commercial telecom network.

Both companies are keen on enhancing cybersecurity, with SK Telecom integrating this technology for a robust quantum-safe communication system and Thales advocating for a shift to quantum-resistant algorithms to ensure ongoing security and privacy in the 5G domain.

Its ultimate goal is to ensure our digital communications' long-term safety in the forthcoming quantum computing era.

A silent but momentous revolution is unfolding in cybersecurity, led by SK Telecom and Thales.

This collaboration may dictate the future of digital security in the era of quantum computing.

With the emergence of quantum computers, which boast the ability to process vast amounts of data at speeds unfathomable to classical computers, a new challenge arises: the threat these machines pose to current encryption methods.

This is where post-quantum cryptography (PQC) enters, a discipline promising to keep our actual data and identity safe when quantum computers become the norm.

Let's dig in.

The Quantum Computing Challenge

Quantum computers, leveraging the principles of quantum mechanics, can theoretically break the cryptographic locks that secure our most sensitive data.

Post-quantum cryptography first stepped onto the scene in the 1980s, when visionary scientists postulated that the unique properties of quantum mechanics could be harnessed to speed up complex calculations.

This idea truly rocked the boat in the 1990s when the renowned mathematician Peter Shor dropped a bombshell: a hypothetical quantum computer could easily break the widely-used public key encryption algorithm.

This looming threat to encryption technologies like RSA and ECC, which underpin the security of virtually all modern data transmission, could leave our digital infrastructure vulnerable.

Post-Quantum Cryptography: The Quantum-resistant Alternative

PQC is not merely an upgrade to our current systems; it's an entirely new arsenal of cryptographic tools designed to be secure against the formidable processing power of quantum machines.

This new cryptography category aims to construct a security infrastructure that can survive the onslaught of quantum decryption capabilities.

The Vanguard of Quantum-Resistant Innovation

The partnership between SK Telecom and Thales has yielded a groundbreaking test of PQC in a real 5G standalone network environment.

The test leveraged Thales' 5G PQC SIM cards and SKT's standalone 5G environment to secure user identities and privacy against quantum threats.

By utilising the Crystals-Kyber algorithm, endorsed by the National Institute of Standards and Technology (NIST), the collaboration is at the forefront of the movement to standardise quantum-resistant cryptographic measures.

The Significance of Crystals-Kyber

Crystals-Kyber represents a class of lattice-based cryptography lauded for its ability to resist quantum and classical decryption attempts.

Its adoption by two industry leaders showcases a proactive approach to securing actual communications against future quantum attacks.

Preparing for the Quantum Era

While quantum supremacy—the point at which quantum computers can perform tasks that classical computers fundamentally can't—is still a topic of debate, the consensus in the security community is clear: the time to prepare is now.

Why?

The U.S. National Institute of Standards and Technology (NIST) projects that by 2029, quantum computers will be capable of decoding existing public key infrastructures, including the widely-used 128-bit AES encryption.

The NSA and other global security authorities have been vocal about transitioning to quantum-resistant algorithms, emphasising the importance of becoming "crypto-agile."

Thales: A Proactive Stance on Quantum Security

Thales has recognised the urgency of developing quantum-resistant solutions and taken tangible steps towards realising them.

In a recent pilot, Thales successfully conducted encrypted phone calls impervious to quantum threats, using their 'Cryptosmart' secure mobile app and Thales' 5G PQC SIM . This represents a significant leap towards crypto agility and positions Thales as a trailblazer in quantum-safe security solutions.

The Quantum Horizon: Looking Ahead

For those seeking to delve deeper into the intricacies of PQC and its implications for our digital future, resources such as ETSI's guidelines for post-quantum cryptography migration and the NSA's FAQ on quantum computing and the Commercial National Security Algorithm Suite 2.0 offer invaluable insights.

Conclusion

The strategic partnership between SK Telecom and Thales is a testament to the power of innovation and forward-thinking in the face of emerging threats.

By embracing the challenges posed by quantum computing, the two companies are not just defending against a potential threat—they're redefining what it means to be secure in the digital age.

The journey of adaptation and the strides made in post-quantum cryptography remind us that with the right approach, even the most daunting challenges can be transformed into opportunities for advancement and growth.