Kudelski IoT Launches Quantum-Resistant Security IP, Future-Proofing Semiconductors Against Emerging Quantum Threats

New Quantum-Resistant Algorithms Integrated into KSE Security IP to Protect the Next Generation of Chips and Devices, Responding to Global Regulations

Cheseaux-sur-Lausanne, Switzerland, and Phoenix, AZ, (November 11, 2024) – Kudelski IoT, a division of the Kudelski Group (SIX: KUD.S), today announced the integration of quantum-resistant cryptography into its KSE security IP products for semiconductor manufacturers, further enhancing their ability to safeguard System on Chip (SoC) products and the devices that use them from emerging quantum computing threats and ensure long-term data protection for their customers.

Quantum-Resistant Cryptography (QRC) is specifically designed to withstand the advanced capabilities of quantum computers, which are expected to surpass the strength of current cryptographic systems within the next decade. Traditional cryptographic methods, such as RSA and Elliptic Curve Cryptography, face the risk of becoming vulnerable. By incorporating quantum-resistant algorithms into the KSE, Kudelski IoT strengthens the security SoCs, protecting them from emerging threats while maintaining performance, efficiency, and flexibility.

KSE is a flexible security IP platform that delivers robust authentication and secure updates for System-on-Chip (SoC) devices. With the integration of quantum-resistant algorithms, KSE now provides a future-proof solution to safeguard the authenticity, integrity, and confidentiality of IoT assets, automotive application assets and AI models in a post-quantum world. The quantum-resistant algorithms integrated into KSE include LMS from NIST special publication SP800-208 for stateful hash-based signature schemes, ML-KEM from FIPS 203 standard for key encapsulation mechanisms, and ML-DSA from FIPS 204 standard for digital signatures. These algorithms, recommended by leading bodies such as the National Institute of Standards and Technology (NIST) and in US CNSA 2.0 (The Commercial National Security Algorithm Suite 2.0), ensure that SoCs are well-protected against quantum-based threats. Quantum-Resistant Cryptography is crucial for devices and data with long lifecycles, making sectors like automotive, telecommunications, energy, finance, healthcare, government and military prime beneficiaries of these advanced cryptographic methods.

A major advantage of Kudelski IoT's solution is its ability to update cryptographic algorithms in the field as new vulnerabilities or advances in cryptography emerge. This ensures that manufacturers can keep their devices secure without the need for costly recalls or hardware replacements, providing a level of security that evolves with technology.

As one of the first companies to offer quantum-resistant security IP for semiconductors and devices, Kudelski IoT is at the forefront of future-proofing connected assets. Combined with its renowned Security Labs and device-to-cloud Public Key Infrastructure solution, keySTREAM,

Kudelski IoT delivers a comprehensive suite of services that assist manufacturers in navigating the transition to quantum security.

“We are tackling the quantum challenge with a comprehensive, end-to-end approach,” said Frédéric Thomas, CTO of Kudelski IoT. “Our team of cryptographers, mathematicians, and security experts is dedicated to ensuring that semiconductors and the products they’re built into are resilient against quantum threats, providing long-term security and value to our customers.”

Kudelski IoT’s quantum-resistant KSE security IP is now available to semiconductor and device manufacturers. As industries prepare for the post-quantum era, Kudelski IoT’s solution empowers manufacturers to design, produce, and deploy secure devices with confidence, ensuring long-term protection for years to come.

For more information on Kudelski IoT’s quantum-resistant security solutions, please visit www.kudelski-iot.com.

About Kudelski IoT

Kudelski IoT is the Internet of Things division of Kudelski Group and provides end-to-end IoT solutions, IoT product design, and full-lifecycle services to IoT device manufacturers, ecosystem creators, and end-user companies. These solutions and services leverage the group’s 30+ years of innovation in digital business model creation; hardware, software and ecosystem design and testing; state-of-the-art security lifecycle management technologies and services and managed operation of complex systems. For more information about Kudelski IoT, please visit www.kudelski-iot.com.

Media contacts

Christopher Schouten
Sr. Marketing Director
+1 (480) 819-5781
christopher.schouten@nagra.com

Marc Demierre
Kudelski Group
Director Corporate Communications
+41 79 190 17 09
marc.demierre@nagra.com