KUDELSKI IOT THINGS

FOCUS AREA

Quantum Resistance

With our expertise in quantum cryptography and quantum security, we provide comprehensive assessments of quantum-related cybersecurity risks and offer robust solutions to create quantum resistant products and ecosystems.

WHAT IS QUANTUM RESISTANCE?

Quantum resistance, a critical concept in modern cybersecurity, encompasses security protocols and algorithms capable of withstanding quantum computer attacks. As traditional encryption becomes more vulnerable with advancing quantum computing, adopting quantum-resistant technologies is key to protecting IoT devices and ecosystems, ensuring data safety, and protecting digital assets against emerging threats. Embracing quantum security today is critical to safeguarding your future

FOUR STEPS

Prepare your company to Quantum computing

Overall, preparing for the threat of quantum computing requires a proactive, agile and forward-thinking approach. By taking these steps, companies can help ensure the security of their products and services in the face of this emerging technology.

1. Assess the risk

Companies should start by assessing the potential impact of quantum computing on their products and services. They should identify the critical assets that need to be protected. Then they should evaluate the strength of their current cryptographic algorithms and protocols used in their company according to the shelf life and sensitivity level of each asset.

2. Develop a quantum strategy

Companies should start developing a strategy for implementing quantum-resistant cryptographic algorithms and protocols. This may involve developing new cryptographic algorithms, updating protocols or using existing quantum-resistant cryptographic algorithms.

3. Stay informed

Companies should stay up to date with the latest developments in quantum computing and quantum-resistant cryptography. This can be done by following the research community, standardization and regulations processes, attending conferences, and engaging with industry experts.

4. Conduct regular security audits

Companies need to have confidence in both hardware and software security implementations. They should validate the robustness of critical assets by conducting regular security assessments to identify vulnerabilities and potential weaknesses in their cryptographic algorithms and protocols. This will help them to proactively address security issues before they can be exploited.

APPROACH

Quantum Security Portfolio

Our mission is to help you distinguish fact from hype, comprehend the technology, understand associated risks, and confidently transition to a future that is quantum-secure. Our extensive expertise ranges from discovering cryptographic vulnerabilities, assessing and developing secure hardware, to quantum cryptography and the implementation of quantum-resistant standards that align with the highest industry demands.

Quantum Education & Training

Equip your team with the knowledge to navigate the quantum security landscape with confidence. Our programs cater to a diverse audience, from academic institutions to businesses and across all levels, from executives and tech leaders to engineers.

Quantum Security Assessment

In our collaborative approach, we identify potential security vulnerabilities in your system and conduct a comprehensive inventory of all cryptographic elements, Leveraging the latest technological advancements, we provide an in-depth quantum threat assessment and strategic recommendations for risk mitigation, aiming to strengthen your defenses in the rapidly evolving quantum landscape.

Quantum-Secure Architecture Design

Are you at the helm of designing a solution from the ground up? Leverage our expertise to seamlessly integrate quantum security at the earliest stages. This is especially critical for long lifecycle products, services, and for enterprises seeking long-term compliance.

Learn more on www.kudelski-iot.com

Secure IP for the Quantum Age

Offering a broad assortment of secure hardware IP integrations, our solutions utilize the most recent cryptographic recommendations from bodies such as NIST/BSI. Combined with our system's inherent crypto-agility, we provide an optimal solution that not only offers resilience against standard attacks but also enables updates to cryptography to comply with emerging algorithms and evolving standards.

Quantum Hardware Evaluation

Our Kudelski IoT Labs, along with our esteemed partners, are ready to assist you in evaluating the security robustness of a product. This includes an assessment of side-channel attack resilience, quality of randomness, adherence to FIPS standards, and more. Leverage our top-tier hardware analysis capabilities to ensure your product's quantum security readiness.

Quantum Migration Advisory and Deployment

Partner with us to devise, execute, and oversee a custom-made strategy for a seamless transition to quantum security. As a technology-agnostic entity, we select the most appropriate countermeasures aligning with your business needs. Our objective is to facilitate an effective quantum security migration tailored to your unique requirements.

ABOUT KUDELSKI GROUP

$100B
revenues enabled annually

500M
devices provisioned & managed

$716M
revenues (2022)

3250
employees

32
offices worldwide

70+
years of innovation