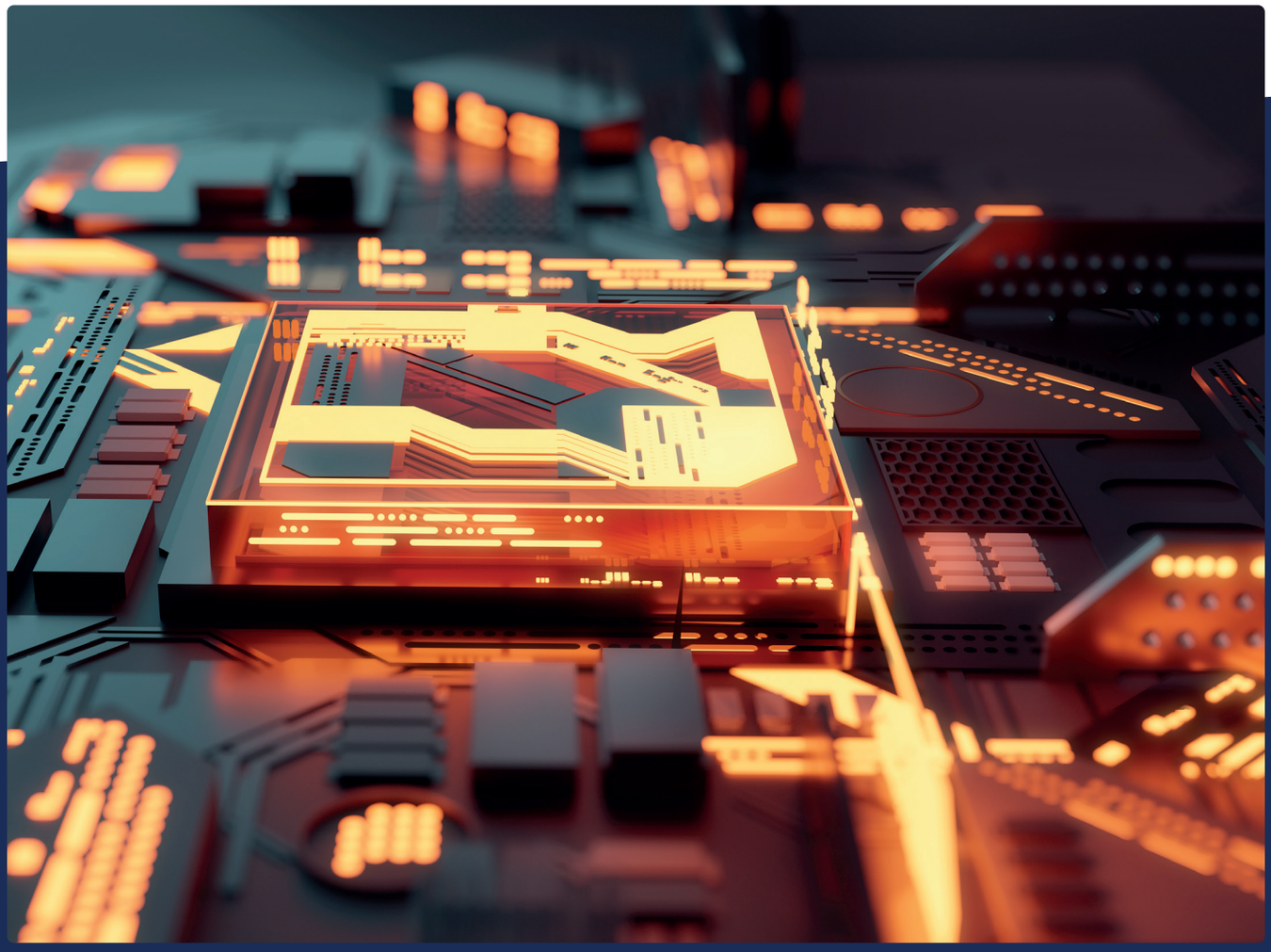
KUDELSKI IOT THINGS



WHITE PAPER

4 Steps to Defending Your Products Against Quantum Computing

Quantum computing has the potential to break current encryption and authentication methods based on classical asymmetric cryptography, which could pose a serious threat to data security and privacy for a wide variety of companies. As such, companies that rely on classical cryptography to protect their products and services should start preparing for the possibility of quantum attacks.

www.kudelski-iot.com

info@kudelski-iot.com

Here are four steps that companies can take to prepare for quantum computing

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-resistant 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. The migration strategy should also focus on evaluating the costs and potential challenges associated with the transition. This may involve investing in new hardware, software, and training for their employees. Product and software development, internal infrastructures, and key management processes shall also be part of this quantum-resistant strategy.

3. Stay informed

Companies should stay up to date[1] 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 assessments

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.

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] NIST(USA), ANSSI (France), BSI (Germany), ENISA (Europe), Cryptec (Japan), China regulation authorities
For the standards updates: PKCS#11(includes HSS), under redactions: ETSI, IETF
Others launching projects on Quantum resistant algorithms: RISQ, QuIC, SQC, WEF Quantum Economy Network.

How does the Kudelski Group address this technological disruption?

Kudelski Group offers a variety of different services and solutions that enable companies and institutions to understand their risks and take action to mitigate them.

Threat Assessment

The first step of all our engagements is to identify the client's exposure to possible threats. This requires understanding not only the technology used, but also how it is deployed and what kind of data is processed therein.

Connected systems and IoT devices are exposed to a wide range of security risks. Companies which develop IoT systems supposed to secure assets, data and processes in the long run, need to identify what are the entry points that matter. Threats and constraints landscape analysis from the business model, technological and contextual standpoints increase awareness of potential threats scenarios and enables development teams to focus their effort on reaching the desired level of security of the IoT system.

A comprehensive device and system-wide threat assessment encompassing the quantum threats will provide a list of envisioned risks and threats scenarios, the likelihood of an event with a successful attack and its impact for the product, the user and/or the business. Quantum-Secure Architecture. The importance to select the right components and to implement the right configuration at start or enable a future shift towards quantum-secure solutions will ensure the desired security level to be reached and maintained over time. The security architecture of an IoT system must provide appropriate measures to protect the most critical assets to reach the business objectives while accepting risk where appropriate.

By incorporating quantum resistance, the system will embed the right features to protect data and communications, ensure the integrity of the device, and address its security lifecycle to hold control over time.

Cryptographic Discovery and Inventory 2

We detect and compile an inventory of all the cryptographic artifacts on the system in exam within hosts, storage, and network. This includes SSL certificates, cryptographic keys, libraries, transmission protocols, and more. Weak cryptography is flagged for inspection.

Quantum-Secure Architecture 3

We help you designing quantum-resistant hardware or software architectures, or to review an existing one. Crucial for long lifecycle products or services, or for enterprises who need long-term compliance.

Quantum Security Assessment and Reporting 4

Our experts perform a detailed evaluation of any issue found in the discovery or testing phase, including cryptographic artifacts, hardware side-channels, and code. We rank these issues by severity and provide mitigation recommendations taking into account the latest technology developments.

We reproduce public attacks on the hardware implementations such as SPHINCS+, CRYSTALS-Dilithium, or CRYSTALS-Kyber and investigate new ones using fault injection and side-channel attacks. We perform research of vulnerabilities on custom solutions. We validate the robustness of quantum-secure algorithms design, implementation and their countermeasures.

"On Protecting SPHINCS+ Against Fault Attacks" https://ia.cr/2023/042 (CHES 2023)

"A Practical Template Attack on CRYSTALS-Dilithium" https://eprint.iacr.org/2023/050.pdf (CHES 2023)

"Power analysis attack on Kyber" https://eprint.iacr.org/2021/1311.pdf

"Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste" https://eprint.iacr.org/2022/1713.pdf

Migration Advisory and Deployment

5

We help you to design, implement, and monitor an effective and tailor-made strategy for a smooth quantum security migration. We are technology-agnostic and will consider the best suitable countermeasure for your use case.

Secure IP

6

We offer a vast portfolio of secure IP, which includes not only resistance against standard attacks, but also support of the latest quantum-resistant cryptographic algorithms and novel features.

Quantum-Secure Solutions for Cryptographic algorithms

In addition to classical cryptographic algorithms, Kudelski IoT's Secure IP optionally embeds several quantum resistant algorithms. Based on the first standard recommendation NIST-SP800-208, the stateful hash-based signatures, LMS, XMSS and their extension could be available. Indeed, IoT devices will remain in the fields several years: depending on their purpose, they should be designed with quantum computing threat in mind. Stateful hash-based signatures offer solutions to secure IoT device initialization and over-the-air updates. Although the standards are not yet available, CRYSTALS (Cryptographic Suite for Algebraic Lattices) based -Kyber and Dilithium could also be embedded in Kudelski's Secure IP. Development and integration of other lattices-based schemes - Frodo-KEM and Falcon- and stateless hash-based signature Sphincs+ are also planned in its roadmap.

Moreover, Secure IP features and interfaces enable hybrid asymmetric cryptography which relies on well-known and evaluated asymmetric algorithms (RSA and ECC based) in combination with quantum resistant algorithms.

Performances and security agility

To bring performance and flexibility, the secure IP uses a RISC-V architecture enhanced by hardware accelerators. For quantum resistant algorithms to guarantee agility and capability to update them according to new specifications releases or new attacks, the implementation is a combination of hardware and software primitives.

To ensure security, robustness against side channel and fault attacks the secure IP designers take them in consideration at the different design phases of hardware and software functionalities.

Considering the constant attacks, security evolutions, and standards updates: the secure IP provides features to enhance life cycle management, secure update mechanism and secure initialization including the quantum computer as a threat.

Education and Training

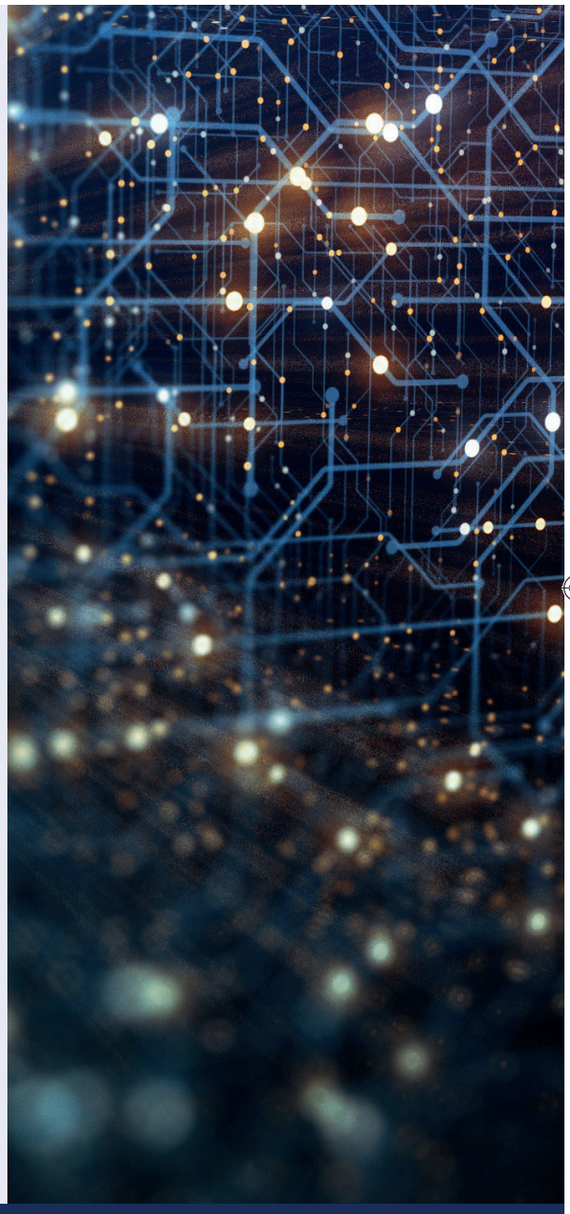
7

We provide expert training and education on quantum computing and quantum security topics, and their applications and implications. From academia to business. For executives, tech leaders, and engineers.

The potential threats posed by quantum computing to product security are significant and must be taken seriously. As quantum computers continue to evolve, traditional encryption methods that have long been relied upon to protect sensitive data and intellectual property may no longer suffice.

However, businesses and organizations can take proactive steps to protect their products from the risks of quantum computing. They can begin by conducting a comprehensive assessment of their current security protocols and identifying areas that may be vulnerable to quantum attacks. Next, they can explore alternative encryption methods that are resistant to quantum computing, such as lattice-based cryptography.

Moreover, businesses can also invest in quantum-safe solutions that have been specifically designed to withstand the power of quantum computing. It is crucial to stay informed and up-to-date on the latest developments in quantum computing and quantum-safe technology to ensure that products remain secure in the face of these emerging threats.



CONCLUSION

While quantum computing poses significant security challenges, there are steps that businesses and organizations can take to protect their products from the threats posed by this emerging technology. By staying proactive and vigilant, organizations can ensure that their products remain secure and protected in the era of quantum computing.