KUDELSKI SECURITY

QUANTUM SECURITY

Quantum Computing and Security in Nutshell

Within the next few years, scalable quantum computing will likely disrupt information processing as we know it. New powerful algorithmic tools will be made possible by large quantum computers, facilitating quantum attacks on the basic cryptographic schemes that underpin all digital infrastructures and systems.

Separating fact from fiction, Kudelski Security can help you understand the implications of quantum computing for your current and future business.

1. What assets are at risk?

Explore & Assess – We discover and collect data that needs to be analyzed, especially relating to cryptography, analyzed, and identify risks.

2. How can you mitigate the risks?

Harden – For identifiable risks, we propose quantum-secure mitigation strategies, leveraging broader IoT and cryptography services, including:

- Help selecting the right cryptographic scheme to replace a quantum-vulnerable one.
- Testing IoT devices in the lab for side-channel vulnerabilities that could be amplified by quantum attacks.
- Auditing quantum-resistant cryptographic code.
- Benchmarking quantum security devices such as QKD and TRNG.

3. Looking to create market differentiation?

Certify – We compile a security assessment report and can provide public certification that Kudelski Security has carried the assessment out.

Access Training - Training modules cover quantum computing and cryptography, quantum security (theory and practice), quantum-resistant cryptography, and quantum algorithms.

If you answer 'yes' to any of the questions below, you will need to ensure that your long-term approach to risk encompasses questions around quantum computing.

Business leaders

- ☐ Do you deal with data, trade secrets, or products that require confidentiality, integrity, and/or authentication?
- ☐ Do your products or services have to retain their security for 5-10 years?
- ☐ Do you deal with high-value, long-term confidential data relating to GDPR, military, health, genomics, etc.?
- ☐ Will you be compliant when the new quantum-secure NIST standards are published by 2023?

System & product developers

- ☐ Do your products use cryptography, e.g. RSA, DSA, Diffie-Hellmann, ElGamal, ECDSA, or elliptic curves?
- ☐ Do your product or services require a source of high-quality randomness?
- ☐ Are you adopting or planning to adopt quantum key distribution (QKD)?
- ☐ Do you use cryptography in hardware devices?

QUANTUM TOPICS MAP

What is Quantum Computing (QC)?

- **Definition:** Experimental computational technology based on quantum mechanics.
- **Impact:** Revolutionary computational paradigm shift that impacts the security of traditional cryptographic algorithms.
- **Status:** Prototypes exist but are not very powerful. It is difficult to estimate if and when large-scale quantum computers will arrive, but progress is accelerating. Many estimates suggest 5-15 years from now.

QC will be applied across applications:

SECURITY APPLICATIONS

- Quantum computers can attack most cryptography used today.
- Consequences for cybersecurity are potentially devastating.

Two Possible Countermeasures:

1 QUANTUM-RESISTANT CRYPTOGRAPHY

Runs on classical hardware (modern computers, smart phones, embedded systems, etc.)

Often called “post-quantum” cryptography

Based on mathematical problems that are too hard even for a quantum computer to solve

No “one-size-fits-all” solution, adoption must be evaluated carefully

NIST standardization process ongoing

2 QUANTUM CRYPTOGRAPHY

Runs on quantum hardware

Ambiguous term, can have two meanings:

MEANING 1

QUANTUM KEY DISTRIBUTION (QKD)

Commercially available today

Requires special hardware

Very secure in theory but has practical limitations

MEANING 2

FULLY QUANTUM CRYPTOGRAPHY

Uses quantum computers to do cryptography on quantum data

Still at the research stage, but very important for the future of quantum networks

Security Applications Not Connected to QC

Quantum radars, quantum navigation sensors, quantum true random number generators

Civilian Applications

Quantum algorithms that can speed up many applications, including: pharma, chemistry, health, genetics, A.I., finance, optimization, and logistics