

Understand and Prepare for the Era of Quantum Computing With Our Consulting and Training Services

Scalable quantum computing will cause a revolution in information processing in the next few years. While the business potential is huge, not all impacts will be positive. Large quantum computers will threaten the security of IT systems by making new kinds of attacks possible. These include quantum attacks on the basic cryptographic schemes that secure all of our infrastructures and systems.

Separating fact from fiction, Kudelski Security's experts in quantum computing and cryptography will help you gain a measured, objective understanding of the relevance and risks to your business and the implications for future and current business and operations.


Who Needs to Be Thinking Quantum?

Many products or services require long-term security assurance. Everything from IoT devices and SCADA systems to data processors and intelligence need to stay secure for the foreseeable future—for reasons of security as well as regulatory compliance.


A Long-Term Approach to Risk Incorporates Questions on Quantum Computing




The Kudelski Security Advantage



Proven expertise in improving client security posture



Consulting service covering all quantum security threats



Expertise in complementary areas e.g. cryptography, IoT

When is it Time to Adopt Quantum-Resistant Cryptography?

Certain data or products require long security assurance time (automotive, financial, military, etc.) Others require an extremely long time (health, genomics).

Encrypted data is being harvested right now by powerful adversarial actors.

A = Time necessary to research and standardize new quantum-resistant cryptography

B = Time necessary to deploy the new cryptography to products in the field

C = Time that today's products (or information processed therein) are required to remain secure

D = Time before a scalable quantum computer is built

If $A + B + C > D$
then the security of your business is already at risk today.



We are currently still in timeframe A—it's time to switch!

Quantum Security Strategic Consultancy & Training

Kudelski Security's team of cryptographers and researchers, with their established quantum computing expertise, can help you understand the implications of the new quantum technology.

Five-Phase Strategic Consultancy Engagement

- 1. Explore:** We work with you to discover and collect data, especially relating to cryptography, that needs to be analyzed.
- 2. Assess:** We analyze the data collected during the discovery phase and identify possible risks.
- 3. Harden:** We propose quantum-secure mitigation strategies.
- 4. Expand:** Kudelski's IoT security and cryptography services offer complementary support, 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.
- 5. Certify:** We compile a security assessment report and can provide "Checked by Kudelski Security" certification.

Quantum Training Program

Training modules are designed for different target audiences from C-level to technical and cover a wide range of topics, including:

- Quantum computing and cryptography
- Quantum security (theory and practice)
- Quantum-resistant cryptography
- Quantum algorithms

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

Info@kudelskisecurity.com | www.kudelskisecurity.com

