**20.05.2019 | QUANTUM COMPUTERS**

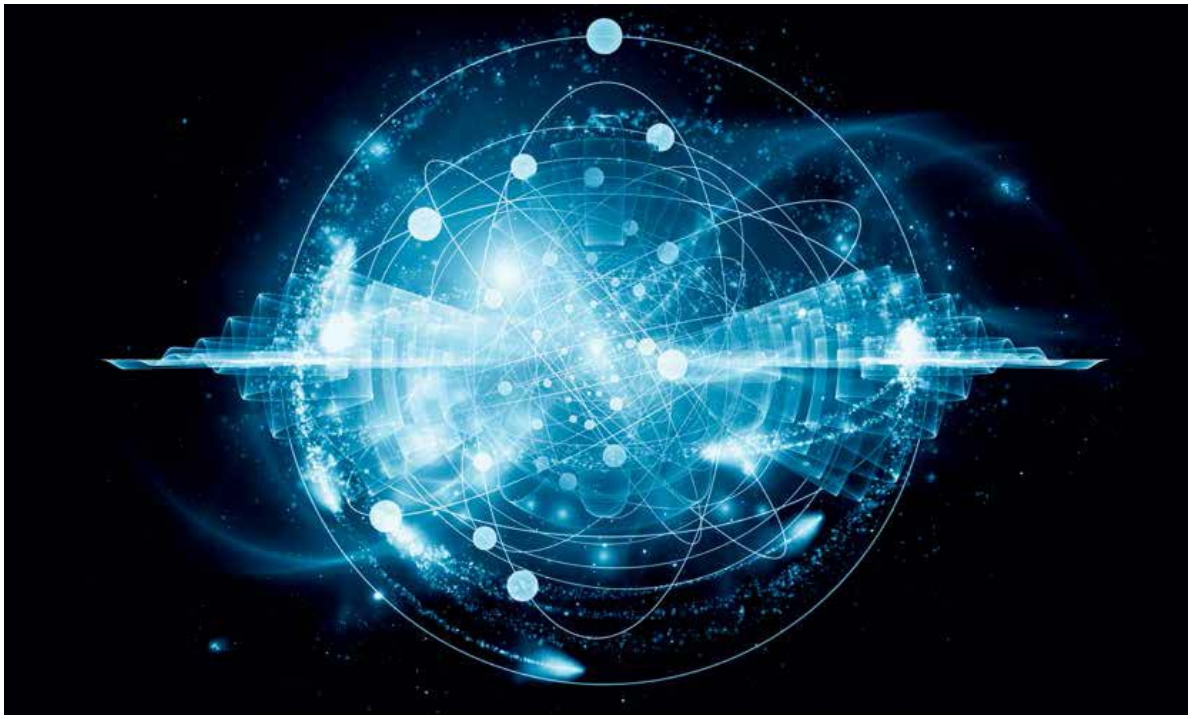
# A THREAT TO CRYPTOGRAPHIC SYSTEMS?

**In theory quantum computers will solve arithmetic problems many times faster than digital computers. Although this promising technology is still at the beginning of its development, it may soon challenge the security of certain cryptographic systems.**

With their potential capacity to process information millions of times faster than today's most advanced supercomputers, quantum computers could solve in minutes problems a conventional computer would take thousands of years to process. Scientists expect that quantum computing will for example enable them to predict and improve chemical reactions in the research for new medicine or develop new materials with innovative properties.

Inside the first IBM Q computation centre, dilution refrigerators with microwave electronics (middle) that operate IBM Q Network clients' cloud access to 20 qubit processor. (Credit: IBM/Connie Zhou)

Certain experts warn that quantum computers could at some point become powerful enough to break today's encryption systems and provoke a so called «cryptocalypse», jeopardizing the security of state secrets, bank accounts and other sensitive information. Are these fears justified? Martin Ågren, cryptographer at Crypto, is more guarded in his assessment: «Quantum computers could pose a threat to certain cryptographic protocols, but definitely not to others. If you are worried about the so-called cryptocalypse, the best thing you can do is to switch to cryptographic systems that are secure against a quantum adversary. At Crypto, we have been using quantum-safe symmetric cryptography for many years!»



Certain experts warn that quantum computers could become powerful enough to break today's encryption systems and provoke a so called «cryptocalypse». (Credit: Shutterstock)

### The solution: quantum-safe encryption

The question therefore arises as to which encryption systems could be threatened by quantum computing. There are basically two types of systems: symmetric and asymmetric. For symmetric encryption processes like the Advanced Encryption Standard (AES), quantum computers pose a relatively minor threat despite the existence of quantum algorithms able to break the encryption. The potential boost in computing performance generated by the new type of computers could easily be countered with slightly longer keys.

For asymmetric encryption processes like RSA (from the last names of its three inventors: Rivest, Shamir and Adleman), it's a different story. Peter Shor's quantum algorithm could theoretically break several encryption codes of this type with the help of a quantum computer. As widespread applications like e-commerce rely on asymmetric cryptography, the concern about the protection of this kind of cryptographic systems in the future is justified. Post-quantum cryptography (PQC) is a subfield of cryptography that precisely deals with this question and cryptologists are already working on a new quantum-safe asymmetric system.

**Better safe than sorry**

By way of conclusion, Martin Ågren pinpoints the fact that organisations and companies dealing with highly sensitive data should act now to be safe in the future: «Intelligence services may already be collecting data that is not encrypted in a quantum-safe way with the intention to break it later, once quantum computers are operational. This is why I strongly recommend to implement a quantum-safe encryption system like the one used by Crypto as soon as possible!»

**How do quantum computers work?**

While the bit of a classical computer can only possess a well-defined state of 0 or 1, the quantum bit (qubit) of a quantum computer can exist in a superposition of both. When combined with carefully engineered algorithms, this leads to enormous computational power. In the midterm quantum computers represent a potential threat to information security because they could manage to crack various algorithms used as a basis for different cryptographic processes.

So far the main obstacles to the development of quantum computers have been hardware limitations. To function properly, a quantum processor must be well-isolated from its surroundings. In addition, most solid-state quantum computers can only operate at an ultralow temperature close to absolute zero (-273°C). Due to these constraints, in a foreseeable future quantum computers are unlikely to replace conventional computers and would remain the privilege of large organisations, cloud services, universities and research centres.

For more information on quantum-safe encryption solutions, visit: www.crypto.ch or contact Crypto's experts: crypto@crypto.ch