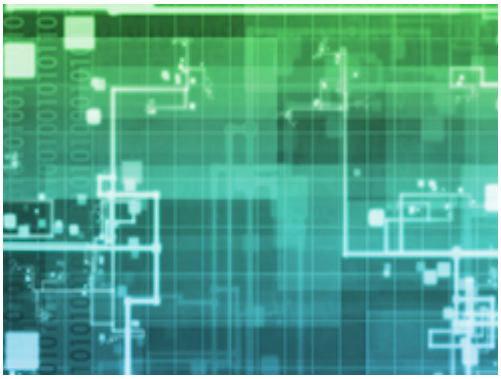
Securing encryption data against the threat of future quantum computers

When quantum computers become available, an existing algorithm will challenge current encryption techniques now considered secure. Work being done by an EU-funded project is laying the grounds for a solution.



© kentoh, Shutterstock

In a paper recently published in the journal 'Nature', researchers outline several approaches to developing new, quantum-attack resistant encryption techniques. One obvious approach is the development of new encryption techniques that avoid the use of current techniques as these could be undermined in the future.

The problem facing current encryption

At the moment our online security largely depends on what is known as the RSA (Rivest-Shamir-Adleman) system which is largely used in encryption. This depends on the use of public keys that consist of the product of two prime numbers. Currently even the most powerful computers we have would take a large amount of time to identify the two primes, a process known as factorisation: the most powerful supercomputers would take centuries to unravel the puzzle.

At the other end of the encrypted data is the receiver of the message who holds a private key in the form of a number known only to them and the sender. By using a mathematical operation, the two prime numbers required to decode the message are obtained with the private key. As long as the private key is not intercepted, the encoding is robust.

But with more powerful quantum computers around the corner, the processing power required to crack the primes will be available, making what until now has been a highly secure process, far more leaky. This has been known since 1994 when an

algorithm for quantum computers that would split a large public key into its two prime numbers in a matter of seconds or minutes was published.

Researchers identify first stages in a solution

The PQCRYPTO (Post-Quantum CRYPTOgraphyfor long-term security) team outline a two-pronged approach: along with the idea that a viable solution could be based on the development of new encryption techniques, another suggestion is to focus on techniques involving mathematical operations for which quantum computers aren't efficient.

The researchers highlight several restraints for the techniques that will have to be developed. These should inspire confidence and not be too costly to apply, and not too demanding on computing systems. They should also avoid keys that are of inordinate lengths. The authors insist on one important aspect for the development of future post-quantum encryption systems: an early attention to standardisation since all parties will have to use the same cryptographic systems.

For more information, please see:
PQCRYPTO project website

Countries

Netherlands

Related projects

HORIZON 2020

PROJECT

Post-quantum cryptography for long-term security

PQCRYPTO

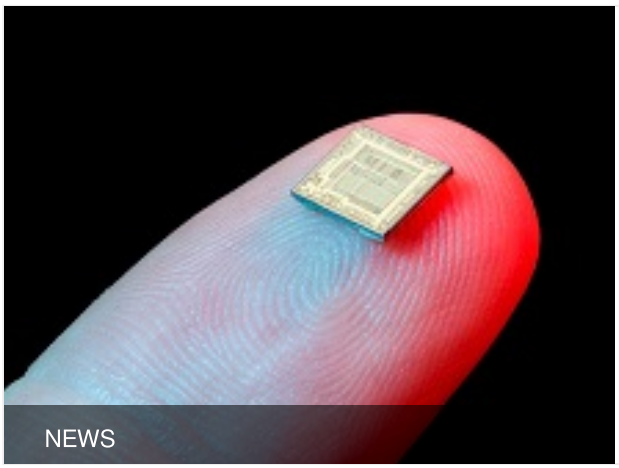
7 September 2023

Related articles

SCIENTIFIC ADVANCES

Can quantum cyberattacks be prevented? An EU initiative says yes, shows how

26 March 2020



SCIENTIFIC ADVANCES

A quantum leap for silicon chips: Spin-photon coupling now a reality

27 February 2018

SCIENTIFIC ADVANCES

The benefits of quantum effects for biological, social and technological networks

9 February 2018

SCIENTIFIC ADVANCES

A quantum leap for ultra-precise measurement and information encoding?

24 November 2017

Andris Ambainis – The mathematics of quantum computing

16 July 2014

NEWS

Last update: 11 October 2017

Permalink: https://cordis.europa.eu/article/id/122627-securing-encryption-data-against-the-threat-of-future-quantum-computers