Race against the big code breaker

Photo: Ralf Werner

Post-Quantum cryptography is the research topic of Juliane Krämer, mathematician and computer scientist at TU Darmstadt.

Quantum computers may be able to crack the encryptions common in the network in ten years – even retroactively. The Darmstadt cryptographer Dr. Juliane Krämer counters with mathematics.

Von Christian J. Meier

"Imagine yourself in the near future, and picture a website where anyone could see your WhatsApp communication of today," says Dr. Juliane Krämer. "At what point wouldn't that bother you any more? In a year? In ten years?" asks the researcher from the profile area CYSEC of the TU Darmstadt. Krämer combines the question with a warning: in just a few years' time, there could be a quantum computer that cracks the encryptions that are common in the Internet today. At the collaborative research centre CROSSING, the cryptographer is developing new methods that will defy code-breakers – a field that is known as post-quantum cryptography. She believes that, depending on the need for protection, we should already be arming ourselves against the computers of tomorrow.

Contact

Research Group Quantum and Physical attack resistant Cryptography (QPC)
Dr. Juliane Krämer
Phone: +49(0)6151/16–20662
E-mail: juliane@qpc.tu-darmstadt.de
www.informatik.tu-darmstadt.de/qpc

The threatened measures protect against eavesdroppers and generate digital signatures without which online banking or software updates would not be trustworthy. To encrypt data, the sender turns them into "mojibake", a jumble of characters that only the recipient can untangle. In order to prevent the two from having to exchange a secret key, so-called "asymmetric cryptography" are used. The recipient, perhaps a bank, makes the key available to the public. This allows the sender to easily encrypt their message to the bank. However, the public key cannot be used for decryption. For this purpose, the recipient alone has a "private key". This is achieved with a kind of mathematical hub, which can be passed in one direction without resistance (encryption by public key). However, when moved in the other direction, it is blocked. Only the owner has a key that unlocks the locking mechanism (decrypting it with the private key) and lets it pass in the blocked direction. Digital signing works in the same way, only with the inverse flow of information: the sender uses their private key to create the electronic signature. The recipient can check their authenticity with the public key.

Today's most widely used "hub" works with very large prime numbers. Multiplying two prime numbers is easy. The reverse way of breaking down the product into its prime factors, however, is so difficult that even a supercomputer would take decades to do so. Anyone can use the product as a public key for encryption. Only the recipient knows the prime factors that they can use as the private key. Every day, this so-called RSA method and related methods secure communication billions of times on the Internet. However, this could be over in one fell swoop once a high-performance quantum computer is ready. Because the digital hubs currently used are precisely not that for it. It will perform the reverse calculation at lightning speed.

Photo: Adobestock

Juliane Krämer is researching new post-quantum methods to protect against quantum computers of the future.

However, the quantum computer will not be an all-rounder. Only a few problems are known, and their resolution will accelerate radically. Researchers believe that it will not be able to solve many problems faster, if at all, than a normal computer. These include other mathematical hubs from the ones currently used in cryptography. Specialists such as Juliane Krämer develop new crypto methods from this. "Post-quantum cryptography is a very active field of research," says the mathematician and computer scientist. She herself is researching so-called "lattice-based cryptography". By "lattice", mathematicians mean a space filled with a regular arrangement of "lattice points". A construction fence resembles a lattice with two dimensions: the intersections of the wires form the lattice points. It is easy for mathematicians to span lattice with hundreds of dimensions – obviously only as a virtual entity. Now an additional point can be added anywhere between the individual lattice points. Because of the many dimensions, it can be extremely difficult to find the next lattice point. But it can also be easy. It depends on how the lattice is described mathematically. Mathematics speaks of a "good" or a "bad" basis. If a "bad basis" is used as the public key and a "good" one as the private one, then a mathematical "hub" has been created.

"Post-quantum cryptography is a very active field of research."

This and similar problems have been known for a long time. "However, which problems will prevail as highly relevant in practice and which will not has yet to be revealed," says Krämer. Development teams were still looking for a suitable balance between security and efficiency of the procedures. The researchers are playing with, for instance, different mathematical representations of lattices. Computational operations run faster with one of them, in the form of "polynomials". But the keys require a relatively large amount of storage space, which is a disadvantage for mobile applications such as mobile phones. "There is no one-size-fits-all solution for increasing efficiency," says Krämer. Creativity is required.

Research teams create many methods with various advantages and disadvantages in terms of securety and efficiency. In 2016, the American standardisation authority NIST called for a process, and around 80 proposals were received in response. After an initial evaluation, 29 methods remained. Most of them are lattice-based. NIST identified weaknesses in the individual procedures, and called on the authors to make improvements. "The methods are public," explains Krämer. Industry colleagues find security gaps that the originators then plug. In the meantime, NIST has further restricted the field of applicants. Juliane Krämer is also working on test methods to ensure that new post-quantum methods actually do protect against quantum computers. However, there can never be absolute certainty, as uncrackability is always based on assumptions even with the procedures currently in use.

Until the standards for post-quantum cryptography have been established, there will always be a kind of encryption gap, warns Krämer. While digital signatures only need to be safe for the moment, encrypted data should often remain so permanently. In a few years' time, today's ciphered data could be cracked by a quantum computer. Anyone who wants to remain on the safe side in the long term should stop using RSA and the like today, advises the cryptographer. Numerous methods are entirely ready for use.

The author is a science journalist with a doctorate in physics.

Links and publications:

Collaborative research centre Crossing at the TU Darmstadt:
www.crossing.tu-darmstadt.de/crc_1119/index.en.jsp

Profile area Cybersecurity (CYSEC) at the TU Darmstadt:
www.cysec.tu-darmstadt.de/cysec/index.de.jsp

Podcast:
https://www.hessen-schafft-wissen.de/podcast/Juliane-Kraemer

Current publication: Krämer, Struck (2020): Encryption Schemes using Random Oracles: from Classical to Post-Quantum Security. PQCrypto, 2020, Paris, France