idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität München
Julia Rinner

08.09.2023
http://idw-online.de/de/news820295

Forschungsergebnisse, Forschungsprojekte
Elektrotechnik, Informationstechnik, Mathematik, Physik / Astronomie
überregional

Quantum-safe data encryption

Due to the special way they function, quantum computers will be capable of breaking current encryption methods. A competition initiated by the US federal agency NIST aims to change this. It is seeking algorithms that will successfully resist cyber attacks from quantum computers. However, it has become evident that it will be far from simple to develop suitable cryptographic schemes. Researchers at the Technical University of Munich (TUM) have submitted two proposals to the NIST competition. They feel optimistic about their results.

We happily surf the internet, disclose our credit card details to online retailers and use online banking without a second thought. We assume that our data are transmitted in encrypted form and are therefore safe.

At present, data encryption methods are based on the idea that the factorization of large numbers is a difficult task. But that will change when quantum computers are powerful enough to solve mathematical problems of this kind.

Competition for new encryption technology

The National Institute of Standards and Technology (NIST) in the USA announced a competition in 2016, calling on developers to submit proposals for new, quantum-resistant encryption standards. The proposed algorithms are expected to resist cyber attacks launched from quantum computers. The NIST has made them publicly accessible to be attacked in order to test their security levels. NIST standards are generally adopted by companies and online services because they are regarded as highly secure.

Of the 69 first-round submissions, 26 made it to the second round and seven reached the final. Shortly before the NIST planned to announce winners, however, four of the finalists came under heavy attack. One of the algorithms actually had to be withdrawn after being defeated within two days by a standard laptop. The vulnerabilities of the remaining candidates were adapted sufficiently for them to remain in the competition.

Despite the many submissions, very few algorithms made it through the knock-out rounds. This shows the importance of standardizing processes that are based on different mathematical problems. This will make it possible to substitute encryption methods if vulnerabilities are identified later.

In the spring of this year the NIST called for submissions of further algorithms. Antonia Wachter-Zeh, a Professor of Coding and Cryptography at TUM, has worked with her team and another research group at TUM and researchers from Universita Politecnica delle Marche in Italy to develop two algorithms based on digital signature schemes. Digital signatures are like an electronic “fingerprint” that ensures that data originate with the expected sender and have not been changed en route.

“There is an urgent need to explore new encryption procedures if we still want our data to be secure a few years from now. We also want to make sure that people cannot decrypt the information that we are sending today,” says Antonia Wachter-Zeh.

Built-in errors ensure secure encryption

The algorithms submitted by Prof. Wachter-Zeh are based on error-correcting codes. These apply the underlying principle that errors constantly occur in the transmission and storage of data and in mobile communication networks. In binary systems, for example, a 0 might be flipped to a 1 when transmitting a string. In error-correcting codes, redundant information is inserted before transmission to allow correction in case of transmission errors. This makes it possible to compensate for a certain number of errors in the data.

Prof. Wachter-Zeh uses the principle of error-correcting codes to encrypt data by deliberately inserting errors before transmission. These are later corrected during decoding. In this way the researcher ensures that the information is protected against unauthorized access but can still be correctly encrypted and stored.

For the NIST competition the research group decided to submit one system based on error-correcting codes in the Lee metric and another that uses restrictive errors in the Hamming metric. The classical Hamming distance indicates the number of positions in which the source code differs from the encrypted code. By contrast, the restrictive Hamming distance allows errors to be assumed only for specific values. It is possible for a significantly greater number of places to be incorrect. The Lee metric also assigns a weighting to the variation in these places.

“The CROSS signature procedure, which uses restrictive errors, is highly competitive and has good chances to be considered as a new encryption standard. In our second algorithm, FuLeeca, based on the Lee metric, vulnerabilities have already been identified. The principle is generally promising, however, although quite new. Consequently, there is still a lot of research to be done,” says Antonia Wachter-Zeh.

Further information

In cryptography two different data encryption methods are used: symmetric and asymmetric encryption. Symmetric encryption schemes are assumed to be adaptable with relative ease and are therefore regarded as quantum-safe. For this reason, the NIST competition is focusing on asymmetric cryptography systems and in particular on digital signatures and key encapsulation mechanisms.

Prof. Wachter-Zeh is currently involved in the German-French DFG-ANR project CROWD on new code classes in cryptography, in which she is the initiator and German coordinator, and the EiC Pathfinder Challenges project DiDaX on DNA-based digital data storage.

Her research has been funded, among other sources, under the DFG Emmy Noether Program and the ongoing ERC project inCREASE (“Coding for Security and DNA Storage”) and the BMBF project 6G-life. Along with many other awards and honors, she received the Heinz Maier-Leibnitz Prize in 2018 and the NVMW Memorable Paper Award in 2019.

wissenschaftliche Ansprechpartner:

Prof. Antonia Wachter-Zeh
Professorship of Coding and Cryptography
antonia.wachter-zeh@tum.de
Phone: +49 89 289 – 23495

URL zur Pressemitteilung:
https://www.tum.de/en/news-and-events/all-news/press-releases/details/daten-quantensicher-verschluesseln