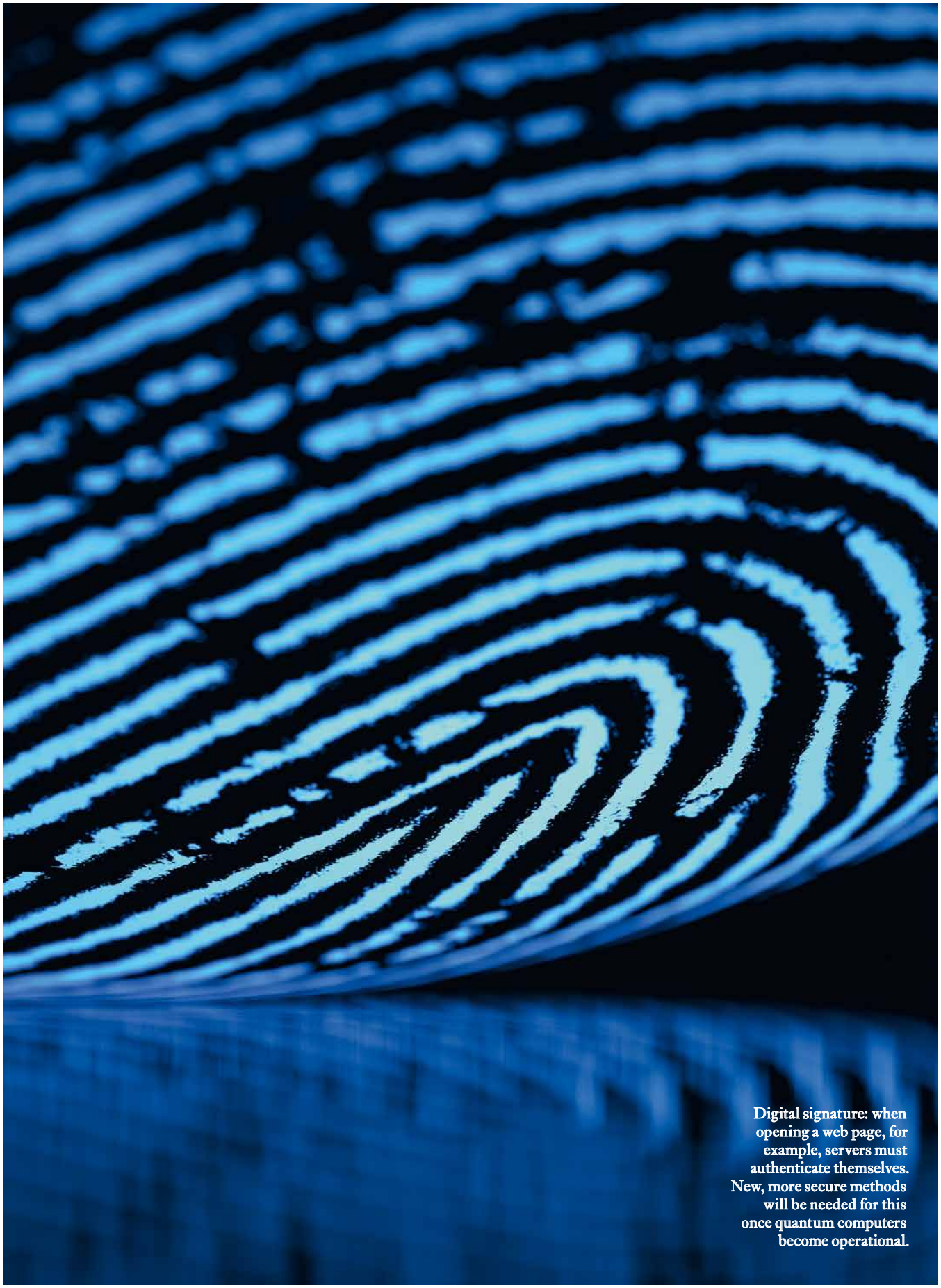


Digital signature: when opening a web page, for example, servers must authenticate themselves. New, more secure methods will be needed for this once quantum computers become operational.

PHOTO: ISTOCK

QUANTUM-PROOF

TEXT: PETER HERGERSBERG

It's a threatening scenario for online communications: the arrival of powerful quantum computers will make current encryption techniques vulnerable overnight. Peter Schwabe, Research Group Leader at the Max Planck Institute for Security and Privacy, is therefore developing methods of post-quantum cryptography with international partners. Four such processes are now being standardized by the National Institute for Standards and Technology in the USA – Peter Schwabe was involved in the design of three of them.

For many, the quantum computer is hugely promising – not least for modern intelligence services. Online services that rely on secure data exchange, on the other hand, also see it as a threat. No one can predict when the first powerful computers of this type will start performing their work. What is clear, however, is that "the cryptographic protocols that protect the vast majority of data traffic today will be worthless as soon as the first quantum computers are available," says Peter Schwabe, Research Group Leader at the Max Planck Institute for Security and Privacy and professor at Radboud University in Nijmegen. "This is because they can efficiently solve the two mathematical problems on which current cryptographic methods are based." For example, they can parse a large number into two prime factors in the blink of an eye. Since conventional computers would need tens of thousands of years to do this and would also consume as much energy as the sun sends to the earth in this period, prime number factorization forms the core of one encryption method that is currently in widespread use.

In order to protect data traffic against attacks using quantum computers in the future, 69 teams submitted proposals for new cryptographic methods to the National Institute for Standards and Technology (NIST); they refer to this as post-quantum cryptography. After several rounds, NIST decided to standardize four of these procedures. "They constitute better protection for digital communication – precisely because quantum computers would render previous encryption methods and signature systems obsolete," says Eike Kiltz, who researches and teaches as a professor at Ruhr University in Bochum and works with Peter Schwabe and numerous partners on such new encryption techniques.

Three of the selected methods are used for authentication, including the Sphincs+ and Crystals-Dilithium methods, which Peter Schwabe helped to develop: "During authentication, a digital signature ensures that a server, for example, is actually what it claims to be." Schwabe also coordinated the international team that designed Crystals-Kyber and made it application-ready. This method is used to securely transmit keys for further communication.

The example of key exchange is a good way to explain some aspects of cryptography. In many applications, be it a messenger service or an online shop, communication is protected using a combination of asymmetric and symmetric cryptography. This means that the key used to encrypt a message is

→

public. Only the code required to decrypt the message is secret. Unlike symmetric cryptography techniques, which use a single secret key, the public keys used in asymmetric techniques can be exchanged over non-secure channels. After all, what channel is really secure? It is not for nothing that we receive a PIN number from the bank as an elaborately packaged scratch code. Sending a secret letter of this kind to every e-mail contact is likely to spoil the joy of online communication rather quickly. Asymmetric methods of cryptography include the widely used RSA method, which is ultimately based on prime number factorization, but can be leveraged by quantum computing.

Simple, efficient, and secure procedures

Considering all this, post-quantum cryptography techniques, such as Crystals-Kyber, work with mathematical problems that are, based on knowledge available today, almost as challenging for quantum computers as they are for conventional computers. The actual calculations in Crystals-Kyber are very simple – just multiplication and addition. A value, more precisely a polynomial, is multiplied by another value, which is the secret key. Another value is added to the product, which complicates the whole thing. The secret key and the added value – which are also polynomials – are small. Nevertheless, this setup makes it arbitrarily difficult to determine the secret key, even if you know the result of this operation and the output polynomial, which together serve as the public key.

"Some of the proposals for post-quantum cryptography are based on this principle," Peter Schwabe explains. However, it is not just the mathematical problem behind a method that matters, but also how the calculation rule is formulated in software code. And that is precisely what Peter Schwabe is particularly good at. "In the implementation, we have to balance numerous factors, because a win for one always comes at the expense of another. My contribution was to make a lot of decisions in a way that ultimately made the process simple, efficient and, above all, secure." Those were precisely the criteria NIST used to make its selection. Now it will write standards for the selected procedures. This means it will provide explanations of the cryptographic techniques and formulate instructions so that online services, for example, can incorporate them into their applications comparatively easily – and, above all, without tearing holes in their existing security precautions.

Nevertheless, there are also reservations about NIST's work. Some critics fear the agency could standardize encryption methods at the behest of the NSA, leaving backdoors open to U.S. intelligence. "We can be pretty sure that this happened in one case in the past," Peter Schwabe tells us. However, he says that the government agency had presumably done this unknowingly and has since admitted that it was a significant mistake. "In contrast to the methods now up for selection, the backdoor method didn't come from academia. These days, the cryptography community is also more involved in the selection process." This means that it is no longer just NIST who looks for ways to exploit possible security vulnerabilities, but also the vast majority of the world's cryptography community. "NIST has already shaped the selection of new cryptography standards twice, as it is doing with post-quantum cryptography," says Peter Schwabe. "The processes that came out of that have proven to be very secure – and they are used all over the world today."

It is therefore quite possible that NIST will set standards with its decision, at least for the USA and Europe. However, the German Federal Office for Information Security (BSI) published a Technical Guideline in 2020, in which it recommends two other methods for key exchange in the age of quantum computing. "We consider these methods to be especially secure," says Stephan Ehlen, a mathematician at the BSI who studies quantumproof encryption. These are based on a mathematical problem related to the principle of Crystals-Kyber. However, the procedures are not as efficient as those that NIST is now standardizing, Ehlen says. For NIST, however, efficiency is an important criterion for ensuring that the methods are also well suited for widespread application in everyday internet use. "It is entirely possible that when we update the Guidelines, we will bring in other procedures, including those that have now been selected by NIST," Ehlen said. If nothing else, this would facilitate secure communications between federal agencies that follow the BSI recommendations and, for example, companies that use the NIST standard. The BSI has yet to select procedures for digital signatures. "This hasn't been

SUMMARY

The arrival of powerful quantum computers will make current encryption techniques vulnerable overnight.

The National Institute for Standards and Technology will now standardize four of 69 proposed post-quantum cryptography methods.

Peter Schwabe played a key role in the development of three of the selected methods, two of which are used for authentication and another for the secure exchange of cryptographic keys.

so urgent because the problem of encrypted communications potentially being intercepted and stored now and decrypted later doesn't exist here."

The computer scientist predicts that standardization could be completed by the end of 2023. But major companies such as Google, Amazon, and the IT security provider Cloudflare, are already experimenting with post-quantum cryptography methods – alongside today's standard methods, which are vulnerable to attacks using quantum computers. In addition, car manufacturers are already looking at post-quantum cryptography to ensure that they can still securely update the software of the vehicles they build today, even in 15 or 20 years' time. "We assume that an increasing number of services will use the new processes after standardization," explains Peter Schwabe. Hopefully, the encryption methods that the Bochum researchers helped to develop will secure visits to websites, e-mail traffic, or banking transactions even before the first powerful quantum computer is available.

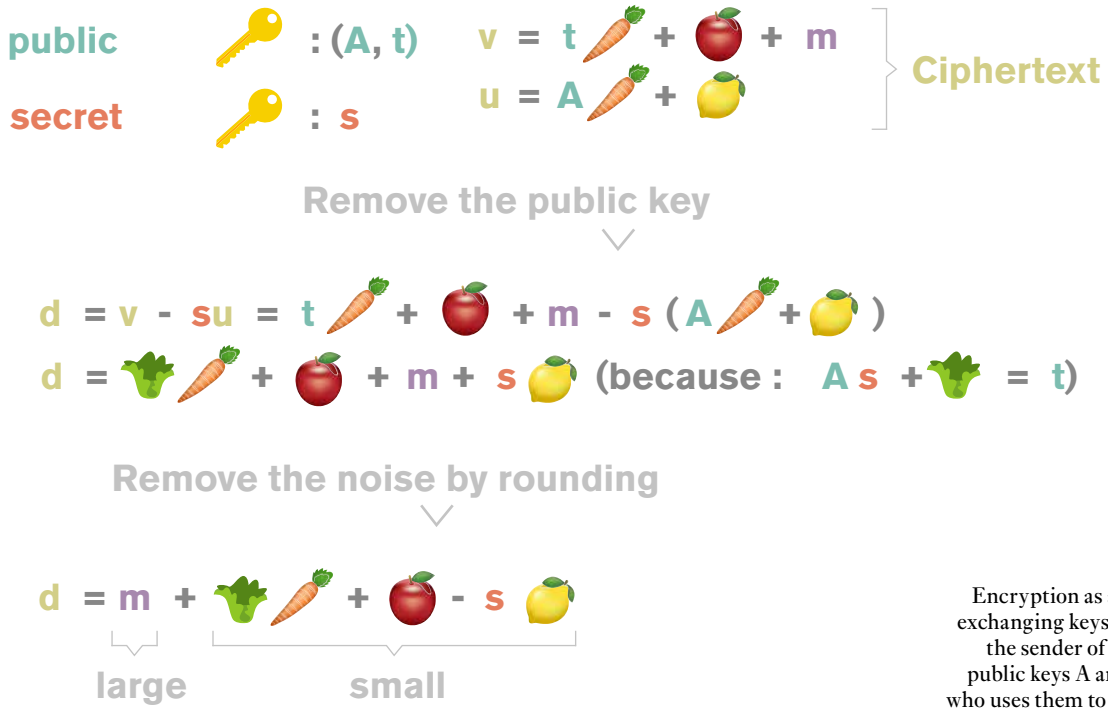
GLOSSARY

AUTHENTICATION ensures in online communication that a computer or server is what it claims to be, such as the server of an e-mail service.

POST-QUANTUM CRYPTOGRAPHY refers to encryption and authentication methods that even quantum computers cannot crack.

KEY EXCHANGE is a cryptographic technique that allows two parties to exchange a shared secret key over an insecure channel.

NIST STANDARDIZATION includes explanations of the encryption methods and guidance on how to integrate the methods securely and as easily as possible into programs for digital services.



GRAPHIC: GCO BASED ON A TEMPLATE BY KYBER AND POST-QUANTUM CRYPTO – HOW DOES IT WORK? RUBEN GONZALEZ, KRIJN REIJNDERS

Encryption as a salad of letters: when exchanging keys using Crystals-Kyber, the sender of a message receives the public keys A and t from the recipient, who uses them to encrypt their message m. The recipient can only decrypt the message with the secret key s. The icons represent small values that easily distort the crucial components and make decryption complicated for attackers. In the last step, they are removed by rounding to the zero or one of a bit.