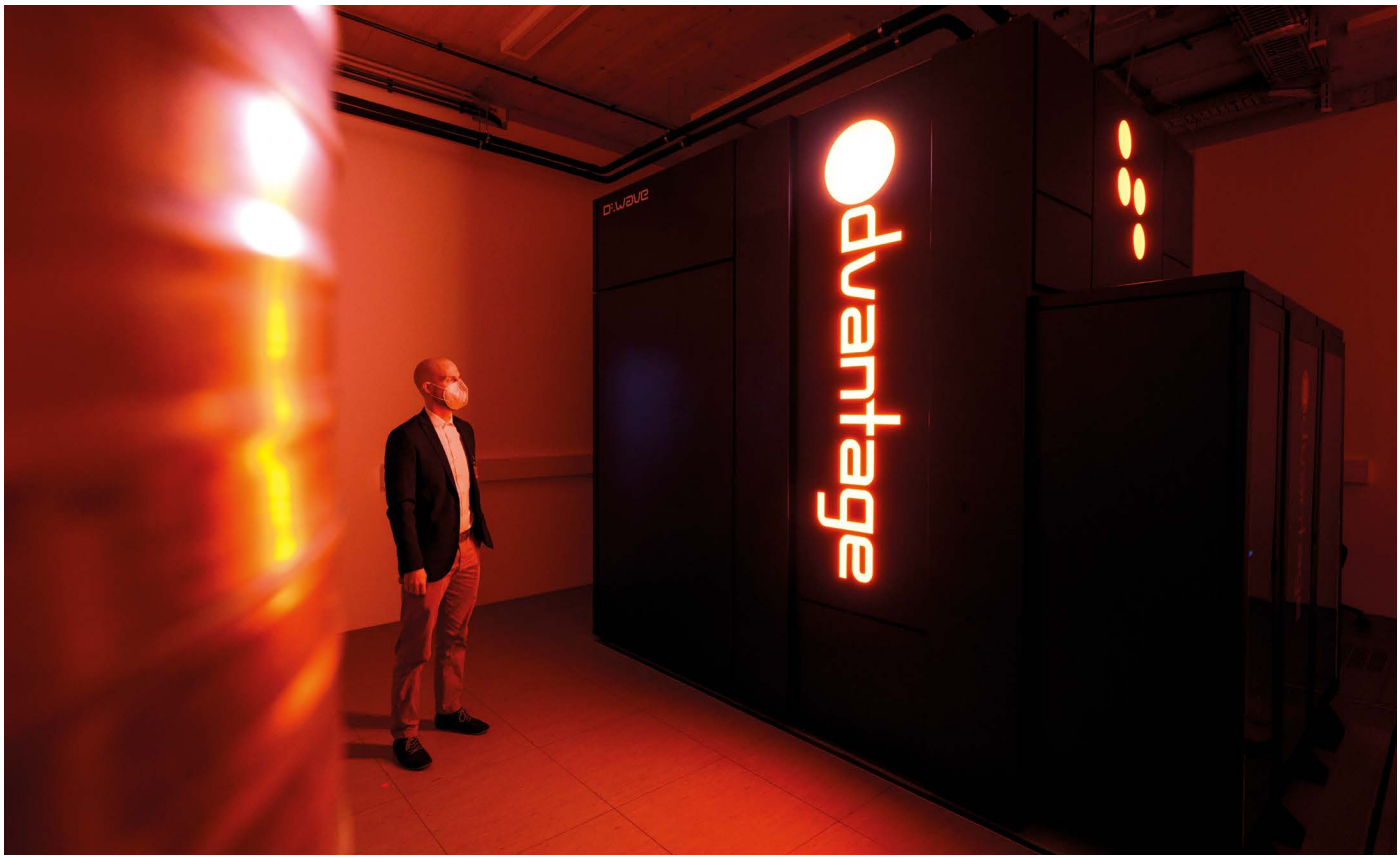
spotlight




LUKAS SCHULZE/GETTY

**The D-wave Systems Advantage quantum computer at the Jülich Research Centre in Germany.**

# KEEPING SECRETS IN A QUANTUM WORLD

## Cryptographers are preparing for computers that will break their ciphers. **By Neil Savage**

In July 2022, a pair of mathematicians in Belgium startled the cybersecurity world. They took a data-encryption scheme that had been designed to withstand attacks from quantum computers so sophisticated they don't yet exist, and broke it in 10 minutes using a nine-year-old, non-quantum PC.

"I think I was more surprised than most," says Thomas Decru, a mathematical cryptographer, who worked on the attack while carrying out postdoctoral research at the Catholic University of Leuven (KU Leuven) in Belgium. He and his PhD supervisor Wouter Castryck had sketched out the mathematics of the approach on a whiteboard, but Decru hadn't been sure it would work — until the pair actually ran it on a PC. "It took a while for me to let it sink in: 'Okay, it's broken.'"

The encryption scheme, dubbed SIKE, was designed for the ambitious purpose of keeping secrets secret. It was one of four algorithms chosen in 2022 for potential adoption by the US National Institute of Standards and Technology (NIST) in its Post-Quantum Cryptography standardization process. The aim is to find algorithms that can safeguard private information from the looming threat of quantum computers.

The world's digital information relies on encryption to keep it secure. Hard drives containing medical data are encrypted, as are the secrets held by national militaries and intelligence agencies. Online credit-card payments, digital signatures, readings from smart meters, the computers in driverless cars and the chips in passports all depend on algorithms, developed in the 1970s, that turn easy-to-read data into encrypted ciphers accessible only to those with a mathematical 'key' to unlock them. Those algorithms, in turn, depend on mathematical functions that are straightforward to use to create keys, but difficult to run in reverse to reveal them: the mathematical equivalent of frying an egg.

If practical quantum computers arrive, however, these hard-to-solve problems will suddenly become child's play. RSA, an encryption scheme that allows systems to share keys, could take a classical computer most of the lifetime of the Universe to reverse-engineer. A quantum computer, researchers estimate, could do the same job in 8 hours. The Diffie–Hellman key exchange, another widely used cryptographic method, named after its two inventors, could also be easily reversed by a quantum machine. A different type of scheme, the Advanced Encryption Standard, is not considered to be under serious threat by computational advances, but it's often used in conjunction with the other methods and can't replace their secret-keeping abilities.

Whereas classical computers work on ordinary digital bits of ones and zeros, quantum

# spotlight

KEVIN FAINGNAERT

**Thomas Decru, one of the two mathematicians who won the SIKE Cryptographic Challenge.**

computers use quantum bits, or qubits. These units take advantage of a quantum-mechanical property called superposition, which allows a qubit to be, for example, 70% '1' (on) and 30% '0' (off) at the same time. The ability to be in many states of partially on and partially off at once lets a quantum computer perform complicated mathematical operations much faster than even the most sophisticated classical computer could. This characteristic brings eon-spanning calculations within easy reach.

Existing quantum computers contain a handful of qubits – a few hundred at most – and have limited capabilities. The global technology firm IBM plans to release a chip with 1,121 qubits sometime this year, and says it will have a computer with more than 4,000 qubits by 2025. Scientists from Google and the Swedish National Communications Security Authority estimated in 2021 that 20 million qubits would be necessary to crack an RSA key of 2,048 bits, a commonly used key length. "The big question is, of course, whether all of the efforts to make quantum computing practical will have any cryptanalytic benefits," says Ronald Rivest, a computer scientist at the Massachusetts Institute of Technology in Cambridge – and the R in RSA, which he developed with fellow computer scientists Adi Shamir at the Weizmann Institute of Science in Rehovot, Israel, and Leonard Adleman at the University of Southern California in Los Angeles. "It still is very much an open question."

But even if practical quantum computers aren't built for another 20 years, the problem is urgent today, researchers say. "Your data could already be lost to a future quantum computer, even though one hasn't been built," explains Dustin Moody, a mathematician in NIST's Computer Security Division, who leads the Post-Quantum Cryptography project. Spy agencies or cybercriminals could collect encrypted data now and simply wait for the technology to catch up. Many researchers think that countries such as China and the United States are doing just that.

In case practical quantum computers do arrive, cryptographers and standards bodies around the world are working to come up with a set of encryption techniques that will be as hard for a quantum computer to unravel as existing schemes are for classical computers. To do that, many researchers are putting the latest algorithms to the test.

## Broken keys

Breaking SIKE earned Decru and Castryck a US$50,000 reward from Microsoft for winning the SIKE Cryptographic Challenge. Once the pair had announced their findings, other groups quickly found ways to unscramble the codes even faster. This wasn't the first futuristic algorithm of NIST's to fall. Another candidate, called Rainbow and based on a different mathematical approach, had been broken five months earlier – in a single weekend – by Ward Beullens, a postdoctoral researcher at IBM Research Zurich in Rüschlikon, Switzerland.

Testing such potentially quantum-resistant algorithms to their breaking point is the aim of a multi-year competition that NIST has been running to develop post-quantum cryptography schemes. "The strongest will survive," says Moody. "Sometimes they look promising, but over the years, they wither out and we say, 'Okay, we've gone as far as we can in that direction. We have to have some new ideas.'"

Of 69 candidate algorithms chosen in late 2017, between 25 and 30 have either been broken entirely or suffered some significant attack, Moody says. In late August this year, NIST published draft standards for three of the remaining algorithms and invited public comment. The agency plans to finalize the standards sometime in 2024.

Of these three algorithms, one – CRYSTALS-Kyber – is designed for general-purpose encryption and the exchange of public keys that protect shared data. The other two, CRYSTALS-Dilithium and SPHINCS+, are used to secure digital signatures, which ensure that a person providing a document is who they say they are. A draft standard for another algorithm for digital signatures, Falcon, is also set to be published by NIST in 2024, and 40 more digital-signature candidates were collected in July, after the agency sent out a call for a new round of submissions. "They are sort of sending the message that they are not happy with the three that they have," says Tanja Lange, a cryptographer who heads the coding theory and cryptology group at Eindhoven University of Technology in the Netherlands, and who contributed to the development of SPHINCS+.

## Tapping extra information

Any cryptography system has to be more than just a hard-to-solve mathematical problem. It also has to allow some way of sharing information about the problem with the person who needs to decode it. And that introduces vulnerability. "There's this game that always has to be played in cryptography," Castryck explains. You have to have a hard problem on which to build a crypto system, "but there's always extra information that is passed along just to make the scheme work".

**"When you want to do Internet communication, both ends need to speak the same cryptography."**

The SIKE system was based on an isogeny, which is a map showing how points on an elliptic curve correspond to points on another such curve. Unlocking SIKE requires finding the right map between 2 random curves out of at least $2^{434}$ such curves – a number so huge there's no word for it in English, and something that should be almost impossible without a key, even for quantum computers. To share a key with the recipient of an encoded message, each sender has to provide information about two points along one of the curves. Castryck and

Decru were able to use that extra information about the points to reconstruct the map, and could therefore break the code without actually solving the hard mathematical problem.

Isogeny as the basis for a cryptographic scheme is not dead, but it's on shaky ground, says Decru, now at the Université Libre de Bruxelles in Belgium. The pair's attack on SIKE does not affect NIST's other proposed standards, which use different mathematical approaches. Two are based on structured lattices, a kind of repeating grid. The hard mathematical problem is to determine how parts of the grid relate to each other. SPHINCS+ is based on hash functions, which take a string of numbers and convert it into a shorter string that forms a recognizable fingerprint of the original. Hash functions are not reversible, so they're easier to create than other approaches are, but because of their one-way nature, they can only be used for signature verification, not for trading cryptographic keys.

Putting cryptographic algorithms to use in a way that balances the competing demands of security and efficiency is another challenge when it comes to making data safe in a quantum world, Castryck says. Longer keys are more secure, because there are more possible solutions to a problem, thus increasing the difficulty of finding the right one. But that also increases the time and computing bandwidth required to generate and transmit the key. "Industry is not asking for a very secure crypto system that takes one hour for a single key exchange," Castryck says.


PABLO MARTINEZ MONSIVAIS/ASSOCIATED PRESS/ALAMY

**Officials are worried about the threats quantum computing poses to national security.**

## Attacks from the side

Peter Schwabe, a cryptographic engineer at the Max Planck Institute for Security and Privacy in Bochum, Germany, is investigating how to protect cryptographic schemes from side-channel attacks. In an attack of this kind, an adversary gathers information from a computer that is not part of the key itself but could provide hints to it. In classical computing, for instance, sending messages to a server and measuring the time it takes to get a response could reveal whether a given bit is a '1' or a '0', or the power usage might vary according to the structure of the cryptographic key. The attacker can use these clues to piece the key together. Or, if the attacker can place some spyware on a server, they might be able to learn what this server is doing by measuring its demand on resources such as memory.

In August, the multinational tech giant Intel released a firmware patch for several brands of chip it has sold since 2015, after Daniel Moghimi, a security researcher at Google in San Diego, California, discovered what he named the Downfall vulnerability. It exploits the way in which the chips speed up the process of gathering data scattered through their memory. An attacker with access to the chip sends requests to encrypt random data, then collects some low-level information that leaks from the process. The attacker can analyse that information and look for patterns, which can eventually be used to piece together the encryption key the system is using.

Although the specifics of the attack will vary with the particular encryption scheme, there is nothing in post-quantum cryptography that inherently rules out such attacks. "One goal of this project is to figure out how we can systematically protect these new crypto systems against these kinds of attacks," Schwabe says.

NIST isn't the only group that is working on cryptographic standards. The German Federal Office for Information Security also provides recommendations about which systems to use. These include two standards that didn't make NIST's final cut. One is FrodoKEM, a key-encapsulation scheme based on lattices. The other is Classic McEliece, which uses error-correction codes that are hard to reverse. Both are considered to be more secure than the NIST proposals, but they involve longer keys, and are thus slower to use.

Other standards organizations are likely to weigh in as well. For example, the Internet Engineering Task Force does not recommend particular cryptography standards, but will have a say in the protocols that incorporate them. Between 2018 and 2019, the Chinese Association for Cryptologic Research held its own competition for new algorithms. The submissions involved the same families of mathematical problems as those in the NIST proposals, and the chosen winner was based on structured lattices.

In the end, there will have to be a small set of internationally agreed standards. "The simple reason is that when you want to do Internet communication, both ends need to speak the same cryptography," Schwabe says. And large international companies will also have a role. For instance, Google announced in August that it was incorporating Kyber into its Chrome browser. "If Google implements key agreement with Kyber, then everybody who wants to speak to Google needs to speak Kyber, no matter where they're sitting in the world," Schwabe says.

It will take time to implement the NIST standards and to spread them, or similar approaches, to computer systems around the world. Meanwhile, cryptographers will keep trying to develop algorithms, and attempting to break those that already exist. But the threat that data could be collected now and decrypted at a later stage means that the issue is urgent, and the sooner the world adopts post-quantum cryptography, the better, Decru says. "Whether the quantum computer exists in 20, 30 or 40 years, we don't know," he says. "But I don't think there's time to waste on that front, really."

**Neil Savage** is a science writer based in Lowell, Massachusetts.

**Correction**

This Spotlight article described SIKE as a finalist in NIST's Post-Quantum Cryptography standardization process. It was, in fact, chosen for further consideration.

Corrected 16 November 2023