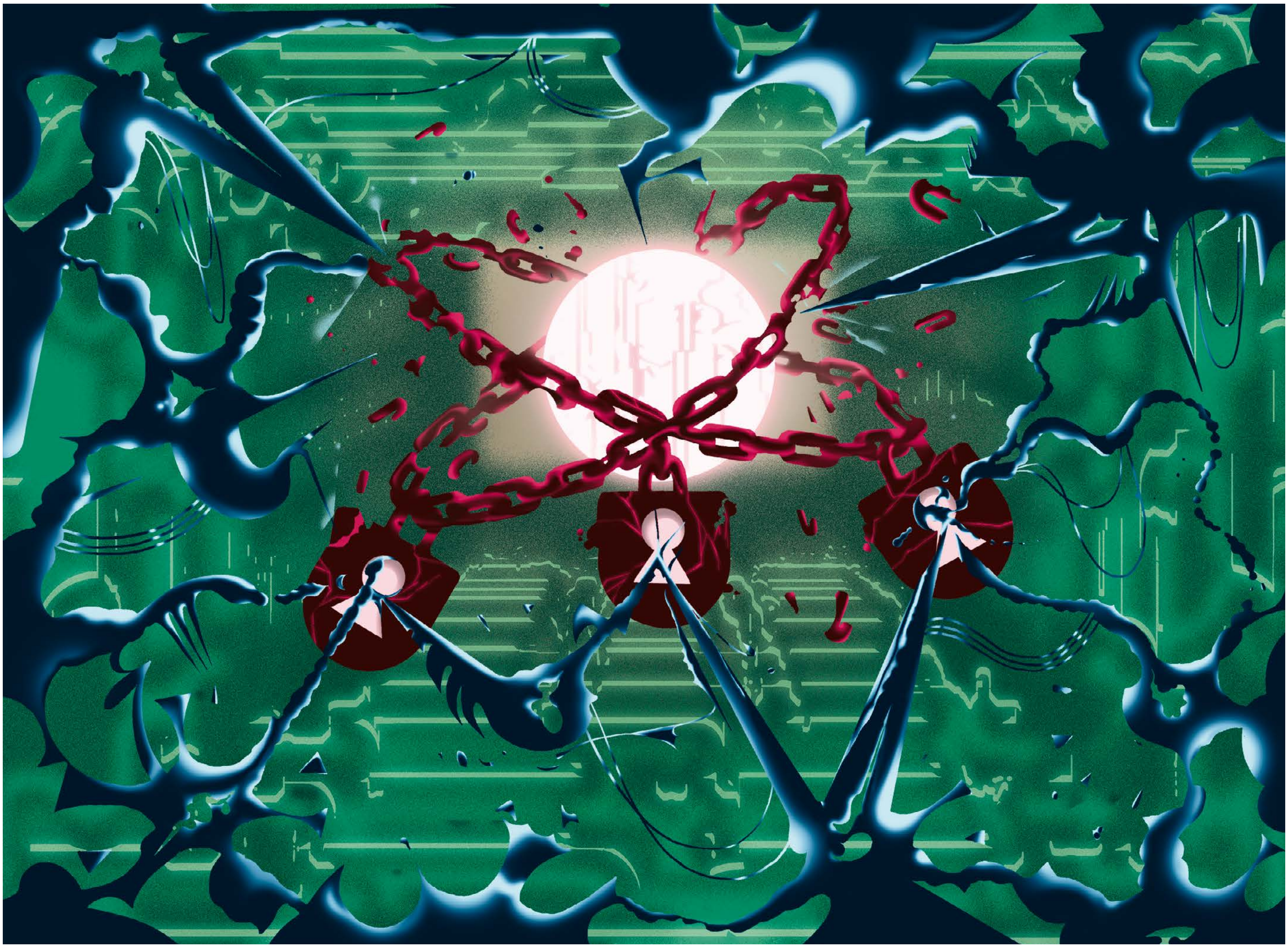


ILLUSTRATION BY DALBERT B. VILARINO

PREPARING FOR Q-DAY

The quantum-computer revolution could give hackers superpowers. New encryption algorithms will keep them at bay. **By Davide Castelvecchi**

In cybersecurity circles, they call it Q-day: the day when quantum computers will break the Internet.

Almost everything we do online is made possible by the quiet, relentless hum of cryptographic algorithms. These are the systems that scramble data to protect our privacy, establish our identity and secure our payments. And they work well: even with the best supercomputers available today, breaking the codes that the online world currently runs on would be an almost hopeless task.

But machines that will exploit the quirks of quantum physics threaten that entire deal. If they reach their full scale, quantum computers would crack current encryption algorithms exponentially faster than even the best non-quantum machines can. "A real quantum computer would be extremely dangerous," says Eric Rescorla, chief technology officer of the Firefox browser team at Mozilla in San Francisco, California.

As in a cheesy time-travel trope, the machines that don't yet exist endanger not only our future communications, but also our current and past ones. Data thieves who eavesdrop on Internet traffic could already be accumulating encrypted data, which they could unlock once quantum computers become available, potentially viewing everything from our medical histories to our old banking records. "Let's say that a quantum computer is deployed in 2024," says Rescorla. "Everything you've done on the Internet before 2024 will be open for discussion."

Even the most bullish proponents of

quantum computing say we'll have to wait a while until the machines are powerful enough to crack encryption keys, and many doubt it will happen this decade – if at all.

But the risk is real enough that the Internet is being readied for a makeover, to limit the damage if Q-day happens. That means switching to stronger cryptographic systems, or cryptosystems. Fortunately, decades of research in theoretical computer science has turned up plenty of candidates. These post-quantum algorithms seem impervious to attack: even using mathematical approaches that take quantum computing into account, programmers have not yet found ways to defeat them in a reasonable time.

Which of these algorithms will become standard could depend in large part on a decision soon to be announced by the US National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland.

In 2015, the US National Security Agency (NSA) announced that it considered current cryptosystems vulnerable, and advised US businesses and the government to replace them. The following year, NIST invited computer scientists globally to submit candidate post-quantum algorithms to a process in which the agency would test their quality, with the help of the entire crypto community. It has since winnowed down its list from 65 to 15. In the next couple of months, it will select a few winners, and then publish official versions of those algorithms. Similar organizations in other countries, from France to China, will make their own announcements.

But that will be only the beginning of a long process of updating the world's cryptosystems – a change that will affect every aspect of our lives online, although the hope is that it will be invisible to the average Internet user. Experience shows that it could be a bumpy road: early tests by firms such as Google haven't all run smoothly.

"I think it's something we know how to do; it's just not clear that we'll do it in time," Peter Shor, a mathematician at the Massachusetts Institute of Technology in Cambridge whose work showed the vulnerabilities of present-day encryption, told *Nature* in 2020.

Even if Q-day never happens, the possibility of code-breaking quantum machines has already changed computer science – and, in particular, the ancient art of cryptography. "Most people I know think in terms of quantum-resistant crypto," says computer scientist Shafi Goldwasser, director of the Simons Institute for the Theory of Computing at the University of California, Berkeley.

Birth of public-key cryptography

Armies and spies have always been able to send messages securely even when a channel – be it a messenger pigeon or a radio link – is susceptible to eavesdropping, as long as their messages were encrypted. However, until the 1970s, this required the two parties to agree on a shared secret cipher in advance.

Then, in 1976, three US computer scientists, Whitfield Diffie, Martin Hellman and Ralph Merkle, came up with the revolutionary concept of public-key cryptography, which allows two people to exchange information securely even if they had no previous agreement. The idea rests on a mathematical trick that uses two numbers: one, the public key, is used to encrypt a message, and it is different from the second, the private key, used to decrypt it. Someone who wants to receive confidential messages can announce their public key to the world, say, by printing it in a newspaper. Anyone can use the public key to scramble their message and share it openly. Only the receiver knows the private key, enabling them to unscramble the information and read it.

> **"IT'S SOMETHING WE KNOW HOW TO DO; IT'S JUST NOT CLEAR THAT WE'LL DO IT IN TIME."**

In practice, public keys are not typically used to encrypt the data, but to securely share a conventional, symmetric key – one that both parties can use to send confidential data in either direction. (Symmetric-key systems can also be weakened by existing quantum algorithms, but not in a catastrophic way.)

For the first two decades of the Internet age from the mid-1990s, the most commonly used public-key-exchange algorithm was RSA, named after its inventors, Ron Rivest, Adi Shamir and Leonard Adleman.

RSA is based on prime numbers – whole numbers such as 17 or 53 that are not evenly divisible by any numbers except themselves and 1. The public key is the product of at least two prime numbers. Only one party knows the factors, which constitute the private key. Privacy is protected by the fact that, although multiplying two large numbers is straightforward, finding the unknown prime factors of a very large number is extremely hard.

More recently, the Internet has been transitioning away from RSA, which is vulnerable even to classical – as opposed to quantum – attacks. In 2018, the Internet Engineering Task Force (IETF), a consensus-based virtual organization that steers the adoption of security standards on a global scale, endorsed another public-key system to replace it. That system is called elliptic-curve cryptography, because its mathematics grew out of a branch of nineteenth-century geometry that studies objects called elliptic curves.

Elliptic-curve cryptography is based on calculating the *n*th power of an integer (which is associated with a point on the curve). Only one party knows the number *n*, which is the private key. Calculating the exponential of a number is easy, but given the result, it is extremely hard to find what *n* was. This technique is faster and more secure than RSA.

All sorts of devices, from mobile phones to cars, use public-key encryption to connect to the Internet. The technology has also spread beyond cyberspace: for example, the radio-frequency chips in everything from credit cards to security passes typically use elliptic-curve algorithms.

Breaking RSA

Just as the number of Internet users worldwide – and the use of public-key cryptosystems such as RSA – was beginning to grow exponentially, Shor, then at AT&T Bell Laboratories in Murray Hill, New Jersey, laid the groundwork for those algorithms' demise. He showed in 1994 how a quantum computer should be able to factor large numbers into primes exponentially faster than a classical computer can (P. W. Shor *Proc. 35th Annu. Symp. Found. Comput. Sci.* 124–134; 1994). One of the steps in Shor's quantum algorithm can efficiently break an elliptic-curve key, too.

Shor's was not the first quantum algorithm, but it was the first to show that quantum computers could tackle practical problems. At the time, it was largely a theoretical exercise, because quantum computers were still dreams for physicists. But later that decade, researchers at IBM performed the first proofs of principle of quantum calculations, by manipulating molecules in a nuclear magnetic resonance machine. By 2001, they had demonstrated that they could run Shor's algorithm – but only to calculate that the prime factors of 15 are 3 and 5. Quantum-computing technology has made enormous progress since then, but running Shor's algorithm on a large integer is still a long way off.

Still, after Shor's breakthrough, the crypto-research world began to pay attention to the possibility of a Q-day. Researchers had already been studying alternative public-key algorithms, and the news attracted lots of talent to the field, says Goldwasser.

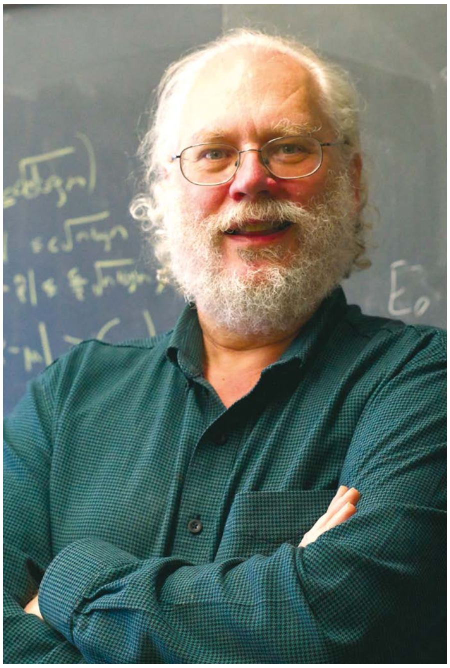
Lattice-based systems

The majority of the algorithms that made it to NIST's final roster rely, directly or indirectly, on a branch of cryptography that was developed in the 1990s from the mathematics of lattices. It uses sets of points located at the crossings of a lattice of straight lines that extend throughout space. These points can be added to each other using the algebra of vectors; some can be broken down into sums of smaller vectors. If the lattice has many dimensions – say, 500 – it is very time-consuming to calculate the smallest such vectors. This is similar to the situation with prime numbers: the person who knows the short vectors can use them as a private key, but solving the problem is extremely hard for everyone else.

Since the 1990s, researchers have developed a plethora of public-key encryption algorithms that either use lattices directly, or are somehow related to them. One of the earliest types, developed in 1996, is called NTRU. Its keys consist of polynomials with integer coefficients, but it is considered secure because of its theoretical similarity to lattice problems. To show that a cryptosystem is trustworthy, researchers often prove that it is at least as hard to crack as a lattice problem.

A popular approach to lattice-based cryptography is called learning with errors (LWE), which forms the basis for several of the NIST finalists. It was introduced in 2005 by computer scientist Oded Regev at New York University. In its simplest form, it relies on arithmetic. To create a public key, the person who wants to receive a message picks a large, secret number – the private key. They then calculate several multiples of that number and add random 'errors' to each: the resulting list of numbers is the public key. The sender adds up these whole numbers and another number that represents the message, and sends the result.

To get the message back, all the receiver has to do is divide it by the secret key and calculate the remainder. "It's really high-school level of mathematics," Regev says.



Peter Shor showed that quantum algorithms could defeat cryptographic systems.

BBVA FOUNDATION

The profound step was Regev's proof in 2009 that anyone who breaks this algorithm would also be able to break the seemingly more complex lattice problem. This means that LWE has the same security as lattices, but without having to deal with multi-dimensional vectors, Goldwasser says. "It's a great formulation, because it makes it easy to work with." Ironically, Regev discovered LWE during an unsuccessful attempt to find a quantum algorithm that would break the lattice problem. "Sometimes failure is success," he says.

Researchers have since worked on tackling a drawback of lattice-based systems. "Lattice-based cryptography suffers from huge public keys," says Yu Yu, a cryptographer at Shanghai Jiao Tong University in China. Whereas the public key of a current Internet application is the size of a tweet, lattice-based encryption typically requires keys that are as large as one megabyte or more. 'Structured lattice' systems use what are essentially algebraic tweaks to drastically reduce the public key's size, but that can leave them more open to attack. Today's best algorithms have to strike a delicate balance between size and efficiency.

Quantum candidates

In 2015, the NSA's unusually candid admission that quantum computers were a serious risk to privacy made people in policy circles pay attention to the threat of Q-day. "NSA doesn't often talk about crypto publicly, so people noticed," said NIST mathematician Dustin Moody in a talk at a cryptography conference last year.

Under Moody's lead, NIST had already been working on the contest that it announced in 2016, in which it invited computer scientists to submit candidate post-quantum algorithms for public-key cryptography, releasing them for scrutiny by the research community. At the same time, NIST called for submissions of digital-signature algorithms – techniques that enable a web server to establish its identity, for example, to prevent scammers from stealing passwords. The same mathematical techniques that enable public-key exchanges usually apply to this problem, too, and current digital-signature systems are similarly vulnerable to quantum attacks.

Teams from academic laboratories and companies, with members from four dozen countries on six continents, submitted 82 algorithms, of which 65 were accepted. True to their creators' nerd credentials, many of the algorithms' names had Star Wars, Star Trek or Lord of the Rings themes, such as FrodoKEM, CRYSTALS-DILITHIUM or New Hope.

The algorithms are being judged by both their security and their efficiency, which includes the speed of execution and compactness of the public keys. Any algorithms that NIST chooses to standardize will have to be royalty-free.

As soon as the algorithms were submitted, it was open season. Crypto researchers delight in breaking each other's algorithms, and after NIST's submissions were made public, several of the systems were quickly broken. "I think people had a lot of fun looking at those algorithms," says Moody.

Although NIST is a US government agency, the broader crypto community has been pitching in. "It is a worldwide effort," says Philip Lafrance, a mathematician at computer-security firm ISARA Corporation in Waterloo, Canada. This means that, at the end of the process, the surviving algorithms will have gained wide acceptance. "The world is going to basically accept the NIST standards," he says. He is part of a working group that is monitoring the NIST selection on behalf of the European Telecommunications Standards Institute, an umbrella organization for groups worldwide. "We do expect to see a lot of international adoption of the standard that we'll create," says Moody.

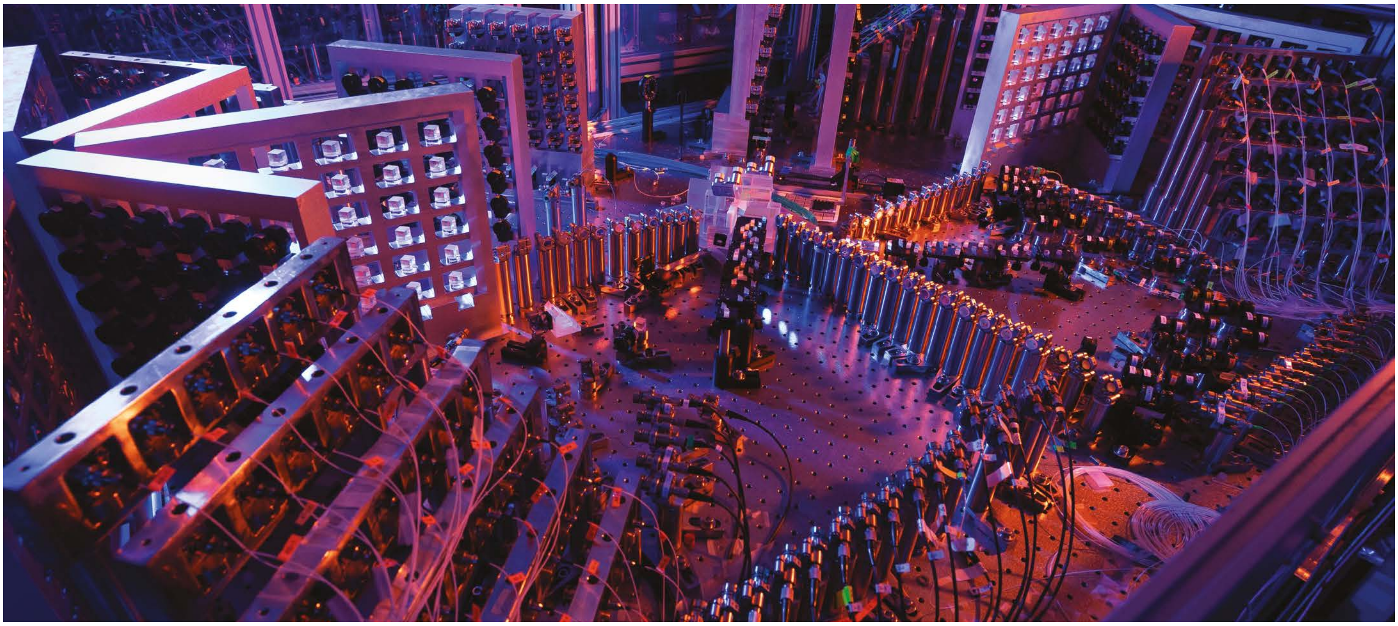
Still, because cryptography affects sensitive national interests, other countries are keeping a close eye – and some are cautious. "The maturity of post-quantum algorithms should not be overestimated: many aspects are still at a research state," says cryptography specialist Mélissa Rossi at the National Cybersecurity Agency of France in Paris. Nevertheless, she adds, this should not delay the adoption of post-quantum systems to strengthen current cryptography.

China is said to be planning its own selection process, to be managed by the Office of State Commercial Cryptography Administration (the agency did not respond to *Nature*'s request for comment). "The consensus among researchers in China seems to be that this competition will be an open international competition, so that the Chinese [post-quantum cryptography] standards will be of the highest international standards," says Jintai Ding, a mathematician at Tsinghua University in Beijing.

Meanwhile, an organization called the Chinese Association for Cryptologic Research has already run its own competition for post-quantum algorithms. Its results were announced in 2020, leading some researchers in other countries to mistakenly conclude that the Chinese government had already made an official choice.

Updating systems

Of NIST's 15 candidates, 9 are public-key systems and 6 are for digital signatures. Finalists include implementations of NTRU and LWE, as well as another tried-and-tested system that uses the algebra of error-correction techniques. Known as 'code-based algorithms', these systems store data with redundancy that makes it possible to reconstruct an original file after it has been slightly damaged by noise. In cryptography, the data-storage algorithm is



CHAO-YANG LU

To crack encryption, quantum computers such as China's Jiuzhang 2.0 will need more qubits.

the public key, and a secret key is needed to reconstruct an original message.

In the next few months, the institute will select two algorithms for each application. It will then begin to draft standards for one, while keeping the other as a reserve in case the first choice ends up being broken by an unexpected attack, quantum or otherwise.

Selecting and standardizing algorithms will not be the end of the story. "It's certainly a solid step to bless a candidate, but as a follow-up, the Internet has to agree on how to integrate an algorithm into existing protocols," says Nick Sullivan, an applied cryptographer at Internet-services company Cloudflare, who is based in New York City.

Both Cloudflare and Google – often in cooperation – have started running real-life tests of some post-quantum algorithms by including them in some beta versions of the Chrome browser and in server software. Testing is crucial because, for Internet communications to go smoothly, it is not enough to have perfectly compatible servers and browsers. To connect them, data must also run through network devices that might block traffic that they flag as unusual because of its unfamiliar encryption protocols. (These systems can be used to prevent hacking or stop users accessing prohibited content.) Antivirus software could cause similar problems. The issues also exist "on a broader, Internet-wide scale, in some countries that keep track of what users are doing", says Sullivan. Network-security workers refer to these issues as 'protocol ossification', he says; it has already complicated the transition from RSA, and might disrupt the roll-out of quantum-secure algorithms, too.

An early test in 2016 implemented New Hope – a structured version of LWE named after the original *Star Wars* movie – in a Chrome beta version, and it ran without a hitch. "This trial showed that it is usable," says Erdem Alkım, a computer scientist now at Dokuz Eylül University in İzmir, Turkey, who wrote some of the code as part of his thesis. "I thought it was a good result for my PhD."

But a larger-scale experiment conducted in 2021 by Google on a different algorithm ran into some snags. Some Internet devices apparently 'broke' – network-security parlance for a gadget that blocks a connection when a client's browser tries to communicate with an unusual protocol. The issue could have been that the browser's opening message was longer than expected, because it carried a large public key. Algorithms that break the Internet in this way could be shelved until these issues are resolved.

"Sometimes you run into situations in which some network element misbehaves when you add something new," comments Rescorla. Persuading vendors to adapt their products – something that can often be done with a simple software update – could take some nudging, he says. "This could take a while."

Still, Rescorla is optimistic, at least when it comes to Internet browsers. Because only a small number of companies control most browsers and many servers, all that needs to happen is that they change encryption systems. "Everybody is pretty confident that once NIST and IETF specify new standards, we'll be able to roll them out pretty quickly."

Where the transition might be trickier is the multitude of modern connected devices, such as cars, security cameras and all kinds of 'smart home' machines, that suffer from protocol ossification – especially those that might have security features hardwired into their chips and that are not replaced often. "It takes five to seven years to design a vehicle, and it's going to be on the road for a decade," says Lafrance. "Is it still going to be secure ten years down the line?"

Either way, initial implementations will be hybrid, using post-quantum technology for added security on top of existing systems. Vadim Lyubashevsky, a computer scientist at IBM in Zurich, Switzerland, whose team has two lattice-based algorithms among the NIST finalists, says he thinks both post-quantum and current encryption methods should run together for a decade before the new algorithms are used exclusively.

If all goes to plan, the Internet will be well into its post-quantum era by the time computing enters its quantum era. This post-quantum Internet could some day be followed, confusingly, by a quantum Internet – meaning a network that uses the principles of quantum physics to make information exchange hacker-proof.

Researchers estimate that to break cryptosystems, quantum computers will need to have in the order of 1,000 times more computing components (qubits) than they currently do. "There's a very good chance that we'll have a quantum computer that can do positive things way before they can break crypto," says Lyubashevsky.

But that is no reason to be complacent. Fully transitioning all technology to be quantum resistant will take a minimum of five years, Rescorla says, and whenever Q-day happens, there are likely to be gadgets hidden somewhere that will still be vulnerable, he says. "Even if we were to do the best we possibly can, a real quantum computer will be incredibly disruptive."

Davide Castelvecchi reports for *Nature* from London.