CAROL HIGHSMITH/BUYENLARGE/GETTY

Today's most widely used encryption methods will not be strong enough resist quantum computers.

INFORMATION SECURITY

Encryption faces quantum foe

Researchers urge readiness against attacks from future-generation computers.

BY CHRIS CESARE

It is an inevitability that cryptographers dread: the arrival of powerful quantum computers that can break the security of the Internet. Although these devices are thought to be a decade or more away, researchers are adamant that preparations must begin now.

Computer-security specialists are meeting in Germany this week to discuss quantum-resistant replacements for today's cryptographic systems — the protocols used to scramble and protect private information as it traverses the web and other digital networks. Although today's hackers can, and often do, steal private information by guessing passwords, impersonating authorized users or installing malicious software on computer networks, existing computers are unable to crack standard forms of encryption used to send sensitive data over the Internet.

But on the day that the first large quantum computer comes online, some widespread and crucial encryption methods will be rendered obsolete. Quantum computers exploit laws that govern subatomic particles, so they could easily defeat existing encryption methods.

"I'm genuinely worried we're not going to be ready in time," says Michele Mosca, co-founder of the Institute for Quantum Computing (IQC) at the University of Waterloo in Canada and chief executive of evolutionQ, a cybersecurity consulting company.

It will take years for governments and industry to settle on quantum-safe replacements for today's encryption methods. Any proposed replacement — even if it seems impregnable at first — must withstand multitudes of real and theoretical challenges before it is considered reliable enough to protect the transfer of intellectual property, financial data and state secrets.

"To trust a cryptosystem, you need a lot of people to scrutinize it and try to devise attacks on it and see if it has any flaws," says Stephen Jordan, a physicist at the US National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland. "That takes a long time."

This week's workshop, held at the Schloss Dagstuhl–Leibniz Center for Informatics in Wadern, is one of several this year bringing together cryptographers, physicists and mathematicians to evaluate and develop cryptographic tools that are less vulnerable to quantum computers. NIST hosted its own workshop in April, and the IQC will team up with the European Telecommunications Standards Institute for another, in early October in Seoul.

Intelligence agencies have also taken notice. On 11 August, the US National Security Agency (NSA) revealed its intention to transition to quantum-resistant protocols when it released security recommendations to its vendors and clients. And in a memo posted on its website earlier this year, the Dutch General Intelligence and Security Service singled out a looming threat that adds even more urgency to the need for quantum-safe encryption. In a scenario it calls 'intercept now, decrypt later', a nefarious attacker could start intercepting and storing financial transactions, personal e-mails and other sensitive encrypted traffic and then unscramble it all once a quantum computer becomes available. "I wouldn't be at all surprised if people are doing that," says Jordan.

As far back as 1994, mathematician Peter Shor showed that a quantum computer would be able to quickly foil 'RSA encryption', one of the major safeguards used today (P. W. Shor Preprint available at http://arxiv.org/abs/quant-ph/9508027v2; 1995). At the time, it was not clear whether such a machine would ever be built, says Mosca, because researchers assumed that it would need to operate flawlessly. But a theoretical discovery in 1996 showed that up to a limit, a quantum computer with some flaws could be just as effective as a perfect one. ▶

MORE ONLINE

THOMAS CROWTHER ET AL/ JAN WILLEM TULP

VIDEO HIGHLIGHT

This week's cover, animated go.nature.com/hzuhns

MORE NEWS

- LHC signal hints at anomalous particle decay go.nature.com/29esur
- Wikipedia seeks to bridge gap with research community go.nature.com/oxule4
- Oliver Sacks: an appreciation go.nature.com/2cloze

NATURE PODCAST

Thinking differently about autism; plankton in our clouds; and untangling Alzheimer's nature.com/nature/podcast

Published experiments with small quantum devices are starting to approach this faultiness threshold, notes Mosca. And because secretive organizations such as the NSA are keenly interested in the technology, it is widely assumed that these published results do not represent the cutting edge of research. "We have to assume there's going to be people that are a few years ahead of what's available in the public literature," says Mosca. "You can't wait for the headlines in *The New York Times* to have your plan in place."

The safety of today's Internet traffic relies in part on a type of encryption called public-key cryptography — which includes RSA — to establish secret communication between users. A sender uses a freely available digital key to lock a message, which can be unlocked only with a secret key held by the recipient. The security of RSA depends on the difficulty of breaking up a large number into its prime factors, which serve as its secret key. In general, the larger the number, the harder this problem is to solve.

Researchers believe that it takes existing computers a long time to factorize big numbers, partly because no one has yet discovered how to do it quickly. But quantum computers could factorize a large number exponentially faster than any conventional computer, and this nullifies RSA's reliance on factoring being difficult.

Several options already exist for new public-key cryptosystems. These replace the factoring problem with other difficult mathematics problems that are not expected to yield to quantum computers. Although these systems are not perfectly safe, researchers think that they are secure enough to protect secrets from quantum computers for all practical purposes.

One such system is lattice-based cryptography, in which the public key is a grid-like collection of points in a high-dimensional mathematical space. One way to send a secret message is to hide it some distance from a point in the lattice. Working out how far the encrypted message is to a lattice point is a difficult problem for any computer, conventional or quantum. But the secret key provides a simple way to determine how close the encrypted message is to a lattice point.

A second option, known as McEliece encryption, hides a message by first representing it as the solution to a simple linear algebra problem. The public key transforms the simple problem into one that seems much more difficult. But only someone who knows how to undo this transformation — that is, who has the private key — can read the secret message.

One drawback of these replacements is that they require up to 1,000 times more memory to store public keys than existing methods, although some lattice-based systems have keys not much bigger than those used by RSA. But both methods encrypt and decrypt data faster than today's systems, because they rely on simple multiplication and addition, whereas RSA uses more-complex arithmetic.

PQCRYPTO, a European consortium of quantum-cryptography researchers in academia and industry, released a preliminary report on 7 September recommending cryptographic techniques that are resistant to quantum computers (see go.nature.com/5kellc). It favoured the McEliece system, which has resisted attacks since 1978, for public-key cryptography. Tanja Lange, head of the €3.9-million (US$4.3-million) project, favours the safest possible choices for early adopters. "Sizes and speed will improve during the project," she says, "but anybody switching over now will get the best security." ■

FUNDING

Germany claims success for elite universities drive

Report praises €4.6-billion scheme to make leading universities more competitive — but some smaller institutions have done just as well.

BY QUIRIN SCHIERMEIER & RICHARD VAN NOORDEN

For a decade, Germany's government has been trying to explode the myth that all the country's universities are equal. In 2006, it launched an 11-year, €4.6-billion (US$5-billion) programme that aimed to make the best German universities more competitive with the likes of Oxford, Cambridge and Harvard. The campaign, called the Excellence Initiative, led to 14 institutions gaining the unofficial label of 'elite'.

A 3 September report by Germany's main research-funding agency, the DFG — which administers the initiative together with Germany's science council — suggests that the cash influx is paying off. Still, a German equivalent of the US Ivy League may be slow to form. An analysis by *Nature*'s news team shows that some universities less favoured by the initiative have improved just as quickly as the elites when it comes to generating highly cited work. "It doesn't require the 'elite' label to produce good research in Germany," says Alfred Forchel, president of the University of Würzburg, an institution that has kept pace without top-up funds.

The DFG sees this as positive. "The Excellence Initiative has met expectations," says Dorothee Dzwonnek, DFG secretary-general. "And it has not weakened universities which don't directly benefit from it." But some critics say that the scheme has benefited administrators more than scientists. And a huge increase in research funding across Germany over the past decade makes it difficult to tease out the influence of the initiative on the country's improvement.

The DFG report, an analysis of funding in German universities that is released every three years, marks the first attempt to measure preliminary outcomes of the initiative. In 2011–13 alone, 45 universities received a total of more than €1 billion for running international graduate schools and setting up specific clusters of excellence. A subset also each received an extra €10 million to €14 million a year for 'institutional strategies' to strengthen the university as a whole — the most prestigious part of the competition (see *Nature* **487,** 519–521; 2012).

The elite group includes some of Germany's largest and best-equipped research universities, such as the Ludwig Maximilian University of Munich and RWTH Aachen University. The report shows that the elites dominate when it comes to winning competitive grants from the DFG. As a group, they secured more than 40% of the agency's total funding from 2011–13. However, the same 14 institutions won almost the same share of DFG funding in 2002–04, before the initiative had launched.

Scientific output is booming at the 45 universities that got cash out of the Excellence Initiative, the DFG report points out. They have boosted their output by 43% in chemistry and physics since 2002, more than the 34% increase in these subjects by all German universities.