Qubits poised to reveal our best-kept secrets


NOWSTOCK/PHOTOLIBRARY

Quantum computers could soon be breaking the codes that protect our data from prying eyes

SASWATO DAS, NEW YORK CITY

IT MIGHT seem like an esoteric achievement of interest to only a handful of computer scientists, but the advent of quantum computers that can run a routine called Shor's algorithm could have profound consequences. It means the most dangerous threat posed by quantum computing – the ability to break the codes that protect our banking, business and e-commerce data – is now a step nearer reality.

Adding to the worry is the fact that this feat has been performed by not one but two research groups, independently of each other. One team is led by Andrew White at the University of Queensland in Brisbane, Australia, and the other by Chao-Yang Lu of the University of Science and Technology of China, in Hefei. Both groups have built rudimentary laser-based quantum computers that can implement Shor's algorithm – a mathematical routine capable of defeating today's most common encryption systems, such as RSA.

RSA is an example of public key cryptography, in which a user holds a pair of mathematically related strings of data, known as a public key and a private key. The public key is widely distributed and used to encrypt messages, while the private key is kept secret and used to decrypt them. An attacker who does not have the private key needs to work out the two very large prime numbers which, multiplied together, make up the public key. Find those factors and you can work out the private key. RSA's security rests on the extreme difficulty of doing this: today's digital computers are just not powerful enough to find the factors of a large key in any practical length of time.

For instance, to find the prime factors of a 10-digit public key, approximately 100,000 calculations are needed; for a 50-digit number about 10 trillion trillion are required. IBM's Blue Gene supercomputer would take a fraction of a second to crack a 10-digit key, but about 100 years for a 50-digit key. And keys are now much longer than 50 digits.

"Blue Gene takes a fraction of a second to crack a 10-digit key, but 100 years for a 50-digit key"

In 1994, mathematician Peter Shor at Bell Labs in New Jersey developed a routine that radically reduces the time required to make those calculations. There was just one rather large catch: it could only run on a computer that exploits quantum mechanics.

Shor's algorithm provides a short cut to finding prime factors by looking for telltale patterns in remainders when a key is divided by a prime factor. Because of the vast number of possible factors for a long key, Shor's algorithm needs to perform a huge number of mathematical operations in parallel – an ability only offered by the quantum bits, or qubits, that carry information in a quantum computer. Thanks to quantum superposition, qubits can inhabit multiple logical states simultaneously, whereas a digital bit can only exist in one state at a time.

The difficulty now is building a quantum computer big enough to carry out the calculations in a reasonable time. Approaches currently being researched include lasers, superconductors, ion traps and quantum dots.

The first implementation of Shor's algorithm was achieved in 2001, when an IBM-led team built a quantum computer using nuclear magnetic resonance (NMR) to run calculations in fluorocarbon molecules. The five fluorine nuclei and two carbon

How long will our banks be safe?

nuclei in a molecule acted as seven qubits: the magnetic spin of each nucleus represented the qubit's state – say, up for 1 and down for 0. Because spin is a quantum property the researchers reckoned the nuclei could be "entangled" into a state that is a mix of both spin up and spin down at the same time – allowing the quantum computer to make calculations in parallel.

Using NMR, the researchers manipulated nuclear spins and coaxed the qubits through Shor's algorithm. As they had hoped, it gave the correct prime factors for 15 as 3 and 5, but doubts emerged over the experiment's quantum credentials. "The NMR was valuable early work. But it is not clear that there was any quantum entanglement in it," White says, and Lu agrees. And there is another problem with NMR: the technology does not scale up. "As the number of NMR qubits increases, the signal disappears in thermal noise," says Carl Williams, of the US National Institute of Standards and Technology in Gaithersburg, Maryland.

Instead of manipulating nuclear spin, both White and Lu's teams plumped for photonic quantum computers. Both used femtosecond lasers to generate photon pairs, which they passed through polarising bismuth borate crystals to create entangled qubits. Using optical devices such as filters, they manipulated the qubits to cajole them into running Shor's algorithm – once again factorising 15 into its constituent primes and reading the results using polarisers and single photon detectors.

Despite the fact that both teams have, like the IBM-led NMR group, only factored the number 15, California-based IT security specialist Bruce Schneier says the way the scientists have done it – with standard lab optics – means problems for encryption may not be far away. Scaling up to solve bigger problems "is now more or less an engineering problem", he says.

"There is no need to panic right now," Schneier says, as cryptography would survive even if RSA was cracked. "RSA has lived with the possibility of being cracked for many years. There are lots of other algorithms, and we'll shift to those."

Computers like White and Lu's are not powerful enough to pose a threat to the world's data, but that may not last. "If we could perform calculations for much larger numbers, then fundamental changes would be needed in cryptography," says White. "And there are paths to a fully scalable quantum computer."

So what does he expect to become of the RSA system when such a quantum computer is finally built?

"It will go overnight," he says. ●

IF RSA IS CRACKED, HERE'S PLAN B

News that researchers have finally built a quantum computer capable of reliably running Shor's algorithm has left cryptographers split over its implications. Some say that quantum computers are nowhere near ready for real-world code breaking, while others believe that cryptography will be forced to move on from its cosy prime-number-based encryption technologies.

The power of Shor's algorithm lies in its potential to use quantum processes to factorise large prime numbers. Just about every strong encryption system relies on the inability of today's computers to do this in any kind of reasonable time. The nightmare for cryptographers would be to find that someone has developed a quantum computer capable of using a massively parallel algorithm, such as Shor's, that would speed this process up to the point at which it became practical – and that is precisely what White and Lu's teams say will now be possible.

UNRESOLVED FACTORS

Some cryptographers are not worried. "Nothing has changed," says Bill Munro of the quantum information processes group at Hewlett-Packard's research laboratories in Bristol, UK. "Going from factoring 15 to factoring a large number is a huge challenge."

Jon Callas, head of technology at the cryptographic software house PGP in Palo Alto, California – maker of the RSA-based Pretty Good Privacy encryption system – says the task facing the wannabe quantum RSA code breakers is the difference between making one transistor and making a 370-million transistor Pentium processor. White and Lu's work used just four qubits. "We currently use about 4000 bits in RSA," Callas says. Cracking that would require a quantum computer with about 50 trillion qubits, he calculates. "We haven't even put that many transistors down on a microchip yet."

What's more, the goalposts are moving. The length of keys is getting longer as traditional computers, thanks to Moore's law, become more powerful, which will push the number of qubits required even higher, Callas says. This is not to say that the number of qubits in quantum computers won't increase. "The major stumbling block to scaling at the moment is to make single-photon sources and detectors that are very efficient," says Daniel Browne of University College London, who is a member of Lu's team.

Research into quantum-dot-based sources and detectors is improving them fast, however.

Eventually, the number of qubits in quantum computers is expected to increase to a point where they can outperform traditional computers and eventually a limit to the length of encryption keys will be reached, but that could be 50 years away.

When it eventually happens, where will that leave encryption? "Cryptographers are smart guys," says Munro. "Shor's algorithm may be a problem for factoring-based codes but there are other cryptographic systems out there that don't use primes."

Hash chains, which use sequential encoding processes, are one example, says Callas. At the moment there is no known way to break these using a quantum computer. "The whole reason that a quantum computer is so fast is that it can be massively parallel," says Callas. "But that doesn't help with a computation that by definition requires you to wait to calculate one thing before you calculate another."

QUANTUM vs QUANTUM

Cryptographers can also turn the quantum beast against itself, of course. Quantum cryptography, which uses entanglement to securely exchange cryptographic keys, currently only works on point-to-point links over relatively short distances and relies on optical networks for its transmission. This makes it impractical for low-end security applications such as buying goods online – but that could all change. By the time quantum computers become a real threat, this may not be the case.

"If we have 10 years' warning we can move out of the way of the quantum train," Callas says. "If we have only three years, we may have to hustle. But we could still probably outrun it." Duncan Graham-Rowe