Beating the codebreakers with quantum cryptography

April 28 2008

SECOQC bank transfer demostration. Source: SECOQC

Quantum cryptography may be essentially solved, but getting the funky physics to work on disciplined computer networks is a whole new headache.

Cryptography is an arms race, but the finish line may be fast approaching. Up to now, each time the codemakers made a better mousetrap, codebreakers breed a better mouse. But quantum cryptography theoretically could outpace the codebreakers and win the race. Forever.

Already the current state of the art in classical encryption, 128-bit RSA, can be cracked with enough raw, brute force computing power available to organisations like the US National Security Agency. And the advent of quantum computing will make it even simpler. The gold standard for secret communication will be truly dead.

Quantum cryptography solves the problem, and it will overcome the remaining stumbling block, the distribution of the code key to the right person, by using quantum key distribution (QKD).

Modern cryptography relies on the use of digital 'keys' to encrypt data before sending it over a network, and to decrypt it at the other end. The receiver must have a version of the key code used by the sender so as to be able to decrypt and access the data.

QKD offers a theoretically uncrackable code, one that is easily distributed and works in a transparent manner. Even better, the nature of quantum mechanics means that if any eavesdropper – called Eve in the argot of cryptographers – tries to snoop on a message the sender and receiver will both know.

That ability is due to the use of the Heisenberg Uncertainty Principle, which sits at the heart of quantum mechanics. The principle rests on the theory that the act of measuring a quantum state changes that state. It is like children with a guilty secret. As soon as you look at them their faces morph plausibly into 'Who, me?'

The practical upshot for cryptography is that the sender and receiver can verify the security of the transmission. They will know if the state of the quanta has changed, whether the key has been read en route. If so, they can abandon the key they are using and generate a new one.

QKD made its real-world debut in the canton of Geneva for use in the electronic voting system used in the Swiss general election last year. The system guaranteed that the poll was secure. But, more importantly perhaps, it also ensured that no vote was lost in transmission, because the uncertainly principle established there was no change to the transmitted data.

The end of the beginning

The canton election was a demonstration of the work done by researchers for the SECOQC project, an EU-funded effort to develop an international network for secure communication based on QKD.

The test of the technology demonstrated that QKD worked for point-to-point communications between two parties. But the demonstration was just the beginning of the SECOQC's overall goal.

"We want to establish a network wide quantum encryption, because it will mean it works over much longer distances," explains Christian Monyk, co-ordinator of the SECOQC project and head of the quantum-technologies unit at the Austrian Research Centres. "Network quantum encryption and QKD mean that many parties can communicate securely, not just two. Finally, it also means quantum encryption could be deployed on a very large scale, for the insurance and banking sectors, for example."

Moving the system from point-to-point communications to a network is an order of magnitude more difficult.

"The quantum science for cryptography and key distribution is essentially solved, and it is a great result," Monyk says. "But getting that system to work across a network is much more difficult. You have to deal with different protocols and network architectures, develop new nodes and new interfaces with the quantum devices to get it to a large-scale, long distance, real-world application."

Working at a distance

Getting the system to work over long distances is also a challenge

because QKD requires hi-fidelity data transmission over high-quality physical networks like non-zero dispersion shifted fibre optics.

“It was not one big problem, it was many, many small computing science and engineering problems,” says Monyk. “We had to work with a large number of technologies. And we have to certify it to experts.”

But SECOQC’s researchers believe they have solved the network issue. The researchers are currently putting the final touches to a demonstration of the technology to be held this October in Vienna, Austria. Industry has shown great interest in the technology. Still the technology is not quite ready for prime time.

“From a technical point of view, the technology will be ready in one or two years,” says Monyk.

And that means that the race will be won, finally, by the codemakers.

Source: ICT Results