

The Royal Society of Edinburgh

James Scott Prize Lecture

Professor Stephen Barnett FRS FRSE, Professor of Quantum Optics, Department of
Physics, University of Strathclyde

Monday 4 February 2008

The Barnett Formula... Security, Insecurity, Paranoia and Quantum Mechanics

Is there any such thing as a foolproof security system for banking transactions and other computer-based communications systems? The bad news is that something called quantum computing will soon make money worthless by cracking all our current security codes in a couple of seconds. But the good news is that quantum computing will be one step ahead of itself, as Professor Stephen Barnett explained at the recent James Scott Prize Lecture...

ATM fraud costs £100 million a year in the UK alone, but this would be virtually nothing compared to future cyber-crime. Armed with a super-fast, super-intelligent quantum computer – more powerful than all the computers we have today added together – criminals could steal every dollar and cent in the world by effortlessly cracking the security systems used by the banks for the transfer of money.

Professor Barnett painted a frightening picture, but he did also look on the bright side, pointing out that quantum computers are some years away – and will also be used to prevent fraud using radical new methods of cryptography.

But what about the flaw in every system – human beings? Acknowledging that every system ultimately must depend on trust, Barnett also said the best protection we have is “the public community of scientists” sharing information and ideas, and keeping a few steps ahead of the bad guys.

First, however, the technology and reasons to be paranoid...

As Barnett explained, money today is a sequence of numbers – information or digital assets. Current systems for encrypting data make it hard to steal this information or disrupt financial networks, but no system is perfect, despite all the clever solutions – and a new threat is on the horizon.

“Internet purchases and international bank transactions rely on the same simple (and unproven) ideas from pure mathematics,” said Barnett. “Developments in quantum theory provide the means (at least in principle) to hack into these transactions, thus rendering money valueless. But quantum theory also provides its own radical solution.”

According to Barnett, the problem lies in the fact that we have to communicate. The more we communicate, the more we endanger our assets. If we could physically isolate data, there would be no problem, but as soon as we start to exchange any data, the problems begin.

The one-time pad or “Vernam cipher” is in theory perfectly secure. It is used for single-key cryptography, and crucially requires the one-time use of a secret key to unlock data scrambled or encrypted by adding a digital message exactly the same length as the original message – like all digital data, a sequence of zeroes and ones – to produce a random “number” or message that appears to be nonsense.

But even this “perfect” solution has drawbacks. First, we need to ensure we have two secret keys for receiver and sender; and second, we also need to generate a very long number to disguise the original message.

Another method – public key cryptography – is more practical and thus is more commonly used by the banks, but it is also vulnerable to hackers with enough determination and intelligence.

The solution, according to Barnett, is quantum mechanics...

To put it simply (if that is possible with quantum mechanics), this means taking advantage of the polarisation of light – the fact that photons have electrical fields which go in six different directions, e.g. vertical, horizontal, diagonal (left & right) and circular (left & right) – to create a new ‘language’ for data more complex and therefore much harder to crack. Classical computers process zeroes and ones, or ‘on’ and ‘off’, but quantum computers would use all the different directions of photons, which means an exponential increase in complexity.

In addition, thanks to new encryption techniques such as quantum key distribution, anyone trying to interfere with the photon-based data would leave a digital “fingerprint” which alerts the receiver and sender. This means a one-time key can be exchanged between two parties, safe in the knowledge that no-one has

eavesdropped. If someone has tried to eavesdrop, they simply throw away the suspect key and send another key until they can guarantee safety, and only then begin to exchange information.

As Barnett put it: “Quantum mechanics (thanks to the principle of superposition) has another throw of the dice..”

In the 1980s, researchers at IBM in the USA successfully used quantum optics to send data over a distance of a few centimetres. Today, we can send data over a few kilometres, and there are already plans to use satellite technology to increase the range of quantum optical signalling across the global financial community.

“Quantum key distribution offers a radically different approach in which security is assured by the laws of quantum physics,” concluded Barnett. “It is the only current candidate for security in a world with quantum computers.”

In other words, the exponential increase in danger will be countered by an exponential improvement in computing and encryption resources. And a prototype for quantum ATM transactions was announced by researchers at Bristol University in late 2007.

So no need to worry, then?

When someone asked Professor Barnett what would happen if someone involved in the technical side of the banking network decides to get greedy – for example, the satellite manufacturer – he admitted that trust is a critical factor in every transaction. He also agreed that storage was extremely important.

And what about terrorists? Could they target the new quantum network?

“I hope they do,” said Barnett, “because they will waste their time trying to do so and never succeed...”

Peter Barr

Opinions expressed here do not necessarily represent the views of the RSE, nor of its Fellows

The Royal Society of Edinburgh, Scotland’s National Academy, is Scottish Charity No. SC000470