# Twists to quantum technique for secret messaging give unanticipated power

February 19 2012

Quantum cryptography is the ultimate secret message service. Now new research, presented at the 2012 AAAS Annual Meeting, shows it can counter even the ultimate paranoid scenario: when the equipment or even the operator is in the control of a malicious power.

Until now, quantum cryptography protocols have always assumed that an adversary would not have access to information about any choices that are made during the process of encryption. "We are challenging this assumption," says Artur Ekert, Director of the Centre for Quantum Technologies (CQT) at the National University of Singapore (NUS) and Professor at the University of Oxford, UK, who will present the research. "We are asking well, what if you are controlled?"

In a world of secrets, it pays to be paranoid. From ancient Rome to the modern age, most classical schemes for cryptography have relied on the 'decoding' step involving some problem that is hard to solve – but hard, rather than impossible. That has left cryptographic schemes, including those in wide use today, vulnerable to clever people or advances in technology.

Quantum cryptography, by contrast, offers security protected by the laws of physics. The technique provides a way for two parties to share a secret key – a random sequence of 1s and 0s – which can then be used to scramble a message. The security comes from quantum laws providing a built-in way to detect eavesdropping attempts. When the key is transmitted, using photons, say, any interception of the signal changes it

in a way the legitimate parties can detect. Insecure keys can then be discarded.

But a "malicious manipulator" might have the ability to control the setup or influence the communicating parties' choice of settings in transmitting the key. The manipulation could even be something enshrined in fundamental physics – a limit on the amount of free will that humans can exercise.

It's a huge challenge to face, but the researchers believe quantum cryptography can still sometimes triumph. Ekert and his colleagues have worked out how to calculate, given the degree of manipulation, how much genuine 'randomness' remains in the key. This offers a measure of how much of the key has been left untouched and will, in turn, determine how much of the key can be guaranteed secret.

The breakthrough, which Ekert presented at AAAS on 18 February, builds on two recent twists that have given quantum cryptography a powerful boost against eavesdroppers.

The first came when researchers showed that one can design quantum cryptography setups such that devices of dubious provenance – such as those purchased from an untrusted supplier, or even an enemy – can still, with some care, be safely used for secure communication. This remarkable feat is known as 'device independent cryptography' and is on the edge of being technologically feasible.

The second twist was the realisation that device-independent schemes transcend the details of the underlying physics. Even if physicists discover new laws, such as a 'theory of everything' that replaces quantum mechanics, these schemes will continue to be secure.

Provided by National University of Singapore