Quantum cryptography: Keeping your secrets secret

March 26 2014

Credit: WinBeta

An article in *Nature* reviewing developments in quantum cryptography describes how we can keep our secrets secret even when faced with the double challenge of mistrust and manipulation.

Revelations of the extent of government surveillance have thrown a spotlight on the security – or lack thereof – of our digital communications. Even today's encrypted data is vulnerable to technological progress. What privacy is ultimately possible? In the 27 March issue of *Nature*, researchers Artur Ekert and Renato Renner review what physics tells us about keeping our secrets secret.

In the history of secret communication, the most brilliant efforts of code-makers have been matched time and again by the ingenuity of code-breakers. Sometimes we can even see it coming. We already know that one of today's most widely used encryption systems, RSA, will become insecure once a quantum computer is built.

But that story need not go on forever. "Recent developments in quantum cryptography show that privacy is possible under stunningly weak assumptions about the freedom of action we have and the trustworthiness of the devices we use," says Ekert, Professor of Quantum Physics at the University of Oxford, UK, and Director of the Centre for Quantum Technologies at the National University of Singapore. He is also the Lee Kong Chian Centennial Professor at the National University of Singapore.

Over 20 years ago, Ekert and others independently proposed a way to use the quantum properties of particles of light to share a secret key for secure communication. The key is a random sequence of 1s and 0s, derived by making random choices about how to measure the particles (and some other steps), that is used to encrypt the message. In the *Nature* Perspective, he and Renner describe how quantum cryptography has since progressed to commercial prospect and into new theoretical territory.

Even though privacy is about randomness and trust, the most surprising recent finding is that we can communicate secretly even if we have very little trust in our cryptographic devices – imagine that you buy them from your enemy – and in our own abilities to make free choices – imagine that your enemy is also manipulating you. Given access to certain types of correlations, be they of quantum origin or otherwise, and having a little bit of free will, we can protect ourselves. What's more, we can even protect ourselves against adversaries with superior technology that is unknown to us.

"As long as some of our choices are not completely predictable and therefore beyond the powers that be, we can keep our secrets secret," says Renner, Professor of Theoretical Physics at ETH Zurich, Switzerland. This arises from a mathematical discovery by Renner and his collaborator about 'randomness amplification': they found that a quantum trick can turn some types of slightly-random numbers into completely random numbers. Applied in cryptography, such methods can reinstate our abilities to make perfectly random choices and guarantee security even if we are partially manipulated.

"As well as there being exciting scientific developments in the past few years, the topic of cryptography has very much come out of the shadows. It's not just spooks talking about this stuff now," says Ekert, who has worked with and advised several companies and government agencies.

The semi-popular essay cites 68 works, from the writings of Edgar Allen Poe on cryptography in 1841, through the founding papers of quantum cryptography in 1984 and 1991, right up to a slew of results from 2013.

The authors conclude that "The days we stop worrying about untrustworthy or incompetent providers of cryptographic services may not be that far away".

More information: A. Ekert and R. Renner "The ultimate physical limits of privacy", *Nature* DOI: 10.1038/nature13132 (2014)

Provided by National University of Singapore