Researchers weight safety of quantum cryptology

March 31 2011

Scientists in Belgium and Spain have proved for the first time that new systems of quantum cryptology are much safer than current security systems. The study was published in the journal *Nature Communications*.

By using keys that are generated using quantum particles, the transmission of data can be guaranteed by the very laws of physics, according to researchers at the Free University of Brussels (ULB) in Belgium and the Institute of Photonic Sciences in Barcelona in Spain. The laws of quantum mechanics state that observing a particle in its quantum state actually modifies that state, which means that in cases where quantum particles are used as keys in the transmission of data, 'spying' can be easily and immediately detected.

As the researchers noted in their paper, 'A central problem in cryptography is the distribution among distant users of secret keys that can be used, for example, for the secure encryption of messages'. They said that 'this task is impossible in classical cryptography unless assumptions are made on the computational power of the eavesdropper. Quantum key distribution (QKD), on the other hand, offers security against adversaries with unbounded computing power'.

This has been the principle behind all the main quantum cryptography systems on the marketplace, but weaknesses in the way that these systems have been implemented in the past has left them open to attack by 'quantum hackers', prompting researchers to look for more effective means of securing data. Based on work by post-doctoral student Jonathan Barrett, researchers at the ULB developed a methodology that was not based on identifying changes to the quantum state of particles.

Instead, quantum devices were used as 'black boxes' that both receive and transmit data; provided that both sender and receiver can detect certain correlations between the data produced by their respective boxes, the safety of the quantum key can be guaranteed. This not only makes any attempt to spy on the data completely pointless but also takes the security of data transmission to the limit of our current understanding of the laws of physics.

What remained to be proven, however, was that this new approach was truly secure, since tests had focused solely on a few limited attacks. What researchers Stefano Pironio of the Faculty of Sciences at ULB and Lluis Masanes and Antonio Acín of the Institute for Photonic Sciences in Barcelona have shown is that this new approach allows keys to be generated at a reasonable rate, comparable to those already used in existing systems, thus ensuring complete security of the system.

The researchers write in *Nature Communications* that their work provides 'a general formalism for proving the security' of quantum key distribution protocols. 'This is done in terms of the strongest notion of security, universally composable security, according to which the secret key generated by the protocol is indistinguishable from an ideal secret key,' they explained.

Although their 'proof' is based on a minor assumption about the way in which quantum devices function, the results of the research show quite clearly that this new approach is indeed possible in principle, paving the way for more secure forms of quantum cryptography. The scientists conclude: 'Our work contributes to narrow the gap between theoretical security proofs and practical realisations of quantum key distribution.'

More information: *Nature Communications* 2, Article number: 238 doi:10.1038/ncomms1244

Provided by Cordis

Citation: Researchers weight safety of quantum cryptology (2011, March 31) retrieved 23 April 2024 from https://phys.org/news/2011-03-weight-safety-quantum-cryptology.html