Making quantum cryptography practical

April 30 2009

Quantum cryptography, a completely secure means of communication, is much closer to being used practically as researchers from Toshiba and Cambridge University's Cavendish Laboratory have now developed high speed detectors capable of receiving information with much higher key rates, thereby able to receive more information faster.

Published as part of IOP Publishing's New Journal of Physics' Focus Issue on 'Quantum Cryptography: Theory and Practice', the journal paper, 'Practical gigahertz quantum key distribution based on avalanche photodiodes', details how quantum communication can be made possible without having to use cryogenic cooling and/or complicated optical setups, making it much more likely to become commercially viable soon.

One of the first practical applications to emerge from advances in the often baffling study of quantum mechanics, quantum cryptography has become the soon-to-be-reached gold standard in secure communications.

Quantum mechanics describes the fundamental nature of matter at the atomic level and offers very intriguing, often counter-intuitive, explanations to help us understand the building blocks that construct the world around us. Quantum cryptography uses the quantum mechanical behaviour of photons, the fundamental particles of light, to enable highly secure transmission of data beyond that achievable by classical encryption.

The photons themselves are used to distribute keys that enable access to encrypted information, such as a confidential video file that, say, a bank

wishes to keep completely confidential, which can be sent along practical communication lines, made of fibre optics. Quantum indeterminacy, the quantum mechanics dictum which states that measuring an unknown quantum state will change it, means that the key information cannot be accessed by a third party without corrupting it beyond recovery and therefore making the act of hacking futile.

While other detectors can offer a key rate close to that reported in this journal paper, the present advance only relies on practical components for high speed photon detection, which has previously required either cryogenic cooling or highly technical optical setups, to make quantum key distribution much more user-friendly.

Using an attenuated (weakened) laser as a light source and a compact detector (semiconductor avalanche photodiodes), the researchers have introduced a decoy protocol for guarding against intruder attacks that would confuse with erroneous information all but the sophisticated, compact detector developed by the researchers.

As the researchers write, "With the present advances, we believe quantum key distribution is now practical for realising high band-width information-theoretically secure communication."

Governments, banks and large businesses who fear the leaking of sensitive information will, no doubt, be watching closely.

More information:

Practical gigahertz quantum key distribution based on avalanche photodiodes

The published version of the paper "Practical gigahertz quantum key distribution based on avalanche photodiodes" (Z L Yuan 2009 New J.

Phys. 11 045019) will be freely available online from Thursday, 30 April. It will be available at stacks.iop.org/NJP/11/045019

Focus on Quantum Cryptography: Theory and Practice

This article features as part of an invited focus issue on the topic of 'Quantum Cryptography: Theory and Practice' edited by Norbert Lütkenhaus and Andrew Shields. The issue includes papers reporting the latest research developments that tackle practical issues, such as increasing the range and bit rate of quantum-cryptographic links and progressing the technology from point-to-point protocols to quantum communication networks, as well as covering theoretical developments to prove the security of these schemes. All articles are permanently free to read and can be found at stacks.iop.org/NJP/11/045005.

Source: Institute of Physics (news : web)