Detector blinding attacks on quantum cryptography defeated

December 1 2010

(PhysOrg.com) -- The Cambridge Research Laboratory of Toshiba Research Europe announced today that it has discovered a simple method to prevent detector blinding attacks on quantum cryptography.

Quantum cryptography is a method to distribute digital encryption keys across an optical fibre. The protocol has been proven to be perfectly secure from eavesdropping. However, any differences between the theoretical protocol and its real-world implementation can be exploited to compromise the security of specific systems.

A recent paper published in the September edition of Nature Photonics suggests a method to blind the Indium Gallium Arsenide (InGaAs) avalanche photo-detectors that are commonly used in quantum cryptography. If successful, this attack could allow an eavesdropper to gain information about the secret key.

Now an investigation by the Cambridge team, to be published in the December edition of Nature Photonics, demonstrates that the detector blinding attack is completely ineffective, *provided* that the single photon detectors are operated correctly.

The new study shows that the attack is only successful if a redundant resistor is included in series with the single photon detector, or if the discrimination levels are set inappropriately. Furthermore, by monitoring the photocurrent generated by the detector it is possible to prevent all bright light attacks on avalanche photodiodes.

Dr Andrew Shields, Assistant Managing Director, Toshiba Research Europe, comments, “Quantum cryptography is now entering a new phase in which the security of particular implementations is carefully analysed and tested. This is important to uncover any security loopholes and to devise appropriate countermeasures. It will allow real-world devices to approach the perfect security that can be proven for the protocol.”

Toshiba recently implemented its quantum key distribution (QKD) technology in the quantum cryptography network set up in the Tokyo metropolitan area in October 2010. In a series of trials Toshiba demonstrated record average secure bit rates on installed fibre in the network. A secure bit rate of 304 kb/s was demonstrated, averaged over a 24 hour period, on a 45km fibre despite a relatively high loss on the link of 14.5dB. In April 2010 the same team announced an average secure bit rate of 1 Mb/s for a laboratory based demonstration on a 50 km fibre spool.

More information: For further information about the work of Toshiba’s Cambridge Research Laboratory in Quantum Information Technology, go to www.toshiba-europe.com/research/crl/qig/index.html

Provided by Toshiba