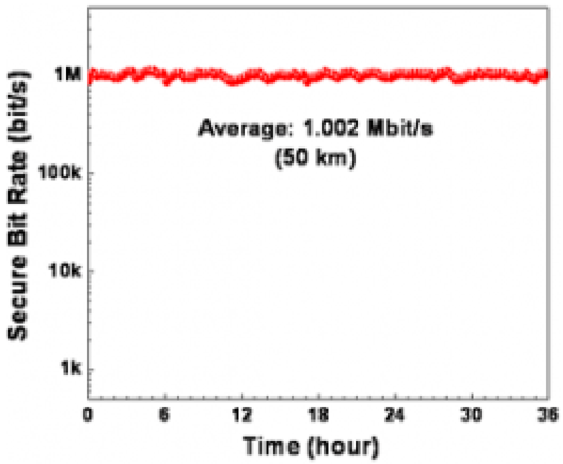
PHYS.ORG

Toshiba researchers achieve new record bit rate for quantum key distribution

April 20 2010



Bit rate over time showing 1 Mbit/s average.

The Cambridge Lab of Toshiba Research Europe today announced a major breakthrough that will allow ultra-secure encryption of sensitive data sent by banks, hospitals and government organisations.

They have succeeded in demonstrating continuous operation of quantum key distribution (QKD) with a secure bit rate exceeding 1 Megabit/sec over 50 km of fibre for the first time. Averaged over a 24 hour period, this is 100-1000 times higher than anything reported previously for a 50 km link. It was achieved using two innovations developed by the Cambridge team: a novel light detector for high bit rates and a feedback system which maintains a high bit rate at all times and requires no manual set-up or adjustment. The results will be reported in the scientific journal, Applied Physics Letters.

Significantly, the breakthrough will enable the everyday use of “one-time pad” encryption, the only known method that is theoretically perfectly secret. Although ultra-secure, the application of one-time pad encryption has been restricted in the past as it requires the transmission of very long secret keys — the same length as the data itself. For this reason it has only been used for short messages in situations requiring very high security, for example by the military and security services. Today's bit rate breakthrough will extend the application of this ultra-secure communication method for everyday use.

Dr Andrew Shields, who directs this work at Toshiba Research Europe commented, “Although the feasibility of QKD with megabits per second has been shown in the lab, these experiments lasted only minutes or even seconds at a time and required manual adjustments. To the best of our knowledge this is the first time that continuous operation has been demonstrated at high bit rates. Although much development work remains this advance could allow unconditionally secure communication with significant bandwidths.”

As an example of the new capability afforded by this system, these higher bit rates would allow real time encryption of video using the one-time pad. This is now possible due to the much higher and continuous bit rates that can be delivered with the new technology. Previously it had been possible to encrypt continuous voice data, but not video images.

Toshiba now plans to install a QKD technology demonstrator at the National Institute of Information and Communications Technology (NICT) in Tokyo. Co-ordinator of the Tokyo QKD Network, Dr. Masahide Sasaki, commented: “The secure key rate of 1 Megabit/sec over 50 km has been a milestone for mission critical applications. The next challenge would be to put this level of technology into metropolitan network operation. Our Japan-EU collaboration is going to do this within the next few years.”

Cryptography, the science of information security, is essential to protect electronic business communication and e-commerce, enabling, for example, confidentiality, identification of users and validation of transactions. All of these applications rely upon digital keys, which are shared between the legitimate users, but must be kept secret from everyone else. Maintaining the ability to distribute keys securely is thus one of the most important battlefields in the cryptography arms race. It is essential to be able to distribute keys between users securely. Furthermore, in order to protect the system from crypto-analysis or key theft it is important to change the keys frequently.

Quantum Key Distribution (QKD) is an automated method for distributing secret keys across an optical fibre. A unique feature of QKD is that its security is derived from the fundamental laws of Quantum Physics and does not therefore rely upon assumptions about the computing power of an eavesdropper. An added benefit is that the keys distributed by QKD will be secure in the future as well as today.

QKD is based upon sending encoding single photons (particles of light) along the fibre. The laws of Quantum Physics dictate that any attempt by an eavesdropper to intercept and measure the photons alters their encoding. This means that eavesdropping on quantum keys can be detected.

The Toshiba QKD system is based on one-way optical propagation and the BB84 protocol using decoy pulses. This protocol has been proven to be unconditionally secure, i.e. satisfying the most stringent security criterion.

Current QKD systems are limited by the semiconductor devices (avalanche photodiodes) used to detect the single photons. One photon triggers an avalanche of millions of electrons in this semiconductor device which can be sensed by electrical circuitry in the QKD system. The problem in present systems is that some of these avalanche electrons can be trapped in the device and later stimulate a second spurious detection count. As these noise counts cause errors in the key, current detectors must be operated with long dead times to allow the decay of any trapped electrons. This has limited the clock rate of current QKD systems to around 10 MHz and thus the average secure key bit rate to a few kbit/sec for a 50 km fibre.

The Toshiba team has devised a method to detect much weaker avalanches. This strongly reduces the chance for an electron to be trapped, allowing the detector to be operated at much faster rates beyond 2 GHz. As the detector is based on a compact and rugged semiconductor device, it is suitable for real-world applications.

More information: Technical preprint: Continuous operation of high bit rate quantum key distribution

Source: Toshiba

Citation: Toshiba researchers achieve new record bit rate for quantum key distribution (2010, April 20) retrieved 3 May 2024 from https://phys.org/news/2010-04-toshiba-bit-quantum-key.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.