Toshiba Plug Loophole in Security of Quantum Cryptography

February 20 2007

Toshiba Research announced today that it has developed two new technologies to realize 'unconditionally secure' quantum key distribution (QKD). To achieve this, Toshiba has overcome a potential security loophole in current commercial QKD systems. Part of these technologies are exhibited in Nano Tech 2007 in Tokyo.

In principle, quantum key distribution provides an absolutely secure means for transmitting secret keys between two parties on fibre optical networks. However, the QKD systems developed so far have a vulnerability which leaves them open to hacking. The weak laser diode used to generate single photon pulses which carry the quantum keys, will sometimes generate pulses with multiple photons.

As a result, an eavesdropper could split off one of these extra photons and measure it, while leaving the other photons in the pulse undisturbed, thus determining part of the key while remaining undetected. Furthermore, an eavesdropper could even determine the entire key, by blocking the single-photon pulses and allowing only the multi-photon pulses to travel through the fibre.

Now two solutions to this problem have been found, the first of which has already been implemented by Toshiba in their QKD system.

Toshiba has implemented a new method for QKD, in which the photon signal pulses are interspersed randomly with a number of “decoy pulses”. These decoy pulses are weaker on average and so very rarely contain two

or more photons. If an eavesdropper attempts a pulse-splitting attack, she will transmit a lower fraction of these decoy pulses than signal pulses. Thus by monitoring the transmission of the decoy and signal pulses separately this type of intervention can be detected.

By introducing decoy pulses, stronger laser pulses may be used securely, increasing the rate at which keys may be sent. Toshiba have demonstrated a 100-fold increase in the rate that keys could be transmitted securely over a 25km fibre to an average bit rate of 5.5kbits/sec – the highest value to date for a full QKD system. This work is part of the EU initiative SECOQC to build a secure communication network based on QKD.

“Using these new methods for QKD we can distribute many more secret keys per second, while at the same time guaranteeing the unconditional security of each. This enables QKD to be used for a number of important applications such as encryption of high bandwidth data links,” said Dr Andrew Shields, Quantum Information Group Leader at Toshiba Research Europe.

The second method, based on nano-technology, will produce even higher bit rates in the future. Toshiba has created the first semiconductor diode that can be controlled with electrical signal input to emit only single photons at a wavelength compatible with optical fibres. This ‘single photon source’ method eliminates the problem of multi-photon pulses altogether. It was developed as part of a DTI funded programme involving the University of Cambridge, Imperial College London and Toshiba.

The single photon diode has a structure similar to an ordinary semiconductor light emitting diode (LED), like those used in traffic lights and indicator lamps, except that it contains a tiny semiconductor quantum dot, measuring just 45 nm in diameter and 10 nm in height.

The dot can hold only a few electrons and so can only ever emit one photon at a time at the selected wavelength. The source operates with only electrical signals, which is essential for practical applications such as QKD. Initial trials with the new device, reported recently in the scientific journal Applied Physics Letters, show the multi-photon rate from the device is fives times lower than that of a laser diode of the same intensity.

"We are now entering the quantum age and we are seeing the first few steps in the development of technologies which will have a profound effect on the development of communications," the Managing Director of Cambridge Research Laboratory in Toshiba Research Europe, Professor Sir Michael Pepper, said. "Some years ago Toshiba took the decision to invest and build up a team of experts to pursue fundamental research in an industrial setting, this breakthrough as well as the entire development of optically based quantum communications is the result of that decision."

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 cryptography allows users on an optical fibre network to refresh frequently their keys in a completely secret way. It takes advantage of the particle-like nature of light. Each bit of the key is encoded upon a single photon (a light particle) sent down the fibre. As a

photon is indivisible and cannot be copied, this ensures that the key cannot be stolen by an eavesdropper without the sender's and receiver's knowledge.

Toshiba have developed a quantum key distribution system where the photons travel one way from sender to receiver, the only configuration that has been rigorously proven secure. This was achieved using an active stabilization system, which manages and automatically adjusts the hardware to maintain continuous operation. The result is an efficient, easy-to-use system, which serves keys for crypto applications and requires no user adjustments.

Source: Toshiba