NEWS RELEASE

NTT

June 14, 2005

Success in distributing single photons for quantum cryptography via an optical switch

- Application of single photon interference phenomena that had annoyed Prof. Einstein -

Nippon Telegraph and Telephone Corp. (NTT; Head Office: Chiyoda-ku, Tokyo; President: Norio Wada) has successfully demonstrated the quantum cryptography with a single photon, whose state is so fragile against the attacks from the eavesdroppers, can be realized in the photonic network of optical fibers. This result was enabled by combining the original protocol of the quantum cryptography developed by the collaboration of NTT and Stanford University (USA) and the NTT developed optical switch to control the flow of photons. The quantum cryptography is expected to be the last resort of the cryptography protocol, and to enhance enormously the safety of the transmitting information.
In this connection, 2005 is the World Year of Physics (*1), and this experiment utilizes the quantum effect, which had puzzled Prof. Einstein about a century ago: *a single photon is like a particle (quanta) but sometimes behaves like a wave and interferes with itself*. Although the modern physics still cannot explain why such an interference occurs, the present work clearly demonstrated that this quantum effect is applicable in the technology of cryptography for the first time.

Background

Secure data: a top secret or financial data, for instance, should be back-upped against an emergency. For that purpose, such data are frequently exchanged via the optical fiber for the exclusive use. In the near future, the subject of data backup will be enlarged into general companies and personal users. Since maintaining an exclusive optical fiber between the users and backup center is too expensive, usage of general network, such as the Internet will be unavoidable.
Then it arises the necessity to setup the procedure to protect the secret data by cryptography while being exchanged through the Internet. Currently, the cryptography system called public-key protocol is widely used. In this protocol, although the eavesdropper may try to decipher the data, he/she cannot decipher in practice since it may take hundred's million years. However, the recent increase of computer ability, which may shorten the time to decipher, and corresponding increase of ciphers to make the deciphering difficult, are in a vicious circle.
Quantum cryptography is assumed as a next generation cryptographic system that may replace the public-key protocol. This technology utilizes the property that the quantum state is very delicate to the external environment and is destroyed by observing it. Namely, the transmitted secret key encoded in the quantum state, single photon, is destroyed when the eavesdropper observed it. Since the eavesdropper cannot resend the quantum state that is identical to the original one, the receiver can easily detect if the secret key had been stolen.

Although the quantum cryptography breaks the vicious circle mentioned above, it is required that the very weak signal of single photon and strong light signal currently used in photonic network can transmit in the same network. Moreover, when it is transmitted via a switchboard, the optical signal should not be transferred to the electric signal since the quantum state is destroyed at the moment of transfer. Therefore, the signal path should be controlled without transferred into the electric signal. Fortunately, PLC(*2) optical switch can control path with the optical signal as it is. However, it was not clear if such a weak signal as single photons can be controlled similarly to the commonly used light signal.

The experiment and Results

This experiment proved that the following two things were possible in an open photonic network environment such as the Internet.

1. A single photon can interfere.
2. In an optical switch with a cross-connecting function among multiple input and output ports, we can control optical paths and send a weak signal on single photons together with large-bandwidth data transmissions on strong lights.

When a light from a laser source passes through a double slit and is projected onto a screen, we can observe a contrast between light and shade, which is due to an interference between lights from two slits (Fig.1 a). If we put a medium with a different refractive index in front of a slit, the interfering pattern changes because the effective length that the light feels changes by the insertion of the medium (Fig.1 b). The optical switch used in the experiment is a planar lightwave circuit (PLC), which is based on the principle explained above.

Figures 1 (c) and (d) show the schematic diagram of the switch. In this switch, an Mach-Zehnder type interferometry occurs where the two lights are divided by the double slit and are recombined, and as a result, the both lights enter into the same output waveguide. When we want to change the path, we change the temperature of one of the two arms in order to change the refractive index. Then, the both lights output from another port because we changed the state of interferometry by changing the effective length of the waveguide that the light feels with temperature control.

Then, what happens when the light power from the laser source is attenuated so that only single photons are output with time intervals to be used quantum cryptography? Each photon seems transmit one of the two arms of the optical switch. The answer to this question can be deduced from the famous Young's experiment of single photon interferometry (Fig. 2). We put a sensitive film plate instead of a screen. Each photon makes a random spot on the plate after passing through the double slit. However, the collective shape of the spots coincides with the interferometry pattern by the lightwaves from the two slits with strong input light. (Fig. 2) Putting a medium with a different refractive index in front of a slit changes the pattern similarly as before. An analogous single-photon interference is observed using a PLC optical switch (Fig. 3).

In the optical switch experiment, a 8x8 matrix switch which is composed of interferometry type switches (PLC-MZ) using a waveguide described above was used. The principle of this switch is as same as the one widely used in the photonic network. First, we confirmed that a weak pulse signal of the single photon level inputs from one port of the switch and is detected from one port, and by changing the switch condition the optical path was controllable (Fig. 4). Next, we sent a weak signal together with large bandwidth data transmissions on strong lights. Though the two lights cross in the matrix switch, we could send them simultaneously and independently with using an optical filter at the receiver's port of weak signal. (Fig. 5)

In this experiment, a Differential-Phase-Shift quantum key distribution (QKD) scheme(*3), which was proposed by NTT and Stanford University, USA, was used. This protocol has several advantages as follows.

- Stable operation is attainable. It is possible to send a light pulse at a high repetition frequency because this system is one-way transmission system.
- Key generation efficiency is twice as high as conventional QKD protocol.
- Free from the backscattering noise because this system is not bi-directional.

In a transmission experiment over a 15-km fiber by way of the optical matrix switch, we obtained a sifted key generation rate of 2k bit-per-second (bps) and a bit error rate (*4) of 6%. A sufficient key generation rate and a bit error rate were obtained to create a fully secure key.
Furthermore, we showed that a weak signal on single photons and large bandwidth data transmission can share the same optical switch, and confirmed the possibility for sending a weak signal for QKD in a commercial photonic network.

Future developments
Since this demonstration is limited to the transmission over a 15-km fiber, the area of application is also bounded. In future, we improve the photon detector and investigate for advancing the system with higher key generation rate and longer distance for transmission. We also proceed with a basic investigation to realize highly secure network with applying quantum cryptography in future optical fiber network including general users.

Glossary
*1 **The World Year of Physics**
The year 2005 celebrating 100 years after Albert Einstein published three revolutionary papers of the photoelectric effect, the Brownian motion, and the special relativity in 1905.

*2 **Planar lightwave circuit (PLC)**
This is a technology to construct the light waveguides made of the core for light propagation and the clad surrounding it on the substrate like Silicon. Various functions can be realized by the design of the waveguides.

*3 **Differential-Phase-Shift Quantum Key Distribution Protocol**
A protocol of quantum cryptography developed by NTT and Stanford University. Compared with the conventional Plug&Play BB84 protocol, which transmits the light in a round-trip mode, this has advantages of one-way transmission, simple setups, and high key generation rate.

*4 **(Quantum) Error rate**
Data error rate originating from the imperfection of the physical system. If this is less than about 10%, the error is eliminated by error-correction algorithm.

- Fig.1 Young's experiment of interferometry and optical switch
- Fig.2 Young's experiments of interferometry with single photons
- Fig.3 Optical switch works with single photons
- Fig.4 Quantum cryptography experiment with optical switch (I)
- Fig.5 Quantum cryptography experiment with optical switch (II)

For further information, contact:
Emi Tamechika and Hirofumi Motai
Planning Division
NTT Science and Core Technology Laboratory Group
Tel: 046-240-5152
E-mail: st-josen@tamail.rdc.ntt.co.jp

Copyright (c) 2005 Nippon telegraph and telephone corporation