Press Release

2008. 3. 26

National Institute of Information and Communications Technology
NEC Corporation
National Institute of Standards and Technology

Longest and fastest quantum key distribution in an installed fiber network

--- Advancement toward realizing cryptographic key distribution with the ultimate information security ---

National Institute of Information and Communications Technology (NICT) has achieved ultra fast quantum key distribution (QKD)* over a 97-km installed telecom fiber. The cryptographic key generation rate was 100 times higher than the previous field experiments and about 10 times higher than the best rate ever reported including laboratory experiments.

Cryptography used in the internet now is public key cryptography. This method is, however, always threatened by advancement of computers, which allows an eavesdropper to decrypt the key with ultrafast computers. In contract, QKD can ensure unbreakable cryptographic scheme regardless of how technologies would advance in future.

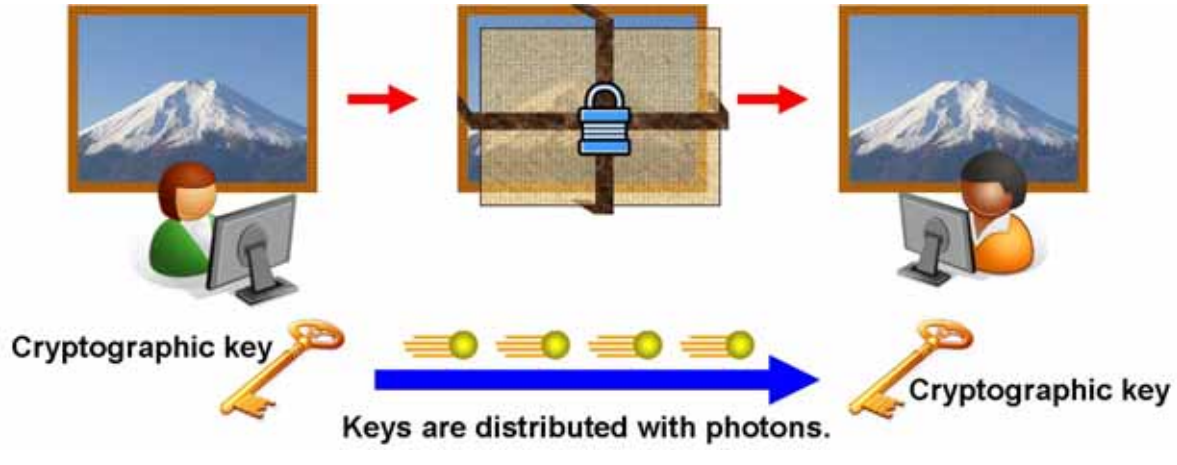
Recently leakage of confidential information from information systems becomes a serious concern. This accelerates an effort to construct a network in which confidential data are managed in a data center, and terminals are linked through secure lines with it. QKD demonstrated here is suitable for such a network.

Most of QKD experiments so far were done in ideal laboratory environment. Our experiment is, however, done in an installed telecom fiber in a city. We have achieved the key generation rate 100 times higher than the previous field experiments, and 10 times higher than the previous labolatory experiments. This is a significant step toward realizing cryptographic key distribution with the ultimate information security.

(This experiment was done in the field test-bed optical fiber network of NICT, called JGN2, with the cooperation of NEC Corporation and National Institute of Standards and Technology (NIST).)

***Footnote**

Cryptographic key : tool to protect information from a sender to receiver against an eavesdropper.
Quantum cryptography : it uses physical properties of photons (particles of light) as cryptographic key.



Background

There has recently been an increasing demand for information security, such as secure e-commerce, personal information protection, leakage protection of confidential information in the internet. Public key distribution which is widely used in the internet now is based on mathematical algorithms that need tremendous time to solve even with supercomputers. This scheme is, however, always threatened by advancement of computers, and also by a possibility of finding new methods to solve, which allow an eavesdropper to decrypt the key.

Quantum cryptography is expected as a next generation cryptography that ensures to be unbreakable regardless of how technologies would advance in future, referred to as unconditionally secure. Quantum cryptography uses physical properties of photons (particles of light) as cryptographic key. A sender and a receiver first share cryptographic key through an optical fiber, and then the sender encrypts information with the key. If someone eavesdrops the key during the key distribution process, it unavoidably leaves traces on the state of photon by the laws of quantum mechanics. The receiver thus can always detect an eavesdropper. This makes the unconditionally secure cryptography possible, regardless of any technological advances in future.

Current status of R&D of quantum cryptography

Practical realization of quantum cryptography is, however, still challenging, because it requires high-techs of controlling photons. Actually in order to implement QKD in installed telecom fiber networks, the receiver must be able to detect photons with low noise in precisely synchronized timing with the sender's clock even under fluctuating field conditions. Most of QKD experiments have so far been done in ideal laboratory environment with bobbin fibers, where the clock was synchronized via short electric cables, referred to as "cunning clock synchronization". Even in such an ideal condition the secure key generation rate have decreased down to a few tens of bits per seconds. Only when one gives up the unconditional security and compromises on the security only for the restricted class of eavesdropping attacks, one can increase the key rate.

Summary of our achievement

We have achieved ultra fast quantum key distribution (QKD) over a 97-km installed telecom fiber with the Bennett-Brassard 84 protocol with decoy states, which was proven to be unconditionally secure. The cryptographic key generation rate was 700 bits per second, which is 100 times higher than the previous field experiments and about 10 times higher than the best rate ever reported including laboratory experiments. This experiment was done in the field test-bed optical fiber network of NICT, called JGN2. The important technologies that made this achievement possible are as follows.

(1) Development of planar light-wave circuit that can cancel disturbance occurring in the transmission process, and can discriminate a key of photon with high visibility.

(2) Development of superconducting single-photon detector that can detect photons with very low noise, high speed, and high stability.

(3) Development of quantum wavelength division multiplexing technique for precise clock synchronization so as not to disturb the transmission of photons through a single fiber.

Impact of our achievement

Our achievement is a significant step toward realizing QKD in practical networks especially for governmental and bank networks with the ultimate information security. Recently leakage of confidential information from information systems becomes a serious concern. This accelerates an effort to construct a network in which confidential data are managed in a data center, and terminals are linked through secure lines with it. QKD demonstrated here is most suitable for such a network.

Future perspective

For practical use of QKD one must realize more stable operation of the system and also increase the key generation rate by a factor of 1000. Our experiment has clarified what kinds of technological issues should be solved toward this goal. It has been within range that QKD systems in the grade of governmental information security could be realized in four or five years. We continue to accelerate research and development of QKD technology, including miniaturization and cost-down of equipments, by strengthen research ties of relevant institutions.

***In this experiment, used were a QKD system developed by NEC in the NICT commission research titled "Research and development for practical realization of quantum cryptography: subject b-1," fast and low noise superconducting single-photon detector developed by the collaboration of NICT and NIST, and quantum wavelength division multiplexing technique developed by NEC, NICT, and NIST. The NICT commission research mentioned above is commissioned to NEC, Mitsubishi Electric Corporation, and NTT.**

Contact information

(1) NICT, Strategic Planning Department, Public Relations Office
Noriyuki Kurihara
Tel：042-327-6923　Fax：042-327-7587
E-mail：publicity@nict.go.jp

(2) NEC, Corporate Communications Division
Kazuhito Ooto
Tel：03-3798-6511 (Direct)
E-mail：k-ooto@bc.jp.nec.com

(3) NICT, Collaborative Research Department, Commissioned Research Promotion Group
Shigeru Amano, and Shunichi Chiba
Tel：042-327-6011（Group）　FAX:042-327-5604

Contact information on research

(1) NICT, New Generation Network Research Center, Advanced Communications Technology Group
Masahide Sasaki
Tel：042－327-6524　Fax：042－327-6629
E-mail：psasaki@nict.go.jp

(2) NEC Laboratory, Research Planning Division, Strategic Planning Group
http://www.nec.co.jp/contact/

Description of experiment

A schematic of our field experiment is shown in Fig. 1. The transmitter and receiver of QKD were set in the Keihanna Open Laboratory of the field test-bed optical fiber network of NICT (JGN2) in Kyoto city. The 97km transmission line was made by 3 round trips through an installed single mode fiber between another terminal in Daianji in Nara city and the Keihanna Open Laboratory. In the transmitter attenuated laser pulse is modulated with 625 MHz repetition In the transmitter, a 1550-nm directly modulated laser diode created 100-ps-wide pulses with a repetition rate of 625 MHz. These pulses were split into a pair of coherent double-pulses with an 800-ps time delay by the planar light-wave circuit. The intensity was adjusted such that less than single photon was in a pulse. These pulsed were decoded by the planar light-wave circuit with four superconducting single-photon detectors.

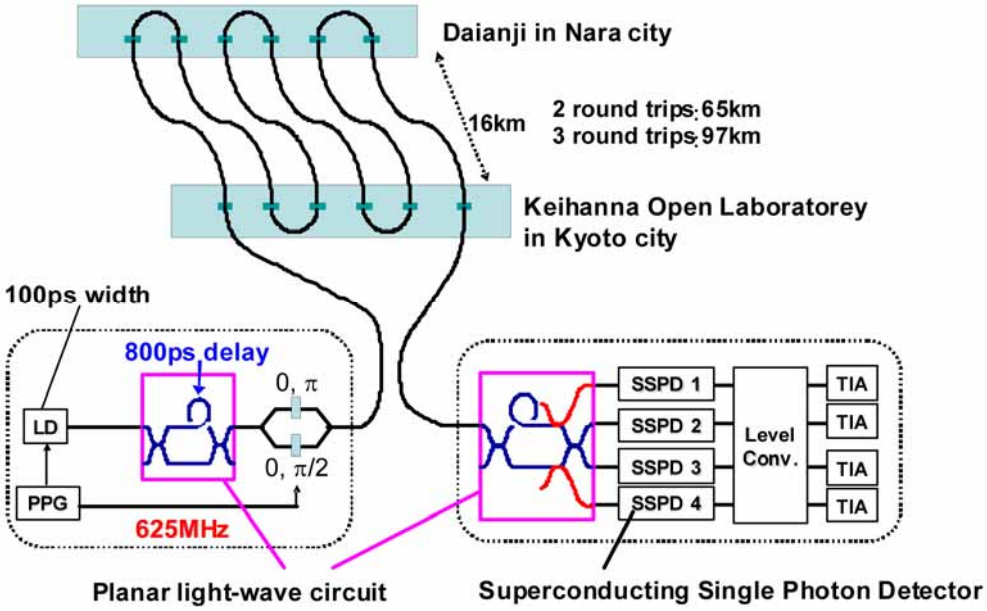


Figure 1 Schematic of the experiment and QKD system with planar light-wave circuit and superconducting single-photon detectors.

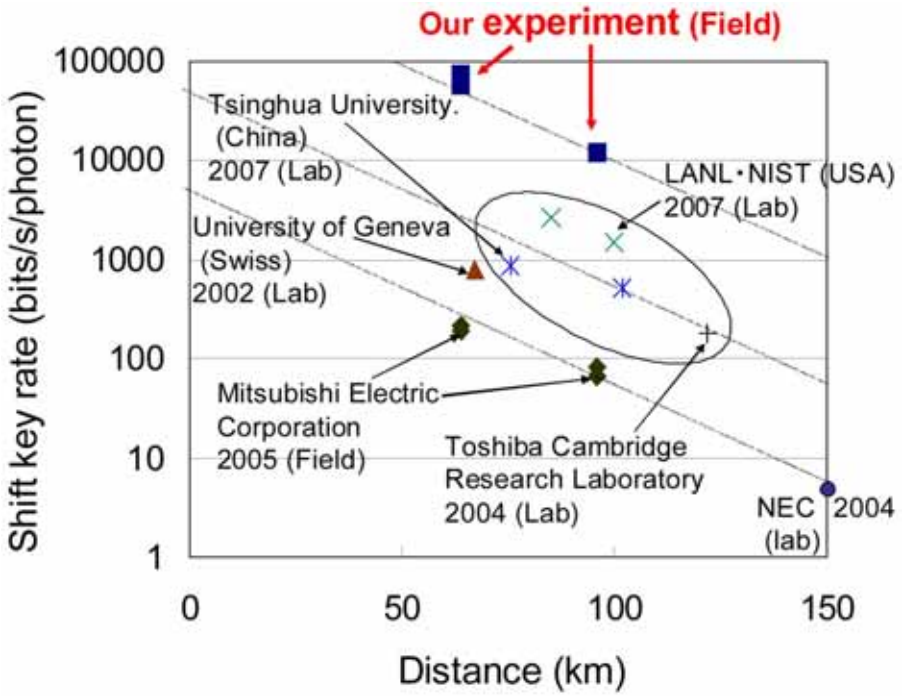


Figure 2 Comparison of the sift key rates per photon for the previous experiments over 60km.

Figure 2 shows comparison of the sift key rates per photon for the previous experiments over 60km. The sift key rate in the vertical axis is the rate of seeds from which the secure key is distilled. We have adopted the sift key rate per photon for comparison with equal footing, even under various differences of experimental conditions and ways of key processing. The key rate was 100 times higher than the previous field experiments and about 10 times higher than the best rate ever reported including laboratory experiments.

Glossary

***1 Bennett-Brassard 84 protocol with decoy states**

The QKD was first proposed by Bennett and Brassard in 1982. In this BB84 scheme, the key is encoded into one of four states which are randomly modulated. Its unconditional security was proven in 1990's. Recently it was found that the security can be enhanced even under some imperfections by adding further random intensity modulation. This is referred to as decoy method.

***2 Superconducting single-photon detector**

It detects single photons by sensing the break of superconducting state of NbN nano wire (100nm width) when a single photon hits the wire. It is possible to detect single photons with much lower noise and shorter time resolution than semiconductor detectors.

***3 Quantum wavelength division multiplexing technique**

QKD requires precise clock synchronization so as not to disturb the transmission of photons through a single fiber. In quantum wavelength division multiplexing technique, quantum channel and classical channel are multiplexed at different wavelengths in appropriate intensity ration, and the receiver applies special filters to eliminate various noises from scattering etc.