3-2 Secure Communication with Quantum Cryptography

HASEGAWA Toshio, NISHIOKA Tsuyoshi, ISHIZUKA Hirokazu, NAMBU Yoshihiro, TOMITA Akihisa, and TAJIMA Akio

Quantum cryptography, which has the advantage of being able to detect eavesdropping on communication channels and security guaranteed by a fundamental physical law, is expected as an absolutely unbreakable cryptography. In 2001, Mitsubishi, NEC and the University of Tokyo started the NICT project "Research and Development on Quantum Cryptography", which includes four research themes: single photon generation, single photon detection, random number generation, and quantum key distribution system. In this paper, we introduce our research activities and some recent results. In Mitsubishi's part, we report the long-distance field trial in a 96-km installed fiber (JGN Ⅱ) and the integrated quantum cryptosystem with existing cryptosystem. In NEC's part, we show fortnight continuous key generation field trial over the 16.3-km commercial access fibers and novel backscattering-free unidirectional QKD system based on planar lightwave circuit platforms.

Keywords
Quantum cryptography, Quantum key distribution, Secure communication, Single photon detection, Field trial

1 Introduction

Quantum cryptography[1] is a technology that offers absolute security in communication. The security of much of modern cryptography is evaluated based on computational complexity theory and cryptanalysis requires massive volumes of calculations. The theoretical basis for this method lies in the assumption that cryptographs requiring such volumes of calculations to decipher are secure. Therefore, modern cryptography may be breakable when ultra-high-speed computers such as quantum computers are realized in the future. Further, modern cryptography is also incapable of detecting eavesdroppers on the communication channel. In contrast, quantum cryptography applies the fundamental principles of physics to maximum effect, offering not only guaranteed transmission security but also solutions to the eavesdropping problem.

In this paper, we introduce the research activities in the NICT project, "Research and Development on Quantum Cryptography", undertaken by the Mitsubishi Electric Corporation, NEC Corporation, and the University of Tokyo, with the aim of putting quantum cryptography to practical use. The main goal of this research project is the development of a long-distance/ high-speed quantum cryptosystem for the telecom wavelength band, and the four items of research are listed below. The research items for theme A to C are the important component technologies of quantum cryptography, and in theme D, the results of the former three are integrated into a total system. Further, theme D is divided into 10 subthemes and researches for which are currently underway by three parties in corporation (See Fig. 1.).

Theme A: Single photon generation technology
Theme B: Single photon detection technology
Theme C: Random number generation technology
Theme D: Technology for a quantum key distribution system

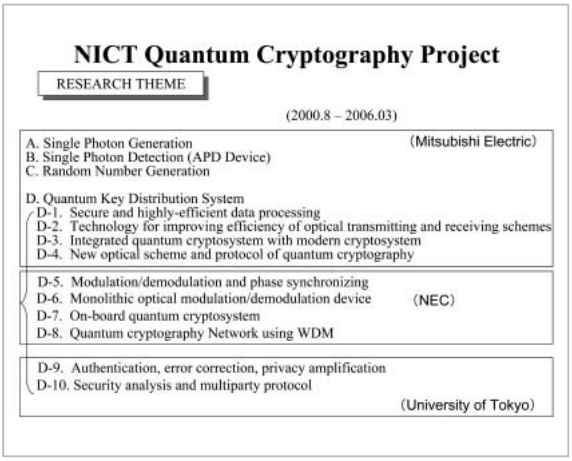

Fig.1 *Items for NICT-commissioned R&D*

2 Research and development of quantum cryptography

2.1 Mitsubishi's research activities

Research on quantum cryptography at the Mitsubishi Electric Corporation began in 1999, and we first succeeded in realizing a short wavelength (830 nm) quantum cryptographic communication system jointly with Hokkaido University in 2000[2]. Since 2001, Mitsubishi has participated in the NICT project entitled "Research and Development on Quantum Cryptography", along with NEC and the University of Tokyo. Mitsubishi is mainly responsible for research and development of technology for "single photon generation", "single photon detection", and "random number generation", as well as "technology for a quantum key distribution system", which integrates the former three. So far major results have included the 1,550-nm high-performance single-photon detectors (dark count probability of approximately 10^{-6}, detection efficiency of approximately 20%)[3], an experiment on a 87-km long-distance quantum cryptographic communication system using these detectors[3] in 2002, and a field experiment of the quantum cryptographic communication system between remote points (Osaka to Kyoto) using an installed 96-km optical fiber in 2004[4]. In development aimed at realizing a higher-speed system, a transmission rate of several tens of kbps has been achieved for a distance of approximately 10 kilometers. Currently, development is underway to achieve 100 kbps over a distance of 100 km. Aside from these results, Mitsubishi also has proposed a "circular-type" quantum key distribution scheme in the area of new optical scheme protocol studies. Compared to conventional methods, this system enables both faster transmissions and multiuser communications, and we confirmed these merits in our actual experiments[5]. Further, Mitsubishi is also active in promoting quantum cryptography technology, through activities such as presentations and showing our quantum cryptosystem at various exhibitions. For example, in 2003, our quantum cryptosystem was demonstrated at ITU Telecom World 2003 in Geneva, Switzerland and the RSA Conference 2005 Japan held in Tokyo, and practical applications such as quantum encrypted secure voice telephone / videophones were presented as useful example applications. This section introduces a 96-km field trial of the quantum cryptosystem and describes an integrated quantum cryptosystem that efficiently combines conventional security systems with quantum cryptography.

The 96-km field experiment

Compared to laboratory experiments, the results of field trials are affected significantly by environmental factors such as temperature variation, vibration disturbance, and loss and reflection at connection points. Before our trial, one using a 67-km optical fiber installed on a lake bottom by the University of Geneva in Switzerland stood as the only practical example of a field trial in this area[6]. Therefore, Mitsubishi Electric developed a quantum cryptosystem suited for a long-distance field trial of up to 100 km, and in November 2004,

a field trial was conducted between two remote points using a 96-km optical fiber installed between Osaka and Kyoto. We designed our system based on three policies intended to overcome the problems specific to field trials—(1) flexible and adjustable instrument setting parameters, (2) stability enhanced by compensating for time shift due to temperature drift and vibration disturbance between two remote points, and (3) compact for portable use. Policy (1) was adopted to allow the unit to adapt flexibly to various experimental environments (such as changes in the communication distance and the need to avoid unpredicted reflection points within an actual installed optical fiber), and for this purpose, several parameters were allowed to have variable settings such as applied voltage, pulse width, delay time, dead time, and laser repletion rate (1–10 MHz). The objective of policy (2) is to realize high-precision optical synchronization with optical transceivers and timing tracking that accommodates the changes to communication path length using it. In policy (3), primarily single photon detectors were designed to be compact and portable.

As shown in Fig. 2, the 96-km field trial was conducted using the installed fiber of the Japan Gigabit Network Ⅱ (JGNⅡ) optical fiber testbed, between Dojima, Osaka and Keihanna, Kyoto (we utilize Daianji, Nara as the relay-point to construct a 96-km fiber line). In our experiments we constructed the communication channel of 96 km of single mode fiber (SMF) without low-noise optical amplifiers. The following conditions were selected for the experiment: a modified Plug & Play set-up[2]-[4] for the optic scheme, the BB84[1] protocol, a laser repetition frequency of 1 MHz, and an average photon number of 0.1, as generally adopted in other previous experiments. The detectors were cooled to approximately 200 K to achieve a low dark count probability of about 10^{-6} for a long-distance transmission. As a result, we were able to achieve a key-sharing rate of 8.2 bps (QBER 9.9%) for a communication distance of 96 km, and confirmed that our secure cryptographic communication under this scheme can work. Most experiments in past studies were conducted in the laboratory, but recently some examples of long-distance field trials between two remote points have been reported, such as the 67-km experiment by the University of Geneva[6], the 96-km experiment by Mitsubishi Electric[4], and a 125-km experiment in China[7]. Since a one-way quantum key distribution scheme is better suited for long-distance experiments, most past experiments have selected this approach rather than a two-way scheme (plug&play scheme), which has higher stability but is affected significantly by backscattering. Thus, as a round-type key quantum distribution field experiment, the 96-km experiment by Mitsubishi holds the record for the longest distance.

An integrated quantum cryptosystem with high-speed modern cryptography

Quantum cryptography enables absolutely secure cryptographic communication. Here,

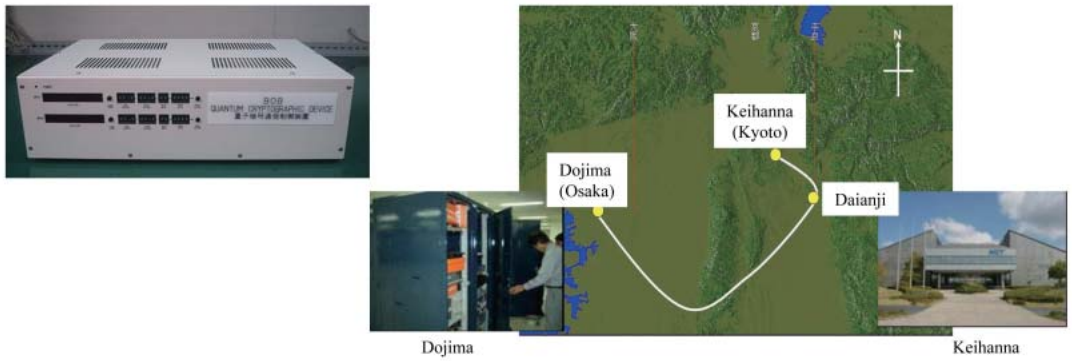

Fig.2 *Our quantum cryptosystem and field experiment location*

after we generate plenty of keys and share these keys between two end users, we encrypt the plaintext and send it with a key of the same length, using a One-Time Pad. However, since the key required for this scheme must be of the same length as the plaintext, the rate of cryptographic communication will be on the same order as the key-sharing rate (at present, approximately 100 Kbps at most) when the One-Time Pad is used. Thus, strategies must be contrived to produce a practical quantum cryptosystem that will increase the speed of cryptographic communication, such as (1) an increase in the key-sharing rate itself of the quantum cryptosystem and (2) construction of a practical system that balances security and speed by integrating quantum and modern cryptographic methods. At Mitsubishi, research and development have been conducted not only on the former but also on the latter strategy, to produce a practical integrated quantum cryptosystem with conventional security systems that exploits both the absolute security of quantum cryptography and the high speed of modern cryptography. This approach was taken under the assumption that quantum cryptography will not immediately replace conventional security methods, and that both quantum and modern cryptography will coexist for some time. This integrated system will expand the applicability of quantum cryptography and is expected to accelerate its integration into the existing security infrastructure. In the integrated quantum cryptosystem developed by Mitsubishi[3], the security and speed of cryptographic communication are selected by the user according to the situation. In other words, the user may select an encryption algorithm from among symmetric key encryption algorithms (such as DES, MISTY, Camellia, AES, etc.) in addition to the One-Time Pad. It is also possible to select several operational modes (e.g., key-fixed mode, dynamic-key-changing mode, rate-fixed key changing mode). Figure 3 shows an example of the software interface of our system.

When absolute security is required, quantum cryptography may be combined with a One-Time Pad, and when only a practical level of security is required, priority is given to transmission speed, and only the key needs to be sent with absolute security, a combination of quantum cryptography and symmetric key encryption scheme will be the system of choice. In the latter case, the security level may be specified in more detail by choosing an operation mode. In key-fixed mode, the shared key is fixed for a certain length of time, while in dynamic-key-changing mode, the shared key is updated every time a quantum cryptosystem generates a key of the same length (for example, 128 bits). In rate-fixed key changing mode, to realize stricter encryp-

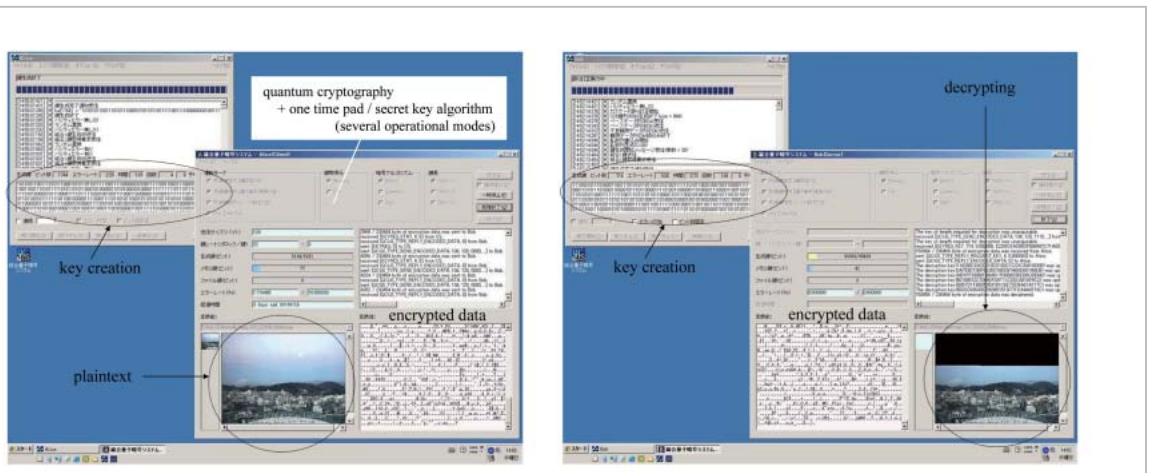

Fig.3 *Software interface of our quantum cryptosystem (Left: encryption on the sender side; right: decryption on the receiver side)*

tion, we can control the number of blocks that may be encrypted by the same key. In the last case, the security level increases when smaller rates (i.e., smaller numbers of blocks) are selected, but this is done generally at the expense of processing speed.

These systems present an approach to resolving the question of how quantum cryptography may be integrated with conventional security systems to create a practical new structure. We may also conclude that the security of conventional cryptosystems may be enhanced through the incorporation of quantum cryptography.

2.2 R&D activities at NEC Corporation

The NEC Corporation began research on quantum information technology in 1998. Initially, the main focus was on experimental studies on entangled photon pairs and theoretical studies on quantum cryptographic protocols. NEC has also been active in promoting this field, and in 1999, NEC Japan held the world's first workshop on quantum cryptography with the NEC Research Institute, Inc. (NECI). At this workshop, the Shor-Preskill method, which is the standard security proof for quantum cryptography, was first presented. Since 2001, NEC has been commissioned under the NICT project entitled "Research and Development on Quantum Cryptography", along with Mitsubishi Electric Corporation and the University of Tokyo, specifically conducting research on quantum cryptosystems. In this project, efforts were particularly focused on quantum cryptographic transmission technologies for single photons, and technologies for stable modulation/demodulation of single-photon-level signals have since been developed both on the device and instrument levels. Using the high-sensitivity differential single-photon detector developed by NEC and the Japan Science and Technology Agency[8] in combination with a monolithic interferometer, NEC has succeeded in a 150-km optical fiber transmission experiment, at a distance that challenged the limits of quantum cryptographic transmission, as well as cryptographic key generation over a distance exceeding 100 km[9]. At the same time, NEC acknowledged the practicability of the Metro-Network and devoted efforts accordingly to the development of an instrument that can operate stably at high speeds[10]. In particular, NEC has been successful in key generation at 100 kbps after transmission over 40-km optical fiber using the results of their development efforts, such as technologies enabling stable operation under variable conditions, technologies to ensure high reliability, and a high-precision automatic synchronization system that can compensate for delay-time variations over the transmission path. Further, using this system, NEC has succeeded in automatic, continuous key generation during a period of 14 days using commercial aerial fibers. They have also produced a highly reliable system incorporating the adoption of one-to-multiple key distribution and backup switching during emergencies. The company is also actively taking part in promoting quantum cryptographic technologies by participating in various exhibitions, such as NICT research presentation meetings aimed at demonstrating the actual instruments. This report introduces a validation experiment for the management of an ultra-fast quantum cryptographic communication system under actual operational conditions for a period of 14 days in the field, as well as the technology for secret key distribution in a one-way quantum cryptosystem using a planar light wave circuit for distances exceeding 100 km. This experiment was designed and the associated technology was examined to investigate the overall feasibility of high-speed, long-distance communication systems.

Development of high-speed quantum cryptographic communication systems

In order to employ quantum cryptographic technologies in practical quantum cryptographic communication systems, it is necessary to confirm by experiment (i) the stable transmission and reception of single-photon signals over extended time periods and (ii) the seamless generation of the final key from the

photon transmission, all under actual operational conditions (laboratory conditions for instruments, field conditions for optical fiber transmissions). These requirements led to the development of technologies for (1) a practical stabilization system and (2) a continuous key generation system[11].

(1) A practical stabilization system

To achieve instrument characteristics that are not dependent on operational temperature and to ensure stable operation over extended periods, a temperature-independent interferometer technology using alternate-shift phase modulation[12] and a highly-reliable compact photon receptor module that operates over a wide temperature range[13] were developed.

(2) Continuous key generation system

In actual operational conditions, large variations in the delay time in the transmission paths are observed due to changes in climate conditions, such as temperature. In order to ensure that final-key generation is carried out seamlessly from photon transmission even under such conditions, a technology for a continuous key generation system consisting of high-precision bit synchronization[14][15], frame synchronization[16], fault detection, and re-synchronization technologies[16] have been established.

An instrument has been created by assembling systems (1) and (2) in a 19-inch rack (dimensions 480 × 180 × 375mm^3). This instrument was placed under normal laboratory conditions and connected to a 16.3-km access optical fiber (in which most sections are aerial), and a long-distance continuous final-key generation experiment was conducted for 24 hours a day over a 14-day period. The experimental configuration is shown in Fig. 4. The results showed that continuous final-key generation was successful for the entire 14-day period without manual adjustments. As shown in Fig. 5, the mean quantum bit error rate and mean final-key generation rate were 7.5% and 13.0 kbps, respectively. Based on these results, we can conclude that the practicability of the quantum cryptosystem has been verified.

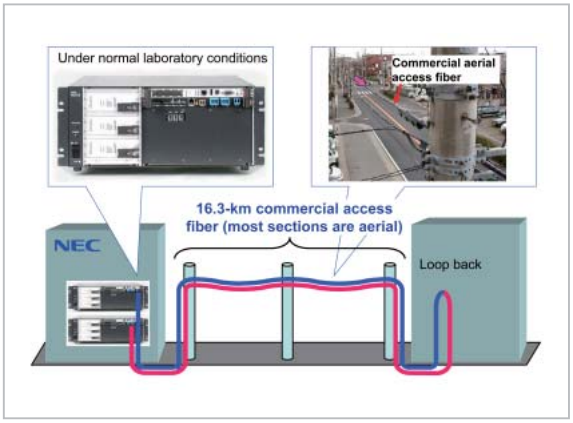

Fig.4 *Experimental configuration*

Development of a one-way quantum cryptographic communication system based on PLC

Since the Plug & Play System is an optical two-way system, it is susceptible to back-scattering light within the optical fiber transmission path and is not suitable for long-distance or high-speed key distributions. In order to overcome this problem, we have developed a one-way quantum cryptosystem based on planar light wave circuit technology[10]. The system is based on a weak-light interferometer system consisting of two planar light wave circuits (PLC) in an asymmetrical Mach-Zehnder interferometer system. By independently controlling the temperature of the two PLCs with a precision of 0.01˚C, it is possible to maintain stable optical interference for over an hour, independent of the polarization characteristics inside the optical fiber. On the transmission side, the key information is encoded using two phase modulators, and on the receiver side, the information is decoded using one phase modulator and two photon detectors. A final key with increased security may be extracted by combining this system with ex-post communication.

Figure 6 presents the results of evaluation of quantum key transmission in the laboratory. The relationship between key generation rates and transmission fiber length are shown using a semi-log plot for cases in which detective quantum efficiencies (DQE) of the photon detector are 10% and 5%. The filled circles

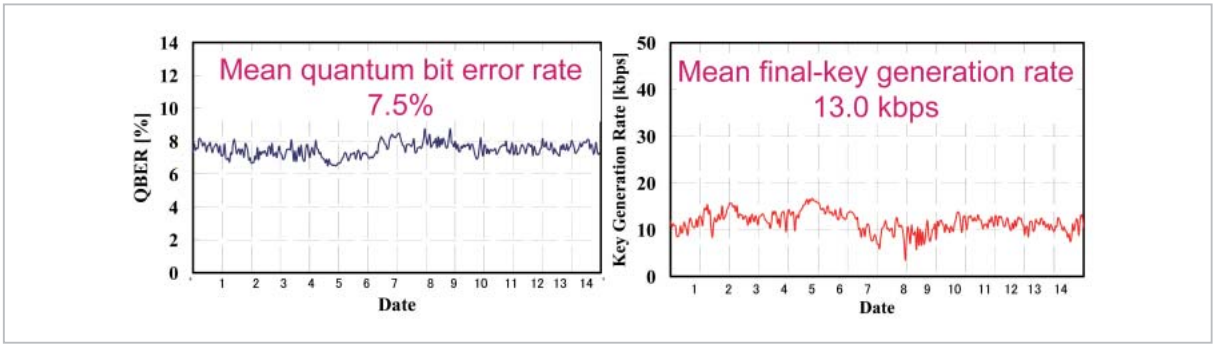

Fig.5 *Transition of quantum bit error rate and final-key generation rate*

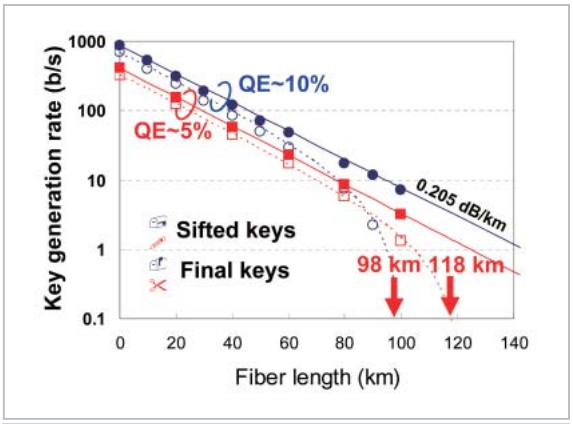

Fig.6 *Results of evaluation of quantum key transmission*

and squares represent the generation rates of shared shifted keys, and open circles and squares represent the generation rates of the final keys. The sorted key generation rates decrease exponentially with increasing fiber length due to fiber loss. The dashed lines form a trend curve of the final-key generation rate calculated from a separately measured bit error rate. The maximum distance of transmission was 98 km at a DQE of 10%. At a DQE of 5%, it was possible to increase the distance to 118 km by improving the S/N ratio of the detector at the expense of the key generation rate. The results of the experiment verified the feasibility of practical application of the long-distance quantum cryptography system to distances exceeding 100 km.

3 Conclusions

This paper introduced the activities and results of the NICT project entitled “Research and Development on Quantum Cryptography” undertaken by the Mitsubishi Electric Corporation, NEC Corporation, and the University of Tokyo beginning in 2001. In the section on Mitsubishi, we reported on a long-distance field trial in a 96-km installed optical fiber network (JGNⅡ) and an integrated quantum cryptosystem incorporating conventional cryptosystems. In the section on NEC, we presented the results of a 14-day continuous key-generation field test over 16.3-km commercial aerial access fibers and described progress in the development of a novel backscattering-free one-way quantum key transmission system based on PLC platforms.

Although not dealt with in this paper, in the area of single-photon generation technology, we have constructed a heralded single photon source for the telecom wavelength employing a parametric down conversion[17] in collaboration with Hokkaido University. Further, in the area of single-photon detection technology, we have designed and developed an avalanche photo diode (APD) suited for quantum cryptography based on the results of an investigation of methods of suppressing surface leakage current and methods of improving detection efficiency. In the area of random number generation, we have investigated and developed incorporating random number evaluation systems, pseudorandom number generation devices, and physical random number generation devices into our quantum cryptosystem. Further, in terms of data processing technology such as error correction and privacy amplification, Mitsubishi Electric

and the University of Tokyo have worked jointly to investigate and evaluate a novel and highly efficient method for error correction using low density parity check (LDPC) codes[18]. The method has been implemented in a quantum cryptosystem and its practicability has been confirmed. With respect to security, the University of Tokyo has performed an evaluation of quantum cryptosystems developed by two companies, and in the final stretch of the commissioned project, Mitsubishi Electric and NEC succeeded in an interconnection experiment using their different quantum cryptosystems, thus integrating the results of the various research themes and the achievements of the three organizations.

Acknowledgments

Part of this research has been carried out under the "Research and Development on Quantum Cryptography" project of the NICT as part of the Ministry of Internal Affairs and Communications of Japan's "R&D on Quantum Communication Technology" program. We are grateful to Professor Hideki Imai of the University of Tokyo (presently at the National Institute of Advanced Industrial Science and Technology and Chuo University), which is participating in the commissioned research, and to all who have participated in the project. We would also like to thank Assistant Professor Shigeki Takeuchi of Hokkaido University, who is conducting joint research with us, and POWERDCOM, Inc. (presently KDDI Corporation) for allowing us use of their access fiber during our experiment.

References

1 C.H.Bennett and G.Brassard, "Quantum cryptography: Public key distribution and coin tossing", in Proc. Int. Conf. Computers, Systems and Signal Processing, Bangalore, India 175, 1984.

2 T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, K.Shimizu, and M.Matsui, "An experimental realization of quantum cryptosystem", IEICE Trans. Fundamentals , E85-A No.1, 149, 2002.

3 T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, M.Matsui, and S.Takeuchi, "Experimental realization of quantum cryptosystem over 87 km", CLEO/QELS2003, QTuB1, Baltimore 2003. T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, M.Matsui, and S.Takeuchi, "Experimental realization of long-distance quantum cryptosystem", SCIS2003, 14D-1, 2003.

4 T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, K.Shimizu, and M.Matsui, "Field experiments of quantum cryptosystem in 96 km installed fibers", CLEO/Europe-EQEC2005, EH3-4, Munich 2005. T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, K.Shimizu, and M.Matsui, "Experiments of quantum cryptosystem in 96km installed fibers", SCIS2005, 2F1-3, 2005.

5 T.Nishioka, H.Ishizuka, T.Hasegawa, and J.Abe, " 'Circular type' quantum key distribution", IEEE Phot. Technol. Lett., Vol.14, No.4, 2002.

6 D.Stucki, N.Gisin, O.Guinnard, G.Ribordy, and H.Zbinden, "Quantum key distribution over 67 km with a plug and play system", New J.Phys., 4, 41, 2002.

7 X.Mo, B.Zhu, Z.Han, Y.Gui, and G.Guo, "Faraday-Michelson system for quantum cryptography", Opt. Lett. 30, 2632, 2005.

8 A. Tomita and K. Nakamura, "Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm", Opt. Lett. 27, 1827-1829, 2002.

9 Y. Nambu et al., "One-way Quantum Key Distribution System based on Planar Lightwave Circuits", to be appeared in Jpn. J. Appl. Phys.

10 A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, T.Takeuchi, A. Tomita, and Y. Nambu, "A High-Speed Quantum Cryptosystem", OCS2005-13, 2005.
11 A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, Y. Nambu, and A. Tomita, "Continuous Key Generation Technologies for Practical Quantum Cryptosystems", Proceeding of CPT2006, J-2, pp.191, 2006.
12 A. Tanaka, A. Tomita, A. Tajima, T. Takeuchi, S. Takahashi, and Y. Nambu, "Temperature independent QKD system using alternative-shifted phase modulation method", Proceeding of ECOC2004, Tu4.5.3, 2004.
13 S. Takahashi, A. Tanaka, W. Maeda, A. Tajima, T. Takeuchi, and A. Tomita, "A minimized Photon Receiver for a high-speed quantum cryptosystem", OPE2005-26 LQE2005-25, 2005.
14 W. Maeda, A. Tajima, A. Tanaka, S. Takahashi, and T. Takeuchi, "High-speed QKD system synchronized by automatic phase-alignment mechanism", Proceeding of OFC2005, OWI4, 2005.
15 W. Maeda, A. Tanaka, S. Takahashi, and A. Tajima, "Automatic Installation in QKD System Using Photon-Counting Optical Power Meter", Proceeding of OFC2006, JThB21, 2006.
16 A. Tanaka, W. Maeda, A. Tajima, and S. Takahashi, "Fortnight Quantum Key Generation Field Trial using QBER monitoring", LEOS2005 WM2, 2005.
17 A.Soujaeff, S.Takeuchi, K.Sasaki, T.Hasegawa, and M.Matsui, "Heralded single photon source for quantum cryptography at 1550 nm", CLEO/Europe-EQEC2005, EG-10, Munich, 2005. A. Soujaeff, S.Takeuchi, K.Sasaki, T.Hasegawa, and M.Matsui, "Heralded single photon source at 1550nm from pulsed parametric downconversion", to be appeared in J.Mod. Opt., 2006.
18 Y.Watanabe, W.Matsumoto, and H.Imai, "Information reconciliation in quantum key distribution using low-density parity-check codes", in Proceedings of ISITA2004, 1265, 2004.
19 Y.Watanabe, W.Matsuimoto, and H.Imai, "Error correction in quantum key distribution using low-density parity-check codes", SCIS2003, 15D-1, 2003. H.Ishizuka, W.Matsumoto, H.Fukushima, T.Shimada, H.Arai, T.Hasegawa, and T.Nishioka, "Evaluation of LDPC code for quantum cryptography", SCIS2004, 2A1-5, 2004.
20 T.Turumaru, "Implementable Quantum Bit-String Commitment Protocol", Phys. Rev. A 71, 012313, 2005.
21 T.Nishioka, T.Hasegawa, H.Ishizuka, K.Imafuku, and H.Imai, "How much security does Y-00 protocol provide us?", Phys. Lett. A 327, 29, 2004.

HASEGAWA Toshio

Head Researcher, Information Technology R&D Center, Mitsubishi Electric Corporation

Information Security, Quantum Information Technology

ISHIZUKA Hirokazu

Head Researcher, Information Technology R&D Center, Mitsubishi Electric Corporation

Information Security, Quantum Information Technology

***TOMITA Akihisa**, Ph.D.*

Principal Researcher, Fundamental and Environmental Research Laboratories, NEC Corporation

Quantum Information Technology

***NISHIOKA Tsuyoshi**, Ph.D.*

Head Researcher, Information Technology R&D Center, Mitsubishi Electric Corporation

Information Security, Quantum Information Technology

***NAMBU Yoshihiro**, Ph.D.*

Principal Researcher, Fundamental and Environmental Research Laboratories, NEC Corporation

Quantum Information Technology

TAJIMA Akio

Principal Researcher ,System Platforms Research Laboratories, NEC Corporation

Optical Communication System