Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments

Yasuhiro Tokura[†] *and Toshimori Honjo*

Abstract

NTT Basic Research Laboratories has been researching and developing differential phase shift quantum key distribution (DPS-QKD), a new QKD protocol. This article introduces the basics of this protocol, proof-of-principle experiments, the development of a prototype system, and a field experiment done at the Tokyo QKD Network demonstration in October 2010.

1. Differential phase shift quantum key distribution (DPS-QKD)

Quantum key distribution (QKD), which is a cryptosystem that uses the principles of quantum mechanics, has recently been attracting much attention as a way to achieve ultimate security in communication. In 2003, NTT and Stanford University jointly proposed differential phase shift quantum key distribution (DPS-QKD) [1], which uses the fact that only part of the relative phase information of attenuated light pulses can be read out. The setup and protocol of DPS-QKD are shown in **Fig. 1**.

First of all, the sender (called Alice) prepares a coherent pulse train and modulates the relative phase of the light pulses randomly with 0 or π. The light is then sent to the receiver (Bob) after being attenuated such that the number of photons per pulse is less than 1. Bob uses a one-pulse delay interferometer to cause successive pulses to interfere and measures the relative phase information with a set of photon detectors located at the interferometer's outputs. Since the source photon power is weak, only part of the relative phase information can be read out, but the obtained relative phase should be exactly the same as the phase modulations at the sender. Bob records the timestamp when a photon was detected and which of the detectors clicked (relative phase information itself). He then generates a key by assigning bit 0 to relative phase 0 and bit 1 to relative phase π. Bob then sends back to Alice only the timestamp information. Alice uses this information and her phase encoding records to generate a key, which is called the sifted key*. Finally, after error-correction and privacy-amplification processes, final secure keys are generated and used in cryptic communication.

2. Proof-of-principle experiments

We have demonstrated the principle of this protocol and evaluated the limits of the key distribution distances and key generation rates using real optical fibers. The experimental setup is shown in **Fig. 2**. Alice modulates the intensity of the light from a laser with a wavelength of 1551 nm to generate 1-GHz repetition pulses. Random phases 0 or π are encoded using a pulse pattern generator. After the light intensity has been adjusted to 0.2 photons per pulse on average, the pulses are sent into an optical fiber. Bob receives the light pulses from Alice and inputs them to a one-pulse delay interferometer and detects photons with the two single-photon detectors

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan

* Sifted key: The sifted key is the initial raw key generated through photon transmission using a QKD protocol such as DPS-QKD or BB84. It has some errors due to system imperfections, so the final key is distilled through the error-correction and privacy-amplification processes.

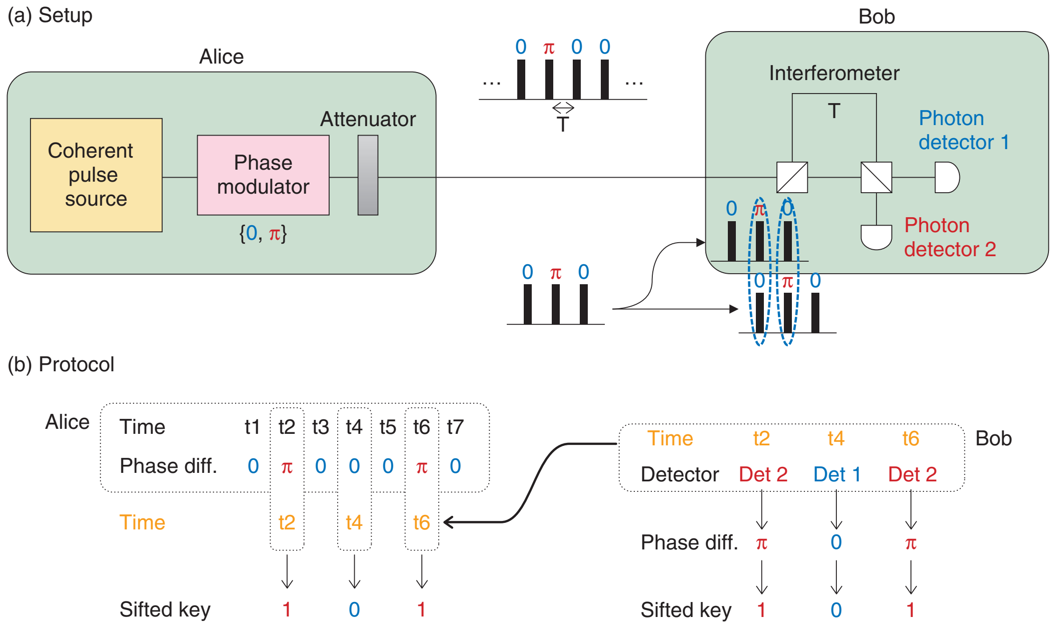

Fig. 1. Setup and protocol of DPS-QKD.

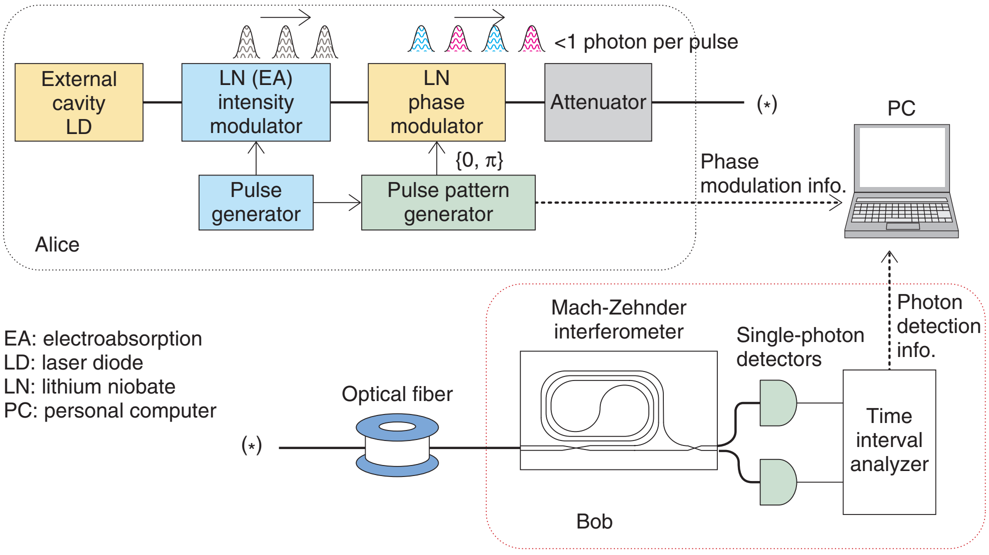

Fig. 2. Setup for the proof-of-principle experiments.

positioned at the interferometer's outputs. A time interval analyzer records the photon detection time and information about which of the detectors clicked. The sifted key is generated from this record by the abovementioned protocol, and the key generation rates and error rates are estimated.

The main issues so far have been the stability of the interferometer and the performance of the photon detectors. To obtain stable photon interference, we used a Mach-Zehnder interferometer (MZI) based on planar lightwave circuit (PLC) technology using quartz glass waveguides; this technology was developed by NTT. Since the optical path difference was ten times longer than that of conventional optical

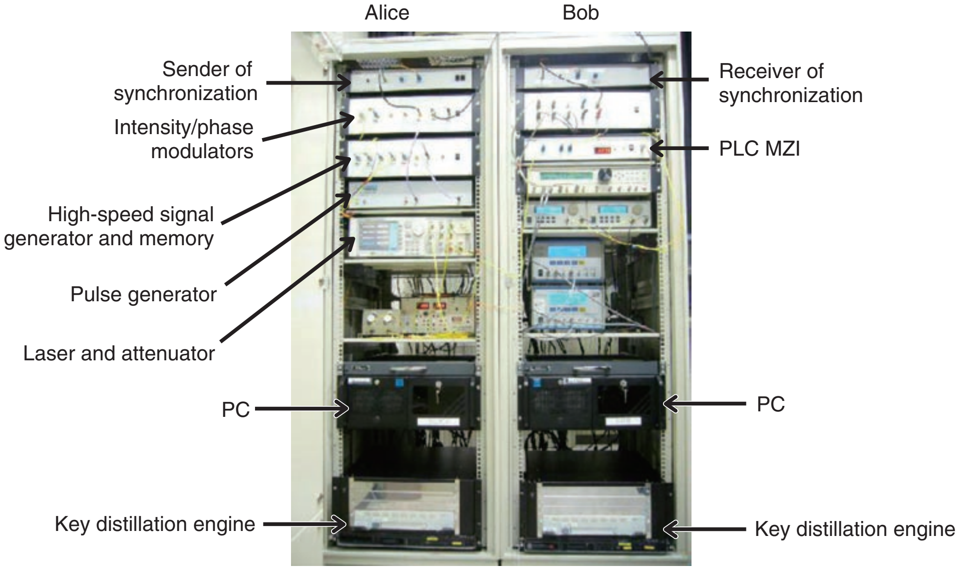
Alice
Bob
Sender of synchronization
Intensity/phase modulators
High-speed signal generator and memory
Pulse generator
Laser and attenuator
PC
Key distillation engine
Receiver of synchronization
PLC MZI
PC
Key distillation engine

Fig. 3. Prototype system.

communications, stabilization had previously been a problem, but this PLC MZI showed an extinction ratio of more than 20 dB (corresponding to a bit error of less than 1%), which enabled us to perform a successful demonstration. As for the photon detectors, performance improvement accompanies the use of a longer key distribution length. The first demonstration in 2004 used an InGaAs avalanche photodiode (APD), and 100-km distribution was demonstrated using a photon detector system by converting long-wavelength photons to a shorter wavelength and detecting them with a fast, high-efficiency Si photon detector [2]. In 2007, we succeeded in achieving 200-km distribution with superconductor-based single-photon detectors, which enabled us to raise the repetition frequency to 10 GHz [3].

As shown in Fig. 1, this protocol requires huge random numbers. While a pseudo-random generator is usually used, a fast physical random generator is necessary to improve the security. Recently, a random generator with a generation rate of more than 1 Gbit/s using chaotic fluctuations of laser light has been developed and applied to DPS-QKD experiments [4].

3. Prototype system

DPS-QKD has been confirmed through several experiments, and we have started developing a prototype system. Its appearance is shown in **Fig. 3**. For the prototype implementation, we developed a high-speed signal generator and its memory unit using a field programmable gate array (FPGA). This is on Alice's side for generating signals to modulate the phase and for keeping them until the key generation stage. As in the proof-of-principle experiments, Alice modulates the intensity of the laser light to generate a 1-GHz pulse train and then modulates the relative phases depending on the phase signal from the FPGA board. After being attenuated, the pulses are sent to Bob. On Bob's side, the relative phases are detected with a PLC MZI and single-photon detectors, and the obtained signal is continuously retrieved by a time-interval analyzer and fed to a personal computer, where a sifted key is generated. At the same time, only the detection time is sent to Alice via a network. Alice extracts the phase information stored in the FPGA board according to Bob's detection times and generates a sifted key. Finally, the sifted keys on both sides are sent to the key distillation engine (developed by NEC), which executes error correction and privacy amplification and generates the final secret key for cryptic communication.

4. Field experiments

With our prototype system, we participated in a testbed network experiment called Tokyo QKD Network [5], led by the National Institute of Information and Communications Technology (NICT). The

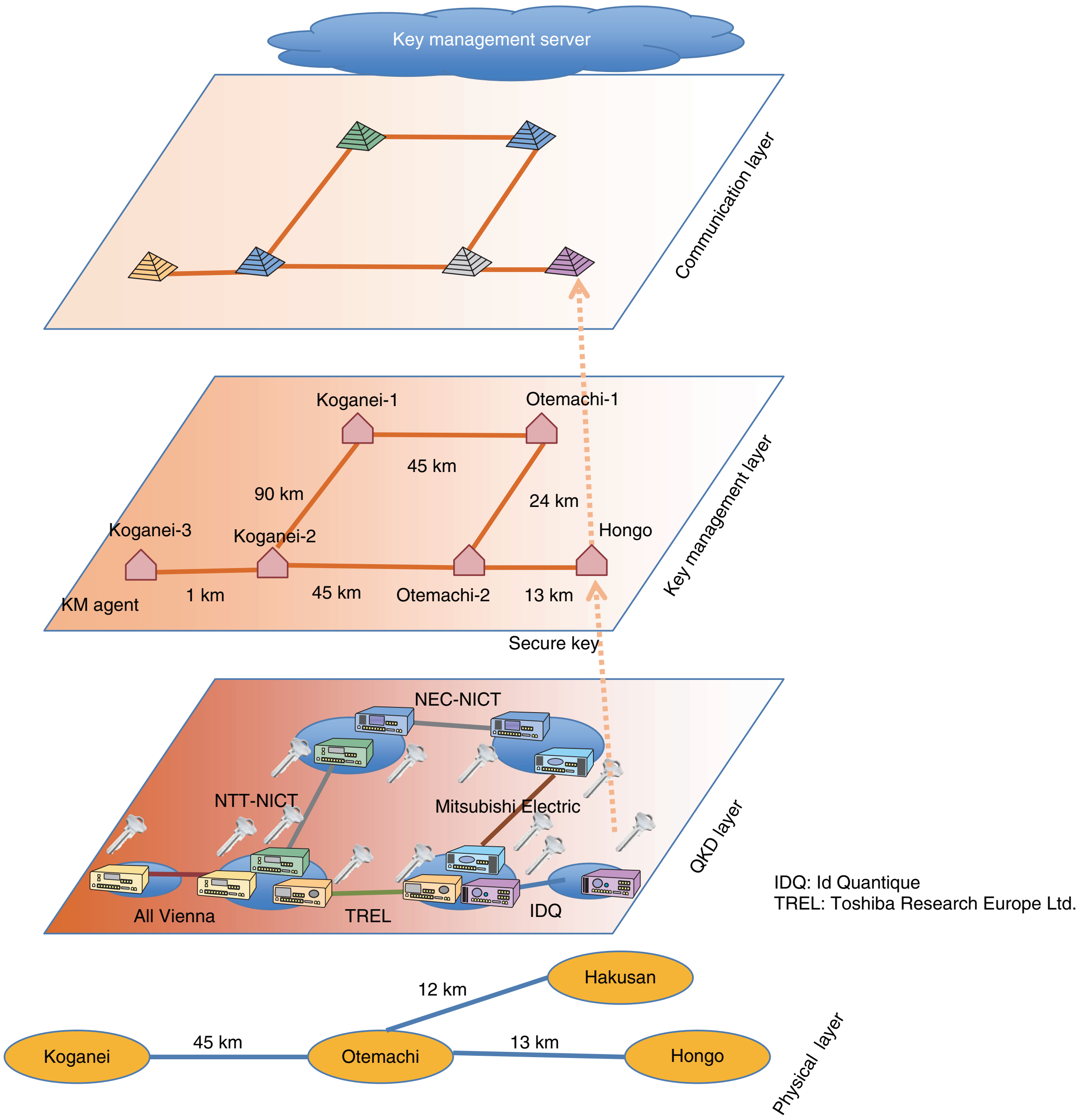

Fig. 4. Structure of Tokyo QKD network.

participants were NEC, Mitsubishi Electric, NTT supported by NICT, Toshiba Research Europe, Id Quantique (Geneva), and the All Vienna team. This QKD network was constructed using the testbed optical fiber network JGN2plus, connecting nodes at Otemachi, Koganei, Hakusan, and Hongo.

The network structure of this experiment is shown in **Fig. 4**. The transmission distances were Otemachi to Koganei: 45 km, Otemachi to Hakusan: 12 km, and Otemachi to Hongo: 13 km. There are many fibers in parallel on the Koganei-Otemachi, Otemachi-Hakusan, and Otemachi-Hongo routes and various network topologies are configured.

The lower layer, called the QKD layer, had six nodes; each team put its equipment at the nodes at both ends of a link. The QKD layer was constructed over the physical layer. For example, NTT used 90 km of fiber between Koganei and Otemachi in a loopback configuration, NEC used 45 km of fiber between Koganei and Otemachi, Mitsubishi used 24 km of fiber between Otemachi and Hakusan in a loopback configuration, and ID Quantique used 13 km fiber between Otemachi and Hongo.

The secret key generated by QKD was supplied to the local key management agent and moved up to the key management layer. The key stored in the key management agent was used for cryptic communications such as a videoconference and voice communication. Between nodes that were not directly connected, the key was exchanged by being repeated at intermediate nodes.

NTT, in collaboration with NICT, was in charge of the longest loop-back segment used in the experiment (about 90 km). With the combination of our prototype system and the superconducting single-photon detectors developed by NICT, we were able to achieve stable key distribution. The stability test of sifted key generation was successfully run for about 8 days, with average generation rate of 18 kbit/s and average bit error rate of 2.2%. The stability test of final key generation including error correction and privacy amplification ran stably for about 4 hours, with a generation rate of 2.1 kbit/s. At an international conference (Updating Quantum Cryptography and Communications, UQCC) [6] in Oct. 2011, this QKD network demonstrated live detection of eavesdropping and subsequent automatic changeover to the redundant standby route, enabling an ultimately secure videoconference.

References

[1] K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution Using Coherent Light," Phys. Rev. A, Vol. 68, No. 2, 022317, 2003.

[2] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km Differential Phase Shift Quantum Key Distribution Experiment with Low Jitter Up-conversion Detectors," Opt. Express, Vol. 14, No. 26, pp. 13073–13082, 2006.

[3] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum Key Distribution over a 40-dB Channel Loss Using Superconducting Single-photon Detectors," Nature Photonics, Vol. 1, No. 6, pp. 343–348, 2007.

[4] T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift Quantum Key Distribution Experiment Using Fast Physical Random Bit Generator with Chaotic Semiconductor Lasers," Opt. Express, Vol. 17, No. 11, pp. 9053–9061, 2009.

[5] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, "Field Test of Quantum Key Distribution in the Tokyo QKD Network," Opt. Express, Vol. 19, No. 11, pp. 10387–10409, 2011.

[6] http://www.uqcc2010.org/

Yasuhiro Tokura

Executive Manager, Optical Science Laboratory, NTT Basic Research Laboratories.

He received the B.S., M.S., and Ph.D. degrees from the University of Tokyo in 1983, 1985, and 1998, respectively. In 1985, he joined NTT Musashino Electrical Communications Laboratories, where he engaged in research on semiconductor nanoscience, quantum transport, and quantum information science. From 1998 to 1999, he was a visiting scientist in the Department of Applied Physics, Technical University of Delft, The Netherlands. Since 2004, he has been the group leader of the Quantum Optical State Control Research Group and a guest professor at Tokyo University of Science. Since 2010, he has also been a guest professor at the National Institute of Informatics.

Toshimori Honjo

Senior Research Engineer, Distributed Data Processing Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in information science from Tokyo Institute of Technology in 1996 and 1998 and the Ph.D. degree in engineering from Osaka University in 2007, respectively. In 1998, he joined NTT Software Laboratories, Musashino, where he engaged in research on the design and implementation of a network protocol stack in operating systems for secure mobile communications. From 2003 to 2010, he engaged in research on quantum optics and quantum key distribution at NTT Basic Research Laboratories. In 2009, he was a visiting researcher at the University of Vienna, Austria. Since 2010, he has been engaged in R&D of a large-scale distributed parallel data processing infrastructure. He moved to NTT Information Sharing Platform Laboratories in April 2011.