Quantum Key Distribution Technology

Yasuhiro Tokura†

Abstract

Quantum key distribution provides the highest security in the communication channel by using the principle of quantum mechanics. This article briefly reviews recent trends of this technology and the status of NTT's research. The following articles give more details.

1. Introduction

Quantum mechanics, born in the early 20th century, has established itself as the fundamental principle controlling various types of nanoscale physics, from electronics as in transistors to molecules and biomaterials. In the 20th century, another rapidly developing field emerged: information and communications technology (ICT). Recently, much attention had been attracted to a new research field, quantum information and communications technology (QICT), which is based on these two seemingly barely interrelated fields. QICT provides a deeper understanding of quantum mechanics via new approaches for verifying its principles, as well as completely new functionalities that cannot be realized by *classical* ICT, for example, enabling us to solve extremely difficult problems in a short time by using quantum computers and to have completely secure communication by quantum key distribution and quantum certification. Among different quantum media from elementary particles to macroscopic quantum states such as superconducting states, the quantum of light, the photon, is the most suitable candidate for quantum communication. The most fundamental form of quantum communication, quantum key distribution (QKD), enables secret keys to be shared between two remote parties through the sending of photons with information encoded on them. The significant feature of this technology is that the act of eavesdropping can be detected, which is almost impossible in conventional communications.

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

2. Short history of QKD

The risk of the digital data exchanged over the modern Internet being stolen or eavesdropped upon cannot be diminished to zero. Therefore, the technology of cryptography is used when people send passwords or credit card numbers. Widely used is the public key cryptosystem: its security is based on certain hard mathematical problems. Therefore, the strength of its security depends on the development of computer performance and mathematical algorithms. In contrast, the one-time pad cryptosystem has long been known to be impossible to break. However, two parties (a sender called Alice and a receiver called Bob) need to share secret keys that are completely random, the same size as the message to be sent, and never used again. QKD can provide a method of distributing such keys in an ultimately secure manner. The basic principle of QKD is depicted in **Fig. 1**. Alice prepares a long random bit array made of 0s and 1s and encodes this binary information on photons, which are sent to Bob through a quantum channel (e.g., an optical fiber). Bob obtains a logical bit array by measuring each photon. So far, this seems the same as classical communications, but a difference becomes evident when an eavesdropper tries to steal the bit information. In classical communication, the classical information can be stolen by branching part of it. But the quantum information encoded on an elementary particle, a photon, cannot be divided any more: the only choices are to take it all or leave it all. The stolen data is equivalent to simple loss, and the remaining random bits can be used as a secret key if Bob later tells Alice the positions of the bits that he knows have been lost. A clever eavesdropper might send fake photons that depend on the measured

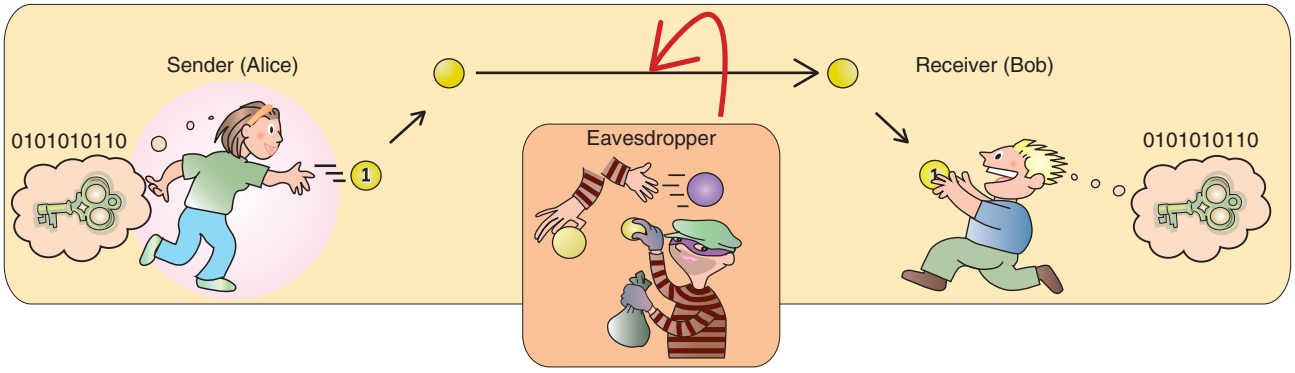

Fig. 1. Principle of quantum key distribution.

results of the stolen photons. However, one cannot measure a photon quantum state without changing it in an uncontrollable manner (measurement back-action), so the fake signals depending on this measurement inevitably introduce bit errors into Bob's measurements. The no-cloning theorem of quantum mechanics prohibits the eavesdropper from making a copy of a photon before measurement. Therefore, the eavesdropper cannot obtain the key information without inducing bit errors. In other words, Alice and Bob can recognize the presence of an eavesdropper by checking the bit errors.

In the first QKD protocol proposed in 1984, called BB84 after the proposers C. H. Bennett and G. Brassard, Alice assigns logical bits 0 and 1 to a polarization state of a photon using two randomly chosen sets (bases), namely, circular polarizations (right-hand circular and left-hand circular) or linear polarizations (horizontal and vertical). Bob measures the photon after choosing the measurement basis at random, but he obtains the correct result only if he has chosen the same basis as Alice. Therefore, after photon transmission, Alice and Bob exchange information about their bases and sift out only the key for that corresponds to the same basis. They compare part of the obtained sifted key to check the error rate. If the error rate is less than a certain threshold value, they can conclude that no eavesdropper is present. Finally, a secure key is generated with post-processes—error correction and privacy amplification—to diminish information that might leak to an eavesdropper.

Unconditional security proof, which certifies secure key distribution even when an eavesdropper tries all physically allowed actions, has been known for the BB84 protocol when we can use an ideal single-photon emitter that emits photons exactly one-by-one. More recently, unconditional security has been proven for an attenuated coherent (laser) source, instead of a single-photon emitter, with the use of an additional procedure (decoy-BB84). Other QKD protocols than BB84 have also been proposed and their security has been investigated.

Optical fibers have been the most popular quantum channel to date, but the polarization states, which were initially proposed in BB84, cannot be maintained stably over a long distance. Instead, as shown in **Fig. 2**, the time-bin basis (a photon is in either the first or second pulse) or the phase basis (the relative phase of a photon extending over two pulses is either 0 or π) can be used. Alternatively, one can use two bases of relative phases $\{0, \pi\}$ or $\{\pi/2, 3\pi/2\}$.

In real systems, the secure key's generation rate and distribution distance are limited by the sensitivity, dark count rate (rate of signal detection without actual arrival of photons) of the single-photon detector (SPD), and the loss of the quantum channel. How far can we distribute a secure key? When we use optical fibers, we need to use photons with a wavelength of 1.5 μm since that has the minimum transmission loss. The biggest technical issue has been the lack of an adequate SPD sensitive to photons of this wavelength. However, the recent development of SPDs has enabled 1-Mbit/s secure key generation for 50-km transmission through fiber [1] or 200 km if the key generation rate is very slow [2], [3]. Although much longer transmission with further-improved SPDs may be difficult, there are three possible solutions. One is to locate trusted relay points every 50–100 km and share the secret key between two distant points by exchanging keys at the relay points. Field testbed experiments were demonstrated in 2008 by the EU's SECOQC project [4] and also in 2010 by the Tokyo

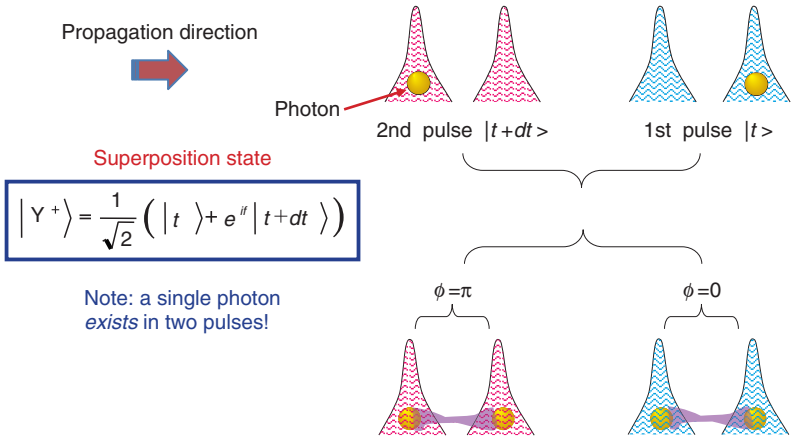

Fig. 2. Time-bin basis and phase basis.

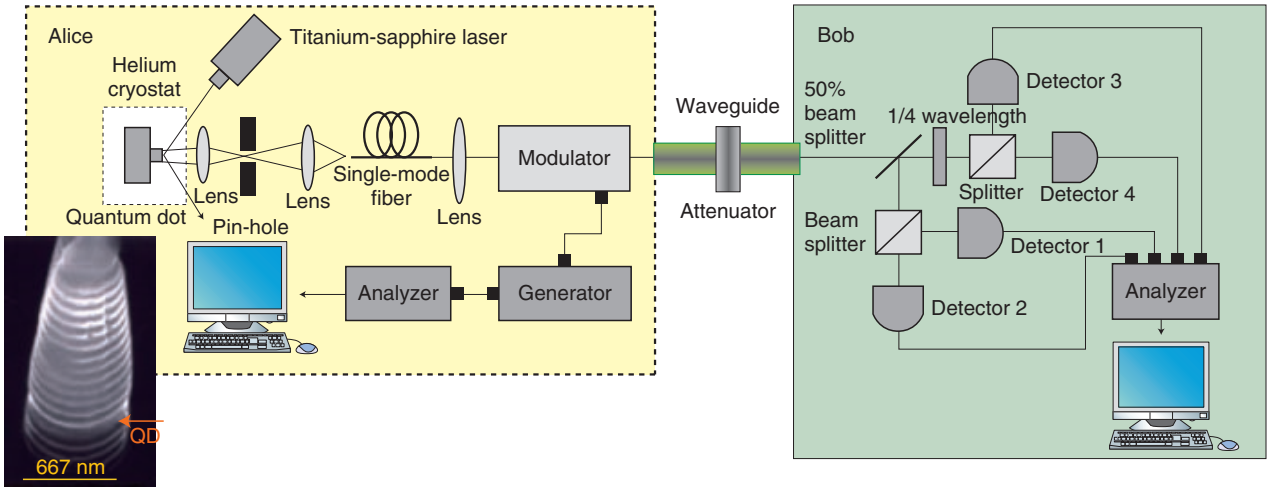

Fig. 3. BB84 QKD experimental setup using single-photon source.

QKD Network project [5], [6] in which NTT participated. The second candidate is to generate a secret key between a satellite and a ground base and then have the satellite swap the key with another ground base. In fact, such experiments are currently being prepared by the EU and Japan [7]. The third candidate is the quantum repeater, which is a future technology for repeating quantum information without converting it into classical information. This is considered to be the core technology for future QICT, as well as QKD, and is now being actively investigated all over the world [8].

3. NTT research and development (R&D)

NTT has been engaged in the basic research field of QICT: quantum optics. For QKD, theoretical investigation came first and experimental efforts started later, in 2000. Our collaboration with Professor Yoshihisa Yamamoto of Stanford University led to BB84 QKD experiments using a single-photon emitter with a quantum dot (wavelength: 0.8 μm) [9]. Single photons emitted from the quantum dot embedded in the pillar structure shown in the scanning electron micrograph, **Fig. 3** (left), are sent to Bob after being encoded in one of four polarization states (two logical bits × two bases). Bob measures the photons

by randomly choosing a basis using polarization beam splitters and four SPDs.

NTT and Stanford University proposed a new QKD protocol, Differential Phase Shift Quantum Key Distribution (DPS-QKD), in 2003 [10]. It applies a modern optical communication protocol, differential phase shift keying (DPSK) to the quantum regime. DPS-QKD uses a weak coherent state extending over multiple pulses, which is in clear contrast to the former QKD proposals that used quantum states of single photons, as shown at the bottom of Fig. 2. The DPS-QKD system is simple and applicable to a high clock rate and has good tolerance to the photon number splitting attack, which is an attack in which the number of photons in a pulse is counted and information is stolen by splitting one of the pulse's many photons. Moreover, in DPS-QKD, all the arriving photons can generate a key, whereas in BB84, half of them on average do not generate a key because of basis mismatch. A related protocol is the Coherent One-Way (COW) protocol [3]. NTT Basic Research Laboratories has used this DPS-QKD protocol and reported system experiments for clock rates from 1 GHz to 10 GHz.

NTT is also developing various improved SPDs. A conventional telecommunications wavelength SPD is the InGaAs avalanche photodiode (APD), which has the problems of low efficiency, high dark count rate, and limited slow gate-mode operation because of the after-pulse signal produced by the residual charges after photon detection. In contrast, the Si APD has a low dark count rate and does not need gate mode operation, but it is highly efficient only for photons with a relatively short wavelength. We have developed and verified a frequency-up-conversion SPD system by raising the photon frequency (making the wavelength shorter) by using periodically poled lithium nitride (PPLN) nonlinear-optics crystal and an intensive pump light and by detecting the photons with a Si-APD. We have also performed a QKD experiment that demonstrated a very high key generation rate with a fast hybrid single-photon detector and frequency up-conversion [11]. Recently, over-1-GHz clock operations have been demonstrated by improving the InGaAs-APD's optical signal analyzing circuit [12]. A superconducting single-photon detector (SSPD) has attracted much attention for its extremely small dark-count and high-speed operations. SSPD performance has been improving rapidly [13].

So far, we have discussed QKD with single photons or attenuated coherent light. It is known that quantum mechanics can allow an intriguing state of multi-quantum systems: the *quantum entangled state*. The technology for generating entangled photon pairs has matured; in particular, NTT has been leading telecommunications-band entangled photon-pair generation and its QKD applications [14]. In the future, we will pursue R&D of quantum repeaters and the connection of remote quantum computers to achieve highly developed quantum networking.

4. Prospects

From the perspective of the importance of privacy protection in the modern information society, the *unconditional security* of QKD seems appealing. However, the security of a system is not the sum of the securities of its components, but their product. For example, the total security is zero if the obtained secret keys are treated carelessly. In this sense, we could regard QKD R&D as a challenge toward ultimate security. Moreover, while previous R&D has been seeds- or hardware-oriented, more weight is expected to be given to applications and software in the future. QKD is an attractive subject with practical applications as well as a fundamental science.

Acknowledgment

Part of this research was done with the support of NICT and JST-CREST.

References

[1] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous Operation of High Bit Rate Quantum Key Distribution," Appl. Phys. Lett., Vol. 96, No. 16, p. 161102, 2010.

[2] H. Takesue, S. Woo 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.

[3] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High Rate, Long-distance Quantum Key Distribution over 250 km of Ultra Low Loss Fibres," New. J. Phys., Vol. 11, No. 075003, 2009.

[4] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys., Vol. 11, No. 075001, 2009.

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

[6] 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.
[7] http://www.quantum.at/quest
[8] For example, H. J. Kimble, "The Quantum Internet," Nature, Vol. 453, No. 7198, pp. 1023–1030, 2008.
[9] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Quantum Cryptography with a Photon Turnstile," Nature, Vol. 420, No. 6917, p. 762, 2002.
[10] Y. Tokura and T. Honjo, "Differential Phase Shift Quantum Key Distribution (DPS-QKD) Experiments," NTT Technical Review, Vol. 9, No. 9, 2011.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa8.html
[11] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, "Megabits Secure Key Rate Quantum Key Distribution," New J. Phys., Vol. 11, p. 045010, 2009.
[12] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, "High-rate Quantum Key Distribution over 100 km Using Ultra-low-noise, 2-GHz Sinusoidally Gated InGaAs/InP Avalanche Photodiodes," Opt. Express, Vol. 19, No. 11, pp. 10632–10639, 2011.
[13] H. Shibata, "Superconducting Single-photon Detectors," NTT Technical Review, Vol. 9, No. 9, 2011.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa9.html
[14] H. Takesue, "Quantum Communication Using Entangled Photon Pairs..Toward Quantum Repeaters," NTT Technical Review, Vol. 9, No. 9, 2011.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa10.html

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.