Quantum Key Distribution Technologies

Kyo Inoue, *Member, IEEE*

(Invited Paper)

***Abstract*—Since it was noted that quantum computers could break public key cryptosystems based on number theory, extensive studies have been undertaken on quantum cryptography (QC), which offers unconditionally secure communication based on quantum mechanics. This paper describes QC technologies, introduces a typical and widely used QC protocol BB84 and then describes a recently proposed scheme called the differential-phase-shift protocol.**

***Index Terms*—Quantum cryptography (QC), quantum key distribution (QKD), secure communication.**

I. Introduction

It is known that a Vernam one-time pad is a cryptosystem with perfect security, where a plain text message is ciphered/deciphered by a secret key (actually a random bit string) whose bit length is equal to that of the plain message. However, a crucial problem is how to deliver a secret key to two legitimate parties in a secure way. Quantum cryptography (QC) or quantum key distribution (QKD) [1] is a system that provides a secret key for a Vernam one-time pad to two legitimate parties. The security of the key is unconditionally guaranteed by quantum mechanics. The first protocol was proposed in 1984 by Bennett and Brassard [2]. This protocol is known as BB84 and is now widely employed in experiments. Although this idea did not attract much attention at first, research efforts have increased since the 1990s when it was proved that quantum computers could break the public-key cryptosystems commonly used in modern cryptography. Various theoretical and experimental studies have been undertaken, and prototype products are now commercially available.

This paper describes QC technologies, without using quantum–mechanical terms such as bra, ket, and nonorthogonality, for those not familiar with quantum mechanics. Section II describes a phase-encoding BB84 system as a conventional QKD protocol and mentions its configuration, operating mechanism, and security against eavesdropping. A new type of QKD using homodyne detection is also briefly mentioned. Section III describes issues related to implementing a BB84 system and presents some experimental results. Section IV is devoted to a new type of QKD called differential-phase-shift (DPS) QKD, which was proposed and developed by the author and coworkers at NTT Japan and Stanford University CA. Finally, future work designed to expand the transmission distance is briefly mentioned.

Manuscript received August 10, 2005; revised January 17, 2006.

The author was with Nippon Telegraph and Telephone (NTT) Basic Research Laboratories, NTT Corporation, Kanagawa 243-0198, Japan. He is now with Osaka University, Osaka 565-0871, Japan (e-mail: kyo@comm.eng.osaka-u.ac.jp).

Digital Object Identifier 10.1109/JSTQE.2006.876606

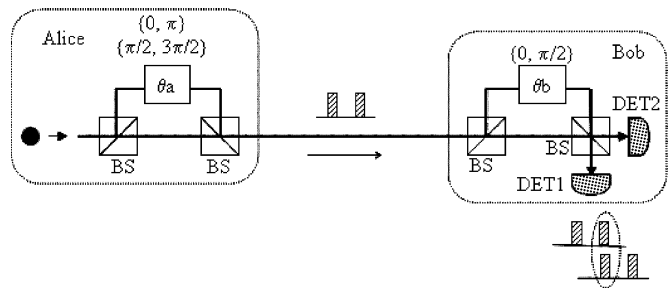

Fig. 1. Basic configuration of phase-encoding BB84 system. DET: photon detector; BS: beam splitter.

II. QKD Systems

Although there are several QKD protocols including BB84 [2], E91 [3], B92 [4], and BBM92 [5], this paper focuses on the BB84 protocol because it is a well-known and widely employed QKD scheme.

A. BB84 Protocol

Although the original proposal of BB84 relies on the polarization state of a photon, phase-encoding BB84 is mainly used these days, because it is inconvenient to use the polarization state as regards fiber transmission. We start by describing phase-encoding BB84 systems. The basic configuration is shown in Fig. 1. A sender (traditionally called "Alice") transmits a photon through an asymmetric Mach–Zehnder interferometer where the phase difference $\theta_{\rm a}$ between the two paths is randomly chosen from one of four values, namely $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. From the interferometer, a photon positioned over two time slots is output with a phase difference of $\theta_{\rm a}$. The photon is sent to a receiver (traditionally called "Bob"). Bob transmits the arriving photon through an interferometer identical to Alice's, in which the phase difference $\theta_{\rm b}$ is randomly chosen from $\{0, \pi/2\}$. The photon is then detected at the interferometer outputs.

The above configuration is equivalent to Young's double-slit interference experiment with a single photon in the time domain. As in the double-slit experiment, the photon probability amplitudes in the two time slots interfere with each other at Bob's interferometer when the photon is counted at the middle time instance as shown in Fig. 1. Either detector 1 or 2 clicks according to the interference. The interference pattern is dependent on Bob's phase $\theta_{\rm b}$ as shown in Fig. 2, where the detection probability at DET 1 is plotted as a function of Alice's phase $\theta_{\rm a}$. The photon count at DET 2 has a complementary probability.

Fig. 2 shows that the detection probability at DET 1 is maximum or minimum for particular combinations of $(\theta_{\rm a}, \theta_{\rm b})$, such as at a peak for (0, 0) and $(\pi/2, \pi/2)$ and at a bottom for $(\pi, 0)$ and $(3\pi/2, \pi/2)$. This means that a photon is deterministically

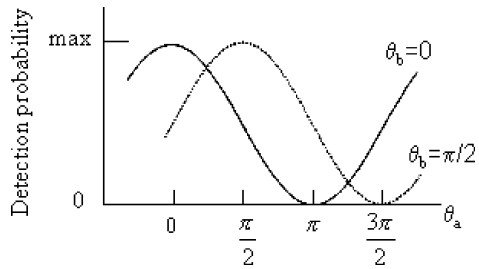

Fig. 2. Photon detection probability at detector 1.

detected by DET 1 for (0, 0) and $(\pi/2, \pi/2)$ and by DET 2 for $(\pi, 0)$ and $(3\pi/2, \pi/2)$ provided that the extinction ratio of the interference is perfect. On the other hand, which detector clicks is probabilistic for the other phase combinations.

Using this setup, a secret key is obtained as follows. 1) A number of photons is transmitted from Alice to Bob. 2) After the transmission, Bob tells Alice which photon was detected and which phase he chose for the detected photon. 3) Alice tells Bob whether she chose $\theta_{\rm a}$ from $\{0, \pi\}$ or from $\{\pi/2, 3\pi/2\}$ for the detected photon. From this phase information, they know whether the detection event was deterministic or probabilistic. 4) For deterministic detection events, Alice regards $\theta_{\rm a} = 0$ or $\pi/2$ as bit "0" and $\theta_{\rm b} = \pi$ or $3\pi/2$ as bit "1," and Bob regards the DET 1 click as bit "0" and the DET 2 click as bit "1." For the probabilistic detection events, on the other hand, they ignore them. A bit string created as above is identical for Alice and Bob. In the above procedure, bit information itself is not disclosed, thus the created bit string can be a secret key.

B. Error Correction and Privacy Amplification

Though the above protocol provides a secret key in principle, the obtained key is not perfect in practice. First, bit errors are not avoidable due to apparatus imperfections. The bit error rate in QKD systems is much higher than that in conventional optical communication systems, e.g., several percent, because there is no threshold processing or, in other words, bit information is processed in an analogue way. Small deviations from ideal conditions, such as phase deviation from $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$ and the residual extinction ratio in interferometers, and noise in photon detectors straightforwardly cause bit error. Thus, an error correction process is usually conducted after the photon transmission. The typical error correction protocol is called "CASCADE" [6], where a bit string is divided into a number of blocks and the parity of each block is checked between Alice and Bob to find and correct errors.

Though an error-free bit string is obtained by error correction, it is not still good enough as a secret key, because there is a possibility that a fraction of the string is leaked by some eavesdropping strategies as described in the following sections. In order to extinguish possible partial leakage, a process called privacy amplification [7] is usually carried out after the error correction. A simple way of privacy amplification is that key bits are paired and the exclusive ORs of each pair are turned to be new key bits. The result of an exclusive OR is unknown to an eavesdropper even when he or she knows one bit of the original pair. A secure key is obtained by this process, while the key length becomes half as a penalty. The above privacy amplification protocol is just an example, and an efficient way has been developed and is usually employed. It should be pointed, however, even the privacy amplification does not work when the information leakage is too large.

C. Eavesdropping

Here we discuss the security of a secret key, obtained as in Section II-A, against certain eavesdropping strategies. A full security analysis is omitted here, since the purpose is to provide an intuitive overview of QC.

1) Beam Splitting Attack: Straightforward eavesdropping is a beam splitting attack. An eavesdropper (traditionally called "Eve") tries to steal information by tapping a transmitted signal. However, this attack would fail because the stolen photons do not reach Bob and thus no key bit is created from them. When Alice uses strongly attenuated laser light as quasi single-photons, which is usually the case in practice, there is a finite probability that both Eve and Bob detect a photon from one signal state according to the Poisson distribution of the photon statistics. Some information is leaked as a result of these detection events, but a small leak can be extinguished by privacy amplification described in the previous section.

2) Intercept–Resend Attack: Another type of eavesdropping is where Eve intercepts a transmitted signal on its way from Alice to Bob, measures its state, and resends a fake signal to Bob based on the result of her measurement. Unfortunately for Eve, however, there is no way to distinguish the four phase values of $0, \pi/2, \pi$, and $3\pi/2$ in one measurement; $\pi/2$ and $3\pi/2$ are ambiguous when she tries to distinguish 0 and π, and 0 and π are ambiguous when she tries to distinguish $\pi/2$ and $3\pi/2$. Thus, Eve cannot resend a perfect copy of Alice's signal to Bob. When Bob creates his key bits from Eve's imperfect signal, some do not match Alice's key bits. Then, Alice and Bob can detect the eavesdropping by checking to see if there are bit mismatches in some test bits. In other words, the key is guaranteed to be secure when there is nothing wrong with the test bits. The probability of Eve's measurement being ambiguous is 1/2, half of which causes a bit mismatch. Thus, the bit-mismatch probability is 1/4.

In actual systems, bit errors are inevitable as described in the previous section. In such situations, Eve can steal a fraction of information by undertaking a partial intercept–resend attack. Eve launches an intercept–resend attack against part of the transmitted signal and does nothing for the other signal. The bit-mismatch probability induced by this partial eavesdropping is $\alpha/4$, where α is a fraction of the intercepted signal. When $\alpha/4 \ll e$, where e is the error rate caused by system imperfections, the eavesdropping is masked by the system error, and α of the information is leaked to Eve. An extreme case is $\alpha/4 = e$, where almighty Eve fully utilizes the error rate assumed by Alice and Bob. The ratio of information leakage is $4e$ in this case, which is the upper bound imposed by the partial intercept–resend attack. To eliminate such a partial information leakage, privacy amplification is usually carried out as long as the leakage or the bit error rate does not exceed a critical level.

3) Photon-Number-Splitting (PNS) Attack: Serious eavesdropping consists of PNS attack against systems using strongly attenuated laser light [8]. Eve probes the number of photons just after Alice's output by using a quantum nondemolition (QND) measurement. When her measurement shows that there are more than two photons in a signal, she extracts one photon and keeps it, and lets the remaining photons pass to Bob through a lossless transmission line that she installed in place of the one used by Alice and Bob. On the other hand, when she detects the presence of one photon, she blocks it as long as the blocking does not reduce Bob's photon counting rate. After the photon transmission, Alice and Bob exchange phase information. Eve listens in and then measures the photons that she has kept. With Alice's information, Eve can make an appropriate measurement and conclusively obtain key bits.

In fact, the PNS attack described above is unrealistic that Eve must perform a QND measurement, extract one photon, store that photon, and install lossless fiber. However, a basic rule in QKD is that Eve can do anything as long as it does not contradict the laws of physics. The term *ultimate or unconditional* security is based on the criterion that QKD is secured even if Eve employs unrealistic but allowable strategies in principle.

The PNS attack severely limits the transmission distance. If the probability that there are more than two photons at Alice's output (from which Eve steals key information) is equal to Bob's photon detection probability, Eve will have copies of all the photons detected by Bob, meaning that all key information is leaked to Eve. This condition can be satisfied in long-distance systems even when the probability of there being more than two photons is small, because Bob's photon detection probability is also small as a result of the large transmission loss. To avoid this condition, the average photon number sent by Alice should be small in accordance with the transmission loss, so that the probability of there being more than two photons is always smaller than the system transmittance. As a result, Bob's detection rate decreases in proportion to the square of the transmittance, and reaches a cut-off value determined by the detector noise. For typical device parameters, the cut-off distance imposed by the PNS attack is around 50 km [9].

The use of a single-photon source that emits no more than one photon prevents a PNS attack and can increase the transmission distance [10]. However, it is a considerable challenging to realize such a light source.

D. Countermeasures Against PNS Attacks

Modified versions of BB84 have been proposed to combat with PNS attacks. In one version [11], photon transmission is conducted in the same way as in conventional BB84, but information exchanged between Alice and Bob after the transmission is different, so that Eve cannot identify the signal state that she keeps even after information disclosure by Alice and Bob. Due to the particular protocol, Eve cannot obtain full information by launching a PNS attack on this system.

Another way to beat the PNS attack involves the use of decoy states [12]. Alice randomly inserts decoy states between signals, whose average photon number is larger than that of the signal states. When Eve conducts a PNS attack, the ratio at which Bob detects photons from the decoy and from the signal changes because the probability of there being more than two photons is different in the decoy and the signal. The PNS attack can be discovered by the change in this detection ratio.

E. QKD Using Coherent Light With Homodyne Detection

A major issue as regards implementing QKD is photon detection. A QKD scheme using homodyne detection was proposed to avoid photon detection difficulties [13], [14]. Alice sends a coherent pulse with an average photon number of around one, whose phase is randomly chosen from $\{0, \pi\}$ $\{\pi/2, 3\pi/2\}$. Bob measures the pulse with a homodyne detection system whose operating condition is randomly selected for measuring $\{0, \pi\}$ $\{\pi/2, 3\pi/2\}$. When Bob's measurement condition matches Alice's phase, he obtains information about Alice's phase, from which Alice and Bob create a key bit. Otherwise, they discard the results.

The structure of this scheme is basically the same as BB84, except that homodyne detection is conducted on a coherent pulse with an average photon number of around one. The security is based on the quantum noise in the homodyne detection, which prevents four phase states from being fully distinguished. It might appear that such a scheme based on quantum noise would be fragile to Eve who splits a fraction of the signal just after Alice's output and lets the remaining signal pass to Bob through a lossless transmission line. In particular, in long-distance systems (i.e., lossy systems), Eve's signal-to-noise ratio can be better than Bob's, and she may identify Alice's phase with more accuracy than Bob. However, a postselection procedure, in which Bob picks up data measured with a high signal-to-noise ratio, enables Bob to create a key bit, only a fraction of which is leaked to Eve. Then, privacy amplification makes it secure.

III. Experiments

A. Photon Detector

A photon detector is a key device when carrying out QKD experiments (except for systems using homodyne detection). Highly biased avalanche photodiodes (APDs) are usually used, in which an electron excited by one photon triggers an avalanche, resulting in a measurable output signal. A high detection efficiency, a low dark-count rate (a click in the absence of a photon), and low afterpulse probability (fake clicks occurring sequentially after an avalanche) are desired. For short wavelengths, Si-APDs with a detection efficiency of 60%–70% and a dark count rate of less than 100 cps are available. In contrast, InGaAs-APDs for the fiber communication wavelength do not perform so well. A gating mode is usually employed for InGaAs-APDs in order to make the dark counts small, where a bias pulse exceeding the breakdown voltage is applied at a possible photon arrival moment. Typical performance characteristics are an efficiency of 10%, a dark count rate of the order of 10^{-5} per gate, and a gating frequency of several MHz, determined by the afterpulse. Record dark count rates are 10^{-7}–10^{-6} per gate [15], [16]. Current QKD system performance is mainly limited by detector

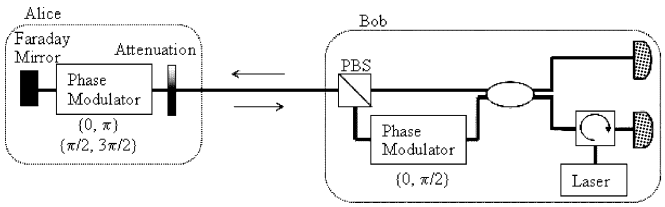

Fig. 3. Basic configuration of "plug and play" BB84 system. PBS: polarization beam splitter.

performances, namely transmission distance by dark count and key creation rate by efficiency and gating frequency.

Recently, an alternative scheme has been studied that uses high-performance Si-APDs rather than InGaAs-APDs [17], [18]. A photon in the 1.5-μm wavelength band is frequency-converted to a short wavelength by using a periodically poled $LiNbO_3$ (PPLN) via the second-order optical parametric interaction (i.e., sum frequency generation), and is then detected with a Si-APD photon detector. With a high pump power, nearly 100% frequency-conversion efficiency is possible, and a net efficiency of 30%–40% has been obtained. Since Si-APDs do not have to be operated in the gating mode, frequency-conversion photon detectors work in the continuous mode, which will result in a high key creation rate in QKD systems.

B. Plug and Play System

Interferometer stability is an issue as regards implementing the phase-encoding BB84 shown in Fig. 1. For correct operation, the optical length difference must be stable within a fraction of the wavelength. To overcome this difficulty, a one round trip setup called "plug and play" system was proposed [19], in which laser light is sent from Bob to Alice and returned back to Bob with strong attenuation at Alice's site, as shown in Fig. 3. Quasi single-photon states resulting from the strong attenuation are transmitted from Alice to Bob. In this setup, two pulses pass through the same route in reverse, and thus the phase difference between the two pulses is automatically stabilized. Most recent BB84 experiments employ this plug and play scheme.

Rayleigh backscattering is an issue with plug and play systems. Light power transmitted from Bob to Alice is relatively large while quasi single-photons are sent from Alice to Bob. They travel over the same fiber bidirectionally. In such a situation, Rayleigh backscattering photons generated by the light transmitted from Bob to Alice reach Bob's detectors, and cause erroneous clicks. To avoid this error, Alice is equipped with a delay fiber so that signal photons arrive at Bob after the Rayleigh backscattering photons. The use of a frequency shifter at Alice's site is also effective [20].

Another issue in plug and play systems is the "Trojan horse" attack. Eve sends a probe light to Alice together with a signal light from Bob, whose power is sufficiently large for Eve to measure Alice's phase modulation from the returning light. To deal with this, Alice has to have a monitoring system to confirm that no such light comes.

Despite its complexity, the plug and play configuration is widely employed because of its stability. Fig. 4 summarizes a

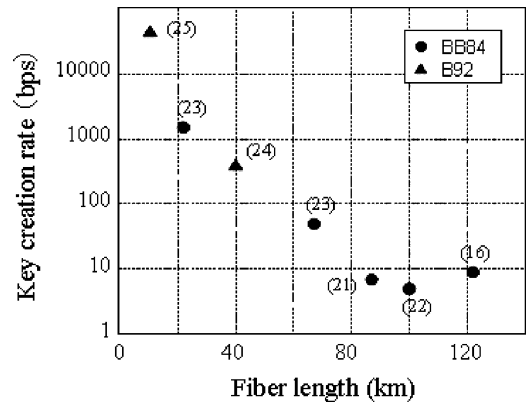

Fig. 4. QKD experimental reports. Reference number is shown. Refs. [16] and [24] use a unidirectional setup, not "plug and play."

number of experimental reports. As shown in the figure, the key creation rate decreases as the fiber length increases because photons hardly reach the receiver in a long-distance system. The longest distance is around 100 km, which is limited mainly by the dark count at the photon detectors. Note that Section II-B3 mentions a length limit of around 50 km that is determined by PNS attacks, while experiments with a 100-km fiber length are shown in Fig. 5. This is because PNS attacks were not taken into account in these experiments, that is, a perfectly secure key was not created there. The results in Fig. 4 are in a sense data for reference. An experimental result for a secure key is shown in Fig. 11 in Section IV-C.

IV. DPS QKD

The DPS protocol [25], [27] is a QKD scheme that was proposed and developed by the author and coworkers at NTT and Stanford University. It has certain advantages including simplicity, high efficiency, and robustness in the face of PNS attacks. This section describes the DPS QKD system and related work undertaken at NTT and Stanford.

A. Configuration

Fig. 5 shows the configuration of the DPS QKD scheme. Alice sends a coherent pulse train with an average optical power of less than one photon (e.g., 0.1) per pulse. Each pulse is randomly phase-modulated by 0 or π. Bob transmits the arriving pulses through an asymmetric Mach–Zehnder interferometer, whose path length difference corresponds to the time interval of the pulse train, and the path phase difference is 0. Photons are then detected at the interferometer outputs, where neighboring pulses interfere with each other as shown in Fig. 5. The photons are detected according to the interference. DETs 1 and 2 click when the phase differences between two pulses are 0 and π, respectively. This configuration is basically the same as that of RZ-DPSK systems that have been extensively studied in the field of optical communications, except that the optical power is highly attenuated.

With this setup, a secret key is created as follows: 1) A pulse train is transmitted from Alice to Bob; 2) After the transmission,

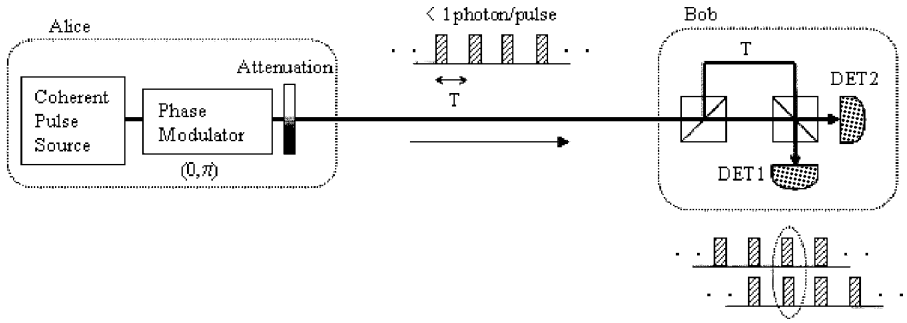

Fig. 5. Configuration of differential-phase-shift QKD system.

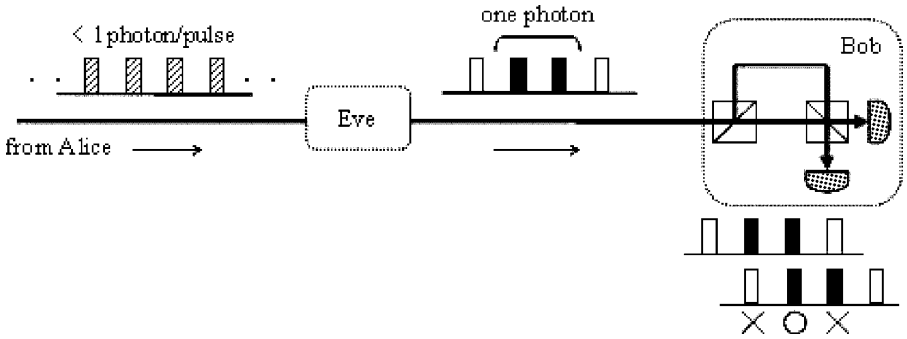

Fig. 6. Intercept–resend eavesdropping against differential-phase-shift QKD system.

Bob tells Alice the photon detection time; 3) By referring to her modulation data, Alice knows which detector clicked at Bob's site; and 4) Alice and Bob create key bits by regarding the DET 1 click as bit "0" and the DET 2 click as bit "1." In this procedure, only the detection time is disclosed, not the bit information. Thus, a bit string created as described above can constitute a secret key.

An advantage of the DPS scheme is its high key creation efficiency. With the DPS protocol, all the photons detected by Bob contribute to the key creation. On the other hand, in conventional BB84 half of the detected photons are discarded because Bob's measurement result is ambiguous when the bias phase of his interferometer does not match Alice's phase. Thus, the key creation rate in the DPS protocol is twice that in the BB84 protocol, provided that the number of detected photons is the same.

B. Eavesdropping Against DPS System

Because the DPS protocol is a new scheme and has a unique structure in terms of quantum mechanics, full security analysis has not been completed. Here, we consider typical eavesdropping.

1) Beam Splitting Attack: Since the DPS system intrinsically uses coherent light whose photon statistics follow the Poisson distribution, there is a finite probability of information leakage caused by beam splitting attacks. Fortunately, the leakage can be small with an appropriate average photon number, and the small leakage can be extinguished by privacy amplification [7] as described in the previous section.

2) Intercept–Resend Attack: In conducting an intercept–resend attack, Eve intercepts the transmitted signal and tries to measure the differential phases of the pulse train. Unfortunately for her, however, she cannot measure all the phase differences, because the average photon number is less than one per pulse and a photon is detected, for example, once in ten time slots. Thus, she cannot resend a perfect copy of the original signal to Bob. In this situation, Eve can send one photon positioned over two pulses for measured time plots and send nothing for unmeasured time slots. This resend strategy does not change Bob's photon counting rate, thus he does not notice the eavesdropping from the counting rate.

However, a bit mismatch occurs when Bob creates a secret key from this fake signal, as described below. The fake signal reaching Bob consists of two sequential pulses with the surrounding slots being vacant, as shown in Fig. 6. From this signal, Bob possibly counts a photon at three time instances: 1) counted from the first pulse passing through the short path in the interferometer, 2) counted from the first pulse passing through the long path and the second pulse through the short path, and 3) counted from the second pulse passing through the long path. The second detection event occurs in accordance with the phase difference between the two pulses, which gives Bob a correct bit. On the other hand, DETs 1 or 2 clicks randomly at the first and third detection events because there is no interference. Bob's key bits created from these detection events can be different from Alice's. Thus, Alice and Bob notice the eavesdropping by checking some test bits. The probability that a photon is counted at the first or third time instance is 1/2, a half of which results in bit mismatch. Thus, the bit-mismatch probability is 1/4.

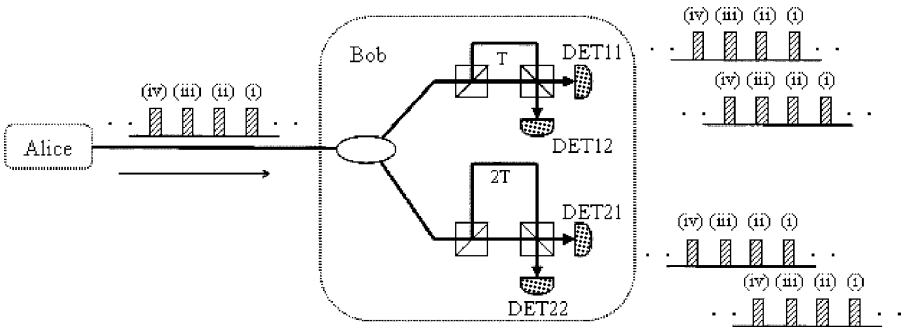

Fig. 7. Configuration of modified differential-phase-shift QKD system for high bit-mismatch probability due to eavesdropping. T: time interval of pulse train; DET: photon detector.

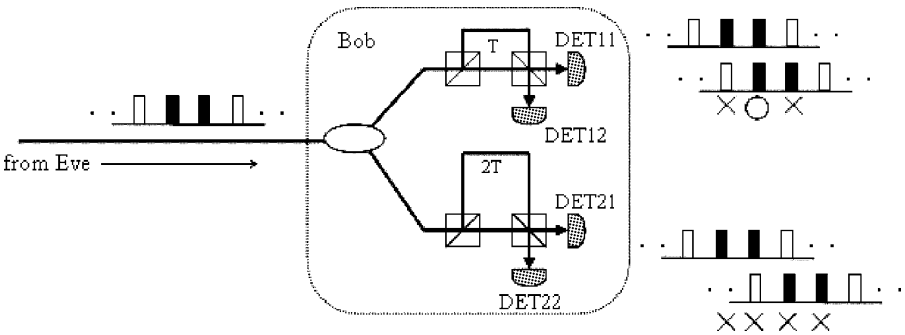

Fig. 8. Bob's detection event against intercept—resend eavesdropping. T: time interval of pulse train; DET: photon detector.

The bit-mismatch probability induced by eavesdropping should be high, since the information leakage caused by a partial intercept–resend attack, described in Section II-B2, is small when the high bit-mismatch probability is high, and the final key length after privacy amplification is long as a result. A modified DPS scheme [28], whose configuration is shown in Fig. 7, can increase the bit-mismatch probability. Alice sends a coherent pulse train as in the original DPS scheme. Bob splits the incoming pulses into two paths, one travels to an interferometer with a length difference equivalent to the pulse interval (hereafter called T-MZI), and the other travels to another interferometer with a length difference equivalent to twice the pulse interval (hereafter called 2T-MZI). At the T-MZI outputs, two neighboring pulses interfere with each other. At the 2T-MZI outputs, two pulses that are two time intervals apart interfere with each other. The interferometer that a photon passes through is determined probabilistically.

With this setup, a secret key is created as follows: 1) A pulse train is transmitted from Alice to Bob. 2) Bob tells Alice the photon detection time and which interferometer the photon passed through. 3) Alice knows which detector clicked at Bob's site from the information disclosed by Bob and her modulation data. 4) Alice and Bob create key bits by regarding a click by DET 11 and DET21 as bit "0" and that by DET 12 and DET 22 as bit "1." A bit string created as described above can constitute a secret key.

When Eve conducts an intercept–resend attack, the following occurs. In detecting the transmitted signal, Eve has to choose which phase difference to measure, that of neighboring pulses or that of pulses separated by two time intervals. Without loss of generality, we assume that she measures neighboring pulses. She then resends a fake signal to Bob in which one photon is positioned over two pulses with the surrounding pulses being vacant, as shown in Fig. 8. For such a signal, the detectors at the T-MZI outputs count a photon at perhaps three time instances, and the detectors at the 2T-MZI outputs count a photon at perhaps four time instances. Of these detection events, a click at the middle instance at the T-MZI outputs, which occurs according to the interference between neighboring pulses, provides Bob a correct bit. On the other hand, the other detection events occur randomly. The probability of a random click is 3/4, half of which causes a bit-mismatch between Alice and Bob. Thus, the bit-mismatch probability induced by eavesdropping is 3/8, which is larger than the probability of 1/4 in the standard DPS scheme and in conventional BB84. The modified DPS scheme described above can detect Eve more easily.

3) PNS Attack: An advantage of the DPS protocol over BB84 systems using attenuated laser light is its robustness against PNS attacks [29]. In a PNS attack, Eve measures the number of photons in the transmitted signal, searching for extra photons to be picked up. Since the bit information is carried by the phase difference between two pulses in DPS systems, she undertakes a probe to see if more than two photons are positioned over two pulses. From two pulses that contain more than two photons, she extracts one photon and then allows the two pulses to pass to Bob through a lossless transmission line. She blocks the other pulses to establish a condition whereby Bob will only receive photons identical to those that she extracted.

Unfortunately for Eve, however, this PNS attack induces a mismatch between Alice's and Bob's key bits. Since Eve blocks

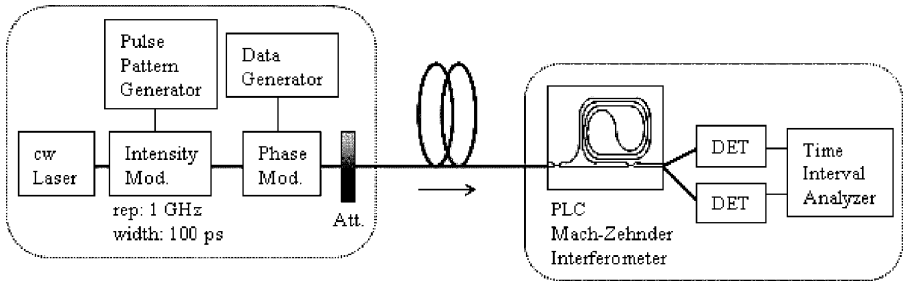

Fig. 9. Experimental setup of differential-phase-shift QKD system.

pulses that contain one or no photons, two sequential pulses with surrounding pulses that are vacant are transmitted from Eve to Bob, as in the intercept–resend attack shown in Fig. 6. Such a signal induces a bit mismatch, as described in the previous section, and Alice and Bob can notice the eavesdropping by checking some test bits.

The above consideration suggests that the average photon number sent from Alice does not have to be reduced in a long-distance system, unlike in BB84 using attenuated laser light. As a result, Bob's detection rate decreases linearly with the transmittance, and the cut-off distance determined by the detector noise is longer than that of conventional BB84 systems.

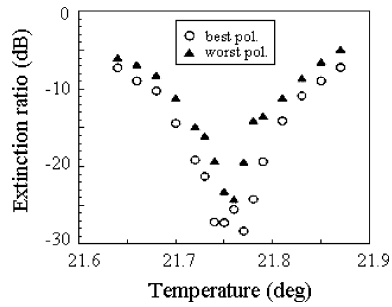

Fig. 10. Extinction ratio as a function of waveguide chip temperature in a PLC Mach–Zehnder interferometer with a path length difference of 20 cm.

C. Experiment

Experiments were carried out to demonstrate the feasibility of our DPS QKD scheme [30], [31], the configuration of which is shown in Fig. 9. A coherent pulse train with a repetition rate of 1 GHz and a pulse width of 100 ps was generated by intensity-modulating cw light ($\lambda = 1551$ nm) from an external-cavity laser diode whose coherence time was sufficiently long. The repetition rate of 1 GHz (i.e., the pulse interval = 1 ns) was chosen according to the time resolution of our photon detection system. Each pulse was then quasi-randomly phase-modulated by 0 or π, attenuated so that there was an average 0.1–0.2 photons per pulse, and launched into a fiber line. At the receiver, the incoming pulses passed through a glass-waveguide Mach–Zehnder interferometer whose length difference of 20 cm corresponded to a pulse interval of 1 ns. Frequency-conversion photon detectors [18], described in Section III-A, were placed at the interferometer outputs, and a time interval analyzer recorded the photon arrival time and which detector clicked.

A key device in our experiment was a waveguide interferometer, which was fabricated by using the planar lightwave circuit (PLC) technologies [32]. The waveguide structure provided stable operation. Fig. 10 shows the interferometer characteristics, and plots the extinction ratio as a function of the waveguide chip temperature. The device was polarization dependent due to the waveguide birefringence, and so the best and worst extinction ratios for different input polarization states were evaluated at each temperature. The figure shows that the extinction ratio was better than -20 dB even in the worst case. The excess loss was 2.5 dB (fiber-to-fiber).

Another key device was a frequency-conversion photon detector. A feature of our DPS system is that it has a high clock rate (compared with other QKD experiments) due to the fact that we use a consecutive pulse train. Photon detectors that can count a photon at any time are preferable if we are to fully utilize this. The nongating operation of the frequency-conversion detector was favored in this regard. A high photon detection rate, meaning a high key creation rate, was achievable through the use of this detector.

The detectors should have a high detection efficiency to realize a large key creation rate and a small dark count rate to achieve a long distance. Unfortunately, however, there is a trade-off between efficiency and dark count in our device. When the pump power launched into the PPLN was increased to increase the frequency conversion efficiency, the dark counts also increased. This might be due to the Raman scattering photons that are spontaneously generated in the system. Then, we examined two operating conditions in QKD experiments; a detection efficiency of 8.8% for short or medium length fiber and a value of 2.0% for long fiber.

The experimental results are shown in Fig. 11, where the creation rates of a secure key after error correction and privacy amplification are plotted as a function of fiber length. Here, information leakage through a combination of a beam splitting attack and a partial intercept–resend attack was assumed in the privacy amplification. A record length of 105 km was achieved for a secure key in our experiment, mainly because of the robustness of the DPS protocol against a PNS attack. The key creation rate was also two orders of magnitude higher than conventional data (Fig. 4), mainly because of the continuous operation of

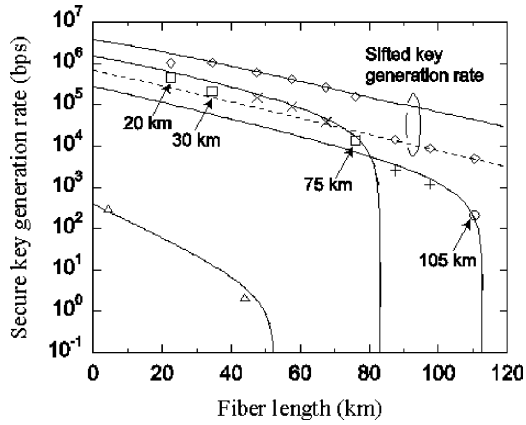

Fig. 11. Experimental results for the secure key creation rate as a function of fiber length. Squares: fiber transmission with detector efficiency of 8.8%; circle: fiber transmission with detector efficiency of 2.0%; plus symbols: simulation experiment using attenuator with detector efficiency of 2.0%; and crosses: simulation experiment using attenuator with detector efficiency of 2.0%. Diamonds denote the corresponding data before error correction and privacy amplification. For comparison, results reported in [33] are shown by triangles, where secure keys are created by the BB84 protocol with InGaAs-APD detectors.

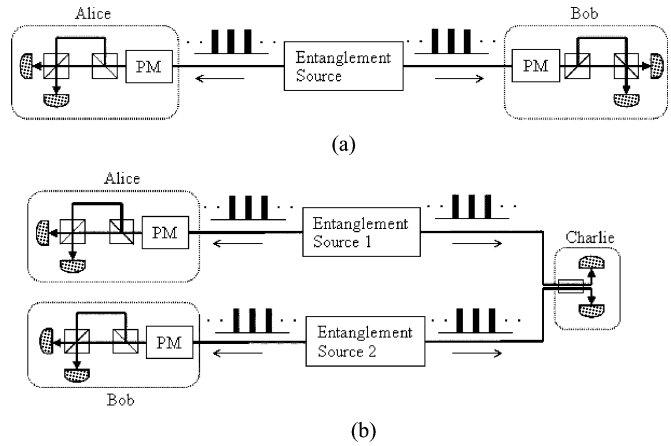

Fig. 12. Configurations of QKD utilizing quantum entangled photons. PM: phase modulator.

the frequency-conversion detectors. These experiments demonstrated the feasibility and high performance of the DPS protocol.

V. Entanglement-Based QKD

The above mentioned systems are simple point-to-point, nonrepeating QKD systems that have a distance limitation because photons vanish before reaching a receiver due to transmission loss. In conventional optical communication systems, it is quite common to use optical amplifiers or repeaters to increase the transmission distance. Unfortunately, such technologies cannot be applied to QKD systems, since a single-photon signal is buried in the amplified spontaneous emission in optical amplifiers or is not preserved through O/E/O conversion. Instead, quantum repeater and quantum relay techniques have been proposed, which utilize quantum entangled photon pairs [34]–[39].

Fig. 12 shows examples of entanglement-based QKD systems [38]. An entangled photon pair is a pair of photons with a unique correlation, such that the property of one photon is automatically and instantly determined at the moment the other photon's property is measured, while their properties are ambiguous in principle before the measurement. For QKD operation, one of an entangled photon pair is delivered to Alice and the other to Bob, who measure these photons at their own site, as shown in Fig. 12(a). The results of each measurement have some correlation due to the entanglement nature, from which Alice and Bob create a secret key. In this system, a photon travels half the distance between Alice and Bob. Thus, roughly speaking, the effective QKD distance is twice that in a simple point-to-point system.

A further increase is possible by using the configuration shown in Fig. 12(b). Entanglement sources 1 and 2 deliver one of photon pairs to Alice and Charlie, and Bob and Charlie, respectively. Charlie carries out a joint measurement on photons from sources 1 and 2, by which the relationship between photons from sources 1 and 2 is determined. Charlie informs the measurement result to Alice and Bob, who measure the photons from sources 1 and 2, respectively. From their own measurement results and Charlie's information, Alice and Bob know the measurement results at the other site, from which they create a secret key. The distance between Alice and Bob can be increased by using this scheme.

The above mentioned is a quantum relay system. A quantum repeater is a more sophisticated method [34], where a quantum memory, nondemolition measurement, and entangle purification are used to make perfect entangled photons and to enlarge the transmission distance.

Although the implementation of entanglement-based systems posses a challenge, they present the possibility of realizing long-distance QKD systems.

VI. Summary

This paper presented an overview of QC technologies. A typical QKD protocol, BB84, was described, including its configuration and operating mechanism, its security against eavesdropping, and the present state of the art as regards implementation. Differential phase shift QKD, a recently proposed protocol by the author, was presented. Quantum-entanglement-based QKD systems that extend the transmission distance were also mentioned as a topic for future study.

Acknowledgment

The author would like to thank T. Honjo and Dr. H. Takesue of NTT Basic Research Laboratories for their collaboration with this study and Prof. Y. Yamamoto and his group at Stanford University for guiding them to this field.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Jan. 2002.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.
[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992.
[5] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb. 1992.
[6] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion in advances," in *Cryptography—EUROCRYPT'93,* Lecture Notes in Computer Science, vol. 765, T. Helleseth, Ed. Berlin, Germany: Springer-Verlag, 1994, pp. 410–423, Springer-Verlag
[7] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pt. part 2, pp. 1915–1923, Nov. 1995.
[8] N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, May 2000.
[9] A. Acin, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A*, vol. 69, p. 012309, Jan. 2004.
[10] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto, "Quantum cryptography with a photon turnstile," *Nature*, vol. 420, p. 762, Dec. 2002.
[11] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementation," *Phys. Rev. Lett.*, vol. 92, p. 067901, Feb. 2004.
[12] W. Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, Aug. 2003.
[13] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection," *Phys. Rev. A*, vol. 68, p. 042331, Oct. 2003.
[14] R. Namiki and T. Hirano, "Practical limitation for continuous-variable quantum cryptography using coherent state," *Phys. Rev. Lett.*, vol. 92, p. 117901, Mar. 2004.
[15] A. Tomita and K. Nakamura, "Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm," *Opt. Lett.*, vol. 27, pp. 1827–1829, Oct. 2002.
[16] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, pp. 3762–3764, Apr. 2004.
[17] M. A. Albota and F. N. C. Wong, "Efficient single-photon counting at 1.55 mm by means of frequency upconversion," *Opt. Lett.*, vol. 29, pp. 1449–1451, Jul. 2004.
[18] C. Langrock, E. Diamanti, R. V. Roussev, Y. Yamamoto, M. M. Fejer, and H. Takesue, "Highly efficient single-photon detection at communication wavelength by use of upconversion in reverse-proton-exchanged periodically poled $LiNbO_3$ waveguide," *Opt. Lett.*, vol. 30, pp. 1725–1727, Jul. 2005.
[19] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play' systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, pp. 793–795, Feb. 1997.
[20] T. Honjo and K. Inoue, "Plug and play quantum key distribution using modulation sidebands for frequency shifting," *Jpn. J. Appl. Phys.*, to be published.
[21] T. Hasegawa, T. Nishioka, H. Ishizuka, J. Abe, and M. Matsui, "Experimental realization of quantum cryptography over 87 km," presented at the CLEO/QUELS 2003, Paper QTuB1.
[22] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using balanced gated-mode photon detector," *Electron. Lett.*, vol. 39, no. 16, pp. 1199–1201, Aug. 2003.
[23] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, *Quantum key distribution over 67 km with a plug & play system. quant-ph/0203118*, Mar. 2002.
[24] O. L. Guerreau, J.-M. Merolla, A. Soujaeff, F. Parois, J.-P. Goedgebuer, and F. J. Malassenet, "Long-distance QKD transmission using single-sideband detection scheme with WDM synchronization," *IEEE J. Sel. Topics Quantum Electron.*, vol. 9, no. 6, pp. 1533–1540, Nov.–Dec. 2003.
[25] A. Yoshizawa, R. Kaji, and H. Tsuchida, "10.5 km fiber-optic quantum key distribution at 1550 nm with a key rate of 45 kHz," *Jpn. J. Appl. Phys.*, vol. 43, pp. L735–L737, May 2004.
[26] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, p. 037902, Jul. 2002.
[27] ——, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, p. 022317, Aug. 2003.
[28] T. Honjo and K. Inoue, "Differential-phase-shift QKD with an extended degree of freedom," *Opt. Lett*, to be published.
[29] K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," *Phys. Rev. A*, vol. 71, p. 042305, Apr. 2005.
[30] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer," *Opt. Lett.*, vol. 29, pp. 2797–2799, Dec. 2004.
[31] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution over 105 km fiber," *New J. Phys.*, vol. 7, p. 232, Nov. 2005.
[32] A. Himeno, K. Kato, and T. Miya, "Silica-based planar lightwave circuits," *IEEE J. Sel. Topics Quantum Electron.*, vol. 4, no. 6, pp. 913–924, Nov.–Dec. 1998.
[33] C. Gobby, Z. L. Yuan, and A. J. Shields, "Unconditionally secure quantum key distribution over 50 km of standard telecom fiber," *Electron. Lett.*, vol. 40, no. 25, pp. 1603–1605, Dec. 9, 2004.
[34] H. J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operation in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, Dec. 1998.
[35] B. C. Jacobs, T. B. Pittman, and J. D. Franson, "Quantum relays and noise suppression using linear optics," *Phys. Rev. A*, vol. 66, p. 052307, Nov. 2002.
[36] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attack," *Phys. Rev. A*, vol. 65, p. 052310, Apr. 2002.
[37] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, "Long distance quantum teleportation in a quantum relay configuration," *Phys. Rev. Lett.*, vol. 92, p. 047904, Jan. 2004.
[38] K. Inoue, "Quantum key distribution using a series of quantum correlated photon pairs," *Phys. Rev. A*, vol. 71, p. 032301, Mar. 2005.
[39] D. Collins, N. Gisin, and H. de Riedmatten, "Quantum relays for long distance quantum cryptography," *J. Mod. Phys.*, vol. 52, pp. 735–753, Mar. 2005.

Kyo Inoue (M'92) was born in Tokyo, Japan, in 1959. He received the B.S. and M.S. degrees in applied physics and the Ph.D. degree in electrical engineering from Tokyo University, Tokyo, in 1982, 1984, and 1997, respectively.

In 1984, he joined Nippon Telegraph and Telephone Corporation (NTT), Kanagawa, Japan, where he studied optical communications (including Mach–Zehnder filters, optical amplifiers, four-wave mixing-in fiber, and all-optical functional devices) and quantum communications. From 2001 to 2003, he was on leave from NTT as a Visiting Scholar at Stanford University, Stanford, CA. In 2005, he joined Osaka University, Osaka, Japan, where he is currently a Professor.

Dr. Inoue is a member of IEEE/LEOS, Japan Society of Applied Physics, and the Institute of Electronics, Information and Communication Engineers of Japan.