# Differential Phase-Shift Quantum Key Distribution Systems

Kyo Inoue

*(Invited Paper)*

***Abstract*—Differential phase-shift (DPS) quantum key distribution (QKD) is a unique QKD protocol that is different from traditional ones, featuring simplicity and practicality. This paper overviews DPS-QKD systems.**

***Index Terms*—Quantum key distribution, quantum mechanics, phase shift keying.**

## I. Introduction

QUANTUM key distribution (QKD) provides a secret key to distant parties for ciphering/deciphering a message, whose security is based on quantum mechanics [1]. The first QKD protocol called BB84 was proposed in 1984 and has been widely studied and developed. Differential phase-shift (DPS) QKD is another QKD scheme proposed about two decades after BB84 [2], [3], which has a unique structure different from BB84, featuring simplicity and practicality. This paper overviews DPS-QKD systems.

## II. Configuration and Operation

The configuration of DPS-QKD is shown in Fig. 1. A transmitter (Alice) sends a highly attenuated coherent pulse train that is randomly phase-modulated by $\{0, \pi\}$ for each pulse. The transmitted signal power is so small that the average photon number per pulse is less than one, e.g., 0.2. A receiver (Bob) receives the transmitted signal with a one-pulse delay Mach–Zehnder interferometer. In the interferometer, adjacent pulses interfere with each other, as illustrated in Fig. 1, and photons are detected according to the phase difference between the interfering pulses such that detector 1 (or 2) clicks for a phase difference of 0 (or $\pi$). Here, photon detection occurs rarely and randomly because of the small number of photons in the pulse train. After signal transmission, Bob tells Alice the photon detection time through a classical channel. With this time information and her phase modulation data, Alice knows which detector clicked at Bob. Then, Alice and Bob obtain identical bit strings, provided that detector 1 (or 2) is assigned to bit 0 (or 1), which can be a secret key.

The features of this protocol are simplicity and high key creation efficiency. The traditional QKD protocol BB84 includes a basis selection procedure, and basis-mismatched photons are discarded. On the other hand, the DPS protocol needs no such process and all detected photons contribute to key bits, resulting in a higher key creation efficiency. The fact that there is no need for the basis selection is also beneficial in terms of receiver complexity and detectors' dark count errors. Practical BB84 systems usually employ a combination of a beam splitter (BS) and two sets of measurement apparatus for the basis selection, where four photon detectors are used. On the other hand, the DPS protocol uses one measurement apparatus with two detectors, i.e., a simpler receiver configuration. In addition, the smaller number of detectors causes lower dark counts, resulting in a larger number of secure key bits after error correction and privacy amplification.

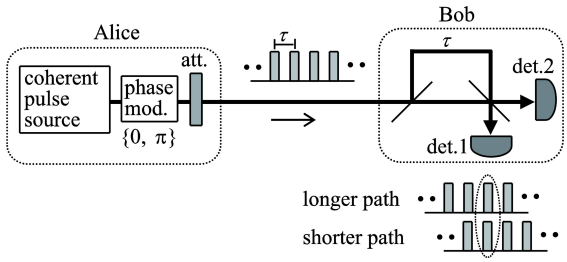


Fig. 1. Configuration of DPS-QKD. att: optical attenuator, $\tau$: time interval of pulses.

Using sequential pulses, each of which can contribute to a key bit, is another feature. The time domain is efficiently utilized, resulting in a high key creation speed in practice. Robustness against photon-number splitting attacks, even when using weak coherent light, is another advantage of the DPS protocol, which is described in more detail in the following section.

## III. Security Issues

The security of DPS-QKD is based on the fact that weak coherent pulse sequences with different $\{0, \pi\}$-phases for each pulse are utilized, which are nonorthogonal with each other and thus cannot be perfectly distinguished by an eavesdropper (Eve). Nevertheless, the security of DPS-QKD has not been fully analyzed in terms of quantum mechanics, owing to its unique structure different from that of traditional QKD protocols. This section describes the security issues of the DPS protocol clarified for the present.

### A. Beam Splitting Attack

The typical and simplest eavesdropping against QKD that uses coherent light is a beam splitting attack. Eve replaces the

Manuscript received July 15, 2014; revised September 12, 2014; accepted September 19, 2014.

The author is with Osaka University, Osaka 565-0871, Japan (e-mail: kyo@comm.eng.osaka-u.ac.jp).

Digital Object Identifier 10.1109/JSTQE.2014.2360362

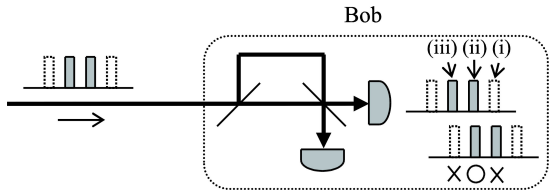


Fig. 2. Bob's detection during intercept-resend attack.

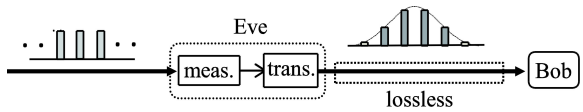


Fig. 3. Sequential attack with amplitude modulation. Lossless transmission line is installed by Eve in order to compensate photon loss resulting from eavesdropping where a fake signal is resent only when Eve consecutively measures pulses.

transmission line by a lossless one, splits and stores Alice's signal with a fraction corresponding to the original transmission loss, and measures the split signal after Bob's detection time is disclosed. This strategy does not change Bob's receiving signal and cannot be noticed at all.

However, the amount of information leaked to Eve through this eavesdropping is limited because of the small photon number in DPS signals. In measuring the split and stored signal, Eve attempts to identify the phase difference between two neighboring pulses from which Bob detected a photon and created a key bit. Here, the corresponding pulses include $2r\mu$ photons on an average, where $\mu$ is the mean photon number sent from Alice per pulse and $r$ is the beam-splitting ratio that is equal to the original transmission loss. Thus, the information rate leaked to Eve through the beam split attack is $2r\mu$, which is small for a small mean photon number $\mu$ and can be excluded from the key bits by privacy amplification [4].

### B. Intercept Resend Attack

Another typical eavesdropping strategy is the intercept-resend attack. Eve intercepts and measures every pulse sent from Alice and resends a fake signal to Bob according to the measurement result. However, Eve cannot measure every phase difference because of the small photon number, and cannot resend a full replica of Alice's signal. An imperfect fake signal causes a bit error in the signal received by Bob, from which the eavesdropping is revealed.

For example, Eve is supposed to measure Alice's signal using apparatus identical to Bob's shown in Fig. 1. She occasionally detects a photon and knows the phase difference between two corresponding pulses. In such a situation, she resends a photon super-positioned over two pulses with the measured phase difference, while sending vacuum at unmeasured time slots. Then, two isolated pulses arrive at Bob, who detects a photon possibly at three time slots as illustrated in Fig. 2: the first slot when the first pulse via the short path reaches the detectors, the second slot when the first pulse via the long path and the second pulse via the long path reach the detectors, and the third slot when the second pulse via the long path reaches the detectors. When a photon is detected at the second time slot, the two pulses interfere with each other, providing a correct bit to Bob. Bob does not notice the eavesdropping in this case. At the first and third time slots, on the other hand, there is no interference and a photon randomly clicks either one of the detectors. This detection event can cause Bob's bit error, from which the eavesdropping is revealed. The probability of a photon being detected at the first or third time slot is 1/2, and thus the bit error rate induced by the eavesdropping is 1/4.

### C. Sequential Attack

A sequential attack [5]–[9] is a kind of intercept-resend attacks. In the example of intercept-resend attacks described in the previous subsection, a bit error is induced when a photon is detected at the first or third time slot, i.e., the edge slots, at which no interference occurs. In order to reduce this bit error rate, Eve waits for consecutive detections and resends a pulse sequence with measured phases instead of two isolated pulses as a fake signal. For this fake signal, the probability of a photon being detected at the edge slots is smaller than that in the simple intercept-resend attack described in the previous subsection. In addition, Eve modulates the envelope of the pulse sequence so that the amplitudes of the edge pulses is smaller than that of the middle pulses, as illustrated in Fig. 3. The photon probability at the edge slots is further reduced with this resending strategy. Subsequently, Bob's bit error rate resulting from no interfering detection at the edge slots becomes smaller than that in the simple intercept-resend eavesdropping.

Several studies have been reported on sequential attacks. They include an attack using the same apparatus as Bob's in the intercepting stage [5], one conducting unambiguous state discrimination (USD) measurement for each pulse [6]–[8], and one conducting USD for phase differences between adjacent pulses [9]. Regarding the pulse envelope resent by Eve, the first two reports [5], [6] assume a rectangular shape, the third one [7] assumes a Gaussian, and the last two [8], [9] optimize the envelope to make Bob's error rate lowest. The last strategy, that employs the USD for phase differences and the optimized pulse envelope, is the most threatening for DPS-QKD systems with large transmission loss, i.e., long-distance systems, among other specific eavesdropping.

### D. Photon Number Splitting Attack

Photon number splitting (PNS) attacks are known to be serious eavesdropping against BB84 using weak coherent light [10], [11]. In order to prevent this eavesdropping, a decoy method [12]–[14] is usually employed in practical BB84 systems, making the key creation process complicated. The DPS protocol, on the other hand, is robust against PNS attacks [15]. In PNS attacks, Eve probes the photon number included in a transmitted signal, and picks up and measures an extra photon when more than two photons are included. Unfortunately for Eve, the phase information of a DPS signal collapses when the photon number is probed, and, as a result, bit errors are induced at Bob. Thus,

PNS attacks are readily revealed in DPS-QKD systems. This is one of the advantages of the DPS protocol compared with the original BB84 protocol.

### *E. General Individual Attack*

General individual attack [5] is conceptual eavesdropping that attacks each key bit (where "individual" does not mean each pulse but each single-photon in a pulse train). Eve takes each single-photon super-positioned over Alice's pulse sequence (though it is questionable how to do it for a long sequence including a lot of photons), makes a unitary interaction with her probe state, and measures the probe state after Bob's photon detection time is announced. The analysis in [5] concludes that the upper bound of the secure key creation rate *R* determined by this eavesdropping is given by

$$R = -p_{\text{click}}[-(1-2\mu)\log_2 P_{c0}(e) + f(e)h(e)] \qquad (1)$$

with

$$P_{c0}(e) = 1 - e^2 - \frac{(1-6e)^2}{2}$$

where $p_{\text{click}}$ is Bob's photon detection probability, $\mu$ is the mean photon number per pulse, $e$ is the system error rate, $h(e) = -e\log_2 e - (1-e)\log_2(1-e)$, and $f(e)$ is a redundancy factor from the Shannon limit. Many DPS-QKD experiments conducted to date have employed the above equation for evaluating their system performance.

### *F. Side-Channel Attack*

Recent QKD studies focus on side-channel attacks, which take advantage of imperfections in actual devices used in practical QKD systems. Such an attack was also proposed against a DPS-QKD system equipped with superconducting single-photon detectors (SSPDs) [16]. Utilizing the operation characteristics of a SSPD, Eve arbitrarily manipulates the SSPD click by injecting bright blinding light. She can then obtain the complete key bit information by an intercept-resend attack using bright light as a fake signal. A countermeasure against this bright illumination attack has also been proposed [17].

However, this eavesdropping can be noticed by monitoring the light power received by Bob. Based on [18], the injection light power should be greater than $-30$ dBm for Eve to perform the bright light illumination attack, which can be easily monitored by a handy optical power meter.

### *G. Sophisticated Attacks*

Collective attacks or coherent attacks are the most sophisticated eavesdropping against QKD systems, where Eve prepares a probe state and makes it interact with Alice's signal as a whole, and then measures the probe state after post information is exchanged between Alice and Bob. General analysis for such eavesdropping against DPS-QKD is difficult, because Alice's pulses last long (e.g., a 4-h continuous operation with a 1-GHz pulse repetition rate was demonstrated in [19]) and the length and the temporal position of one sequence can be arbitrarily selected by Bob in the signal processing stage after detecting photons.

Several studies on conditional collective attacks have been reported instead. They include eavesdropping that attacks pairs of adjacent pulses [20], one assuming that Alice's pulse sequence includes just one photon [21], one against noiseless systems [22], and one attacking blocks of a pulse sequence with a fixed length where the carrier phase is random for each block [23]. The results in the last report [23] indicate that the system performance of DPS-QKD in terms of the transmission distance is worse than that of BB84 with a decoy method. The first report [20] analyses another QKD scheme called the coherent-one-way (COW) protocol [24] as well as DPS-QKD, which suggests that the system performances of COW and DPS are similar but DPS is somewhat better than COW. Nevertheless, it is an open question whether to assume a given length of one signal sequence is appropriate for DPS-QKD systems where Bob can arbitrarily select one sequence (i.e., a series of pulses from which a key string is created) from Alice's consecutive signal and thus Eve does not know which series of pulses should be interacted with her probe state.

## IV. Experiments

Since the first proposal of DPS-QKD, a number of experiments have been performed.

The first experiment over a fiber line was reported in 2004 [25]. The main feature of this experiment was the use of a waveguide interferometer. In phase-encoded QKD systems in general, the stability of interferometers used to decode phase information is an issue for system implementation. A waveguide interferometer was employed for the first time in this experiment, owing to which the stable QKD operation was achieved without phase stabilization circuits. A laser source with a narrow spectral linewidth was also a key device used in this experiment. In conducting a DPS-QKD experiment, the carrier phase in a pulse train should be stable for Bob to create correct bits. In order to achieve this, an external-cavity semiconductor laser with a spectral linewidth of about 200–300 kHz was employed for a 1-GHz pulse repetition rate. The requirement for the laser linewidth used in DPS-QKD systems was quantitatively investigated in [26].

The benchmark experiment was reported in 2007 [27], using superconducting single-photon detectors. QKD transmission over a 200-km fiber was achieved on account of the low dark count rate of the detectors. A long-distance QKD experiment over 260 km was also reported employing the DPS protocol [28]. These experiments assume the general individual attack described in Section III-D, which is less powerful than the sequential attacks mentioned in Section III-C. Thus, unfortunately, the secret keys created in those experiments are not perfectly secured [8], [9].

One feature of DPS-QKD is a high key creation rate owing to efficient usage of the time domain and efficient usage of detected photons, i.e., no detected photon is discarded. High speed QKD experiments have been also reported using the DPS protocol,

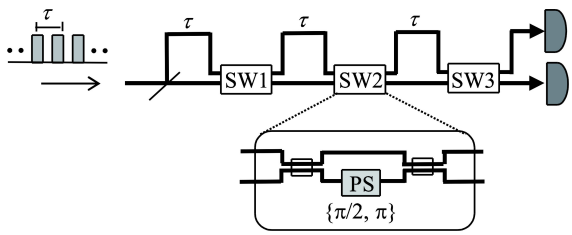


Fig. 4. Bob's setup in delay selected DPS-QKD. SW denotes a Mach–Zehnder interferometer switch and PS denotes a phase switch.

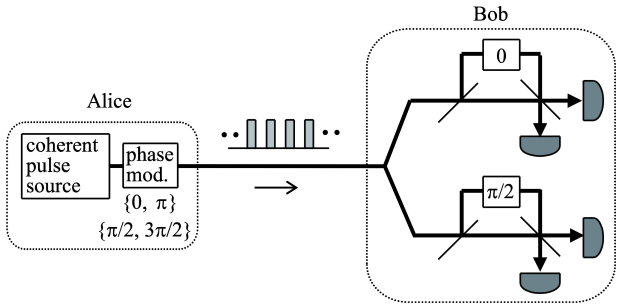


Fig. 5. Four-level differential-phase-shift quantum key distribution.

involving a key creation speed of 1.3-Mbps over 10-km [29] and that of 24-kb/s over 100-km [30].

Practicality is also a feature of DPS-QKD. Field experiments have been conducted [19], [31], confirming the feasibility in practical environments.

## V. Extended Schemes

In order to improve the system performance or practicality, several schemes extended from the original DPS protocol have been proposed. Although the quantitative system performances of these schemes are not clarified at the present when even the original DPS protocol is not fully analyzed, this section introduces such schemes to show potential extensibilities of DPS-QKD.

### A. Delay Selected DPS-QKD

In DPS-QKD, Bob creates a key bit from the phase difference between neighboring pulses. A one-pulse delay interferometer is used for measuring the phase difference. An extended version of DPS-QKD is a delay selected scheme, where Bob arbitrarily chooses an interfering pulse-pair by selecting the delay time in an interferometer [32].

Fig. 4 shows an example of Bob's setup for implementing this scheme, where the number of selectable time delays is three. The setup consists of a beam splitter, symmetric Mach–Zehnder (MZ) interferometer switches in series (SW1, SW2, and SW3), and delay lines connecting these switches. The delay time of each delay line is equal to the time interval of incoming pulses. The MZ switch operates either as a 50:50 beam splitter (BS) or a through-connector (TC). The mode of the operation is chosen by a phase switch attached in one arm in the MZ interferometer such that phases of $\pi/2$ and $\pi$ select the former and latter operations, respectively. With this receiver setup, Bob selects the time interval of interfering pulses from which a key bit is created, such that the time interval is $\tau$, $2\tau$, or $3\tau$ when {SW1 = "BS," SW2 = "TC," SW3 = "TC"}, {SW1 = "TC," SW2 = "BS," SW3 = "TC"}, or {SW1 = "TC", SW2 = "TC", SW3 = "BS"}, respectively, where $\tau$ is the time interval of neighboring pulses in the incoming signal.

This delay-selected DPS protocol improves the security. Bob randomly selects the delay time, which cannot be predicted by Eve. Thus, the ambiguity for Eve about which pulse pair should be attacked is enhanced, and the security is improved as a result. For example, when Eve tries the simple intercept-resend attack described in Section III-B, Bob's error rate induced by eavesdropping becomes [32]

$$P_{\mathrm{e}} = \frac{1}{2}\left(1 - \frac{1}{2M}\right) \tag{2}$$

where $M$ is the number of candidates of the time delay. For a large $M$, this error rate is close to 1/2, meaning that Eve obtains almost no information.

An ultimate extension of the above idea is a system in which Bob arbitrarily selects two interfering pulses out of $L$ pulses with $L$ being the number of pulses in one sequence of Alice's signal. This system was proposed and analyzed in [33], which shows that the production length of a secure key will be

$$G = N\left[1 - h(e_{\mathrm{bit}}) - h\left(\frac{\nu_{\mathrm{th}}}{L-1}\right)\right] \tag{3}$$

where $N$ is the sifted key length (i.e., the number of detected photons), $h$ denotes Shannon entropy $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$, $\nu_{\mathrm{th}}$ is the critical photon number satisfying $\nu_{\mathrm{th}} < (L-1)/2$, and $L$ is the number of pulses in one sequence. The second and third terms in (3) represent the key compression rates caused by error correction and privacy amplification, respectively. It is noteworthy that the privacy amplification factor, i.e., the third term, is independent of perturbation caused by eavesdropping unlike conventional QKD protocols. This is a unique feature of this system, though its implementation is hard in practice.

### B. Four-Level DPS-QKD

As suggested in Section III, the security issue is a weakness of DPS-QKD, compared with BB84. With this background, a scheme introducing a concept of BB84 into the DPS protocol was proposed [34].

Fig. 5 shows the configuration of the scheme. Alice sends a weak coherent pulse train in which each pulse is randomly phase-modulated by $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$ instead of just by $\{0, \pi\}$ in the original DPS protocol. Bob receives the signal with two delay interferometers followed by photon detectors, where the phase differences in the interferometers are 0 and $\pi/2$, respectively. The interferometers with 0 and $\pi/2$ phase differences distinguish the differential phase of $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$, respectively.

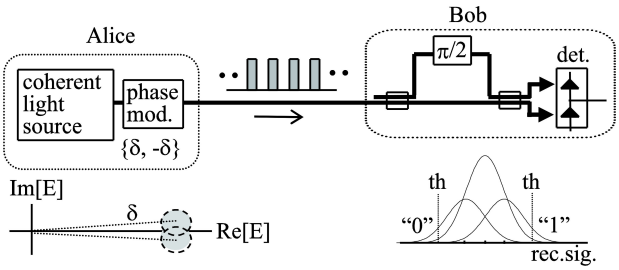


Fig. 6. Macroscopic differential-phase-shift quantum key distribution. "th" denotes threshold.

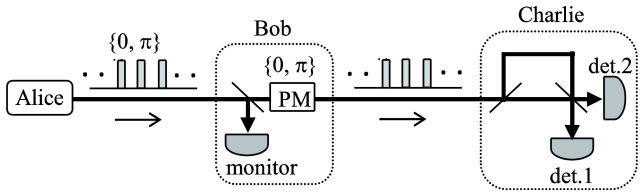


Fig. 7. DPS quantum secret sharing. PM: phase modulator.

The two sets of differential phases of $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$ form two nonorthogonal bases and the concept of BB84 of using two nonorthogonal bases is introduced in this scheme. As a result, the ambiguousness for Eve to identify key bits is enhanced and the security improvement can be expected. For example, this scheme is robust against the sequential attacks described in Section III-C, because the USD performance is low for nonorthogonal four states. Note that robustness of DPS-QKD against PNS attacks is still achieved because of the use of a coherent pulse sequence, though the other feature of simplicity is lost.

### C. Macroscopic DPS-QKD

Continuous variable QKD using conventional photo-detectors instead of single-photon detectors has been studied [1]. Its security relies on the quantum noise of coherent light, and post-selection and reverse reconciliation enable QKD transmission over a lossy channel. DPS-QKD can be also implemented using conventional photo-detectors.

Fig. 6 shows the configuration of such a system [35]. Alice sends coherent light randomly phase-modulated by $\{\delta, -\delta\}$. Its intensity is so high as to be detected by a conventional photo-detector, and $\delta$ is so small that the two signal states partially overlap with each other due to the quantum noise, as illustrated in Fig. 6. Bob receives the signal by a delay interferometer with a phase difference of $\pi/2$, and the outputs of the interferometer are coupled into a balanced detector. The detected signal has three output levels corresponding to differential phases of $+2\delta$, 0, and $-2\delta$ in the incoming signal, accompanied with fluctuations due to the quantum noise, as illustrated in Fig. 6. For this signal distribution, Bob sets two thresholds; one at the higher-side tail of the peak corresponding to $+2\delta$, and the other at the lower-side tail of the peak corresponding to $-2\delta$, as shown in Fig. 6. He creates bits "1" and "0" when the signal is larger and smaller than the upper and lower thresholds, respectively. These detection events occur occasionally and randomly, and cannot be predicted by Eve. This situation is equivalent to the photon detection event in the original DPS-QKD system. Subsequently, Alice and Bob share a secret key via procedures similar to the original DPS protocol.

The security of this scheme relies on the fact that the two signal states of $\{\delta, -\delta\}$ are nonorthogonal and thus cannot be perfectly distinguished by Eve. Reverse reconciliation is also helpful to enhance security, as in conventional continuous variable QKD. The setup of this QKD system is the same as that of optical differential-phase-shift keying (DPSK) systems well-developed in conventional optical communication. Therefore, this scheme is readily implemented with off-the-shelf devices, whereas conventional continuous variable QKD systems need homodyne detection with phase-locked local light.

### D. DPS Quantum Secret Sharing

Quantum secret sharing (QSS) is a type of QKD, which distributes a full key to one party (Charlie) and partial keys to two parties (Alice and Bob). While neither Alice nor Bob can decipher Charlie's ciphered message with his/her partial key alone, they can decipher the message only when using their keys together. This QSS operation can be achieved based on the idea of the DPS protocol.

Fig. 7 shows the configuration of such a system [36]. Alice sends a DPS signal, i.e., a weak coherent pulse train phase-modulated by $\{0, \pi\}$ for each pulse, to Bob. Bob additionally imposes $\{0, \pi\}$-phase modulation onto the incoming signal while monitoring the incident power, and sends the signal to Charlie. Charlie receives it with a delay interferometer followed by photon detectors, where detector 1 (or 2) clicks when the differential phase is 0 (or $\pi$). He creates bit "0" and "1" from the clicks of detectors 1 and 2, respectively.

In this signal transmission, Charlie's measurement result is an exclusive OR of Alice's and Bob's phase modulation. Thus, Alice and Bob can know Charlie's bits only when they collaborate, i.e., the secret sharing function is achieved. The security of shared keys relies on the use of a weak coherent pulse train, as in DPS-QKD.

A unique function required for QSS is to prohibit one party from knowing the others' key by oneself. The monitoring detector in Bob's site is equipped to prevent Alice from probing Bob's key by sending strong pulses and measuring them after Bob.

### E. Entanglement-Based Scheme

Entanglement-based QKD increases the transmission distance, where an entanglement source positioned at the middle between Alice and Bob sends quantum-entangled signal to each of them. Alice and Bob measure the received signals while selecting measurement basis (in case of BBM92 [37]), and then create key bits from basis-matched detections. The feature of DPS-QKD viz., no basis selection is applicable to entanglement-based QKD.

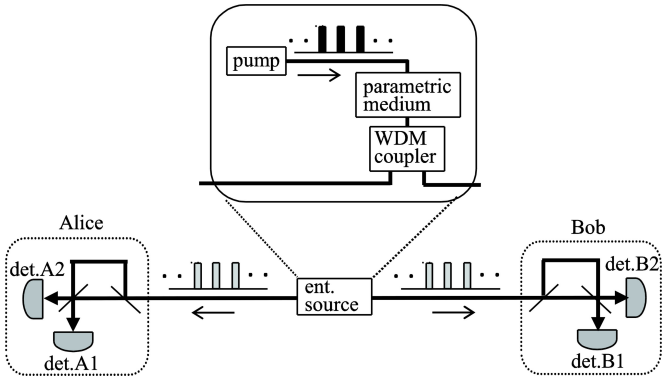


Fig. 8. Entanglement based DPS-QKD. WDM coupler: wavelength division multiplexing coupler, ent.source: time-bin entanglement source.

Fig. 8 shows the configuration of such a system [38]. An entanglement source positioned between Alice and Bob generates a sequence of time-bin entangled photon pairs by injecting a coherent pump pulse train into an optical parametric medium, and sends each of the photon pair to Alice and Bob, respectively. The mean photon number in the generated photon sequence is adjusted to be small as in DPS-QKD, which is made by the pump power. Alice and Bob measure the received photon sequence with delay interferometers followed by photon detectors. Here, the detection events are correlated between Alice and Bob such that when both of them detect photons at an identical time slot, detector 1 (or 2) clicks both at Alice and Bob. From this correlation, secret key bits are created. The security of the transmitted photon sequence relies on the same mechanism as in DPS-QKD.

## VI. Summary

In this paper, DPS quantum key distribution was overviewed. DPS-QKD has a unique structure different from traditional QKD protocols, i.e., no basis selection procedure, featuring simplicity and practicality. Extended schemes based on the idea of the DPS protocol were also described. The traditional BB84 protocol has been widely studied and developed both experimentally and theoretically. The DPS protocol, on the other hand, has not been well analyzed owing to its unique structure. Further studies are expected.

## References

[1] V. Scarani, H. Pasquinucci, N. Cerf, M. Dušek, and N. Lütkenhaus, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Jul.–Sep. 2009.

[2] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, pp. 037902-1–037902-3, Jul. 2002.

[3] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, pp. 022317-1–022317-3, Aug. 2003.

[4] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[5] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," *Phys. Rev. A*, vol. 73, no. 7, pp. 012344-1–012344-9, Jan. 2006.

[6] M. Curty, L. L. Zhang, H. -H. Lo, and N. Lütkenhaus, "Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states," *Quant. Inf. Comput.*, vol. 7, no. 7, pp. 665–688, 2007.

[7] T. Tsurumaru, "Sequential attack with intensity modulation on the differential-phase-shift quantum key distribution protocol," *Phys. Rev. A*, vol. 75, no. 6, pp. 062319-1–062319-6, Jun. 2007.

[8] M. Curty, K. Tamaki, and T. Moroder, "Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks," *Phys. Rev. A*, vol. 71, no. 77, pp. 052321-1–052321-20, May 2008.

[9] H. Gomez-Sousa and M Curty, "Upper bounds on the performance of differential-phase-shift quantum key distribution," *Quantum Inf. Comput.*, vol. 9, no. 1/2, pp. 62–80, 2009.

[10] B. Huttuner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, no. 3, pp. 1863–1869, Mar. 1995.

[11] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug. 2000.

[12] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, pp. 057901-1–057901-4, Aug. 2003.

[13] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, pp. 230503-1–230503-4, Jun. 2005.

[14] H. -H. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, pp. 230504-1–230504-4, Jun. 2005.

[15] K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," *Phys. Rev. A*, vol. 71, no. 4, pp. 042305-1–042305-4, Apr. 2005.

[16] L. Lyderson, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocol," *J. Mod. Opt.*, vol. 58, no. 8, pp. 680–685, May 2011.

[17] T. Honjo, M. Fujiwara, K. Shimuzu, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Countermeasure against tailored bright illumination attack for DPS-QKD," *Opt. Exp.*, vol. 21, no. 3, pp. 2667–2675, Feb. 2013.

[18] M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, and M. Sasaki, "Characteristics of superconducting single photon detector in DSP-QKD system under bright illumination blinding attack," *Opt. Exp.*, vol. 21, no. 5, pp. 6304–6312, Mar. 2013.

[19] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, May 2011.

[20] C. Branciard, N. Gisin, and V. Scarani, "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography," *New J. Phys.*, vol. 10, pp. 013031-1–013031-25, Jan. 2008.

[21] K. Wen, K. Tamaki, and Y. Yamamoto, "Unconditional security of single-photon differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 103, pp. 170503-1–170503-4, Oct. 2009.

[22] Y. Zhao, C. F. Fung, Z. Han, and G. Guo, "Security proof of differential phase shift quantum key distribution in the noiseless case," *Phys. Rev. A*, vol. 78, no. 4, pp. 042330-1–042330-13, Oct. 2008.

[23] K. Tamaki, M. Koashi, and G. Kato, "Unconditional security of coherent-state-based differential phase shift quantum key distribution with block-wise phase randomization," [Cornell Univ. Library, e-print serv.] arxiv.org/abs/1208.1995, 2012.

[24] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, pp. 194108-1–194108-4, Nov. 2005.

[25] 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, no. 29, pp. 2797–2799, Dec. 2004.

[26] T. Honjo, T. Inoue, and K. Inoue, "Influence of light source linewidth in differential-phase-shift quantum key distribution systems," *Opt. Commun.*, vol. 284, pp. 5856–5859, Sep. 2011.

[27] 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 single-photon detector," *Nature Photon.*, vol. 1, pp. 343–348, Jun. 2007.

[28] S. Wang, W. Chen, J. Guo, Z. Yin, H. Li, Z. Zhou, G. Guo, and Z. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Opt. Lett.*, vol. 37, no. 6, pp. 1008–1010, Mar. 2012.

[29] Q. Zhang *et al.*, "Megabits secure key rate quantum key distribution," *New J. Phys.*, vol. 11, pp. 045010-1–045010-9, Apr. 2009.

[30] 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. Exp.*, vol. 19, no. 11, pp. 10632–10639, May 2011.

[31] T. Honjo, S. Yamamoto, T. Yamamoto, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, and K. Inoue, "Field trial of differential-phase-shift quantum key distribution using polarization independent frequency up-convertors," *Opt. Exp.*, vol. 15, no. 24, pp. 15920–15927, Nov. 2007.

[32] T. Honjo and K. Inoue, "Differential-phase-shift QKD with an extended degree of freedom," *Opt. Lett.*, vol. 31, no. 4, pp. 522–524, Feb. 2006.

[33] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, pp. 475–478, May 2014.

[34] K. Inoue and Y. Iwai, "Differential-quadrature-phase-shift quantum key distribution," *Phys. Rev. A*, vol. 79, no. 2, pp. 022319-1–022319-9, Feb. 2009.

[35] T. Kukita, H. Takada, and K. Inoue, "Macroscopic differential phase shift quantum key distribution using an optical pre-amplified receiver," *Jpn. J. Appl. Phys.*, vol. 49, pp. 122801-1–122801-11, Dec. 2010.

[36] K. Inoue, T. Ohashi, T. Kukita, K. Watanabe, S. Hayashi, T. Honjo, and H. Takesue, "Differential-phase-shift quantum secret sharing," *Opt. Exp.*, vol. 16, no. 20, pp. 15469–15476, Sep. 2008.

[37] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992.

[38] K. Inoue and H. Takesue, "Quantum key distribution using entangled-photon trains with no basis selection," *Phys. Rev. A*, vol. 73, no. 3, pp. 032332-1–032332-4, Mar. 2006.

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

From 1984 to 2005, he was with Nippon Telegram and Telephone Corporation, where his work involved optical communications and quantum communications. He is currently a Professor at Osaka University, Osaka, Japan.