

# Differential-phase-shift quantum secret sharing

K. Inoue,<sup>1,2,3</sup> T. Ohashi,<sup>1,3</sup> T. Kukita,<sup>1,3</sup> K. Watanabe,<sup>1,3</sup> S. Hayashi,<sup>1,3</sup> T. Honjo,<sup>2,3</sup> and H. Takesue<sup>2,3</sup>

<sup>1</sup> Osaka University, 2-1 Yamada-oka, Suita-shi, Osaka, 565-0871, Japan

<sup>2</sup> NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan

<sup>3</sup> CREST, JST, 4-1-8 Honcho, Kawaguchi-shi, Saitama, 332-0012, Japan

\*Corresponding author: [kyo@comm.eng.osaka-u.ac.jp](mailto:kyo@comm.eng.osaka-u.ac.jp)

**Abstract:** A quantum secret sharing (QSS) protocol based on a differential-phase-shift scheme is proposed, which quantum mechanically provides a full secret key to one party and partial keys to two other parties. A weak coherent pulse train is utilized instead of individual photons as in conventional schemes. Compared with previous QSS protocols, the present one features a simple setup, is suitable for fiber transmission, and offers the possibility for a high key creation rate. An experiment is also carried out to demonstrate the operation.

©2008 Optical Society of America

OCIS codes: (270.270) Quantum optics.

---

## References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145-195 (2002).
2. K. Inoue, "Quantum key distribution technologies," *IEEE J. Sel. Top. Quantum Electron.* **12**, 888-896 (2006).
3. M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A* **59**, 1829 (1999).
4. A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Phys. Rev. A* **59**, 162 (1999).
5. L. Xiao, G. Long, F. Deng, and J. Pan, "Efficient multiparty quantum-secret-sharing schemes," *Phys. Rev. A* **69**, 052307 (2004).
6. S. K. Singh and R. Srikanth, "Generalized quantum secret sharing," *Phys. Rev. A* **71**, 012328 (2005).
7. Z. Zhang, Y. Li, and Z. Man, "Multiparty quantum secret sharing," *Phys. Rev. A* **71**, 044301 (2005).
8. C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing," *Phys. Rev. Lett.* **95**, 230505 (2005).
9. H. Takesue and K. Inoue, "Quantum secret sharing based on modulated high-dimension time-bin entanglement," *Phys. Rev. A* **74**, 012315 (2006).
10. J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, "Active polarization in optical fibers suitable for quantum key distribution," *Opt. Express* **15**, 17928-17936 (2007).
11. G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," *Opt. Express* **16**, 1867-1873 (2008).
12. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A* **61**, 052304 (2000).
13. K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A* **68**, 022317 (2003).
14. E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," *Phys. Rev. A* **73**, 012344 (2006).
15. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion in advances," in *Cryptography-EUROCRYPT'93, Lecture Notes in Computer Science*, **765**, T. Hellesest, (Springer Verlag, Berlin, Germany, 1994), pp. 410-423.
16. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Info. Theory* **41**, 1915-1923 (1995).
17. 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.* **29**, 2797-2799 (2004).

## 1. Introduction

Quantum key distribution (QKD) is being studied to realize ultimate secure communications based on quantum mechanics [1, 2]. Quantum secret sharing (QSS) is a kind of QKD that distributes a full key to one party (Charlie) and partial keys to two parties (Alice and Bob) or more. Neither Alice nor Bob can decipher Charlie's ciphered message with her/his partial key alone. They can decipher the message only by using their keys together.

The first QSS protocol proposed by Hillery et al. uses a three-photon entangled Greenberger-Horne-Zeilinger (GHZ) state [3]. Although this scheme elegantly presents a quantum mechanical way of accomplishing the above secret sharing function, its implementation seems problematic due to the difficulty of preparing GHZ photons. Since this first proposal, several other QSS protocols have been presented [4-9]. Among them, the simplest one uses polarization-modulated single-photons [8], where single-photons in one of four polarization states are transmitted:  $\{ (|H\rangle + |V\rangle)/\sqrt{2}, (|H\rangle - |V\rangle)/\sqrt{2} \}$  and  $\{ (|H\rangle + i|V\rangle)/\sqrt{2}, (|H\rangle - i|V\rangle)/\sqrt{2} \}$  with  $|H\rangle$  and  $|V\rangle$  being the horizontal and vertical polarization states. This scheme is a QSS variant of the traditional BB84 QKD protocol, and looks more practical than entanglement-based protocols. A primitive experiment was also demonstrated [8]. However, this scheme requires a polarization controlling technique for fiber systems [10, 11], since the polarization state varies during fiber transmission. In addition, it will be fragile against the photon-number-splitting (PNS) attack when using weak coherent pulses as in the BB84 QKD protocol [12].

This paper proposes another QSS scheme without using entanglement. Its idea is based on differential-phase-shift (DPS) QKD [13] that employs a weak coherent pulse train instead of single-photons. It features a simple setup, is suitable for fiber transmission because key information is carried on relative phases between neighboring pulses, and is robust against the PNS attack, as in DPS-QKD.

## 2. Differential-phase-shift quantum secret sharing

Figure 1 shows the configuration of our differential-phase-shift (DPS) QSS system, where Charlie will have a full key for ciphering, and Alice and Bob will have partial keys for deciphering. First, Alice sends a weak coherent pulse train to Bob that is randomly phase-modulated by  $\{0, \pi\}$  for each pulse. The optical power is set at less than 1 photon (e.g., 0.1 – 0.2) per pulse on average. Bob also phase-modulates the received signal by  $\{0, \pi\}$  for each pulse and then sends it to Charlie, while monitoring the received signal power by splitting and detecting a part of it. Charlie measures the phase difference of adjacent pulses with a one-pulse delayed Mach-Zehnder interferometer, such that detectors 1 and 2 count a photon for a phase difference of 0 and  $\pi$ , respectively. Here, a photon is detected occasionally and randomly because the received signal power is smaller than one photon per pulse. While measuring the signal, Charlie records the photon detection time and which detector counts a photon.

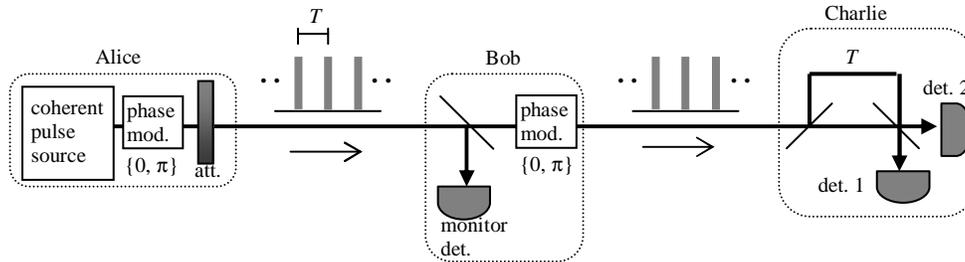


Fig. 1. Configuration of differential-phase-shift quantum secret sharing system.

Using the above setup, the three parties create their own key as follows. First, Charlie creates his key bits such as bit “0” from a detector-1 click and bit “1” from a detector-2 click. Then, he discloses the photon detection time. With this time information and their own phase modulation data, Alice and Bob create their own key bits such as bit “0” and “1” from 0 and  $\pi$  phase difference imposed on the time slots corresponding to Charlie’s photon detection time.

When the differential phases imposed by Alice and Bob are  $\{0, 0\}$  and  $\{\pi, \pi\}$ , the total differential phase is 0 and detector 1 counts a photon. When Alice’s and Bob’s differential phases are  $\{0, \pi\}$  and  $\{\pi, 0\}$ , the total differential phase is  $\pi$  and detector 2 counts a photon. Thus, Charlie’s bits are exclusive ORs of Alice’s and Bob’s bits. That is, Alice and Bob know Charlie’s key bits only when they cooperate, and the QSS operation is accomplished. Although we assume above that Alice and Bob have their own partial keys, the number of parties having partial keys can be extended simply by placing additional Bobs in the transmission line.

An advantage of this DPS-QSS scheme is its high key creation efficiency. All received photons contribute to key creation, unlike the previous scheme based on BB84 [8]. In addition, it is preferable for fiber transmission systems because the relative phase between adjacent pulses does not suffer from fiber fluctuation unlike the polarization state used in the previous scheme.

Note that Charlie does not know Alice’s and Bob’s partial keys in this system. One may think that the same function can be accomplished in a way that Charlie shares secret keys with Alice and Bob respectively by a conventional QKD protocol and then creates his secret key from the exclusive OR of these respective keys. In this scheme, Charlie fully knows Alice’s and Bob’s keys. Thus, for example, he can arbitrarily replace Alice or Bob with another party after a key is once established among them. On the other hand, QSS systems do not provide Alice’s and Bob’s keys to Charlie, and prohibit Charlie from doing such a tyrant-like behavior.

### 3. Eavesdropping against DPS QSS

The security of the above DPS-QSS against an external eavesdropper (Eve) is considered the same as DPS-QKD [14]. A beam-splitting attack does not succeed because the probability that both Charlie and Eve count photons at an identical time slot is low for weak coherent light, and thus Eve cannot obtain full key information. Intercept-resend attacks also fail because Eve cannot measure every differential phase and is forced to resend an imperfect fake signal to a legitimate receiver, resulting in bit errors in the secret key. Against other general individual attacks, including the photon number splitting attack [12], DPS-QKD is proven to be secured [14], which is also true for DPS-QSS. Unfortunately, a full security analysis considering more general attacks allowed by quantum mechanics has not been completed for DPS-QKD and thus for DPS-QSS, since the DPS scheme is a new and unique idea.

In addition to external eavesdroppers, we must also be wary of malicious Alice or malicious Bob in QSS. QSS protocols have to prohibit Alice or Bob from knowing Charlie’s key by herself/himself. In the following, we discuss whether this requirement is satisfied in DPS-QSS.

First, Alice’s betrayal is considered. Suppose that she wants to know Charlie’s key by herself. A simple way to do so is to send a DPS signal directly to Charlie, bypassing Bob, with which Charlie’s measurement result straightforwardly follows Alice’s modulation phase, so she knows all of Charlie’s bits. In addition to Charlie’s bits, she should also know Bob’s modulation phase, because she will have to pass a test-bit checking among Alice, Bob, and Charlie that is made after raw-key creation. A configuration for Alice to do so is shown in Fig. 2. In addition to directly sending a DPS signal to Charlie, she also sends a pulse train to Bob and measures it at the output of Bob’s site, by which Alice knows Bob’s modulation phase. In this attack, she has to measure all of Bob’s differential phases because she cannot predict from which time slots Charlie will create key bits. To do this, she should send a pulse train with more than one photon per pulse. However, Bob is equipped with a monitoring detector that checks whether the incoming light power is at a normal level (i.e., less than one photon per pulse). Thus, launching more than one photon per pulse is prohibited by Bob’s monitoring

detector. Then, she sends the probe signal with normal power, which only provides her with part of Bob's modulation data. Without complete information, malicious Alice introduces bit errors in the test-bit checking, revealing her betrayal.

The probability of error induced by the above Alice's eavesdropping is considered as follows. The probability that Alice knows Bob's differential phase corresponding to Charlie's bit is  $2\mu T_{ab}$  [12], with a strategy that stores the pulse train output from Bob and makes two corresponding pulses interfere with each other after Charlie discloses the photon detection time. Here,  $\mu$  is the average photon number per pulse sent from Alice and  $T_{ab}$  is the transmittance from Alice to Bob's output. Then, the probability that Alice does not know Bob's bit is  $(1 - 2\mu T_{ab})$ , and the resultant bit error rate is  $(1 - 2\mu T_{ab})/2$ . Note that this bit error rate is dependent of Bob's monitoring detector in practice. When the photon counting rate of Bob's detector fluctuates, Alice can send photons of more than an initially designed number, utilizing this fluctuation, and reduce the bit error rate as a result. For a fluctuation of 10 %, for example, the upper bound of the error rate is given by  $(1 - 2\mu T_{ab})/2$  with  $\mu' = 1.1\mu$ . Then, the information leakage to Alice, which is described later, is increased by this amount.

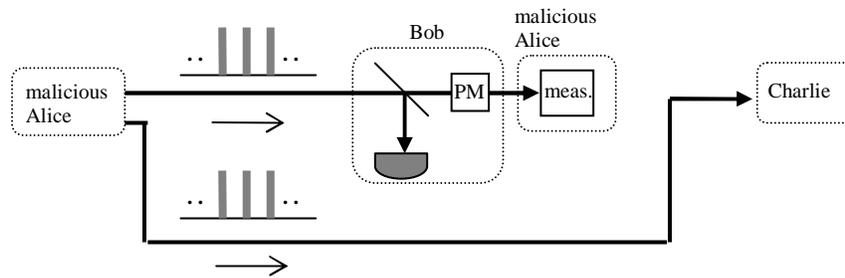


Fig. 2. Configuration of eavesdropping by malicious Alice. PM: phase modulation, meas: measurement apparatus.

Next, we discuss Bob's betrayal. He wants to know Charlie's key by himself, and also needs to know Alice's modulation phase to pass the test-bit checking. A configuration for Bob to do so is shown in Fig. 3. He measures Alice's signal just at the outside of her site while sending his DPS signal to Charlie. Unfortunately for Bob, however, while he fully knows Charlie's key, he obtains just a fraction of Alice's bits because her signal averages less than one photon per pulse. Without full information, malicious Bob introduces bit errors in the test-bit checking, and thus his betrayal is revealed. The probability of error induced by this Bob's strategy is considered as follows. The probability that Bob knows Alice's differential phase corresponding to Charlie's bit is  $2\mu$ , with a strategy that stores the pulse train from Alice and makes two corresponding pulses interfere with each other after Charlie discloses his photon detection time. Then, the probability that Alice does not know Bob's bit is  $(1 - 2\mu)$ , and the resultant bit error rate is  $(1 - 2\mu)/2$ .

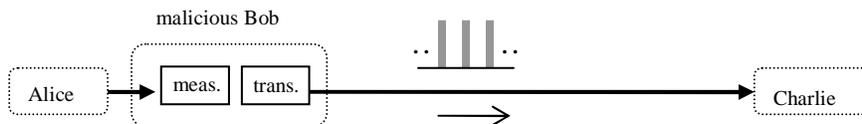


Fig. 3. Configuration of eavesdropping by malicious Bob.

In the above discussions, we assume that Alice (or Bob) should know Bob's (or Alice's) bits as well as Charlie's bits to pass test-bit checking. In fact, however, she (or he) can pass it

without knowing Bob's (or Alice's) bits, depending on the order of the announcement in the test-bit checking. When Charlie and Bob (or Alice) disclose their test bits first, Alice (or Bob) can declare her (or his) bits in accordance with Charlie's and Bob's (or Alice's) ones, regardless of her (or his) actual bits. To avoid overlooking such cheating, Alice and Bob are alternatively asked to disclose her or his test bit first. With this ordering in the test-bit checking, both Alice and Bob betrayals are noticed.

#### 4. Error correction and privacy amplification

In QKD in general, error correction and privacy amplification are applied to raw keys to obtain a final secret key [15, 16]. The same is true for QSS. However, to the best of the authors' knowledge, previous QSS studies have paid little attention to final-key creation through these post procedures. In this section, we discuss error correction and privacy amplification in DPS-QSS.

For error correction, the CASCADE protocol [15], which is widely used in QKD, can also be applied to QSS with the following modification. First, Alice, Bob, and Charlie estimate the bit error rate by disclosing some test bits. Next, they divide their own keys into blocks with an equal number of bits so that one block includes one bit error on average and calculate the parity of each block. Then, Alice and Bob disclose their own parities to Charlie. If Charlie's parity is the XOR of Alice's and Bob's parities, he judges there is no error in his block. If not, Charlie tells Alice and Bob the result, and they proceed with the above procedures (i.e., making blocks, calculating and announcing parities, and checking XOR) until Charlie finds an error bit. One different point of the above protocol from the conventional CASCADE is that Charlie checks the XOR of Alice's and Bob's parities, while the two parties simply compare their parities in QKD. The number of times of Charlie's announcement in this modified protocol is the same as the information exchange between Alice and Bob in the conventional CASCADE. Thus, the amount of information leakage through the above error correction is considered the same as in CASCADE.

We next discuss privacy amplification. To compress a raw key string through privacy amplification, we must estimate the amount of information leakage due to eavesdropping in addition to that due to error correction. In QSS, there are three possible eavesdroppers: an external intruder (Eve), malicious Alice, and malicious Bob. Information leakage due to Eve's eavesdropping is regarded as the same as in DPS-QKD. The different point is Eve's position. She conducts eavesdropping at Bob's output to obtain Charlie's key in QSS, while she does so at Alice's output in conventional QKD.

In principle, information leakage to malicious Alice or malicious Bob is prevented because their betrayal induces bit errors, as described in the previous section. In actual systems, however, bit errors exist resulting from imperfections in apparatus, and Alice or Bob can obtain partial information by exploiting these system errors. The bit error rate induced by Alice's betrayal is  $(1 - 2\mu I_{ab})/2$ , and that by Bob's betrayal is  $(1 - 2\mu)/2$ , as discussed in the previous section. Malicious Bob introduces a smaller error rate than malicious Alice, meaning that Bob can obtain a larger amount of Charlie's key. Thus, we just consider the amount of information leaked to malicious Bob in the following.

Provided that system error rate is  $e$ , the upper bound for the allowable rate of Bob's eavesdropping shown in Fig. 3,  $\alpha$ , is given by

$$\alpha \left( \frac{1 - 2\mu}{2} \right) \frac{1}{2} = e, \quad (1)$$

where a factor 1/2 is attached to the left-hand side because Alice and Bob alternatively disclose their key bits in the test-bit checking and a bit error is revealed when Bob discloses his bit first. From Eq. (1), we have

$$\alpha = \frac{4e}{1 - 2\mu}. \quad (2)$$

As described in the previous section,  $2\mu$  is the probability for Bob to obtain Alice's bit by the eavesdropping shown in Fig. 3. Thus, the information leakage to Bob through this partial eavesdropping is  $2\mu\alpha$ . For the remaining part of Alice's signal,  $(1 - \alpha)$ , Bob phase-modulates and sends it to Charlie as in the normal condition. Here, however, he can also conduct a beam-splitting attack utilizing the transmission loss from Bob to Charlie, as shown in Fig. 4. Provided that the transmittance from Bob to Charlie is  $T$ , Bob splits  $(1 - T)$  Alice's signal, stores it, and makes two pulses interfere with each other after Charlie discloses the photon detection time. This beam-splitting attack gives Bob partial information with a ratio of  $2\mu(1 - \alpha)(1 - T)$ . Then, Bob obtains  $2\mu\alpha + 2\mu(1 - \alpha)(1 - T)$  of Charlie's key in total.

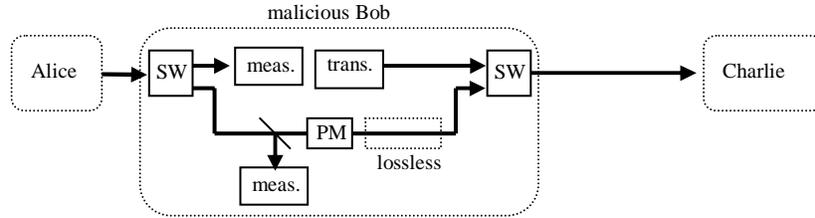


Fig. 4. Bob's eavesdropping. PM: phase modulator, SW: optical switch.

We must also heed Bob's other eavesdropping shown in Fig. 5, where Bob conducts a general individual attack at Alice's output as carried out by Eve in conventional DPS-QKD [14], phase-modulates the signal after the general individual attack, and then sends it to Charlie. The information leakage by this eavesdropping is considered the same as that by the general individual attack in the conventional DPS-QKD.

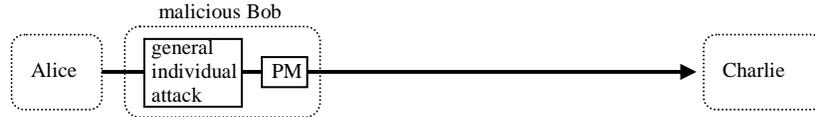


Fig. 5. Bob's general individual attack.

Based on the above considerations, we simulated the final-key creation rate as a function of fiber transmission distance in our DPS-QSS. The result is shown in Fig. 6, where the key creation rates are plotted considering Eve's eavesdropping (dashed line), Bob's eavesdropping shown in Fig. 4 (dotted line), and Bob's eavesdropping shown in Fig. 5 (solid line). Eve is assumed to conduct the general individual attack in this simulation. The results indicate that Bob's general individual attack is the most powerful eavesdropping, by which the QSS system performance is restricted.

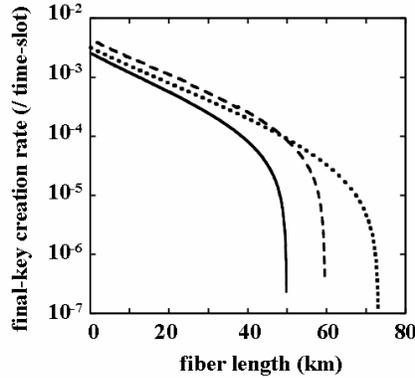


Fig. 6. Simulation results for final-key creation rate as a function of fiber transmission length. Dashed line, dotted line, and solid line assume Bob's betrayal (Fig. 4), Eve's general individual attack, and Bob's general individual attack (Fig. 5), respectively. Fiber length is the distance between Alice and Charlie, and Bob is assumed to be positioned at the middle between them in the normal condition. Fiber loss coefficient = 0.25 dB/km, detector efficiency = 10 %, detector dark-count rate =  $10^{-5}$ /slot, error rate due to imperfect interference = 1 %. The average photon number sent from Alice is optimized to obtain the highest key creation rate at each length.

## 5. Experiment

To demonstrate DPS-QSS operation, an experiment was carried out with the configuration shown in Fig. 7. Its setup was basically identical as our previous DPS-QKD experiment [17], except that Bob was inserted in the transmission line. In Alice's site, cw light from an external-cavity LD ( $\lambda = 1.55 \mu\text{m}$ ) was intensity-modulated to be a pulse train by an electro-absorption modulator. The repetition rate and the pulse width were 1 GHz and 125 ps, respectively. The created pulse train was then phase-modulated by  $\{0, \pi\}$  for each pulse by a LiNbO<sub>3</sub> phase modulator driven by a pseudo random binary stream, and attenuated to be 0.27 photon/pulse, which was an optimized number based on our security analysis. The signal from Alice was sent to Bob. At Bob's site, part of the incoming signal was split to a monitoring photon detector with a splitting ratio of 1 %, and the main part was phase-modulated by  $\{0, \pi\}$  for each pulse. The phase-modulated signal was then sent to Charlie. At Charlie's site, the incoming signal was input to a waveguide asymmetric Mach-Zehnder interferometer whose path length difference was 20 cm that corresponded to the pulse interval of 1 ns. The interferometer was a PLC (planar lightwave circuit) based device, which provided stable operation under the temperature control within 0.05 degree. The detail of the device is described in Ref. [17]. The outputs of the interferometer were coupled into InGaAs-APD photon detectors (idQuantic) gated at 1 MHz. The signals from the detectors were fed into a time interval analyzer that recorded the photon detection time and the detector tag signal. Attenuators of 1.25 dB were inserted between Alice and Bob and between Bob and Charlie to simulate 5-km fiber loss.

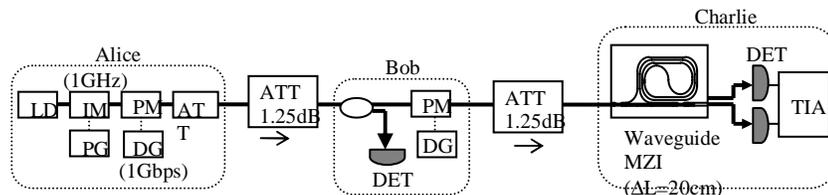


Fig.7. Experimental setup of DPS-QSS. LD: external-cavity laser diode, IM: intensity modulator, PM: phase modulator, PG: pulse generator, DG: data generator, DET: photon detector, MZI: Mach-Zehnder interferometer, TIA: time interval analyzer.

With the above setup, we obtained a sifted key at a rate of 5.3 kbps with a quantum bit error rate of 2.6%, which included an error rate due to the detector dark count of 1.3%, that due to imperfection in the interferometer of 1.0%, and that due to the detection jitter of 0.3%. Based on the eavesdropping discussions in the previous section, a final key can be created at a rate of 750 bps after error correction and privacy amplification. Thus, we successfully demonstrated our DPS-QSS operation.

## 6. Summary

Differential-phase-shift (DPS) quantum secret sharing (QSS) was proposed. Alice sends a coherent pulse train phase-modulated by  $\{0, \pi\}$  to Bob, who additionally phase-modulates it by  $\{0, \pi\}$  and sends it to Charlie, who receives it with a one-bit delayed interferometer. With this configuration, Charlie has a full key for ciphering and Alice and Bob have partial keys for deciphering. After presenting the setup and operation mechanism, we evaluated the system performance with error correction and privacy amplification, considering external eavesdropping and both Alice's and Bob's betrayals. An experiment demonstrated the operation, where a final key based on our discussions was created at a rate of 750 bps.