MDI-DPS-QKD utilizing QSS setup

Muataz Alhussein[1] and Kyo Inoue[1]
Graduate School of Engineering, Osaka University
Email: muataz@opt.comm.eng.osaka-u.ac.jp

Introduction: Measurement device independent quantum key distribution (MDI-QKD) was proposed to be free from side-channel attacks utilizing imperfections in measurement devices. In conventional MDI-QKD, Charlie, who is assumed to be an untrusted party, performs Bell state measurement (BSM) on Alice's and Bob's signals. The main experimental challenge for such MDI-QKD schemes is to establish synchronization between the received signals in term of the timing, the polarization state, the temporal and spectrum shapes for the BSM. In order to avoid such experimental difficulties, this paper proposes a new scheme of MDI-QKD based on differential phase shift (DPS) quantum secret sharing (QSS) [1], which features no use of BSM. Compared to conventional MDI-QKD scheme, the proposed scheme presents a simple setup, suitable for practical implementation.

Configuration and operation: The setup of the proposed scheme is shown in Fig.1, where a weak coherent pulse train phase-modulated for each pulse by (0, π) is sent from Alice to Bob with a power level of less than 1 photon per pulse on average (0.1-0.2). Bob further modulates the transmitted signal by (0, π) for each pulse without measuring it, and sends it to Charlie (untrusted party), while monitoring the incoming signal power by splitting and detecting its fraction. Charlie, positioning just after Bob, measures the phase difference of adjacent pulses with a one-pulse delayed Mach-Zehnder interferometer, through which detectors 0 and 1 count a photon for a phase difference of 0 and π, respectively. When the differential phases imposed by Alice and Bob are as {Alice=0, Bob= 0} or {Alice=π, Bob= π}, the total differential phase is 0 and detector 0 counts a photon. On the other hand, when Alice's and Bob's differential phases are {Alice=0, Bob= π} or {Alice=π, Bob=0}, the total differential phase is π and detector 1 counts a photon. Because the photon average number is less than 1 per pulse, the detection event is occasional and random. After the measurement, Charlie exposes the time and detector information through a classical channel to Alice and Bob, who can create an identical key bit based on Charlie's information and their own modulation data as follows. First, Alice/Bob creates bits 0 and 1 from her/his differential phases of 0 and π, respectively. In case that detector 0 clicked at Charlie, Bob holds the bit. In case that detector 1 clicked at Charlie, Bob flips his bit. In this way, Alice and Bob have an identical bit. This scheme prevents malicious Charlie, who performs measurement, from identifying the created bit, because he only knows the result of XOR, which does not provide the key bit information. Thus, attacks against the measurement device are meaningless and this scheme can be regarded as MDI-QKD.

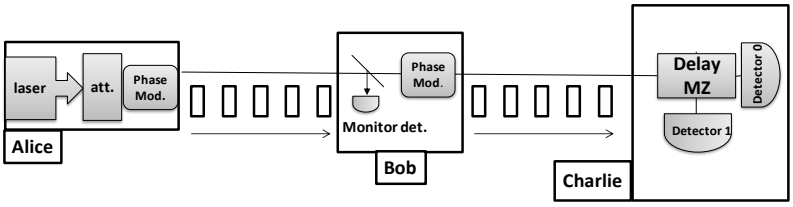

Figure 1: Setup of MDI-DPS-QKD utalazing QSS setup.

Calculation: The transmitted signals in this scheme are basically the same as those in DPS-QKD. Thus, its security can be equivalent to that in DPS-QKD. Based on this analogy, we evaluated the system performance considering the general individual attack, which has been analyzed against DPS-QKD [2]. The main difference in system evaluation is that detection errors, which determines the system performance, occur in untrusted Charlie in the present scheme instead of Bob in DPS-QKD. In the present simulation, we assume, as an example, that Charlie uses a receiver typically employed in DPS-QKD. Under this assumption, the key creation rate as a function of the key distribution distance is similar to that in DPS-QKD, as shown in Fig. 2.

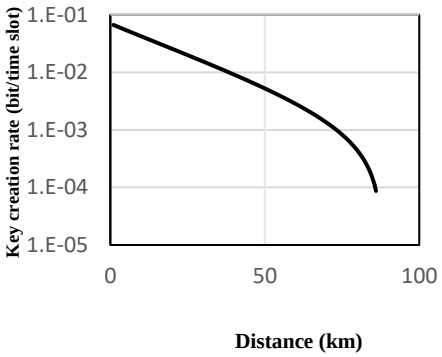

Figure 2: System performance against general individual attack.

Summary: We proposed a novel scheme of MDI-QKD, which uses no BSM for key bit creation and thus offers a simple setup.

References

[1] K. Inoue *et al.*, "Differential-phase-shift quantum secret sharing," *Opt. Express*, vol. 16, no. 20, pp. 15469–15475, 2008.

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

Supplementary for (MDI-DPS-QKD utilizing QSS setup)

Muataz Alhussein[1] and Kyo Inoue[1]
Graduate School of Engineering, Osaka University
Email: muataz@opt.comm.eng.osaka-u.ac.jp

MDI-DPS-QKD using the secret quantum-sharing configuration

Figure 1 shows the configuration of our system, where legitimates parties (Alice and Bob) will only perform modulation to share a complete key. First, Alice sends a weak coherent pulse train to Bob that is randomly modulated in phase by $\{0, \pi\}$ for each pulse. Optical power is set to less than 1 photon (eg 0.1 - 0.2) per pulse on average. Bob also phase-modulates the signal transmitted by $\{0, \pi\}$ for each pulse and then sends it to Charlie, while monitoring the power of the received signal by dividing and detecting the fraction. Charlie measures the phase difference of adjacent pulses with a one-pulse delayed Mach-Zehnder interferometer, so that detectors 1 and 2 count a photon for a phase difference of 0 and π, respectively. In this case, a photon is occasionally and randomly detected because the power of the received signal is less than one photon per pulse. While measuring the signal, Charlie records the photon detection time and the detector that counts a photon. Using the above setting, Alice and Bob create their own key as follows. First, Charlie announces his measurement results via a public channel. Alice and Bob first create their own key bits as bits "0" and "1" of their phase differences 0 and π, respectively. 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 the differential phases of Alice and Bob are $\{0, \pi\}$ and $\{\pi, 0\}$, the total differential phase is π and detector 2 counts a photon. So, in case detector 0 snapped at Charlie, Bob holds the bit. In case Detector 1 snapped at Charlie, Bob flips his bit. In this system, legitimate parties (Alice and Bob) only perform modulation, and thus we can regard it as MDI-QKD. Note that the proposed scheme does not use BSM even though it achieves the MDI-QKD function, which solves experimental challenges of synchronization in conventional MDI-QKD, such as temporal and polarization synchronization for the BSM.

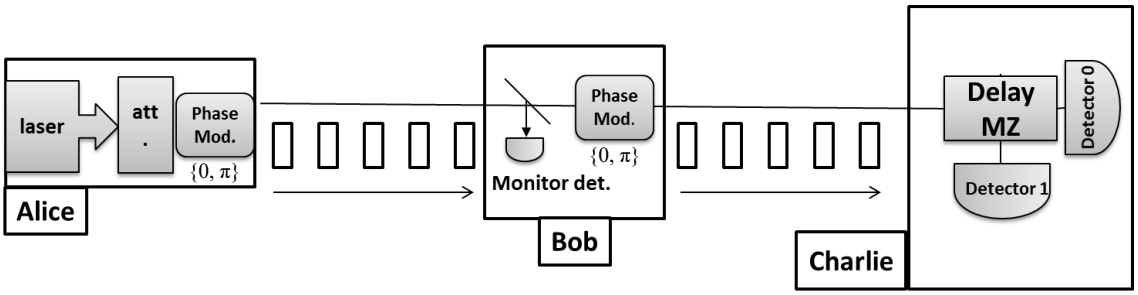

Figure 1: Setup of MDI-DPS-QKD utilizing QSS setup

Eavesdropping against this system

The security of the above system against an external spy (Eve) is considered as same as DPS-QKD [1]. A Beam splitting attack is unsuccessful because the propability that both Charlie and Eve count photons in an identical time slot is low for weak coherent light and therefore Eva cannot obtain complete key information. Intercept and resend attacks also fail because Eve cannot measure every differential phase and is forced to send an imperfect false signal to Charlie, resulting in bit errors in the secret key. Against other general individual attacks, including photon

number splitting attack [2], DPS-QKD is proven to be safe [1], which is also true for the present protocol. Unfortunately, a complete security analysis has not been completed considering the more general attacks allowed by quantum mechanics for DPS-QKD and therefore for the current system. The main difference in evaluating the system is that the detection errors, which determine system performance, occur in unreliable Charlie in the current scheme instead of Bob in DPS-QKD.

A possible eavesdropping against this system is that Eve sends an intense light of wavelength different from Alice's signal's, and measures it at the Bob's output, by which she knows Bob's modulation. However, this eavesdropping can be prevented by equipping an optical filter and/or a high-sensitive optical power meter that monitors the incident light at the Bob's input as shown in fig 1.

In addition to external eavesdropping, we must also be careful with malicious Charlie. The current system has to prohibit Charlie from knowing the key information, even if he cooperates with Eva, since Charlie is allowed to measure only the XOR of the signals of Alice and Bob, which gives no useful information by itself.

Simulation

In this work, we are interested in simplifying MDI-QKD for practicality, so we restrict our discussion only to individual attacks. In these attacks, Eve is assumed to individually attack each photon over many pulses with a fixed phase modulation pattern.

The mathematical model for this eavesdropping system is provided for DPS-QKD [1]. The main difference of the present system from DPS-QKD is that quantum bit errors that determine system performance occur in untrustworthy Charlie in the present scheme instead of Bob in DPS-QKD. In the present simulation, we assume that Charlie uses a receiver that is typically used in DPS-QKD. The key creation rate with general individual attack can be expressed as follows [1]:

$$R = R_{sifted} \{\tau + f(e) [e \log_2 e + (1-e) \log_2 (1-e)]\},$$

where R_{sifted} is the sifted key rate, f (e) characterizes the performance of error correction algorithm. Parameter τ is the privacy amplification rate expressed as:

$$\tau = - [1-2 \mu (1-T)] \log_2 [1-e^2 - (1-6e)^2 /2],$$

where T is the transmittance given by:

$$T = \eta 10^{-(\alpha L+Ls)/10,}$$

The quantum bit error rate e can be written as following:

$$e= (1/2P_{dark} + b P_{signal})/ P_{click,}$$

$$P_{click} \approx p_{signal} + p_{dark,}$$

$$P_{dark} = 2d,$$

Where P_{click} is the probability that Charlie detects a photon in a given clock cycle.

Detection events may be triggered by photons (p_{signal}) or by dark counts (p_{dark}).
We assumed system parameters as: Fiber loss (α) = 0.2 dB/km for 1.55 μm, loss of detection circuit (Ls) = 0 for no loss, the detector quantum efficiency (η) = 10%, dark count (d) = 10^{-5} counts/time window, and baseline error (b) = 0.01, while the rate is numerically optimized with respect to average photon number (μ) for each value of the fiber length. Length (L) ranges from 1 to 150 km

References:

1. E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," Phys. Rev. A 73, 012344 (2006).
2. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A 61, 052304 (2000).