BB84 and DQPS-QKD experiments using one polarization-insensitive measurement setup with a countermeasure against detector blinding and control attacks

Muataz Alhussein[1], Kyo Inoue[1], Toshimori Honjo[2]
1. *Graduate School of Eng., Osaka University, 2-1 Yamada-oka, Suita-shi, Osaka, 565-0871, Japan*
2. *NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan*
Email: muataz@opt.comm.eng.osaka-u.ac.jp

Abstract: This paper demonstrates phase-encoding BB84-based QKD experiments with active basis selection using one interferometer with no phase and polarization controls, unlike conventional BB84-QKD experiments. A countermeasure against detector blinding attack is also implemented.

OCIS codes: (270.0270) Quantum optics; (270.5568) Quantum cryptography.

1. Introduction

In one-way BB84-based QKD systems, the receiver randomly selects the measurement basis. In phase-encoding BB84-based QKD protocols that transmit sequential pulses with phase differences of {0, π} {π/2, 3π/2}, the basis selection is performed by {0, π/2} phase modulation (PM) onto one arm of a delay Mach-Zehnder interferometer (MZI), i.e., active basis selection occurs, which requires phase stabilization for the MZI and polarization control for the phase modulation in practical implementation [1]. Alternatively, a combination of a beam splitter and two MZIs with path phase differences of 0 and π/2, respectively, followed by four single-photon detectors (SPDs), can also be used for passive basis selection [2]. This method is free from the phase- and polarization-control issues, but the receiver is massive and expensive. In view of the above issues in practical implementation of BB84-based QKD systems, this paper demonstrates BB84 and DQPS-QKD experiments that use one MZI and two SPDs with no phase stabilization control, equipping polarization-insensitive PM in front of a waveguide MZI. A countermeasure against detector blinding and control attacks is also implemented. Our scheme enables simple and cost-effective QKD system implementation.

2. Polarization-insensitive active basis selection

We performed the phase-encode BB84 and DQPS-QKD [2] protocols, wherein sequential pulses with phase differences of {0, π} {π/2, 3π/2} were transmitted and received with the setup shown in the dashed box, indicated by "Bob" in Fig. 1. The received pulses were passed through a phase modulation circuit (PMC) that imposed {0, π/2}-phase onto each pulse, and then were coupled to a MZI with a path phase difference of 0. This arrangement of the PMC and the MZI enabled active basis selection, in effect. The MZI was fabricated on a glass waveguide circuit [3], for which no phase stabilization control was necessary. In order to have no polarization control, the PMC was configured as illustrated in the inset Fig. 1, with "Bob." The incoming signal was divided into two polarization components via a polarization beam splitter (PBS), transmitted through phase modulators (PMs) aligned to each polarization state, and then recombined via another PBS, where the two path lengths were equal and the pulses were modulated at identical timings. With this setup, the PMC worked irrespective of the polarization state of the incoming signal. The above receiver setup enabled active basis selection with no polarization and phase-stabilization controls.

3. Countermeasure against detector blinding and control attacks

Side-channel attacks manipulating SPDs have been a threat to actual QKD systems these days [4]. We recently proposed a simple countermeasure against such attacks, which was also implemented in the present experiment. In BB84 using weak coherent light or DQPS-QKD, Bob's two SPDs can click simultaneously, by chance, at basis-mismatched measurement, because a coherent pulse has a finite probability of including multiple photons. These coinciding counts can be utilized to find the detector blinding and control attack [5]. When Eve conducts this attack, no coinciding counts occur even at basis-mismatched measurements taken by Bob. Therefore, the eavesdropping is prohibited by monitoring the coinciding counts.

4. Experiment setup

We carried out the experiment using the setup shown in Fig. 1, which could be used to run either BB84 or DQPS-QKD protocol, depending on the pulse sequences prepared by Alice. For BB84, Alice prepared a sequence of two

pulses, while for DQPS-QKD, she prepared a train of pulses, by intensity-modulating light from a laser source. The pulse interval was 1 ns. Each pulse was randomly phase-modulated with one of the four phases {0, π} {π/2, 3π/2}, and then attenuated to be 0.1 photon per pulse on an average. The created signal was passed through an attenuator that simulated the transmission loss, and was received by the measurement system described above, where the outputs of the MZI were coupled to APD-based SPDs (idQuantique: ID200) gated at 4 MHz. In order to confirm the polarization independent operation, a polarization controller (PC) was inserted between the transmitter and the receiver, with which the polarization state of the transmitted signal was varied. The change in the polarization state was monitored by splitting a fraction of the PC output and measuring its power via a polarizer. The transmission loss between Alice and Bob was 6 dB, including the splitter for the polarization state monitoring and the attenuator, which corresponded to a 30-km fiber. We ran BB84 without a decoy method (but it still possible to be implemented) as we aimed at showing the polarization-independent operation and the feasibility of monitoring coincident counts.

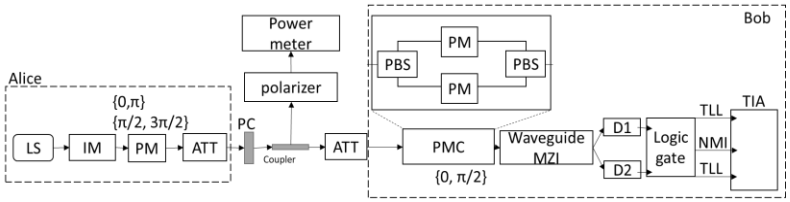

Fig. 1. Experimental setup. PMC: phase modulation circuit, LS: laser source, IM: intensity modulator, PM: phase modulator, ATT: attenuator, PC: polarization controller, PBS: polarization beam splitter, D1, D2: single-photon detectors, MZI: Mach-Zehnder interferometer, TIA: time interval analyzer.

5. Results

The results of the BB84 experiment are shown in Fig. 2. The shifted key rate and the quantum bit error rate (QBER) are plotted as functions of the degree of the polarization state between two orthogonal states. Figure *x* in the horizontal axis means that the power ratio of two orthogonal polarization components was *x*: (1–*x*). The key rate and the QBER were within 1.4–1.7 kbps and 2.9–3.55%, respectively, for various polarization states. These were 1.95–2.57 kbps and 2.2–3.3% in the DQPS experiment. Therefore, the polarization-insensitive operation was demonstrated. Figure 3 shows the measured coincidental counts. A number of coinciding counts were actually obtained, indicating the feasibility of our counter-measure against the detector blinding and control attacks.

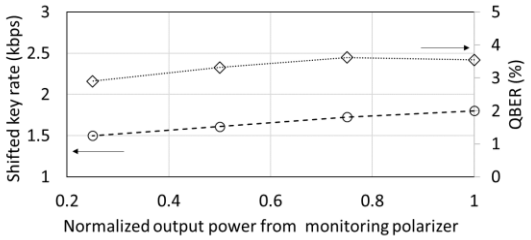

Fig. 2. System performance for various polarization states.

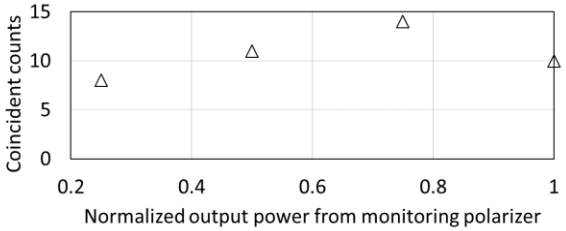

Fig. 3. Measured coincident count.

6. Summary

We demonstrated phase-encoded BB84 and DQPS-QKD experiments using one interferometer with active basis selection, employing a polarization-insensitive phase-modulation scheme. A countermeasure against the detector blinding and control attacks was also demonstrated.

References

[1] Dixon, A. R. et al., "Quantum key distribution with hacking countermeasures and long term field trial," Scientific Reports **7**, 1978 (2017).
[2] K. Inoue and Y. Iwai, "Differential-quadrature-phase-shift quantum key distribution," Phys. Rev. A **79**, 022319 (2009).
[3] T. Honjo, K, Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planer light-wave circuit Mach-Zehnder interferometer," Opt. Lett. **29**, 2797-2729 (2004).
[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photon. **4**, 686-689 (2010).
[5] M. Alhussein, K. Inoue, and T. Honjo, "Monitoring coincident clicks in differential-quadrature-phase shift QKD to reveal detector blinding and control attacks," Jpn. J. Appl. Phys. **58**, 012006 (2018).