BB84 experiment using one polarization-insensitive measurement setup with a countermeasure against blinding and controlling attack

Muataz Alhussein[1], Kyo Inoue[1] , Toshimori Honjo[2]
1 Graduate School of Engineering, Osaka University
2 NTT Basic Research Laboratories, NTT Corporation
Email: muataz@opt.comm.eng.osaka-u.ac.jp

Introduction: In phase-encoding BB84-based QKD protocols, Bob selects the measurement basis by {0, π/2} phase modulation (PM) onto one arm of a delay Mach-Zehnder interferometer (MZI) [1]. Alternatively, he can use a combination of a beam splitter and two MZIs with path phase differences of 0 and π/2, respectively, for stable operation. The former scheme requires phase and polarization state controls, and the latter one makes the receiver massive and expensive. In view of these issues in practical implementation of BB84-based QKD systems, this paper demonstrates a BB84 experiment that employs a polarization-insensitive PM circuit followed by one waveguide MZI. A countermeasure against detector blinding and control attacks is also implemented. Our scheme enables simple and cost-effective QKD system implementation.

Polarization-insensitive active basis selection: We performed the phase-encode BB84, 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. In order to have no polarization control, the PMC was configured as illustrated in the inset in "Bob" in Fig.1. The incoming signal was divided into two polarization components via a polarization beam splitter (PBS), transmitted through phase modulators 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.

Countermeasure against blind and control attack: In BB84 using weak coherent light, 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 [2]. When Eve conducts this attack, no coinciding counts occur even at Bob's basis-mismatched measurements. Therefore, the eavesdropping is prohibited by monitoring the coinciding counts.

Experiment: We carried out the experiment using the setup shown in Fig. 1. Alice sent double-pulses with an interval of 1 ns and a mean photon number of 0.1/pulse, Bob received them with the setup described above. Between Alice and Bob, a polarization controller (PC), a splitter, and an attenuator simulating the transmission loss were inserted, whose total loss was 6 dB. The polarization state was varied by the PC, which was monitored by a polarizer followed by a power meter. The obtained sifted key rate and QBER are shown in Fig. 2(a). The key rate and the QBER were within 1.4–1.7 kbps and 2.9–3.55%, respectively, for various polarization states, confirming the polarization-insensitive operation. Fig. 2(b) shows the coincident counts, which were measured in a time interval within which 4 M clicks were registered. A number of coinciding counts were actually obtained (around 10 counts), indicating the feasibility of our counter-measure against the detector blinding and control attacks.

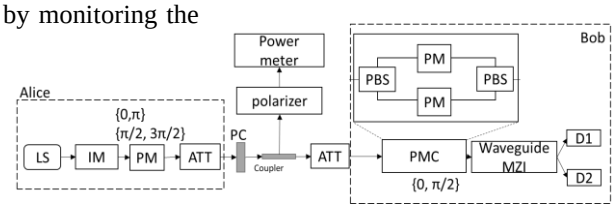

Fig. 1. Experimental setup. PMC: phase modulation circuit, LS: laser source, IM: intensity modulator, PM: phase modulator, ATT: attenuator, PC: polarization controller, PBS: polarization beam splitter, D1, D2: single-photon detectors, MZI: Mach-Zehnder interferometer.

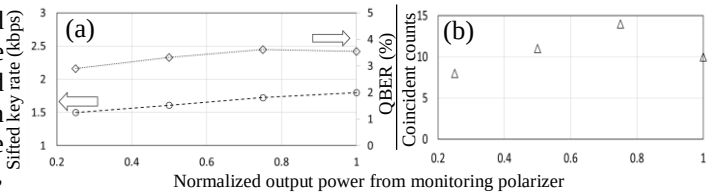

Fig.2. System performance for various polarization states.

Summary: We demonstrated a phase-encoded BB84 experiment 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.

[1] Dixon, A. R. et al., "Quantum key distribution with hacking countermeasures and long term field trial," Scientific Reports **7**, 1978 (2017).
[2] 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).