Robust Quantum Key Distribution Systems Using a Dual-Parallel Modulator

Yu KADOSAWA†, Kensuke NAKATA, Akihisa TOMITA, Kazuhisa OGAWA and Atsushi OKAMOTO

Graduate School of Information Science and Technology, Hokkaido University, Kita14-Nishi9, Kita-ku, Sapporo

E-mail: †kadosawa@optnet.ist.hokudai.ac.jp

1. Introduction

Quantum key distribution (QKD) attracts attention as a method for unconditionally secure key distribution. BB84 is the most popular quantum key distribution protocol, where the number of the secure final key decreases as bit error rate δ_X and phase error rate δ_Y increase. In addition, if quantum states are different from those assumed in the protocol (state preparation flaw Δ), we need to increase the estimation of δ_Y. The state preparation flaw severely impacts the security in a lossy channel [1].

2. A Dual-Parallel Modulator

We proposed the use of a dual-parallel modulator (DPM) for the state preparation in QKD systems in the previous report [2]. It is more robust modulator to the inaccuracy in the applied voltage than conventional modulators. Fig. 1 is the structure of DPM. Phase shifts ϕ_1 and ϕ_2 are yielded in the upper and lower Mach-Zehnder interferometers by the applied voltage $V_{\phi1}$ and $V_{\phi2}$, respectively. The electric field of the light output E_o is given by

$$E_o = \frac{\cos\phi_1 + i\cos\phi_2}{2} E_i \quad (1)$$

where E_i is the electric field of the input light.

In this report, we examined the benefit from the use of DPM in a decoy-BB84 system. The upper limit of the eavesdropping information is estimated by considering the state preparation flaw. The final key rate R is as follows:

$$R = -S_{\mu s} H_2(\delta_X) + \mu_s e^{-\mu_s} S_1 \left(1 - H_2\left(\delta_Y^{(1)}\right)\right) \quad (2)$$

where $S_{\mu s}$ is count rate of signal pulses, $H_2(x)$ is Shannon entropy, δ_X is bit error rate in signal pulses, μ_s is mean photon number of signal pulses, S_1 is count rate of the single photon of the signal, $\delta_Y^{(1)}$ is phase error rate in single photon pulses [1]. We calculated the final key rate when the applied voltage $V_{\phi1}$ deviated from the designed value by $V_\pi/20$ to compare the effect for DDM (dual-drive modulator: the type of a phase modulator used in current QKD system) with that for DPM. The results are shown in Fig. 2. The predicted state preparation flaws of DDM and DPM were $\Delta = 5.8\times10^{-4}$ and 1.2×10^{-6}, respectively. The reduction of Δ increases key rate, and improves the maximum transmission distance of DPM over 100km.

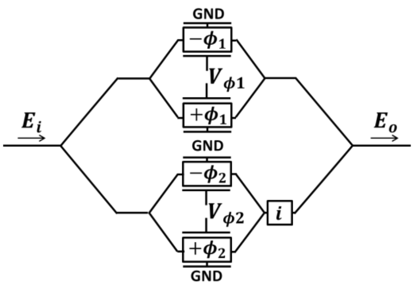

Figure 1. The structure of DPM

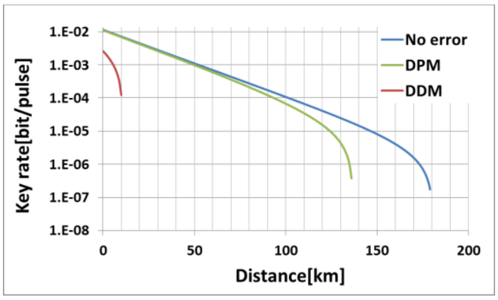

Figure 2. Key rate assuming that the applied voltage $V_{\phi1}$ deviates by $V_\pi/20$ from original voltage

3. Experiment

We experimentally quantified the effect on the output state with respect to the change of the applied voltage to DDM and DPM. We measured the visibility of the interference in the receiver by changing the bias voltage (DC) and the amplitude of the modulation signal (AC).

Measured values of the visibility for DDM and DPM agreed well with the theoretical values. For example, when the applied voltage was shifted by $V_\pi/10$ from the designed value for Y0 state, the visibility observed in Y basis for DDM was 0.940, while that for DPM was 0.967. Those value corresponded to the theoretically value of the visibility, 0.951 and 0.998, respectively. In addition, we calculated the final key rate by using the measured values. The results showed that the key rate of DPM was higher than that of DDM, which proved the robustness of the DPM to the inaccuracy in the applied voltage.

References

[1] M.Koashi, arXiv:quant-ph/0505108, 2005

[2] Y.Kadosawa *et al.*, Qcrypt2015, Poster session, No.40, 2015