Robust Quantum State Generation with a Dual-Parallel Modulator and Its Application for Quantum Key Distribution Systems

Yu KADOSAWA Kensuke NAKATA Akihisa TOMITA and Atsushi OKAMOTO

Graduate School of Information Science and Technology, Hokkaido University Kita14-nishi9, Kita-ku, Sapporo

1. Introduction

BB84 is the first and most popular quantum key distribution (QKD) protocol. BB84 uses the phase difference between the coherent pulse components (double-pulse) in phase coding, where a phase modulator defines four values of the relative phase of one component to the other. However, if the voltage applied to the phase modulator is not accurate, the phase difference deviates from the original value, and thus the quantum states are different from those assumed in the protocol. The state preparation flaw increases the error in the quantum communication, which decreases the final key rate. Furthermore, the state preparation flaw impacts the security severely in a lossy quantum channel to increase the number of bits to be discarded in the privacy amplification [1].

2. Proposal of a Dual-parallel Modulator for state preparation

We here introduce Dual-parallel modulator (DPM) as a robust phase modulator in QKD system. The structure of DPM is shown in Fig. 1. Two Mach-Zehnder interferometer (MZI) modulators are nested in parallel. Suppose the phase shifts ϕ_1 and ϕ_2 are induced by the applied voltage $V_{\phi 1}$ and $V_{\phi 2}$ to the upper and lower electrodes, respectively. The electric field E_o of the output light is as follows.

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

where, E_i represents the electric field of the input light. The BB84 states is prepared by setting the phase $\phi_1 = \phi_2 = 0$ for the first component of the pulse and the one of the following for the second: $\{\phi_1 = \phi_2 = 0;\ \phi_1 = \pi, \phi_2 = \pi;\ \phi_1 = 0, \phi_2 = \pi;\ \phi_1 = \pi, \phi_2 = 0\}$. Since

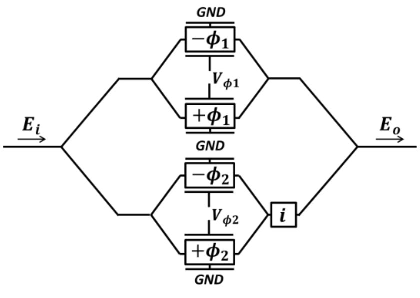

Figure1. The structure of DPM.

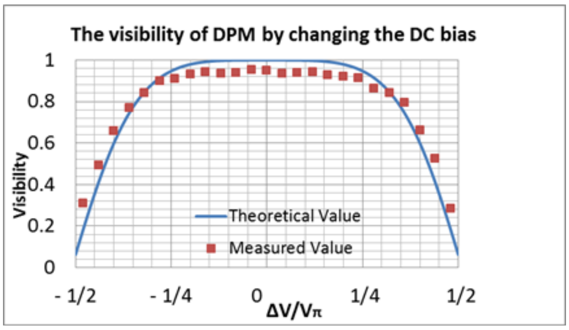

Figure2. Visibility by changing the DC bias.

the first derivative of $\cos\phi$ is zero at $\phi = 0, \pi$, the state preparation flaw grows proportional to the second order term of the small phase deviation. Therefore, the states generated by a DPM should be robust to the inaccuracy of the applied voltage.

3. Experiment

The accuracy of the states can be evaluated by the visibility of the interference. The visibility is closely related to the error rate in quantum communication. We measured the change of the visibility as the applied voltage shifts from the optimum value. We varied the bias voltage in this experiment. Assuming that V_θ is the applied voltage to yield the phase difference between double pulses by θ, we varied V_θ between $-V_{\pi/2}$ and $V_{\pi/2}$, and recorded the changes in intensity of the middle pulse components at the two output ports of the planar light-wave circuit asymmetric MZI.

Figure 2 shows the visibility measured by changing the DC-bias voltage with the simulated values, where the Y0 state was transmitted and measured in Y basis. Measured values of the visibility agree the theoretical values. Figure 2 indicates that the visibility of the state generated by the DPM maintained a high value (>0.96) even if the bias voltage varies by about 25% of V_π. The results prove that DPM is robust to the inaccuracy in the applied voltage.

Reference

[1] D. Gottesman et al., Quantum Inf. Comp. **4**, 325 (2004.)