Free-space BB84 양자암호에서의 편광 의존 광자손실의 효과

Effects of weak polarization-dependent losses in free-space BB84 quantum cryptography

김용수, 정연창, 김윤호
포항공과대학교 물리학과
yskim25@postech.ac.kr

Quantum cryptography or quantum key distribution (QKD) allows two distant parties, Alice and Bob, to share a string of random bits (0's and 1's) or cryptographic keys securely from an eavesdropper[1]. Since the security of QKD is based on the laws of quantum physics, it provides the most secure way of distributing cryptographic keys.

In free-space based QKD, qubits are usually encoded in the polarization of the photon and the loss in the quantum channel may be polarization-dependent. In this experiment, we have implemented a QKD system based on the BB84 quantum cryptography protocol[2] and investigated how polarization-dependent losses affect the performance of the system.

The schematic of our BB84 experimental setup, which consists of the transmitter (Alice), the receiver (Bob), and the quantum and public channels linking Alice and Bob, is shown in Fig. 1. Let us first discuss the transmitter (Alice) part of the BB84 QKD setup. The photon source in our experiment is a pulsed diode laser which emits a 780 nm laser pulse (5 ns) at the repetition rate of 1 MHz. The laser pulse is strongly attenuated so that the average photon number per pulse $\mu<1$. The photon pulse is then randomly encoded in one of the four polarization states ($|H\rangle$, $|V\rangle$, $|-45\rangle$, and $|+45\rangle$) by using a pair of Pockels cells (PC1 and PC2). To generate the encoding signal for the Pockels cells, two sets of pseudo-random strings of 0's and 1's are generated and recorded at

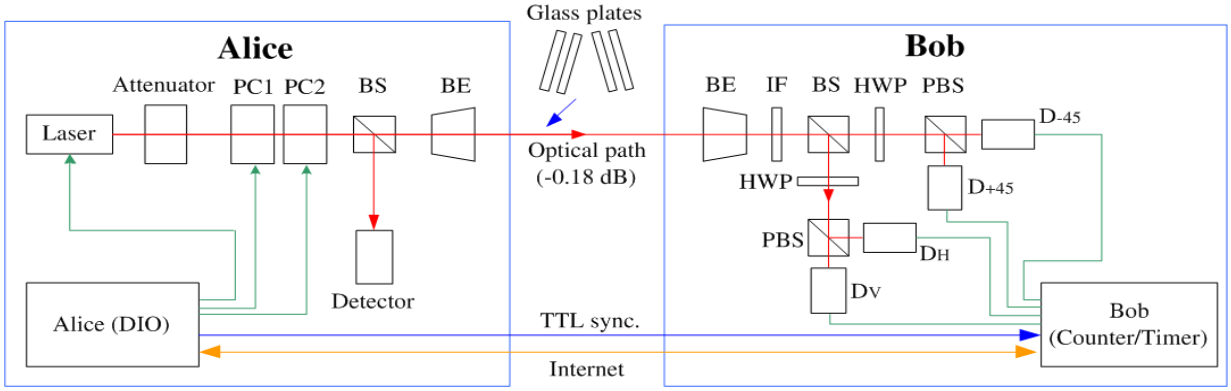

Fig. 1. Our BB84 QKD experimental setup. Attenuated laser pulses are used as the source and polarization encoding was done with a set of Pockels cells PC1 and PC2. The single-photon detectors associated with the measurement bases are D_H, D_V, D_{-45},and D_{+45}. To investigate the effect of weak polarization-dependent losses on the quantum channel, a set of uncoated glass plates at the Brewster angle was inserted Alice's computer.

the Pockels cells, two sets of pseudo-random strings of 0's and 1's are generated and recorded at These random number strings are converted by a digital input/output (DIO) board to 1 MHz TTL signals to control the Pockels cells. A beam splitter (BS) then splits the photon pulse into two: the reflected one is used to monitor the average photon number per pulse μ and the transmitted photon pulse is launched to Bob via a ×5 beam expander (BE).

Incoming photons at Bob's setup are received via a ×5 BE to reduce the beam diameter and an interference filter (IF) with 3 nm full width at half maximum bandwidth is used to cut-down the level of environmental noise. A beam splitter (BS) is then used to randomly direct the incoming photon to one of the two measurement bases {|H>, |V>} or {|−45>, |+45>}. The polarization measurement basis is set with a half-wave plate (HWP) and a Glan-Thompson polarizing beam splitter (PBS). The physical distance between Alice and Bob was 17 m for this experiment but the long-distance capability of the setup was tested with added losses in the quantum channel.

A set of QKD experiments was performed using several different values of the average photon number per pulse μ. For each experimental run, we record the sifted key generation rate (in bits per second) and evaluate the quantum bit error rate (*QBER*) of the sifted key. Our system achieved *QBER* and sifted key generation rate of the experimental data are not showed in this summary.

To investigate how the free-space BB84 QKD system would behave under polarization-dependent losses in the quantum channel, we have inserted a set of uncoated glass plates at the Brewster angle (for the horizontally polarized photon) in the path of the photon. The experimental results are summarized in Fig. 2. Clearly, the loss results in the reduction of the sifted key generation rate and the ratio between the bit values 0 and 1 becomes unbalanced as more glass plates (at the Brester angle) are added. On the other hand, *QBER* remains the same if the dark count contributions are subtracted.

More complete experimental results as well as analysis and implications to long-distance free-space QKD will be presented.

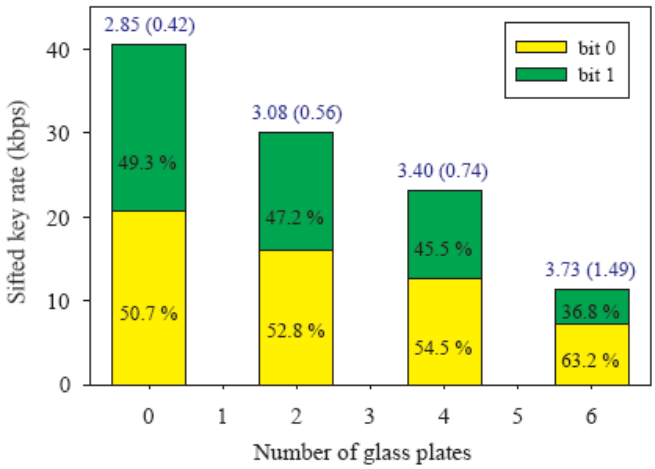

Fig.2. Effects of weak polarization-dependent losses to the performance of the free-space BB84 QKD. The average photon number used for this measurement was μ=0.242. *QBER* values are shown above the data bars.

1. N. Gisin *et al.*, Rev. Mod. Phys. **75**, 145 (2002).
2. C.H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, IEEE Press, New York, 175-179, (1984).