대기 중에서 약한 레이저 펄스를 이용한 B92 양자 암호 프로토콜의 구현

Implementation of B92 quantum cryptography protocol using weak laser pulse in free space

Youn-Chang Jeong†, Yong-Su Kim, and Yoon-Ho Kim
Department of Physics, Pohang University of Science and Technology (POSTECH),
Pohang, 790-784, Korea
†w3140@postech.ac.kr

Quantum cryptography or quantum key distribution (QKD) is a method of establishing a shared random string of secret key bits (0's and 1's) between two parties, Alice and Bob, that can later be used to encode/decode messages for secure communication[1]. The first QKD protocol, proposed in 1984 by Bennett and Brassard (the BB84 protocol), makes use of two non-orthogonal sets of polarization basis states (i.e., four states, which belong to two non-orthogonal polarization basis states, are necessary) of a single-photon for the quantum channel. After eight years, C.H. Bennett noticed that two non-orthogonal states are sufficient for quantum key distribution and proposed new protocol (the B92 protocol) using two non-orthogonal state[2].

In this paper, we report a complete implementation of the B92 QKD protocol in free-space. Our system was based on the weak-pulse polarization-encoding and was tested for several different average photon number per pulse (μ) and the long-distance capability of the system was checked by adding additional optical losses to the quantum channel.

Our experimental setup to implement the B92 QKD protocol is schematically shown in Fig. 1. The transmitter (Alice) uses 780 nm weak laser pulses that have 1 MHz repetition rate and 5 ns pulse width. A Pockels cell is employed to prepare polarization state ($|V\rangle$, $|-45°\rangle$) at Alice. Beam

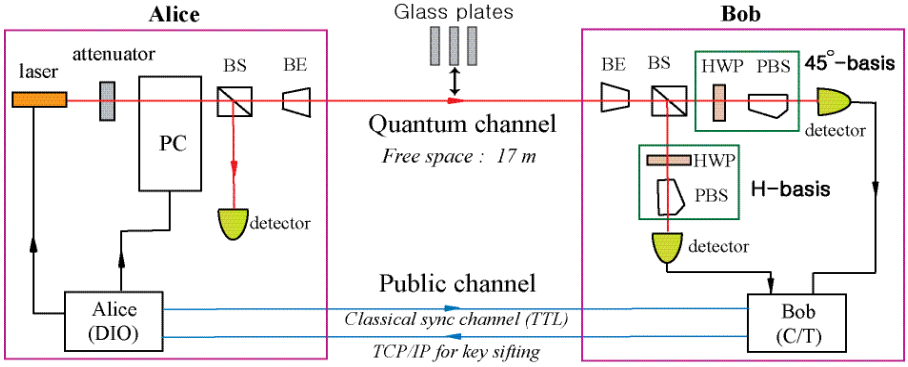

FIG. 1: B92 QKD experimental setup. Alice: Attenuated laser pulses are polarization-encoded with a Pockels'cell (PC). Alice's laser and PC are controlled by a digital input/output card (DIO). Bob: Beam splitter (BS) is used to randomly direct the incoming photon to either $|H\rangle$ or $|45°\rangle$ measurement basis. Bob's results are recorded using a PC-based counter/timer (C/T).

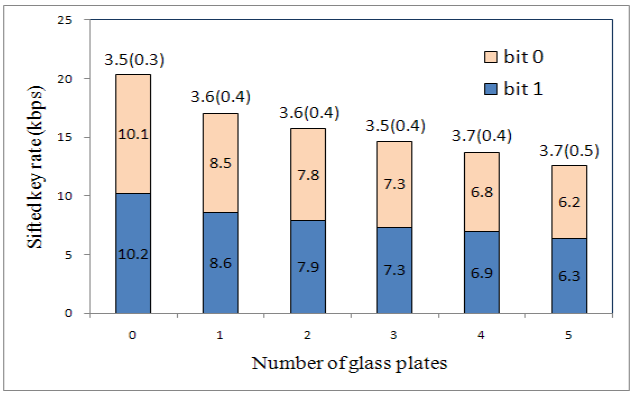

Fig. 2: Experimental data for the B92 QKD experiment with several different values of μ. The QBER value 3.5 (0.5) refers to the total QBER of 3.5 % of which 0.5 % is from the dark counts. The sifted key generation rate and QBER (above the data bars) are shown as a function of the average photon number per pulse μ.

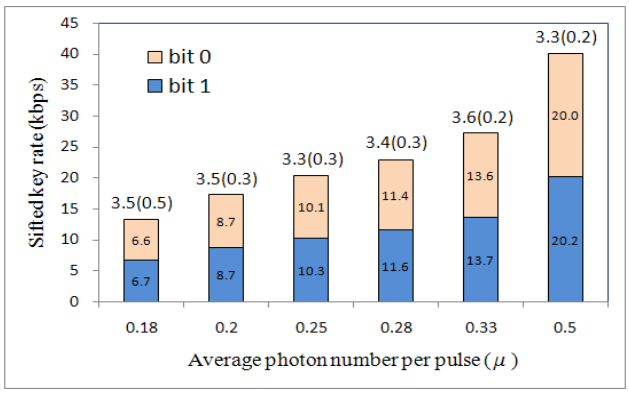

Fig. 3: Experimental data. Effects of additional channel loss to QBER for μ = 0.25. The sifted key generation rate and QBER (above the data bars) are shown as a function of the number of uncoated glass plates inserted in the quantum channel to introduce additionanl losses.

splitter (BS) of Alice is used to split the beam into two for checking the values μ < 1 and launching the pulse to receiver (Bob) via a ×5 beam expander (BE). The quantum channel is a 17 m free-space optical path between Alice and Bob. The public channel consists of a TCP/IP connection for key sifting and a coaxial cable for synchronization. Bob uses a beam splitter (BS) to randomly select one of the two measurement bases (|H〉 , |45°〉). The detectors are turned on only for roughly 100 ns around the expected arrival times of the photons. The detection events are recorded at Bob's computer using counter/timer (C/T) board which is synchronized to Alice's clock signal and they are directly converted to Bob's bit values using the information on the measurement basis (i.e., which detector has clicked). To generate shared secret key bits (sifted keys) between Alice and Bob, Bob sends the string of "click"/"no-click" events (without the information on the measurement basis) to Alice via the internet and Alice uses this information to sift her raw keys to establish a set of shared secret key bits.

We tested our QKD system for the average photon number per pulse μ = 0.18 ~ 0.50. The experimental data are summarized in Fig. 2 and it shows the number of sifted keys generated and QBER for a given μ. It is clear that our implementation of B92 QKD protocol is quite successful as the number of sifted bit values 0' and 1' are roughly the same and QBER rather low. The sifted key generation rate agreed well with the theoretically expected value.

We have also investigated how our B92 QKD implementation behaves under the presence of additional channel losses by introducing a set of uncoated glass plates to the quantum channel. The experimental data for this measurement are summarized in Fig. 3. The data suggest that our B92 QKD system is not affected much by additional channel losses, i.e., QBER is almost constant with increasing losses. Slight increase in QBER is likely to be caused by misalignment and polarization effects of the glass plates (oriented orthogonal to the path of the photons).

References

1. N. Gisin et al., "Quantum cryptography," Rev. Mod. Phys. **74** 145-195 (2002)

2. C.H. Bennett, "Quantum cryptography using any two non-orthogonal states", Phys. Rev. Lett. **68** 3121-3124 (1992)