# 대기 중에서 약한 레이저 펄스에 의한 SARG04 양자 암호 프로토콜의 구현

# Weak-pulse implementation of SARG04 quantum cryptography protocol in free space

Youn-Chang Jeong†, Kwan-Young Hong, 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

The single-photon source is one of the essential elements that are needed to build a secure quantum cryptography system[1]. An efficient single-photon source suitable for quantum cryptography, however, is not yet available. Instead, many current researches on long-distance quantum cryptography are done by using strongly attenuated laser pulses, such that the average photon number per pulse $\mu < 1$, as the photon source.

Since the laser follows the Poisson photon statistics closely, strongly attenuated laser pulses ($\mu < 1$) are mostly empty (i.e., contains no photons) or, with much less probability, there is one photon during the duration of the pulse. However, the probabilities of finding two or more photons are always non-zero. An eavesdropper, Eve, could then implement the photon number splitting (PNS) attack, making use of these multi-photon events, to the quantum channel to extract some of the shared key bits without being detected.

Recently, Scarani, Acin, Ribordy, and Gisin proposed a quantum cryptography protocol (SARG04) which is known to be robust against the PNS attack[2]. In this paper, we report an implementation

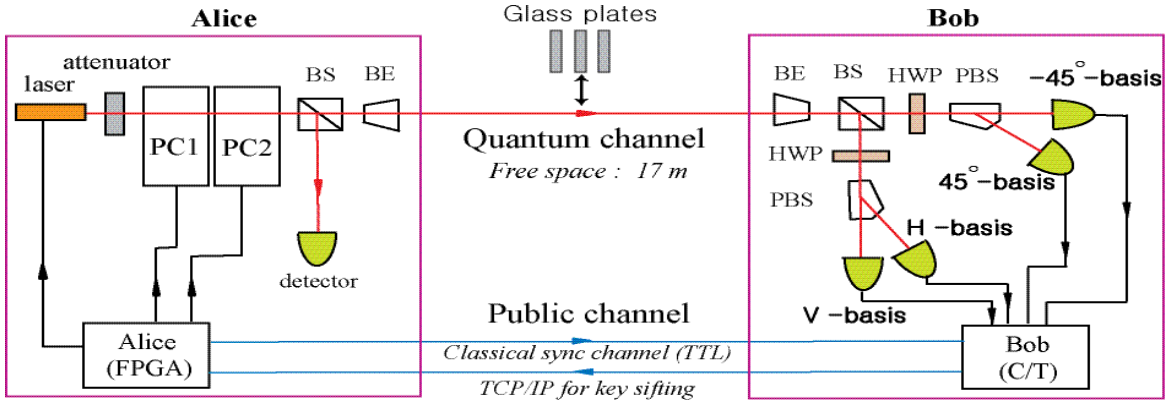


Fig. 1. SARG04 QKD protocol experimental setup. Alice: Attenuated laser pulses are polarization-encoded with two Pockels'cell (PC1, PC2). Alice's laser and Pockels'cell are controlled by a field programable gate array module (FPGA). Bob: Bob's detection events are recorded using a PC-based counter/timer (C/T).

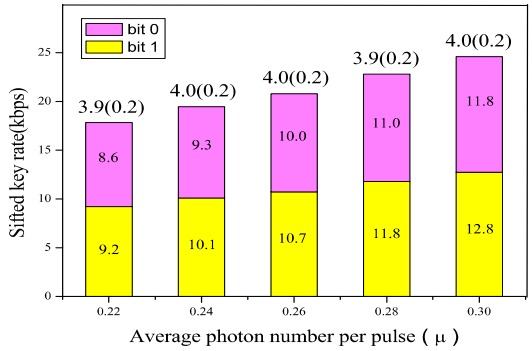


Fig. 2. Experimental data. The sifted key generation rate and QBER (above the data bars) are shown as a function of the average photon number per pulse μ. The QBER value 3.9 (0.2) refers to the total QBER of 3.9% of which 0.2% is from the dark counts.

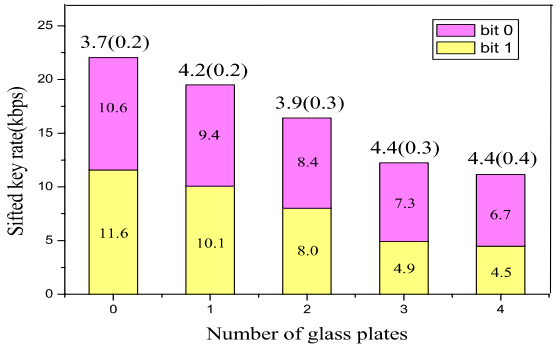


Fig. 3. Experimental data. The sifted key generation rate and QBER (above the data bars) are shown as a function of the number of uncoated glass plates inserted in the quantum channel to introduce additional losses.

of the SARG04 quantum cryptography protocol in free-space over the optical table. The performance of the system was tested for several different values of μ and the long-distance capability of the
system was checked by adding additional optical losses to the quantum channel.

The experimental setup to implement the SARG04 QKD protocol is schematically shown in Fig. 1. The laser emits a train of 16 ns laser pulses and operates at 1 MHz clock rate which derived from Alice' computer equipped with a field programmable gate array (FPGA) module. The laser pulse is attenuated so that average photon number per pulse $\mu < 1$. Two Pockels cells prepare one of the four polarization states ( $|V\rangle$ , $|H\rangle$ , $|45°\rangle$ , $|-45°\rangle$ ) for the attenuated laser pulses. Beam splitter (BS) of Alice is used to split the beam into two for checking the value μ and launching the pulse to Bob via a ×5 beam expander (BE). Bob's beam splitter (BS) randomly direct the incoming photon to one of the two measurement bases. The detectors are gated for roughly 100 ns about the expected arrival times of the photon. The detection events are recorded at Bob's computer using a counter/timer board which is synchronized to Alice's clock signal.

We tested our QKD system for the average photon number per pulse $\mu = 0.22 \sim 0.30$. The experimental data are summarized in Fig. 2. The data show that the sifted key generation rate improves as the average photon number per pulse slowly increases up to $\mu = 0.3$. QBER, however, remains virtually the same during this process.

We have also checked the long-distance capability of the system by adding optical losses to the quantum channel. The optical losses were simulated by adding a set of uncoated glass plates at the normal angle. Fig. 3 shows the experimental results. It is clear that, while the sifted key generation rate is reduced, QBER remains virtually the same if the dark count contributions are subtracted.

References

1. N. Gisin et al., "Quantum cryptography," Rev. Mod. Phys. **74**, 145-195 (2002)
2. V. Scaraniet al., "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**, 057901 (2004).