BB84와 SARG04 양자 암호에서의 Depolarizing 채널 효과
Effects of depolarizing quantum channels on BB84 and SARG04 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 using both the quantum channel and the classical channel.(1)

Since the BB84 protocol was first introduced in 1984(2), a number of QKD protocols have been introduced and experimentally demonstrated.(1) In particular, the SARG04 protocol uses identical quantum states as BB84 for encoding but it differs from BB84 in the key sifting procedure which makes use of the classical channel. In practical QKD in which weak coherent states are used in place of true single-photon states for qubit encoding, the SARG04 protocol is known to be more robust against the photon-number splitting attack.(3)

In this paper, we investigate experimentally how a non-ideal quantum channel between Alice and Bob affects both BB84 and SARG04 protocols. In particular, we consider the effect of a depolarizing quantum channel, which turns an initial pure state to a mixed state, on the quantum bit error rates. The effect of a depolarizing quantum channel on the quantum state (pure state, $|\psi\rangle$) sent by Alice is that Bob instead receives a mixed state. This can be described as(4)

$$\varepsilon[|\psi\rangle] = F|\psi\rangle\langle\psi| + D|\psi^{\perp}\rangle\langle\psi^{\perp}|, \tag{1}$$

where $F+D=1$ and the degree of mixedness depends on the values F and D.

Under the depolarizing channel, the quantum bit error rate (QBER) of BB84 and SARG04 protocol show different behavior. After consideration it, (It will be shown in our talk.) QBER of BB84 and SARG04 protocol can be given as

$$QBER_{BB84} = \frac{D}{F+D} = \frac{1-V}{2} \tag{2}$$

$$QBER_{SARG04} = \frac{D}{\frac{1}{2}(F+D)+D} = \frac{1-V}{2-V}. \tag{3}$$

The experimental setup to test the above results, eqs. (2) and (3), is schematically shown in left of Fig.1. The Alice part of the QKD setup consisted of a 780 nm pulsed laser operating at 1 MHz repetition rate and two Pockels cells were used to encode the polarization state according to the random bit sequences generated at Alice's PC. The Bob part of the QKD setup consisted of four

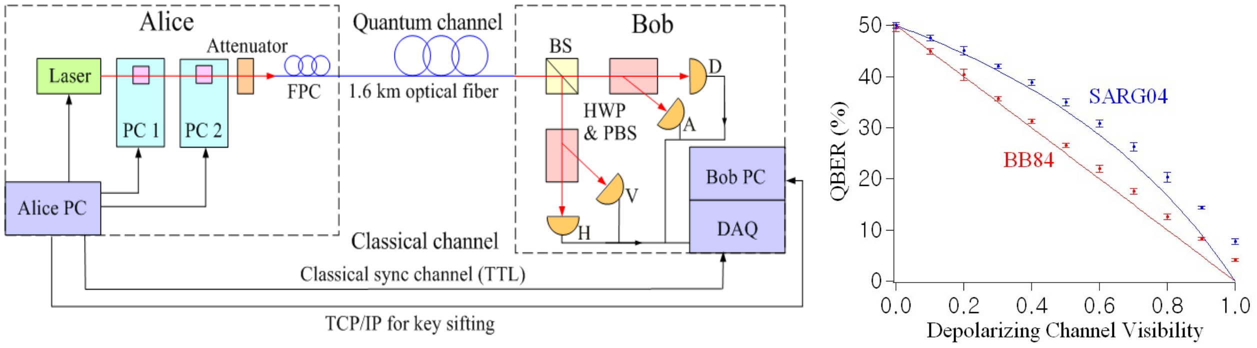

Fig. 1: (left) Attenuated laser pulse at 780 nm are polarization encoded with a set of Pockels cell PC1 and PC2. Four single-photon counting modules are used to detect polarization-encoded single-photon at $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$. (right) The effect of depolarizing channels on BB84 and SARG04 protocols. Solid lines are eqs. (2) and (3).

single-photon counting modules which allow us to detect photons at the $\{|H\rangle, |V\rangle\}$ basis and at the 45° rotated $\{|D\rangle, |A\rangle\}$ basis. The detected events as well as the measurement basis information are stored at Bob's PC.

The effect of the depolarizing quantum channel was then implemented by randomly flipping the state $|\psi\rangle$ stored at Alice's PC to its orthogonal state $|\psi^{\perp}\rangle$. For example, to test the quantum bit error rates at $V=1$, no bit flipping should be done. As V is lowered below 1, however, more bits needs to be flipped and the ratio of the flipped/unflipped bits can be readily calculated from the visibility V.

The experimental data to test the relations in eqs. (2) and (3) are shown in right of Fig. 1. The solid lines are from eqs. (2) and (3) and the solid squares are from the experiment. The experimental data confirm that the quantum bit error rate behaviors as functions of the depolarizing channel visibility follow the predictions in eq. (2) and (3). Slightly different slopes of the experimental data, with respect to eqs. (2) and (3), are due to non-zero QBER at $V=1$ and they are caused by non-perfect polarizing beam splitters, detector dark counts, non-ideal performance of the Pockels cells, etc.

The experiment clearly demonstrates that, when the effect of depolarization in the quantum channel is considered, BB84 poduces less QBER than SARG04. Since the secure key generation rate is closely related to the QBER, BB84 would perform better than SARG04 in the case of depolazing quantum channels.

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).
3. V. Scarani *et al.*, Phys. Rev. Lett. **92**, 057901 (2004).
4. C. Branciard *et al.*, Phys. Rev. A **72**, 032301 (2005).