광섬유에서 미끼 상태(decoy state) 양자 암호의 실험적 구현

Experimental implementation of decoy state quantum cryptography in optical fiber

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) offers the promise of unconditional security. The single-photon source is one of the most essential elements that are needed to build a secure quantum cryptography system[1]. However, a highly efficient single photon source suitable for quantum cryptography is not yet available commercially. Instead, many current researches on long-distance quantum cryptography are done using weak laser pulses, such that the average photon number per pulse is much less then unity, as the photon source of a QKD system.

Since the laser follows the Poisson photon statistics closely, a weak laser pulse ($\mu < 1$) still has the probability of having two or more photon per pulse. An eavesdropper, Eve, could then implement the photon number splitting (PNS) attack to the quantum channel to extract some of the shared key bits without being detected.

In 2003, Hwang proposed a scheme that allows one to build a secure QKD system using weak laser pulses as the photon source[2], and this scheme is now known as the decoy method.

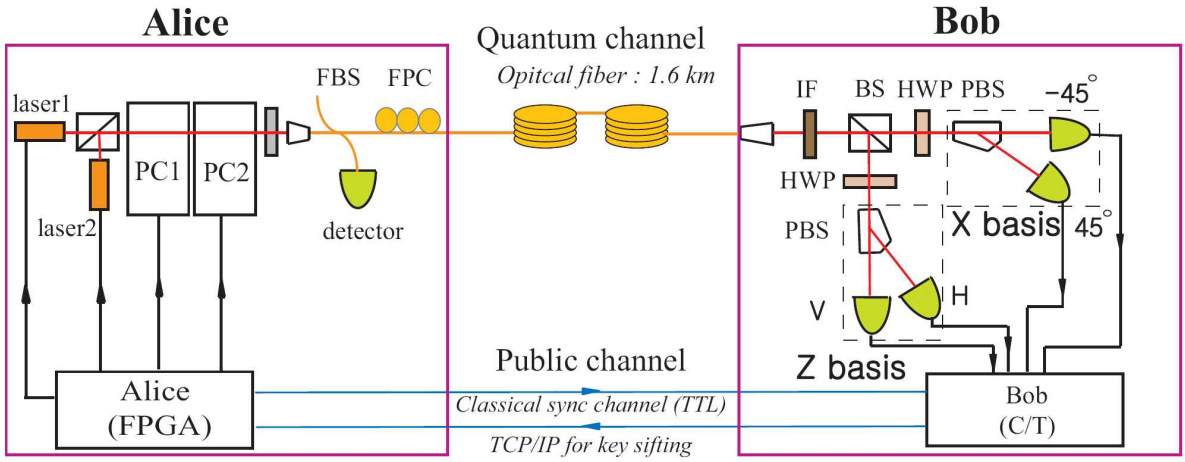

Fig. 1. Experimental setup. Alice: Attenuated laser pulses are polarization-encoded with two Pockels'cell (PC1, PC2). Alice's laser and Pockels'cells are controlled by a field programable gate array (FPGA) module. Bob: Bob's detection events are recorded using a PC-based counter/timer (C/T).

In the decoy state method, Alice generates several different intensities of photon states which are called decoy states and signal states, and send them to Bob. Since Eve does not know which pulses are decoys (or signals), she must perform the PNS attack to all of the pulses. Different average intensities of the signal and decoy pulses then lead to different yields on Bob's detectors[2],[3]. By monitoring the yields for the signal and the the decoy pulses, Alice and Bob can find out the presence of Eve's attack.

The experimental setup to implement the BB84 QKD protocol using the decoy state method is schematically shown in Fig. 1. The experimental setup consists of the transmitter (Alice), the receiver (Bob), the optical fiber quantum channel (1.6 km single-mode optical fiber with a loss of 3 dB/km), and the public channel (coaxial cables and the internet).

The signal and decoy lasers emit a train of 3 ns laser pulses (780 nm) and operate at at 1 MHz clock rate which is derived from Alice's computer equipped with an FPGA module. Alice first generates and records three sets of pesudo-random bit strings. The first and second string sets are used for Alice's raw keys and basis information. These strings are converted to a specific 1 MHz waveform to control the two Pockels cells which in turn prepare one of the four polarization states ($|V\rangle$, $|H\rangle$, $|45^{o}\rangle$, $|-45^{o}\rangle$) for the decoy and signal laser pulses. Third string set is for the information on decoy and signal pulses. All these operations are done in almost real time by the FPGA board in the Alice's computer.

Bob's beam splitter (BS) randomly directs the incoming photon to one of the two measurement bases (X basis and Z basis). 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 C/T which is synchronized to Alice's clock signal.

To generate shared sifted keys between Alice and Bob, the BB84 protocol is used. Additionally, Alice calculates the parameters of the decoy state method (gain, signal QBER and decoy QBER).

The theoretical key generation rate is given by $R \approx \eta\mu f(e_d)H_2(e_d) + \eta\mu e^{-\mu}[1-H_2(e_d)]$, where e_d is the probability that a photon hits the erroneous detector, $f(x)$ is the bidirectional error correction efficiency, and $H_2(x)$ is the binary Shannon information function[3]. We calculated the optimal average photon numbers of signal and decoy pulses using computer simulation based on experimental parameters. In the experiment, $\mu_{signal} \approx 0.5$ and $\mu_{decoy} \approx 0.10$ were used. Detailed experimental setup, communication processes, and data analysis will be presented.

References

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

2. W.-Y. Hwang, ''Quantum Key Distribution with High Loss: Toward Global Secure Communication,'' Phys. Rev. Lett. **91**, 057901 (2003).

3. X. Ma, B. Qi, Y. Zhao, and H.K. Lo, ''Decoy State Quantum Key Distribution,'' Phys. Rev. A **72**, 012326 (2005).