Performance of the BB84 Quantum Key Distribution System

Santhad Phithakwongsaphorn, Watchara Pornkaveerat, Surasak Chiangga

Abstract

We present the experiment results of the Bennett-Brassard 1984 (BB84) protocols for a free space quantum key distribution system (QKD). The QKD system under laboratory controlled enables to generate sifted-key rate of 5 Kbits/s with average quantum bit error rate (QBER) of 0.4%.
1. Introduction

Quantum key distribution, also known as quantum cryptography, was proposed by Bennett and Brassard in 1984 (Bennett et al., 1984). The first experimental setup was realized by the same group in October 1989 (Bennett et al., 1992). The original experiment was based on a coding scheme involving polarized photons, in which the linear and diagonal polarization states formed the required pair of bases. Since then on, there has been a great deal of interest in developing the technique in order to investigate its potential for applications in real communication systems. Various QKD protocols have been implemented either through fiber or free space (Gisin et al., Black et al. and S. Gary, 2002, 2002, and 2005). Much of interest in QKD originates from the fact that its security relies on laws of quantum mechanics, in contrast to classical cryptography systems which rest on difficult mathematical problems. Some current difficult problem such as factoring large integers becomes easy problem for quantum computer (S. Lloyd, 1993). This ability would allow a quantum computer to break many of the cryptographic systems in use today. Now, quantum cryptography has come out from laboratory to real products, but a numbers of practical problems remain to be solved see for example (Gisin et al, 2002) and (N. Lütkenhaus, A. Poppe et al., D. Stucki et al., 1999, 2004, and 2005). The significant drawbacks of many practical quantum cryptography systems are unavailable single-photon source and imperfect detectors. The most of practical sources rely on attenuating laser pulses. One disadvantage of these sources is the pulse contains more than one photon with significant probability. Eavesdropper can harm those systems through a beam splitter attack (Bennett et al., 1984). Less efficient single-photon detectors have obviously impacted on the bit rate and maximum span length (Gisin et al., 2002). We are developing QKD to improve some of the implementation features in quantum cryptography, including hardware design, software integration and rate of key generation. In this paper, we give first a general discussion of the principle of quantum cryptography based on the BB84 protocol (Bennett et al., 1984) in section 2. We then describe in detail the design of the transmitter and the receiver in section 3. The experimental features of the presented QKD system based on polarization encoding of attenuated laser pulses is described in section 4.
Finally, we conclude the performance of the presented system with an example in which we implement it for the short-range free space quantum key generation.

2. Principle of Quantum Cryptography

In Bennett and Brassard’s protocol (BB84), the sender, Alice, prepares quantum carriers such as spin-1/2-particles with equal probability in the computational basis $|+_{z}\rangle = |0\rangle, |-_{z}\rangle = |1\rangle$ or the conjugate basis $|+_{x}\rangle, |-_{x}\rangle$ given by

$$
|+_{x}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle),

|-_{x}\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
$$

The pairs of pure states $|0\rangle, |1\rangle$ and $|+_{x}\rangle, |-_{x}\rangle$, show in Fig. 1 are Eigen states of $\sigma_{z}$ and $\sigma_{x}$, respectively. Alice encodes bit 0 onto $|0\rangle$, and encodes bit 0 onto $|1\rangle$. Similarly in the conjugate basis, bit 0 and 1 are encoded as $|+_{x}\rangle$ and $|-_{x}\rangle$, respectively. The qubit is then sending to Bob, who randomly projects each quantum carrier onto either, the computational or $|\pm_{x}\rangle$ basis. The probability that Bob correctly receives Alice’s transmitted bit can be obtained by computing the overlap between the states of two orthogonal bases. According to the randomness of Alice’s choice of basis, there is symmetry between these two bases. Hence, we shall compute the probability for Bob of obtaining correct bit when he measures in $\sigma_{z}$ basis.

$$
P_{c} = \frac{1}{4} \left( |\langle 0|0\rangle|^2 + |\langle 1|1\rangle|^2 + |\langle 0|+_{x}\rangle|^2 + |\langle 1|-_{x}\rangle|^2 \right) = \frac{3}{4} \tag{2}
$$
After the transmission, Bob tells Alice which type of measurement basis he used but keeps the result secret. Alice tells Bob for which detection they had chosen the basis. They then agree to discard all the events in which they used a different measurement basis. Alice and Bob should therefore share an identical sequence of random bit. This sequence is called the “sifted” key. In present of an eavesdropper, Eve is inevitable to introduce some error into the sifted key. On the other hand, in the realistic quantum cryptographic systems have some problems with noise, so the sifted key will contain some errors. These is, in principle, impossible distinguish between an error caused by an eavesdropper and error due to noise. In order to give a guarantee of security, Alice and Bob now choose a random subset of the remaining bit string to test for the presence of Eve. If no errors are found Alice and Bob can be confident that the remaining bits which have not been disclosed publicly are secure and therefore constitute a useful shared secret “reconciled” key. During the reconciliation, some information about the sifted-key is available to eavesdropper. Therefore their reconciled bit string is only partially secret, and has to be compressed by privacy amplification to gain security. The privacy amplification procedure of Bennett et al. requires Alice and Bob to estimate the maximum bits of the reconciled key that Eve could know, and then they agree on publicly decided random compression function to compute the shared key bits after their error correction.

3. Experimental Realization

3.1 General description of the system

A schematic diagram of the reported QKD system is shown in Fig.2. The transmitter uses four 850-nm-wavelength Vertical cavity surface laser diodes. Each laser diode is directly modulated its injection current by applying a train of 2 ns electrical pulses at a repetition rate of 1 MHz. The beams are then polarized horizontally/vertically by the 5 mm cube polarizing beam splitters (PBS). A quarter-wave plate (QP1) with axis at 45° rotates horizontal and vertical polarization to right-circular and left-circular polarization,
Fig. 2 Schematic diagram of the QKD experiment. PBS: polarization beam splitter. LD: laser diode. BS: beam splitter. QP: quarter wave plate. L: lens. IF: interference filter. APD: avalanche photo diode, MMF: Multimode fiber.

respectively. The four beams overlap at a 5 mm cube non-polarizing beam splitter (BS1). The output laser pulses are reduced the intensity to a mean photon number of about 0.1 photons per pulse after passing through an iris diaphragm. The 8 cm focal length lens forms a collimated beam. A PCI card is used to control the timing of sequence of laser pulses. Alice’s choice of polarization basis is selected randomly by the pseudo-random number generated by a computer that addresses each laser diode. The receiver consists of similar optical elements to the transmitter, an 830±3 nm interference filter (IF) to reduce the background noise, and four C30902S-DTC, silicon avalanche photodiodes (APDs) with built-in thermoelectric cooler to detect single photons. The polarization analyzing optics consists of a symmetry cube beam splitter (BS2) that randomly directs collected photons onto either of two distinct optical paths. The lower optical path contains a quarter-wave plate (QP2) followed by a cube polarizing beam splitter (PBS4) to test photons for left circular polarization and right circular polarization in transmission and reflection, respectively. The upper optical path contains a cube polarizing beam splitter (PBS3) to test for horizontal and vertical polarization in transmission and reflection direction, respectively. The signal output from each APD is acquired by a PCI card to the personal computer for bits analysis.
4. Results

The polarization state of the system is measured using a near infrared polarizer, a wave plate and a photodiode. Fig. 3 shows the visibility of the transmitter for the H, V, R, and L which are 0.97, 0.97, 0.99 and 0.99 respectively.

![Fig. 3 Polarization of a transmitter for the H-V basis (Left) and R-L basis (Right)](image)

Fig. 3 Polarization of a transmitter for the H-V basis (Left) and R-L basis (Right)

Fig. 4 shows the visibility of the receiver for the H-V, and R-L which are 0.97, 0.97, approximately 0.98, and 0.98 respectively. This visibility indicates that the average QBER of is 1%.

![Fig. 4 Polarization of a receiver for the H-V basis (Left) and R-L basis (Right)](image)

Fig. 4 Polarization of a receiver for the H-V basis (Left) and R-L basis (Right)

In order to characterize the system, the laser was pulsed with the same bit many times at clock frequency of 1 MHz. Our goal is to evaluate the mean number of polarized photon per pulse, the visibility and synchronization of the system. For each run, the
measurements were taken about 8 s of the data acquisition time. A total of \(8.8 \times 10^4\) photons are recorded after polarized encoding. We assume that the transmission efficiency of Alice’s is 0.9, thus the mean photons number per pulse was \(\mu = 0.1\). The QKD system was operated over 1 m indoor optical path, and they located on an optical breadboard. We evaluate the sifted key rate from the amount of keys recorded in PC. We found that the sifted-key rate is 5 Kbits/s and the average QBER is 0.4\% (H: 0.7\%, V: 0.2\%, R: 0.0\%, L: 0.6\%).

5. Conclusion and Outlook

We present a laboratory QKD system based on the BB84 protocol. The experimental test for short-range implementation shows that this QKD system is capable of generating the shared secret key of 5 Kbits/s, and with the QBER of 0.4\%. Further improvements in clock rate, increasing visibility and detector timing resolution will further improve system performance.

Acknowledgments

This work was supported by the Kasetsart University Research and Development Institute.

References


