Experimental Quantum Cryptography based on the BB84 Protocol

S. Deachapunya[1], S. Chiangga[1], H. Weinfurter[2,3]
[1]Department of Physics, Kasetsart University, Bangkok 10900
[2] Sektion Physik, Ludwig-Maximilians-Universität München,
Schellingstr. 4/III, D-80799 München, Germany
[3] Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany

Abstract

Quantum cryptography is a new technique that provides verifiable secure key exchange between the sender and receiver. The security of the quantum cryptographic system is protected by the laws of quantum physics, which ensure that any eavesdropping can always be detected. This is in strong contrast with classical key exchange, where the security depends on (unprovable) assumptions. Recent experimental implementation of quantum cryptography achieved about 50 km point-to-point key exchange over optical fibers and about 1 km over a free space connection in daylight. Here we report the development of experimental free space quantum cryptographic systems based on the BB84 protocol. Our system does not use any active manipulation elements, resulting in compactness, reliability and easy handling.

Keywords: quantum cryptography, quantum information

1. INTRODUCTION

Cryptography is the study of techniques and applications of secure communication. The fundamental objective of cryptography is to transmit information over an insecure channel in such a way that an opponent cannot understand it. This goal can be achieved if the sender and receiver both possess some secret information, referred to as a key. The safety of the information transmission thus depends entirely on the safety of the key [1]. With conventional communications, it is taken for granted that digital communication can always be passively monitored or copied. Numerical cryptoanalysis is possible for many systems. Their security therefore depends crucially on the computational power a potential eavesdropper might have.

By contrast, the security of quantum cryptographic keys is based on fundamental and immutable laws of quantum physics, one of which is the Heisenberg uncertainty principle. Any eavesdropping attempts to intercept the communication channel can always be detected. The original quantum cryptography scheme was proposed in 1984 by Bennett and Brassard [2] abbreviated as BB84. The first prototype constructed in 1989 was based on a coding scheme involving polarized photons, in which the linear and circular polarization states formed the required pair of bases. Due to the Heisenberg uncertainty principle, measuring, say, the linear polarization of a single photon projects its state into an eigenstate of linear polarization and perfectly destroys any prior value one might have had for circular polarization. Therefore, if the wrong choice of measurement basis is made by the eavesdropper, he will raise the key error rate above a threshold value which alerts the legitimate users of the presence of an eavesdropper.

In this paper, we give a short introduction into the theory of quantum cryptography. Then we describe the experimental aspects involved in the actual realization of our quantum cryptographic system based on polarization encoding of attenuated coherent light pulses.

2. THEORY

The general quantum cryptographic system comprises of a transmitter and a receiver. The transmitter consists of the sources of photons and an optical system. In realistic systems, the sender (Alice) generates an approximation to the desired sequence of single photons by attenuating short pulses of light from laser diodes. The optical system randomly assigns polarization states to the photons. Each photon's polarization state is then encoded by the sender according to a random, binary number "1" or "0".

The receiver (Bob) comprises of an optical system similarly to the transmitter and of the single photon detectors. The receiver randomly projects the incoming photon onto either one of two distinct perpendicular optical paths, where each optical path is oriented to detect a specific polarization state and the bit number "1" or "0" encoded by the receiver. The quantum key generation requires several steps as follow: [3], [4].

1. Alice sends a sequence of photons, each randomly encoded with one of the four polarization states, and each occupying a well-defined time slot.

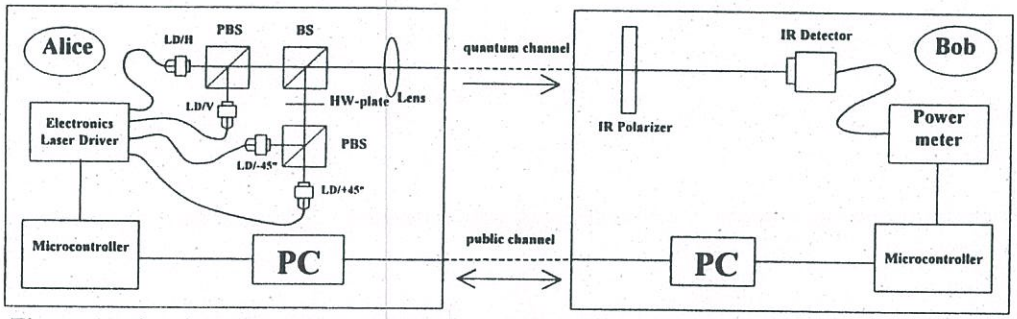


Figure 1. The simplified diagram of our practical quantum cryptography transmitter.

2. Bob's clock is well synchronized with Alice's clock and in each of the time slots he randomly chooses to measure one of the two polarization types; i.e. circular or linear. He records the result of that measurement.

3.After the transmission, Alice and Bob communicate publicly e.g. telephone, newspaper etc.:Bob tells Alice when he detected a photon and which type of polarization measurement he used in this particular time slot, but keeps the result secret.

Alice tells Bob for which detection they had chosen the same basis. They then agree to discard all the events in which they used a different measurement basis.

4. Alice and Bob now choose a random subset of the remaining bit string, which they use to test for the presence of an eavesdropper.

This test again is carried out over the public channel, but now Alice and Bob perform a statistical comparison of their selected bits. If no errors are found Alice and Bob can be sure that the remaining bits which have not been revealed publicly are secure and therefore constitute a useful shared secret key.

3. EXPERIMENTAL SETUP

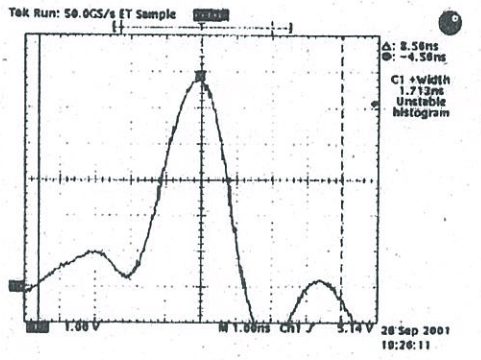
A simplified diagram of our quantum key distribution transmitter module is shown in Figure 1. The attenuated pulse is generated by applying a 1.7 ns electrical pulse with a 2.86

MHz repetition rate to one of four low power laser diodes (Hitachi, 830nm 40mW) which is selected randomly with the pseudo-random number generated from a personal computer. The Coherence states $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle$ are generated by each laser operation well above the threshold. In our case the amplitude $|\alpha|^2 = 0.1$ was chosen, to give a photon number distribution per pulse according to $P_n = e^{-|\alpha|^2}|\alpha|^{2n}/n!$. A passive optical system sets the photon's polarization to $|H\rangle$, $|V\rangle$, $|+45\rangle$, or $|-45\rangle$ depending on whether the binary number is a "0" or a "1". It is comprised of a half wave plate ($\lambda/2$), two polarizing beam splitters (PBS), a beam splitter (BS) and lens. A pair of laser diodes in the upper paths is oriented so that the light beams overlapped at PBS have horizontal polarization, $|H\rangle$ (after transmission) and vertical polarization, $|V\rangle$ (after reflection). A pair of laser diodes on the lower path is also oriented similarly to the first pair, but a half wave plate rotates the plane of polarization by 45°. Therefore, they allow us to set the necessary $|+45\rangle$ and $|-45\rangle$ polarization states. The polarizer and the optical power meter (Newport, 1830-C) in series is used to test the performance of the transmitter.

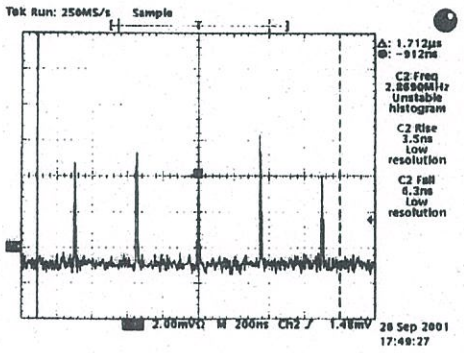
4. RESULTS

Figure 2(a) shows the 1.7 ns, 2.86 MHz input signal to the four laser diodes monitored with an oscilloscope (Tektronix, TDS784D). The optical pulse signal generated by a laser diode, measured with the Si-PIN photodiode (Thorlab, DET210), is shown in Figure 2(b). The observed width of 7 ns is currently limited from below by the bandwidth of the detection system, but surely is not longer than the driving pulse.

Figure 3 presents the variation of the observed intensity depending on the angle of the analyzing IR-polarizer for the four input polarizations. We observe visibilities of V_H=0.97, V_V=0.93, $V_{+45°}$=0.97, and $V_{-45°}$=0.97, which clearly demonstrates the usability of our simple transmitter for low-noise, free-space quantum cryptography.



(a)



(b)

Figure 2. (a) The 1.7 ns, 2.86 MHz input signal, (b) The optical output signal, measured with the Si-PIN photodiode

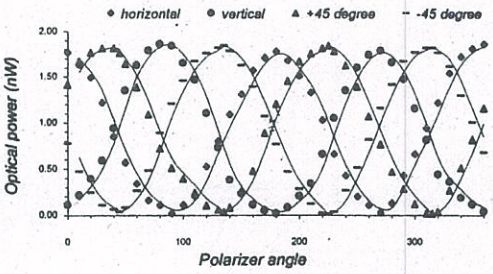


Figure 3. The polarization analysis of the transmitter

5. CONCLUSION

In this work, we present first tests of the quantum cryptographic transmitter module for a free space application of the BB84 protocol. The data measured with the optical power meter shown in Figure 3 indicate that it is feasible to send the random polarization state of photons to the receiver by our fast and compact transmitter. By contrast to other experimental set-ups which commonly use some active manipulation devices to set the photon's polarization, our system utilizes merely laser diodes and a few passive optical components. Most of the hardware is constructed in our laboratory, resulting in cost effective and easy to reconfigure systems.

6. ACKNOWLEDGEMENTS

S. Chiangga acknowledged financial support by Kasetsart University Research and Development Institute under contract □.□. 12.43 and by the Thailand Research Fund under grant PDF 22/2543. And S. Deachapunya appropriately acknowledged financial support by UDC scholarship.

REGERRENCES

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. pp. 175-179, December 10-12, 1984. *Proceedings of the International Conference on Computers, Systems & Signal Processing*, Bangalore, India.

[2] Charles H. Bennett and Gilles Brassard. An update on quantum cryptography. In G. R. Blakley and D. C. Chaum, editors, *CRYPT084,* pp. 475-480. Springer, 1985. Lecture Notes in Computer Scitnce No. 196.

[3] Gilles Brassard, Charles H. Bennett and Arthur K. Eckert. Quantum cryptography. *Scientific American*, pp. 26-33, October 1992.

[4] Richard J. Hughes et al., Secure communications using quantum cryptography, *SPIE Proceedings* **3076**, 2 (1997).