The FPGA Implementation of Quantum Key Distribution Based on BB84 protocol

Huifang Li[1, a], Minghui Zhang[1, b], Kaibin Wang[2, c]

[1] School of Electronics and Information, Northwestern Polytechnical University, Xi'an, China

[2] Xi'an Research Institute of China Coal Technology & Engineering Group Corp

[a]Lhuifang@nwpu.edu.cn, [b]nikkoch@163.com, [c]wangkaibin@cctegxian.com

Keywords: Quantum key distribution; Polarization encoding; BB84 Protocol; FPGA.

Abstract. A new QKD implementation scheme of BB84 protocol is introduced based on FPGA. Firstly, the overall design method and the functional division are described in detail. Then, the logic design of the sub-module are significantly studied, including random data module, laser source drive module, error correcting module, receiver/transmitter interface module, extracting original key module and error rate estimation module. Finally, the partial simulation results are given to verify the correctness of the design function. The set-up advantage is the small size, high bitrates, flexible configuration, and convenient algorithm update.

Introduction

With the sustaining growth of computer networks, there is an increasing need for encryption to ensure that the information cannot be acquired by third parties. Remarkably, quantum mechanics, which seemingly do not related to encryption, now directly be brought to bear on the problem of communication security in the emerging technology called as quantum cryptography.

Quantum key distribution (QKD), as an important part of quantum cryptograph, generates a safe key shared between the sender and receiver. It not only highly hold back eavesdropping, but also makes the level of communication security higher in telecommunication channel. The most widely used QKD scheme for long-distance QKD is BB84 protocol announced by Bennett-Brassard in 1984 [1], which can prevent the eavesdropping and attack, and also provides the unconditional security. Nowadays, many QKD schemes have been brought up and a lot of efforts have been done to improve the practicability of QKD [2]. While BB84 protocol is still being widely used [3][4][5], and it has been proved unconditional secure.

Up to now, many groups' efforts to implement QKD experiments, even a whole QKD system. Especially, this year China will launch quantum communication experimental satellite.

In this paper, we propose a FPGA method to implement a high speed bit coding for BB84 protocol. Based on Xilinx XC5VLX50T experimental platform of FPGA digital control system, the hardware implementation system of BB84 quantum key distribution protocol is designed with the advantage of hard core provided by Xilinx. The our work not only verifies the feasibility of the suggested scheme, but also provides support for building complete quantum secret communication system, and has certain significance for the research of quantum cryptography.

The QKD System and the BB84 Protocol

A typical scheme of QKD system is shown as figure 1. The system mainly consists of quantum information cell/sink, coding/decoding, modulation/ demodulation and channel, including quantum channel and classical channel (or auxiliary channel) etc. In fact, the stable and reliable quantum channel and the classical (or auxiliary) channel are the basic requirement of quantum secret communication. Auxiliary channel without confidentiality requirement is a public channel, but needs to confirm the integrity and authenticity of the data, so that it is possible to make sure there is no third party eavesdropping.

The standard BB84 protocol is divided two main steps: (i) quantum communication, in which Alice and Bob give a correlated bit string; and (ii) classical post-processing, in which they extract a secret key from the bit string. The usual realization of BB84 is also regard as prepare and measure, namely, Alice prepares random quantum states and Bob measure later.

Firstly, Alice randomly chooses her symbol with a random basis, which the single photon is polarized in one of the four states (0°, 45°, 90°, 135°), and send it to Bob .

Secondly, Bob randomly chooses his basis, and measures the polarization of arriving photons with the chosen basis. The measure result and the corresponding basis chosen by Bob would be recorded. Then, over a classical channel, Bob tells Alice the time slits of photons he received and the basis he chose.

Thirdly, Alice tells Bob the correct bases he chose, the others will be discarded. Alice and Bob compare these symbols of raw keys to obtain a sifted key. Afterward, Bob could use the sifted keys to decode the information and implement error correct and privacy amplification to get the final secret keys.

If Alice and Bob use the same basis but the different polarization to measure a photon, the error of sifted key would be generated, which increases the bit error rate and decrease the number of final secret keys. If the bit error rate is higher than 11%, all of these keys should be abandoned.

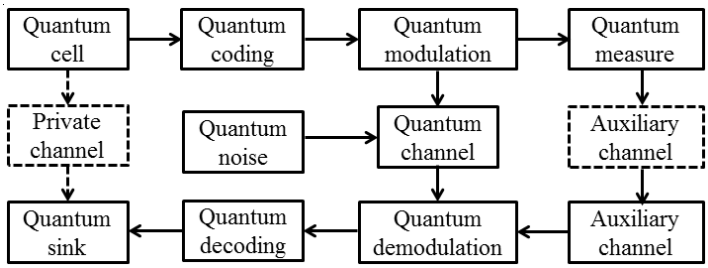

Fig. 1 quantum secret communication system

The Set-up Design of the BB84 Protocol

The QKD set-up, as illustrated in figure 2, is based on the BB84 protocol. Alice's main electric circuits include random data module, laser source drive module, error correcting module, extracting original key, error rate estimation, and receiver/transmitter interface module. The random data module provides the random bit numbers by a VHDL random generator before the start of communication and stores them in a local memory. Once quantum communication starts, the laser source drive module reads the random data and controls the four LDs to send polarized photons based on the bit value (1 or 0) of random strings. Here, the photon polarization encoding method is used and the four LDs stand for 4 different polarization states "Horizontal", "Vertical", "+45°" and "- 45°". Bob's main electric circuits include measure module, QKD control module and receiver/ transmitter interface module. The receiver/ transmitter interface module used to communication over classical channel.

The control circuit of the actual set-up is implemented by FPGA with VHDL programming language based on the Vortex - 5 platforms.

Firstly Alice tells Bob to begin the communication. As the first stage of the process of quantum communication begins, the random sequence is generated by random data module, and every bit of polarization encoding is completed. Laser source drive signal is generated, and is used to control the laser sources, so that the transmitting of the single photon polarization is implemented. After the polarized light is send Bob over a quantum channel. On the Bob's site, Bob receives photons, converts from photon signal to electric signal, and measures with the chosen basis, and sends to Alice.

At the second stage, when Bob send data back to Alice over the classical feedback channel, at Alice's site, extracting original key module gets raw key, and error rate estimation module calculates the error between raw key and original key, and completes key comparison.

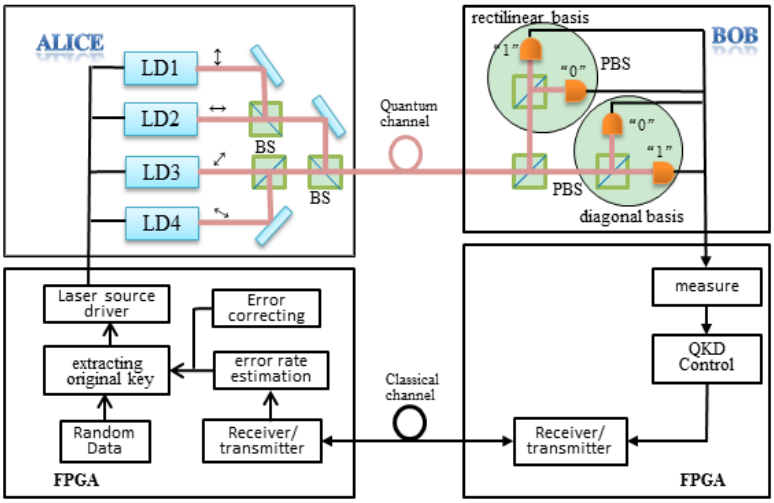

Fig. 2 experimental model of the system

The Implementation of The Module Implementation

According to the steps of BB84 protocol and the scheme in figure 2, the top-level module design scheme is based on the asynchronous Moore state machine. The top-level module state transition diagram is shown as figure 3. There are eight states for the state machine: Idle (Idle state), Encode (polarization encoding), Q_trans (polarization send), P_rec1 (receiving Bob measurement), Compare (measurement basis comparison), P_trans (compared result send), P_rec2 (calibration sequence receive), and Misestimate (error estimate). When the reset signal is effective, the system is reseted. The state machine has been waiting until the rising edge arrival of start signal, and then the state machine is transferred to Encode state, and so on; the BB84 protocol process begins to work.

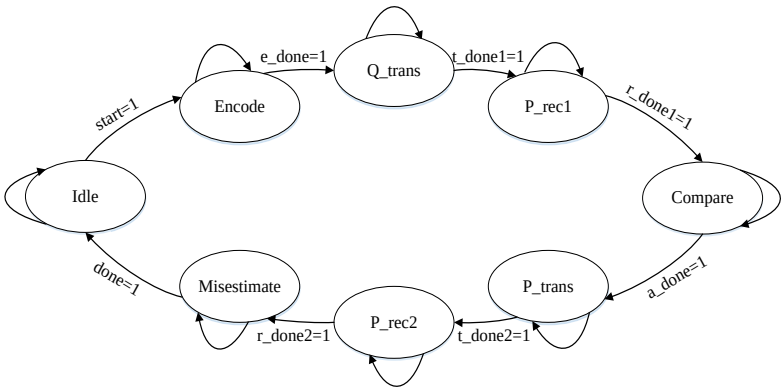

Fig. 3 Top-level module state machine

In the process of Quantum key distribution, the critical factor of polarization encoding lies in the random choice of the sending basis, and Alice needs to convert the initial key generated in random into corresponding photon polarization. In this scheme, two RAM regions (RAM0 and RAM1) are used to complete this function. RAM0 is used to code 0, and RAM1 is used to code 1. RAM is implemented by calling IP core in the design.

The simulation diagram of original key extraction module is illustrated in the figure 4. In figure 4, alice_alphabet denotes sending base sequence; bob_alphabet denotes measure base sequence. Two sequences are compared bit by bit. When Comparison results are consistent with the bits in the ini_key, the bit are sifted and stored in registers orig_key. Finally, Alice and Bob get the original key 00110100, and num denotes that the number of the raw keys is eight.

In original key extraction module, Alice compares the base sequences in same time slice sent back by Bob. The basis consistent with initial key is chosen as an original key, and the comparison results tell Bob. The logic design is shown as below:

if Alice_alphabet(i) = Bob_alphabet(i) then

```
        addr <= conv_std_logic_vector (i,4);
    orig_key(n) <= ini_key(i);
        n := n + 1;
        i := i+1;
        end if;
```

After completing the comparison of the measurement basis, Alice needed to estimate error. The diagram of the partial simulation result is shown in figure 5.

Summary

In this paper the FPGA logic design based on BB84 protocol is principally introduced. The logic design mainly includes the overall design, the top-level module design, and sub-module design. In the sub-module design, the partial simulation results are given to verify the correctness of the design function. The set-up advantage is the small size, high bitrates, and flexible configuration.

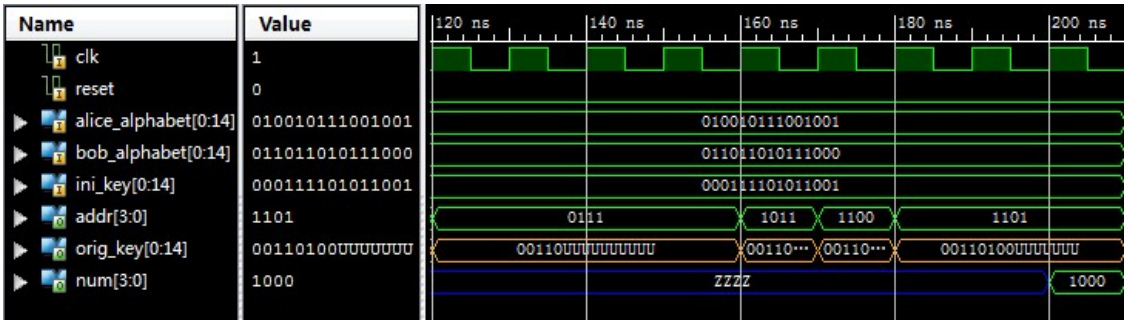

Fig. 4 The simulation diagram of original key extraction module

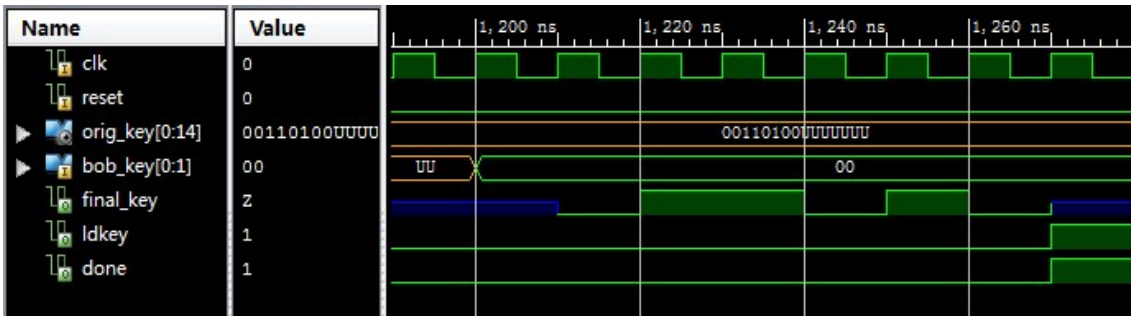

Fig. 5 the simulation diagram of error estimation module

Reference

[1] C. Bennett and G. Brassard: in Proceedings of the IEEE ICCSSP, 1984, p. 175.

[2] Wang C Z, Guo H, Ren J G: Sci China-Phys Mech Astron, Vol. 57(2014), p.1233.

[3] Zhang C X, Guo B H, Cheng G M: Sci China-Phys Mech Astron, Vol. 57(2014), p.2043.

[4] Wallden, P., Dunjko, V., Kent, A: Phys. Rev. A, Vol. 91 (2015), p. 34.

[5] Amor Gueddana, Moez Attia, Rihab Chatta:Proc. of SPIE, Vol. 9136(2014),

doi: 10.1117/ 12.2048809.