Gigahertz Clocked Quantum Key Distribution System using FPGA

Toshimori Honjo

NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan, honjo@will.brl.ntt.co.jp

Abstract *An implementation of 1-GHz clocked differential-phase-shift quantum key distribution system is reported. High speed signal generation and its storage were realized by using FPGA. A stable operation was demonstrated for over a 1-hour.*

Introduction

Quantum key distribution (QKD) has been widely investigated to realize unconditional secure communication [1]. Up to now, many preliminary QKD experiments have been successfully demonstrated, and then many groups started to implement a whole QKD system. Especially, several QKD systems were demonstrated within SECOQC project [2].

My group also has been working on QKD. We proposed a new QKD scheme called Differential phase shift QKD (DPS-QKD) [3]. One of the attractive features of this scheme is the possibility to realize a high repetition frequency due to its simple setup and one-way transmission. 1-10GHz clock preliminary experiments were successfully demonstrated [4-6]. In order to show the possibility to realize a whole DPS-QKD system, we started to implement the prototype.

In this paper, I report an implementation of one gigahertz clocked DPS-QKD system. A Field Programmable Gate Array (FPGA) board was used to realize high speed signal generation and its storage.

Differential-phase-shift QKD (DPS-QKD)

First of all, I briefly explain our QKD scheme. Differential-phase-shift QKD (DPS-QKD) is a new quantum key distribution scheme that was proposed by K. Inoue et al. [3]. Figure 1 shows the setup of the DPS-QKD scheme. Alice randomly phase-modulates a pulse train of weak coherent states by $\{0, \pi\}$ for each pulse and sends it to Bob with an average photon number of less than one per pulse. Bob measures the phase difference between two sequential pulses using a 1-bit delay Mach-Zehnder interferometer and photon detectors, and records the photon arrival time and which detector clicked. After transmission of the optical pulse train, Bob tells Alice the time instances at which a photon was counted. From this time information and her modulation data, Alice knows which detector clicked at Bob's site. Under an agreement that a click by detector 1 denotes "0" and a click by detector 2 denotes "1", for example, Alice and Bob obtain an identical bit string.

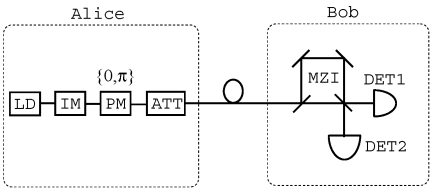

Fig. 1. Schematic diagram of differential-phase-shift QKD.

High speed signal generation and its storage

When we implement high speed QKD system, high speed signal generation and its storage are crucial issues. High speed signal is indispensible to encode bit information onto the optical pulse. Furthermore, the bit information must be kept until the basis information is disclosed by the receiver.

To overcome these problems, we implement high speed signal generator and its storage by using FPGA. I used Xilinx Virtex-5 Evaluation plathome (Tokyo Electron Device TB-5V-LX50T), which has 4 high speed serial interfaces (RocketIO, up to 3.2Gbps), DDR2 memory interface and gigabit ethernet interface. Figure 2 shows the diagram. The signal generation part captures random bit signal by way of the high speed serial interface part (or generates pseduo random bit signal), and then sends it to high speed serial interface part and memory interface part simultaniously. The high speed serial interface part outputs the random NRZ signal, and the other syncronized clocks. The memory interface part saved the random bit signal to the 512MB DRAM in a FIFO manner. The random bit can be stored for ~4 seconds in a 1-GHz clock system. The gigabit ethernet interface is used to access to the memory to retirive the random bit information.

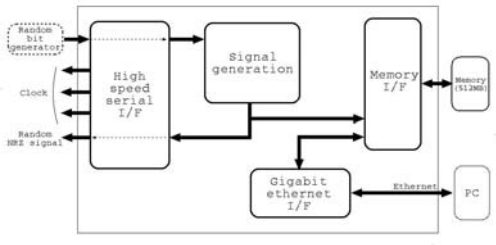

Fig. 2. Block diagram

Experimental setup

I implemented a 1-GHz clocked DPS-QKD system using the above FPGA board. Figure 3 shows the experimental setup. A 1-Gbps physical random bit generator with chaotic semiconductor lasers was used in this experiment [7,8]. 1-GHz master clock signal from the synthesizer was converted into 3 different synchronized clocks (1GHz, 100MHz, 10MHz) by a clock divider (National Semiconductor LMK01000). The 1-GHz clock was for a pulse generator, the 100-MHz clock was for the FPGA board and the 10-MHz clock was for the receiver's site. A quantum channel was organized as follows. A 1551-nm continuous light from an external cavity

978-3-8007-3173-2

semiconductor laser was modulated into a pulse stream with a 1-GHz clock frequency using a *LiNbO*3 intensity modulator. The intensity modulator was driven by the pulse generator (Picosecond Pulse Labs 3600) synchronized with the 1-GHz clock. The pulse width was 70 ps. Each pulse was randomly phase-modulated by $\{0, \pi\}$ with a *LiNbO*3 phase modulator which was driven by the random bit signal from the FPGA board. The optical pulse was attenuated to 0.2 photons per pulse and then transmitted to Bob's site over 25-km dispersion shifted fiber (DSF). The excess loss of the DSF was 5.7 dB.

The 100-kHz start signal, which indicated the head of a 10-kbit block of random bits in the sequence, was also generated by the FPGA board, and converted into an optical start pulse by a distributed feedback laser with an electro-absorption modulator (EA-DFB). The wavelength of the start pulse was 1547 nm. The 10-MHz clock signal from the clock divider was also converted into an optical clock pulse by a distributed feedback laser with an EA-DFB. The wavelength of the 10-MHz clock pulse was 1555 nm. These signals were combined with a WDM (Wavelength Division Multiplexing) coupler, and transmitted over the other 25-km DSF.

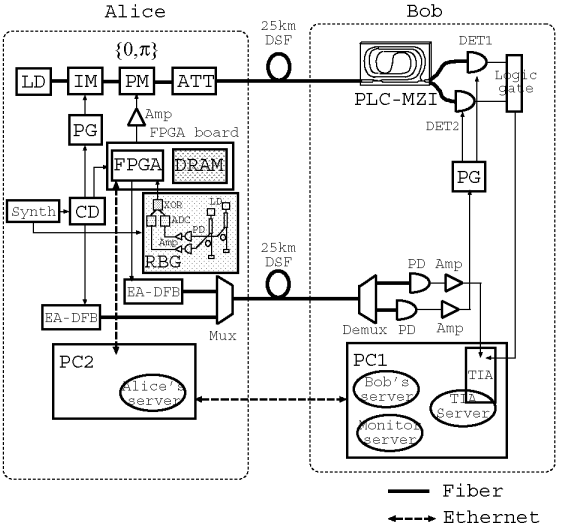

Fig. 3. Experimental setup.

After the transmission, the 1-GHz pulse stream was input into a Mach-Zehnder interferometer based on planar lightwave circuit technology [4]. The path length difference and the excess loss were 20 cm and 2.0 dB, respectively. The output ports of the Mach-Zehnder interferometer were connected to single photon detectors based on InGaAs APDs (Id-quantique id200). The detectors were operated in a gate mode, and the gate frequency was 4 MHz. The 4-MHz trigger signal for the detectors was generated from the 10-MHz optical clock pulses received by a photo diode (PD). The quantum efficiency and dark count rate were 7.5% and 189 cps, respectively. The detected signals were input into a time interval analyzer (TIA) (Fastcomtec P7889) by way of a logic gate to record the photon detection events. The start pulses were received by a PD and converted into an electrical signal, which was used as a reference time in the TIA. The TIA device was installed in a personal computer (PC2). The TIA server, Bob's server and monitor server were installed on PC2. The TIA server continuously retrieved the detection events from the TIA device, and sent them to Bob's server. Bob's server was driven by a detection event packet sent from the TIA server. From these packets, Bob's server generated his sifted key and sent the time information to Alice's server, installed on PC1, through the Ethernet. Bob's server also sent his key to the monitor server. On the other hand, Alice's server generated her key from the phase modulation information and the time information received from Bob's server. Alice's server could access to the DRAM on the FPGA board through the gigabit ethernet interface to retrieve the phase modulation information. Her key was sent to the monitor server. The monitor server received the keys from Alice's and Bob's servers, and estimated the key generation and quantum bit error rates.

Experimental results

Using the setup described above, we performed DPS-QKD experiment. Figure 4 shows the sifted key generation rate and quantum bit error rate as a function of time. We successfully demonstrated the continuous operation over an hour and generated sifted keys at a rate of 9.0 kbps with an average QBER of 3.2%.

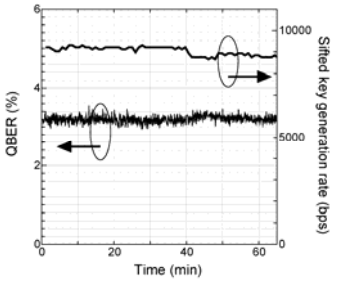

Fig. 4. Experimental results.

Summary

I reported an implementation of one gigahertz clocked DPS-QKD system. High speed signal generation and its storage were realized by using FPGA board. I showed the possibility to realize the high speed QKD system by using FPGA.

This work was supported in part by the National Institute of Information and Communications Technology (NICT) of Japan.

References

1 N. Gisin et al., Rev. Mod. Phys. **74**,145-195 (2002).
2 SECOQC http://www.secoqc.net/
3 K. Inoue et al., Phys. Rev. A **68**,022317 (2003)..
4 T. Honjo et al., Opt. Lett. **29**, 2797 (2004).
5 E. Diamanti et al., Opt. Express **14** 13073 (2006).
6 H. Takesue et al., Nature Photonics **1**, 343 (2007).
7 A. Uchida et al., Nature Photonics **2**, 728 (2008).
8 A. Uchida et al., CLEO/Europe-EQEC CB.P1 (2009).