Megabits secure key rate quantum key distribution

Qiang Zhang¹,², Hiroki Takesue³, Toshimori Honjo³, Kai Wen¹, Toru Hirohata⁴, Motohiro Suyama⁵, Yoshihiro Takiguchi⁴, Hideohiko Kamada⁴, Yasuhiro Tokura³, Osamu Tadanaga³, Yoshihi Yamamoto¹,²

¹ Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA
² National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan
³ NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan
⁴ Central Research Laboratory, Hamamatsu Photonics K.K.
⁵ Electron Tube Division, Hamamatsu Photonics K.K.

*Email: qiangzh@stanford.edu

Abstract: Imperfect practical conditions limit communication speed of Quantum cryptography. Here we implement differential phase shift quantum key distribution with up-conversion assisted hybrid photon detector to achieve 1.3M bits/s secure key rate over a 10-km fiber.

© 2009 Optical Society of America

OCIS codes: (270.5568) Quantum cryptography; (190.7220) Upconversion

In the differential phase shift (DPS) quantum key distribution (QKD) protocol [1], the sender first encodes one photon into a sequential pulse train, randomly sets the relative phase of each pulse in the train as 0 or π, and then sends it to the receiver through a fiber link. The receiver uses a 1-bit delay Mach-Zehnder interferometer (MZI) to make the sequential pulses interfere. Each output of the MZI is connected to a single photon detector, respectively. The relative phase of the sequential pulses decides which detector will receive the photon. When one of the detectors fires, the receiver can conclude whether the phase is 0 or π according to the which-detector information. The receiver records the phase result and the time instance information when he detects a photon. Later the receiver reports the time instance information, from which the sender can tell the value of the relative phase. Therefore the sender and receiver can share the random phase as the quantum key. This protocol is simple but tolerant against all individual attack including the photon number splitting (PNS) attack [2].

Here we utilize periodically poled Lithium Niobate (PPLN) waveguide based up-conversion hybrid photon detectors in the experiment [3]. We mix the signal photon with strong pumping light at 980 nm in a wavelength division multiplexing (WDM) coupler and send them to a fiber pigtailed PPLN waveguide for sum frequency generation (SFG) [3]. This device can convert the 1550 nm signal to a 600 nm sum frequency output with an internal conversion efficiency of 99%, detected by a hybrid photon detector (HPD). The HPD incorporates an avalanche diode (AD) into a vacuum tube to receive and amplify the photoelectron from its cathode [4]. In our case, the photon is first injected into the GaAsP cathode (3mm effective diameter) to generate a photoelectron. The photoelectron is then accelerated by –8,500 V bias and focused onto the 1mm AD, which is 400 V biased. Then, the electron deposits its kinetic energy in the AD and produces thousands of electron hole pairs, which is called an electron bombarded gain. The generated electrons drift in the AD, and are further multiplied by ten to one hundred times by impact ionization. The up-conversion detector’s overall quantum efficiency and noise could be controlled by adjusting the pumping laser of the up-conversion detector. The timing jitter (full width of half maximum) of the HPD at Megahertz count rates is still less than 200 ps. To achieve a Megabits per second secure key rate over 10 km fiber, we set the quantum efficiencies of the detectors at 4% and the noise count rates at 30 kHz with 120 mW pump power. We chose a time window of 280 ps and the noise count rate per window was 8.4×10⁶.
The experimental setup is shown in Figure 1. A CW laser was first modulated into a 2 GHz pulse train by a LiNbO3 intensity modulator (IM), with a pulse duration of 70-ps full width at half maximum (FWHM) of a central wavelength of 1550 nm. A 3 GHz pulse pattern generator drove a pseudo random number sequence into a phase modulator to encode the pulse train. We attenuated the encoded pulse train by around 80 dB and set the average photon number per pulse as 0.2. Then we sent the encoded, attenuated pulse to the receiver through a 10-km dispersion shifted fiber (DSF). The receiver used a 1 GHz, 1-bit delay MZI to make the sequential pulses interfere. Each output of the MZI is directly connected to an up-conversion assisted HPD, respectively. The output signals of the up-conversion HPDs were sent to a time interval analyser (TIA) to record the detection time instances and which-detector information. This information was used to generate the sifted key.

In the experiment, sifted keys were actually generated between the sender and receiver, and the error rate was measured by directly comparing the sender’s key with the receiver’s. For each data point described below, we undertook five QKD runs, and the secure key rates were achieved with the experimental results for the sifted key generation rates and bit error rates [2]. The sender and receiver were located in the same room. We performed the 10-km fiber transmission experiment using fiber spools, while other data points were taken with an optical attenuator simulating fiber loss.

![Figure 2 Theoretical curves and experimental results for the secure key generation rate as a function of fibre length.](a514_1.pdf)

We have demonstrated a quantum cryptography system with megabits per second secure key rate over 10 km fiber link, which was tolerant to all individual attacks including the PNS attack and all known sequential attacks [5,6]. We believe it will be operable in a standard telecommunication network soon. The transmission distance could be extended by reducing the noise counts caused by the parasitic nonlinear process by using an 1810 nm pump. A higher bit rate could be achieved by either develop a special cathode for the 600 nm SFG wavelength or reduce the cathode thickness to improve the timing jitter.

Q.Z. thanks C. Langrock for his useful discussion during this research. Financial support was provided by the the National Institute of Information and Communications Technology (NICT) of Japan, CREST and SORST programs of the Japan Science and Technology Agency (JST), Hamamatsu Photonics.

[1] K. Inoue, E. Waks, and Y. Yamamoto, “Differential-phase-shift quantum key distribution.” Phys. Rev. Lett. 89, 037902 (2002).
[2] E. Waks, H. Takesue, and Y. Yamamoto, “Security of differential-phase-shift quantum key distribution against individual attacks.” Phys. Rev. A 73, 012344 (2006).
[3] M. Asobe, H. Miyazawa, O. Tadanaga, Y. Nishida and H. Suzuki, “Wavelength Conversion Using Quasi-Phase Matched LiNbO3 Waveguides.” the Optical Electronics and Communications Conference, Yokohama, Japan, July 8-12 2002, paper PD2-8.
[4] K. Fukasawa, J. Haba, A. Kageyama, H. Nakazawa, and M. Suyama, “High Speed HPD for Photon Counting.” IEEE Trans. Nucl. Sci. 55, 758 (2008).
[5] M. Curty, L. Zhang, H.-K. Lo, N. Lütkenhaus, “Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states.” QIC, 7, 665 (2007).
[6] T. Tsurumaru, “Sequential Attack with Intensity Modulation on the Differential-Phase-Shift Quantum Key Distribution Protocol.” Phys. Rev. A 75, 062319 (2007).