Field trial of differential-phase-shift QKD
using polarization independent freqeuncy up-conversion detectors

T. Honjo (1), H. Takesue(1), H. Kamada (1), K. Tamaki (1), H. Shibata (1), K. Shimizu (1), Y. Tokura (1),
S. Yamamoto (2), T. Yamamoto (2), Y. Nishida (3), O. Tadanaga (3), M. Asobe (3), and K. Inoue (1,4,5)
1: NTT Basic Research Laboratories, NTT Corporation,
3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan, honjo@will.brl.ntt.co.jp
2: *NTT Network Innovation Laboratories, NTT Corporation,* 3: *NTT Photonics Laboratories, NTT Corporation*
4: Osaka University

Abstract

We report a field trial of differential phase shift quantum key distribution (DPS-QKD) using polarization independent frequency up-conversion detectors (UCDs). A UCD is a promising device for achieving a high key generation rate when combined with a high clock rate QKD system. However, its polarization dependence prevents it from being applied to practical QKD systems. Applying a modified polarization diversity configuration, we performed a field experiment over a 17.6-km installed fiber. We successfully demonstrated stable operation for 6 hours and achieved a sifted key generation rate of 120 kbps and an average quantum bit error rate of 3.14 %.

Introduction

Many fiber-based QKD experiments have been performed both inside the laboratory and in the field, and the feasibility of QKD has been demonstrated. Our team has been investigating a differential phase-shift QKD (DPS-QKD) system, which has suitability for fiber transmission and high clock rate [1]. Up to now we have applied several types of single photon detectors, such as InGaAs avalanche photodiodes (APDs), frequency up-conversion detectors (UCDs), sinusoidally gated InGaAs/InP APDs, and superconducting single-photon detectors (SSPDs) to our DPS-QKD system. Then, we achieved 100-km secure key distribution with UCDs [2], and 200-km secure key distribution with SSPDs [3]. To go a step further, we tried a field experiment. In this paper we report a DPS-QKD field experiment with polarization independent frequency up-conversion detectors.

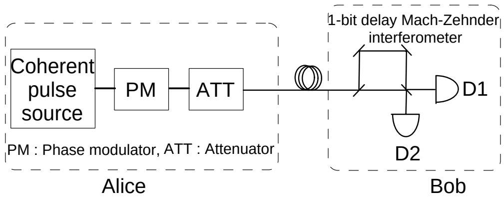

Figure 1: Diagram of DPS-QKD.

Differential-phase-shift QKD

Figure 1 shows a diagram of a DPS-QKD system. Alice randomly modulates the phase of a weak coherent pulse train 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 of each consecutive pulse with a 1-bit delay Mach-Zehnder interferometer followed by two detectors placed at the interferometer output ports. Detector 1 (D1) clicks when the phase difference is 0 and detector 2 (D2) clicks when the phase difference is π. Because the average photon number per pulse is less than one, Bob observes clicks only occasionally and at random time instances. Bob informs Alice of the time instances at which he observed clicks. From her modulation data, Alice knows which detector clicked at Bob's site. By designating D1 and D2 clicks as 0 and 1, respectively, they can share an identical bit string.

Polarization independent frequency up-conversion single photon detector

In a UCD, 1.5-μm photon is converted into short wave length photon and detected by high speed Si-APD. Since a UCD can be operated in a non-gated mode, thanks to the low afterpulse probability of the Si-APD, a high key generation rate will be achieved when they are combined with a high clock rate QKD system. However, the efficiency of a nonlinear process in a periodically poled lithium niobate (PPLN) waveguide utilized for frequency conversion is polarization dependent so the polarization of a single incoming photon must be adjusted for proper operation. This polarization dependence prevents it from being applied to practical QKD systems. To overcome this drawback, we applied a modified polarization diversity configuration.

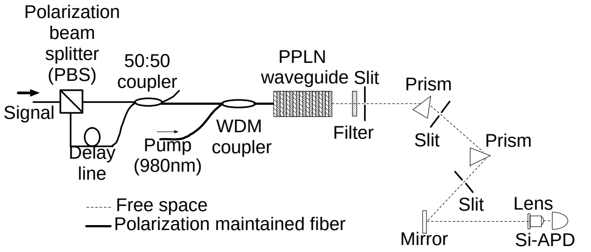

Figure 2: Setup of polarization independent frequency up-conversion detector.

Figure 2 shows the setup. A 1.5-μm signal pulse (photon) was input into a fiber-coupled polarization beam splitter (PBS), which split the polarization of the incoming photon into horizontally and vertically polarized pulses. All the components after the PBS, described below, were connected with polarization maintaining fibers. The horizontally polarized pulse was directly input into a polarization maintaining 50:50 coupler. The vertically polarized pulse was input into a fiber delay line as a horizontally polarized pulse by twisting the axis at the connection between the PBS output fiber and the delay fiber. The pulse passed through the delay line, and was input into the polarization maintaining 50:50 coupler. The delay line was used to avoid interference at the 50:50 coupler. Since the pulse width in our experiment was 66 ps, we chose a delay time of 200 ps. One output of the

50:50 coupler was connected to a wavelength division multiplexer (WDM) coupler, which meant this setup had an intrinsic loss of 3 dB. The 1.5-µm signal pulse output from the 50:50 coupler was combined with a strong pump light whose wavelength was 980 nm at a wavelength division multiplexer (WDM) coupler, and injected into a PPLN waveguide. In the PPLN waveguide, a 600 nm photon was generated via the sum frequency generation (SFG) process. The converted signal, pump, and spurious light after the PPLN waveguide were separated by using a combination consisting of a short-pass filter, prisms and a spatial filter. The SFG photon was detected with a single photon counting module (SPCM) based on a Si-APD (MPD). The jitter of this Si-APD was low enough to discriminate a 1-GHz signal [2]. When the input pomp power was 20 mW, the quantum efficiency and dark count rate were 0.66 % and 2.8 kcps, respectively.

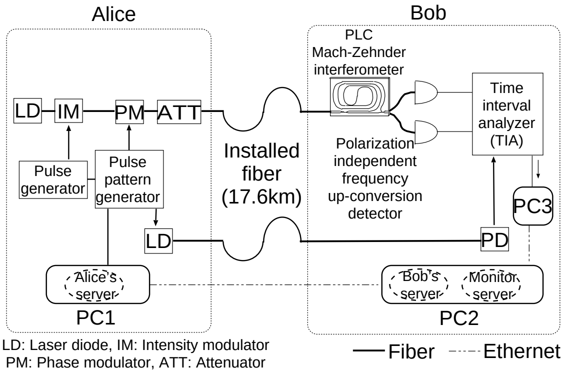

Figure 3: Experimental setup.

Field trial of DPS-QKD

Using the above polarization independent frequency up-conversion detectors, we performed a DPS-QKD experiment over installed fibers. In this experiment, we used two round-trip dispersion shifted fibers installed between our research center and an NTT (Nippon Telegraph Telephone corporation) telephone exchange office. The total length of these fibers was 17.6km. Figure 3 shows the experimental setup. At Alice's site a continuous light from an external cavity semiconductor laser was modulated into a pulse stream with a 1-GHz clock frequency using a $LiNbO_3$ intensity modulator. The pulse width was 66 ps. Each pulse was randomly phase-modulated by 0, π with a $LiNbO_3$ phase modulator. We used a pseudo-random bit sequence with a length of 11 k bits as the phase modulation signal. The pulse was attenuated to 0.2 photons per pulse and then transmitted to Bob's site over the installed fiber. The start pulse, which indicated the head of a pseudo-random bit sequence, was generated by a distributed feedback laser with an electroabsorption modulator (EA-DFB), and transmitted over the other installed fiber. The interval of the start pulse was 11 usec. The excess losses of these installed fibers were 7.0 and 7.2 dB, respectively. After the transmission, the 1-GHz pulse stream was input into a planar lightwave circuit Mach-Zehnder interferometer (PLC-MZI). The path length difference and the excess loss were 20 cm and 2.0 dB, respectively. The extinction ratio was greater than 20 dB and the polarization dependence was negligible [4]. The phase difference between the two paths in the Mach-Zehnder interferometer could be stably adjusted by controlling the temperature of the waveguide chip. In this experiment, no feed-back mechanism that adjusted the the temperature of the Mach-Zehnder interferometer depending on the fluctuation of the center frequency of the laser source was implemented. The output ports of the Mach-Zehnder interferometer were connected to the polarization independent up-conversion detectors. The detected signals were input into a time interval analyzer (TIA) by way of a logic gate to record the photon detection events. A personal computer (PC3) continuously retrieved the detection events from the TIA, and transmitted them to another computer (PC2). Following the DPS-QKD protocol, Alice's server on PC1 and Bob's server on PC2 generated the sifted key. The monitor server received the keys from Alice's and Bob's servers, and estimated the key generation and quantum bit error rates.

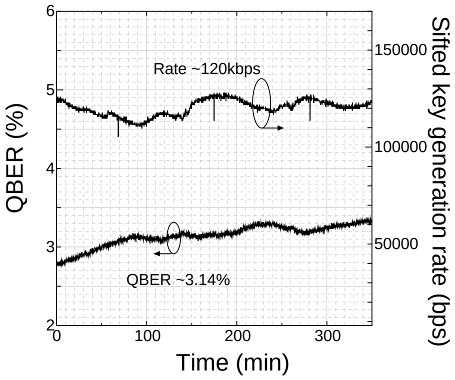

Figure 4: Experimental results.

Figure 4 shows the experimental results, which reveal that stable operation was obtained over 6 hours. We achieved a sifted key generation rate of 120 kbps and an average quantum bit error rate of 3.14 %. Note that the sifted key generation rate is not an estimated value but an actually obtained value including classical communications and other data processing, which means the sifted key was continuously generated at a rate of 120 kbps at Alice's and Bob's servers.

Summary

A field trial of DPS-QKD using polarization independent frequency up-conversion detectors was reported. We successfully demonstrated stable operation for 6 hours over a 17.6-km installed fiber, which showed the feasibility for applying UCDs to practical QKD system.

Acknowledgement

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

References

1. K. Inoue et al Phys. Rev. A **68**, 022317 (2003).
2. E. Diamanti et al Opt. Express 14, 13073 (2006).
3. H. Takesue et al Nature Photonics 1, 343 (2007).
4. T. Honjo et al Opt. Lett., 29, 2797 (2004).