Fiber-optic quantum key distribution at 1550 nm

Naoto Namekata and Shuichiro Inoue
Institute of Quantum Science, Nihon University
1-8 Kanda-Surugadai, Chiyoda-ku, Tokyo 101-8308, Japan
Tel./Fax. 03-3259-0918
nnao@phys.cst.nihon-u.ac.jp

Quantum key distribution (QKD) invented by Bennett and Brassard in 1984 is a technique for sharing an assuredly secret, cryptographic key over unsecured optical links [1]. In QKD, information is encoded in the quantum state of individual photons and security is guaranteed by photons' fundamental quantum properties. Since the first demonstration of QKD over 40 cm in 1992, QKD has been extensively tested over distances of a few tens of kilometers in optical fibers at a wavelength of 1300 nm. However, for a quantum cryptographic system to be suitable for practical use, it should be compatible with the standard telecommunications network at a wavelength of 1550 nm. The 1550-nm wavelength is clearly superior to 1300 nm in long-distance fiber-optic QKD, because the fiber losses for 1550 nm are 0.2 dB/km compared with 0.35 dB/km for 1300 nm.

In this paper, we report on the fiber-optic QKD based on BB84 protocol at 1550 nm in which InGaAs/InP avalanche photodiodes (APDs) are used for single-photon detection.

A schematic of our cryptosystem is shown in Fig.1. The system is composed of a polarization splitting time-multiplexed interferometer [2, 3] and single-photon detectors at 1550 nm [4-8]. Bob and Alice are separated by a 10.5-km link of standard telecom single-mode optical fiber (SMF). At Bob's station, a 1550 nm DFB laser, pulsed at a repetition rate of 9 kHz, sends 50-ps pulses to the polarization maintaining fiber (PMF) connected to the input port of a circulator. The polarization of the optical pulses is oriented along the slow axis of the PMF. The slow axis of the PMF from the output port of the circulator is rotated by 45 degrees and connected to the input port of the first polarizing beamsplitter (PBS1). Then the pulses are again horizontally polarized as they pass through PBS1. The slow axis of the PMF from the output port of PBS1 is rotated by 45 degrees and connected to the input port of the second polarizing beamsplitter (PBS2). Then PBS2 evenly divides the pulse into orthogonal components P1 and P2. P1 passes straight through PBS2 and onto the 10.5-km link, while P2 is sent through a polarization maintaining fiber loop, which delays it by 70 ns before it returns to PBS2 and is sent onto the link.

They are reflected by a Faraday mirror (FM) and arrive simultaneously at PBS2 and recombine into a single pulse P0 with a polarization state that depends only on the difference of the applied phase shift, $\Delta\phi = \phi_A - \phi_B$. The polarization of P0 is oriented along the fast axis of the PMF when the phase difference $\Delta\phi = 0$. Then P0 is reflected by PBS1 and detected by the single-photon

detector D2. On the other hand, the polarization of P0 is oriented along the slow axis of the PMF when $\Delta\phi = \pi$. Then P0 passes through PBS1 and detected by the single-photon detector D1.

Our single photon detectors are Epitaxx APDs (EPM239BA) operated in gated mode at –55 degrees Celsius [8]. Each gate pulse has an amplitude of 4 V and a full width at a half- maximum of 1 ns. The excess bias voltage was set to be 3 V. Table I summarizes the performance of D1 and D2 in our cryptosystem. The interference fringes at D1 and D2 of our time-multiplexed interferometer are shown in the inset of Fig.1. Here the average photon number per pulse was 2 and Alice's modulator voltage was changed. The fringe visibilities are 0.998 at D1 and 0.999 at D2. The optical losses at Bob's station are ~4 dB to D1 and ~5 dB to D2. The key generation rate was 7.4 bps and the corresponding quantum bit-error rate was 0.24 % when the BB84 protocol was performed by randomly changing ϕ_A and ϕ_B. Here the average photon number per pulse was 0.1.

In conclusion, we have demonstrated quantum key distribution based on BB84 protocol at 1550 nm with a quantum bit error rate of 0.24 % for a 10.5-km single-mode fiber link. The use of a polarization maintaining fiber enabled us not only to realize a high visibility without polarization control but also to reduce the optical losses in a receiver's station compared with the other schemes.

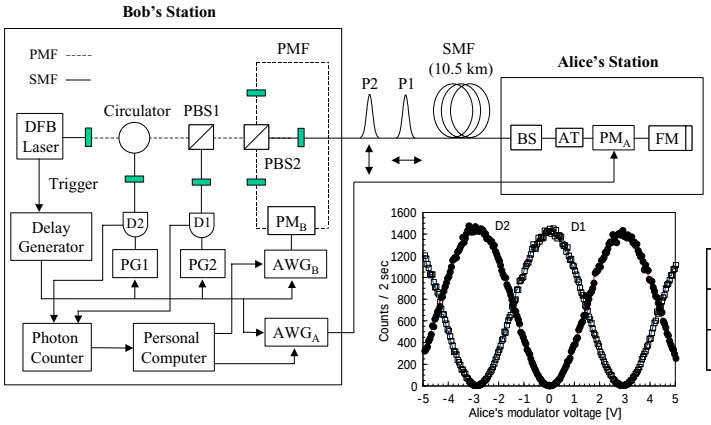

Table I Performance of D1 and D2

	D1	D2
Quantum Efficiency (%)	16.2	18.2
Dark-count probability	2.2×10^{-6}	1.2×10^{-5}

Fig.1 Schematic diagram of our cryptosystem: PBS1, PBS2 Polarizing Beamsplitters; SMF Single-mode Fiber; PMF Polarization Maintaining Fiber; BS 50/50 Beamsplitter; AT Attenuator; PM_A, PM_B Phase Modulators; FM Faraday Mirror; D1, D2 Single-photon Detectors; PG1, PG2 Pulse Generators; AWG_A, AWG_B; Arbitrary Waveform Generators. The inset shows the interference fringes at D1 and D2 when Alice's modulator voltage is changed.

References

[1] C. H. Bennet and G. Brassard, Proc. Int. Conf. Computer Systems and Signal Processing, Bahgalore, 175 (1984). [2] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett., **34**, 2116 (1998). [3] D. Bethune and W. Risk, IEEE J. Quantum Electron., **36**, 340 (2000). [4] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tegaye, D. Ljunggren, and E. Sundberg, Opt. Express, **4**, 383 (1999). [5] A. Yoshizawa and H. Tuchida, Jpn. J. Appl. Phys. Pt. 1, **40**, 200 (2001). [6] P. Hiskett, G. Bonfrate, G. Buller, and P. Townsend, J. Modern Opt., **48**, 1957 (2001). [7] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. G. Rarity, and T. Wall, J. Modern Opt., **48**, 1967 (2001). [8] N. Namekata, Y. Makino, and S. Inoue, Opt. Lett., 27, 954 (2002).