Fundamental Security Technologies

Recent Progress in Quantum Key Transmission

By Akihisa TOMITA*, Yoshihiro NAMBU* and Akio TAJIMA†

ABSTRACT Recent developments in Quantum Key Distribution (QKD) system are reviewed. A high sensitivity photon detector combining the two avalanche photon diodes (APD) has been demonstrated for qubit discrimination in 1,550nm. A stable interferometer on a planer light-wave circuit (PLC) has been developed. Single-photon interference over 150km has been achieved as a result of the above improvements. A temperature insensible QKD system is being developed for high speed (100kbps) key transmission over a 40km fiber.

KEYWORDS **Quantum cryptography, Photon detector, Interferometer**

1. INTRODUCTION

Quantum cryptography and quantum key distribution (QKD), in particular, is an important application of photonic quantum information technology. This is because it is the closest to achieving a practical (commercial) use. QKD allows two remote parties (Alice and Bob) to generate a secret key, with privacy guaranteed by quantum mechanics[1,2]. The secret key will provide perfect security when it is used in the one-time pad cryptosystem. The security will never be threatened by any progress in computer hardware/software. Even a quantum computer cannot break it. Although one-time-pad cryptosystem has been known for a long time, the lack of a secure key distribution method has prevented it from practical use. QKD offers perfect security in key distribution. Though QKD can be performed using current technology alone, there still remain many issues to be improved in order to satisfy the specification that would be necessary for the practical systems. The transmission distance and the transmission speed are two most important issues. Ever since the introduction of the BB84 protocol by Bennett and Brassard in 1984[1] and their first bench-top implementation of QKD over 30cm of free-space in 1992[2], extensive efforts by numerous groups[3-10] have been devoted to extending the QKD distance by using optical fibers. Then, over what distance should the QKD transmission cover? The further the better is the answer. However, the first customers would be government offices (military, foreign affairs, and so on), or finance (banks, stock traders, for example.) These organizations usually reside in the centers of cities. In most of the big cities the city center lies within a circle of about 10km radius. However, if we consider the use of a network, the fiber distance would reach several tens or a hundred km. Our first goal would be several tens (say, forty) km, then over a hundred. Practical use of QKD will also require fast key transmission, and/or key generation. The rate might be slower than current data transmission (Gbps), because the amount of valuable information that requires perfect security would be much smaller. Nevertheless, fast and secure random number (key) distribution will open up wide applications for QKD.

We here concentrate on the recent progress in single photon transmission for QKD. A problem in practical systems is that a trade-off exists between the transmission distance and the transmission rate, because photon loss in fibers decreases the photon arrival rate over a long distance transmission. Two directions may be explored: one is a slow but long distance transmission, the other is a short but high rate transmission. For both directions, one of the most important devices is the single photon detector (SPD). The SPD limits both the transmission distance and the transmission rate. We have developed a high performance SPD, combining the two avalanche photon diodes (APDs) that has been demonstrated for qubit discrimination at 1,550nm[11]. We have reduced dark count without sacrificing detection efficiency. We have demonstrated single photon transmission over a 100km fiber with the SPD[12]. We have also developed integrated-optic asymmetric

*Fundamental and Environmental Research Laboratories

†System Platforms Research Laboratories

Mach-Zehnder interferometers for time-bin and phase coding the QKD system[13,14]. We have achieved single-photon interference over 150km using integrated-optic interferometers and balanced gated-mode SPDs. The key transmission speed has also been improved with the new SPDs. We have also demonstrated a key transmission rate of 100kbps after 40km fiber transmission[15].

2. SINGLE PHOTON DETECTOR

2.1 Sensitivity of a Photon Detector

The key device for the optical implementation of quantum information technology is an SPD to determine the quantum state, or to discriminate qubits. The SPD should show a high detection efficiency, low dark count, and short response time. The ratio of the detection efficiency η to the dark count probability P_d determines the error rate e_B as,

$$e_B = \frac{1}{2}\frac{S(1-\nu)\eta + P_d}{P_{DET}} = \frac{1}{2}\frac{S(1-\nu) + P_d/\eta}{S(1-P_d) + P_d/\eta}, \qquad (1)$$

where ν is the visibility of the interferometer, and P_{DET} represents the detection probability per pulse. P_{DET} is related to the probability S that at least one photon arrives at the detector by

$$P_{DET} = S\eta + P_d - S\eta P_d. \qquad (2)$$

The probability S is a function of the loss in the transmission line and the receiver. The photon loss in a L km-long-fiber is given by αL[dB]. When we assume that the receiver loss is β[dB], S is given by

$$S = 10^{-(\alpha L+\beta)/10} \qquad (3)$$

for a single photon source, and

$$S = 1 - \exp[-\mu 10^{-(\alpha L+\beta)/10}] \qquad (4)$$

for a coherent photon source with the average photon number of μ. The error rate (1) is given by a half of the inverse of the signal-to-noise ratio S/N (Note that noise will give the error with a probability of 1/2.) Eq.(1) shows that the ratio P_d/η is a figure of merit of an SPD that determines the error probability, because P_d and 1-ν are small. The error rate should be kept lower than the threshold for secure QKD. The threshold varies according to the assumptions on the method of attack and error correction. A typical value is around 11%[16]. The ratio P_d/η should be smaller than 10^{-3} for 100km fiber transmission in 1,550nm even with an ideal single photon source.

2.2 Afterpulse Effect

Clock frequency is limited mainly by the afterpulse (false photon detections caused by residual electrons created by the previous detections.) We cannot send a photon pulse during a period of large afterpulse probability. The afterpulse effect remains typically until 1μs after the photon detection. This period may vary depending on the devices and the operating conditions. The afterpulse effect on error probability can be formulated as follows. We assume two detectors 1 and 2 to discriminate bit values 0 and 1, respectively. The probabilities $p_1(t_n)$ that detector 1 fires and that $p_2(t_n)$ detector 2 fires are given by the bit value $b(t_n)=\{0,1\}$ at time of the n-th clock t_n as

$$p_1(t_n) = S\eta q(t_n) + P_d + \sum_{i=-\infty}^{n-1} f(t_n - t_i)p_1(t_i)$$

$$p_2(t_n) = S\eta(1 - q(t_n)) + P_d + \sum_{i=-\infty}^{n-1} f(t_n - t_i)p_2(t_i) \qquad (5)$$

where the function

$$q(t_n) = \nu(1 - b(t_n)) + (1-\nu)b(t_n) \qquad (6)$$

defines the fraction that a photon enters the detector 1, and the memory function $f(t_n - t_1)$ represents the afterpulse effect. Here we assume

$$f(t) = \begin{cases} A & (0 \le t \le t_M) \\ 0 & (t < 0, t > t_M) \end{cases}, \qquad (7)$$

for simplicity. The afterpulse probability A remains constant during M periods of the clock in this model. Then Eq. (5) can be solved for the asymptotic values. The error probability is given by

$$\hat{e}_B = \frac{1-\nu+P_d/S\eta}{1+2P_d/S\eta} + \frac{\nu - 1/2}{1+2P_d/S\eta}AM \approx e_B + \frac{1}{2}AM, \qquad (8)$$

if we neglect the events that both detectors fire simultaneously. Eq. (8) shows that the afterpulse effect increases the error probability by $AM/2$. For example, $A=10^{-3}$ and $M=100$ result in a 5% increase in the error probability.

2.3 Spike Noise Suppression with Balanced Detector

The QKD experiments in 1,550nm have employed the SPDs using InGaAs/InP APDs in Gaiger mode, where a reverse bias higher than the break down voltage is applied. The high bias increases the avalanche gain to enable single photon detection. However, this also results in a large dark count probability and afterpulse, which cause errors in the qubit discrimination. The dark count probability and the afterpulse can be reduced by using gated-mode, where gate pulses combined with DC bias are applied to the APD. The reverse bias exceeds the break down voltage only in the short pulse duration. Though this method works well, the short pulses produce strong spikes on the transient signals. A high threshold in the discriminator is therefore necessary to avoid errors, which is at the cost of detection efficiency. A high gate pulse voltage is also required to obtain large signal amplitude by increasing the avalanche gain. Impedance matching helps to reduce the spikes to some extent[17]. Bethune and Risk have introduced a coaxial cable reflection line to cancel the spikes[18]. We propose the much simpler method of canceling the spikes by taking the balanced output of the two APDs required for the qubit discrimination[11].

Figure 1 is a schematic depiction of the SPD. Two APDs (Epitaxx EPM239BA) and load resisters were cooled to 140K - 213K by an electric refrigerator. Short gate pulses of 2.5Vp-p and 750ps duration were applied to the APDs after being combined with DC bias by Bias-Tees. The output signals from the APDs were subtracted by a 180° hybrid junction of 2 - 2,000MHz bandwidth. The differential signal was amplified and separated by two discriminators. Since the spikes were the common mode input for the 180° hybrid junction, they would not appear at the output. The APD 1 provided negative signal pulses at the output, while the APD 2 provided positive pulses. We can determine which APD detects a photon from the sign of the output signals. **Figure 2** shows the output signal of the amplifier without photon input. Almost identical I-V characteristics of the APDs enabled us to obtain a good suppression of the spikes. We observed the lowest dark count probability of 7×10^{-7} per pulse with detection efficiency of 11% at 178K. The ratio P_d/η was as small as 6×10^{-6}, which corresponds to 270km QKD transmission with an ideal photon source. The detection efficiency and the dark count probability are increasing functions of the bias. The maximum value of the detection efficiency is obtained when the DC bias is set to the breakdown voltage. We obtained larger values of the maximum detection efficiency at higher temperatures with a detection efficiency of 20% at 213K with a dark count probability of 3×10^{-5} per pulse.

Afterpulse probability was measured by applying two successive gate pulses to the APDs. Afterpulse is prominent at low temperatures. We found that afterpulse probability remained about 10^{-4} for the 1μs pulse interval at temperatures higher than 178K. This corresponds to an error probability of 10^{-5} (per pulse) for 10% detection efficiency. Based on the observation of the dark count probability and the afterpulse probability, we conclude that the optimal operation temperature for the present APDs is around 178K. The obtained afterpulse effect was shorter than for previous reports. We believe that this is due to the decrease in the gate pulse voltage. This is another advantage of our SPDs.

Recently we obtained a dark count probability of 2×10^{-7} per pulse at the detection efficiency of 10%. The S/N, or the ratio P_d/η is improved about 50 times (17dB) as much as the values previously reported from other organizations.

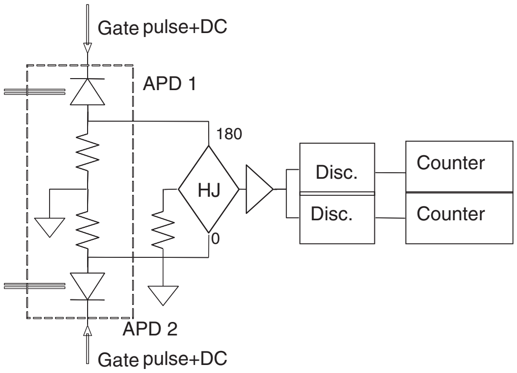

Fig. 1 A schematic diagram of the photon detector HJ and DISC stand for hybrid junction, and discriminators.

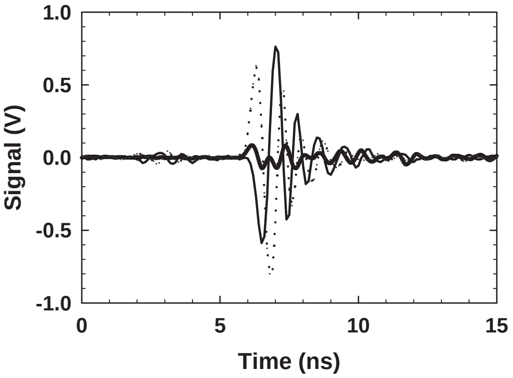

Fig. 2 Cancellation of the transient spike. Thin solid: APD 1, Dots: APD 2, Thick solid: the differential output of the APD 1 and the APD 2.

3. SINGLE PHOTON TRANSMISSION OVER 100KM

3.1 Plug and Play System

Recently, QKD systems on fibers employ phase coding, in order to avoid polarization rotation in the fiber. Time-division interferometers for optical pulses composed of either one or two asymmetric Mach-Zehnder interferometers (AMZs) have been used to code the random keys. A train of double pulses of a single photon carries bit data, where information is encoded in the relative phase between two pulses. The first breakthrough was made by Townsend et al. in 1993[3], who achieved a 10km transmission of a single photon with high visibility, which was a one-order longer transmission than that for polarization-based methods. A problem with the system was to stabilize it against the path length fluctuation and polarization change during the transmission. The next breakthrough was made by using Faraday mirrors (FM) to self-align the polarization and to self-balance the path length of the interferometer[7]. The transmission length was at first limited to 23km[6], but recently Stucki et al. have succeeded in extending QKD over 67km using the P&P system[19]. Our improved SPDs are expected to increase the distance of QKD. In the following, we outline the results of testing interference fringe visibility by combining the balanced, gated-mode SPD and the P&P system over 100km in conventional optical fibers[12].

The experimental system is based on a phase-encoded interferometric QKD scheme[3] with a P&P configuration[7,8]. The configuration consists of 100km long fiber, an AMZ on the Bob side and a FM on the Alice side, with two phase-modulators (PM_A and PM_B) on each side. The system operates at a wavelength of 1,550nm and the laser light pulse is attenuated to obtain a pseudo single-photon level transmission. The average photon number per pulse coming back from Alice was set to 0.1 in this experiment. The repetition rate for the laser operation, the APD gating, and biasing of the phase modulator was 500kHz to avoid an after-pulse effect. Pulse widths for the laser, APDs and phase modulator were 0.5ns, 0.75ns, and 20ns, respectively.

We measured photon counting probability or key generation rate as a function of transmission distance. The photon counting probability decreases almost exponentially with an increase in distance. Measured points are well fitted by a linear line with a transmission loss of the used fiber (0.25dB/km). The interference fringe visibility

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}$$

after 100km transmission was 83% and 80% for APD1 and APD2, respectively. Note that these visibilities include the errors due to system noise and dark counts. The visibilities were smaller than those of the original interferometer (to be measured in back-to-back transmission.) The corresponding fidelity of the QKD system, defined as F=(1+V)/2, was of more than 90% and a quantum bit error rate (QBER), defined as 1-F, of less than 10%. A drift in temperature of the fibers and the resulting timing deviation during the measurements probably causes the deviation of the measured points from the fitted line that starts around 80km. This can be eliminated by actively adjusting the gating time of the APDs. Temporal broadening of the photon arrival time due to a wavelength dispersion of the fibers, 1.7ns/nm-100km at 1,550nm, must be negligible. Dark counts or detector noise was 0.1 count/s or 2×10^{-7} per pulse and error counts caused by stray photons were (0.6 count/s or 1.2×10^{-6} per pulse). The detector noise corresponds to an S/N ratio of 57dB. The stray photons are mainly caused by Rayleigh backscattering during fiber transmission, which appears after connecting the transmission line and still exists even when the Alice part is removed.

Furthermore, the number becomes roughly a quarter by halving the repetition rate. We do not know the exact function of backscattering against distance but it was roughly the same from 40 to 100km. By using a balanced, gated-mode APD-SPD, we could improve the S/N ratio by 17dB from the conventional unbalanced SPD. Nevertheless, we could only extend the distance by an amount corresponding to 9dB because of the backscattering noise. This backscattering will be reduced by inserting a storage line on the Alice side and using burst photon trains[9]. If we stick to a rule-of-thumb for a secure QKD system, that is, 10% as the QBER criteria, the maximum distance without the backscattering effect is estimated to be 140km. The fiber we used for this experiment had a loss of 0.25dB/km, which is a commonly assumed value for actual communication, but not that of the best of the commercially available fibers. If we could use a fiber with a 0.17dB/km transmission loss, which is already commercially available, this SPD would make it possible to achieve a 200km long QKD.

3.2 Integrated Interferometer for Unidirectional Transmission

Almost all the recent experiments on QKD utilized an auto-compensating ‘Plug & play’ (P&P) system[6-10,18,19]. Although it works well for QKD systems using a weak pulse up to 100km[12], to extend the transmission distance will be difficult even if a lower noise SPD is developed. This is because backscattering noise in the fiber dominates the detector noise, which is intrinsic to the bidirectional auto-compensating system. Although the use of storage lines and burst photon trains would reduce the backscattering, this would also reduce the effective transmission rate by one-third. We propose a solution to this conflict between stability and transmission distance by showing a unidirectional system using integrated-optic interferometers based on planar lightwave circuit (PLC) technology[13]. Our system is also compatible with QKD systems using true single photon or quantum correlated photon pairs. AMZs with a 5-ns delay in one of the arms, were fabricated on a silica-based PLC platform. Since the AMZs were fabricated using the same mask, they had the same path length difference between the two arms, but their phase settings were not well determined. To set the phase, it is enough to control the path length difference for the temperature of the Si substrate. The optical loss was 2dB (excluding the 3dB intrinsic loss at the coupler). Polarization-dependent loss was negligible (0.32dB), but the birefringence of the waveguide cannot be ignored. One of the couplers was made asymmetric to compensate for the difference in the optical loss between the two arms, so the device was effectively symmetric. A Peltier cooler attached to the back of the substrate enabled control of the device temperature with up to 0.01°C precision. Polarization-maintaining fiber (PMF) pigtails aligned to the waveguide optic-axis were connected to the input and output of the AMZ.

Two AMZs were connected in series by optical fiber to produce a QKD interferometer system (**Fig. 3**). Optical pulses that were 200ps long and linearly polarized along one of the two optic-axes were introduced into the PMF pigtail of Alice’s AMZ from a DFB laser at 1,550nm. The input pulse was divided into two coherent output pulses polarized along the optic-axis of the output PMF, one passing through the short arm and the other through the long arm. The two optical pulses were attenuated to an average photon number of 0.2. The two weak pulses are propagated along the optical fiber and experience the same polarization transformation. This is because the polarization in fibers fluctuates much more slowly than the temporal separation between the two pulses. After traveling through Bob’s AMZ, these pulses created three pulses in each of the two output ports. Among these three pulses, the middle presents the relative phase between the two pulses. The interfering signal at the middle pulses was differentiated by adjusting the applied gate pulse timing. The system repetition rate was 1MHz to avoid APD after-pulsing.

Precise control of the relative phase setting between the two AMZs and the birefringence in the two arms of Bob’s AMZ are necessary to obtain high visibility. Both of these can be achieved by controlling the device temperatures. To set the phase, it is sufficient to control the path length difference within $\Delta L=\lambda/n$, where $n\sim1.5$ is the refractive index of silica. The path length difference depends linearly on the device temperature with 5μm/K, due to the thermal expansion of the Si substrate.

The birefringence in the two arms can be balanced by controlling the relative phase shift between two polarization modes, because the two arms have the same well-defined optic-axes on the substrate. If the path length difference is a multiple of the beat length $\Delta L_B=\lambda/\Delta n$, where Δn is the modal birefringence, the birefringence in the two arms is balanced and two pulses interfere at the output coupler of Bob’s AMZ no matter what the input pulse polarization is. Since Δn/n was the order of 0.01 for our devices, the birefringence was much less sensitive to the device temperature than the relative phase. Therefore, we could easily manage both the phase setting and the birefringence balancing simultaneously.

We measured the photon counting probability given by the key generation rate divided by the system repetition rate and plotted it as a function of the transmission distance (**Fig. 4**). The measured data fits well with the upper limit determined by the loss of the fiber used (0.22dB/km). In Fig. 4, the base lines present the dark count probabilities. The interference fringe is shown in the inset. The visibility at 150km was 82% and 84% for the two APDs[14], which

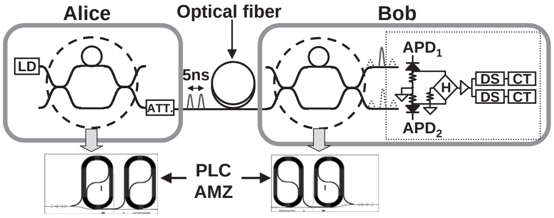

Fig. 3 A schematic diagram of the integrated-optic interferometer system for quantum key distribution. LD: laser diode, ATT: attenuator, APD: avalanche photodiode, DS: discriminator, CT: counter, H: 180° hybrid junction.

corresponds to a quantum bit error rate (QBER) of 9% and 8%, respectively. These satisfy the rule-of-thumb for secure QKD. The interference was stable for over an hour, which is good enough for a QKD system. Our system was able to achieve a much longer transmission distance than had been attained in a previous experiment using the auto-compensating system[19].

4. REFINEMENTS TOWARD A PRACTICAL QKD SYSTEM

4.1 Temperature Insensitive Interferometer

The P&P system uses a Faraday mirror (FM) in order to achieve good interference performance with ease. This system would be suitable for a short distance QKD system, because of the simple optical control. In practical systems, however, the system should be robust and capable of countering environmental changes. Temperature in a rack-mounted set may vary from –5°C to 70°C. The temperature dependence of the rotation angle at the FM causes errors, and thus the final secret key generation rate will vary. A temperature insensible system is indispensable for a practical installation. We propose a temperature insensible auto-compensating device with a simple optical structure[15].

Before presenting our proposals, we summarize the role of the FM in P&P systems. Since the reflected light propagates in the opposite direction, we need to be careful about the coordinates. In the following, we fix the direction of the axes. The FM effect on the basis of linear polarization is to read the σ_x rotation. The effect of the transmission line (fiber) on the polarization can be expressed by the unitary transform:

$$U = e^{i\alpha} R_z(2\beta) R_y(2\gamma) R_z(2\delta) \tag{9}$$

where Ry and Rz stand for the rotation on the y axis

$$R_y(2\gamma) = \begin{pmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{pmatrix}, \tag{10}$$

and the rotation on the z axis

$$R_z(2\delta) = \begin{pmatrix} e^{-i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix}, \tag{11}$$

respectively. The above unitary transform (9) is general, as long as we can neglect depolarization in the fiber. We can see that the total effect (excluding the global phase) of going-around the transmission line is just the transformation by the FM

$$R_z(2\delta) R_y(2\gamma) R_z(2\beta) \sigma_x R_z(2\beta) R_y(2\gamma) R_z(2\delta) = \sigma_x . \tag{12}$$

The outward and homeward polarizations are orthogonal, regardless of the disturbance at the transmission line and the initial polarization. This condition is essential for stable interference. However, the rotation angle of FM depends on the temperature and the transformation by the FMs deviation from σ_x as the temperature changes. Auto-compensation becomes no longer perfect.

We found that a loop mirror as depicted in **Fig. 5** can provide the same effect as FM. Two input/output terminals of a polarization beam splitter (PBS) are connected by the PMF to make a loop. The polarizations at the terminals are aligned to the slow axis of the PMF, so that one defined polarization runs in the fiber loop. Note that input horizontal polarization turns to the vertical polarization at the output, and vice versa. A Phase modulator (PM_A) is placed at an

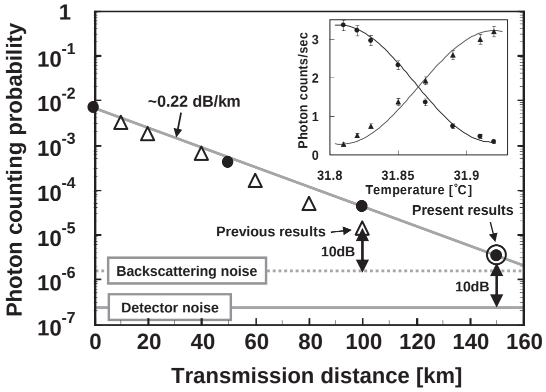

Fig. 4 Photon counting probability against transmission distance. The open triangles indicate the results of the P&P system. Inset: Fringe observed in photon count rate, obtained by changing the device temperature at 150km.

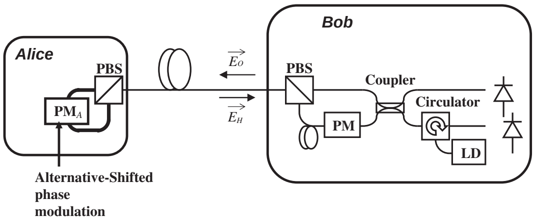

Fig. 5 A schematic diagram of the proposed Quantum key distribution system with a novel loop mirror by alternative-shifted phase modulation.

off-center position in the loop. In a P&P system, two pulses S and L enter Alice's loop mirror. The PBS divides the input photons by the polarization. Then, the four pulses travel in the loop: S_H, S_V, L_H, and L_V. PM_A can apply the phase shift to the four pulses independently by the timing of the modulation. We put the following phase shifts to the four pulses: none to S_H, π to S_V, φ_A to L_H, and $\varphi_A+\pi$ to L_V (we named it "alternative-shifted phase modulation.") The four pulses are combined by PBS into two (S and L.) The two experience the transforms $S\rightarrow\sigma_x S$ and $L\rightarrow\exp[i\varphi_A]\sigma_x L$, respectively. Temperature dependence of phase modulators is smaller than that of FMs, and it can be easily adjusted by the pulse voltage to the PM_A.

We examined the temperature dependence of the P&P QKD systems. Type 1 and Type 2 used typical FM, whereas Type 3 used the proposed loop mirror. The ambient temperature of Alice was changed using a thermostatic chamber from –5 to 75°C, which is the possible range inside the equipment. The extinction ratio was averaged over 1,000 measurements, while changing the polarization randomly. A polarization controller scrambled the polarization randomly with the four random digits generated by the "48 bit linear congruential method." **Figure 6** shows the extinction ratios against the temperature. The solid line shows the simulated results based on the assumption that the depolarization was 0.8% and the rotation angle changed by –0.013deg/K. The dashed and dotted lines show the measured results. In Fig. 6 we can see a great difference between Type 1, Type 2 and Type 3. As the temperature increased, the extinction ratio decreased in both Type 1 and Type 2 systems, whereas the extinction ratio remained high in the Type 3 system. This demonstrated the advantages of our system over conventional P&P systems[19].

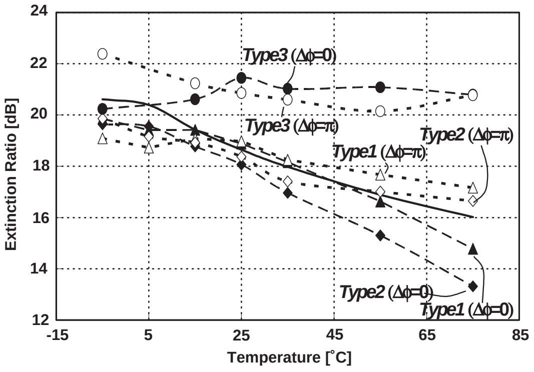

Fig. 6 Extinction ratios against temperature change. Type 1 and type 2 represent the result of conventional systems. Type 3 shows the temperature dependence in the proposed system.

· High Speed Operation

As stated before, the clock rate of QKD systems is limited by the afterpulse effect. In a short distance system, we can increase the clock rate by optimizing the SPD for small afterpulse effects. The SPDs in the previous sections were optimized for a low dark count probability in order to increase the S/N for long distance transmission. In a short distance system, the effect of the fiber loss is less serious, so that error probability can be kept below the security criteria with larger ratio P_d/η.

We implemented a high speed secret key generation experiment using the Type3 QKD system described above. At Bob, a 1,500nm directly modulated DFB-LD creates 500ps-wide pulses with a repetition rate of 62.5MHz. The sequence of optical pulses is split by a polarization maintained coupler (PMC). Transmission over a single mode fiber (SMF) was carried out. The optical power was adjusted so that the average photon number μ at Alice becomes 0.6 photons/pulse, which is slightly higher than the reported experiments. QKD is shown to be still secure assuming practical attacks[20], and we believe that we can circumvent a photon number splitting attack with the help of 'decoy' states. We used NEC's APDs at –40°C in the balanced SPD to reduce the afterpulse effect. The measured value of the dark count probability, the detection efficiency and the afterpulse probability were about 1×10^{-4}, 7%, and 1×10^{-3} respectively, for operation at 62.5MHz. **Figure 7** shows the QBER and the raw key generation rate against the transmission distance. We obtained a raw key generation rate of about 100kHz and QBER of 4% over SMF 40km transmission[15]. We sent the sequences of all "0" and all "1" in this experiment. Because the

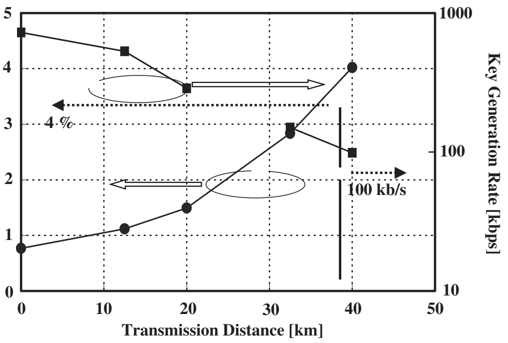

Fig. 7 QBER and raw key generation rate against the transmission distance.

afterpulse probability was not negligibly small, Eq. (8) suggests that QBER would increase about a few percent for random bit sequences. Even if so, QBERs remain lower than the criteria, and moreover, the afterpulse-induced impairment can be avoided by setting an adequate dead time at the APDs.

5. CONCLUSION

Above, we have reviewed our research on the fiber-optics based quantum communication. Though our current researches are focused on QKD systems, the techniques developed can be applied to other quantum information processing involving photons. Combination with other efforts that are not mentioned here, such as entangled-photon-sources, single photon sources, two-qubit gates, and so on, will provide a rigid foundation for future quantum information technologies.

ACKNOWLEDGMENTS

The authors would like to thank the collaborators, Mr. A. Tanaka, Ms. W. Maeda, Mr. T. Takeuchi, and Mr. S. Takahashi, who conducted most of the experiments described in this article. A part of this work was supported by NICT.

REFERENCES

[1] C. H. Bennett and G. Brassard, Proc. Int. Conf. Comput. Syst. Signal Process., Bangalore, pp.175-179, 1984.

[2] C. H. Bennett, F. Bessate, et al., *J. of Cryptography*, **5**, 3, 1992.

[3] P. D. Townsend, J. G. Rarity and P. R .Tapster, *Elec. Lett.*, 29, 634, 1993.

[4] J. D. Franson and B. C. Jacobs, *Elec. Lett.*, 31, 232, 1995.

[5] R. Hughes, G. Morgan and C. Peterson, *J. of Modern Optics*, 47, 533, 2000.

[6] A. Muller, H. Zbinden and N. Gisin, *Europhysics Lett.*, 33, 335, 1996.

[7] A. Muller, T. Herzog, et al., *Appl. Phy. Lett.*, 70, 793, 1997.

[8] H. Zbinden, J. D. Gautier, et al., *Elec. Lett.*, 33, 586, 1997.

[9] G. Ribordy, J.-D. Gautier, et al., *Elec. Lett.*, 34, 2116, 1998.

[10] G. Ribordy, J.-D. Gautier, et al., *Elec. Lett.*, 34, 2116, 1998.

[11] A. Tomita and K. Nakamura, *Opt. Lett.*, 27, 1827, 2002.

[12] H. Kosaka, A. Tomita, et al., *Elec. Lett.*, 39, 1199, 2003.

[13] Y. Nambu, T. Hatanaka and K. Nakamura, *Jap. J. of Appl. Phy.*, 43, L1109, 2004.

[14] T. Kimura, Y. Nambu, et al., *Jap. J. of Appl. Phy.*, 43, L1217, 2004.

[15] A. Tanaka, A. Tomita, et al., 30th European Conference on Optical Communication (ECOC), Stockholm, Sweden (Sep. 5-9, 2004), Tu4.5.3.

[16] N. Lutkenhaus, Phy. Rev., A 61, 052304, 2000.

[17] A. Yoshizawa and H. Tsuchida, *Jap. J. of Appl. Phy.*, 40, 200, 2001.

[18] D. S. Bethune and W. P. Risk, *IEEE J. of Quantum Electronics*, 36, 340, 2000.

[19] D. Stucki, N. Gisin, et al., *New J. of Phy.*, 4, 41, 2002.

[20] M. Du?ek, M. Jahma, and N. Lutkenhaus, *Phy. Rev.*, A 62, 022306, 2000.

Received November 30, 2004

* * * * * * * * * * * * * * *

Akihisa TOMITA received his M.S. degree in physics and Ph.D. in electronics from University of Tokyo in 1984 and 1998. He joined NEC Corporation in 1984, and is now Principal Researcher of Fundamental and Environmental Research Laboratories. He is engaged in the studies on quantum information.

Dr. Tomita is a member of Physical Society of Japan, Japanese Society of Applied Physics, the Institute of Electronics, Information and Communication Engineers, and Optical Society of America.

Yoshihiro NAMBU received his M.E. degree in applied physics from Kyoto University in 1987. He joined NEC Corporation in 1987, and is now Principal Researcher of Fundamental and Environmental Research Laboratories. He is engaged in research on quantum cryptography.

Akio TAJIMA received his B.E. and M.E. degrees in electrical engineering from Tokyo Institute of Technology, Tokyo, Japan, in 1990 and 1992, respectively. In 1992, he joined NEC Corporation, and now is Assistant Manager of System Platforms Research Laboratories. He is engaged in the development of quantum cryptosystem.

Mr. Tajima is a member of the Institute of Electronics, Information and Communication Engineers of Japan.