Quantum key distribution at 1550 nm using a pulse heralded single photon source

Alexandre Soujaeff, *Tsuyoshi Nishioka, *Toshio Hasegawa, Shigeki Takeuchi, *Toyohiro Tsurumaru, Keiji Sasaki and *Mitsuru Matsui

JST/Research Institute for Electronic Sciences, Hokkaido university, Kita 12 Nishi 6, Kita ku, Sapporo, 060-0812, Japan.

**Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501, Japan.*

alex@es.hokudai.ac.jp

Abstract: Quantum key distribution with pulsed heralded single photon source was performed over 40 km of fiber for the first time to our knowledge. QBER was measured to be 4.23% suggesting security against unconditional attack.

OCIS codes: (270.5290) Photon statistics; (060.0060) Fiber optics and optical communications.

References and links

1. C.H. Bennett and G. Brassard, in *proceedings of the IEEE International Conference on Computers, Systems and Signals Processing*, (Institute of Electrical and Electronics Engineers, New York 1984), pp. 175-179 .
2. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," J. Cryptology **5**, 3-28 (1992).
3. P. Townsend, J. G. Rarity and P. R. Tapster, "Single photon interference in a 10 km long optical fiber interferometer," Electron. Lett. **29**, 634-639 (1993a).
4. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett. **85**, 1330-1333 (2000).
5. V. Scarani, A. Acín, G. Ribordy and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**, 0579014 (2004).
6. K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," Phys. Rev. A **71** , 042305 (2005).
7. H.-K. Lo and X. Ma and K. Chen,"Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
8. Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian,"Experimental quantum key distribution with decoy states," Phys. Rev. Lett. **96**, 070502 (2006).
9. S. Fasel, O. Alibart, A. Beveratos, S. Tanzilli, H. Zbinden, P. Baldi and N. Gisin,"High-quality asynchronous heralded single-photon source at telecom wavelength," New J. of Phys. **6**, 163 (2004).
10. Shigeki Takeuchi, Ryo Okamoto, and Keiji Sasaki,"High-yield single-photon source using gated spontaneous parametric downconversion," Appl. Opt. **43** , 5708-5711 (2004).
11. Ryo Okamoto, Shigeki Takeuchi, and Keiji Sasaki, "Detailed analysis of a single-photon source using gated spontaneous parametric downconversion," J. Opt. Soc. Am. B **22**, 2393-2401 (2005).
12. A. Trifonov and A. Zavriyev,"Secure communication with a heralded single-photon source," J. Opt. B **7**, S772–S777 (2005).
13. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145-195 (2002).
14. E. Waks, A. Zeevi and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," Phys. Rev. A **65**, 052310 (2002).
15. H. Briegel, W. Dür, J. I. Cirac and P. Zoller,"Quantum repeaters: the role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932-5935 (1998).
16. A. Soujaeff, S. Takeuchi, K. Sasaki, T. Hasegawa and M. Matsui, "Heralded single photon source at 1550 nm from pulsed parametric downconversion," quant-ph/0611112, (2006).

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

17. D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices,Quantum inf. comput. **4**, 325-360 (2004).
18. H. K. Hong and L. Mandel, "Experimental realization of a localized one-photon state," Phys. Rev. Lett. **56**, 58-60 (1986).
19. Using a model presented in reference [10, 11, 16], we estimated the average number of photon pairs μ at the crystal output to be 0.168 at the maximum pump power (195 mW), and 3 pairs event probability at the crystal ouput to be a fraction equal to 0.056 of the two pairs generation probability for this pump power.
20. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121-3124 (1992).
21. M. Koashi, "Efficient quantum key distribution with practical sources and detectors," quant-ph/0609180, (2006).
22. M. Hayashi, "Practical evaluation of security for quantum key distribution," Phys. Rev. A **74**, 022307 (2006).
23. Y. Adachi, T. Yamamoto, M. Koashi, N. Imoto," Simple and efficient quantum key distribution with parametric down-conversion," quant-ph/0610118, (2006).

1. Introduction

From its introduction 20 years ago, quantum key distribution (QKD) using the BB84 protocol [1] was soon followed by first experimental demonstration over air [2] and fiber [3], and is now available commercially from various companies. One of the important issues in the field of QKD is to extend the distance over which absolute security is obtained for eavesdropper attack. It was pointed out that the secure distance of original BB84 protocol with weak coherent pulse (WCP) is very strictly limited even when the average number of photons per pulse is optimized, since the probability to have two photons in one pulse $P(2)$ cannot be decreased without sacrificing $P(1)$, the probability to have one photon in one pulse [4]. Recently some new protocols using WCP have been proposed to solve this problem [5, 6, 7], and for example experimental demonstration was recently reported for decoy state protocol [8].

QKD using a heralding single photon source (HSPS) is an alternative approach to achieve longer secure distance [4]. HSPS is usually realized using pairs of photons produced via spontaneous parametric down conversion (SPDC). The detection of one of the photons of the pair is used as a signal to 'herald' the signal photons transmitted from sender to receiver. There have been reports about such sources [9, 10, 11] and a QKD system including one of them [12], however, all of them are using parametric fluorescence with CW pumping. In this case, there are some problems because the signal photons are produced at random times. First, it is very difficult to synchronize the sender and receiver stations. Second, such a system may not be used for future systems equipped with quantum relays [13, 14] or quantum repeaters [15], because the accuracy of timing/position of photons is indispensable for bell state analysis using two-photon interference.

In this paper we present the first demonstration of BB84 based QKD experiment using pulsed-HSPS performed over 40 km on fiber, which exceeds achievable distance with QKD based on the original BB84 protocol with WCP. A HSPS using non-degenerate parametric downconversion with femto-second laser pumping was used in our experiment [16]. The photon source was coupled to a one-way QKD system realized with two unbalanced Mach-Zehnder interferometers and phase modulators. With strong suppression of the two-photon component ($P(2) = 1.48 \times 10^{-5}$) achieved after the sender station, we achieved QKD experiment with the quantum bit error rate (QBER) 4.23 % suggesting unconditional security [17]. Since we adopted pulsed HSPS, the system clocks (82 MHz) at the sender and the receiver were well synchronized, and is suitable for the future quantum-relays and quantum repeaters.

We organized this paper as follows. In section 2, we will briefly detail the HSPS used in the experiment, then the pump laser power dependence of the photon number distribution, and the spectrum of the signal photon. In section 3, we describe the diagram of the one-way QKD system used in the experiment. We report our experimental results with gain analysis for coherent attack based on the reference [17] in section 4 before conclusion.

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

2. Heralded Single Photon Source

2.1. Principle

When a pump beam interacts with a non-linear crystal and the phase matching condition is fulfilled, a photon pair is generated and the detection of one photon of the pair informs us of the presence of an other photon. This scheme was used first by Hong and Mandel to prepare a single photon state [18]. One of the main advantages of this technique is that if the first photon of the pair is detected in a given direction and for a specified spectral range, we can find and collect its brother photon thanks to the momentum and energy conservation relation they share through phase matching in the crystal.

For QKD at 1550 nm, we realized a source using pulsed non degenerate type I SPDC (see reference [16] for more details). A femtosecond pump (150 fs) at 390 nm is focused inside

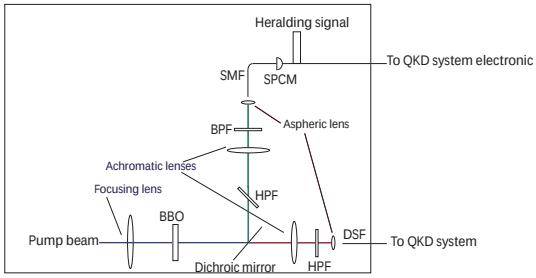

Fig. 1. HSPS experimental set up, bandpass filter (BPF) and highpass filter (HPF) reject residual pump in idler and signal path.

a 5 mm BBO crystal which is cut to give a photon pair with signal photon at 521 nm and idler photon at 1550 nm. These photons are separated with a dichroic mirror, collimated in each path and then focused into single mode fiber (see experimental scheme on Fig. 1). Lenses were selected to match the mode of the pump and mode of the signal and idler in the crystal. Compared to previous experiment [16], we used achromatic lenses rather than biconvex lenses to collimate the photons in each path. The Heralding signal is provided by a single photon counting module (SPCM) placed in the signal path.

2.2. HSPS statistics

The multi-photon component statistics of our HSPS was measured using a Hanburry Brown and Twiss (HBT) setup consisting of a 50/50 fiber beam splitter and two single photon detectors at 1550 nm based on avalanche photodiode (APD) (Id Quantique id200). To obtain photon number distribution from coincidence measurements, we made the following assumptions. Average number of photon pairs per mode at the crystal output is much lower than 1, and photon number contribution higher than $n = 3$ can be neglected [19].

As we used only two detectors, we limited ourselves to the measurement of $P(1)$ and $P(2)$, the probability to have one or two photons at our HSPS output when a trigger signal was recorded in the signal path. Coincidences were recorded using a photon counter (Stanford Research SR400) for different pump powers. Accidental coincidence counts caused mostly by the simultaneous detection of a dark count and a single photon in the HBT setup were subtracted from the measured coincidences [9]. The Results of our measurements are given in table 1.

In ideal HSPS, $P(1)$ is unity. In experiment $P(1)$ is limited by coupling efficiency of idler photons into single mode fiber (0.351) and also by optical losses (transmission coefficient of

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

Table 1. HSPS photon number distribution and triggering rate. For $P(1)$, statistical fluctuation were negligible (less than 2% of the total count)

Pump power (mW)	Trigger rate (KHz)	P(1)	P(2)$\times 10^{-3}$	$P_c(2) \times 10^{-3}$
195	299	0.296	16.6 ± 0.40	16.6 ± 0.40
98	136	0.271	8.8 ± 0.80	10.5 ± 0.95
49	64	0.259	3.2 ± 0.95	4.18 ± 1.24
24.5	30.2	0.235	1.6 ± 0.365	2.54 ± 0.58
9.8	15.2	0.215	0.6 ± 0.43	1.1 ± 0.82

0.842). The increase of $P(1)$ (from 0.18 to 0.296) compared to our previous experiment [16] can be explained by the new lens inserted in the setup and also a better aligment procedure. $P(1)$ decreases when decreasing pump power, due to a technical reason: When inserting optical attenuators in the pump beam to control pump power, the pump beam propagation axis was sligthly deviated, which caused a decrease of coupling efficiency for idler photons. The effect was compensated by realigning carefully the fiber coupler in the idler path when we performed QKD experiments.

We measured $P(2)$ for different pump power. In table 1 we give $P(2)$ with standard deviation calculated from experimental data. To find the true dependance of $P(2)$ to the pump power and avoid artifact due to the degradation of coupling losses caused by the optical attenuators, we applied a correction to $P(2)$, $P_c(2) = P(2) \times (0.296)^2/P(1)^2$ which is plotted in Fig. 2. The linear regression for $P_c(2)$ gives a coefficient of 8.65×10^{-5} pairs of photons per mW at our HSPS output. As our set up to measure $P(2)$ is limited by accidental coincidences, we cannot

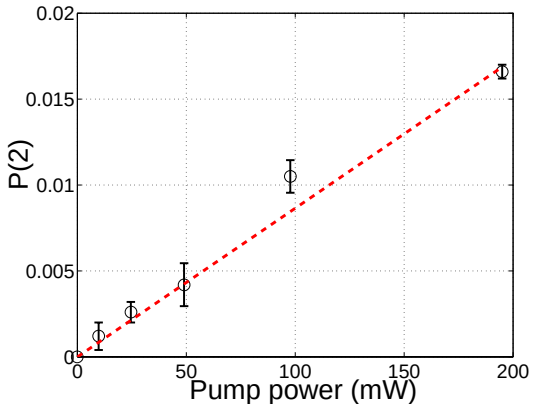

Fig. 2. $P_c(2)$ of HSPS as a function of pump power for a constant $P(1)$ of 0.296. Black circles are measurement results, plotted with error bars. The dashed red line is the linear regression curve for $P_c(2)$.

measure $P(2)$ below 1.24×10^{-4}. For further QKD experiments with lower value of $P(2)$, we calculated our source $P(2)$ using the linear law governing $P(2)$ derived above.

2.3. HSPS spectrum

For transmission over a long distance of single mode fiber, it is important to characterize the optical bandwidth of the HSPS. Dispersion will cause a spread of the initial pulse duration, which can be a problem when using gated single photon detection if the spread of the arrival time at the receiver is larger than the time gate. To measure HSPS bandwidth, we inserted a

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

tunable bandpass filter (0.9 nm FWHM) between HSPS and our single photon detector. We scanned the filter over 40 nm every 2.5 nm, and recorded coincidence counts. The FWHM of the HSPS was 21 nm.

In the case of CW pumping for type I SPDC, the bandwidth depends on the crystal length (the longer the crystal, the smaller the bandwidth, as the phase matching becomes more stringent for a longer crystal) and can be reduced using a thin bandpass filter in the signal path as done in reference [12]. In our case there is in addition to this phenomenon the influence of our non monochromatic pump. Each spectral component of the pump (2 nm FWHM) will produce down conversion, with a finite spectral width (which depends on the phase matching relation) as in the CW case. Then all SPDC produced by each pump spectral component will sum, which explains the relatively large bandwidth of our source compared to a CW source.

For dispersion shifted fiber (DSF), dispersion is zero at the central wavelength of our HSPS. But as the FWHM bandwidth of our source is 21 nm, it cannot be neglected. We made an experiment to check if dispersion limits transmission of photons produced by our HSPS. We inserted 40 km of DSF between the HSPS and a gated single photon detector with 2 ns gate, and scanned in time the detector gate respective to the heralding signal. The FWHM of the gated APD (time interval for which the count is more than half the maximum count value) ouput count signal was 500 ps with no fiber inserted and 1200 ps for 40 km of DSF. The time spread can be attributed to the dispersion experienced by a photon in the fiber, and correspond to an evaluation of 1260 ps given by the product between dispersion average value (1.5 ps/nm/km), source FWHM and fiber length. There were no additional losses due to increase of the time arrival window of single photon at the receiver. For longer distance, dispersion compensation fiber should be used, at the cost of additional losses in the optical channel.

3. QKD system

The most robust coding for QKD over fiber is phase coding, originally introduced by Bennet [20]. Encoding is made using two identical unequilibrated Mach-Zehnder interferometers. Interference can be observed when photons take indistinguishable paths through both interferometers, and non interfering event are discarded using a time gate at the detector. To encode and measure their photons according to the BB84 protocol, Alice and Bob place each other a phase modulator in their set up. Alice applies randomly one of four phase shift (0, π, $\pi/2$ and $3\pi/2$) on one of the two optical signals (separated by the interferometer path delay) at the output of her interferometer. Bob applies one of two phase shifts (0, $\pi/2$) on one of the two optical signals before his interferometer to choose the measurement basis. Bob could also use a beam splitter and two interferometers (passive choice of the base) instead of a phase modulator and a Mach-Zehnder. The main drawback of this system is that half of the photons are lost at the first Mach-Zehnder due to the unused interferometer output at Alice, and an other half are lost at Bob's interferometer due to non interfering events.

The complete QKD system is presented in figure 3. We use planar lightwave circuit (PLC) manufactured by NTT Electronics as interferometers. In PLC, Mach-Zehnder interferometer is realized on a silica chip. The whole interferometer is hermetically sealed and precisely temperature controlled. The path length can be adjusted using local heating of interferometer arms. The path difference between the long and the short arm is 40 cm (2 ns delay) in our case. To apply phase shifts to the optical pulses, we use a phase modulator PMA (Eospace) located after Alice's PLC. Bob uses also a phase modulator PMB (Eospace) placed before his interferometer. The quantum channel between Alice and Bob is made of DSF. As PLC waveguides are slightly birefringent, to get high visibility we aligned at emitter and receiver the polarization of photons along one axis of the PLC waveguides. The two polarization controllers (PC) before the PLCs in both stations are adjusted one by one using heralded single photons, which are

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

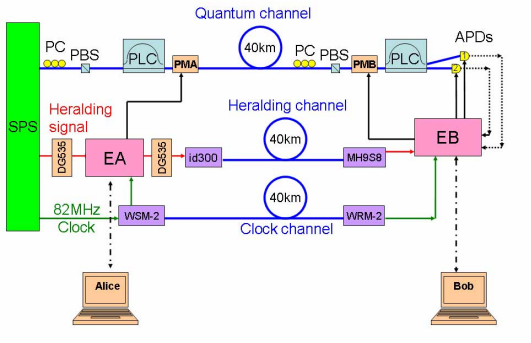

Fig. 3. QKD system, thick blue lines are DSF channel, red line is the HSPS heralding signal and green line is the 82 MHz clock signal. Black lines represent driving signal for phase modulation and APD gated operation. Doted black lines are output signals from APD, and dashed-doted black lines are signals exchange between personal computers and EA and EB.

linearly polarized in nature, to maximize the transmittance after the PBSs.

Alice and Bob cryptographic systems are each driven by a computer controlled module (EA and EB). Alice and Bob computer can communicate via an internet connection for reconciliation and QBER measurement. There are two optical channels made of DSF dedicated to timing synchronization between these modules, also made of DSF. The first channel is used to transmit the heralding signal from the HSPS source using a pulsed laser (idQuantique id300) and an optical receiver (Anritsu MH9S8). The HSPS signal from the SPCM passes through a digital delay line (Stanford research DG535) to EA and then to another similar digital delay line. The first delay line imposes a dead time of 1 μs and the second one is used to adjust delay between Alice and Bob. The second channel carries the 82 MHz clock signal from the femtosecond pump laser using a special optical emitter (Gravitron WSM-2) and receiver (Gravitron WRM-2) with very low jitter. This clock is used as a time reference for our QKD system. Phase modulation signals at Alice and Bob as well as detector gating signal at Bob are synchronized to the 82 MHz clock signal and applied only when a heralding signal is also present. With such a system, we are freed from the jitter (500 ps) of the gate signal due to SPCM (intrinsic jitter). The three optical channels could be multiplexed for transmission over only one fiber using standard wavelength division multiplexing technique. Time division multiplexing should also be used, to avoid propagation at the same time of the quantum signal and synchronization signals in order to reduce optical crosstalk at Bob's receiver.

The module EA drives the phase modulator PMA. Phase modulation signal is synchronized with the optical pulse that took the short path in the PLC, and levels at EA output are adjusted to produce all four phase shifts required for BB84 protocol. EB drives the two APD based detectors of Bob and the phase modulator PMB. The detection system of Bob consists of two APDs (Epitaxx) cooled down to 203 K. The gate pulse can be adjusted between 1 ns and 2 ns, short enough to discriminate between the three adjacent peaks spaced by 2 ns interval at Bob's Mach-Zehnder outputs. Dark count probability d_B per gate and quantum efficiency η_B of detector are 2.05×10^{-6} and 9.62% for detector 1, and 2.05×10^{-6} and 8.64% for detector 2.

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

4. QKD results analysis

We performed QKD over 40 km of DSF (9.8 dB loss). The system was first adjusted using WCP, to match Alice and Bob's interferometer. Then we replaced the attenuated laser source by our HSPS. The pump power of the HSPS was set at the maximum for initial aligment (timing signal adjustment for phase modulation and detector's time gate, as well as polarization state alignment). From our measurement of HSPS photon number statistics (see section 2.2), we then adjusted pump power to get a $P(2)$ low enough to ensure security for QKD over 40 km. After inserting optical attenuators, we realigned the HSPS and then measured $P(1)$. HSPS rate was 12.4 kHz, $P_A(1)$ and $P_A(2)$, the probability to have one or two photons at Alice PMA output were estimated respectively to be 0.0423 and 1.48×10^{-5} taking the losses in Alice set up into account. For the pump power used, three pairs event probability at the crystal output represent a fraction equal to 0.0028 of the two pairs probability. Bob receiver's optical losses were 7.3 dB, and average visibility was 97% for interference fringes.

To perform QKD, 400 random modulation sequences of 8192 bits each were applied at Alice and Bob. The average time necessary for a key exchange was 264 seconds. It is simply the ratio between the number of bits sent (8192 bits$\times$400) and the heralding signal rate (12.4 kHz). At the end of the exchange, we obtained 271 bits in the raw key (raw key generation rate of 1.02 Bits/s), and then 142 bits in the sifted key after basis reconciliation (sifted key generation rate of 0.54 bits/s). The number of errors in the sifted key was 6 bits, which translates in a QBER of 4.23% . We checked the stability of the system by recording counts at the detector as well as system visibility for 30 min and didn't notice any degradation. It is well known that change in temperature or stress applied on the fiber can change randomly the polarization state of the photons, causing extra losses and increase of the QBER. Therefore, for an experiment outside of the laboratory on installed fiber an active compensation scheme should be used to control the polarization of the photons.

The QBER is a valuable parameter for experimentalists to know if the system is operating properly, but to really evaluate QKD security, the gain figure G is more pertinent. The gain G represents the ratio of the length of the secret key Alice and Bob share over the number of bits sent by Alice after the complete protocol is accomplished (including error correction and privacy amplification). From the experimental data that are $P_A(2)$, QBER, total number of bits sent and number of detection signals recorded by Bob (raw count), we can calculate G [17]: given in equation 1:

$$G = \frac{1}{2} p_{exp} \left[\left(1 - \frac{p_m}{p_{exp}} \right) \left(1 - H \left(\frac{Q}{\left(1 - \frac{p_m}{p_{exp}} \right)} \right) \right) - H(Q) \right] \quad (1)$$

$$H = -Q \log_2(Q) - (1-Q) \log_2(1-Q) \quad (2)$$

Q is the QBER, p_{exp} is the probability for Bob to have a detection in a time slot, p_m is the probability to have two photons at Alice output (equals to $P_A(2)$). H is the entropy function. This gain was calculated in an asymptotic case, valid for on/off detectors with balanced quantum efficiencies [21]. QKD with security against coherent attack was confirmed for our experiment, with a positive G of 1.35×10^{-5}, equivalent to 44 bits in the final key (secret key creation rate is 0.16 secure bit/s). We estimated statistical fluctuation in our experiment. For our system, the expected QBER calculated from measured system parameters (detectors noise and quantum efficiency, losses, visibility and $P_A(1)$) is $4.18 \pm 1.77\%$. This is consistent with our experiment result. We also checked the reliability of the measured QBER using hypothesis testing, and found that with a confidence of 90 % QBER is $\leq 7\%$, which is below the threshold QBER (8.61 %) for secure QKD.

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

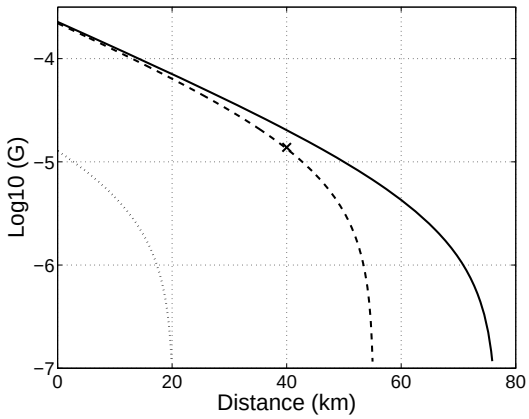

Fig. 4. Calculated gain figure of our QKD system with HSPS (dashed), for a single photon source with same P(1) as our HSPS (black) and for WCP based on original BB84 protocol with optimum average photon number (dot). The Black cross is the gain figure for the 40 km QKD experiment.

In Fig. 4, we plotted the theoretical gain figure for our QKD system operated with HSPS and also for single photon source and WCP source based on the original BB84 protocol. For the latter, we optimized the average photon number for the longest distance possible, which results in secure transmission over 20 km only. Our HSPS allows us to transmit over 55 km securely. For SPS with $P(1)$ similar to our HSPS (and $P(2) = 0$), secure communication is achievable over 76 km. With a further decrease of the $P(2)$ of our source, we can approach this limit.

5. Conclusion

We realized for the first time secure QKD using an HSPS using pulsed pumping with synchronization of the QKD system to the pump laser clock over 40 km of DSF. Longer transmission distances are possible with our system under two conditions. First, a dispersion compensation scheme should be used because of our HSPS's large optical spectrum. Second, as source rate decreases when minimizing P(2), the proportion of false heralding signals increase (due to dark count of the SPCM which is constant, 100 c/s typically) and becomes non negligible, lowering the effective P(1) of the source (and as a consequence the signal to noise ratio of the QKD system). Sending the laser clock and the gate signal into a coincidence circuit, influence of the random noise of the SPCM can be decreased. We believe it is one other advantage of pulsed pumping over CW pumping.

Note the security proof [17, 21] used in our analysis is valid for on/off detectors with balanced quantum efficiencies. Unfortunately, no security proof exists with on/off detectors with unbalanced efficiencies. One possible way to compensate the efficiency would be for Bob to discard some of the detection signals from the detector with the highest efficiency at random. If we follow this scenario, the QBER becomes 4.47 %, which is slightly larger than the measured QBER of 4.23 % but still smaller than the QBER threshold (8.61 %) for secure key generation.

For future investigation, long-term operation of the system and evaluation of the security using a proof considering finite key length and statistical fluctuation, for example [22] may be an important issue. Recently, a group published a new idea inspired by decoy state protocol using heralded single photon source as ours [23]. Their proposal requires just a slight modification of the protocol, not of the set up, and can allow to have secure bits generation more efficiently.

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006

Acknowledgement

This work was supported in part by Core Research for Evolutional Science and Technology, Japan Science and Technology Agency, and National Institute for Communication Technology. We would also like to thank R. Okamoto, J. Abe, H. Ishizuka for fruitful discussions, and M. Koashi for discussion on security issues.

#74210 - $15.00 USD Received 18 August 2006; revised 28 November 2006; accepted 29 December 2006