100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors

Eleni Diamanti[1], Hiroki Takesue[2,3], Carsten Langrock[1], M. M. Fejer[1] and Yoshihisa Yamamoto[1]

[1] *Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4088*

[2] *NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, 243-0198, Japan*

[3] *CREST, Japan Science and Technology Agency, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

ediam@stanfordalumni.org

Abstract: We present a quantum key distribution experiment in which keys that were secure against all individual eavesdropping attacks allowed by quantum mechanics were distributed over 100 km of optical fiber. We implemented the differential phase shift quantum key distribution protocol and used low timing jitter 1.55 μm single-photon detectors based on frequency up-conversion in periodically poled lithium niobate waveguides and silicon avalanche photodiodes. Based on the security analysis of the protocol against general individual attacks, we generated secure keys at a practical rate of 166 bit/s over 100 km of fiber. The use of the low jitter detectors also increased the sifted key generation rate to 2 Mbit/s over 10 km of fiber.

OCIS codes: (270.0270) Quantum optics; (270.5570) Quantum detectors

References and links

1. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," J. Cryptology **5,** 3–28 (1992).
2. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74,** 145–195 (2002).
3. T. Honjo, K. Inoue and H. Takahashi, "Differential-phase-shift quanum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," Opt. Lett. **29,** 2797–2799 (2004).
4. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105 km fibre," New J. Phys. **7,** 232 (2005).
5. C. Gobby, Z. L. Yuan and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84,** 3762–3764 (2004).
6. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, A. E. Lita and S. W. Nam, "Long distance decoy state quantum key distribution in optical fiber," quant-ph/0607186 (2006).
7. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, (IEEE, New York, 1984), 175–179.
8. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61,** 052304 (2000).
9. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Limitations on Practical Quantum Cryptography," Phys. Rev. Lett. **85,** 1330–1333 (2000).

#74039 - $15.00 USD Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

10. C. Gobby, Z. L. Yuan and A. J. Shields, “Unconditionally secure quantum key distribution over 50 km of standard telecom fibre,” Electron. Lett. **40,** 1603–1605 (2004).
11. Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, “Simulation and implementation of decoy state quantum key distribution over 60 km telecom fiber,” Proc. IEEE Int. Symp. Inf. Theor. 2006, 2094–2098.
12. H.-K. Lo, X. Ma and K. Chen, “Decoy State Quantum Key Distribution,” Phys. Rev. Lett. **94,** 230504 (2005).
13. X.-B. Wang, “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography,” Phys. Rev. Lett. **94,** 230503 (2005).
14. K. Inoue, E. Waks and Y. Yamamoto, “Differential Phase Shift Quanum Key Distribution,” Phys. Rev. Lett. **89,** 037902 (2002).
15. K. Inoue, E. Waks and Y. Yamamoto, “Differential-phase-shift quanum key distribution using coherent light,” Phys. Rev. A **68,** 022317 (2003).
16. E. Diamanti, H. Takesue, T. Honjo, K. Inoue and Y. Yamamoto, “Performance of various quantum-key-distribution systems using 1.55-μm up-conversion single-photon detectors,” Phys. Rev. A **72,** 052311 (2005).
17. K. Inoue and T. Honjo, “Robustness of differential-phase-shift quanum key distribution against photon-number-splitting attack,” Phys. Rev. A **71,** 042305 (2005).
18. E. Waks, H. Takesue and Y. Yamamoto, “Security of differential-phase-shift quantum key distribution against individual attacks,” Phys. Rev. A **73,** 012344 (2006).
19. C. Langrock, E. Diamanti, R. V. Roussev, Y. Yamamoto, M. M. Fejer and H. Takesue, “Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled $LiNbO_3$ waveguides,” Opt. Lett. **30,** 1725–1727 (2005).
20. R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden and N. Gisin, “Low jitter up-conversion detectors for telecom wavelength GHz QKD,” New J. Phys. **8,** 32 (2006).
21. H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer and Y. Yamamoto, “10-GHz clock differential phase shift quantum key distribution experiment,” Opt. Express **14,** 9522–9530 (2006).

1. Introduction

Since the first demonstration of a quantum key distribution (QKD) system in 1992 [1], there have been numerous efforts toward the implementation of such systems [2] with the goal of making quantum cryptography practical by achieving the longest possible communication distance and the highest possible communication rate. The rapid progress in the field has recently led to the implementation of fiber-based QKD systems that operated at 1 GHz clock frequency [3, 4] and extended the key distribution distance to more than 100 km [4, 5, 6].

Most of the previous experiments, however, have not been able to guarantee the security of the generated keys against general eavesdropping attacks, despite the fact that security proofs providing the conditions required for unconditional security exist for the implemented protocols. Often the average photon number per pulse is set to the arbitrary value 0.1, which is not the result of a security proof. In the best cases, only a limited set of potential eavesdropping attacks is taken into account. For implementations of the BB84 protocol [7] with a Poisson source this set usually does not include the powerful photon number splitting attack, rendering these systems ultimately insecure [8, 9]. Generation of keys that were secure against general individual attacks and their distribution over 50 km of optical fiber using the BB84 protocol with a Poisson source and InGaAs/InP avalanche photodiodes (APDs) with a very small dark count rate was reported in [10]. Furthermore, [6] and [11] reported implementations of the decoy state BB84 protocol [12, 13], which achieved secure key distribution over 107 km and 60 km of fiber using superconducting transition-edge sensors and InGaAs/InP APDs, respectively. All these systems, however, featured a very small secure key generation rate, which prevents their integration into practical telecommunication networks.

In the experiment presented in [4], we implemented the differential phase shift quantum key distribution (DPS-QKD) protocol, which uses a Poisson light source [14, 15] but is robust to photon number splitting attacks [4, 16, 17]. In this implementation, the security analysis against a limited set of eavesdropping attacks, in particular the beamsplitter, intercept-resend and photon number splitting attacks, was taken into account. Although it is important to demonstrate a practical QKD system that is secure against these realistic attacks, it is also crucial to consider

#74039 - $15.00 USD Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

more elaborate attacks that will be within technological reach in the near future and guarantee the security of the system against these types of attacks. The security of the DPS-QKD protocol against all individual attacks allowed by quantum mechanics, including photon number splitting attacks, was proven in [18]. An individual attack against the DPS-QKD protocol is slightly different than the commonly considered individual attack; rather than defining an action against an individual qubit, which for example can be a single-photon pulse for a polarization qubit or a quantum state spanning two time slots for a time-bin qubit, it defines an action against a single photon, whose quantum state spans many time slots in the DPS-QKD protocol, as we will see in Sec. 2, and thus is not a qubit. In both cases, however, the attack is directed against each single photon, and so the term ‘individual’ can still be applied. Based on the security analysis of [18], the experiment described in [4] did not generate keys secure against these general individual attacks over 105 km of fiber. The main limiting factor for the secure key distribution distance in this system was the large bit error rate caused by the broadening of the received signal induced by the large timing jitter of the single-photon detectors employed in the system. These detectors were based on frequency up-conversion in periodically poled lithium niobate (PPLN) waveguides and Si APDs [19], and had a jitter of $\sim$ 500 ps. However, up-conversion detectors using Si APDs with improved timing jitter characteristics were recently reported [20].

In this paper, we use the security analysis of the DPS-QKD protocol against general individual attacks appropriately defined for this protocol and low jitter up-conversion detectors to implement a secure high speed and long distance quantum key distribution system. The use of the low jitter detectors significantly improved the signal to noise ratio, which resulted in a smaller bit error rate. Thus, despite the tight security requirements, we achieved the distribution of keys that were secure against all individual attacks allowed by quantum mechanics over 100 km of optical fiber at a rate of 166 bit/s, which is two orders of magnitude higher than previously reported values. Furthermore, using the low jitter detectors allowed us to increase the sifted key generation rate to 2 Mbit/s over 10 km of fiber, which is double than the previous record [4].

2. Security of the differential phase shift quantum key distribution protocol

A quantum key distribution system that implements the DPS-QKD protocol is shown in Fig. 1. Alice generates a train of coherent pulses, which are attenuated such that the average photon number per pulse is less than 1, randomly phase modulated by 0 or π, and sent over an optical fiber to Bob. Each photon coherently spreads over many pulses with a fixed phase modulation pattern. In the receiver side, Bob divides the incoming pulses into two paths and recombines them using 50/50 beamsplitters. The time delay introduced by his interferometer is equal to the inverse of the clock frequency, or else equal to the time separation between sequential pulses. Single-photon detectors are placed at the output ports of the second beamsplitter. After passing through Bob’s interferometer, the pulses interfere at the output beamsplitter and the phase difference between two consecutive pulses determines which detector records a detection event. Detector 1 in Fig. 1 records an event when the phase difference is 0 and detector 2 records an event when the phase difference is π. Because the average photon number per pulse is less than one, Bob observes detection events only occasionally and at random time instances. Bob announces publicly the time instances at which a photon was detected, but he does not reveal which detector detected it. From her modulation data, Alice knows which detector in Bob’s site recorded the event. Thus, by assigning bit values 0 and 1 to detection events recorded by detector 1 and 2, respectively, they form a secret key.

In general terms, the security of the DPS-QKD protocol stems from the nondeterministic collapse of a wavefunction in a quantum measurement. In particular, if the number of pulses in the coherence time of Alice’s source is n_p, then each of Alice’s photons is in a superposition of

Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

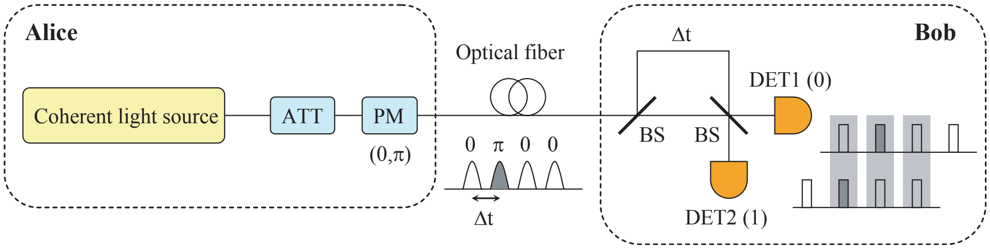

Fig. 1. Quantum key distribution system for the implementation of the DPS-QKD protocol. ATT, attenuator; PM, phase modulator; BS, beamsplitter; DET, detector.

all the states that correspond to the n_p time instances with the appropriate phase applied to each one of them. The overall wavefunction is a product state of these individual photon states. At Bob's site, a detection event at a certain time instance t_n reveals the phase difference between the pulses in time instances t_n and t_{n+1}, which corresponds to one bit of information. However, these detection events occur completely randomly, so an eavesdropper cannot deterministically collapse the wavefunction in the same time instance and obtain the same bit of information as Bob.

The security of the DPS-QKD protocol against general individual attacks appropriately defined for this protocol was rigorously proven in [18]. This analysis considered a twofold eavesdropping strategy. Eve, the eavesdropper, measures the photon number in the n_p-slot wavefunction using a quantum non-demolition (QND) measurement. Then, she sends to Bob $n_p\mu T$ photons, where μ is the average photon number per pulse and T is the total transmission efficiency of the quantum channel and Bob's detection setup, and she stores $n_p\mu(1-T)$ photons coherently to be measured after Alice and Bob have revealed all classical information. This is the photon number splitting attack in the case of the DPS-QKD protocol. In the case that Eve is assumed to store and measure her photons individually it was shown in [18] that she can obtain complete information for a fraction $2\mu(1-T)$ of the sifted key. When $T \ll 1$ and μ is small this attack is relatively ineffective for the DPS-QKD protocol. However, in the presence of system errors, Eve can also apply an optimal measurement attack on a fraction of the photons transmitted to Bob. Assuming that Eve attaches an individual probe state to each single photon, and then measures the probes independently after all classical information has been revealed, it was shown that the collision probability for each bit p_{c_0} is bounded as follows [18]:

$$p_{c_0} \le 1 - e^2 - \frac{(1-6e)^2}{2} \tag{1}$$

where e is the innocent system error rate.

Taking into account the results of the photon splitting and general individual attacks analysis, the average collision probability for the n-bit sifted key, which is a measure of Eve's mutual information with Alice and Bob, is given by the expression:

$$p_c = p_{c_0}^n = \left[1 - e^2 - \frac{(1-6e)^2}{2}\right]^{n[1-2\mu(1-T)]} \tag{2}$$

Then, the shrinking factor applied during privacy amplification to guarantee the security of the generated key is calculated as follows:

$$\tau = -\frac{\log_2 p_c}{n} = -[1-2\mu(1-T)]\log_2\left[1 - e^2 - \frac{(1-6e)^2}{2}\right] \tag{3}$$

#74039 - $15.00 USD
Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

Finally, using the techniques of the generalized privacy amplification theory the secure key generation rate after error correction and privacy amplification is given by the expression [8]:

$$\begin{aligned} R_{\text{secure}} &= R_{\text{sifted}}\{\tau + f(e)\,[e\log_2 e + (1-e)\log_2(1-e)]\} \\ &= R_{\text{sifted}}\{-[1-2\mu(1-T)]\log_2[1-e^2-\frac{(1-6e)^2}{2}] \\ &\quad + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\} \end{aligned} \tag{4}$$

where the sifted key generation rate R_{sifted} is given by Eq. (5) below for the up-conversion single-photon detectors and $f(e)$ characterizes the performance of the error correction algorithm. The QKD experiments presented in Sec. 4 are based on the results of the security analysis described here, and in particular Eq. (4).

3. The low jitter up-conversion detector

In the 1.55 μm up-conversion single-photon detector [19], a single photon at 1.55 μm is combined with a strong pump at 1.32 μm in a wavelength division multiplexing coupler, and subsequently the two beams interact in a PPLN waveguide, designed for sum frequency generation at these wavelengths. This device allows for an internal conversion efficiency exceeding 99% of the signal to the 713 nm sum frequency output. After a long-pass filter, a dichroic beamsplitter and a prism that serve the purpose of eliminating the residual pump and its second harmonic, the converted photon is detected by a Si APD. The up-conversion detector presents more favorable characteristics for fiber-based quantum cryptography than the commonly used InGaAs/InP APD [16]. This is mainly because Si APDs have a low afterpulse probability, which enables free-running or nongated Geiger mode operation. Thus, the sifted key generation rate in the DPS-QKD system is only limited by the dead time of the Si APD, and is written as:

$$R_{\text{sifted}} = \nu\mu T e^{-\nu\mu T t_d/2} \tag{5}$$

where t_d is the detector dead time, ν the system clock frequency, and the factor $1/2$ in the exponent appears because the average number of photons per second that reach each detector in Bob's setup is $\nu\mu T/2$. For commercial Si APDs with a dead time on the order of 50-80 ns, the exponential term becomes appreciable for low fiber losses and high count rates. The nongated mode operation, however, does not impose any severe limitation on the QKD system clock frequency, which is only determined by the speed of the electronic equipment and the Si APD timing jitter. In the experiments described in this paper a clock frequency of 1 GHz was used, while a 10 GHz system is also possible with these detectors [21].

The quantum efficiency and dark count rate experimental data for the up-conversion single-photon detectors with the low jitter Si APDs (MPDs) that were used for the QKD experiments are shown in Fig. 2. The quantum efficiency of the MPD device at the output signal wavelength of 713 nm is $\sim$ 25%, and so the maximum quantum efficiency of the up-conversion detector, including the coupling, propagation, and collection setup losses, did not exceed 9% for 130 mW of pump power. The dark counts, on the other hand, increase approximately quadratically with the pump power because of parasitic nonlinear processes in the waveguide and the input fiber [19].

In order to evaluate the performance of the low jitter up-conversion detectors for the DPS-QKD system we perform timing jitter measurements. For these measurements, pulses with a full width at half maximum (FWHM) of 66 ps at a repetition rate of 100 MHz are sent to the detector and the detection signal is recorded with a time interval analyzer. Under these conditions, a typical detection signal from the up-conversion single-photon detector with the low jitter Si APD is shown in Fig. 3 for a count rate of 10^5 counts/s. As we observe in Fig. 3, the FWHM

Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

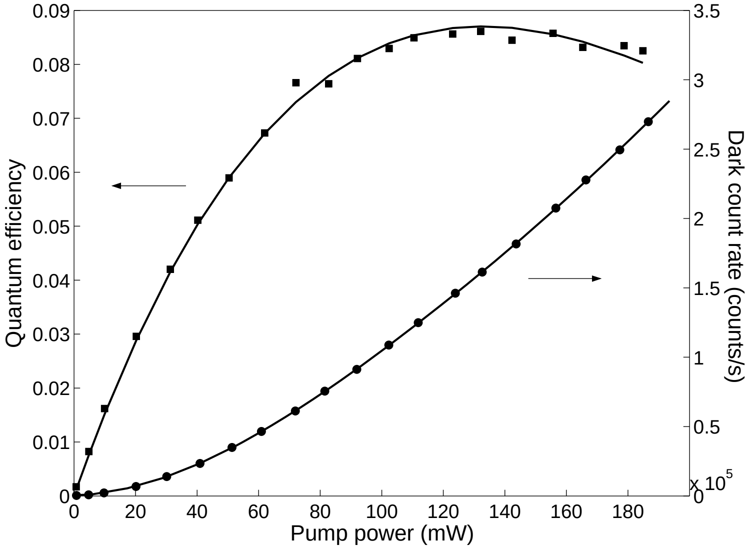

Fig. 2. Quantum efficiency and dark count rate of the low jitter up-conversion detector as a function of pump power.

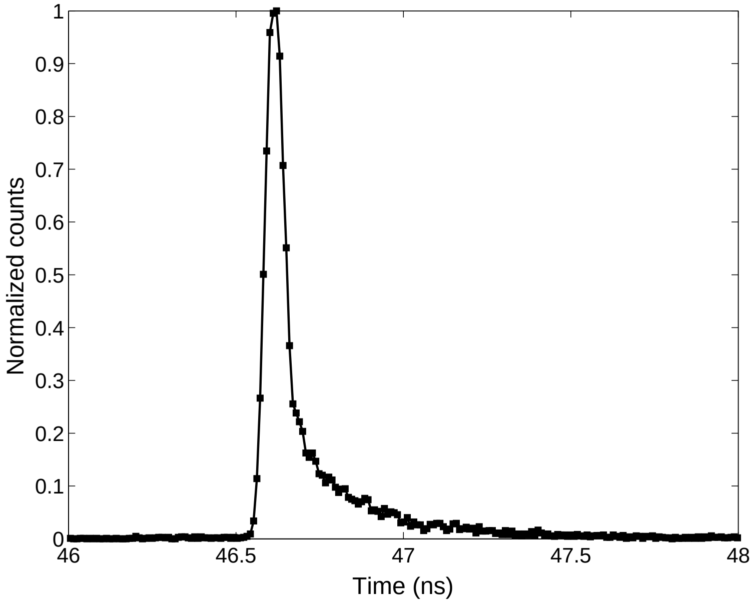

Fig. 3. Typical detection signal from the low jitter up-conversion detector when 66 ps pulses are used. This curve corresponds to a count rate of 10^5 counts/s.

#74039 - $15.00 USD Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

is 75 ps, which is significantly smaller than the 500 ps jitter obtained in experiments with high jitter up-conversion detectors. Nevertheless, the detection signal is clearly not Gaussian; there is a tail that can potentially cause errors in the adjacent 1 ns time slot in a DPS-QKD experiment with a clock frequency of 1 GHz. Fig. 3 shows, however, that 1 ns away from the peak the tail is sufficiently small to prevent intersymbol interference. It is clear that the improvement in timing jitter achieved with the low jitter Si APDs is significant, and so the error rate should be considerably lower in QKD systems employing these detectors.

4. DPS-QKD experimental setup and results

The experimental setup for the quantum key distribution experiments that we performed at a 1 GHz clock frequency to implement the DPS-QKD protocol with low jitter up-conversion single-photon detectors is shown in Fig. 4. At Alice's site, a continuous wave light at 1.55 μm generated from an external cavity semiconductor laser was modulated into a coherent pulse train with a 1 GHz clock frequency using a LiNbO$_3$ intensity modulator. The modulator was driven by a 15 GHz pulse pattern generator, so the pulse width was 66 ps. Subsequently, following the DPS-QKD protocol that is illustrated in Fig. 1, the phase of each pulse was modulated by 0 or π with a LiNbO$_3$ phase modulator. The phase modulation signal was a 1 Gbit/s pseudo-random bit sequence with a length of $2^7 - 1$ bits, which was generated by a data generator. The pulses were appropriately attenuated and sent to Bob's site through an optical fiber, where a 1-bit delay Mach-Zehnder interferometer based on planar lightwave circuit (PLC) technology was installed. The insertion loss of the interferometer was 2 dB, and the extinction ratio was greater than 20 dB. One 1.55 μm up-conversion single-photon detector was connected to each of the output ports of the interferometer. The events detected by the two Si APDs were recorded using a time interval analyzer.

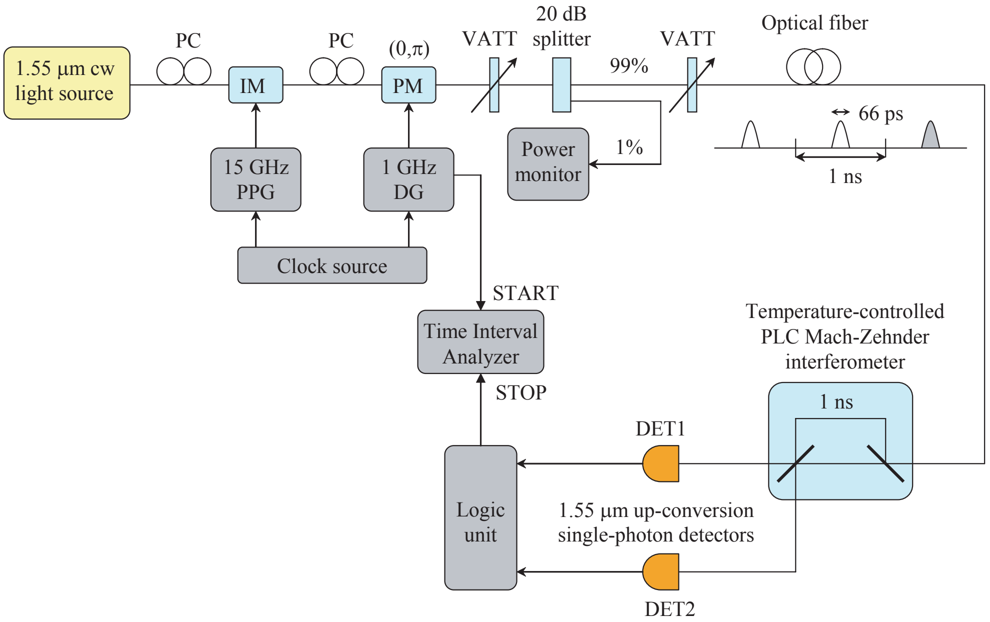

Fig. 4. Experimental setup for the 1 GHz DPS-QKD system. PC, polarization controller; IM, intensity modulator; PM, phase modulator; VATT, variable attenuator; PPG, pulse pattern generator; DG, data generator.

Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

In order to reduce the bit error rate caused by the large dark counts of the up-conversion detector we set the pump power at relatively low levels, at the expense of reduced quantum efficiency and thus reduced key generation rate as well. To further reduce the bit error rate due to dark counts we applied a time window to the recorded data. Because of the improved timing jitter characteristics of the up-conversion detector, which induces a small pulse broadening as illustrated in Fig. 3, the signal counts are concentrated in small time segments while the dark counts are randomly distributed. Therefore, we can use short measurement time windows to reduce the effective dark counts and improve the signal to noise ratio. This results in a significantly smaller bit error rate.

Before performing QKD experiments, we set the average photon number per pulse μ at its optimal value. In particular, based on the experimental parameters of the system, we maximized the secure key generation rate with respect to μ using Eq. (4) which corresponds to the general individual attacks security analysis. The optimal value was 0.2, and was practically independent of the channel transmission efficiency. Subsequently, we performed QKD experiments, that is we measured the generation rate of the sifted keys that Alice and Bob exchanged, and by directly comparing the yielded keys we also measured the bit error rate of the transmission. For each fiber length, we measured the sifted key generation rate and error rate five times and took the average values. We then calculated the secure key generation rate from Eq. (4) using the experimental results for the sifted key generation rates and bit error rates. Alice and Bob were located in the same room and we performed fiber transmission experiments using fiber spools, while some additional data were taken with an optical attenuator simulating fiber loss. Fig. 5 shows the theoretical curves and experimental results for the sifted and secure key generation rate as a function of fiber length that we obtained with the described setup and procedure for two different experimental conditions.

We first set the detector operating condition to levels appropriate for achieving high speed quantum key distribution over a short communication distance. More specifically, the quantum efficiency and dark count rate of the low jitter up-conversion detectors were set to 6% and 98 kHz, respectively. These values do not correspond to the same pump power level in Fig. 2 because the performance of the detectors was slightly degraded when the QKD experiments were performed compared to when the quantum efficiency and dark count rate data were taken. We set the time window width to 200 ps, so the dark counts per time window in these experiments were $d = 1.95 \times 10^{-5}$. The use of the 200 ps time window also decreased the effective quantum efficiency by 40%. Under these operating conditions, we performed QKD experiments for 10 km of optical fiber. We used dispersion-shifted fiber and so chromatic dispersion induced pulse broadening was negligible compared to the one caused by the detector timing jitter. The curves (a) of Fig. 5 correspond to the theoretical prediction for the sifted and secure key generation rate under these experimental conditions, when μ is optimized to maximize the secure key generation rate using the general individual attacks security analysis. A baseline system bit error rate of 1.5% was assumed in these calculations. The clear square represents the fiber transmission experimental result for the secure key generation rate, while the sifted key generation rate at the corresponding fiber length is represented by the clear diamond. The clear circles and stars show the experimental results when we simulated additional fiber loss with an optical attenuator. As we observe in Fig. 5, the theoretical curves fit very well with the experimental results. At the fiber length of 10 km we achieved a sifted key generation rate of 2 Mbit/s with a bit error rate of 2.2%, thus the secure key generation rate at this fiber length was 0.468 Mbit/s. The use of the low jitter detectors resulted in a double sifted rate at small fiber loss compared to previous experiments with high jitter up-conversion detectors [4] because of the significantly reduced error rate.

Subsequently, we set the quantum efficiency, dark count rate, and time window width to

Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

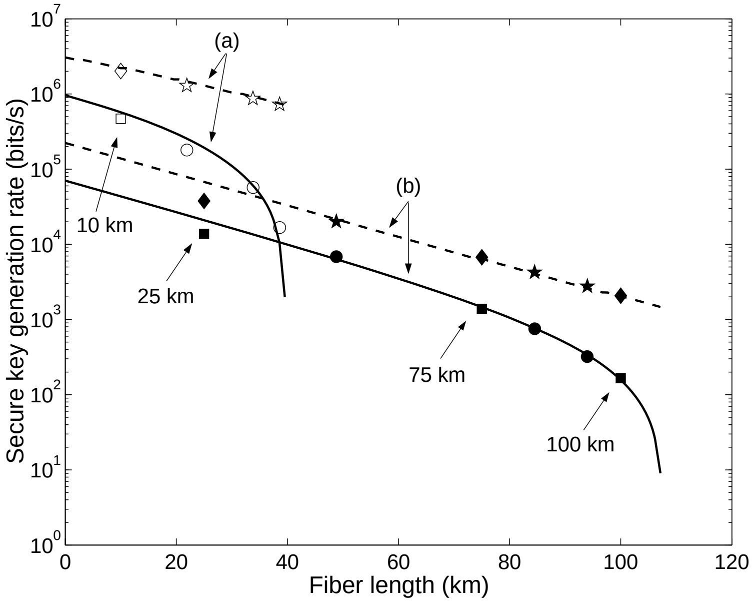

Fig. 5. Secure and sifted key generation rate as a function of fiber length for two cases. (a) The dashed and solid curves are theoretical predictions for the sifted and secure rate, respectively, when $\eta = 6\%$ and $d = 1.95 \times 10^{-5}$. The clear diamond and square are the experimental fiber transmission data for the sifted and secure key generation rate under these conditions. The clear stars and circles are the data taken with attenuation used to simulate additional fiber loss. (b) The dashed and solid curves are the theoretically predicted sifted and secure rate, when $\eta = 0.4\%$ and $d = 3.5 \times 10^{-8}$. The filled diamonds and squares are the experimental fiber transmission data under these conditions. The filled stars and circles are the simulated attenuation data. A baseline system error rate of 1.5% is assumed in all theoretical calculations.

0.4%, 350 Hz and 100 ps, respectively, to further reduce the errors caused by dark counts and thus improve the signal to noise ratio to achieve long distance quantum cryptography. The use of the 100 ps time window set the dark counts per time window to $d = 3.5 \times 10^{-8}$, and also reduced the effective quantum efficiency of the detector by 54%. Under these operating conditions, we performed QKD experiments for 25, 75 and 100 km of optical fiber. The 75 km fiber was dispersion-shifted fiber while the 25 km fiber was a standard single-mode fiber. Again, pulse broadening caused by chromatic dispersion was negligible compared with the one caused by detector timing jitter. The curves (b) of Fig. 5 correspond to the theoretical prediction for the sifted and secure key generation rate when the above experimental conditions are assumed. The filled squares and diamonds represent the fiber transmission experimental results, while the filled circles and stars correspond to data taken using the attenuator to simulate additional fiber loss. As in the previous case, we observe that the theoretical curves fit very well with the experimental data. By using these operating conditions, keys that were secure against general individual eavesdropping attacks appropriately defined for the DPS-QKD protocol were distributed at a rate of 166 bits/s over 100 km of fiber. The bit error rate for the 100 km experiment was 3.4%, of which 1% is attributed to imperfect interferometry, 1.7% to detector dark counts, and the remaining 0.7% to the timing jitter. This result shows that the key distribution distance for which security against all individual attacks allowed by quantum mechanics is guaranteed for the DPS-QKD protocol was considerably extended because of the improved timing jitter

Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006

characteristics of the up-conversion detectors employed in the system. These characteristics led to small pulse broadening, which allowed the use of a short measurement time window to substantially reduce the effective dark counts, thus improving the signal to noise ratio and decreasing the bit error rate.

The above results show that the quantum cryptography system we implemented achieves a sufficiently high communication rate and a long enough communication distance to be able to operate in a standard telecommunication network. However, the realization of a full scale QKD system ready for practical implementation in a network will require some important additional elements. In particular, the pseudo-random number generator used in the experiment to provide the phase modulation signal will need to be replaced by a true random number generator, while it is also necessary to perform the classical data post-processing steps of the DPS-QKD protocol, namely error correction and privacy amplification, with appropriate algorithms rather than calculating the secure key generation rate using the experimental values of the sifted key generation rate and the bit error rate. Finally, although in our experiment a clock synchronization signal provided locally using a short electric line between Alice and Bob was sufficient, in a practical system remote synchronization will be mandatory, and will probably involve multiplexing of the quantum and clock signals in the same transmission fiber using different wavelengths.

5. Conclusion

We presented a quantum key distribution experiment, in which we implemented the differential phase shift quantum key distribution protocol with low jitter up-conversion detectors. We showed that the improved timing jitter characteristics of the detectors allowed us to significantly increase both the key distribution rate and distance of the DPS-QKD system, while at the same time guaranteeing its security against the most general individual eavesdropping attacks allowed by quantum mechanics. With this system we achieved a 2 Mbit/s sifted key generation rate with a corresponding secure key generation rate of 0.468 Mbit/s over 10 km of optical fiber, and secure key distribution over 100 km of fiber at a rate of 166 bit/s, which is two orders of magnitude higher than previously reported values. The system's capabilities can be further extended by improving the dark count behavior of the up-conversion detectors and the timing jitter characteristics of the Si APDs. The dark counts caused by noise photons generated via spontaneous Raman scattering can be reduced by using a shorter signal wavelength than pump wavelength, while single-photon detectors with a Gaussian response and narrow FWHM based for example on photomultiplier tubes may soon become available. This will open the way to megahertz secure key generation rates and very long distance secure communication.

Acknowledgements

The authors would like to thank E. Waks for useful comments and G. Kalogerakis for providing fiber spools and electronic components. H. Takesue also thanks T. Honjo and Y. Tokura for helpful discussions and support during his stay at Stanford University. Financial support was provided by the SORST program of Japan Science and Technology Agency (JST), the National Institute of Information and Communications Technology (NICT) of Japan, and the MURI Center for Photonic Quantum Information Systems (ARO/ARDA DAAD19-03-1-0199).

Received 14 August 2006; revised 8 November 2006; accepted 8 November 2006