1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm

Hai Xu, Lijun Ma, Alan Mink, Barry Hershman, and Xiao Tang

Information Technology Laboratory, National Institute of Standards and Technology 100 Bureau Drive, Gaithersburg, MD 20899
xiao.tang@nist.gov

Abstract: We show that the performance of a 1310-nm quantum key distribution (QKD) system with up-conversion detectors pumped at 1550 nm is comparable with or better than that of current 1550-nm QKD systems with a pump at shorter wavelength. The nonlinearly-induced dark counts are reduced when the wavelength of the pump light is longer than that of the quantum signal. We have developed a 1550-nm pump up-conversion detector for a 1310-nm QKD system, and we experimentally study the polarization sensitivity, pump-signal format, and various influences on the dark count rate. Using this detector in a proof-of-principle experiment, we have achieved a secure key rate of 500 kbit/s at 10 km and 9.1 kbit/s at 50 km in a 625-MHz, B92, polarization-coding QKD system, and we expect that the system performance could be improved further.

OCIS codes: (060.4510) Optical communication; (060.2330) Fiber optics communications; (030.5260) Photon counting; (270.5570) Quantum detectors

References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Comput. Syst. Signal Process, Bangalore, India, 1984, pp. 175–179.
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
3. J. Bienfang, A. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. Su, C. Clark, C. Williams, E. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization," Opt. Express **12**, 2011-2016, (2004).
4. X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. C. Bienfang, D. Su, R. F. Boisvert, C. W. Clark, and C. J. Williams, "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s," Opt. Express **14**, 2062-2070 (2006).
5. K. Gordon, V. Fernandez, G. Buller, I. Rech, S. Cova, and P. Townsend, "Quantum key distribution system clocked at 2 GHz," Opt. Express **13**, 3015-3020 (2005).
6. http://www.idquantique.com
7. C. Gobby, Z. L. Yuan, and A. J. Shields, "Unconditionally secure key distribution over 50 km of standard telecom fiber," Electron. Lett. **40**, 1603- 1605 (2004).
8. R. H. Hadfield, J. L. Habif, J. Schlafer, L. Ma, A. Mink, X. Tang, S. Nam, "Quantum key distribution with high-speed superconducting single-photon detectors," submitted to CLEO/QELs 2007.
9. H. Xu, L. Ma, J. C. Bienfang, and X. Tang, "Influence of avalanche-photodiode dead time on the security of high-speed quantum-key distribution systems," CLEO/QELs 2006, Long Beach, CA, May 21-26, 2006, paper JTuH3.
10. http://optoelectronics.perkinelmer.com/catalog/Product.aspx?ProductID=SPCM-AQR-14.
11. http://www.picoquant.com/getfs.htm?products/pdm/pdmseries.htm.
12. 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 LiNbO3 waveguides," Opt. Lett. **30**, 1725-1727 (2005).
13. 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**, 1–12 (2005).
14. 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**, 1–12 (2006).
15. H. Takesue, T. Honjo, and H. Kamada, "Differential phase shift quantum key distribution using 1.3- m up-conversion detectors," Jpn. J. Appl. Phys. **45**, 5757–5760 (2006).

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

16. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304, 1–10 (2000).
17. N. I. Nweke, P. Toliver, R. J. Runser, S. R. McNown, J. B. Khurgin, T. E. Chapuran, M. S. Goodman, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, N. Dallmann, "Experimental characterization of the separation between wavelength-multiplexed quantum and classical communication channels," Appl. Phys. Lett. **87**, 1–3 (2005).
18. http://www.hcphotonics.com/waveguide.htm.
19. X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, G. C. Guo, "Faraday-Michelson system for quantum cryptography," Opt. Lett. **30**, 2632 – 2634 (2005).
20. A. Mink, X. Tang, L. Ma, T. Nakassis, B. Hershman, J. C. Bienfang, D. Su, R. Boisvert, C. W. Clark and C. J. Williams, "High speed quantum key distribution system supports one-time pad encryption of real-time video," Proc. SPIE **6244**, 62440M (2006).
21. A. Nakassis, J. Bienfang, and C. Williams, "Expeditious reconciliation for practical quantum key distribution," in Defense and Security Symposium: Quantum Information and Computation II, Proc. SPIE **5436**, 28-35 (2004).

1. Introduction

Quantum key distribution (QKD) was first introduced in 1984 [1]. Since that time both the speed and the distance of QKD systems have been greatly improved over both free space and fiber [2−5]. For fiber-based QKD over transmission distances longer than 10 km, the wavelength of the quantum signal must be in the low-loss windows of telecommunications fiber, usually around 1310 nm or 1550 nm. The available single-photon detectors that are directly sensitive to these wavelengths are InGaAs avalanche photodiodes (APDs) [6] and superconducting single-photon detectors [7]. Due to strong afterpulsing effects, InGaAs APDs are usually operated in a gated mode, typically limiting the clock rate of the system to several MHz [6]. As a result, the sifted-key rate is also limited [8]. Superconducting single-photon detectors can operate in the free-running mode and their only limitation to the sifted-key rate is the dead time, usually below 10 ns [8, 9]. Moreover, the time response of superconducting single-photon detectors can be less than 100 ps. However superconducting single-photon detectors are not generally available and need to be operated at low temperatures (typically 4 K). In contrast, silicon-based APDs (Si-APDs) are readily available and easy to operate. Their dead time is approximately 50 ns and their timing resolution is 300 ps or less [10, 11]. Unfortunately, while the peak detection efficiency of Si-APD can be as high as 70% around 650 nm their detection efficiency decreases rapidly at wavelengths longer than 1000 nm.

Recently, sum frequency generation has been applied to up-convert photons from the low-loss fiber windows to wavelengths where they can be efficiently detected by Si-APDs. With periodically poled $LiNbO_3$ (PPLN) conversion efficiencies can approach 100% [12], and this up-conversion technique was used by Takesue *et al* to demonstrate a QKD system with a secure key rate of approximately 200 bit/s over 100 km [13].

In most current QKD systems with up-conversion detectors, the quantum signal is transmitted at 1550 nm and the wavelength of the pump is shorter than the signal, for example 1310 nm [13] or 980 nm [14]. The advantage of this scheme is that the fiber loss is minimal (0.2 dB/km) around 1550 nm. On the other hand, a large amount of nonlinearly-induced dark counts occur when the high-power pump co-propagates with the signal. As a result, it has been necessary to decrease the pump power, which reduces the up-conversion efficiency. The nonlinear process generating the dark counts is widely believed to be the Raman Stokes process, in which the pump generates a photon in the signal band and then up-converts this photon to the detection wavelength [12−14], though this has not been strictly proven. In this work, we refer to the *linearly induced noise photons* as those pump photons and those classical-channel photons that are directly detected by Si-APD after leaking through the filter, and we refer to the remaining noise photons as the *nonlinearly induced noise photons*. Because the anti-Stokes component of the Raman process is much weaker than the Stokes component, the dark counts can be reduced by operating the pump light at a wavelength longer than the signal wavelength [12, 15]. However, it is difficult to find a high-power laser or a high-power amplifier beyond 1600 nm for a 1550-nm QKD system, and even if such a

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

pump source were available, the up-converted photons would not be within the optimal range of Si-APDs.

Another solution is to use 1310 nm for the signal and 1550 nm for the pump, which, for convenience, we refer to as the 1550-nm pump scheme. We also refer to the current 1550-nm signal with a 1310-nm pump as the 1310-nm pump scheme. In Ref. [12] it was shown that the dark-count rate was reduced by a factor of 50 by switching from the 1310-nm pump scheme to the 1550-nm pump scheme with the same PPLN module. However, with the notable exception of Ref. [15], the 1550-nm pump scheme is seldom applied because of the greater fiber losses at 1310 nm (>0.3 dB/km). Qualitatively speaking, at a given pump power level and at a moderate distance the sifted-key rate in the 1310-nm pump scheme is larger than in the 1550-nm pump scheme due to lower fiber loss, but the error rate is higher due to higher dark counts. We note that while the sifted-key rate may be higher in the 1310-nm pump scheme, the higher error rate decreases the extraction efficiency of secure key from the sifted key [16]. Consequently, it is not clear which scheme provides a higher secure key rate, and thus better QKD system performance.

In this paper, we compare theoretically the secure-key rate in the 1310-nm pump scheme and in the 1550-nm pump scheme. We show that the performance of the 1550-nm pump scheme can be better than the 1310-nm pump scheme in a BB84, polarization-coding QKD system with a transmission clock rate of 1.0 GHz and a mean photon number of 0.1. We also present an experimental demonstration of the performance of the 1550-nm pump scheme in a polarization-coding 1306-nm QKD system. We present a quantitative investigation of this detection scheme, focusing on polarization sensitivity and pump signal format. We also present a quantitative characterization of different dark count sources. From this characterization we are able to minimize the dark count rate. Finally, we present the results of a proof-of-principle demonstration of the B92 protocol at 1306-nm QKD system with a transmission rate of 625 MHz. We observe a secure key rate of 9.1 kbit/s over 50 km of standard single-mode fiber.

2. Theoretical comparison of 1310-nm pump scheme and 1550-nm pump scheme

In Ref. [12], Langrock *et al.* compared the performance of PPLN in the 1310-nm pump scheme and the 1550-nm pump scheme. By applying their results to a theoretical model in which we simulate BB84 polarization-coding QKD, we compare the sifted-key rates, error rates, and secure-key rates in the two pump schemes. In this model, we assume that the data rate (f_{data}) is 1 GHz and the mean photon number (μ) at the output of the transmitter (Alice) is 0.1. The fiber loss (α_{fiber}) is 0.33 dB/km and 0.20 dB/km at 1310 nm and 1550 nm, respectively. The detection efficiency and the dark count rate as a function of the pump power, $\eta_{\text{det}}(P_{\text{pump}})$ and $f_{\text{dark}}(P_{\text{pump}})$, of each up-conversion detector are extracted from Fig. 2 of [12]. In Ref. [12] the filter at the output of the PPLN has 8% more loss in the 1550-nm pump scheme than that in the 1310-nm pump scheme, and we compensated for this additional loss by increasing both the conversion efficiency and dark counts in the 1550-nm pump scheme from [12] by this factor. The additional loss of the system (α_{extra}) is set to 1.0 dB.

The sifted-key rate (SKR) as a function of pump power at a given distance is calculated as follows [4, 14]:

$$\text{SKR}\left(P_{\text{pump}}\right) = f_{\text{data}} \times \mu \times \alpha_{\text{fiber}} \times \alpha_{\text{extra}} \times \alpha_{\text{protocol}} \times \eta_{\text{det}}\left(P_{\text{pump}}\right) \times k_{\text{dead}} \tag{1}$$

where α_{protocol} represents the photon loss due to the protocol implementation, and it equals 0.5 in BB84. The factor k_{dead} accounts for the reduction of the photon detection rate due to the dead time of Si-APDs [9]. In the calculation of k_{dead} the dead time is assumed to be 50 ns.

With $\text{SKR}(P_{\text{pump}})$ obtained in Eq. (1), we can then calculate the error rate (ER) as a function of the pump power by:

$$\text{ER}\left(P_{\text{pump}}\right) = \frac{f_{\text{dark}}\left(P_{\text{pump}}\right) \times N_{\text{APD}}}{\text{SKR}\left(P_{\text{pump}}\right)} \times P_{\text{ER}} + \text{ER}_0 \tag{2}$$

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

where N_{APD} is the number of detectors used in the system. In a polarization-coding QKD system, N_{APD} = 4 in the BB84 protocol. The quantity P_{ER} is the conditional probability that an error is induced given a dark count occurs. In BB84, this probability reduces to 0.25. With 50% probability, Bob will guess an incorrect basis and the corresponding detection reports will be sifted off inducing no error. Of the remaining 50%, only half will induce an incorrect guess of the bit value and thus create an error. The background error rate (ER_0) is assumed to be 2.5% and is induced by other imperfect component performance characteristics such as finite extinction ratio of the polarizer, finite extinction ratio of the data modulator, and timing jitter in the system etc [4, 15]. The value of ER_0 is obtained from our experimental results shown in Sec. 4.3.

We then used a widely accepted algorithm [16] to calculate the secure key rate SecKR(P_{pump}) as a function of pump power from SKR(P_{pump}) and ER(P_{pump}) obtained in Eq. (1) and Eq. (2). The maximum value of SecKR(P_{pump}) then gives the optimal system performance at a given distance. In Fig. 1(a), we show this maximum secure key rate over distances up to 100 km. In Figs. 1(b), 1(c), and 1(d) we show, as an example, the variation of secure key rate, error rate, and sifted-key rate as a function of pump power at 25 km.

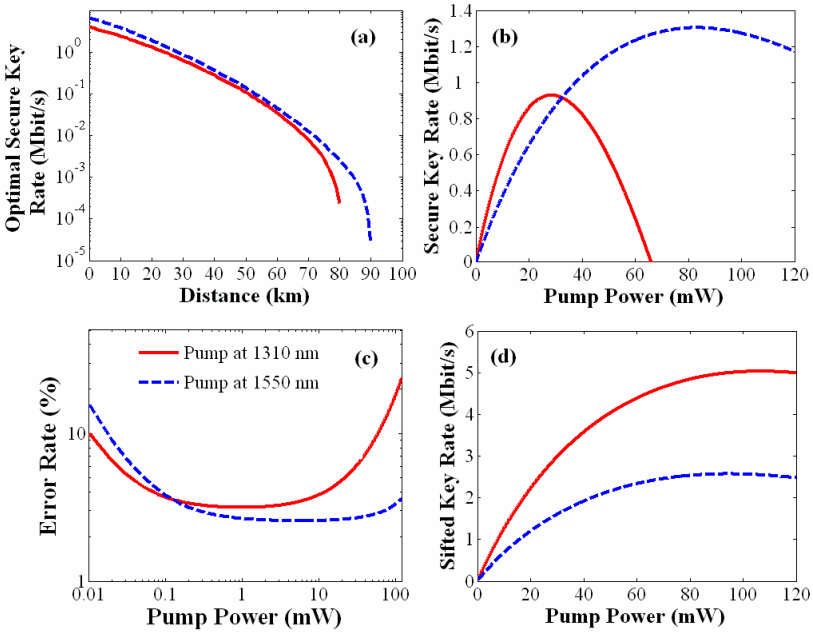

Fig. 1. (a). The optimal secure key rate at various propagation distances. (b) The secure key rate, (c) the error rate, and (d) the sifted-key rate as a function of pump power at 25 km. Red solid line, 1310-nm pump scheme. Blue dashed line, 1550-nm pump scheme.

As shown in Fig. 1, the 1550-nm pump scheme produces a higher secure key rate in polarization-coding BB84 QKD systems. Because the dark count rate is lower in the 1550-nm pump scheme than in the 1310-nm pump scheme, it is possible to operate at relatively high pump power to achieve high conversion efficiency (thus large sifted-key rate) and low error rate [see Figs. 1(b) and 1(c)]. By comparison, in the 1310-nm pump scheme the conversion efficiency (the sifted-key rate) is compromised, *i.e.*, the pump power is reduced, to achieve an acceptably low dark count rate and thus low error rate. Moreover, even with reduced pump power the 1310-nm scheme incurs higher error rates than the 1550-nm scheme, thus requiring a larger amount of sifted-key bits to generate a given amount of secure key bits. Thus, in the 1550-nm pump scheme the secure key rate is higher regardless of higher signal losses in the fiber.

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

The situation could be different in other protocols such as differential-phase-shifted (DPS) protocol. In DPS system, one does not need to sift off the detected photons with incompatible bases and therefore the sifted-key rate is higher. In this case, a given amount of dark counts induces less error. In another words, the DPS is less sensitive to the dark counts when compared with the BB84 system. Such higher tolerance of dark counts has small effect in the 1550-nm pump scheme because in this scheme the dark count rate is already low while in the "noisy" 1310-nm pump scheme, the improvement is more significant. Consequently, we speculate that in DPS the advantage of the 1310-nm pump scheme over the 1550-nm pump scheme would be diminished, and that after a certain distance the 1550-nm pump scheme may even out perform the 1310-nm scheme.

In general, our results indicate that under certain circumstances 1550-nm pump scheme can provide better performance despite the higher transmission loss. This is particularly true when one wishes to distribute a higher secure key rate over a relatively short distance. In this case, the benefit of the lower dark count rate predominates over the higher fiber loss in the 1550-nm pump scheme.

The 1550-nm pump scheme has another advantage: It is possible to co-propagate the 1310-nm quantum channel and a 1550-nm classical channel in the same fiber. The large separation in wavelengths prevents the classical channel from inducing large amounts of noise in the quantum channel. It has been shown that noise increases dramatically as one allocates the quantum channel in the same wavelength band as that of the classical channel [17]. One can also use separate fibers to carry the classical and the quantum channel but then may need to extract the clock signal from the quantum channel itself: Different fiber fluctuate differently and the clock extracted from the classical channel received from one fiber may not synchronize the quantum channel in another fiber. This clock issue would be more stringent when one transmits the quantum key in a higher clock rate.

3. Up-conversion detector using a pump at 1550 nm

Figure 2 shows the configuration of the up-conversion detector. A 1557-nm CW light is modulated to form an optical pulse train, which is then amplified using an erbium-doped fiber amplifier (EDFA). An optical filter, FLT_0, with a full-width half maximum (FWHM) of 7 nm is used to suppress noise at the output of the EDFA, particularly between 1000 nm and 1300 nm. As we will show later, noise in this region can induce a large amount of dark counts and the wavelength-division multiplexer (WDM) may not be sufficient to suppress it. After FLT_0, the 1557-nm pulse is split by a 3-dB coupler so that we can pump two up-conversion detectors with one source. After polarization control on the quantum channel is achieved, the quantum-channel signals at 1306 nm are combined with the 1557-nm pumps by the WDMs and sent to PPLN waveguides [18]. The 710-nm outputs of PPLN waveguides are further filtered and sent to Si-APDs [10]. The output of $PPLN_2$ is coupled to a 700-nm single mode fiber (5-μm core), which cuts off the strong 1557-nm pump light. The FLT_2 contains two filters: a 20-nm band-pass filter and a short-pass filter. The short-pass filter attenuates the light between 730 nm and 1000 nm by more than 50 dB. This combination of filters helps to attenuate the light by more than 80 dB between 730 nm to 1000 nm, above which the filtering is insignificant.

Due to a manufacturing fault, the output of $PPLN_1$ is coupled to a standard single-mode fiber. As a result, the strong 1550-nm pump is not attenuated sufficiently after $PPLN_1$ and we use another short-pass filter to replace the one used in FLT_2. The short-pass filter in FLT_1 sufficiently attenuates light between 730 nm and 1600 nm by approximately 50 dB but around 710 nm it has a larger loss than the one in FLT_2. This inappropriate fiber pigtail also causes the optical pulse to be broadened by nearly 100 ps by multi-mode propagation of the 710-nm signal. In Table 1, we list the transmittance parameters of the two up-conversion detectors. By multiplying the transmittance of all components (top six entries) in Table 1 except for the input coupling of PPLN at 1557 nm, and comparing the results with the measured overall efficiency (last entry), we can estimate that the internal quantum conversion efficiency of the two PPLNs is almost 100%. However, the coupling loss is significantly larger than those in [12] and therefore degrades the overall detection efficiency.

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

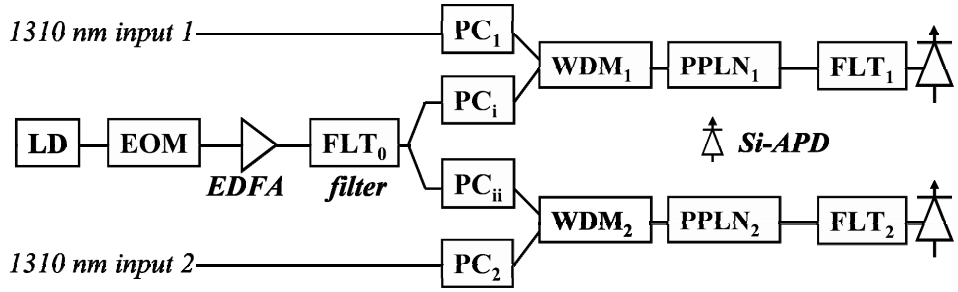

Fig. 2. Configuration of the 1550-nm pump up-conversion detectors. LD: Laser diode; EOM: Electric-optic modulator ($LiNbO_3$); EDFA: Erbium-doped fiber amplifier; FLT: Optical filter; PC: Polarization controller; WDM: Wavelength-division multiplexer for 1306 nm and 1550 nm; PPLN: Periodically-poled $LiNbO_3$ module.

Table 1. Transmittance of different components and overall detection efficiencies of the 1550-nm pump up-conversion detectors

Components	$PPLN_1$	$PPLN_2$
PC and WDM around 1306 nm	70%	74%
Input coupling of PPLN around 1550 nm*	52%	71%
Input coupling of PPLN around 1310 nm*	44%	59%
Output coupling of PPLN around 710 nm*	92%	77%
Filter before APD*	75%	88%
APD efficiency around 710 nm*	70%	70%
Overall efficiency	15%	20%

*: These parameters are provided by the manufactures. Others are measured.

Next we investigate three properties of the PPLN-based up-conversion: polarization sensitivity, influence of the pump format, and effects of the pump noise.

3.1 Polarization sensitivity of PPLN

Up-conversion in PPLN is polarization sensitive. In Fig. 3 we show the dependence of the conversion efficiency on the orientation of the 1306-nm input polarization state in $PPLN_1$. Similar results were obtained for $PPLN_2$. The deviation angle is the angle (in Jones space) between the given input polarization state and the state at which the conversion efficiency is maximized. The conversion efficiency is normalized to 1 by dividing by its maximum value. As shown in the figure, the polarization extinction ratio of PPLN is more than 25 dB.

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

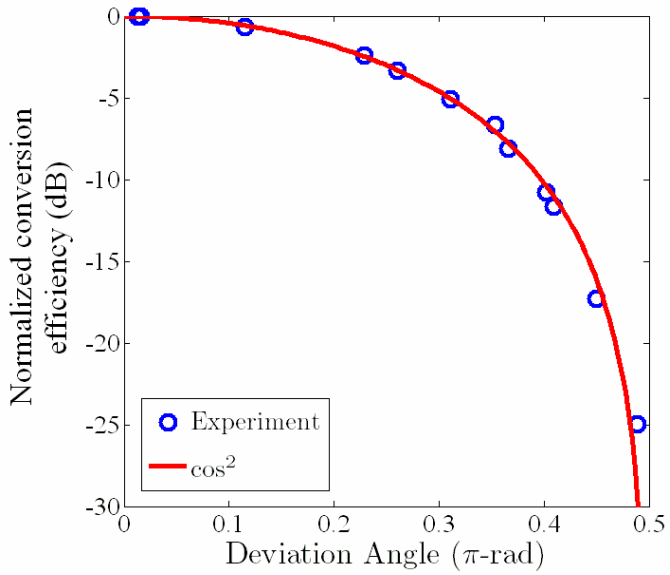

Fig. 3. The normalized conversion efficiency as a function of deviation angle of the input 1306-nm signal of the $PPLN_1$. The *x*-axis shows the deviation angle in unit of π-rad. The deviation angle is the angle between the given polarization state and the state at which the conversion efficiency is maximized. Open circle: Measurement results; Solid line: $\cos^2$ curve. The polarization sensitivity of $PPLN_2$ is similar.

In a phase-coding system it is possible to use a faraday mirror to implement a polarization insensitive interferometer, making it necessarily to stabilize only the static phase [19]. If one were to use PPLN-based up-conversion detectors in such a system it would also be necessary to optimize the input polarization states of the incoming signal when a PPLN is applied. By comparison, polarization-coding systems are inherently polarization sensitive and the application of a PPLN does not add an additional dimension of complexity. Moreover, with a polarization extinction ratio higher than 25 dB, PPLN waveguides act as an additional polarizer.

The conversion efficiency of PPLN is also dependent on the polarization state of the pump signal. When compared with the quantum signal, the pump signal propagates only a short distance (typically less than 10 m) to PPLN and its polarization state can be stable for hours.

3.2 Comparison of pump format

As shown in Fig. 2, the pump can be formatted to a periodic pulse train that is bit-synchronized to the signal. We can also turn off the pulse modulation so that the pump becomes a continuous-wave (CW), a format used in previous works [12−15]. For both CW and pulsed pumps, the dark count rate and the conversion efficiency of the two up-conversion detectors are shown in Fig. 4. The signal is a 625-MHz random pulse train. The FWHMs of the signal and the pump are 220 ps and 620 ps respectively.

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

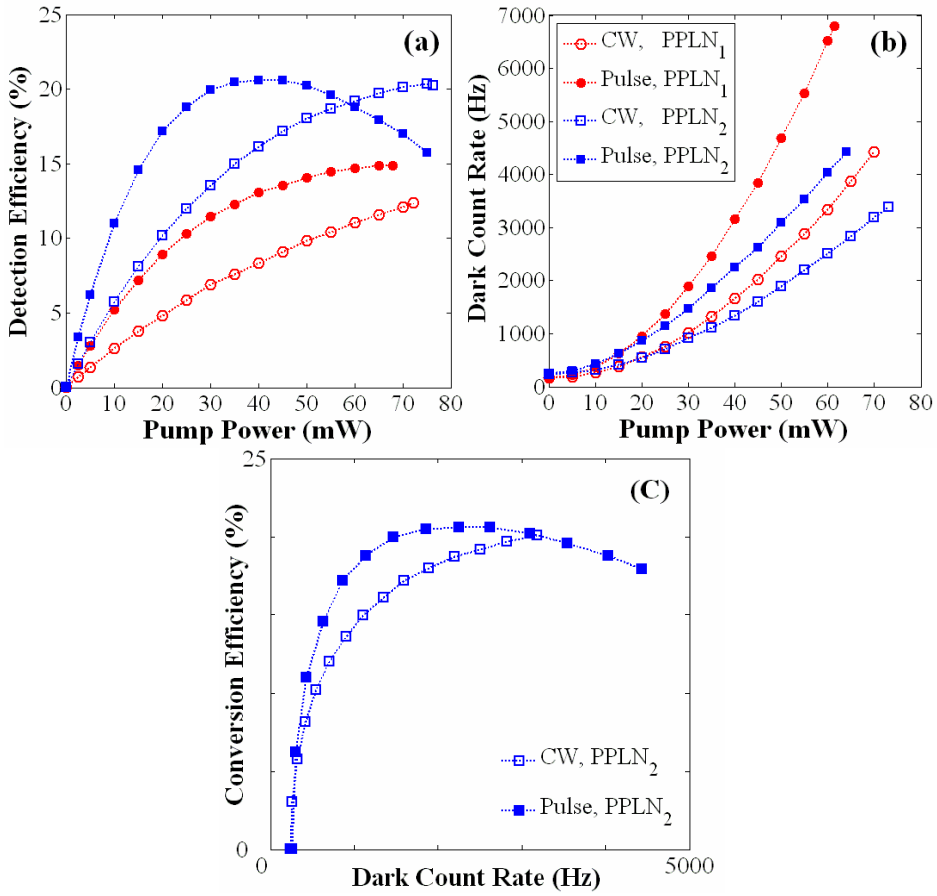

Fig. 4. The detection efficiency (a) and dark count rate (b) as a function of pump power at the PPLN input. Four cases are studied: two up-conversion detectors, each with CW and pulsed pump, as shown in the inset of Fig. 4(b). (c) The conversion efficiency vs the dark count rate in $PPLN_2$.

Both our signal pulse and pump pulse are generated by modulating CW light with a pulse train from a 625-MHz pattern generator. The rise time and the fall time are approximately 100 ps in both signal and pump as we measured with a 12.5-GHz detector followed by a 40-GHz oscilloscope. Therefore, when we set the signal pulse width (FWHM) to 220 ps and the pump pulse width to 620 ps, the full width at 90% of the maximum of the pump pulse is larger than the full width at 10% of the maximum of the signal. This allows nearly all of the signal photons to be converted inside the PPLN with proper pump power [See Table 1 and Fig. 4(a)] and the timing jitter of the system will not induce significant fluctuation in the conversion efficiency.

When the pump pulse is much wider than the signal pulse, the internal conversion efficiency of PPLN is determined by the peak power. In this case, at a given peak pump power and thus a given detection efficiency, the dark counts increase as one increases the duty ratio (pulse width) of the pump because the dark counts now can be generated in wider time window. Consequently, at a given detection efficiency the CW light (duty ratio of 1) induces more dark counts than the pulsed pump. By comparison, at a given average pump power the peak power of the pulse is higher than that of the CW. Moreover, the function $f_{dark}(P_{pump})$ has a large amount of second-order components, *i.e.*, nonlinearly induced dark counts. Consequently, as shown in the figure, the pulsed pump generates more dark counts than the CW pump when the average pump power is the same. Nevertheless, less average pump power

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

is needed in the pulsed format to achieve a given detection efficiency, resulting in lower dark counts, as shown in Fig. 4(c). For example, in the pulsed case, the detection efficiency is 15% and dark count rate is 660 count/s when the average pump power of $PPLN_2$ is set to 16 mW. In the CW case, one needs 35 mW of average pump power to achieve the same detection efficiency of 15% and at that power level the dark count rate is 1100 counts/s. The pulse pump helps to reduce the dark count rate.

Above all, the pump pulse needs to be wider than the signal pulse to achieve 100% of internal conversion efficiency. In the mean time, the wider pump pulse induces more dark counts. There exists an optimal pump pulse width, whose value varies with signal pulse width, timing jitter, pulse shape etc.

As shown in Fig. 4, the performance of the up-conversion detector based on $PPLN_2$ is better than the detector based on $PPLN_1$. The peak detection efficiency of $PPLN_2$ is higher due to lower loss components, as shown in Table 1. Moreover, the $PPLN_1$ detector requires more pump power to achieve a given detection efficiency due to the higher input coupling losses around 1550 nm. $PPLN_1$ also has a larger amount of dark counts. This larger amount of dark counts is induced by various effects. For example, the output coupling of $PPLN_1$ is higher than $PPLN_2$ yielding more noise photons coupled out of the $PPLN_1$ waveguide. The blockage of the short-pass filter in FLT_1 is less than that in FLT_2 so that more noise photons are blocked in FLT_2. In addition, the exact structure of the PPLN waveguide could also play a role. However, we are unable to characterize the waveguide.

3.3 Filtering of the pump noise

As shown in Fig. 4(a), we attain dark count rates around several thousands counts per second, which is significantly lower than those of shorter-wavelength-pump schemes [12–14]. In achieving such a low dark count rate, the 'post-filtering' after PPLN (FLT_1 and FLT_2) alone is not sufficient and the optical band-pass filter before PPLN (FLT_0) is also important. FLT_0 blocks a large amount of EDFA noise, particularly the noise between 1000 nm and 1300 nm shown in Fig. 5(a). The noise in this region can induce a large amount of noise photons which cannot be blocked by FLT_1 and FLT_2, see Fig. 5(b). The WDMs located before the PPLNs are specified by the manufacturer to filter out the light between 1300 nm and 1330 nm by more than 20 dB but they do not block the noise between 1000 nm and 1300 nm.

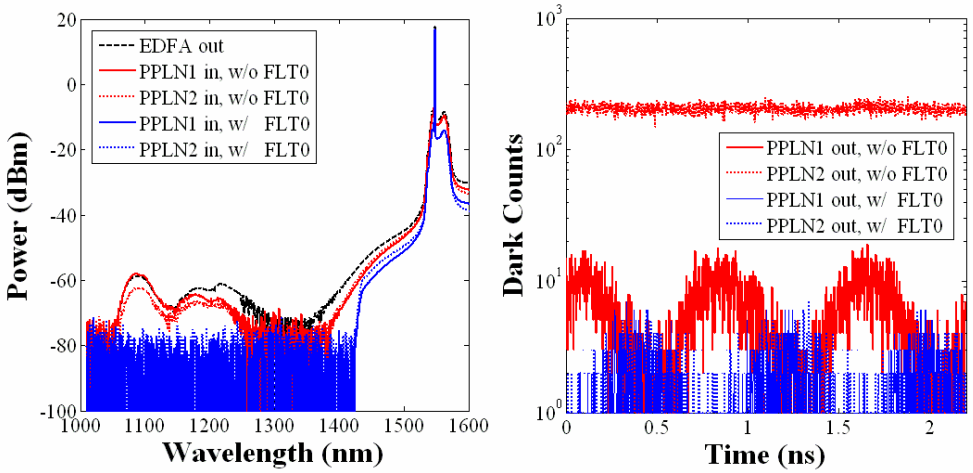

Fig. 5. (a). The optical spectrum of the pump light immediately after the EDFA and at the input of the PPLNs, each measured with and without FLT_0. (b) The photon counts over time collected by a photon counting card at the output of two up-conversion detectors, each with and without FLT_0. During the measurement, no signal at 1306 nm was present and only the pump light was sent to the PPLNs. The pump power was approximately 40 mW before each PPLN.

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

As shown in Fig. 5(b), in each detector the dark counts are induced by the EDFA noise via different processes and thus have different magnitudes (4.0×10^4 counts/s in the $PPLN_1$ and 1.1×10^6 counts/s in the $PPLN_2$). An EDFA noise photon can be directly detected by the Si-APD (linear process) or it can be up-converted by the 1550-nm pump to a photon around 710 nm and then detected by the Si-APD (nonlinear process). The linearly induced dark counts resemble white noise while the nonlinearly induced ones would exhibit the pulse pattern of the pump. As shown in the figure, most of the $PPLN_1$'s dark counts are induced nonlinearly from the EDFA noise and the pulsed pump. The linearly induced dark counts are negligible because the short-pass filter successfully blocks the EDFA noise before Si-APD. In the $PPLN_2$ detector, the short-pass filter cannot block the light beyond 1000 nm sufficiently and the 710-nm single-mode fiber is not sufficient to block the photons between 1000 nm and 1300 nm. Therefore, a large amount of noise photons reach the Si-APD inducing a large amount of white-noise-like dark counts. Using FLT_0 to suppress the EDFA noise, we greatly reduced the dark counts in both detectors, as shown in Fig. 5(b). The dark count rate with FLT_0 has already been shown in Fig. 4.

Above all, using pulsed pump light at 1557-nm and a signal at 1306 nm, and applying proper filtering, we achieve substantially lower dark count rates in the up-conversion detector. When the pump power is set to 40 mW, the dark count rate is 3.2×10^3 counts/s in the $PPLN_1$ detector and is 2.2×10^3 counts/s in the $PPLN_2$. Such dark count rates are nearly two orders of magnitude lower than that given by the 1310-nm pump scheme [12].

4. Experimental study of a QKD system with the 1310-nm-pumping up-conversion detector

4.1 System configuration

We applied the 1550-nm pump up-conversion detector to our B92 polarization coding QKD system shown in Fig. 6. The QKD system uses a custom printed circuit board with a field-programmable gate array (FPGA), which is attached to Alice's and Bob's computers via the PCI bus, to handle all activities up to and including the sifting protocol layer. A more complete operational description can be found in Ref. [20]. Alice's board generates a random stream of quantum data for each of the two quantum channels. To polarization-encode the quantum channel from these electrical quantum data streams, we start by modulating a 1306-nm CW light into a 625-MHz pulse train with a FWHM of 220 ps and evenly splitting it into two polarization channels. Each pulse train is further modulated by one of the 625-Mbit/s quantum channel data streams. The two complementary quantum streams are passed through polarizers and then combined by a 45-degree polarization-maintaining combiner with their polarization states being separated by 45 degrees in the Jones space. The combined 1306-nm quantum stream is attenuated to a mean photon number of 0.1 per bit and then multiplexed with the 1480-nm classical channel via a WDM and transmitted over a standard single-mode fiber.

At Bob, another WDM is used to demultiplex the quantum and the classical channels. The 625-MHz clock is extracted from the classical data stream and is used to generate the pump pulse train with a FWHM of 620 ps. A 3-dB fiber coupler splits the quantum signal evenly, which will be detected by the up-conversion detectors. As described in Section 3 and shown in Fig. 2, the polarization decoding is performed using PCs for polarization compensation of the fiber transmission and PPLNs as polarizers. Bob's board samples the electrical output of the APDs searching for detection events from which it builds its version of the sifted key stream. The location of these keys are sent to Alice via Bob's 1580 nm classical channel, using the same fiber, so Alice can formulate her sifted key stream from her stored copy of the quantum data stream. Each sifted key stream is passed to the computers via their PCI bus where reconciliation algorithms correct errors between Bob and Alice's key stream versions followed by privacy amplification algorithms [21] to produce the duplicate streams of secret key.

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

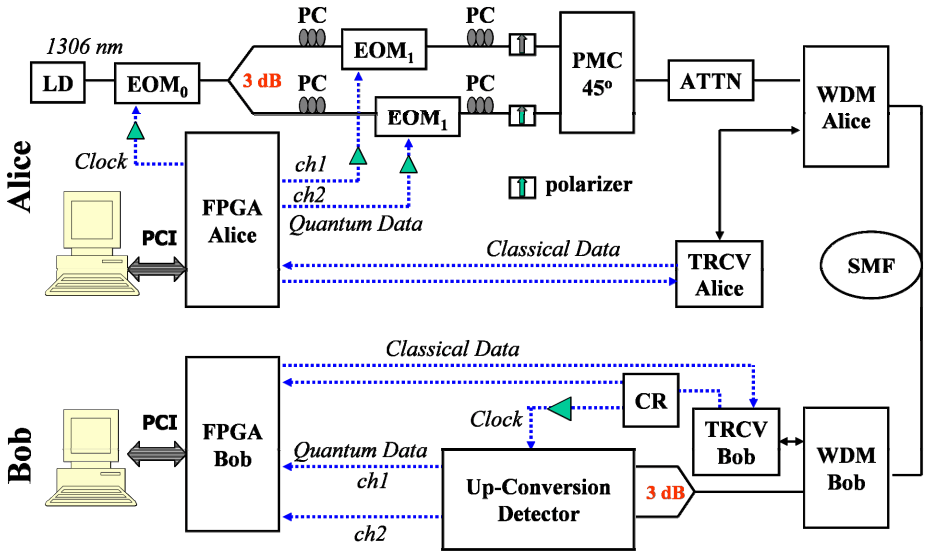

Fig. 6. The B92 polarization coding QKD system. **LD**: Laser diode; **EOM**: Electric-optic modulator ($LiNbO_3$); **PC**: Polarization controller; **PMC-45°**: Polarization maintaining combiner that combines two light signals that are separated by 45 degrees; **ATTN**: Optical attenuator; **WDM**: Wavelength-division multiplexer; **SMF**: Standard single-mode fiber; **TRCV**: Optical transceiver; **CR**: Clock recovery module; **FPGA**: Custom printed circuit board controlled by a field-programmable gate array; **PCI**: PCI connection; **Up-conversion detector**: See Fig. 2; **Dotted line**: Electric cable; **Solid line**: Optical fiber.

As the propagation distance between Alice and Bob increases, the size of the memory buffer on Alice's board becomes insufficient. All the data in Alice's buffer has been transmitted before Bob's response returns to Alice allowing that space to be freed. This causes Alice to stall any new transmissions until Bob's response is received. Although we are fabricating boards with increased memory, in the current system this periodic stalling reduces the measured key rates directly proportional to the stall time. In this paper we corrected the measured key rates to obtain the accurate key rates, *i.e.*, the sifted-key rate we would achieve if the system has enough memory and thus the transmission would not stall. We used our code to record the total number of quantum bits Alice sent and the total number of sifted keys Bob received. From this number of bits sent we obtain the effective time over which we actually transmitted quantum bits and generated sifted keys. Dividing the total number of sifted keys by this effective time, we obtained an accurate value of the sifted-key rate. We calculated the secure-key rates using the sifted-key rates and the error rates.

4.2. Dark counts induced by the classical channel

The 1306 nm quantum channel is uni-directional and the classical channel is bi-directional, all share a common single fiber. In the classical channel Alice sends at 1480 nm and Bob sends at 1580 nm. The output power of the classical channel is approximately 0 dBm. The classical channel could induce dark counts in two ways [17]: directly from transceiver noise, and via nonlinear effects. The transceiver emits a certain amount of optical noise around 1306 nm. Some of this noise will leak into the PPLN and be up-converted. The 1480-nm and 1580-nm signals may nonlinearly generate photons around 1306 nm via the anti-Stokes Raman process and these nonlinearly induced 1306-nm photons may also be up-converted to 710 nm in the PPLNs. In Fig. 7 we show the extra dark count rate induced by the classical channel at various distances. To obtain the extra dark count rate, we measure the dark count rate when one or both of the transceivers are on, and then subtract the results of the dark count rate when both

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

transceivers are off (Fig. 4). The photon leakage can be evaluated by the extra dark counts in the back-to-back connection while the nonlinearly induced noise photon effect will vary over the transmission distance.

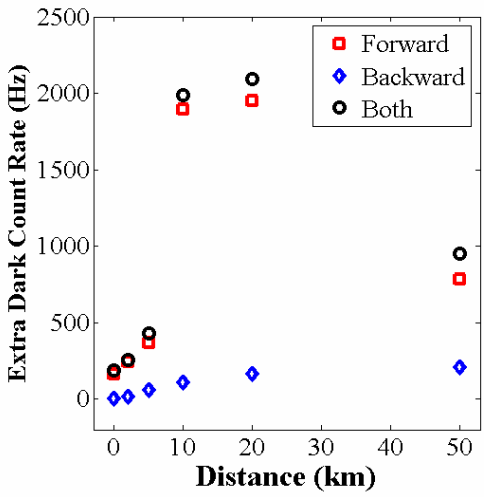

Fig. 7. The extra dark count rate induced by the classical channel in the $PPLN_1$ detector in three cases: square, only transceiver at Alice is on; diamond, only transceiver at Bob is on; circle, both transceivers are on. The $PPLN_2$ detector exhibits similar behaviors.

As shown in the figure, the number of noise photons leaked is small and the dark counts are mainly induced by the anti-Stokes Raman process, particularly from the 1480-nm light propagating from Alice to Bob (forward anti-Stokes). The forward anti-Stokes is stronger than the backward one (the backward anti-Stokes noise generated by the 1580-nm light from Bob) because the 1480-nm light is 100 nm closer to the 1306-nm than the 1580-nm light. The figure shows that the amount of dark counts induced by the forward anti-Stokes increases up to distances of 20 km because the accumulated anti-Stokes process predominates over the accumulated fiber loss. Above 20 km the 1480-nm light is attenuated so that a smaller amount of anti-Stokes noise is newly generated. The anti-Stokes noise generated below 20 km is also attenuated by the fiber loss. By comparison, the amount of dark counts induced by the backward anti-Stokes noise also increases with distance but in this case it saturates after 20 km: both the 1580-nm light and backward anti-Stokes noise are sufficiently attenuated by the fiber loss and therefore almost no additional anti-Stokes noise is reflected back as the fiber length reaches beyond 20 km. In general, both the forward propagating and the backward propagating classical channels could induce a significant amount of dark counts via the anti-Stokes Raman process, particularly when the classical channel is not sufficiently longer than the quantum channel. In these two cases, after approximately 20 km, the amount of the dark counts induced by the forward anti-Stokes reduces, while the dark counts induced by the backward anti-Stokes saturates. A longer-wavelength transceiver was not available for these experiments. Therefore, we chose the 1480-nm transceiver at Alice (forward) and the 1580-nm transceiver at Bob (backward) so that the dark counts at 50 km are small.

4.3. System performance and discussion

The system performance is shown in Fig. 8. During the measurements, the pump power is fixed at 40 mW. After correcting the reduction of the key rate due to the periodic stalling, the sifted-key rate is 2.5 Mbit/s with a back-to-back connection (0 km), 1 Mbit/s at 10 km, and 60 Kbit/s at 50 km. The error rate is approximately 3% for back-to-back, remains below 4% for up to 20 km, and reaches 8% at 50 km. The finite extinction ratio of the modulator and the

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

timing jitter of the system induce a background error rate ER0 of approximately 2.5% and the remaining portion of the error rate is from the dark counts, generated by both the pump light and the classical channel, as described earlier. We also calculated the sifted-key rate and error rate using Eq. (1) and Eq. (2). These calculated values agree well with our experimentally measured values. In Fig. 8(b) we use our experimentally measured SKF and ER to calculate the secure key rate using two different algorithms, [20, 21] and [16]. They yielded similar results. We were able to generate secure keys in real time and used them as a one-time-pad for a continuous 200-Kbit/s encrypted video transmission over 10 km even though we incurred periodic stalling due to the limited buffer size.

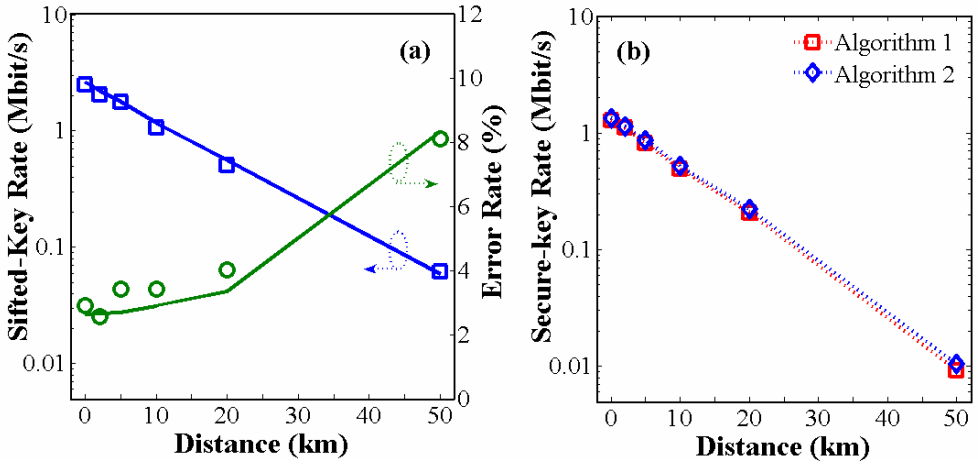

Fig. 8. The system performance of the B92 polarization-coding QKD system with the 1557-nm up-conversion detector. (a) Left blue line: the sifted-key rate calculated in Eq. (1); Left blue square: the sifted-key rate measured in the experiment; Right green line: the error rate calculated in Eq. (2); Right green circle: the error rate measured in the experiment. (b) The secure-key rate calculated using algorithm 1 [20, 21] and algorithm 2 [16]. The calculation is coded on the sifted-key rate and error rate measured in the experiment.

Although we fixed the pump power close to the maximum up-conversion efficiency, the error rate remains small until 20 km due to the low dark count rate of the 1550-nm up-conversion detector. A secure-key rate of approximately 9.1 Kbit/s is achievable at 50 km.

The above work is only a proof-of-principle experiment. The system performance can be further improved using protocols more efficient than B92, for example, BB84 protocol. Moreover, a more secure protocol such decoy-state B84 allows for a higher mean photon number. We used a data rate of 625 Mbit/s but it could be upgraded to 1.0 Gbit/s without much increase in the error rate [13]. Finally our PPLNs have a large coupling loss and it is possible to reduce this loss below 80%, according to [12]. These upgrades could improve the system performance.

5. Summary

We have shown that a 1306-nm QKD system with a 1550-nm pump up-conversion detector can yield better system performance, particularly when the system is aimed at a high secure-key rate over relatively short distances. Such detection systems have high polarization sensitivity, with a polarization extinction ratio larger than 25 dB. We find that pulsing the pump light helps to reduce the dark count rate while the internal conversion efficiency remains close 100% as long as the pump pulse is sufficiently wider than the signal pulse. The optical noise in the pump light could induce dark counts via both linear and nonlinear processes. Proper filtering after the PPLN is important to reduce the dark counts. We find that it is also important to filter out the pump noise before the PPLN, and by this means we reduced the dark count rate from 1.1 MHz to 2.2 kHz. In addition, we characterized the dark

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007

counts induced by the classical channel propagating in the same fiber. We find that in this system most of the dark counts are generated via the anti-Stokes Raman process. The dark count rate generated by forward anti-Stokes noise increases with propagation distance, while above 20 km it decreases as the accumulated fiber loss predominates over the generation of new anti-Stokes noise. The dark counts generated by the backward anti-Stokes noise also increase up to 20 km and then saturates. We have applied the up-conversion detector to a B92 polarization-coding QKD system and observed approximately 500 Kbit/s and 9.1 Kbit/s of secure-key rates at 10 km and 50 km, respectively. Even with the periodic stalling due to insufficient memory, we find that the system can generate secure keys in real time for one-time-pad encryption of continuous 200 Kbit/s encrypted video transmission over 10 km. More importantly, with the low dark count rate in the 1550-nm pump up-conversion detector we expect significant improvements when one applies more advanced protocols, better PPLN modules, and higher data rates.

Acknowledgment

The authors acknowledge the support of the DARPA QuIST program and NIST Quantum Initiative. We thank Jingyun Fang for his suggestions on the up-conversion detectors and thank Joshua Bienfang for the technical discussions and support on the QKD system.

#79866 - $15.00 USD Received 7 Feb 2007; revised 16 May 2007; accepted 20 May 2007; published 30 May 2007