Continuous-variable quantum key distribution with 1 Mbps secure key rate

Duan Huang,[1] Dakai Lin,[1] Chao Wang,[1] Weiqi Liu,[2] Shuanghong Fang,[2] Jinye Peng,[2] Peng Huang,[1,3] and Guihua Zeng[1,2,4]

[1]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Laboratory on Navigation and Location-based Service, and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China*
[2]*College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China*
[3]*huang.peng@sjtu.edu.cn*
[4]*ghzeng@sjtu.edu.cn*

Abstract: We report the first continuous-variable quantum key distribution (CVQKD) experiment to enable the creation of 1 Mbps secure key rate over 25 km standard telecom fiber in a coarse wavelength division multiplexers (CWDM) environment. The result is achieved with two major technological advances: the use of a 1 GHz shot-noise-limited homodyne detector and the implementation of a 50 MHz clock system. The excess noise due to noise photons from local oscillator and classical data channels in CWDM is controlled effectively. We note that the experimental verification of high-bit-rate CVQKD in the multiplexing environment is a significant step closer toward large-scale deployment in fiber networks.

OCIS codes: (270.0270) Quantum optics; (270.5565) Quantum communications.

References and links

1. L. B. Samuel and V. L. Peter, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513 (2005).
2. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621 (2012).
3. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
4. F. Grosshans, G. Van Asshe, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
5. A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A **77**, 042325 (2008).
6. R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**, 190503 (2006).
7. M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," Phys. Rev. Lett. **97**, 190502 (2006).
8. R. Renner and J. I. Cirac, "de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," Phys. Rev. Lett. **102**, 110504 (2009).
9. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
10. F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks," Phys. Rev. Lett. **109**, 100502 (2012).
11. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**, 070501 (2015).
12. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nat. Photonics **1**, 343–348 (2007).

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

13. K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Appl. Phys. Lett. **104**, 051123 (2014).
14. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378–381 (2013).
15. Y. M. Chi, B. Qi, W. Zhu, L. Qian, H. K. Lo, S. H. Youn, A I Lvovsky, and L. Tian, "A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution," New J. Phys. **13**, 013003 (2011).
16. D. Huang, J. Fang, C. Wang, G. Q. He, P. Huang, R. H. Yang, and G. H. Zeng, "A wideband balanced homodyne detector for high speed continuous variable quantum key distribution systems," presented at the 3rd international conference on quantum cryptography, Waterloo, Canada, 5–9 Aug. 2013.
17. P. Jouguet and S. Kunz-Jacques, "High performance error correction for quantum key distribution using polar codes," Quantum Inf. Comput. **14**, 329-338 (2014).
18. P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **84**, 062317 (2011).
19. S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle–Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," New J. Phys. **11**, 045023 (2009).
20. P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle–Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, "Field test of classical symmetric encryption with continuous variables quantum key distribution," Opt. Express **20**, 14030–14041 (2012).
21. S. Ast, M. Mehmet, and R. Schnabel, "High-bandwidth squeezed light at 1550 nm from a compact monolithic PPKTP cavity," Opt. Express **21**, 13572–13579 (2013).
22. S. Ast, A. Samblowski, M. Mehmet, S. Steinlechner, T. Eberle, and R. Schnabel, "Continuous-wave nonclassical light with gigahertz squeezing bandwidth," Opt. Lett. **37**, 2367–2369 (2012).
23. J. Lodewyck, T. Debuisschert, R. Tualle–Brouri, and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution," Phys. Rev. A **72**, 050303 (2005).
24. P. Huang, G. Q. He, and G. H. Zeng, "Bound on noise of coherent source for secure continuous-variable quantum key distribution," Int. J. Theor. Phys. **52**, 1572-1582 (2013).
25. P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," Phys. Rev. A **86**, 032309 (2012).
26. Y. Shen, X. Peng, J. Yang, and H. Guo, "Continuous-variable quantum key distribution with Gaussian source noise," Phys. Rev. A **83**, 052304 (2011).
27. H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek, and S. Schiller, "Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements," Opt. Lett. **26**, 1714–1716 (2001).
28. R. Okubo, M. Hirano, Y. Zhang, and T. Hirano, "Pulse-resolved measurement of quadrature phase amplitudes of squeezed pulse trains at a repetition rate of 76 MHz," Opt. Lett. **33**, 1458–1460 (2008).
29. B. Qi, W. Zhu, L. Qian, and H. K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," New J. Phys. **12**, 103042 (2010).
30. R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," arXiv preprint arXiv:1412.1403 (2014).
31. P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," New J. Phys. **12**, 063027 (2010).
32. K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," Phys. Rev. X **2**, 041010 (2012).
33. J. Lodewyck, M. Bloch, R. García–Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).
34. Q. D. Xuan, Z. S. Zhang, and P. L. Voss, "A 24 km fiber-based discretely signaled continuous variable quantum key distribution systems," Opt. Express **17**, 24244 (2009).
35. D. K. Lin, D. Huang, P. Huang, J. Y. Peng, and G. H. Zeng, "High performance reconciliation for continuous-variable quantum key distribution with LDPC code," Int. J. Quantum Inform. **13**, 1550010 (2015).
36. IEEE 10GBASE-ER 802.3ae-2002.

1. Introduction

Continuous-variable quantum key distribution (CVQKD) has been explored as an efficient approach to achieve possibly high secret key rates [1, 2]. It has been shown that the CVQKD has the potential advantage since the first experimental demonstration of the Gaussian-modulated coherent states (GMCS) protocol [3, 4]. In the protocol, the key information is encoded by Alice in the amplitude and phase of coherent light which are according to a centred Gaussian

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

distribution, and subsequently performed shot-noise-limited homodyne detection at Bob's side. The secret key shared by two distant partners, Alice and Bob, is extracted by using classical reconciliation [5] and privacy amplification. The security of the QKD scheme stems from Heisenberg inequalities has been demonstrated, in principle, secure against general collective eavesdropping attacks, which are optimal in both the asymptotic case [6–8] and the finite-size regime [9–11].

However, the most significant progresses in QKD were performed with discrete-variable (DV) systems but not CV systems [12–14]. This is due to the fact that the CVQKD scheme was initially plagued with various kinds of problems on extending the secure communication distance and increasing secure key rates. Recently, the issue pertaining to the secure distance was reduced in the work of P. Jouguet *et al.*, i.e., 80 km CVQKD [14]. On the other hand, there are two major hurdles that limit the secure key rate. The first is the available bandwidth of shot-noise-limited homodyne detector [15, 16] and the second is the limited speed and efficiency of classical reconciliation [17, 18]. To date, most of field test of CV systems were still working at 0.5 MHz within 25 km transmission distance [19, 20]. Therefore, to increase the secure key rate, the obvious way is to improve the currently achievable transport frequencies.

In this paper, we demonstrate a high-speed CVQKD experiment over a fiber link in a coarse wavelength division multiplexers (CWDM) environment. Record secure key rate of 1 Mbps is achieved, and it is corresponding to the highest key rate of CVQKD implementation over a fibre link yet demonstrated. The result is realized by using two following major advanced techniques: the use of 1 GHz shot-noise-limited homodyne detector and the implementation of a 50 MHz clock system, where the latter includes a 5 GS/s synchronous sampling procedure and a high-speed error-correcting procedure.

The paper is organized as follows. In Section 2, we describe specific techniques used in the experiment, including the CWDM setup for real-time high-bit-rate QKD and the high-speed shot-noise-limited homodyne detection. In Section 3, we analyze and control the excess noise due to noise photons from local oscillator (LO) and classical data channels in CWDM. In Section 4, we report the experimental results of the CVQKD system and Section 5 concludes the paper.

2. System description

2.1. Experimental set-up

We integrate the CVQKD setup into a CWDM environment as shown in Fig. 1(a). The classical communication channels are implemented with standard Small Form-factor Pluggable (SFP) data transceivers. We multiplex the quantum channel along with three classical channels using off-the-shelf CWDM modules instead of the standard dense wavelength division multiplexers (DWDM). This is because such a kind of coexistence architecture allows us to achieve a larger wavelength separation, so that quantum signals are impacted as minimally as possible by classical channel. The multiplexer (MUX) and the demultiplexer (DEMUX) modules of CWDM feature an insertion loss of 0.8$\sim$1.2 dB at passbands, centered at 1550, 1570, 1590, and 1610 nm. We use a 25 km SMF-28 fiber spool with a typical attenuation coefficient α of 0.2 dB/km at the wavelength of 1550 nm. To suppress the Raman scattering during the propagation process, the 1550 nm band is assigned to the quantum subsystem and the launch power of SFP transceivers at 1590 nm and 1610 nm band is attenuated as much as possible. The sensitivity of SFP receiver, defined as the minimum receiving optical power required to achieve a bit error ratio no higher than 10^{-12}, is measured to be -32 dBm at a data modulation rate of 1.25 Gbps. Therefore, taking the fibre loss into account, the launch power of -25 dBm for SFP transceivers is sufficient for the receivers of 25 km data transmission. For synchronization in our QKD experiment, we employ a diode laser pulsed at 10 MHz. The lower pulsing rate compared with

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

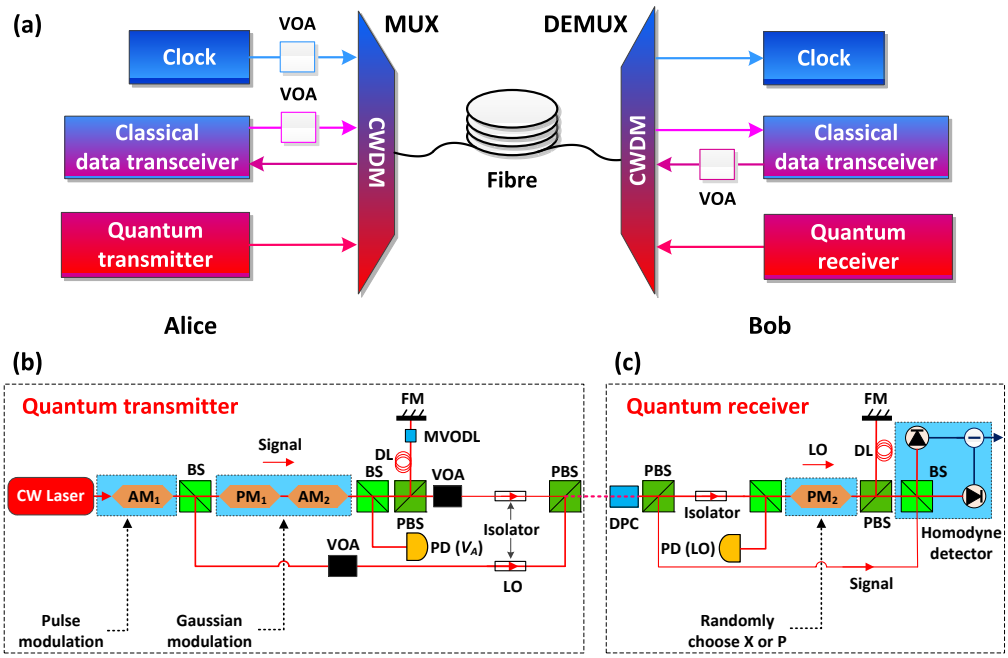

Fig. 1. Experiment setup of CVQKD. (a) Schematic for multiplexing of quantum transmitter (1550 nm), data transceiver (forward 1590 nm and backward 1610 nm) and clock (1570 nm). (b) Quantum transmitter. (c) Quantum receiver. MUX, multiplexer; DEMUX, demultiplexer; CW laser, continuous wave laser; AM, amplitude modulator; BS, beam splitter; VOA, variable optical attenuator; PM, phase modulator; PD, photodetector; PBS, polarizing beamsplitter; DL, delay line; MVODL, manual variable optical delay line; FM, faraday mirror; DPC, dynamic polarization controller.

SFP transceivers allows a much lower launch power of clock laser to be used, such that the photon scatter into the quantum channel is reduced. The launch optical power of clock laser at 1570 nm band is set as -45 dBm in our experiment.

In Figs. 1(b) and 1(c), we adopt the GMCS protocol for our CVQKD experiment. A 1550 nm wavelength continuous-wave (CW) laser provides a narrow linewidth up to 1.9 kHz. The CW light is transformed into a 50 MHz clock pulse train by using a customized 10 GHz Lithium Niobate electro-optic amplitude modulator (AM) with an extinction ratio of near 65 dB. The full width at half maximum (FWHM) of each optical pulse is 2 ns which is determined by an arbitrary waveform generator with 12 GS/s sampling rate. The x and p quadratures of coherent states are modulated by using a 5 GS/s digital analog converter in according to a centered Gaussian distribution of variance V_A in the units of N_0, where the N_0 represents the shot noise variance that appears in the Heisenberg uncertainty relation $\Delta x \Delta p \geq N_0$. The gaussian-modulated weak signal pulses are then send together with a strong LO in a standard telecom fiber by using polarization-multiplexing and time-multiplexing techniques. The delay of the LO pulse and signal pulse is adjusted to 130 ns. The time delay accuracy is guaranteed by a manual variable optical delay line with a 10 ps timing resolution. While the polarization-multiplexing is realized by using a faraday mirror and a polarizing beamsplitter. Bob, the receiver, randomly measures the x or p quadrature of these states by making the quantum signal pulses interfere with the LO in a 1 GHz bandwidth shot-noise-limited homodyne detector. The detected pulse peak values are proportional to the modulated quadratures and recorded with a 5 GS/s analog

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

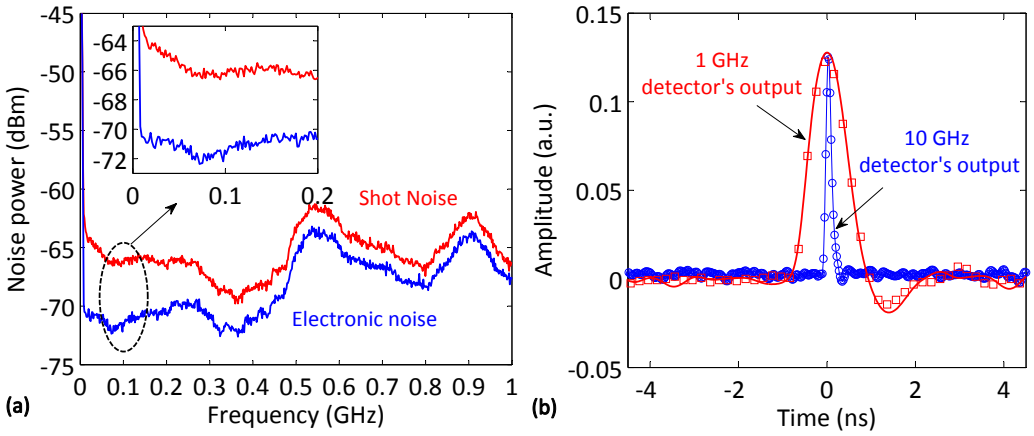

Fig. 2. (a) Shot noise characterization of homodyne detector in frequency domain. Top red trace, shot noise is measured at LO power of 0.5 mW. Bottom blue trace, electronic noise is measured without LO. The noise clearance between shot noise and electronic noise ranges from about 6 dB at 50 MHz, 4 dB at 0.2 GHz, and slowly degrades to and 1 dB at 1 GHz. (b) Pulse characterization with 300 ps optical pulse input. The blue circles are measured with a 9.5 GHz commercial detector and a 40 GS/s oscilloscope. The red squares are measured with our 1 GHz shot-noise-limited homodyne detector and a 5 GS/s analog digital converter.

digital converter.

2.2. *1 GHz shot-noise-limited homodyne detector*

High-speed CVQKD implementation relies on using wideband shot-noise-limited homodyne detector. Conceptually, the detector's photo-current shot noise determines the fundamental quantum limit for phase and amplitude homodyne measurements of optical signals. Previous study on the shot noise of non-classical light revealed a squeezing strength 3 dB from 100 MHz to 1.2 GHz [21], promising to realize a high-speed entanglement-based CV system. However, the simulation shows it is still quite difficult to carry out such high-speed experiment because that the observation of squeezing up to 10 dB would require a homodyne detector with 99 % detection efficiency.

We have reported a 300 MHz bandwidth shot-noise-limited homodyne detector for high-speed CVQKD experiment [16]. Inspired by the novel design of high-speed detector [21, 22], here we introduce a 1 GHz bandwidth shot-noise-limited homodyne detector to conduct a 50 MHz CVQKD experiment with coherent states. Practically, we employed two balanced photo-detectors with built-in preamplifiers and pHEMT ultra-low noise microwave amplifiers to fabricate the homodyne detector. The integrated preamplifiers in small enclosed package reduce the input capacitance, and consequently provide a much improved bandwidth, as well as lower electronic noise. As shown in Fig. 2(a), noise clearance between shot noise and electronic noise is about 6 dB at 50 MHz, 4 dB at 0.2 GHz and 1 dB at 1 GHz. It is worth mentioning that the noise clearance decreases with the microwave frequencies. This is mainly because the microwave devices in both photo-detectors exhibit slightly different responses for gain and noise versus frequency. The shot noise characterization is achieved at 0.5 mW ($\sim 10^7$ photons/ns), which is corresponding to an available LO power in Bob's side for our CVQKD experiment. Figure 2(b) shows the the characterization of rise and fall time of output pulse with a 300 ps optical pulse train from a pulsed laser source (ID Quantique id300). The blue electronic pulse

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

is the measurement result of the short pulse by using a commercial 9.5 GHz detector (Thorlabs PDA8GS) and a 40 GS/s oscilloscope (LeCroy WaveMaster 8 Zi-A). The red electronic pulse is the measurement result of the short pulse by using our 1 GHz detector (one photodiode is blocked) and a 5 GS/s analog digital converter. Although the FWHM of the red line was approximately 1 ns, which is larger than that of the input optical pulse, the electronic pulse does not have a long tail ($<$ 3 ns). Therefore, we can significantly reduce the excess noise caused by pulse overlap in the high-speed experiment. In addition, the 5 GS/s analog sampling converter features a 200 ps time window, and enable us to obtain peak values of pulses with 50 MHz repetition rate.

3. Excess noise analysis and controlling

Excess noise is the most critical issue pertaining to high-bit-rate CVQKD experiment. In analysis of the excess noise, we restrict ourselves in a realistic mode, where Eve cannot tamper with the devices in Alice and Bob's boxes. Based on our practical experiment, we need to study quantitatively the amount of excess noise that could be introduced by different noise sources. We note that Eve would be able to exploit the internal defects in both sides, such as the inherent laser phase noise [23, 24] and the imperfect modulation [25, 26] in Alice's side, or the unbalanced homodyne detector [15] in Bob's side. Fortunately, the excess noise due to the imperfection of CVQKD devices mentioned above could be controlled within a tolerable limit through careful design of the experiment because these kinds of excess noise are irrelevant to the repetition rate. Here, we focus on the excess noise associated with sources due to imperfect implementation of higher transport frequencies with shot-noise-limited homodyne detector and CWDM, which are two key ingredients of a practical high-bit-rate CVQKD system.

In GMCS QKD protocol, the LO used in the shot-noise-limited homodyne detector can be viewed as a 'mode selector'. This 'built-in' filtering property can help us to suppress out-of-band noise photons in the 'unmatched mode' of the LO. However, the noise photons due to the 'matched mode' of LO will contribute to in-band excess noise. On the one hand, the in-band excess noise could be induced by photons leakage $\langle \hat{N}_{LE}^{in} \rangle$ from strong LO path to weak quantum signal in a realistic optical system with a finite extinction ratio. On the other hand, the in-band excess noise could be contributed by in-band photons $\langle \hat{N}_{WDM}^{in} \rangle$ of the strong classical signals in the WDM environment. In the following, we will find that the causes of the excess noise are related to the requirement of higher transport frequencies in the high-bit-rate CVQKD.

Because the noises due to the in-band photons depend on the optics, it is difficult to completely remove the excess noise. To avoid compromising the security of our CVQKD implementation, it is reasonable for us to assume that it is in fact generated and controlled by Eve. Therefore, the excess noise ε_{in} (in shot noise units) contributed by noise photons $\langle \hat{N}_{noise}^{in} \rangle$ in matched mode (at Alice side, i.e. at the input) is given by

$$\varepsilon_{in} = \frac{2\langle \hat{N}_{noise}^{in} \rangle}{\eta_D \eta_B T}, \tag{1}$$

where η_D is the transmittance of DEMUX placed at Bob's side, η_B is the transmittance of box at Bob's side, $T = 10^{-\alpha L/10}$ is the transmission coefficient with a fibre length of L, the average photon number $\langle \hat{N}_{noise}^{in} \rangle = \langle \hat{N}_{LE}^{in} \rangle + \langle \hat{N}_{WDM}^{in} \rangle$.

Generally, the leakage photons $\langle \hat{N}_{LE}^{in} \rangle$ are caused by finite extinction ratio. This may be partly attributed to the fact that homodyne detection of coherent states under the shot noise limit (SNL) requires sufficient LO power. Although previous study of homodyne detector has shown a low demand of LO power ($\sim 10^6$) to reach the SNL in a low-frequency spectrum [27], most wideband shot-noise-limited homodyne detector ($>$ 50 MHz) require a higher LO power of $10^7 \sim 10^8$ photons/pulse at Bob's side [15, 16, 28]. This is because the electronic noise increases with the

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

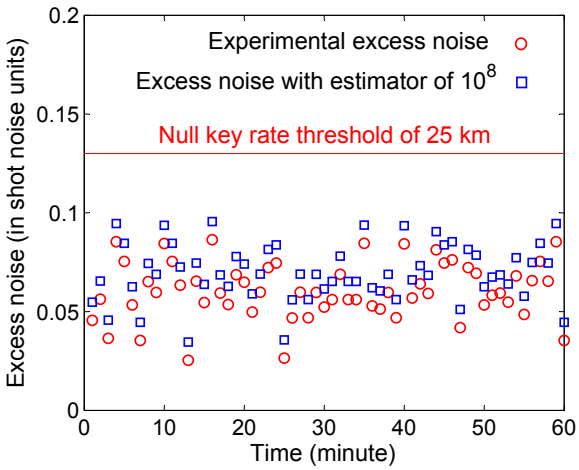

Fig. 3. Excess noise measurement. The lower red circles are measured at 25 km with finite-size block size of 10^8. The effective excess noise under worst-case estimator (red square) is employed to compute the final secret key rate. The red line defines the tolerable maximal value of excess noise at 25 km.

available bandwidth, we have to make the tradeoff between the LO power and transport frequencies in this case. According to Eq. (1), with a practical η_D of 0.8 ($\sim$ 1 dB insertion loss), η_B of 0.5 and a LO power $\langle \hat{N}_{LO} \rangle$ of 10^8 photons/pulse at Alice's side, one has to achieve extinction ratio R_e of $\sim$ 100 dB in a 25 km CVQKD system to avoid the excess noise ε_{in} beyond 0.01 ($\langle \hat{N}^{in}_{LE} \rangle$=$\langle \hat{N}_{LO} \rangle$/$R_e$). In our experiment setup, we achieved such an overall equivalent extinction ratio of the total system with customized optics. It involves 65 dB in pulse modulation and 35 dB in polarization-multiplexing. The practical LO power in Alice's side was attenuated to 10^8 photons/pulse so as to achieve a tolerable excess noise and shot-noise-limited homodyne detection in a 50 MHz CVQKD experiment.

While the noise photons $\langle \hat{N}^{in}_{WDM} \rangle$ could be contributed by several sources due to nonlinear processes in a practical coexistence architecture based on WDM [29]. The main motivation for us to deal with the $\langle \hat{N}^{in}_{WDM} \rangle$ is that the classical reconciliation of high-speed CVQKD need a large amount of classical data to be exchanged between Alice and Bob, so increasing the optical rate too much would result in a higher level of optical power of classical channels for nearly error-free communication. It has been shown that Spontaneous anti-Stokes Raman scattering (SASRS) is the dominant excess noise source when the wavelength of quantum channel λ_Q is the shortest among the WMD configuration, and the corresponding noise photons $\langle \hat{N}^{SASRS}_{WDM} \rangle$ is given by [30–32]

$$\langle \hat{N}^{SASRS}_{WDM} \rangle = \frac{1}{2}\left[\frac{\lambda_Q^3}{hc^2}\gamma\eta_D\left(P^{in}_{fwd}Le^{-\alpha L} + P^{in}_{bwd}\frac{1-e^{-\alpha L}}{2\alpha}\right)\right], \tag{2}$$

where h is the Planks constant, c is the speed of light, γ is the Raman scattering coefficient, P^{in}_{fwd} and P^{in}_{bwd} is the input power of forward and backward classical channel respectively. According to Eqs. (1) and (2) and a typical γ of 3×10^{-9} (km nm)$^{-1}$, in our experiment, the expected excess noise induced by data transceiver channel of forward and backward propagating direction with an attenuated optical power of -25 dBm can be controlled in the order of 10^{-5}. While the optical power of clock synchronization channel is approximately two orders of magnitude smaller than either data transceiver channel, so the excess noise induced by the noise photons

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

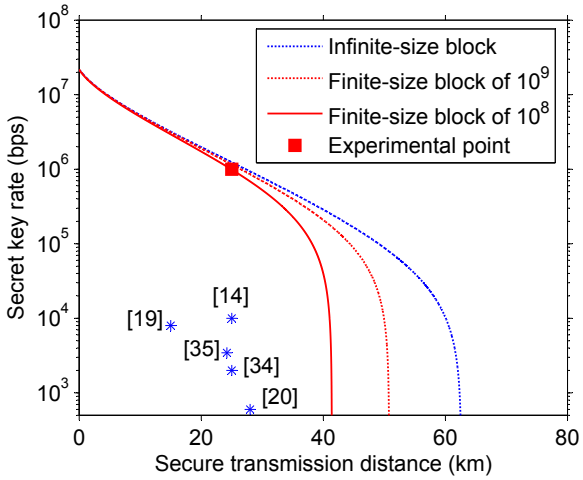

Fig. 4. Secret key rate under general collective attacks in finite-size scenarios. From left to right, curves correspond, respectively, to block lengths of $N = 10^8$, 10^9 and infinite. The blue points are the previous experiment resluts [14, 19, 20, 33, 34]. The red square is our experiment result, which is calculated from a group of time-varying excess noise. The modulation variance V_A is optimized, the quantum efficiency η_B is 0.5, the electronic noise υ_{el} is 0.3 (in shot noise units), the practical reconciliation efficiency β is 93%, the security parameter of privacy amplification procedure is set as 10^{-10}.

of clock channel is negligible.

The measurement of excess noise ε of our experiment is shown in Fig. 3. Each experimental point is measured on a sampling block over 1 minute for a distance of 25 km. A sifting procedure discarded 10% of the raw key for parameter estimation, which includes N_0, V_A, T, and ε. While 90% of the raw key is used for generating the final key. The achieved excess noise is around 0.06 (lower red circles). The corresponding excess noise under the worst-case estimator (higher blue square) is employed to compute the secret key rate when the extreme finite-size effects is taken into account. In our experiment, we find the practical excess noise is much larger than the theoretically expected values and drifts with time. There are several reasons why this variation occurs. More specifically, the first major reason for the increase of excess noise is induced by the variation of the LO power. Different from the shot noise we observed in Fig. 2(a) by using a specific LO power, the practical LO power in CVQKD varies with time and has a direct effect on the excess noise. This instability is caused by drifts of the bias voltage of AM in pulse modulation in Alice's side and the polarization demultiplexing in Bob's side as shown in Fig. 1(c). The second major reason for the excess noise increase is the the vibrational environment, thus producing faster phase drifts. Another major increase in the excess noise stems from the finite resolution of our 5 GS/s analog digital converter [25], which features an effective number of bits (ENOB) of 10 bits. Indeed, the controlling of the excess noise is much complex and difficult, however more ways to decrease excess noise can result in a significant increase of the secure key rate.

4. Reconcilation and secret key generation

The high-bit-rate CVQKD require high-speed error-correction. Previous state-of-art experiment demonstrated a 10 Mbps decoding speed [14], which is sufficient for 1 MHz CVQKD. We have reported high performance low density parity check (LDPC) error-correction codes (ECC) for

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015

25 MHz CVQKD system [35], which enable us to achieve an efficiency β of 96.9% at a signal-to-noise ratio (SNR) threshold of 0.02. We remark here that the practical SNR of our 25 km experiment is determined by the optimized modulation variance V_A. The achievable SNR is around 1 in our experiment, which is higher by approximately two orders of magnitude compared with the SNR threshold of our ECC. Therefore, the complexity of the recursive decoding is reduced. In our experiment, a Graphic Processing Unit of Nvidia Tesla K80 provides a huge amount of parallelism that allows us to achieve a 50 Mbps error-correction. Considering the finite-size effects in the parameters estimation procedure, the maximum secret key rate for our experiment bounded by collective attacks is given by

$$K = \frac{nR}{N}[\beta I_{AB} - \chi_{BE} - \Delta(n)], \tag{3}$$

where N is the block length of raw key, the n denotes the fraction of raw key effectively used for generating the final key, the sifted key rate n/N is $3/10$ in our case, R is repetition rate of the experiment, I_{AB} is the Shannon mutual information between Alice and Bob, χ_{BE} is the Holevo bound on the information between Bob and Eve, $\Delta(n)$ is related to the security of the privacy amplification [9].

Figure 4 shows the secret key rate with respect to transmission distance. We used a block length of 10^8 of raw key to calculate the key rate with parameter estimation. The secret key rate within the transmission distance of 25 km is slightly affected by finite-size effects. For comparison, we plot the previous results of CVQKD experiment [14, 19, 20, 33, 34], it is clear that we increased the secret key rate by two orders of magnitude by improving the repetition rate of whole system to 50 MHz. The improvement of CVQKD is therefore adapted to metropolitan communications (up to 40 km) with high-speed requirements.

5. Conclusion

We have demonstrated a CVQKD experiment over 25 km fibre channel with a record secret key rate of 1 Mbps. A 1 GHz shot-noise-limited homodyne detector is developed enable us to realize a 50 MHz experiment. The integration of quantum subsystem and classical communication channels into a CWDM environment satisfied the requirement of high-speed reconciliation procedure. We investigated and controlled the excess noise due to the increase of transport frequency in high-speed CVQKD. Further improvement of key rate is promising in our experiment with higher repetition rate. In addition, to boost the secret key rate, the next step is to adopt DWDM technology with 10 Gbps classical data communication, which is naturally accommodate a higher number of quantum channels and the DWDM 10 Gbps communication defined by the IEEE standard [36] has been widely used in existing fiber infrastructures. However, a 10 Gbps classical data channel might require 10 times higher lasers launching power than 1 Gbps and thus produce more noise photons scattering into the weak quantum channel. We anticipate that our study will serve as a stepping stone for future high-bit-rate quantum network.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grants No: 61170228, 61332019, 61471239), the Hi-Tech Research and Development Program of China (Grant No: 2013AA122901), and China Postdoctoral Science Foundation (Grant No: 2013M540365).

#234792 Received 17 Feb 2015; revised 17 Apr 2015; accepted 2 Jun 2015; published 26 Jun 2015