High-speed continuous-variable quantum key distribution over atmospheric turbulent channels

Zhen Qu, Ivan B. Djordjevic

Zhen Qu, Ivan B. Djordjevic, "High-speed continuous-variable quantum key distribution over atmospheric turbulent channels," Proc. SPIE 10118, Advances in Photonics of Quantum Computing, Memory, and Communication X, 101180B (20 February 2017); doi: 10.1117/12.2250213

Event: SPIE OPTO, 2017, San Francisco, California, United States

High-speed continuous-variable quantum key distribution over atmospheric turbulent channels

Zhen Qu* and Ivan B. Djordjevic
University of Arizona, Department of Electrical and Computer Engineering, 1230 E. Speedway Blvd., Tucson, AZ 85721, USA

ABSTRACT

We experimentally demonstrate a RF-assisted four-state continuous-variable quantum key distribution (CV-QKD) system in the presence of turbulence. The atmospheric turbulence channel is emulated by two spatial light modulators (SLMs) on which two randomly generated azimuthal phase patterns are recorded yielding Andrews' azimuthal phase spectrum. Frequency and phase locking are not required in our system thanks to the proposed digital phase noise cancellation (PNC) stage. Besides, the transmittance fluctuation can be monitored accurately by the DC level in this PNC stage, which is free of post-processing noise. The mean excess noise is measured to be 0.014, and the maximum secret key rate of >20Mbit/s can be obtained with the transmittance of 0.85, while employing the commercial PIN photodetectors.

Keywords: Continuous-variable quantum key distribution (CV-QKD), atmospheric turbulence, discrete modulation, phase noise cancellation (PNC), secret key rate (SKR)

1. INTRODUCTION

Quantum key distribution (QKD) is the most developed application of quantum cryptography, which has been recognized as the only method so far to guarantee secure communication [1,2]. In a typical QKD system, the cryptographic keys are exchanged over a quantum channel and shared by two legitimated users called "Alice" and "Bob". The unconditional security of QKD protocols is protected by the laws of quantum mechanics [1]. In general, the QKD implementations are established over optical fibers [3-5] and free-space optical links [6-8]. The latter one offers a great flexibility for infrastructure establishment and has attracted increasing attentions for short-distance optical communications [9]. Compared to the fixed transmittance in fiber-optics channel, the transmittance fluctuation through the free-space optical (FSO) links is treated as untrusted noise, which brings the post-processing noise into the system [10].

In the state-of-art QKD protocols, continuous-variable QKD (CV-QKD) protocols have played a critical role in high-speed QKD communications. It has been shown that any two non-orthogonal quantum states in principle suffice to insure secure QKD [2]. CV-QKD protocols based on coherent states with Gaussian modulation have been proved to be unconditionally secure against collective attacks [11]. In addition, CV-QKD protocols based on discrete modulation, e.g., the four-state protocol has been demonstrated to be secure against collective attacks and introduced for the facility of high reconciliation efficiency [12,13]. Currently, the best candidate for reconciliation is a low-density parity-check (LDPC) coding, which has been realized in real-time with the help of FPGAs [14,15]. Typically, the self-homodyne detection is commonly used in CV-QKD transmission systems, in which the brighter local oscillator (LO) light is emitted at Alice's side, multiplexed and co-propagated with the quantum keys through the quantum channels, and then mixed in the coherent detector at Bob's side [16]. Although the excess noised caused by the laser noise can be effectively mitigated, the LO fluctuation potentially opens a loophole for Eve to intercept the secret key [17].

In this paper, we experimentally demonstrate a discrete modulated CV-QKD protocol suitable for use over atmospheric turbulent channels. The turbulence channel is emulated by two spatial light modulators (SLMs), which are loaded with two randomly generated azimuthal phase patterns yielding Andrews' azimuthal phase spectrum. An RF-assisted coherent detection, followed by a simple phase noise cancellation (PNC) stage is introduced to monitor the transmittance fluctuation in the quantum channel and control the excess noise. The mean excess noise is measured to be 0.014, and the maximum secret key rate of >20Mbit/s can be obtained with the transmittance of 0.85.

Advances in Photonics of Quantum Computing, Memory, and Communication X, edited by Zameer Ul Hasan,
Philip R. Hemmer, Hwang Lee, Alan L. Migdall, Proc. of SPIE Vol. 10118, 101180B
© 2017 SPIE · CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2250213

The paper is organized as follows. In Section 2, the proposed RF-assisted four-state CV-QKD system is described, together with corresponding atmospheric turbulence emulator. In the same section, the proposed PNS stage is introduced, and the theory behind SKR calculation is briefly described. In Section 3, the experimental results are provided including the analysis of SKR and excess noise. Some important concluding remarks are provided in Section 4.

2. RF-ASSISTED FOUR-STATE CV-QKD SYSTEM MODEL

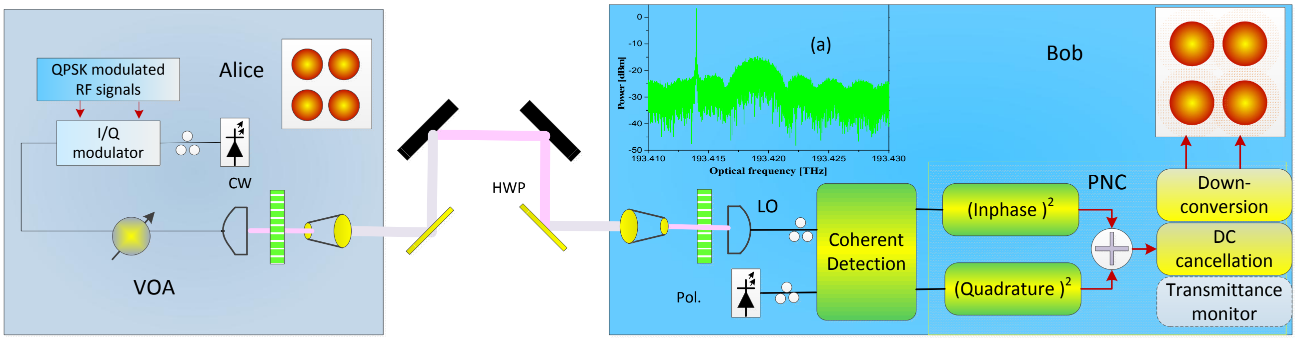


Fig. 1. The schematic of the proposed RF-assisted four-state CV-QKD system. PNC: phase noise cancellation stage.

The schematic of the proposed RF-assisted four-state CV-QKD system is depicted in Fig. 1. A series of QPSK symbols, i.e., $I(t), Q(t) \in \{-1, +1\}$ is generated, and then up-converted to the RF domain at Alice's side. The corresponding in-phase and quadrature signals denoted as $S_I(t)$, $S_Q(t)$ are expressed as

$$S_I(t) = I(t)\,cos(w_1 t) - Q(t)\,sin(w_1 t) \tag{1}$$

$$S_Q(t) = I(t)\,sin(w_1 t) + Q(t)\,cos(w_1 t) \tag{2}$$

where w_1 is the RF angular frequency. The generated RF signals are then used as inputs of electro-optical I/Q modulator, which are operated at the quadrature point in both the in-phase and quadrature branches. The resulting optical field out of Alice's side can be written as:

$$\begin{aligned} E_{sm}(t) &= \{cos\left[AS_I(t) + \frac{\pi}{4}\right] + j \cdot cos\left[AS_Q(t) + \frac{\pi}{4}\right]\} \cdot \sqrt{P_s} e^{j[wt+\varphi_1(t)]} \\ &\approx \{J_0[AS_I(t)] - 2J_1[AS_I(t)] + j \cdot J_0[AS_Q(t)] - 2j \cdot J_1[AS_Q(t)]\} \cdot \sqrt{P_s} e^{j[wt+\varphi_1(t)]} \\ &\approx \sqrt{2P_s} e^{jwt+\frac{\pi}{4}} - A \cdot [I(t) + jQ(t)] \sqrt{P_s} e^{j[(w+w_1)t+\varphi_1(t)]} \end{aligned} \tag{3}$$

where A denotes the modulation index; while P_s, w, and $\varphi_1(t)$ represent the power, angular frequency, and phase noise of the optical carrier, respectively. In Eqn. (3), $J_0(\cdot)$ and $J_1(\cdot)$ denote the zeroth and first order Bessel functions of the first kind, respectively. The modulation variance V_A of the signal, expressed in shot-noise units, measured by sampling scope in electrical domain, is adjusted by tuning the modulation index and a variable optical attenuator (VOA). Notice that small signal modulation is required to get a simple approximation equation. A typical optical spectrum during the channel transmission is shown as an inset of Fig. 1(a). There are other sidebands co-existing with the major signal band, but they will not represent the security loophole. This is not only because their power is far smaller than that of the major signal band, but rather the fact that signals carried in these sidebands are not linearly related to the original QPSK signal.

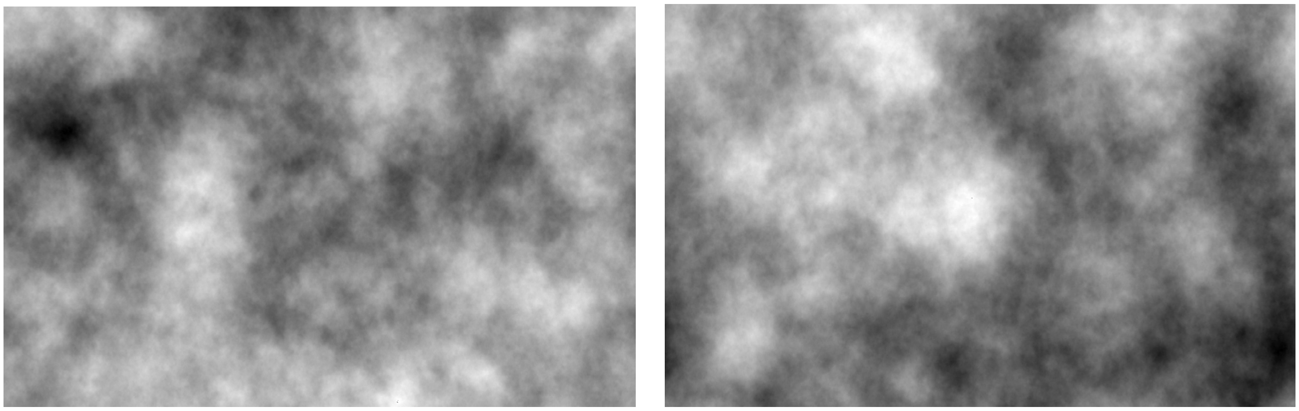
The turbulence channel is emulated by two spatial light modulators (SLMs), on which two randomly generated azimuthal phase patterns following Andrews' spectrum are recorded [18-19]. When atmospheric turbulence emulator is turned on, Fig. 2 presents two illustrative examples of the phase patterns used in the emulator.

The channel-introduced noise variance is expressed as $\chi_{line} = 1/T + \epsilon - 1$, where T is the transmittance, and ϵ denotes the excess noise. The SKRs for the QPSK-based protocol with coherent detection can be determined with the assumption of collective eavesdropping attacks, as discussed in [12].

At Bob's side, the electric field of LO laser is denoted as

$$E_{LO}(t) = \sqrt{P_{LO}} e^{j[w_{LO}t+\varphi_2(t)]} \tag{4}$$

where P_{LO}, w_{LO}, and $\varphi_2(t)$ represent the power, angular frequency, and phase noise of LO, respectively. The coherent receiver includes an optical 90^0 hybrid and two balanced photodetectors (PDs). Our coherent detector is characterized by the efficiency η and electrical noise V_{el}. The detector-added noise variance can be expressed as $\chi_{het} = (2 + 2V_{el} - \eta)/\eta$. The total noise variance added between Alice and Bob reads as $\chi_{tot} = \chi_{line} + \chi_{het}/T$.


(a)

(b)

Fig. 2. Illustration of two azimuthal phase patterns, denoted as (a) and (b), which are uploaded onto the SLMs

The photocurrents of the in-phase and quadrature arms after coherent receiver can be expressed as:

$$\begin{gathered} i_I(t) \propto \sqrt{2}T\,cos\left[(w - w_{LO})t + \varphi_1(t) - \varphi_2(t) + \frac{\pi}{4}\right] \\ -ATI(t)\,cos[(w + w_1 - w_{LO})t + \varphi_1(t) - \varphi_2(t)] \\ +ATQ(t)\,cos[(w + w_1 - w_{LO})t + \varphi_1(t) - \varphi_2(t)] + n_I \end{gathered} \tag{5}$$

$$\begin{gathered} i_Q(t) \propto \sqrt{2}T\,sin\left[(w - w_{LO})t + \varphi_1(t) - \varphi_2(t) + \frac{\pi}{4}\right] \\ -ATI(t)\,cos[(w + w_1 - w_{LO})t + \varphi_1(t) - \varphi_2(t)] \\ +ATQ(t)\,cos[(w + w_1 - w_{LO})t + \varphi_1(t) - \varphi_2(t)] + n_Q \end{gathered} \tag{6}$$

where n_I and n_Q represent in-phase and quadrature components of the additive noise process. By combing the squares of in-phase and quadrature photocurrents, we obtain:

$$\begin{gathered} i_C(t) = i_I^2 + i_Q^2 \\ = 2T^2 + 2A^2T^2 - 2\sqrt{2}AI\,cos\left(w_1 t - \tfrac{\pi}{4}\right) + 2\sqrt{2}AQ\,cos\left(w_1 t - \tfrac{\pi}{4}\right) + n_C + \text{crossterms} \end{gathered} \tag{7}$$

where n_C is the total noise after combination, and cross-terms are located in high-frequency domain. The DC component, i.e., $2T^2 + 2A^2T^2$ can be used to monitor the transmittance of the channel. After cancelling the DC component, and filtering out the high frequency-terms, for small signal modulation assumption, which is required in CV-QKD systems, the final result is obtained as

$$\begin{gathered} i_s(t) \propto 2\sqrt{2}AI(t)\,cos\left(w_1 t - \frac{\pi}{4}\right) + 2\sqrt{2}AQ(t)\,cos\left(w_1 t - \frac{\pi}{4}\right) \\ +2\sqrt{2}\{n_I\,cos\left[(w - w_{LO})t + \varphi_1(t) - \varphi_2(t) + \frac{\pi}{4}\right] \\ +n_Q\,sin\left[(w - w_{LO})t + \varphi_1(t) - \varphi_2(t) + \tfrac{\pi}{4}\right]\} \end{gathered} \tag{8}$$

After QPSK demodulation, the resulting in-phase and quadrature noisy signals are given as

$$r_I = -\sqrt{2}AI + n_I' \tag{9}$$

$$r_Q = \sqrt{2}AQ + n_Q' \tag{10}$$

where n_I' and $n_Q'$are the equivalent additive noise processes. Thus, we can retrieve the transmitted QPSK symbols without frequency fluctuation and phase noise, originating from the laser.

When Alice and Bob use reverse reconciliation, the secret key rate is given by

$$\Delta I = \beta I_{AB} - \chi_{BE}, \tag{11}$$

where β is the reconciliation efficiency, I_{AB} is the Shannon information between Alice and Bob, χ_{BE} is the Holevo bound, and they can be identified as

$$I_{AB} = \log_2(\tfrac{V+\chi_{tot}}{1+\chi_{tot}}) \tag{12}$$

$$\chi_{BE} = G\left(\tfrac{\lambda_1-1}{2}\right) + G\left(\tfrac{\lambda_2-1}{2}\right) - G\left(\tfrac{\lambda_3-1}{2}\right) - G(\tfrac{\lambda_4-1}{2}) \tag{13}$$

where $V = V_A + 1$, and $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$. The symplectic eignevalues $\lambda_{1,2,3,4}$ are given by [12]

$$\lambda_{1,2} = \sqrt{\tfrac{1}{2}(A \pm \sqrt{A^2 - 4B})} \tag{14}$$

$$\lambda_{3,4} = \sqrt{\tfrac{1}{2}(C \pm \sqrt{C^2 - 4D})} \tag{15}$$

where

$$A = V^2 + T^2(V + \chi_{line})^2 - 2TZ_4^2,$$

$$B = (TV^2 + TV\chi_{line} - TZ_4^2)^2,$$

$$C = \frac{A\chi_{het}^2 + B + 1 + 2\chi_{het}\left[V\sqrt{B} + T(V + \chi_{line})\right] + 2TZ_4^2}{[T(V + \chi_{tot})]^2},$$

$$D = \frac{(V + \chi_{het}\sqrt{B})^2}{[T(V + \chi_{tot})]^2},$$

$$Z_4 = V_A(\xi_0^{\frac{3}{2}}\xi_1^{-\frac{1}{2}} + \xi_1^{3/2}\xi_2^{-1/2} + \xi_2^{3/2}\xi_3^{-1/2} + \xi_3^{3/2}\xi_0^{-1/2}),$$

$$\xi_{0,2} = 1/2e^{-V_A/2}[cosh(V_A/2 \pm \cos{(V_A/2)})],$$

$$\xi_{1,3} = 1/2e^{-V_A/2}[sinh(V_A/2 \pm \sin{(V_A/2)})].$$

3. EXPERIMENTAL RESULTS AND ANALYSIS

We experimentally demonstrate and study the proposed RF-assisted four-state CV-QKD system. At Alice's side, the 1550-nm continuous-wave lightwave is generated by a laser source with a linewidth of <10 kHz. The 2.5 G Baud QPSK signals are loaded onto a RF carrier with the carrier frequency of 5 GHz. The RF signals are shaped with the help of an arbitrary waveform generator (AWG) and then used as inputs of an electro-optical I/Q modulator, where both RF ports are biased at quadrature point. The modulation variance of the generated quantum signal is adjusted by a VOA.

In the emulated turbulent channel link, the rate of atmospheric channel fluctuations is of 50Hz, which represents the worst case scenario given that in a deep fade, due to atmospheric turbulence, a large number of transmitted QPSK symbols will be affected. The channel induces transmittance fluctuations, which can be monitored by the PNC stage via analyzing the DC level. As shown in Fig. 3, the mean transmittance obtained is 0.55, and the maximum transmittance can be reached is ~0.9.

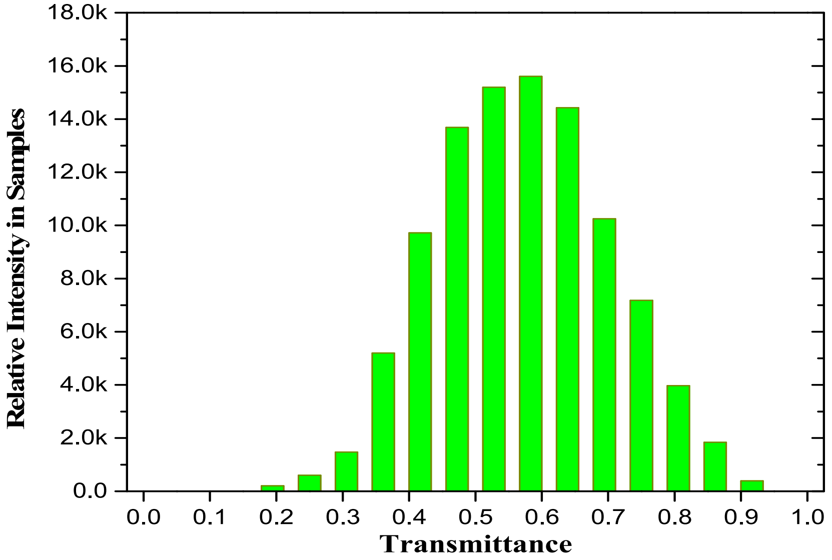


Fig. 3. Measured probability distribution of fluctuating channel transmittance.

At Bob's side, another laser with a linewidth of <10 kHz serves as a LO laser. Two polarization controllers (PCs) are used to align the polarizations of the signal light and LO before being mixed in the coherent receiver. The coherent receiver includes an optical 90^0 hybrid, two 23 GHz balanced PDs, and real-time oscilloscope with 100 GSa/s sample rate and 33 GHz analog bandwidth. The digitalized in-phase and quadrature signals are then passed to the PNC stage; implemented by two square operators, one addition operator, and the cross-terms from DC and high-frequency components will be eliminated by the DC cancellation block and LPF, respectively. This PNC scheme is robust against high noise levels, but sensitive to the bias fluctuation of the I/Q modulator. After the system calibration [20], Bob's apparatus yields a detection efficiency of $\eta = 0.5$ and electrical noise of $V_{el} = 0.9$.

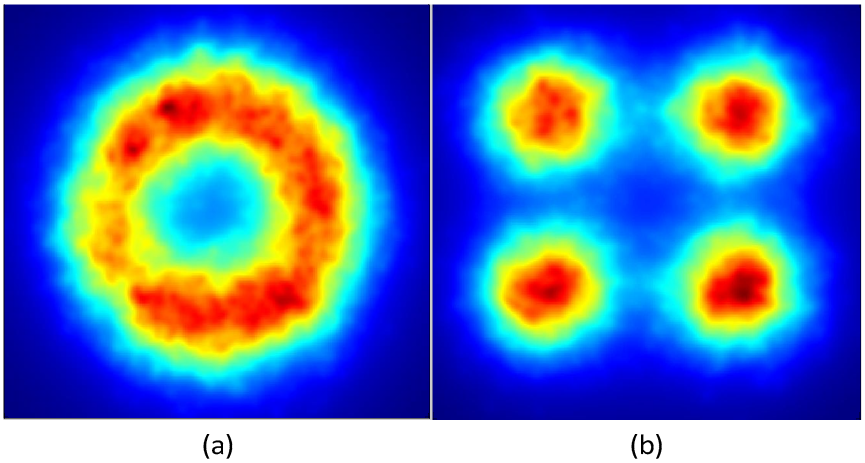


Fig. 4. Recovered constellation diagrams: (a) without PNC and (b) with PNC.

When the channel's transmittance T is 0.6 and the modulation variances V_A is 20, the recovered constellation diagrams without and with PNC stages are shown in Fig. 4, where 10^5 points are included in each constellation diagram. Compared to the circle-like constellation diagram shown in Fig. 4(a), we can see from Fig. 4(b) that the frequency dithering and laser phase noise can be effectively compensated for. To specify the level of excess noise, Fig. 5 shows the excess noise level (in linear scale) of the proposed system as a function of time for the modulation variance of V_A=0.3 and the transmittance of T=0.55. Each realization is measured with a block (frame) size of 10^6 points. The variance of the excess noise is mainly arising from the bias fluctuation of the I/Q modulator and the timing jitter of our oscilloscope. The mean value of the excess noise is estimated to be 0.014, well below the zero key rate threshold.

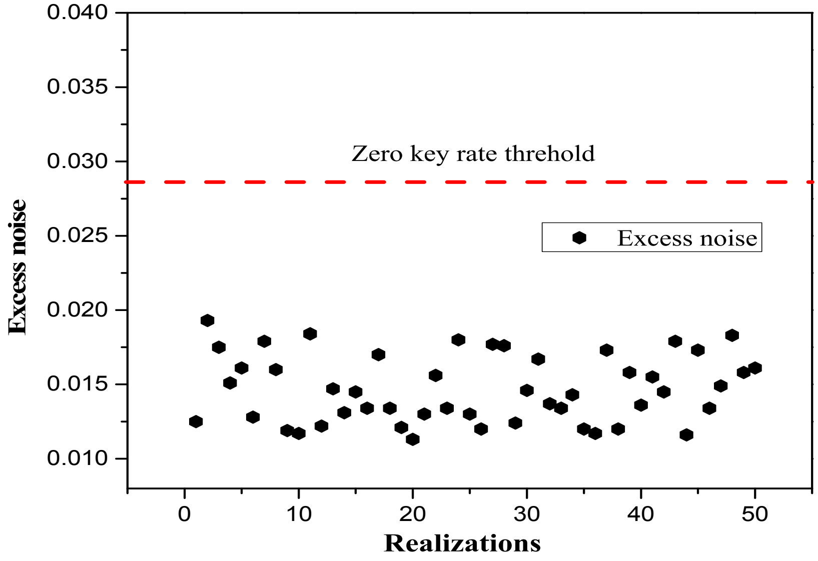


Fig. 5. Excess noise measurements. Each point is measured with a finite block size of 10^6 points.

The average SKRs with a reconciliation efficiency of 0.8 are measured experimentally for different modulation variances and transmittances, as shown in Fig. 6. The reconciliation efficiency in use has been realized by the LDPC codes [21,22].The maximum SKR of >20 Mbit⁄s can be obtained when T=0.85, and V_A= 0.35. We find that the SKR of >4 Mbit⁄s can be obtained when T=0.55, and the minimum transmittance of T= 0.35 is required to guarantee secure CV-QKD transmission. It is also easy to figure it out that the optimal range of modulation variance is [0.25, 0.45]. Considering that the excess noise level is very small, the large electrical noise and low detection efficiency become the limiting factors in our system.

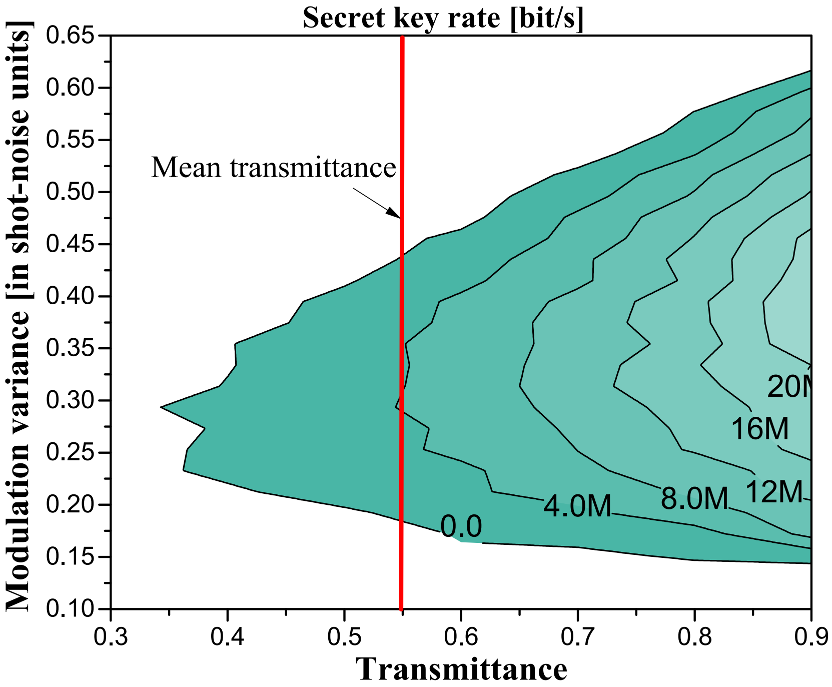


Fig. 6. Experimental SKRs as a function of the modulation variance and transmittance.

4. CONCLUDING REMARKS

We described an RF-assisted four-state CV-QKD system based on coherent detection, where the discrete modulated QPSK signals have been prepared and sent from Alice to Bob, and a classical coherent detection has been implemented at Bob's side with a phase noise cancellation stage to control the excess noise level. The atmospheric turbulence channel has been emulated by two spatial light modulators on which two randomly generated azimuthal phase patterns have been recorded yielding Andrews' azimuthal phase spectrum. The transmittance fluctuation has been monitored accurately by the DC level in thus PNC stage, which has been found free from post-processing noise. The mean excess noise has been experimentally measured to be 0.014, and the maximum secret key rate of >20Mbit/s has been obtained with the transmittance of 0.85. A minimum transmittance of 0.35 can be reached to guarantee secure transmission, and a SKR of >4 Mbit⁄s can be obtained in case of the mean transmittance.

Acknowledgement

This work is supported by Office of Naval Research (ONR) (N00014-13-1-0627).

REFERENCES

[1] Ekert, A.K., "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67(6), 661-663 (1991).

[2] Bennett, C. H., "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. 68(21), 3121-3124 (1992).

[3] Xuan, Q. D., Zhang, Z. and Voss, P. L., "A 24 km fiber-based discretely signaled continuous variable quantum key distribution system". Optics express, 17(26), 24244-24249 (2009).

[4] Qu, Z., Djordjevic, I. B. and Neifeld M. A., "RF-subcarrier-assisted Four-state Continuous-variable QKD Based on Coherent Detection," Optics Letters, 41(23), 5507-5510, (2016).

[5] Qu, Z., Lin C., Liu T. and Djordjevic, I. B, "Experimental Investigation of GF(3^2) Nonbinary LDPC coded Non-uniform 9-QAM Modulation Format," ECOC, 1112-1114 (2016).

[6] Sun, X., Djordjevic, I. B. and Neifeld M. A., "Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels," IEEE Photonics J. 8(3), 1-13 (2016).

[7] Heim, B., Peuntinger, C., Killoran, N., Khan, I., Wittmann, C., Marquardt, C. and Leuchs, G., "Atmospheric continuous-variable quantum communication," New Journal of Physics 16(11), 113018 (2014).

[8] Sun, X., Djordjevic I. B. and Neifeld M. A., "Multiple spatial modes based QKD over marine free-space optical channels in the presence of atmospheric turbulence," Optics Express, 24(24), 27663- 27673 (2016).

[9] Qu, Z. and Djordjevic, I. B., "500Gb/s Free-Space Optical Transmission over Strong Atmospheric Turbulence Channels," Optics Letters 41(14), 3285-3288, 2016.

[10] Semenov, A. A., Töppel, F., Vasylyev, Y. D., Gomonay H. V. and Vogel W., "Homodyne detection for atmosphere channels", Phys. Rev. A 85(1), 013826 (2012).

[11] Grosshans, F., "Collective attacks and unconditional security in continuous variable quantum key distribution," Phys. Rev. Lett. 94(2), 020504 (2005).

[12] Zhang, H., Fang, J. and He G., "Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers," Phys. Rev. A 86(2), 022338 (2012).

[13] Becir, A., El-Orany, F. A. A. and Wahiddin, M. R. B., "Continuous-variable Quantum Key Distribution protocols with eight-state discrete modulation," Int. J. Quant. Inf. 10 (1), 1250004 (2012).

[14] Zou, D. and Djordjevic, I. B., "FPGA-based rate-adaptive LDPC-coded modulation for the next generation of optical communication systems," Optics Express 24(18), 21159-21166 (2016).

[15] Zou, D. and Djordjevic, I. B., "FPGA implementation of concatenated non-binary QC-LDPC codes for high-speed optical transport," Optics Express 23(10), 14501-14509 (2015).

[16] Ralph, T. C., "Continuous variable quantum cryptography," Phys. Rev. A 61(1), 010303(R) (1999).

[17] Jouguet, P., Kunz-Jacques, S. and Diamanti, E., "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," Phys. Rev. A 87(6), 062313 (2013).

[18] Andrews, L. C., Phillips, R. L. and Young, C. Y., Laser Beam Scintillation with Applications. SPIE Press, 2001.

[19] Qu, Z. and Djordjevic, I. B., "Coded orbital angular momentum based free-space optical transmission in the presence of atmospheric turbulence," in Proc. Asia Commun. Photonics Conf, paper AS3D.3 (2015).

[20] Fossier, S., Diamanti, E., Debuisschert, T., Villing, A., Tualle-Brouri, R. and Grangier, P., "Field test of a continuous-variable quantum key distribution prototype," New Journal of Physics, 11(4), 045023 (2009).

[21] Djordjevic, I. B., Cvijetic, M. and Lin, C., "Multidimensional Signaling and Coding Enabling Multi-Tb/s Optical Transport and Networking," IEEE Sig. Proc. Mag., 31(2), 104-117 (2014).

[22] Lin, C., Zou, D., Liu, T. and Djordjevic, I. B., "Capacity Achieving Nonbinary LDPC Coded Non-Uniform Shaping Modulation for Adaptive Optical Communications," Optics Express, 24(16), 18095-18104 (2016).