Optics Letters

High-performance long-distance discrete-modulation continuous-variable quantum key distribution

YAN TIAN,[1,2] YU ZHANG,[1,2] SHUAISHUAI LIU,[1,2] PU WANG,[3] ZHENGUO LU,[1,2] XUYANG WANG,[1,2,4] AND YONGMIN LI[1,2,4,*]

[1] State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China
[2] Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China
[3] School of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China
[4] Hefei National Laboratoty, Heifei 230088, China
*yongmin@sxu.edu.cn

Received 30 March 2023; revised 23 April 2023; accepted 27 April 2023; posted 27 April 2023; published 24 May 2023

We experimentally demonstrate a high-rate discretely modulated continuous-variable quantum key distribution over 80-km standard single-mode fiber with a 2.5 Gbaud, 16-symbol, two-ring constellation. With the help of well-designed digital signal processing algorithms, the excess noise of the system can be effectively suppressed. The achieved secret key rates are 49.02 Mbits/s, 11.86 Mbits/s, and 2.11 Mbits/s over 25-km, 50-km, and 80-km optical fiber, respectively, and achieve 67.4%, 70.0%, and 66.5% of the secret key rate performance of a Gaussian-modulated protocol. Our work shows that it is feasible to build a high-performance, long-distance continuous-variable quantum key distribution system with only a small constellation size.

https://doi.org/10.1364/OL.492082

Quantum key distribution (QKD) allows for the generation and distribution of information-theoretical secure keys between two parties over an insecure quantum channel, in which the security of the shared keys is guaranteed by the fundamental laws of quantum mechanics. Combined with the one-time-pad (OTP) encryption protocol, secure communication can be realized. However, because the OTP protocol requires that the key can only be used once and is no less than the encrypted message, the resulting huge key consumption is a great challenge.

Continuous-variable (CV) QKD protocols [1] encode the key information on quadratures of quantized electromagnetic fields, which can be measured by low-cost and high-efficiency coherent detectors. Moreover, the high-speed coherent detection technology and infinite-dimensional Hilbert space of the encoding promise potential higher secret key rates (SKRs) over a metropolitan area [2]. Furthermore, because of the spatial and temporal filtering of the local-oscillator (LO) field, CV-QKD is robust against noise photons in various quantum channels. Thus, CV-QKD has attracted a lot of attention in recent years for its high key rate, low cost, and compatibility with coherent optical telecommunication networks [3–9].

The Gaussian-modulated (GM) CV-QKD protocol has been widely studied and demonstrated in the past 10 years. It can achieve an optimal theoretical secure key rate and has better resistance to excess noise. GM CV-QKD has been theoretically proved to be secure against arbitrary collective attacks and coherent attacks, even when considering the finite-size effects. However, a Gaussian modulation is an unbounded continuous modulation and around 10,000 states (90 × 90 size constellation) are required to satisfactorily simulate a Gaussian distribution [10]. This imposes heavy burdens on the random number generation and high-speed linear electro-optic modulation devices; the latter is necessary to achieve a low-level modulation noise that is critical to the system performance [11]. Moreover, the data reconciliation of Gaussian variables at low signal-to-noise ratio (SNR) is also a challenge.

Discrete-modulation (DM) CV-QKD protocols [12] prepare the coherent states chosen from a finite constellation in phase space and effectively overcome the limitations faced by the GM protocols. The security of the DM CV-QKD protocols in the asymptotic regime has been established by applying numerical-method-based convex optimization techniques [12,13]. Subsequently, an analytical lower bound on the asymptotic SKR of CV-QKD with an arbitrary modulation of coherent states was proposed [14]. Lately, several DM CV-QKD protocols have been experimentally implemented, including the phase-shift keying (PSK) constellation [15,16], the quadrature amplitude modulation (QAM) constellation coupled with probabilistic constellation shaping (PCS) [5,17], and the amplitude- and phase-shift-keying (APSK) constellation with PCS [18]. To achieve a SKR comparable to the GM protocol, the constellation size of previous experiments is still relatively large (64, 128, or 256). The high-cardinality constellations increase the modulation complexity and imperfections and lead to excessive modulation noise (the main source for the excess noise of the CV-QKD system), especially in the case of a high symbol rate and long transmission distance. Furthermore, a small constellation size consumes a smaller number of random numbers and enables more efficient post-processing.

Recently, it has been shown that a high key rate DM protocol comparable to the GM protocol can be achieved using only 10 or so coherent states by implementing suitable key

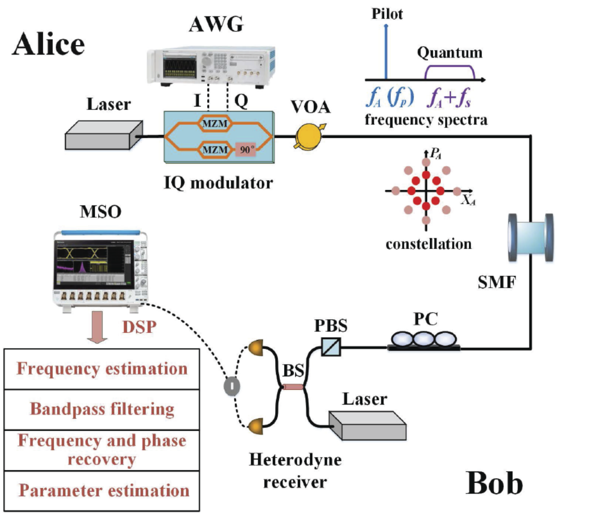

Fig. 1. Experimental setup. AWG, arbitrary waveform generator; BS, beam splitter; IQ modulator, in-phase-and-quadrature modulator; MSO, mixed signal oscilloscope; PBS, polarization beam splitter; PC, polarization controller; SMF, single-mode fiber; VOA, variable optical attenuator. The two-ring constellation and frequency spectra of the quantum and pilot signals are depicted.

map and numerical convex optimization techniques [19]. In this work, we experimentally implemented this high-rate and small constellation size DM CV-QKD protocol with a local local oscillator (LLO) and telecom-grade components over 80 km of single-mode fiber (SMF), for the first time to our knowledge. The protocol operates with a 2.5 Gbaud, 16-symbol two-ring constellation (eight states in the inner ring and eight states in the outer ring). Our experimental results show that the QKD system can achieve 70.0% (66.5%) of the secret key rate performance of GM CV-QKD at a distance of 50 km (80 km), under the asymptotic regime. Our modulation formats use only two amplitude levels and eight uniformly spaced phase angles that are critical for a chip-based QKD system, for which simple modulation formats are beneficial to the suppression of modulation noise. The concise implementation and high-rate performance makes our system an attractive alternative for cost-effective secure quantum communication.

The procedures of the two-ring constellation protocol implemented in our experiment can be described as follows [19]: Alice prepares the coherent states $|\alpha\rangle = \left|\alpha_k e^{ix\pi/4}\right\rangle$ with $x \in \{0, 1, 2, 3, 4, 5, 6, 7\}$, and $k \in \{1, 2\}$, where α is the ring's amplitude of the two-ring constellation, x is the state's index within each ring, and k is the ring's index. The coherent states in the inner (outer) ring are chosen according to an equal probability of p_1 (p_2) that satisfies $p_1 + p_2 = 1/8$. The diagram of the two-ring constellation is plotted in Fig. 1. Alice randomly sends the prepared coherent states to Bob through an insecure quantum channel. At the receiver's side, Bob performs heterodyne detection and records the measurement outcomes. Then, Alice and Bob randomly select a portion of their data for parameter estimation of the QKD system, and the asymptotic SKR is estimated using the numerical security proof method. Finally, Alice and Bob perform data reconciliation and privacy amplification through an authenticated public channel to generate the final secret key.

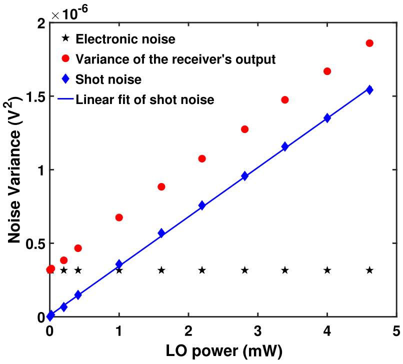

Fig. 2. Linear relationship between output noise of balanced receiver and LO power.

The experimental setup is illustrated schematically in Fig. 1. Alice exploits a single-frequency continuous-wave (cw) 1550-nm laser with 100 Hz linewidth (NKT Koheras BASIK X15). An in-phase-and-quadrature (IQ) modulator (Eospace) is used to modulate the amplitude and phase quadratures of the laser beam in phase space with single sideband modulation. The symbol rate of the baseband signal is set to 2.5 Gbaud, and a digital raised cosine (RC) pulse shape filter with a roof-off factor of 0.3 is adopted. To avoid low-frequency noise from the experimental system, such as the laser and detector, the baseband RC signal is digitally upconverted by 4 GHz (f_s = 4 GHz). The quantum signal is frequency multiplexed with a DC pilot signal, i.e., f_p = 0 Hz, which is used to estimate the frequency offset and phase noise between the quantum signal and the LLO; its SNR is about 32 dB. The radio frequency (RF) signals generated by a two-channel arbitrary waveform generator (AWG, Tektronix, AWG70002A) with a 25 Gsample/s sampling rate and 10 bits resolution are fed into the RF ports of the IQ modulator. The modulated laser beam is attenuated to a suitable level with modulation variance V_A by a variable optical attenuator, and then sent to Bob through a standard SMF spool. Bob recovers the state of polarization of the signal beam using a polarization controller (PC). An independently running single-frequency cw laser with a linewidth of 100 Hz is used to generate the LLO, the center wavelength of which can be finely tuned. The power of the LLO is 4.5 mW, and the frequency of Bob's laser is downshifted 50 MHz from the frequency of Alice's laser. Subsequently, the signal beam interferes with the LLO at a 50:50 beam splitter (BS) and the output beams are detected by a balanced receiver (Optilab BPR-23-M) with a bandwidth of 23 GHz. The response characteristics of the detector for a vacuum field input are measured and shown in Fig. 2; we can see that the detector exhibits good linearity, which is critical for the correct measurement of the shot noise and the quadratures. The output signal of the balanced receiver is sampled using a 10 GHz high-speed mixed signal oscilloscope (MSO, Tektronix, MSO64B) with 25 Gsample/s sampling rate and 12 bits resolution. The sampled electrical signals are stored for offline digital signal processing (DSP).

The DSP mainly includes the following steps.

(1) Frequency offset estimation. Owing to the frequency drift, the frequency difference between two independent and free-running lasers fluctuates with time. By performing Fourier transformation on the sampled signal and finding the peak value in the frequency domain, the frequency offset of the

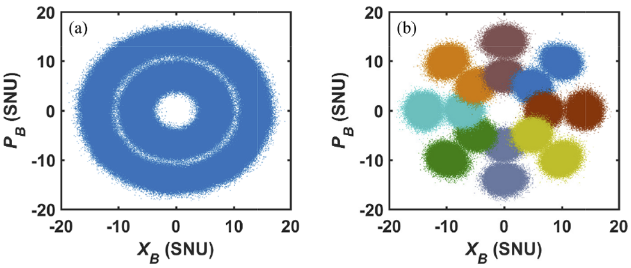

Fig. 3. 16-symbol two-ring constellation: (a) without DSP; (b) with DSP. SNU, shot noise units.

two lasers is estimated as $\Delta\hat{f} = f_A - f_B$, where f_A and f_B are, respectively, the center frequencies of Alice's laser and Bob's laser.

(2) Bandpass filtering. The quantum and pilot signals were bandpass-filtered using digital filters, and the central frequency and bandwidth of pilot (quantum) signal are $\Delta\hat{f}$ ($\Delta\hat{f} + f_s$) and 5 MHz (3.25 GHz), respectively.

(3) Digital demodulation and phase noise compensation. The baseband quadrature signals of the quantum and pilot are demodulated from the intermediate frequency signals by orthogonal downconversion and low-pass filtering. Because it experiences the same phase drift in the long-distance transmission fiber, the phase noise of the quantum signal can be compensated by using the estimated phase of the pilot signal. In our experimental implementation, we define the quantum state by weighted averaging the sampled data within one period. The number of samples per transmitted symbol is 10 (calculated by dividing the 25 Gsample/s sampling rate with the 2.5 GHz symbol rate). Thus, the amplitude and phase quadratures of the quantum signal are obtained by weighted averaging 10 samples per symbol.

(4) Parameter estimation. This includes estimation of the quantum channel transmittance, excess noise, and SKR.

For the case where no long-distance transmission fibers are connected and the modulation variance V_A is set to 60, the recovered constellation diagrams without and with DSP stages are depicted in Fig. 3, where 1.6×10^6 samples are included in each constellation diagram. We can see that the initial constellation without DSP [Fig. 3(a)] is a two-circle pattern, owing to the frequency offset and phase noise of two independent lasers. In contrast, the frequency offset and phase noise can be effectively compensated by running the DSP chain and the recovered constellation is shown in Fig. 3(b), where 16 symbols can be clearly discriminated.

The calibration of shot noise is extremely important because all the measured signals of Bob are normalized to shot noise units (SNU). The electronic noise variance can be measured when both the lasers at the transmitter and receiver are turned off, and the sum of shot noise variance and electronic noise variance can be measured when the laser at the transmitter is turned off. To obtain the correct electronic noise and shot noise, the same DSP operations applied to the quantum signals are applied simultaneously to the samples of the shot noise and electronic noise. More precisely, the raw data are bandpass-filtered, downconverted, and weighted averaged. The excess noise referred to

Table 1. Experimental Modulation Parameters, Averaged Excess Noise ε, SNR of Quantum Signal, and SKR at Different SMF Lengths

L (km)	α_1	α_2	p_1	α_c	V_A	SNR (dB)	ε	SKR (Mbits/s)
25	0.675	1.55	3.2/48	1.025	2.73	−9.24	0.0257	49.02
50	0.65	1.5	3.5/48	1.075	2.37	−14.85	0.0228	11.86
80	0.6	1.4	3.5/48	1.133	2.05	−21.48	0.0289	2.11

Alice's site is expressed as

$$\varepsilon_A = 2 \cdot \frac{V_B - 1 - V_{ele}}{\eta T} - V_A, \tag{1}$$

where V_A, V_B, and V_{ele} denote the modulation variance of Alice, the variance of Bob's data, and the electronic noise variance of the balanced receiver, respectively, which have been normalized to SNU. In addition, T is the channel transmittance and η is the quantum efficiency of the receiver. The factor of two comes from the image band vacuum, owing to the heterodyne detection. The asymptotic SKR against collective attacks is given by [13,19]

$$K^{\infty} = R_s \cdot (1-a) \cdot (1 - \mathrm{FER}) \cdot \left(\min_{\rho_{AB} \in S} D\left[\mathcal{G}(\rho_{AB}) \,\|\, \mathcal{Z}(\mathcal{G}(\rho_{AB}))\right] - p_{\mathrm{pass}} \delta_{EC} \right), \tag{2}$$

where R_s is the signal repetition rate of the system, a is the overhead ratio for parameter estimation, and FER is the frame error rate (see Supplement 1 for details).

We implemented the high-rate LLO DM CV-QKD scheme over different lengths of standard telecom optical fiber (SMF-28). For each channel length, the QKD system was operated continuously over 150 min of acquisition time. A total of 50 original data blocks were taken with each block size of 768 M, which means that each block contains 76.8 M symbols (quadratures), and the interval between each data block was about 3 min (acquiring and saving the data). Notice that the modulation parameters, including the two ring amplitudes α_1, α_2, the boundary between the inner and outer regions α_c, and the choice probabilities p_1, p_2, are crucial to the SKR. To maximize the SKR at each transmission distance, we numerically searched the optimal modulation parameters based on the experimental parameters: the quantum efficiency η of the receiver is 0.336, the electronic noise v_e is 0.215 SNU, and the reconciliation efficiency β is 0.95. Table 1 shows the experimental modulation parameters, excess noise ε, and SKR at SMF lengths of 25, 50, and 80 km, respectively.

The experimental results of excess noise of the QKD system over 25 km, 50 km, and 80 km of standard telecom SMF are illustrated in Fig. 4; each data block of 76.8 M is used for the estimation of excess noise. In Fig. 4, the dots plot the experimental results of the excess noise for 50 sampled data blocks; the mean excess noise is 0.0257, 0.0228, and 0.0289 SNU over transmission distances of 25 km, 50 km, and 80 km, respectively. With the increase of transmission distance, the fluctuation of excess noises is stronger; this is mainly caused by the larger loss of fiber link and the shot noise fluctuation. Moreover, the excess noise in our experimental system is mainly attributed to the residual phase noise between the LLO and the signal field, and the measurement noise at the receiver side.

The experimental SKR at different transmission distances is depicted in Fig. 5. The dots represent the experimental

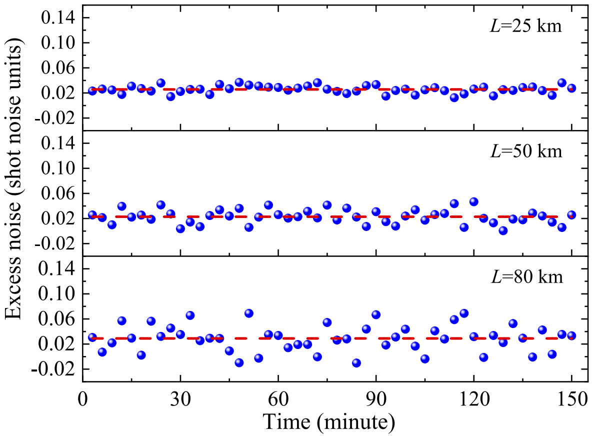

Fig. 4. Experimental excess noise at different SMF lengths. Dots show the experimental results. Dashed curves denote the average value of the excess noise, 0.0257 SNU (L = 25 km), 0.0228 SNU (L = 50 km), and 0.0289 SNU (L = 80 km), respectively.

averaged SKR at transmission distances of 25 km, 50 km, and 80 km, which are 49.02 Mbits/s, 11.86 Mbits/s and 2.11 Mbits/s, respectively. For comparison, the SKR of the GM protocol (solid curve) are also plotted in Fig. 5. As can be seen, the performance of our 16-symbol two-ring constellation is very close to the GM protocol. More precisely, it can achieve 67.4%, 40.6%, and 66.5% of the SKR performance of GM at distances of 25 km, 50 km, and 80 km, respectively. In Fig. 5, the simulated SKR of 16-symbol QAM and APSK constellations under the security frame of the analytical SKR are also included for comparison [14]. The SKR of 16-symbol QAM (APSK) is 45.8% (28.8%), 40.6% (16.9%), 26.9% of GM at distances of 25 km, 50 km, and 80 km, respectively. We find that the SKR of our system has a significant improvement in comparison with previous works. This is because the security frame of our protocol can enable a high SKR comparable with the GM protocol even if a small constellation size is employed. In this case, we can achieve a higher system symbol rate (2.5 Gbaud) and low excess noise level, even at a long distribution distance of 80 km.

In conclusion, we have experimentally demonstrated a high-performance discrete-modulation LLO CV-QKD at a symbol rate of 2.5 Gbaud over 80 km of telecom SMF by using the 16-symbol two-ring constellation protocol. Benefiting from the performance of the protocol implemented by us, a high SKR comparable with the GM was realized based on a small constellation size, and the excess noise is low enough to support our system to operate at high symbol rates and long distances. The achieved SKR of 49.02 Mbits/s, 11.86 Mbits/s, and 2.11 Mbits/s over 25-km, 50-km, and 80-km SMF can reach 67.4%, 70.0%, and 66.5% of the GM protocol. Our system provides an attractive alternative for a high-SKR, cost-effective, metropolitan-area quantum private network. In our future work, we will improve the system performance by suppressing the excess noise to an ultra-low level and consider the impact of the finite-size effect. Furthermore, real-time DSP will be developed.

Funding. Innovation Program for Quantum Science and Technology (2021ZD0300703); National Natural Science Foundation of China (62175138, 62205188); Key Research and Development Program of Guangdong Province (2020B0303040002); Shanxi 1331KSC.

Disclosures. The authors declare no conflicts of interests.

Data availability. Datasets generated and analyzed for simulation are available from the corresponding author upon reasonable request.

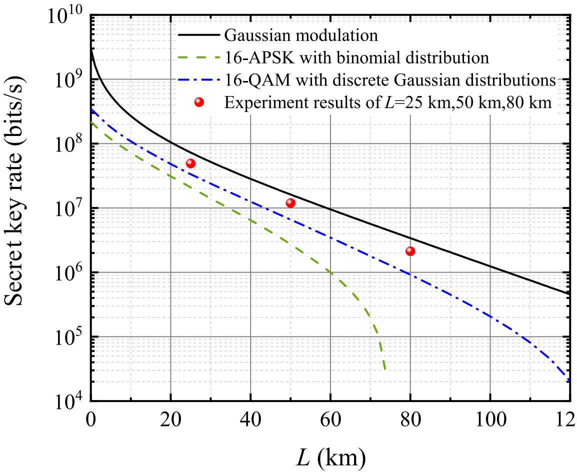

Fig. 5. SKR versus transmission distance. Dots show experimental results over transmission distances of 25 km, 50 km, and 80 km. Solid curve: simulation result of GM. For comparison, simulation results of 16-APSK (dashed curve) and 16-QAM (dashed-dotted curve) are also plotted. Parameters a and FER are 0.1 and 0.15, respectively. Simulation parameter of excess noise is 0.0258.

Supplemental document. See Supplement 1 for supporting content.

REFERENCES

1. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
2. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
3. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Phys. Rev. Lett. **125**, 010502 (2020).
4. B. Qi, H. Gunther, P. G. Evans, B. P. Williams, R. M. Camacho, and N. A. Peters, Phys. Rev. Appl. **13**, 054065 (2020).
5. Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, B. Liu, W. Huang, and B. Xu, Opt. Lett. **47**, 3307 (2022).
6. Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Optica **9**, 492 (2022).
7. N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, and U. L. Andersen, Nat. Commun. **13**, 4740 (2022).
8. P. Huang, T. Wang, R. Chen, P. Wang, Y. Zhou, and G. Zeng, New J. Phys. **23**, 113028 (2021).
9. M. Zhang, P. Huang, P. Wang, S. Wei, and G. Zeng, Opt. Lett. **48**, 1184 (2023).
10. E. Kaur, S. Guha, and M. M. Wilde, Phys. Rev. A **103**, 012412 (2021).
11. W. Liu, X. Wang, N. Wang, S. Du, and Y. Li, Phys. Rev. A **96**, 042312 (2017).
12. S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Phys. Rev. X **9**, 021059 (2019).
13. J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X **9**, 041064 (2019).
14. A. Denys, P. Brown, and A. Leverrier, Quantum **5**, 540 (2021).
15. S. Kleis, M. Rueckmann, and C. G. Schaeffer, Opt. Lett. **42**, 1588 (2017).
16. D. Milovancev, N. Vokic, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, J. Lightwave Technol. **39**, 3445 (2021).
17. F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. Trigo Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, "Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution," arXiv, arXiv:2207.11702 (2022).
18. D. Pereira, M. Almeida, M. F. ao, A. N. Pinto, and N. A. Silva, Opt. Lett. **47**, 3948 (2022).
19. P. Wang, Y. Zhang, Z. Lu, X. Wang, and Y. Li, New J. Phys. **25**, 023019 (2023).