Long-distance discrete-modulated continuous-variable quantum key distribution over 126.56 km of fiber with a local local oscillator

Yan Pan[1, †], Mingze Wu[2, †], Heng Wang[1], Junhui Li[2, *], Yun Shao[1], Jie Yang[1, 2], Yaodi Pi[1], Ting Ye[1], Ao Sun[1], Lin Jiang[3], Lianshan Yan[3], Wei Pan[3], Yang Li[1], Wei Huang[1], Song Yu[2], Yichen Zhang[2], and Bingjie Xu[1, **]

(1) National Key Laboratory of Security Communication, Institute of Southwestern Communication, Chengdu 610041, China

(2) State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

(3) Center for Information Photonics & Communications, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, 611756, Sichuan, China

[†]These authors contributed equally. Corresponding authors: [*]lijunhuiphy@bupt.edu.cn, [**]xbjpku@163.com

Supplementary Note 1: Transmission performance analysis of QPSK and 16-QAM protocols

In classical coherent optical communications, lower-order modulation formats such as QPSK indeed enable longer transmission distances than higher-order formats like 16QAM. However, although four-state protocols offer improved noise suppression, within the theoretical framework of protocol security, their theoretical security bounds are generally less tight than those enabled by higher-order modulation schemes. This observation has been well established in the literature [S1-S3]. Meanwhile, regarding the comparison of transmission performance between QPSK and 16QAM, we have supplemented our analysis with simulations that evaluate the protocol performance under different excess noise levels, as shown in Fig. S1. The modulation variances of both the QPSK and 16QAM protocols are optimized, and all other parameters are consistent with our experimental settings. These simulations help to identify the crossover point in the secret key rate performance. Under our experimental parameters, when the excess noise is 0.04, QPSK modulation supports a maximum transmission distance of only about 70 km, whereas 16QAM modulation can achieve transmission distances exceeding 180 km. Furthermore, Fig. S1 shows that, under the same or even higher excess noise conditions, the transmission performance of 16QAM is significantly superior to that of QPSK. Therefore, 16QAM is selected in this work for the experimental validation of long-distance transmission.

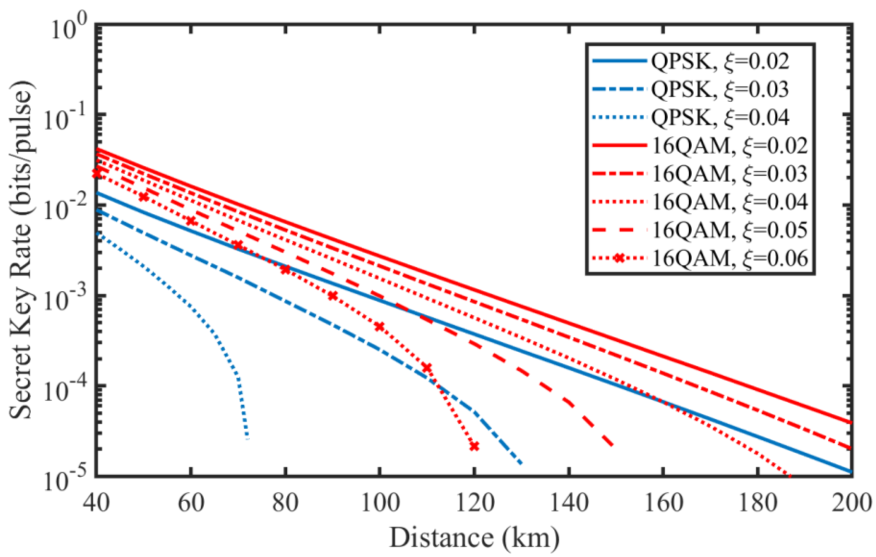

Fig. S1 Performance comparison of QPSK protocol and 16QAM protocol under different excess noise.

Supplementary Note 2: The LMS-based fractionally spaced equalizer

The phase noise and frequency offset of the quantum signal can be mainly corrected by the reference optical signal, but the correction accuracy is limited due to the synchronization and sampling precision between the reference and quantum signals. In this case, residual phase noise, IQ imbalance, sampling offset, and inter-symbol interference (ISI) will introduce uncontrollable noise. Residual phase noise, arising from phase mismatch between the reference and quantum signals, can be compensated by estimating a constant phase offset from the training sequence. IQ imbalance, caused by discrepancies between the *x* and *p* quadratures during modulation and transmission, can be addressed using a butterfly filter structure. Sampling offset and ISI are effectively suppressed by the fractionally spaced nature of the equalizer. In our experiment, the LMS-based fractionally spaced equalizer (FSE) is capable of compensating for all three effects simultaneously, implemented using a real-valued FIR filter trained by the LMS algorithm [S4].

Let s_x and s_p be the x and p components of quantum signal, respectively. The outputs of the real-valued finite-impulse response (FIR) filters are given as:

$$s_x^o = \omega_{11}^T s_x + \omega_{12}^T s_p$$
$$s_p^o = \omega_{21}^T s_x + \omega_{22}^T s_p \tag{S1}$$

where ω_{11}, ω_{12}, ω_{21} and ω_{22} are the tap weights of the FIR filters, and T represents transposition. Here, a pilot-aided least-mean-square algorithm is used to update the tap weights as follows:

$$\omega_{11}(n+1) = \omega_{11}(n) + \mu\varepsilon_x(n)s_x$$
$$\omega_{12}(n+1) = \omega_{12}(n) + \mu\varepsilon_x(n)s_p$$
$$\omega_{21}(n+1) = \omega_{21}(n) + \mu\varepsilon_p(n)s_x \tag{S2}$$
$$\omega_{22}(n+1) = \omega_{22}(n) + \mu\varepsilon_p(n)s_p$$

where μ is the step size parameter, ε_x and ε_p can be obtained from the error functions as follows:

$$\varepsilon_x = TS_x - s_x^o$$
$$\varepsilon_p = TS_p - s_p^o \tag{S3}$$

where TS_x and TS_p are the training symbols. After the convergence of the training process, the optimal tap weights of the real-valued FIR filters can be obtained. More details about the pilot-aided equalization can be found in Ref. S5. To quantitatively evaluate the performance of this LMS-based FSE, we processed the same dataset using three different approaches: fixed phase compensation, symbol-spaced equalization (SSE), and fractionally spaced equalization (the proposed method). The resulting cross-correlation coefficients are summarized in Table S1. The data indicates that the LMS-based FSE significantly enhances the correlation between Alice's and Bob's data while simultaneously reducing the cross-correlation between the x and p quadratures. These results demonstrate that the proposed algorithm effectively improves the quality of the raw key data.

Table S1 Correlation coefficients of the x and p quadratures after different algorithms

Correlation Coefficient	Before compensation/ equalization	Fixed phase compensation	Symbol-spaced equalization	Fractionally spaced equalization
$\langle x_A, x_B\rangle$	0.0357	0.0627	0.0681	0.0786
$\langle x_A, p_B\rangle$	-0.0516	-0.0017	0.0005	0.0003
$\langle p_A, x_B\rangle$	0.0528	0.0026	-0.0007	-0.0002
$\langle p_A, p_B\rangle$	0.0357	0.0636	0.0684	0.0787

It should be noted that, when the LMS algorithm has not yet converged, the filter weights randomly fluctuate around the optimal point, and the output signal still contains uncompensated distortion components. In this case, the compensation of the LMS algorithm exhibits significant uncertainty. Theoretically, the LMS filter behavior during the non-converged stage represents a noisy transient process, which cannot reliably reflect the actual system response. As shown in Fig. S2, the quantum signal after LMS compensation exhibits noticeable distortion in the initial non-converged period, where the signal variance may be lower than the shot-noise variance. It should be emphasized that such non-converged compensation may lead to either negative or abnormally large excess noise values in CV-QKD systems. The observed inaccurate excess noise was therefore not a physical phenomenon but rather an artifact caused by using non-converged data during the equalization stage. Once the equalizer reaches convergence, the excess noise returns to its expected level.

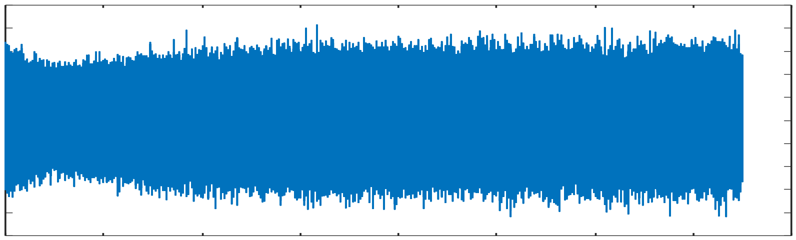

Fig. S2 The amplitude of the *x*-component of the quantum signal after equalization in the case of μ=2e-6

Supplementary Note 3: Detection efficiency calibration method

Based on the responsivity of the polarization diversity receiver module provided by the manufacturer, we first estimated an approximate detection efficiency by $\eta_1 = R \times \frac{hc}{\lambda e}$, where R=0.95 A/W, $\frac{hc}{\lambda e} = 0.8$. Then, we can calculate that the approximate detection efficiency η_1 is 0.76. To obtain a more accurate calibration of the receiver's quantum detection efficiency, we performed the following procedure:

1) The optical power of the transmitted quantum signal was precisely measured using a high-accuracy power meter, from which the corresponding modulation variance was derived.

2) As shown in Fig. 1 of the manuscript, the transmitter and receiver were directly connected in a back-to-back configuration, and data were acquired under this condition.

3) The collected data were processed, and the link transmittance T was estimated using the initial efficiency η_1.

4) η_1 was then corrected by taking into account the pre-calibrated connector loss, the insertion loss of the polarization controller, and the estimated T, yielding the system-calibrated detection efficiency η_2.

5) The above measurement was repeated ten times, and the final detector quantum efficiency was determined as the average value of all η_2 results.

During the experimental procedure, multiple polarization diversity receiver modules were carefully calibrated, and the module exhibiting the superior detection efficiency was selected. Finally, the polarization diversity receiver module with a calibrated detection efficiency of 0.714 (a value close to those reported in Refs. [S5-S7]) was employed in the experiments.

Supplementary References

[S1] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," Quantum, 5(1), 540 (2021).

[S2] P. Wang, Y. Zhang, Z. Lu, X. Wang, and Y. Li, "Discrete-modulation continuous-variable quantum key distribution with a high key rate," New J. Phys. 25, 023019 (2023).

[S3] Y. Pan, H. Wang, Y. Shao, et al., “Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system,” Opt. Lett. 47(13): 3307-3310 (2022).
[S4] M. S. Faruk, and S. J. Savory, “Digital Signal Processing for Coherent Transceivers Employing Multilevel Formats,” J. Lightwave Technol., 35(5): 1125-1141 (2017).
[S5] N. Jain, H. Chin, H. Mani, et al., “Practical continuous-variable quantum key distribution with composable security,” Nature Communications, 13(1):4740, 2022.
[S6] J. Liao, Z. Chen, J. Wang, et al., “Experimental demonstration of highspeed continuous variable quantum key distribution enhanced by phase-sensitive amplifier,” npj Quantum Information, 11(1):105, 2025.
[S7] F. Roumestan, A. Ghazisaeidi, J. Renaudier, et al., “Shaped constellation continuous variable quantum key distribution: Concepts, methods and experimental validation,” Journal of Lightwave Technology, 42(15): 5182-5189, 2024.