

# High-Rate Discrete-Modulated Continuous-Variable Quantum Key Distribution with Composable Security

Mingze Wu<sup>1,\*</sup>, Yan Pan<sup>2,\*</sup>, Junhui Li<sup>1</sup>, Heng Wang<sup>2</sup>, Lu Fan<sup>1</sup>, Yun Shao<sup>2</sup>,  
Yang Li<sup>2</sup>, Wei Huang<sup>2</sup>, Song Yu<sup>1</sup>, Bingjie Xu<sup>2,†</sup> and Yichen Zhang<sup>1,‡</sup>

<sup>1</sup>State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, *Beijing University of Posts and Telecommunications*, Beijing 100876, China

<sup>2</sup>National Key Laboratory of Security Communication, Institute of Southwestern Communication, Chengdu 610041, China



(Received 14 March 2025; revised 14 February 2026; accepted 23 April 2026; published 20 May 2026)

Continuous-variable quantum key distribution holds the potential to generate high secret key rates, making it a prime candidate for high-rate metropolitan quantum network applications. However, despite these promising opportunities, the realization of high-rate continuous-variable quantum key distribution systems with composable security remains an elusive goal. Here, we report a discrete-modulated continuous-variable quantum key distribution system with a composable secret key rate of 18.93 Mbps against collective attacks over a 25-km fiber channel. This record-breaking rate is achieved through the probability-shaped 16 quadrature amplitude modulation-modulated protocol, which employs semidefinite programming to ensure its composable security. Furthermore, we have employed a fully digital and precise quantum signal processing technique to reduce excess noise to extremely low levels, thereby facilitating efficient broadband system operation. While ensuring low complexity and cost, our system achieves a performance advantage of over an order of magnitude compared to previous continuous-variable quantum key distribution systems, providing a promising solution for future deployment of quantum key distribution.

DOI: [10.1103/882y-w4zy](https://doi.org/10.1103/882y-w4zy)

Subject Areas: Quantum Information

## I. INTRODUCTION

Quantum key distribution (QKD) is a pioneering method for secret key distribution with information-theoretical security between two remote parties [1–4]. Continuous-variable (CV) QKD is a promising technological pathway, which can achieve high key rates within metropolitan areas and exhibits strong compatibility with optical communication systems [5,6]. CV-QKD can adopt two typical modulation formats: Gaussian modulation [7–9] and discrete modulation [10–14]. Gaussian-modulated CV-QKD protocols have advanced significantly in terms of theoretical security analysis [15–18], and various high-performance systems implementing these protocols have been reported [19–26].

Despite these advancements, development of a high-rate experimental CV-QKD system with composable security

remains a challenge. The Gaussian-modulated protocol requires thousands of constellations to approximate a continuous Gaussian distribution [27], which demands sophisticated modulation devices and rigorous classical error correction programs [10]. These intricate processes present a significant challenge in suppressing excess noise, particularly at high repetition rates. In contrast, discrete-modulated CV-QKD protocols employ a smaller constellation space, thereby enhancing their compatibility with high-speed wireline components [28]. This advantage allows discrete-modulated protocols to achieve higher repetition frequencies and lower excess noise. More importantly, it compensates for the performance degradation introduced by composable security, making discrete-modulated protocols a strong candidate for addressing the demands of high-rate CV-QKD systems with composable security.

Over the past few years, significant progress has been made in proving the asymptotic security of discrete-modulated CV-QKD using various methods [11–14]. Building on these theoretical foundations, various experimental implementations of discrete-modulated CV-QKD with asymptotic security have been reported [29–35]. Recently, the composable security of quadrature phase shift keying (QPSK)-modulated CV-QKD protocols has also been proven [36,37], marking another important milestone in enhancing the security of these systems.

\*These authors contributed equally to this work.

†Contact author: [xbjpku@163.com](mailto:xbjpku@163.com)

‡Contact author: [zhangyc@bupt.edu.cn](mailto:zhangyc@bupt.edu.cn)

Published by the American Physical Society under the terms of the *Creative Commons Attribution 4.0 International* license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

These theoretical advancements make it possible to implement discrete-modulated CV-QKD systems with composable security. However, a QPSK-modulated protocol using small constellations falls short in meeting the performance requirements of high-rate systems. Therefore, there is a pressing need to address this challenge and explore alternative modulation techniques or system architectures that can support high-rate CV-QKD with composable security.

In this paper, we address the critical challenge of enhancing the key rate in discrete-modulated CV-QKD systems with composable security. Recognizing that approximate Gaussian distribution outperforms uniform distribution in the quantum state preparation process of CV-QKD, we adopt probability-shaped 16 quadrature amplitude modulation (QAM) as a strategy to break through the performance limitation of the discrete-modulated CV-QKD system. Given the lack of a security analysis for 16QAM-modulated CV-QKD protocols with composable security, we embark on a comprehensive theoretical analysis using an advanced security analysis method grounded in semidefinite programming (SDP) [36]. Building upon this theory, we proceed to conduct an experimental demonstration of the 16QAM-modulated CV-QKD protocol. To enhance the system's flexibility and improve its excess noise suppression performance, a fully digital and high-precision quantum signal processing method is proposed and successfully validated. Notably, our system achieves a remarkable composable key rate of 18.93 Mbps over a 25-km fiber channel. This performance surpasses previous CV-QKD systems by more than an order of magnitude and is competitive with the most advanced high-rate discrete-variable QKD systems. Our findings not only demonstrate the feasibility of high key rates CV-QKD systems with composable security, but also pave the way for promising future deployments of QKD technologies.

This paper is structured as follow. In Sec. II, the CV-QKD protocol with 16QAM modulation is introduced and its composable security is analyzed. Modeling the channel, protocol performance is simulated. In Sec. III, an experimental system for the protocol is demonstrated. Lastly, discussions are offered, and the work is concluded in Sec. IV.

## II. PROBABILITY-SHAPED 16QAM-MODULATED CV-QKD PROTOCOL WITH COMPOSABLE SECURITY

In this section, a probability-shaped 16QAM-modulated CV-QKD protocol with composable security is described. Following this, analysis of its theoretical security is presented. To evaluate performance of the composable 16QAM-modulated CV-QKD protocol, the channel is theoretically modeled as a noisy and lossy Gaussian channel, simulating protocol performance.

### A. Protocol description

First, the composable 16QAM-modulated CV-QKD design is shown in Fig. 1. The protocol is described as follows.

- (i) *State preparation*—For each round, Alice prepares one of the 16 coherent states  $|\alpha_k\rangle$  which are centered at possible equidistant points with probability  $P_k$  and transmits it to Bob through the quantum channel, where

$$\alpha_k = q_k + ip_k, \quad k \in \{0, 1, 2, \dots, 15\}, \quad (1)$$

$$P_k = \frac{\exp(-\nu(q_k^2 + p_k^2))}{\sum_{k=0}^{15} \exp(-\nu(q_k^2 + p_k^2))}. \quad (2)$$

Among them, adjacent states are equally spaced, and we can fix the position of each state by controlling the total variance of each coordinate.  $\nu$  needs to satisfy  $\nu > 0$ .

- (ii) *Heterodyne measurement*—After receiving the quantum states, Bob performs trusted heterodyne detection with efficiency  $\eta_d$ , electrical noise  $\nu_{el}$ , and finite detection range  $M$  to obtain measurement result  $Y_j \in \mathbb{C}$  for each round. The schematic diagram of the 16QAM-modulated CV-QKD protocol with trusted detector model is shown in Fig. 2.

After repeating the above physical steps  $N$  times, Alice and Bob perform the classical postprocessing steps.

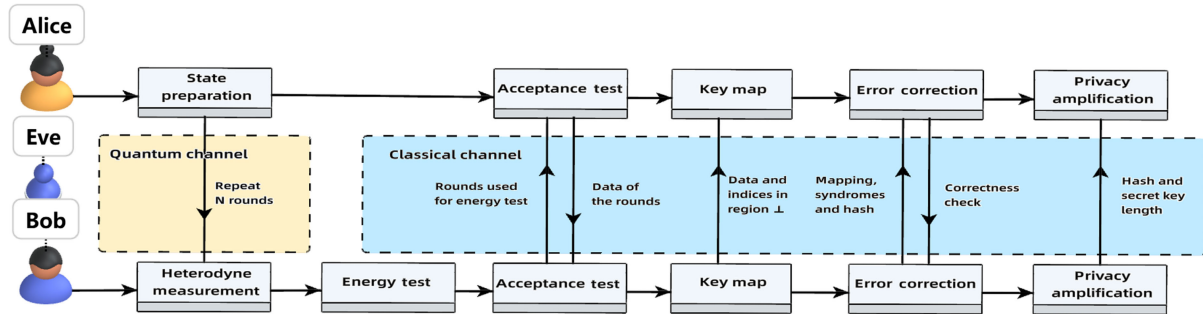


FIG. 1. Composable discrete-modulated CV-QKD protocol. The protocol mainly includes state preparation, heterodyne measurement, energy test, acceptance test, key map, error correction, and privacy amplification, specified in Sec. II A.

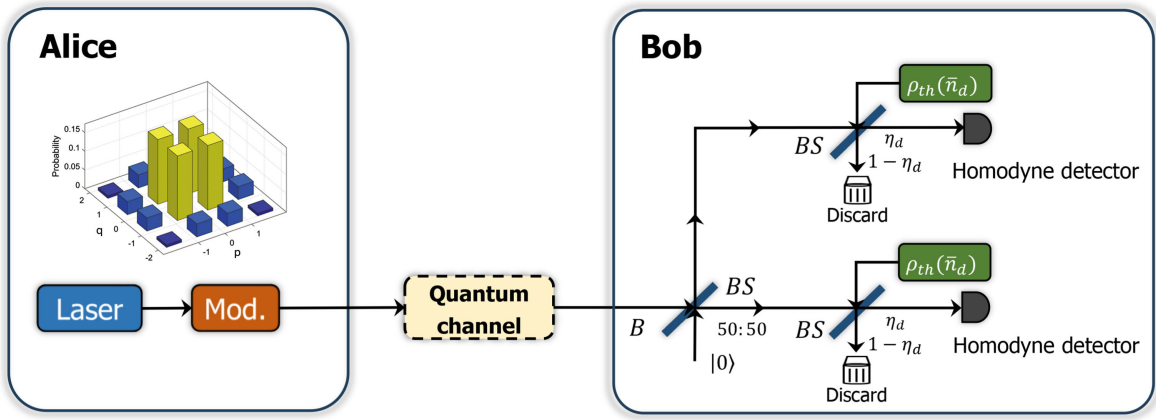


FIG. 2. Schematic diagram of a 16QAM-modulated CV-QKD protocol with trusted detector model, where  $\rho_{th}(\bar{n}_d)$  is a thermal state with average photon number  $\bar{n}_s$ . Mod, modulator; BS, beam splitter;  $\eta_d$ , detection efficiency. The inset of Alice shows the probability distribution of the modulation format.

- (iii) *Energy test*—Bob performs energy test using  $m \ll N$  rounds of raw measurement results. Bob selects test parameter  $0 < \beta_{test} \leq M$  and number of rounds  $l_T$  that may not satisfy the testing condition. If  $\Pr[\{Y_j : |Y_j|^2 < \beta_{test}\} | \leq l_T] \leq \epsilon_{ET}$ , which means that most of the weights of transmitted signals are located in a finite-dimensional Hilbert space [36], the test passes, except for a small error probability  $\epsilon_{ET}$ . Otherwise, Alice and Bob abort the protocol.
- (iv) *Acceptance test*—If the energy test passed, Bob discloses which rounds are used for energy test through classical channel, and Alice discloses the data sent in these rounds to estimate the statistics of their observations. Afterward, Bob define an acceptance set  $S^{AT}$  that can be considered as a list of accepted observations. If the statistical estimators are within the acceptance set, the test passes, except for a small error probability  $\epsilon_{AT}$ . Otherwise, Alice and Bob abort the protocol.
- (v) *Key map*—For the remaining  $n := N - m$  rounds, Bob performs a reverse coordination key map to determine the raw key data  $Z$ . For this purpose, Bob's measurement results  $Y_j$  are discretized into a set  $z \in \{0, 1, 2, \dots, 15, \perp\}$ , discarding the symbols mapped to  $\perp$ :

$$Z_j = \begin{cases} z & \text{if } Y_j \in A_z, \\ \perp & \text{otherwise,} \end{cases} \quad (3)$$

where  $A_z$  represents the regions illustrated in Fig. 3 and are further elaborated in Appendix A.

- (vi) *Error correction*—Alice maps the data to  $\{0, 1, 2, \dots, 15\}$  according to the corresponding rules

$$x_j = k, \quad \text{if } |\psi_j\rangle = |\alpha_k\rangle, \quad (4)$$

where  $k \in \{0, 1, 2, \dots, 15\}$ . Alice and Bob publicly communicate over classical channel to reconcile their

- raw keys  $X$  and  $Z$ . After the error correction, Alice and Bob share the raw key, except for a small portion  $\epsilon_{EC}$ .
- (vii) *Privacy amplification*—Alice and Bob apply two universal hash functions to their raw keys. Except for a small failure probability of  $\epsilon_{PA}$ , Alice and Bob share the secret key.

## B. Security analysis

Next, we analysis the security of the 16QAM-modulated CV-QKD protocol. Based on the security analysis framework [36], secret key length  $\ell$  of the 16QAM-modulated CV-QKD protocol with  $\epsilon = \epsilon_{EC} + \max\{\frac{1}{2}\epsilon_{PA} + \bar{\epsilon}, \epsilon_{ET} + \epsilon_{AT}\}$  security satisfies

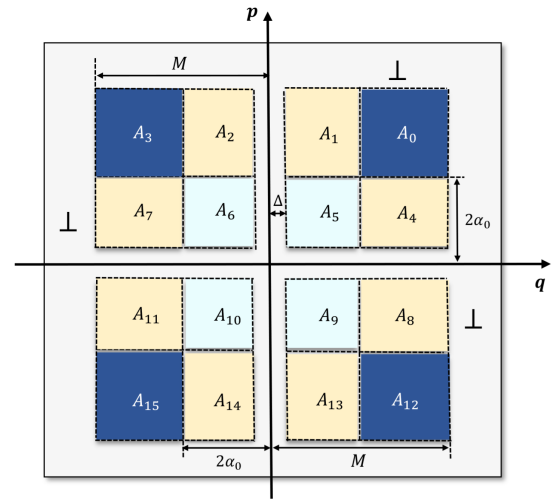


FIG. 3. Bob's key map process involves assigning values to the measurement results  $Y$ . Each region  $A_z$  corresponds to a specific key map value  $z$ , and  $\alpha_0$  represents the distance between adjacent average states at Bob's side. During the postselection phase, measurement results falling within a range of less than  $\Delta$  from the coordinate axis or exceeding the detection limit are disregarded and instead marked with the symbol  $\perp$ .

$$\frac{\ell}{N} \leq \frac{n}{N} \left[ \min_{\bar{\rho} \in S^{\text{E\&A}}} H(X|E')_{\bar{\rho}} - \Delta(w) - \delta(\bar{\epsilon}) \right] - \delta_{\text{leak}}^{\text{EC}} - \frac{2}{N} \log_2 \left( \frac{1}{\epsilon_{\text{PA}}} \right), \quad (5)$$

where  $n$  is the rounds used to generate secret key,  $N$  is the total number of rounds,  $\delta_{\text{leak}}^{\text{EC}}$  takes the classical error correction cost into account,  $\delta(\bar{\epsilon}) = 2 \log_2[\text{rank}(\rho_A) + 3] \sqrt{\log_2(2/\bar{\epsilon})/n}$ ,  $\bar{\epsilon}$  is the security parameter for smoothing, and  $\Delta(w)$  is the determine correction term as

$$\Delta(w) := \sqrt{w} \log_2(|Z|) + (1 + \sqrt{w}) h\left(\frac{\sqrt{w}}{1 + \sqrt{w}}\right), \quad (6)$$

where  $|Z|$  represents the dimension of key map,  $h(\cdot)$  is binary entropy, and, for 16QAM-modulated CV-QKD, the bound weight  $w$  satisfies

$$w = \sum_{k=0}^{15} P_k \frac{\langle \hat{n}_{\beta_k}^2 \rangle - \langle \hat{n}_{\beta_k} \rangle}{N_c(N_c + 1)}, \quad (7)$$

where  $N_c$  is the subspace dimension parameter. The minimization term  $\min_{\bar{\rho} \in S^{\text{E\&A}}} H(X|E')_{\bar{\rho}}$  needs to be calculated using SDP.  $S^{\text{E\&A}}$  contains all states that pass both the energy test and acceptance test except for probability  $(\epsilon_{\text{ET}} + \epsilon_{\text{AT}})$ .

To cope with practical experiments, we consider the trusted detector noise model [38], as shown in Fig. 2, where both detectors exhibit identical efficiency  $\eta_d$  and have the same level of electronic noise  $\nu_{\text{el}}$ . The electronic noise is modeled as a thermal state  $\bar{n}_s$  with average photon number  $\bar{n}_s$ , where  $\bar{n}_s = \nu_{\text{el}}/[2(1 - \eta_d)]$ , and the efficiency is modeled as a beam splitter with transmittance  $\eta_d$ . The conditional entropy  $H(X|E')_{\bar{\rho}}$  of the 16QAM-modulated protocol is detailed in Appendix A. On this basis, the SDP can be described as

$$\text{minimize } H(X|E')_{\bar{\rho}} \\ \bar{\rho} \in S^{\text{E\&A}}$$

subject to

$$\begin{cases} 1 - w \leq \text{Tr}(\bar{\rho}) \leq 1, \\ \frac{1}{2} \|\text{Tr}_B(\bar{\rho}) - \tau_A\|_1 \leq \sqrt{2w - w^2}, \\ \text{Tr} \left[ \left( \frac{1}{P_k} |k\rangle\langle k| \otimes \hat{n}_{\beta_k} \right) \bar{\rho} \right] \leq \langle \hat{n}_{\beta_k} \rangle + \mu_{\hat{n}_{\beta_k}}, \\ \text{Tr} \left[ \left( \frac{1}{P_k} |k\rangle\langle k| \otimes \hat{n}_{\beta_k} \right) \bar{\rho} \right] \geq \langle \hat{n}_{\beta_k} \rangle - \mu_{\hat{n}_{\beta_k}} - w \|\hat{n}_{\beta_k}\|_{\infty}, \\ \text{Tr} \left[ \left( \frac{1}{P_k} |k\rangle\langle k| \otimes \hat{n}_{\beta_k}^2 \right) \bar{\rho} \right] \leq \langle \hat{n}_{\beta_k}^2 \rangle + \mu_{\hat{n}_{\beta_k}^2}, \\ \text{Tr} \left[ \left( \frac{1}{P_k} |k\rangle\langle k| \otimes \hat{n}_{\beta_k}^2 \right) \bar{\rho} \right] \geq \langle \hat{n}_{\beta_k}^2 \rangle - \mu_{\hat{n}_{\beta_k}^2} - w \|\hat{n}_{\beta_k}^2\|_{\infty}, \\ \bar{\rho} \geq 0, \end{cases} \quad (8)$$

where  $\hat{n}_{\beta_k}$  is the displaced photon number operator,  $\hat{n}_{\beta_k}^2$  is the displaced squared photon number operator,  $\beta_k = \sqrt{\eta} \alpha_k$  is the mean position of received state in the phase space after passing through the channel with transmittance  $\eta$ , the photon-number operator  $\hat{n} = \hat{a}^\dagger \hat{a}$ , and  $X_\gamma = \hat{D}(\gamma) X \hat{D}^\dagger(\gamma)$ , where  $\hat{D}(\gamma)$  is the displacement operator with complex parameter  $\gamma$ .  $\langle \hat{n}_{\beta_k} \rangle$  and  $\langle \hat{n}_{\beta_k}^2 \rangle$  are expectation of operators, which need to be calculated through measured result. The estimation method of the statistics is detailed in Appendix B.  $\mu_{\hat{n}_{\beta_k}}$  and  $\mu_{\hat{n}_{\beta_k}^2}$  are parameters introduced by acceptance test which are defined as

$$\mu_{\hat{n}_{\beta_k}} := \sqrt{\frac{\|\hat{n}_{\beta_k}\|_{\infty}^2}{2k_T} \ln\left(\frac{2}{\epsilon_{\text{AT}}}\right)}, \quad (9)$$

$$\mu_{\hat{n}_{\beta_k}^2} := \sqrt{\frac{\|\hat{n}_{\beta_k}^2\|_{\infty}^2}{2k_T} \ln\left(\frac{2}{\epsilon_{\text{AT}}}\right)}. \quad (10)$$

$\tau_A$  is the quantum state of Alice's system which can be described as

$$\tau_A = \sum_{k,k'=0}^{15} \sqrt{P_k P_{k'}} \langle \varphi_{k'} | \varphi_k \rangle |k\rangle \langle k'|_A. \quad (11)$$

In summary, the upper bound of composable secret key length against collective attacks can be obtained from Eq. (5).

### C. Simulation method

To evaluate the protocol performance, we simulate the quantum channel as a Gaussian channel with transmission  $\eta_t$  and excess noise  $\xi$ , where  $\eta_t = 10^{-\alpha L/10}$  for transmission distance  $L$  in kilometers and  $\alpha = 0.2$  dB/km is the fiber loss. The excess noise  $\xi$  is determined at the channel input, for example, as preparation noise, so that Bob sees effective noise  $\eta_t \xi$ .

According to the channel model, the statistical estimators used for SDP can be calculated as [39]

$$\langle \hat{n}_{\beta_k} \rangle = \frac{\eta_t \xi}{2}, \quad (12)$$

$$\langle \hat{n}_{\beta_k}^2 \rangle = \frac{\eta_t \xi (\eta_t \xi + 1)}{2}. \quad (13)$$

The cost of error correction is determined by the simulated joint probability distribution. When Alice prepares coherent state  $|\alpha_k\rangle$ , the probability of Bob obtaining key mapping result  $z$  is given by the following integral:

$$P(Z = z|X = k) = \int_{A_z} \frac{1}{\pi(1 + \frac{1}{2}\eta_d\eta_t\xi + \nu_{el})} \times \exp\left(\frac{-|y - \sqrt{\eta_d\eta_t}\alpha_k|^2}{1 + \frac{1}{2}\eta_d\eta_t\xi + \nu_{el}}\right) dy, \quad (14)$$

where  $X$  and  $Z$  represent Alice's and Bob's key strings, respectively,  $k \in \{0, 1, 2, \dots, 15\}$ ,  $z \in \{0, 1, 2, \dots, 15, \perp\}$ , and  $A_z$  is the postselection range as shown in Appendix A. Furthermore, error correction leakage can be bounded by

$$\delta_{\text{leak}}^{\text{EC}} \leq p_{\text{pass}} \left\{ n[(1 - \beta)H(Z) + \beta H(Z|X)] + \log_2\left(\frac{2}{\epsilon_{\text{EC}}}\right) \right\}. \quad (15)$$

Here,  $n$  is the number of rounds used for key generation,  $\beta$  is the reconciliation efficiency,  $\log_2(2/\epsilon_{\text{EC}})$  is the leaked information of correctness verification, and  $p_{\text{pass}}$  is the probability that a round passes the postselection.

Based on the above model, the numerical method in Refs. [40,41] can be used to simulate the composable secret key rate of 16QAM-modulated CV-QKD protocol.

#### D. Simulation results

In the following simulation, we set the parameters to be  $\epsilon_{\text{EC}} = 2 \times 10^{-11}$ ,  $\epsilon_{\text{PA}} = 2 \times 10^{-11}$ ,  $\epsilon_{\text{AT}} = 7 \times 10^{-11}$ ,  $\epsilon_{\text{ET}} = 1 \times 10^{-11}$ , and  $\bar{\epsilon} = 1 \times 10^{-11}$  for a trade-off between security and performance [36], and the subspace dimension  $N_c = 10$  for a relatively fast computing [39]. In order to match with practical experiments, unit of modulation variance here is SNU, where 1 SNU corresponds to variance of 0.5 NU defined in the QPSK-modulated protocols [13,36].

In Fig. 4, the composable secret key rate of QPSK-modulated, 16QAM-modulated and Gaussian-modulated CV-QKD with an ideal detector is shown against transmission distance. Different total numbers of signals  $N = 10^9, 10^{10}, 10^{11}, 10^{12}$ , and asymptotic situation are simulated. The testing ratios are fixed as  $r_{\text{test}} = 10\%$ . For the QPSK-modulated protocol, modulation variance  $V_A$  is set to be 0.49 SNU, which is close to its optimal value [36]. For the 16QAM-modulated and Gaussian-modulated protocol [18], modulation variance  $V_A = 2$  SNU, excess noise  $\xi = 0.01$ , and reconciliation efficiency  $\beta = 0.95$ . Postselection of discrete-modulated protocols is not considered ( $\Delta = 0$ ). Simulation results indicate that, in asymptotic cases, when transmission distance is small, the composable secret key rate achieved by the 16QAM-modulated protocol is virtually indistinguishable from that of the Gaussian-modulated protocol, given the same modulation variance. In terms of key rate, ignoring postselection, it surpasses the CV-QKD protocol utilizing QPSK modulation with optimal modulation variance by approximately one order of magnitude under the total

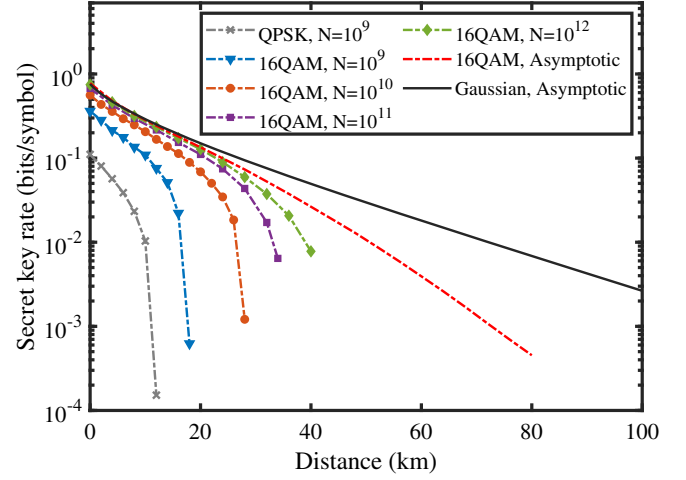


FIG. 4. Composable secret key rate versus distance for QPSK-modulated CV-QKD, 16QAM-modulated CV-QKD, and Gaussian-modulated CV-QKD with ideal detectors. Different total number of signals  $N$  are simulated, and the testing ratios are fixed as  $r_{\text{test}} = 10\%$ . For the QPSK-modulated protocol, modulation variance  $V_A = 0.49$  SNU. For the 16QAM-modulated and Gaussian-modulated protocol, modulation variance  $V_A = 2$  SNU, excess noise  $\xi = 0.01$ , and reconciliation efficiency  $\beta = 0.95$ . The postselection of discrete-modulated protocols is not considered ( $\Delta = 0$ ).

number of signals. When the total number of signals  $N = 10^9$ , the 16QAM-modulated CV-QKD protocol can achieve maximum transmission distance  $L = 18$  km. When the total number of signals reaches  $10^{12}$ , the

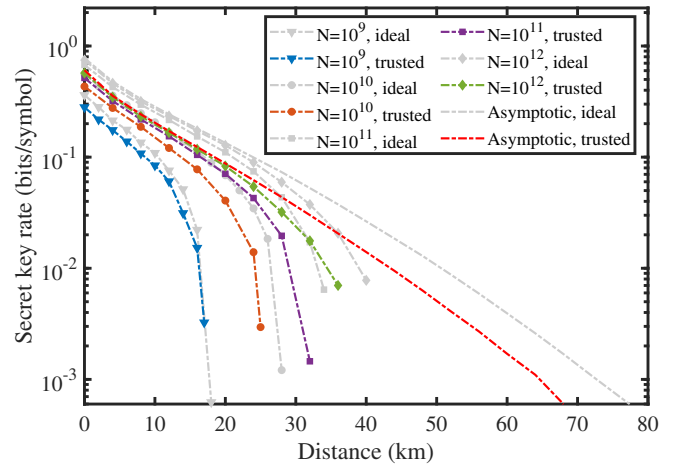


FIG. 5. Influence of detector model. Composable secret key rate versus distance for 16QAM-modulated CV-QKD with ideal detectors (gray dashed line) and trusted detectors (colored dashed line). Different total number of signals  $N$  are simulated, and the testing ratios are fixed as  $r_{\text{test}} = 10\%$ . Modulation variance  $V_A = 2$  SNU, excess noise  $\xi = 0.01$ , detection efficiency  $\eta_d = 0.7$ , detector noise  $\nu_{el} = 0.08$ , and reconciliation efficiency  $\beta = 0.95$ , and postselection is not considered ( $\Delta = 0$ ).

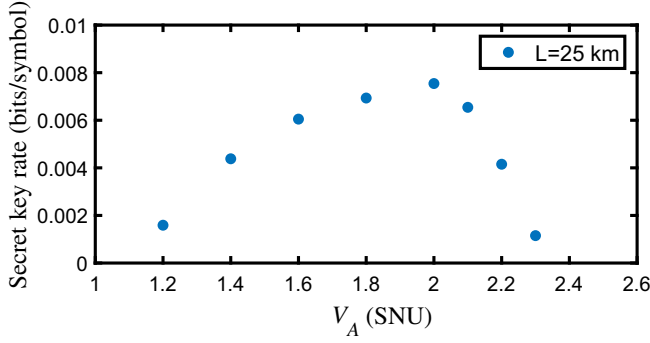


FIG. 6. Composable secret key rate versus modulation variance  $V_A$  for 16QAM-modulated CV-QKD with transmission distance  $L = 25$  km. The total number of signals  $N = 10^{10}$  and the testing ratio  $r_{\text{test}} = 10\%$ . Excess noise  $\xi = 0.01$ , detection efficiency  $\eta_d = 0.7$ , detector noise  $\nu_{\text{el}} = 0.08$ , and reconciliation efficiency  $\beta = 0.95$ , and postselection is not considered.

maximum transmission distance can be increased to over 40 km.

In Fig. 5, the composable secret key rate with ideal detectors and trusted detectors is shown versus the transmission distance. For the trusted, nonideal detectors, we set detection efficiency  $\eta_d = 0.7$  and detector noise  $\nu_{\text{el}} = 0.08$ ; other parameters are the same as in Fig. 4. Results show that, compared to the ideal detector situation, the composable secret key rates with the trusted detector have slightly decreased, and the maximum transmission distances have also been decreased. Even without considering postselection, a transmission distance of 25 km can still be achieved at  $N = 10^{10}$ . When the total number of signals reaches  $10^{12}$ , the maximum transmission distance is limited to 40 km. These results indicate that the 16QAM-modulated protocol can achieve high-rate practical key distribution under a short distance.

In Fig. 6, modulation variance  $V_A$  is optimized for 16QAM-modulated CV-QKD protocol with transmission

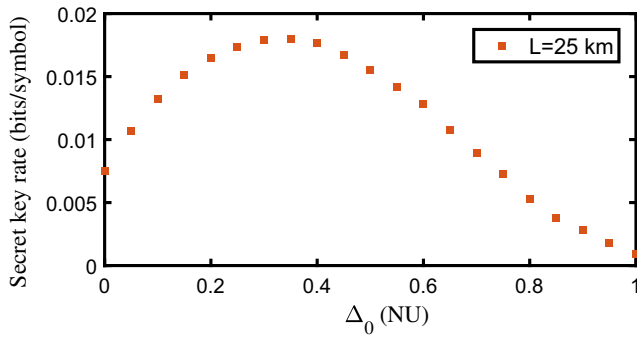


FIG. 7. Optimization of postselection parameter  $\Delta_0$  for composable 16QAM-modulated CV-QKD with transmission distance  $L = 25$  km, respectively. The total number of signals  $N = 10^{10}$  and the testing ratio  $r_{\text{test}} = 10\%$ . Modulation variance  $V_A = 2$  SNU, excess noise  $\xi = 0.01$ , detection efficiency  $\eta_d = 0.7$ , detector noise  $\nu_{\text{el}} = 0.08$ , and reconciliation efficiency  $\beta = 0.95$ .

distance  $L = 25$  km. Other parameters are the same as in Fig. 5. Results show that the optimal modulation variance is close to 2 SNU in the cases of  $L = 25$  km.

In Fig. 7, postselection parameter  $\Delta_0$  is optimized for the 16QAM-modulated CV-QKD protocol with transmission distance  $L = 25$  km, where  $\Delta_0 := \Delta / \sqrt{\eta_r \eta_d}$ . Modulation variance is set as  $V_A = 2$  SNU, and other parameters are the same as in Fig. 6. Results show that, when the transmission distance is 25 km, the optimal postselection parameter is around  $\Delta_0 = 0.35$  NU, and, compared to no postselection ( $\Delta_0 = 0$ ), the composable secret key rate can be increased by more than twice. This shows that a reasonable postselection scheme can significantly improve the performance of the 16QAM-modulated CV-QKD protocol.

### III. EXPERIMENTAL DEMONSTRATION

In this section, based on theoretical security analysis, experimental demonstration of the composable discrete-modulated CV-QKD protocol is provided.

#### A. Experimental setup

The experimental setup for local local oscillator (LLO) discrete-modulated CV-QKD system is illustrated in Fig. 8. On Alice's side, a continuous-wave laser emitting at 1550.22 nm with a linewidth below 100 Hz functions as the optical carrier. This laser beam is divided into two paths via a BS. One path traverses an in-phase/quadrature modulator driven by a two-channel arbitrary waveform generator (AWG) operating at 10 GSa/s, featuring 10-bit resolution. This arrangement generates the quadrature components ( $x$  and  $p$ ) of probability-shaped 16QAM signals, with a frequency shift of 1 GHz. These signals are modulated at a symbol rate of 1 Gbaud, employing a discrete Gaussian distribution and a root-raised cosine filter (roll-off factor of 0.3) for waveform shaped. An automatic bias control (ABC) module is employed to stabilize the operating point of the modulator.

For channel training, QPSK training symbols, 4 times more powerful than the quantum signals, are interleaved with the quantum signals in the time domain. A variable optical attenuator (VOA1) adjusts the modulation variance, while an optical switch (OS1) manages the quantum link for parameter calibration, thereby generating discrete-modulated coherent states. The reference path incorporates VOA2 and OS2, and both the discrete-modulated coherent states and reference signals are multiplexed in polarization and frequency. To minimize the impact of strong reference signal on the quantum signal, the reference signal's frequency is shifted to a region with weaker detector response while maintaining sufficiently high signal-to-noise ratio (SNR). Furthermore, frequency separation between the quantum and reference signals can be increased.

The multiplexed signal then passes through an acoustic-optic modulator (AOM) for real-time shot noise calibration.

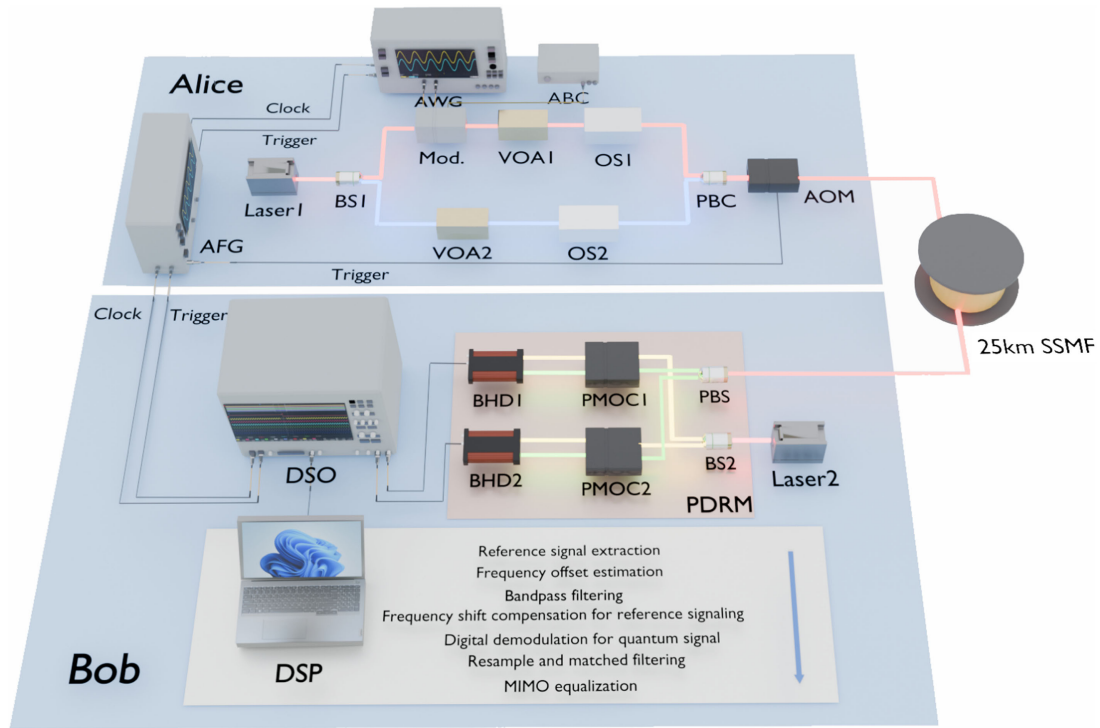


FIG. 8. Experimental setup of the LLO discrete-modulated CV-QKD system. Mod, IQ modulator; BS, beam splitter; AWG, arbitrary waveform generator; ABC, automatic bias control module; VOA, variable optical attenuator; OS, optical switch; AFG, arbitrary function generator; PBC, polarization beam combiner; AOM, acousto-optic modulator; SSMF, standard single-mode fiber; PBS, polarization beam splitter; PMOC, polarization-maintaining optical coupler; BHD, balanced homodyne detector; PDRM, polarization diversity receiver module; DSO, digital storage oscilloscope; DSP, digital signal processing.

Here, shot noise calibration is performed by leveraging the AOM's high extinction ratio, fast switching capability, and flexible control at the transmitter side. Since no external attacks are introduced during the experiment, the calibration results are accurate. In practical applications, a high-precision optical power meter can be employed to monitor the calibration window in real time, effectively preventing Eve from injecting light during this period. The transmission path comprises 25 km of standard single-mode fiber (SSMF). On Bob's side, a second independent continuous-wave laser with a linewidth of  $< 100$  Hz serves as the local oscillator (LO), detuned by approximately 2 GHz from Alice's laser. Here, we shift the reference signal to a higher-frequency region where the detector response is weaker. This effectively reduces the reference signal's amplitude while maintaining a sufficiently high SNR, as noise in this frequency range can be well suppressed. The signal and LO are coherently detected using a polarization diversity receiver module (PDRM). The PDRM is carefully selected to ensure that the two internal balanced detectors have closely matched characteristics, including electronic noise, clearance, and frequency response. In the future, photonic integration could provide more balanced and stable polarization-diversity receivers. It consists of a polarization beam splitter (PBS), a beam splitter (BS2), two polarization-maintaining optical couplers (PMOC), and two balanced

homodyne detectors (BHD), offering 3 dB bandwidth of 1.6 GHz, responsivity of 0.95 A/W, and gain of  $3.0 \times 10^4$  V/A. Notably, this experimental setup eliminates the need for active polarization state control of the incoming light signal at the receiver. Instead, full DSP is leveraged for polarization compensation, enhancing system robustness and ensure that the CV-QKD system operates with minimal excess noise, thereby enhancing its performance and security.

Ultimately, electrical signals are digitized by a digital storage oscilloscope (DSO) operating at 8 GSa/s with 10-bit resolution, followed by offline digital signal processing (DSP) to recover and analyze the raw data. Here, clock signals for both AWG and DSO are provided by a 10-MHz sine wave generated by an arbitrary function generator (AFG). Simultaneously, the AFG outputs a 50% duty cycle pulse signal to synchronize the AWG, AOM, and DSO, enabling coordinated generation, control, and acquisition of signals.

As shown in Fig. 8, the main DSP algorithms including (1) *Reference signal extraction*—Because of random polarization fluctuations, the reference signal intensities received along the two principal axes of the PDRM may vary. Since polarization state changes are typically slow, the stronger of the two signals is usually extracted as the reference signal through a comparison of their intensities.

- (2) *Frequency offset estimation*—The reference signal is generated by the beat note between two independently operating narrow-linewidth lasers, whose actual frequency varies randomly and slowly over time. Therefore, frequency offset estimation is performed in the frequency domain to accurately determine the instantaneous frequency of the extracted reference signal.
  - (3) *Bandpass filtering*—To suppress the out-band noise, a frequency-domain ideal filter with bandwidth of 1.3 GHz and 200 kHz is used for quantum and reference signals, respectively.
  - (4) *Frequency shift compensation for reference signal*—A digital frequency shift with 1 GHz is performed for the reference signal to remove the center frequency difference between the quantum and reference signal.
  - (5) *Digital demodulation for quantum signal*—The  $x$  and  $p$  components of quantum states are demodulated from the intermediate frequency signal digitally, and carrier frequency shift and phase noise introduced by Alice's and Bob's lasers are compensated by the filtered reference signal.
  - (6) *Resample and matched filtering*—The demodulated quantum signal is resampled to  $4\times$  oversampling, which preserves the sampling accuracy while reducing the computational complexity of the subsequent fractionally spaced equalizer. To filtering the high-frequency noise, the resampled signal is filtered by a root-raised cosine filter with a roll-off factor of 0.3.
  - (7) *multiple-input multiple-output equalization*—A  $4\times 2$  multiple-input multiple-output equalization is performed to quantum signal, which not only compensates for the random polarization fluctuations in the link, but also compensates for imbalances in the  $x$  and  $p$  components, downsamples the quantum signal from 4 times oversampling to 1 sample per symbol, and reduces residual noise.
- Denoting  $TS_{inx}^X$ ,  $TS_{inp}^X$ ,  $TS_{inx}^Y$ , and  $TS_{inp}^Y$  as the received training symbols, then, the training processing can be described by

$$\begin{aligned} TS_{outx}^X &= \omega_{11}TS_{inx}^X + \omega_{12}TS_{inp}^X + \omega_{13}TS_{inx}^Y + \omega_{14}TS_{inp}^Y, \\ TS_{outp}^X &= \omega_{21}TS_{inx}^X + \omega_{22}TS_{inp}^X + \omega_{23}TS_{inx}^Y + \omega_{24}TS_{inp}^Y. \end{aligned} \quad (16)$$

The update processing of the tap coefficients  $\omega_{1j}(j \in \{1, 2, 3, 4\})$  is

$$\begin{aligned} \omega_{1j}(m+1) &= \omega_{1j}(m) + \mu \epsilon_x^X(n) TS_{outx}^X, \\ \omega_{2j}(n+1) &= \omega_{2j}(n) + \mu \epsilon_p^X(n) TS_{outp}^X, \end{aligned} \quad (17)$$

where  $\mu$  is the step size and  $\epsilon_x^X(n)$  and  $\epsilon_p^X(n)$  are the error value, which can be calculated by

$$\begin{aligned} \epsilon_x^X &= TS_x^X - TS_{outx}^X, \\ \epsilon_p^X &= TS_p^X - TS_{outp}^X, \end{aligned} \quad (18)$$

where  $TS_x^X$  and  $TS_p^X$  are the transmitted training symbols. To accelerate convergence and improve accuracy, we further employ a time-domain superposition method to enhance the SNR of the training sequence [42], and raw data are subsequently acquired based on the enhanced sequence to evaluate system performance. It is worth noting that static DSP operations, when applied to quantum signals, affect shot noise and electronic noise in a consistent manner [43]; whereas in dynamic DSP processing, the algorithmic matrix is normalized to ensure that the model remains applicable to quantum signals [44]. Meanwhile, we design tap coefficients to ensure that the dynamic process does not alter the SNU for the  $X$ -polarization direction.

## B. Experimental results

We collect 20 sets of data blocks and use ten sets for test, each block contains 640 M symbols. In order to evaluate the performance of our system, we consider two situations: the secret key rate with Gaussian channel assumption and the secret key rate in a general situation. It is worth mentioning that Gaussian attack is not optimal in discrete-modulated CV-QKD protocols. However, in our laboratory system, there is no actual eavesdroppers, and we can still consider the channel as Gaussian to estimate channel transmittance and excess noise to evaluate system performance preliminarily attributing to theoretical results. In practical situations, the system may be attacked by eavesdroppers, which may be non-Gaussian and results in a worse key rate. Therefore, it is necessary to estimate the statistical estimators  $\langle \hat{n}_{\beta_k} \rangle$  and  $\langle \hat{n}_{\beta_k}^2 \rangle$  required for SDP using experimental data directly and obtain a more reliable secret key rate.

The statistical estimators  $\langle \hat{n}_{\beta_k} \rangle$  and  $\langle \hat{n}_{\beta_k}^2 \rangle$  are estimated in a general situation and compared to the value with Gaussian channel assumption as shown in Fig. 9. The statistics  $\langle \hat{n}_{\beta_k} \rangle$  and  $\langle \hat{n}_{\beta_k}^2 \rangle$  fluctuate around the estimated values with the Gaussian channel assumption due to measurement and statistical errors, and the fluctuation of  $\langle \hat{n}_{\beta_k}^2 \rangle$  is greater. Since there is no Eve in our laboratory, when the amount of data is infinite, the statistical values in a general situation should be infinitely close to the experimental estimations with the Gaussian channel assumption.

The experimental parameters and estimated results are summarized in Table I. With the security parameters  $\epsilon_{EC} = 2 \times 10^{-11}$ ,  $\epsilon_{PA} = 2 \times 10^{-11}$ ,  $\epsilon_{AT} = 7 \times 10^{-11}$ ,  $\epsilon_{ET} = 1 \times 10^{-11}$ , and  $\tilde{\epsilon} = 1 \times 10^{-11}$ , the security parameter of each block is  $\epsilon = 10^{-10}$ , and the total security parameter is  $\epsilon = 10^{-9}$ . In order to optimize the performance of our system, we optimize the postselection parameter  $\Delta_0$  using the parameters in the Gaussian channel and decide the optimal postselection parameter is around 0.35 NU.

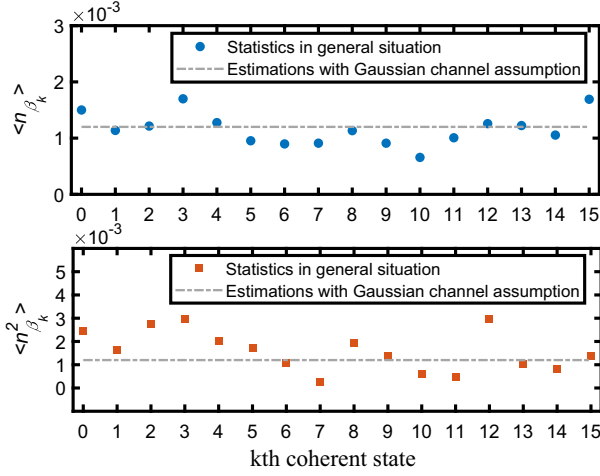


FIG. 9. Experimental estimation of the statistics  $\langle \hat{n}_{\beta_k} \rangle$  and  $\langle \hat{n}_{\beta_k}^2 \rangle$ . The dots are the statistics in a general situation, and the line is the estimations with the Gaussian channel assumption.

Based on the optimized postselection parameter, we calculate the secret key rates under the Gaussian channel assumption and general situation, respectively, as shown in Fig. 10. Because error correction is not performed in our experiment, we consider typical parameters: reconciliation efficiency  $\beta = 0.95$  and frame error rate  $\text{FER} = 0.15$ . With system repetition frequency  $R = 1$  GHz, and 25% of the keys are used for training sequences, the experimental key rate in a general situation is 18.93 Mbps as shown by the red star. The black curve is the simulation result using experimental parameters with the Gaussian channel assumption as a reference for system performance. Compared to previous Gaussian-modulated CV-QKD systems featuring composable security, the 16QAM-modulated system demonstrates

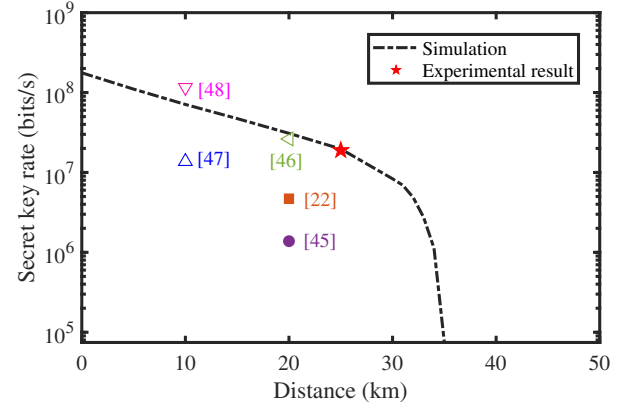


FIG. 10. Composable secret key rate versus transmission distance with experimental parameters in Table I. The red star is a general experimental secret key rate, and the black curve is the simulation using experimental parameters with the Gaussian channel assumption. The solid orange square represents the experimental result of previous Gaussian-modulated CV-QKD systems corresponding to Ref. [22]. The solid purple circle represents the QPSK-modulated CV-QKD system during the same period corresponding to Ref. [45]. The hollow triangles with square bracket numbers represent the experimental results of previous discrete-variable QKD systems corresponding to Refs. [46–48].

improvement of more than one order of magnitude in terms of secret key rate and achieves longer transmission distance [22]. Furthermore, when compared to the CV-QKD system employing QPSK modulation, our system exhibits a performance advantage of nearly 2 orders of magnitude [45]. Compared to previous high-rate discrete-variable QKD systems with composable security [46–48], our system can also achieve a comparable level of secret key rate. Results indicate that the CV-QKD system with 16QAM modulation can ensure high composable key rates over medium to short distances while maintaining low complexity and cost, further demonstrating the practical advantages in urban areas.

TABLE I. Experimental parameters and estimated results.

| Parameter                          | Symbol                                | Value                 |
|------------------------------------|---------------------------------------|-----------------------|
| The total data amount              | $N$                                   | $1.28 \times 10^{10}$ |
| The test data amount               | $m$                                   | $6.4 \times 10^9$     |
| Modulation variance                | $V_A$                                 | 2.03 (SNU)            |
| Probability distribution parameter | $\nu$                                 | 0.2                   |
| Worst-case channel transmittance   | $T_{wc}$                              | 0.3465                |
| Worst-case excess noise            | $\xi_{wc}$                            | 0.0083                |
| Electronic noise                   | $\nu_{el}$                            | 0.0883                |
| Detection efficiency               | $\eta_d$                              | 0.714                 |
| Displaced photon number            | $\langle \hat{n}_{\beta_k} \rangle$   | 0.0012                |
| Displaced squared photon number    | $\langle \hat{n}_{\beta_k}^2 \rangle$ | 0.0012                |
| Transmission distance              | $L$                                   | 25 (km)               |
| Fiber loss                         | $\alpha$                              | 0.184 (dB/km)         |
| Post-selection parameter           | $\Delta_0$                            | 0.35 (NU)             |
| Reconciliation efficiency          | $\beta$                               | 0.95                  |
| Frame error rate                   | FER                                   | 0.15                  |
| Training sequences ratio           | $a$                                   | 0.25                  |
| System repetition frequency        | $R$                                   | 1 (GHz)               |
| Total security parameter           | $\epsilon$                            | $10^{-9}$             |

#### IV. DISCUSSION AND CONCLUSION

Over recent years, the theoretical security of discrete-modulated CV-QKD has been progressively refined. The advanced nonlinear SDP security framework provides strong support for the security and performance of the discrete modulation CV-QKD protocol, but there are also many challenges.

First, the nonlinear semidefinite programming (SDP) method leads to a more compact constraint on the secret key rate. Based on this approach, the security of the QPSK modulated CV-QKD protocol against coherent attacks has been proven using entropy accumulation theory [37,49] and further improved via the generalized entropy accumulation theory [50,51]. This allows discrete-modulated CV-QKD protocols to achieve the highest level of security. However,

under coherent attacks, the independent and identically distributed assumption for quantum states no longer holds, which complicates security analysis, significantly degrades protocol performance, and raises considerable challenges for experimental implementation. Recently, the marginal constrained entropy accumulation theory [52] has been proposed, providing an effective tool for the security analysis of practical discrete-modulated protocols against coherent attacks. Moreover, by employing conic optimization, the composable secret key rate can be computed efficiently [53]. The experimental verification of discrete-modulated CV-QKD under coherent attacks will be addressed in future work.

Second, while this security framework is scalable and can, in principle, be extended to arbitrary modulation constellations, a key limitation of such protocols is that, as the constellation size increases, the matrix dimension required for solving the SDP grows correspondingly, resulting in significantly longer computation times. With currently available computing resources, it remains difficult to extend the approach to higher-order modulation formats such as 64QAM and beyond. Therefore, it is urgently necessary to improve the algorithms for solving the optimization problems in order to reduce computational complexity. Although several enhanced algorithms have been proposed [54–56], their effectiveness still falls short of meeting the demands of very high-order modulation. Moreover, increasing the number of modulation points imposes stricter requirements on experimental devices, complicates excess noise control, and makes it harder to improve the system repetition rate. For these reasons, we adopt 16QAM as a balanced modulation format to achieve the best possible system performance under practical constraints.

Furthermore, the requirement for Bob to discretize his data in the nonlinear SDP-based protocol entails both practical advantages and theoretical challenges. On the one hand, the signal is already naturally digitized by a low-resolution analog-to-digital converter, which simplifies experimental implementation and reduces operational complexity. On the other hand, this discretization fundamentally transforms the nature of the information reconciliation problem: The equivalent communication channel shifts from a binary-input additive white Gaussian noise channel to a binary symmetric channel. This fundamental shift primarily complicates the design of high-efficiency error correction codes for long-range, extremely low-SNR scenarios, where sustaining performance is particularly difficult [57]. Moreover, this makes the method of using all data for parameter estimation and key extraction in the Gaussian-modulated protocol [22] no longer applicable. As a result, significant key consumption arises with finite-size effect. These are the theoretical challenges that need to be solved for the practical application of discrete-modulated CV-QKD protocols, which are left for future work.

In conclusion, in order to address the issue of low secret key rate in CV-QKD systems with composable security, we

propose the probability-shaped 16QAM-modulated CV-QKD protocol. Theoretical performance is analyzed and experimental demonstration is provided. Performance of the 16QAM-modulated protocol significantly surpasses that of QPSK modulation and is comparable to the Gaussian-modulated protocol at close range. Specifically, our system achieves a composable secret key rate of 18.93 Mbps over a 25-km fiber channel. The secret key rate exceeds that of previous Gaussian-modulated CV-QKD systems by more than an order of magnitude, exceeds the QPSK CV-QKD system of the same period by nearly 2 orders of magnitude, and is comparable to high-rate discrete-variable QKD systems, all while maintaining low system complexity and cost. Our work offers a valuable solution for the future deployment of QKD.

## ACKNOWLEDGMENTS

The authors thank Florian Kanitschar for valuable discussions about theoretical security analysis and numerical calculation in the early preparation stage. We acknowledge financial support from the National Cryptologic Science Fund of China (Grants No. 2025NCSF02050, No. 2025NCSF02052, and No. 2025NCSF02053), the National Natural Science Foundation of China (Grants No. U24B20135, No. U22A2089, No. U25B2014, No. 62471446, and No. 62301517), the Sichuan Science and Technology Program (Grants No. 2026NSFSC0391, No. 2024JDDQ0008, No. 2025ZYD0152, No. 2022ZDZX0009, No. 2026NSFSC0392, and No. 2025ZNSFSC1473), the National Key Laboratory of Security Communication Foundation (Grants No. 6142103042504 and No. 6142103042406), and Stability Program of National Key Laboratory of Security Communication (Grants No. WD202503, No. WD202502, No. WD202501, and No. WD202508).

## DATA AVAILABILITY

The data that support the findings of this article are not publicly available because they are owned by a third party and the terms of use prevent public distribution. The data are available from the authors upon reasonable request.

## APPENDIX A: REGION OPERATORS OF 16QAM-MODULATED CV-QKD

In the security analysis framework [40,41], the conditional entropy  $H(X|E')_{\bar{\rho}}$  is usually represented as  $D(\mathcal{G}(\bar{\rho})||\mathcal{Z}[\mathcal{G}(\bar{\rho})])$ , where  $\mathcal{G}$  is a completely positive and trace-preserving map that outlines several classical post-processing procedures associated with the protocol,  $\mathcal{Z}$  is a pinching quantum channel, and  $D(\rho||\sigma)$  is the quantum relative entropy. In the case of reverse reconciliation,  $\mathcal{G}(\sigma) = K\sigma K^\dagger$ , where  $K = \sum_{z=0}^{15} |z\rangle_R \otimes I_A \otimes (\sqrt{R^z})_B$  and  $R^z$  are region operators. The region operators are defined as

$R_B^z = (1/\pi) \int_{A^z} |\zeta\rangle\langle\zeta| d^2\zeta$ , where  $A^z$  are the regions in phase space. For the trusted noise scenario, the noisy region operators are [38]

$$[R_B^z]' = \int_{\zeta \in A^z} G_\zeta d^2\zeta, \quad (\text{A1})$$

and the key map positive operator-valued measure (POVM) elements

$$[P^z]' = I_A \otimes [R_B^z]'. \quad (\text{A2})$$

Because the base of our protocol is  $\{|i\rangle_A \otimes |n_{\beta_i}\rangle_B\}$ , the matrix elements of the POVM are [39]

$$\begin{aligned} [P^z]'_{klmn} &= \langle m_{\beta_l} | [R_B^z]' | n_{\beta_k} \rangle \\ &= \int_{A^z} \langle m_{\beta_l} | G_\zeta | n_{\beta_k} \rangle d^2\zeta \\ &= \frac{1}{\eta_d \pi} \int_{A^z} \langle m | D\left(\frac{\zeta}{\sqrt{\eta_d}} - \beta_k\right) \rho_{th}(\bar{n}) D^\dagger \\ &\quad \times \left(\frac{\zeta}{\sqrt{\eta_d}} - \beta_k\right) | n \rangle d^2\zeta \\ &= \int_{A^z} \langle m | G_{\zeta - \sqrt{\eta_d}\beta_k} | n \rangle d^2\zeta. \end{aligned} \quad (\text{A3})$$

The integral function of POVM element  $G_{\zeta - \sqrt{\eta_d}\beta_k}$  in photon-number basis is

$$\langle m | G_{\zeta - \sqrt{\eta_d}\beta_k} | n \rangle = \frac{1}{\eta_d \pi} \exp\left[-\frac{|\zeta - \sqrt{\eta_d}\beta_k|^2}{\eta_d(1 + \bar{n}_d)}\right] \frac{\bar{n}_d^m}{(1 + \bar{n}_d)^{n+1}} \left(\frac{(\zeta - \sqrt{\eta_d}\beta_k)^*}{\sqrt{\eta_d}}\right)^{n-m} \left(\frac{m!}{n!}\right)^{1/2} L_m^{(n-m)}\left[-\frac{|\zeta - \sqrt{\eta_d}\beta_k|^2}{\eta_d \bar{n}_d(1 + \bar{n}_d)}\right], \quad (\text{A4})$$

where  $\bar{n}_d = (1 - \eta_d + \nu_{el})/\eta_d$  and  $L_a^{(b)}(c)$  is the generalized Laguerre polynomial of degree  $a$  with a parameter  $b$  in the variable  $c$ .

For our 16QAM-modulated protocol, we use the Cartesian coordinate system, and  $\zeta = x + iy$ . The integration limits  $A_z$  are

$$\int_{\Delta_{y,low}}^{\Delta_{y,up}} \int_{\Delta_{x,low}}^{\Delta_{x,up}} \langle m | G_{x+iy - \sqrt{\eta_d}\beta_k} | n \rangle dx dy, \quad (\text{A5})$$

where

$$\begin{aligned} \Delta_{x,low} &= \{2\alpha_0, \Delta, -2\alpha_0, -M, 2\alpha_0, \Delta, -2\alpha_0, -M, 2\alpha_0, \Delta, -2\alpha_0, -M\}, \\ \Delta_{x,up} &= \{M, 2\alpha_0, -\Delta, -2\alpha_0, M, 2\alpha_0, -\Delta, -2\alpha_0, M, 2\alpha_0, -\Delta, -2\alpha_0\}, \\ \Delta_{y,low} &= \{2\alpha_0, 2\alpha_0, 2\alpha_0, 2\alpha_0, \Delta, \Delta, \Delta, \Delta, -2\alpha_0, -2\alpha_0, -2\alpha_0, -2\alpha_0, -M, -M, -M, -M\}, \\ \Delta_{y,up} &= \{M, M, M, M, 2\alpha_0, 2\alpha_0, 2\alpha_0, 2\alpha_0, -\Delta, -\Delta, -\Delta, -\Delta, -2\alpha_0, -2\alpha_0, -2\alpha_0, -2\alpha_0\}, \end{aligned} \quad (\text{A6})$$

and  $M$  is the detection limit. The measurement results falling within a range of less than  $\Delta$  from the coordinate axis or exceeding the detection limit are disregarded and instead marked with the symbol  $\perp$ ; this step is called postselection. In order to strike a balance between numerical computation complexity and performance improvement, we have considered the postselection scheme that involves discarding measurement results close to the axis.

## APPENDIX B: STATISTICAL ESTIMATION

First, we use traditional parameter estimation methods to estimate channel transmittance  $T$  and excess noise  $\xi$  of the system. We model the quantum channel as an additive

Gaussian white noise channel, for heterodyne detection scheme, that satisfies

$$y = \sqrt{0.5\eta_d T} x + \delta, \quad (\text{B1})$$

where  $x$  and  $y$  represent the input and output of the channel, respectively,  $\delta$  is the Gaussian noise with variance  $T\eta_d\xi/2 + 1 + \nu_{el}$ ,  $T$  is the channel transmittance, and  $\eta_d$  is the detection efficiency. In this case, the channel transmittance  $T$  and excess noise  $\xi$  can be estimated as

$$T = \frac{(\sum_{i=1}^m x_i y_i / m)^2}{0.5\eta_d}, \quad (\text{B2})$$

$$\xi = \frac{V_B - 0.5\eta_d TV_A - \nu_{el} - 1}{0.5\eta_d T}, \quad (B3)$$

where  $V_A$  represents the modulation variance of Alice,  $V_B$  represents the variance of Bob's data,  $\nu_{el}$  is the variance of detector electrical noise, and  $m$  is the amount of data used for tests. Because of the fluctuation of statistical values under the finite-size effect, we consider the worst-case estimate [18]

$$T_{wc} \simeq T - w \frac{2T}{\sqrt{2k_T}} \sqrt{\frac{\xi + \frac{2+\nu_{el}}{\eta_d T}}{V_A}}, \quad (B4)$$

$$\xi_{wc} \simeq \frac{T}{T_{wc}} \xi + w \sqrt{\frac{1}{k_T} \frac{\eta_d T \xi + 2 + \nu_{el}}{\eta_d T_{wc}}}, \quad (B5)$$

where the parameter  $w$  can be given by the inverse error function and is related to the security parameter  $\epsilon_{pe}$  as

$$w = \sqrt{2} \operatorname{erf}^{-1}(1 - \epsilon_{pe}). \quad (B6)$$

Because of the fact that Gaussian attacks are not optimal for discrete-modulated CV-QKD protocols, general statistical estimations are also necessary. In order to calculate the statistics  $\langle \hat{n}_{\beta_k} \rangle$  and  $\langle \hat{n}_{\beta_k}^2 \rangle$ , we first distinguish the number of rounds for sending each state  $|\alpha_k\rangle$ , denoted as  $C_k$ . The average measurement value of each state corresponding to Bob is

$$\bar{Y}^k = \frac{1}{C_k} \sum_{j=1}^{C_k} (q_j^k + i p_j^k). \quad (B7)$$

We can calculate the displaced values

$$\tilde{q}_j^k = q_j^k - \operatorname{Re}(\bar{Y}^k), \quad (B8)$$

$$\tilde{p}_j^k = p_j^k - \operatorname{Im}(\bar{Y}^k). \quad (B9)$$

Because the expected value of displaced observation calculated on original undisplaced data is the same as the expected value of undisplaced observation calculated on the displaced data, according to further deductions, we can calculate the statistics with detector noise [58]:

$$\langle [\hat{n}_{\sqrt{\eta_d} \beta_k}]' \rangle = \frac{1}{C_k} \sum_{j=1}^{C_k} \left[ \frac{1}{2} (\tilde{q}_j^k)^2 + \frac{1}{2} (\tilde{p}_j^k)^2 - 1 \right], \quad (B10)$$

$$\begin{aligned} \langle [\hat{n}_{\sqrt{\eta_d} \beta_k}^2]' \rangle &= \frac{1}{C_k} \sum_{j=1}^{C_k} \left[ \frac{1}{4} (\tilde{q}_j^k)^4 + \frac{1}{2} (\tilde{q}_j^k)^2 (\tilde{p}_j^k)^2 \right. \\ &\quad \left. + \frac{1}{4} (\tilde{p}_j^k)^4 - \frac{3}{2} (\tilde{q}_j^k)^2 - \frac{3}{2} (\tilde{p}_j^k)^2 + 1 \right]. \end{aligned} \quad (B11)$$

According to this, we can reconstruct the effective ideal expectations as [39]

$$\langle \hat{n}_{\beta_k} \rangle = \frac{\langle [\hat{n}_{\sqrt{\eta_d} \beta_k}]' \rangle - \nu_{el}}{\eta_d}, \quad (B12)$$

$$\begin{aligned} \langle \hat{n}_{\beta_k}^2 \rangle &= \frac{1}{\eta_d^2} (\langle [\hat{n}_{\sqrt{\eta_d} \beta_k}^2]' \rangle - 2\nu_{el}^2 - \nu_{el} \\ &\quad - (4\nu_{el} + 1 - \eta_d) (\langle [\hat{n}_{\sqrt{\eta_d} \beta_k}]' \rangle - \nu_{el})). \end{aligned} \quad (B13)$$

These statistics can be incorporated into SDP to calculate the secret key rate.

- 
- [1] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in *Proceedings of the IEEE International Conference on Computers* (IEEE, New York, 1984).
  - [2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, *Advances in quantum cryptography*, *Adv. Opt. Photonics* **12**, 1012 (2020).
  - [3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Secure quantum key distribution with realistic devices*, *Rev. Mod. Phys.* **92**, 025002 (2020).
  - [4] C. Portmann and R. Renner, *Security in quantum cryptography*, *Rev. Mod. Phys.* **94**, 025008 (2022).
  - [5] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, *Continuous-variable quantum key distribution system: Past, present, and future*, *Appl. Phys. Rev.* **11**, 011318 (2024).
  - [6] V. C. Usenko, A. Acín, R. Alléaume, U. L. Andersen, E. Diamanti, T. Gehring, A. A. Hajomer, F. Kanitschar, C. Pacher, S. Pirandola *et al.*, *Continuous-variable quantum communication*, *arXiv:2501.12801*.
  - [7] T. C. Ralph, *Continuous variable quantum cryptography*, *Phys. Rev. A* **61**, 010303(R) (1999).
  - [8] F. Grosshans and P. Grangier, *Continuous variable quantum cryptography using coherent states*, *Phys. Rev. Lett.* **88**, 057902 (2002).
  - [9] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Quantum cryptography without switching*, *Phys. Rev. Lett.* **93**, 170504 (2004).
  - [10] A. Leverrier and P. Grangier, *Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation*, *Phys. Rev. Lett.* **102**, 180504 (2009).
  - [11] Z. Li, Y.-C. Zhang, and H. Guo, *User-defined quantum key distribution*, *arXiv:1805.04249*.
  - [12] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, *Asymptotic security of continuous-variable quantum key distribution with a discrete modulation*, *Phys. Rev. X* **9**, 021059 (2019).
  - [13] J. Lin, T. Upadhyaya, and N. Lütkenhaus, *Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution*, *Phys. Rev. X* **9**, 041064 (2019).
  - [14] A. Denys, P. Brown, and A. Leverrier, *Explicit asymptotic secret key rate of continuous-variable quantum key*

- distribution with an arbitrary modulation, *Quantum* **5**, 540 (2021).
- [15] A. Leverrier, *Composable security proof for continuous-variable quantum key distribution with coherent states*, *Phys. Rev. Lett.* **114**, 070501 (2015).
  - [16] A. Leverrier, *Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction*, *Phys. Rev. Lett.* **118**, 200501 (2017).
  - [17] S. Pirandola, *Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks*, *Phys. Rev. Res.* **3**, 043014 (2021).
  - [18] S. Pirandola and P. Papanastasiou, *Improved composable key rates for CV-QKD*, *Phys. Rev. Res.* **6**, 023321 (2024).
  - [19] 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 (2013).
  - [20] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu *et al.*, *An integrated silicon photonic chip platform for continuous-variable quantum key distribution*, *Nat. Photonics* **13**, 839 (2019).
  - [21] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, *Long-distance continuous-variable quantum key distribution over 202.81 km of fiber*, *Phys. Rev. Lett.* **125**, 010502 (2020).
  - [22] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer *et al.*, *Practical continuous-variable quantum key distribution with composable security*, *Nat. Commun.* **13**, 4740 (2022).
  - [23] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, *Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber*, *Optica* **9**, 492 (2022).
  - [24] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, *Sub-mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber*, *Opt. Lett.* **48**, 1766 (2023).
  - [25] A. A. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, *Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator*, *Sci. Adv.* **10**, eadi9474 (2024).
  - [26] Y. Bian, Y. Pan, X. Xu, L. Zhao, Y. Li, W. Huang, L. Zhang, S. Yu, Y. Zhang, and B. Xu, *Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip*, *Appl. Phys. Lett.* **124**, 174001 (2024).
  - [27] 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).
  - [28] A. A. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, and T. Gehring, *Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver*, *Optica* **11**, 1197 (2024).
  - [29] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang *et al.*, *Sub-gbps key rate four-state continuous-variable quantum key distribution within metropolitan area*, *Commun. Phys.* **5**, 162 (2022).
  - [30] Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, B. Liu, W. Huang, and B. Xu, *Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system*, *Opt. Lett.* **47**, 3307 (2022).
  - [31] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, *Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres*, *Opt. Lett.* **47**, 3948 (2022).
  - [32] Y. Tian, Y. Zhang, S. Liu, P. Wang, Z. Lu, X. Wang, and Y. Li, *High-performance long-distance discrete-modulation continuous-variable quantum key distribution*, *Opt. Lett.* **48**, 2953 (2023).
  - [33] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, *Shaped constellation continuous variable quantum key distribution: Concepts, methods and experimental validation*, *J. Lightwave Technol.* **42**, 5182 (2024).
  - [34] Y. Pan, M. Wu, H. Wang, J. Li, Y. Shao, Y. Li, W. Huang, S. Yu, Y. Zhang, and B. Xu, *Long-distance discrete-modulated continuous-variable quantum key distribution over 126.56 km of fiber*, in *Proceedings of the 2025 Optical Fiber Communications Conference and Exhibition (OFC)* (IEEE, New York, 2025) pp. 1–3.
  - [35] Y. Bian, L. Fan, X. Xu, L. Zhao, M. Wu, S. Yu, and Y. Zhang, *40-km mbps discrete-modulated continuous variable quantum key distribution with constellation shaping pre-optimization*, in *Proceedings of the 2025 Optical Fiber Communications Conference and Exhibition (OFC)* (IEEE, New York, 2025) pp. 1–3.
  - [36] F. Kanitschar, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus, *Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols*, *PRX Quantum* **4**, 040306 (2023).
  - [37] S. Bäuml, C. Pascual-García, V. Wright, O. Fawzi, and A. Acín, *Security of discrete-modulated continuous-variable quantum key distribution*, *Quantum* **8**, 1418 (2024).
  - [38] J. Lin and N. Lütkenhaus, *Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution*, *Phys. Rev. Appl.* **14**, 064030 (2020).
  - [39] T. Upadhyaya, T. van Himbeek, J. Lin, and N. Lütkenhaus, *Dimension reduction in quantum key distribution for continuous-and discrete-variable protocols*, *PRX Quantum* **2**, 020325 (2021).
  - [40] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, *Numerical approach for unstructured quantum key distribution*, *Nat. Commun.* **7**, 11712 (2016).
  - [41] A. Winick, N. Lütkenhaus, and P. J. Coles, *Reliable numerical key rates for quantum key distribution*, *Quantum* **2**, 77 (2018).
  - [42] Y. Pan, Y. Bian, L. Ma, H. Wang, J. Dou, Y. Shao, Y. Pi, T. Ye, J. Yang, Y. Li *et al.*, *High-rate quantum access network using coherent states*, in *Proceedings of the 2024 Optical Fiber Communications Conference and Exhibition (OFC)* (IEEE, New York, 2024) pp. 1–3.
  - [43] Z. Chen, X. Wang, S. Yu, Z. Li, and H. Guo, *Continuous-mode quantum key distribution with digital signal processing*, *npj Quantum Inf.* **9**, 28 (2023).

- [44] L. Fan, Z. Li, S. Liu, X. Xu, T. Zhang, J. Mi, D. Wang, D. Zhang, H. Li, S. Yu, and Y. Zhang, *Practical continuous-variable quantum key distribution using dynamic digital signal processing: Security proof and experimental demonstration*, [arXiv:2602.05206](#) (2026).
- [45] A. A. Hajomer, F. Kanitschar, N. Jain, M. Hentschel, R. Zhang, N. Lütkenhaus, U. L. Andersen, C. Pacher, and T. Gehring, *Experimental composable key distribution using discrete-modulated continuous variable quantum cryptography*, [Light Sci. Appl.](#) **14**, 255 (2025).
- [46] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, *Provably secure and high-rate quantum key distribution with time-bin qudits*, [Sci. Adv.](#) **3**, e1701491 (2017).
- [47] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami *et al.*, *10-mb/s quantum key distribution*, [J. Lightwave Technol.](#) **36**, 3427 (2018).
- [48] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan *et al.*, *High-rate quantum key distribution exceeding 110 mb s<sup>-1</sup>*, [Nat. Photonics](#) **17**, 416 (2023).
- [49] F. Dupuis, O. Fawzi, and R. Renner, *Entropy accumulation*, [Commun. Math. Phys.](#) **379**, 867 (2020).
- [50] C. Pascual-García, S. Bäuml, M. Araújo, R. Liss, and A. Acín, *Improved finite-size key rates for discrete-modulated continuous-variable quantum key distribution under coherent attacks*, [Phys. Rev. A](#) **111**, 022610 (2025).
- [51] T. Metger, O. Fawzi, D. Sutter, and R. Renner, *Generalised entropy accumulation*, [Commun. Math. Phys.](#) **405**, 261 (2024).
- [52] A. Arqand and E. Y.-Z. Tan, *Marginal-constrained entropy accumulation theorem*, [arXiv:2502.02563](#).
- [53] M. Navarro, A. G. Lorente, P. V. Parellada, C. Pascual-García, and M. Araújo, *Finite-size quantum key distribution rates from rényi entropies using conic optimization*, [arXiv:2511.10584](#).
- [54] H. Hu, J. Im, J. Lin, N. Lütkenhaus, and H. Wolkowicz, *Robust interior point method for quantum key distribution rate computation*, [Quantum](#) **6**, 792 (2022).
- [55] M. Karimi and L. Tuncel, *Efficient implementation of interior-point methods for quantum relative entropy*, [INFORMS J. Comput.](#) **37**, 3 (2025).
- [56] G. Koßmann and R. Schwonnek, *Optimising the relative entropy under semi definite constraints—a new tool for estimating key rates in qkd*, [npj Quantum Inf.](#) **12**, 23 (2026).
- [57] A. Leverrier, *Information reconciliation for discretely-modulated continuous-variable quantum key distribution*, [arXiv:2310.17548](#).
- [58] T. Upadhyaya, *Tools for the security analysis of quantum key distribution in infinite dimensions*, Master's thesis, University of Waterloo, 2021.