




# Multiple-quadrature-amplitude-modulation continuous-variable quantum key distribution realization with a downstream-access network

Junyu Zhang , Xiangyu Wang ,\* Fan Xia , and Song Yu

*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Ziyang Chen 

*State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China*



(Received 15 November 2023; accepted 26 April 2024; published 17 May 2024)

Quantum networks based on quantum key distribution ensure the security which is guaranteed by the fundamental laws of quantum physics between multiple parties. The discrete-modulation (DM) continuous-variable quantum key distribution (CV-QKD) protocols have the characteristics of simple implementation and compatibility with classical digital communication, making them very suitable for deployment in large-scale communication networks. However, the actual communication network has a huge communication capacity and a large number of units. To solve this problem, we propose a multiple-quadrature-amplitude-modulation (MQAM) DM protocol with a numerical method and complete the security analysis of the DM protocol in a downstream-access network situation. By introducing an extra dimension of signal modulation, the high-order modulated MQAM protocol greatly improves the number of supported units and the key rate of each unit. We give the results of a 16 quadrature amplitude modulation CV-QKD protocol in a downstream-access network which achieves 64 supported network units even in the case of high excess noise, which shows the application prospects of high-order discrete-modulation CV-QKD in network security.

DOI: [10.1103/PhysRevA.109.052429](https://doi.org/10.1103/PhysRevA.109.052429)

## I. INTRODUCTION

Quantum key distribution establishes secret key sharing between separated parties in the presence of any eavesdropper (Eve), with the strict security guaranteed by theoretical physics [1–3]. It targets the vulnerability of classical cryptography when attacked by a quantum computer. Beginning with the Bennett-Brassard 1984 protocol [4], there have been many achievements achieved in discrete-variable quantum key distribution (DV-QKD) through the discrete variables of physical properties of a single photon [5–7].

Different from DV-QKD, continuous-variable quantum key distribution (CV-QKD) relies on the quadratures of the quantized electromagnetic field mapped into the phase space of coherent states or squeezed states for carrying different signals. Due to the simplicity and availability of CV-QKD, there are plenty of remarkable achievements made on the basis of Gaussian modulation [8], for instance, the integration of well-established modern digital signal processing techniques [9]. Theoretically, the security analysis constantly promotes the upper bound of the key rate and elevates the security against the loophole and eavesdropper [10–17]. Through Gaussian-modulation CV-QKD, a lot of achievements have been made in terms of quantum access networks. In the access network applied to QKD [18–20], the achievements based on upstream-access networks keep emerging [21–23]. The

security analysis of downstream-access networks has improved recently [24]. By Gaussian modulation, the theoretical upper bound of the high key rate limited by channel capacity can be reached. Because of the complex postprocess and error correction procedure as well as strict precision requirements for experimental equipment, the development is constrained for the large-scale deployment of quantum secure communication networks.

In the process of implementing quantum network, its is difficult to select the continuous amplitude for coherent states due to the limited modulation and accuracy of detection. Discrete modulation (DM) sets a finite alphabet as the sending state candidate, with several selected coherent states usually contained instead of the coherent states with continuous random amplitude in Gaussian modulation. Thus, discrete modulation receives attention with discrete-alphabet encoding schemes for coherent states [25–28]. The security analysis of discrete modulation is also constantly improving [29–32]. Recently, the development of a numerical method for discrete modulation has improved [33,34]. The security analysis framework has been processed [35,36]. There are more realistic issues considered in security analysis, such as untrusted detector noise and finite-dimensional convex optimizations [37,38]. Protocols with complex constellations are published, and achieve a higher secret key rate [39–43]. Meanwhile, some significant techniques have also been applied to discrete modulation, such as machine learning and postselection [44,45]. In terms of experiment, there are many attempts made to realize discrete modulation in practice [46–50]. In quantum

\*xywang@bupt.edu.cn

networks, DM CV-QKD is compatible with modern optical communication devices and some well-developed technologies of classical access networks. The application of DM CV-QKD plays a significant role in promoting the large-scale deployment of secure quantum communication networks.

In this paper, we propose the security analysis of a multiple-quadrature-amplitude-modulation (MQAM) constellation protocol with a numerical method and realize DM CV-QKD in a downstream-access network. Different from the previous multiple phase shift keying protocol, the quadrature amplitude is used to denote the signals instead of only phase, which allows the protocol to carry more information through extra dimensions. It leads to a substantial advancement of the DM protocol modulation mode and a significant increase in the number of supported optical network units. On this basis, the security analysis is conducted in the downstream-access network. Considering the practical quantum network environment, an applicable trusted detector model is presented to ensure that the key map for the region operator is consistent with the key map for calculating error rate. Through the numerical simulation performed in the downstream-access network under the 16QAM protocol, the large number of optical network units supported in the downstream-access network is demonstrated. It illustrates the potential of high-order discrete-modulation CV-QKD in the application of large-scale quantum networks.

This paper is organized as follows. In Sec. II, we briefly introduce the security analysis of discrete-modulation CV-QKD and downstream-access networks with Gaussian modulation CV-QKD. In Sec. III, the security analysis of the MQAM discrete-modulation protocol is conducted, and the numerical method of 16QAM for simulation is proposed. In Sec. IV, the simulation results of the 16QAM protocol in the downstream-access network are presented and discussed. In Sec. V, the conclusion is drawn and prospects are outlined.

## II. BASIS OF DISCRETE-MODULATION CV-QKD AND ACCESS NETWORKS

### A. Discrete-modulation CV-QKD

In this section, quadrature phase shift keying (QPSK) is exemplified to introduce the basic protocol and method of security analysis of discrete-modulation CV-QKD. As shown in Fig. 1, the sender Alice randomly selects a coherent state from the alphabet  $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$  with a uniform probability as the signal state. Then the prepared state is sent to Bob through the quantum channel. After the state is received, Bob performs a heterodyne measurement of the received state, with the measurement result  $y \in \mathbb{R}$  obtained. After  $n$  rounds, Alice and Bob select a small proportion of the data for parameter estimation. After passing the parameter estimation sifting, Bob maps the remaining measurement results according to the following rules as the raw sequence for secret key generation:

$$z = \begin{cases} 0 & \text{if } \theta \in [-\frac{1}{4}\pi, \frac{1}{4}\pi) \\ 1 & \text{if } \theta \in [\frac{1}{4}\pi, \frac{3}{4}\pi) \\ 2 & \text{if } \theta \in [\frac{3}{4}\pi, \frac{5}{4}\pi) \\ 3 & \text{if } \theta \in [\frac{5}{4}\pi, \frac{7}{4}\pi) \end{cases}. \quad (1)$$

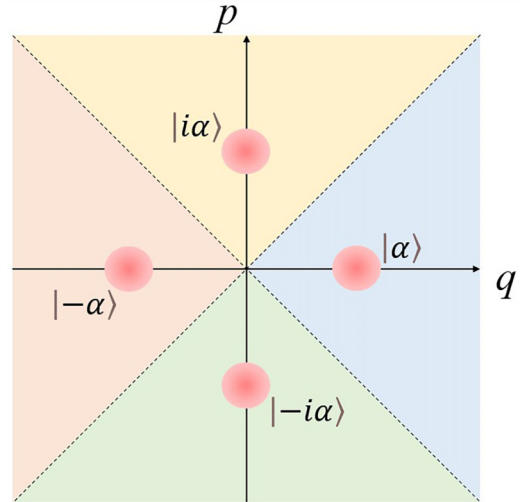


FIG. 1. Schematic diagram of the constellation for QPSK protocol. Alice randomly selects a sending state from alphabet  $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$  for each round. Then Bob maps the measurement outcomes basis on the corresponding region delineated by dotted lines.

Finally, Alice and Bob extract the secret key rate from the raw sequence by a suitable error correction and a suitable postprocessing method.

In the equivalent  $EB$  model, the bipartite state prepared by Alice can be expressed as

$$|\psi\rangle_{AA'} = \sum_x \sqrt{p_x} |x\rangle_A |\alpha_x\rangle_{A'}, \quad (2)$$

where  $x$  represents the orthogonal basis of register  $A$ . Then Alice sends the state  $|\alpha_x\rangle_{A'}$  to the channel and keeps the register  $A$ . Alice will take a positive operator-valued measure (POVM) measurement to register  $A$  with the basis  $M^A = \{M_x^A = |x\rangle\langle x|\}$  and obtain her raw discrete sequence  $X$ . The probability of each measurement result is equal to the probability  $p_x$  of each prepared Einstein-Podolsky-Rosen state. The state  $|\alpha_x\rangle_{A'}$  which was sent to Bob through the channel map  $\varepsilon_{A' \rightarrow B}$ , becomes the state of system  $B$ . Then we get the quantum state between Alice and Bob:

$$\rho_{AB} = (id_A \otimes \varepsilon_{A' \rightarrow B})(|\psi\rangle\langle\psi|_{AA'}), \quad (3)$$

where  $id_A$  is the identity channel on register  $A$ . Bob makes a POVM  $G_y$  for system  $B$  to obtain state  $\rho_B$ , after receiving the state which passed through the channel map. Next, we will simply introduce the calculation method of the key rate for DM CV-QKD. First, in the scenario of reverse reconciliation and collective attack, the Devetak-Winter formula can be expressed as follows:

$$R^\infty = \min_{\rho_{AB} \in \mathcal{S}} D\{\mathcal{G}(\rho_{AB}) \parallel \mathcal{Z}[\mathcal{G}(\rho_{AB})]\} - p_{\text{pass}} \delta_{\text{EC}} \quad (4)$$

where  $D(\rho \parallel \sigma)$  is the quantum relative entropy defined as  $\text{Tr}(\rho \log_2 \rho) - \text{Tr}(\rho \log_2 \sigma)$ ,  $\delta_{\text{EC}}$  is the entropy which is used for error correction,  $p_{\text{pass}}$  is the sift probability for secure key generation,  $\mathcal{G}$  is a completely positive and trace nonincreasing map for postprocessing,  $\mathcal{Z}$  is a pinching quantum channel that

reads out the result of the key map, and  $S$  denotes all feasible probability density operators in experimental observations.

For the first part of Eq. (4), the minimum of relative entropy  $D\{\mathcal{G}(\rho_{AB}) \parallel \mathcal{Z}[\mathcal{G}(\rho_{AB})]\}$  is needed with all the feasible region  $S$ . We use semidefinite programming (SDP) tools to solve this convex optimization problem. This convex optimization problem is described as follows:

$$\begin{aligned}
 & \text{minimize } D\{\mathcal{G}(\rho_{AB}) \parallel \mathcal{Z}[\mathcal{G}(\rho_{AB})]\} \\
 & \text{subject to} \\
 & \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{F}_Q)] = p_x \langle \hat{F}_Q \rangle_x, \\
 & \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{F}_P)] = p_x \langle \hat{F}_P \rangle_x, \\
 & \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{S}_Q)] = p_x \langle \hat{S}_Q \rangle_x, \\
 & \text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{S}_P)] = p_x \langle \hat{S}_P \rangle_x, \\
 & \text{Tr}_B[\rho_{AB}] = \sum_{i,j=0}^n \sqrt{p_i p_j} \langle \alpha_j | \alpha_i \rangle |i\rangle\langle j|_A, \\
 & \text{Tr}[\rho_{AB}] = 1, \\
 & \rho_{AB} \geq 0,
 \end{aligned} \tag{5}$$

where  $x$  denotes which state Alice sent from the alphabet,  $\hat{F}_Q$  and  $\hat{F}_P$  are the first-moment operators of  $q$  and  $p$  orthogonal components respectively, and  $\hat{S}_Q$  and  $\hat{S}_P$  are the second-moment operators of  $q$  and  $p$  orthogonal components respectively. The result of partial trace  $\text{Tr}_B[\rho_{AB}]$  is the state  $\rho_A$  of system  $A$ , due to the assumption that Eve is unable to access system  $A$ .  $x \in [0, n]$ , where  $n$  is the number of constellation points minus 1 and  $n = 3$  in the QPSK situation. This equation describes the minimization of relative entropy while satisfying all the constraints mentioned below.

The definition of postprocessing map  $\mathcal{G}$  is  $\mathcal{G}(\sigma) = K\sigma K^\dagger$ . The Kraus operator  $K$  is given by

$$K = \sum_{z=0}^n |z\rangle_R \otimes \mathbb{I}_A \otimes (\sqrt{R_z})_B \tag{6}$$

where the register  $R$  keeps the result of the key map, and  $R_z$  is the region operator which is related to the region partition of Bob's key map. The pinching quantum channel is given by

$$\mathcal{Z}(\sigma) = \sum_{j=0}^n (|j\rangle\langle j|_R \otimes \mathbb{I}_A) \sigma (|j\rangle\langle j|_R \otimes \mathbb{I}_A). \tag{7}$$

For the last part of Eq. (4),  $p_{\text{pass}}$  is the probability of signal passing postselection.  $\delta_{\text{EC}}$  represents the entropy that will be leaked during the error correction step and is definite in the reverse-reconciliation scenario:

$$\begin{aligned}
 \delta_{\text{EC}} &= H(Z) - \beta I(X; Z) \\
 &= (1 - \beta)H(Z) + \beta H(Z|X)
 \end{aligned} \tag{8}$$

where  $\beta$  is reconciliation efficiency, and  $Z$  and  $X$  are the raw sequences of Bob and Alice, respectively.  $H(Z|X)$  is the conditional entropy of sequence  $Z$  and  $X$ , relative with the conditional probability density between them.

A tight lower bound on the security key rate can be achieved by using a two-step procedure. First, the Frankwolf [34] algorithm is utilized to iteratively repeat SDP [51,52] in order to approach the minimum of relative entropy. In an ideal scenario, we would obtain the optimal state  $\rho_{AB}$  which ensures maximum security while satisfying all constraints. However, because of numerical imprecision, we are only able to attain

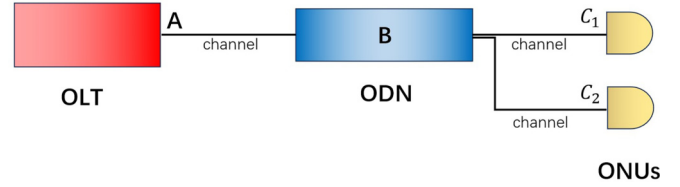


FIG. 2. Simple model of the downstream-access network with two ONUs. Alice, located in the OLT, sends a coherent state to the quantum channel. Mode  $A$  transmits through ODN and is passively divided into each channel for ONUs. The received modes by the ONUs are  $C_1$  and  $C_2$ .

a suboptimization state  $\rho_{AB}^*$ . In the second step, by solving the dual problem of SDP and the linearization of the key rate function at the state  $\rho_{AB}^*$ , we obtain a tight lower bound on the key rate that accounts for linear undercuts within the feasible set. The tight lower bound provided slightly underestimates the key rate of the optimal state  $\rho_{AB}$ , which is crucial for ensuring security.

## B. Basis of the downstream-access network

The access network is constructed through the optical line terminal (OLT), the optical network units (ONUs), and the optical distribution network (ODN), for classical communication. First, the classical downstream-access network will be introduced. As shown in Fig. 2, this system is composed of the OLT, ONUs and ODN. The OLT sends the signal or data packet to ONUs. The signal or data packet first arrives at the ODN, and passes through the beam splitters (BSs) fixed in the ODN. Then, this signal or data packet is passively divided and sent to each downstream ONU. The BS is passive to division and makes no active selection for the destination of the divided signal, which is equivalent to the OLT making a networkwide broadcast. All ONUs receive an identical signal or data packet. In classical communication, encryption ensures the security of the protocol. The OLT encrypts the signal before it is sent, only with a private key held by both the OLT and corresponding ONU that can decrypt these signals. After the signal is broadcast, only the specific ONU which keeps the private key can decrypt the signal. Other ONUs are unaware of the information in signal.

The CV-QKD downstream-access network is of the same structure as the classical downstream-access network. Its model of sending and receipt is constructed by adopting the prepare-and-measure model. Therefore, in practice, the CV-QKD downstream-access network can directly utilize the equipment of the classical network. The receiving and sending devices need to be replaced by standard CV-QKD devices, with coherent lasers and heterodyne detection devices chosen in our scheme. First, a coherent state is prepared by the OLT device and input into the network through the fiber. When the quantum signal arrives at the ODN, it is passively divided into  $n$  paths by the BS. Then, the  $n$  path quantum signal is transmitted to each ONU. After a quantum signal is received, the ONU performs measurement using its CV-QKD receivers. Being the same as classical communication, in the CV-QKD downstream-access network, the OLT only communicates with one ONU at a time. That is to say, only the

specific ONU is capable to extract the secret key. Therefore, our focus is the amount of secret key rate that can be extracted.

Next, the security analysis of the CV-QKD downstream-access network is briefly introduced as the example of a four ONU downstream-access network. As shown in Fig. 2, the communication ONU is assumed to be  $C_1$ . In reverse reconciliation, the secret key rate is written as [53,54]

$$K = \beta I_{AC_1} - \chi_{EC_1}, \quad (9)$$

where  $I_{AC_1}$  is the mutual information between system  $A$  and  $C_1$ , and  $\chi_{EC_1}$  is the total information that Eve can eavesdrop, which is given by

$$\chi_{EC_1} = S(E) - S(E|C_1), \quad (10)$$

where  $S(\cdot)$  is von Neumann entropy. In standard security analysis, when Eve reaches the upper bound of information that can be eavesdropped, the von Neumann entropy satisfies

$$\begin{aligned} S(E) &= S(AB_1C_1C_2C_3C_4), \\ S(E|C_1) &= S(AB_1C_1C_2C_3C_4|C_1). \end{aligned} \quad (11)$$

To ensure security, considering the worst case, we need to subtract the information that is related to the other ONUs:

$$K' = K - \chi_{C_1C_2} - \chi_{C_1C_3} - \chi_{C_1C_4}, \quad (12)$$

where  $\chi_{C_1C_2}$ ,  $\chi_{C_1C_3}$ , and  $\chi_{C_1C_4}$  comprise the information that system  $C_1$  relates with the other ONUs. For calculating the secret key rate, all the other ONUs must be considered when the formula of safety analysis is derived. It is necessary to write down the covariance matrix  $\gamma_{AB_1C_1C_2C_3C_4}$  or calculate the state  $\rho_{AB_1C_1C_2C_3C_4}$ . The complexity of calculation increases with a rise in the number of ONUs. This hinders its practical application. To solve this problem, it is assumed that Eve is powerful enough to control all the other ONUs. Under such an assumption, all the other ONUs are considered as part of the channel and are controlled completely by Eve except for the communicating ONU. An upper bound that can be held by Eve's information is estimated [55–58]:

$$\begin{aligned} S(E) &= S(EB_1C_1C_2C_3C_4) = S(AC_1), \\ S(E|C_1) &= S(EB_1C_1C_2C_3C_4|C_1) = S(A|C_1), \end{aligned} \quad (13)$$

since Eve can control system  $B_1C_2C_3$  and  $C_4$ . It is sufficient to consider only the state  $\rho_{AC_1}$  or covariance matrix  $\gamma_{AC_1}$  in security analysis. Next, it is necessary to consider the channel parameters in the above situation. As shown in Fig. 2, the ODN divides the channel into two parts. The transmittance and excess noise between OLT and ODN are expressed as  $T_{OLT-ODN}$  and  $\varepsilon_{OLT-ODN}$ ; the transmittance and excess noise between ODN and  $C_1$  are expressed as  $T_{ODN-C_1}$  and  $\varepsilon_{ODN-C_1}$ ; the transmittance and excess noise of ODN are expressed as  $\eta_{ODN}$  and  $\varepsilon_{ODN}$ . It is convenient to perform calibration in practice. The total transmittance  $T_{tot}$  and total excess noise  $\varepsilon_{tot}$  are defined as

$$\begin{aligned} T_{tot} &= T_{OLT-ODN} * T_{ODN-C_1} * \eta_{ODN}, \\ \varepsilon_{tot} &= \varepsilon_{OLT-ODN} + \varepsilon_{ODN-C_1} + \varepsilon_{ODN} \end{aligned} \quad (14)$$

where  $\eta_{ODN}$  is related to the number of ONUs. It can be seen from Eq. (14) that the influence of the ODN is considered as part of the influence of the channel. This means, in our security analysis, the BS in the ODN is untrusted. In this way, it is

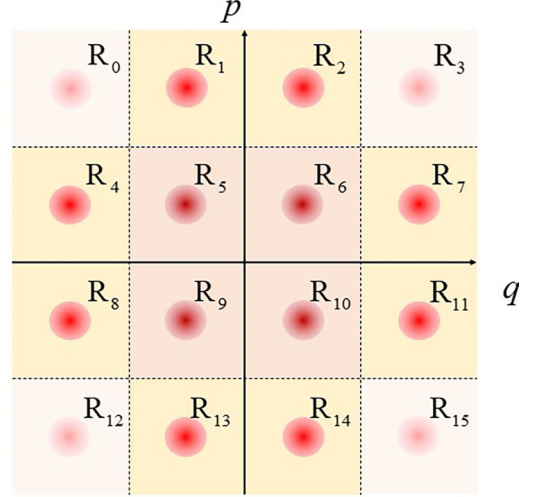


FIG. 3. Schematic diagram of the constellation for 16QAM protocol. We number the state and mapping region from left to right and from top to bottom.  $R_2$  represents the mapping region. The color depth of the coherent state represents the probability of being selected.

adequate to consider only the total transmittance and the total excess noise for parameter estimation. Also, it is sufficient to consider only the modes  $A$  and  $C_1$ , instead of having to write a complicated quantum state or covariance matrix that contains all the modes. Therefore, security analysis can be conducted independently between any two points in the access network.

### III. DISCRETE-MODULATION CV-QKD WITH MQAM CONSTELLATION

On the basis of QPSK security analysis, the constellation is expanded to MQAM. As Fig. 3 shows, Alice makes a random selection from the alphabet  $\alpha_i = [-a_n \cdots -a_1, -a_0, a_0, a_1 \cdots a_n]$  as the amplitude of the prepared state on the  $q$  orthogonal component, where  $n = \frac{\sqrt{M}}{2} - 1$ , and  $M$  represents the number of constellation points of MQAM, which is equivalent to the  $p$  orthogonal component. In practice, it is necessary to optimize the parameter  $a_x$  within a certain range. However, due to the substantial resource consumption for optimizing every parameter, it is impossible to achieve search optimization. For this reason, the scheme that fixes the distance between adjacent constellation points is chosen, which means  $a_x = (2x + 1)a_0$  ( $x \in [0, n]$ ). It is adequate to optimize only the parameter  $a_0$  in this scheme. Now, the alphabet Alice chooses from becomes  $\alpha_i = [\mp(2x + 1)a_0]$  ( $x \in [0, n]$ ), and the state prepared is

$$|\alpha_{ij}\rangle = |\alpha_i + i\alpha_j\rangle \quad (i, j \in [0, n]). \quad (15)$$

The sending states in the constellation are numbered in order from left to right and from top to bottom, i.e.,  $x = j(n + 1) + i$ . Thus, the sending states are written as  $\rho_x = |\alpha_x\rangle$ . Alice selects the state from the set  $\{|\alpha_x\rangle\}$  randomly with probability  $P_x$ , which is defined as

$$P_{q_x p_x} = \frac{\exp[v(q_x^2 + p_x^2)]}{\sum_{q_x p_x} \exp[v(q_x^2 + p_x^2)]}, \quad (16)$$

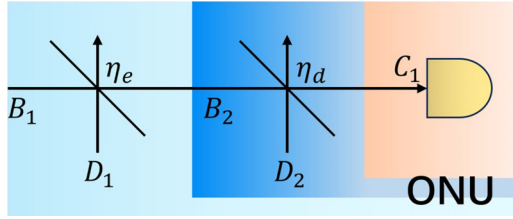


FIG. 4. The model for a noisy detector located in ONUs. The first BS imitates the electronic noise; the second BS imitates the detection efficiency. Then the mode  $C_1$  arrives at the ideal detector.

where  $v$  is the parameter related to probability distribution and will be optimized in the following calculation. This probability distribution confirms to a Gaussian distribution, and the probability  $P_x$  depends on its amplitude of  $q$  and  $p$  orthogonal components. As shown in Fig. 3, we take the 16QAM constellation as an example, with the probabilities indicated by color. Additionally,  $v$  affects the degree of the probability concentrated at the internal constellation points. After state preparation, Alice inputs the state  $|\alpha_x\rangle$  into the quantum channel. Bob takes a heterodyne measurement after receiving the measurement result  $y$ . Bob carries out parameter estimation and draws the key map. In the region of the key map, the number of parameters is also reduced through the scheme of the fixed distance between adjacent constellation points corresponding to the scheme of alphabet  $\{\alpha_x\}$  in the context of MQAM. The boundary of the key map region is set as  $a_{z_i} = \{-\infty, -na_c \cdots -2a_c - a_c, 0, a_c, 2a_c \cdots na_c, \infty\}$ . Therefore, the key map of MQAM is written as

$$z = i + j(n + 1) \quad (17)$$

if  $\{\text{Re}(y) \in (a_{z_i}, a_{z_{i+1}}) \text{ and}$   
 $\text{Im}(y) \in (a_{z_j}, a_{z_{j+1}})\}$

as shown in Fig. 3 in the 16QAM situation. The key map region is numbered from left to right and from top to bottom as  $z$ , with  $z \in [0, 15]$  for 16QAM.

One of the challenges in MQAM compared with QPSK is to optimize parameters, which is due to the increase in the number of constellation points. Thus, it is impossible to optimize them completely. To solve this problem, some suboptimal choices must be made to minimize the number of parameters. Even though these choices may not lead to the highest secret key rate in a particular scenario, the choices of parameters can still perform better in each scenario.

Figure 4 shows the model of the trusted detector set in this paper [24]. The signal needs to pass through the BS with transmittance  $\eta_e$  first, which represents the effect of electronic noise. Then, the signal passes through the BS with transmittance  $\eta_d$ , which represents the effect of detector efficiency. In this trusted detector model, only the loss caused by detector efficiency is considered as trust, and the influence of electronic noise is considered as a part of the channel. Thus, we set  $T_{\text{tot}} = T_{\text{OLT-ONU}} * \eta_e$  in heterodyne detection. This is an underestimate to ensure security for the secret key rate. Notably, after transformation of the BS, the probability distribution of state  $C_1$  varies compared to  $B_1$ . So, it is inappropriate to delimit the boundary of the key map for state  $C_1$  directly through

a demarcated boundary of the key map for state  $B_1$ . To ensure that the key map for the region operator is consistent with the key map for error rate calculation, the key map basis of the probability distribution of state  $C_1$  is used for subsequent numerical calculation. In this scheme, the POVM element  $G_y$  is equivalent to the operator for the ideal detector:

$$\langle m | G_y | n \rangle = \frac{1}{\pi \sqrt{m!n!}} e^{-(q^2+p^2)} (q-ip)^n (q+ip)^m. \quad (18)$$

The region operator is

$$\langle m | R_z | n \rangle = \int_{a_{z_i}}^{a_{z_{i+1}}} \int_{a_{z_j}}^{a_{z_{j+1}}} dq dp \langle m | G_y | n \rangle \quad (19)$$

where  $i, j \in [1, 2(n+1)]$ . This is the same as the first-moment and second-moment observables in Eq. (5):

$$\begin{aligned} \hat{F}_Q &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \sqrt{2} q G_y dq dp, \\ \hat{F}_P &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \sqrt{2} p G_y dq dp, \\ \hat{S}_Q &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} 2q^2 G_y dq dp, \\ \hat{S}_P &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} 2p^2 G_y dq dp. \end{aligned} \quad (20)$$

The simulation statistics with the effect of detector efficiency  $\eta_d$  are given by

$$\begin{aligned} \langle \hat{F}_Q \rangle &= \sqrt{2\eta_d T_{\text{tot}}} \text{Re}(\alpha_x), \\ \langle \hat{F}_P \rangle &= \sqrt{2\eta_d T_{\text{tot}}} \text{Im}(\alpha_x), \\ \langle \hat{S}_Q \rangle &= 2\eta_d T_{\text{tot}} \text{Re}(\alpha_x)^2 + 1 + \frac{1}{2}\eta_d T_{\text{tot}} \varepsilon_{\text{tot}}, \\ \langle \hat{S}_P \rangle &= 2\eta_d T_{\text{tot}} \text{Im}(\alpha_x)^2 + 1 + \frac{1}{2}\eta_d T_{\text{tot}} \varepsilon_{\text{tot}}, \end{aligned} \quad (21)$$

where  $\xi$  is excess noise, and the values of  $\text{Re}(\alpha_x)$  and  $\text{Im}(\alpha_x)$  are selected from  $[\mp(2i+1)a_0]$  ( $i \in [0, n]$ ). The conditional probability distribution of Bob's measurement  $y$  is given by

$$\tilde{P}(y|x) = \frac{1}{\pi(1 + \frac{1}{2}\eta_d T_{\text{tot}} \varepsilon_{\text{tot}})} \exp\left[-\frac{|y - \sqrt{\eta_d T_{\text{tot}}} \alpha_x|^2}{1 + \frac{1}{2}\eta_d T_{\text{tot}} \varepsilon_{\text{tot}}}\right]. \quad (22)$$

Based on this equation, the conditional probability  $P(y|x)$  can be calculated depending on the key map of state  $C_1$ ,

$$P(y|x) = \int_{a_{z_i}}^{a_{z_{i+1}}} \int_{a_{z_j}}^{a_{z_{j+1}}} dq dp \tilde{P}(q+ip|x), \quad (23)$$

to obtain the  $H(Z|X)$  in Eq. (8).

Despite simplified schemes developed for parameters in the MQAM protocol, there remains a stronger need to achieve optimization than for the QPSK protocol. Also, with a rise in the number of constellation points, there is also an increase in the dimension of each matrix in numerical simulation, which hinders the optimization of all parameters due to high computational complexity. In this case, a coarse-precision search is conducted to choose a set of parameters that are more suitable in each scenario for numerical simulation, although it may not be the optimal strategy in a particular scenario.

It is also worth discussing the calculation of region operator  $R_z$ . Regarding the MQAM protocol, it is necessary to calculate more region operators than for QPSK. Also, a high cutoff photon number  $N$  is set. Since the parameter  $a_c$  affects the division of the key map region, it needs to be recomputed frequently. It is necessary to reduce the computational complexity of region operator  $R_z$ . We use MATHEMATICA to obtain the analytical polynomial of the integral formula Eq. (19). In this way, it is enough to take the integral upper and lower bounds into the polynomial and obtain the result directly,

$$\begin{aligned} &\{q \in (0, x_1]p \in [y_2, \infty)\}, \quad \{q \in [x_1, x_2]p \in [y_2, \infty)\}, \quad \{q \in [x_2, \infty)p \in [y_2, \infty)\}, \\ &\{q \in (0, x_1]p \in [y_1, y_2]\}, \quad \{q \in [x_1, x_2]p \in [y_1, y_2]\}, \quad \{q \in [x_2, \infty)p \in [y_1, y_2]\}, \\ &\{q \in (0, x_1]p \in (0, y_1]\}, \quad \{q \in [x_1, x_2]p \in (0, y_1]\}, \quad \{q \in [x_2, \infty)p \in (0, y_1]\}. \end{aligned} \quad (24)$$

Then, the analytical polynomial of the region operator is obtained in the first quadrant. Lastly, it is only necessary to follow the symmetry relation between quadrants for obtaining all the region operators.

The gap between region operators computed through the analytical polynomial and the integral method is approximately of magnitude  $10^{-16}$  for numerical simulation of the 16QAM protocol. With the cutoff photon number  $N = 15$ , the time to calculate all the 16 operators  $R_z$  by the analytical polynomial is reduced to under 3 s. This makes it possible to do optimization for parameter  $a_c$ .

#### IV. PERFORMANCE ANALYSIS OF DM CV-QKD IN THE DOWNSTREAM-ACCESS NETWORK

In this section, the performance of the 16QAM protocol is demonstrated in downstream-access network, through the numeral method described in Sec. III. The channel is set as a Gaussian channel with transmittance  $T$  and excess noise  $\varepsilon$ . Based on the discussion about the downstream-access network in Sec. II B, the transmittance becomes  $T_{\text{tot}}$  and the excess noise becomes  $\varepsilon_{\text{tot}}$ . The definition of total transmittance is  $T_{\text{tot}} = 10^{-\frac{aL}{10}} \eta_{\text{ODN}} \eta_e$  in the distance  $L$  with  $a = 0.2$  dB/km, where  $\eta_{\text{ODN}}$  is related to the number of ONUs. For the MQAM protocol, it is a challenge to determine proper parameters. In the 16QAM protocol for deployment of constellation points, the parameters are set as follows. The amplitude of Alice's alphabet is  $\alpha_0 = 0.45$ , the amplitude of the region boundary for the key map is  $a_c = 1.5\alpha_0$ , and the probability distribution parameter is  $v = 0.5$ . The optimization of these parameters is shown in Fig. 7. Note that the selection of these parameters may not be the optimal value in a particular situation, but it produces an excellent performance in each scenario. The reconciliation efficiency is set as  $\beta = 0.95$  [59,60]. The parameters regarding the detector include detection efficiency  $\eta_d = 0.48$  and electronic noise  $\eta_e = 0.9$ . Based on the practical implications of the downstream-access network, the distance is limited to 30 km and the number of ONUs ranges from 2 to 64. Given a compromise on computation time, the cutoff number is set to  $N_{\text{cut}} = 15$  to perform the Frank-Wolfe iterations until sufficient convergence.

instead of spending a lot of time on calculating the integral for every key map region. Notably, the numerical value of MQAM is mutually symmetrical between the region operators in each quadrant. So, it is sufficient to calculate the region operator of only one quadrant. Since the integral upper and lower bounds contain zero and infinity, the limit in calculating the analytical polynomial should be avoided to improve the speed. Thus, the analytical polynomial is classified into nine types, depending on the upper and lower bounds of the integral:

Figure 5 shows the key rate with different numbers of ONUs and distances. When the number of ONUs falls below 4, a high key rate is maintained within 30 km. With more ONUs in connection with the network, the secret key rate declines. When the number of ONUs exceeds 20, the secret key rate drops sharply. When it reaches above 64, the transmission distance is limited to under 10 km. Figure 6 shows the range of tolerable excess noise with different numbers of ONUs and distances. The tolerable excess noise is scanned with the accuracy of 0.0002 for simulation. Apparently the tolerable excess noise is maintained at a satisfactory level when the ONU number is smaller than 4. The tolerable excess noise decreases progressively as the distance increases to 30 km. With the number of ONUs as the abscissa variable, the tolerable excess noise decreases sharply when the number of ONUs is under 10 and gradually when the number of ONUs exceeds 20. Even though the number of ONUs is 64, the tolerable excess noise remains above 0.03, which indicates the high performance of our protocol in the presence of excess noise. Compared with the performance of the QPSK protocol in the downstream-access network shown in Fig. 8, the 16QAM

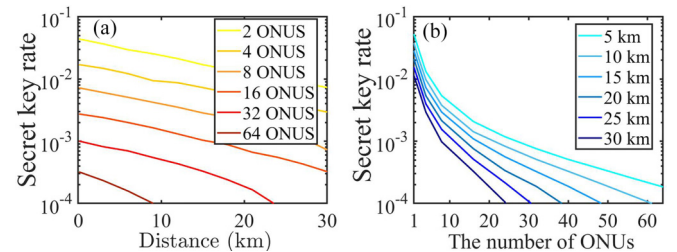


FIG. 5. Achievable secret key rate of DM CV-QKD against the number of ONUs accessed in the downstream-access network and transmission distance. (a) The function of secret key rate and transmission distance with a different number of ONUs. (b) The function of secret key rate and the number of ONUs with different distance. Simulation parameters: the excess noise  $\varepsilon_{\text{tot}} = 0.04$ , reconciliation efficiency  $\beta = 0.95$ , detection efficiency  $\eta_d = 0.48$ , electronic noise  $\eta_e = 0.9$ , the sending amplitude  $\alpha_0 = 0.45$ , the amplitude of region boundary  $a_c = 1.5\alpha_0$ , the probability distribution parameter  $v = 0.5$ .

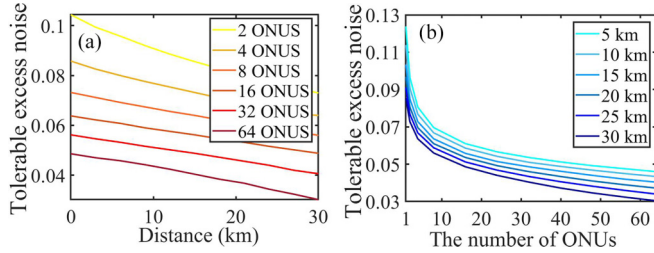


FIG. 6. Tolerable excess noise of DM CV-QKD against the number of ONUs accessed in the downstream-access network and transmission distance. (a) The function of tolerable excess noise and transmission distance with a different number of ONUs. (b) The function of tolerable excess noise and the number of ONUs with different distance. Simulation parameters: reconciliation efficiency  $\beta = 0.95$ , detection efficiency  $\eta_d = 0.48$ , electronic noise  $\eta_e = 0.9$ , the sending amplitude  $\alpha_0 = 0.45$ , the amplitude of region boundary  $a_c = 1.5a_0$ , the probability distribution parameter  $v = 0.5$ .

protocol achieves the sufficiently supported number of ONUs and tolerable excess noise required for implementing DM-CV QKD in the downstream-access network.

Figure 7 shows the optimization of parameters:  $v$ ,  $\alpha_0$ , and  $\alpha_c$  with  $T_{\text{tot}} = \frac{1}{2}$ ,  $\frac{1}{10}$ , and  $\frac{1}{100}$ . Due to the complexity of computation, it is difficult to achieve optimization under each scenario. Therefore, these three typical scenarios are simulated, and the parameters that perform well with each  $T_{\text{tot}}$  are chosen, even though it may not be optimal. The situation with  $T_{\text{tot}} = \frac{1}{2}$  represents the general point-to-point case within 30 km; the situation with  $T_{\text{tot}} = \frac{1}{10}$  represents the case of a small number of ONUs within 30 km; and the situation with

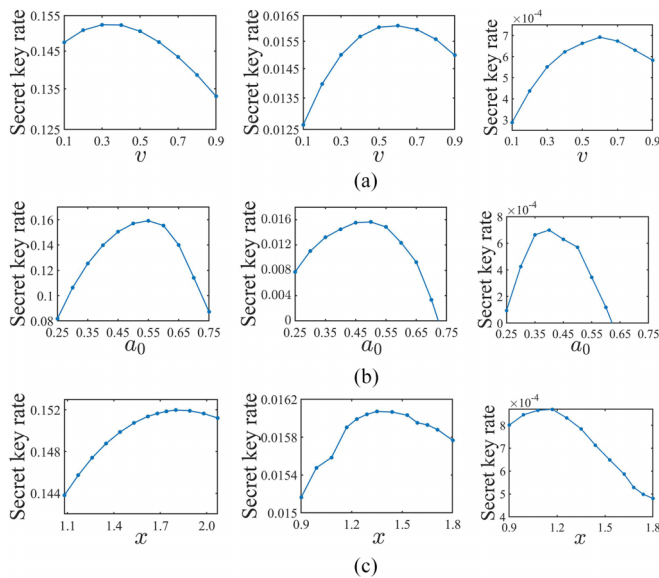


FIG. 7. The curve between secret key rate and the parameters: (a) the probability distribution parameter  $v$ , (b) the amplitude of Alice's alphabet  $\alpha_0$ , (c) the amplitude of the region boundary for the key map  $\alpha_c = x\alpha_0$ , with  $T_{\text{tot}} = \frac{1}{2}$ ,  $\frac{1}{10}$ , and  $\frac{1}{100}$ , from left to right, respectively. Simulation parameters: reconciliation efficiency  $\beta = 0.95$ , excess noise  $\varepsilon_{\text{tot}} = 0.04$ , detection efficiency  $\eta_d = 1$ .

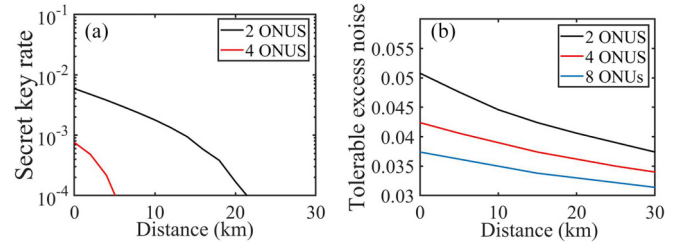


FIG. 8. The performance of QPSK protocol in the downstream-access network. (a) The function of secret key rate and transmission distance with different number of ONUs. (b) The function of tolerable excess noise and transmission distance with a different number of ONUs. Simulation parameters: the excess noise  $\varepsilon_{\text{tot}} = 0.04$ , reconciliation efficiency  $\beta = 0.95$ , detection efficiency  $\eta_d = 0.48$ , electronic noise  $\eta_e = 0.9$ , the sending amplitude  $\alpha = 0.7$ .

$T_{\text{tot}} = \frac{1}{100}$  represents the case where there are more ONUs connected or a small number of ONUs with long distance communication. We finally select the parameters:  $v = 0.5$ ,  $\alpha_0 = 0.45$ , and  $a_c = 1.5a_0$ . Note that, in order to cover a wide range of scenarios, we set  $\eta_d = 1$ . This does not imply that this optimization is restricted to exclusive use by an ideal detector. As Eq. (21) shows,  $\eta_d T_{\text{tot}}$  can be considered as a whole. In other words, the actual scenarios we choose are  $\eta_d T_{\text{tot}} = \frac{1}{2}$ ,  $\frac{1}{10}$ , and  $\frac{1}{100}$ . For the practical nonideal detector, we can initially determine the value of  $\eta_d T_{\text{tot}}$  and select the suitable parameters according to Fig. 7.

Figure 8 shows the secret key rate and tolerable excess noise of the QPSK protocol with a different number of ONUs and distance. We choose the parameter  $\alpha = 0.7$  based on the result of the scan optimization in the downstream-access network. The other parameters we set are based on measurements from our actual system. The QPSK protocol can only support communication at a distance of 20 km when the number of ONUs is 2. The number of ONUs that can be supported is at most 4 when  $\varepsilon_{\text{tot}} = 0.04$ . The most excess noise is 0.05. By contrast, the 16QAM protocol is capable of supporting up to 64 ONUs as shown in Fig. 5.

## V. CONCLUSION

This paper focuses on the MQAM discrete-modulation continuous-variable quantum key distribution protocol in a downstream-access network. In order to support more units in the quantum network, an extra dimension is introduced for signal modulation by quadrature amplitude modulation to address the severe loss and excess noise in the quantum network. By solving the multiplier computational complexity caused by the extra dimension, the application of high-order discrete-modulation CV-QKD is facilitated. Given the actual quantum network, a suitable trusted detector model is given. This trusted detector model, which can be implemented in the quantum network, ensures that the key map for the region operator is consistent with the key map for error rate calculation.

Furthermore, the security analysis of the downstream-access quantum network can be conducted with MQAM CV-QKD. Finally, the simulation of the 16QAM protocol is performed in the downstream-access network. Even though

the number of ONUs reaches 64, our protocol remains effective in ensuring a communicable distance of 5 km and a tolerable excess noise of 0.03. If the number of ONUs is no greater than 4, it is possible to achieve a high secret key rate and tolerable excess noise of at least 0.07 within 30 km. These results also confirm that the 16QAM constellation scheme improves the supported number of ONUs by 16 times compared to the QPSK constellation scheme.

In this paper, MQAM CV-QKD is achieved in a downstream-access quantum network, which paves the way for construction of large-scale practical quantum-key-

distribution networks and the application of high-order discrete modulation in quantum networks.

### ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China under Grants No. 62371060, No. 62001041, and No. 62201012; the Fundamental Research Funds of BUPT under Grant No. 2022RC08; and the Fund of State Key Laboratory of Information Photonics and Optical Communications under Grant No. IPOC2022ZT09.

- 
- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
- [2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photon.* **12**, 1012 (2020).
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [4] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [5] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-speed measurement-device-independent quantum key distribution with integrated silicon photonics, *Phys. Rev. X* **10**, 031030 (2020).
- [6] H.-L. Yin, P. Liu, W.-W. Dai, Z.-H. Ci, J. Gu, T. Gao, Q.-W. Wang, and Z.-Y. Shen, Experimental composable security decoy-state quantum key distribution using time-phase encoding, *Opt. Express* **28**, 29479 (2020).
- [7] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Squashing model for detectors and applications to quantum-key-distribution protocols, *Phys. Rev. A* **89**, 012325 (2014).
- [8] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation: The theory of practical implementations, *Adv. Quantum Technol.* **1**, 1800011 (2018).
- [9] 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).
- [10] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [11] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 5235 (2014).
- [12] M. M. Wilde, M. Tomamichel, and M. Berta, Converse bounds for private communication over quantum channels, *IEEE Trans. Inf. Theory* **63**, 1792 (2017).
- [13] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. Cope, G. Spedalieri, and L. Banchi, Theory of channel simulation and bounds for private communication, *Quantum Sci. Technol.* **3**, 035009 (2018).
- [14] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, *Phys. Rev. Lett.* **114**, 070501 (2015).
- [15] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Korpts, 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).
- [16] 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).
- [17] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, *Phys. Rev. A* **97**, 052327 (2018).
- [18] P. D. Townsend, Quantum cryptography on multiuser optical fibre networks, *Nature (London)* **385**, 47 (1997).
- [19] M. Razavi, Multiple-access quantum key distribution networks, *IEEE Transactions on Communications* **60**, 3071 (2012).
- [20] S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk, and F. Hipp, Quantum key distribution over optical access networks, in *Proceedings of the 2013 18th European Conference on Network and Optical Communications and 2013 8th Conference on Optical Cabling and Infrastructure (NOC-OC&I)* (Graz, Austria, 2013), pp. 11–18.
- [21] X. Wang, Z. Chen, Z. Li, D. Qi, S. Yu, and H. Guo, Experimental upstream transmission of continuous variable quantum key distribution access network, *Opt. Lett.* **48**, 3327 (2023).
- [22] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, A quantum access network, *Nature (London)* **501**, 69 (2013).
- [23] B. K. Park, M. K. Woo, Y.-S. Kim, Y.-W. Cho, S. Moon, and S.-W. Han, User-independent optical path length compensation scheme with sub-ns timing resolution for  $1 \times N$  quantum key distribution network system, *Photon. Res.* **8**, 296 (2020).
- [24] Y. Huang, T. Shen, X. Wang, Z. Chen, B. Xu, S. Yu, and H. Guo, Realizing a downstream-access network using continuous-variable quantum key distribution, *Phys. Rev. Appl.* **16**, 064051 (2021).
- [25] 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).
- [26] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, Asymptotic security of binary modulated continuous-variable quantum key



- distribution under collective attacks, *Phys. Rev. A* **79**, 012307 (2009).
- [27] D. Sych and G. Leuchs, Coherent state quantum key distribution with multi letter phase-shift keying, *New J. Phys.* **12**, 053019 (2010).
- [28] K. Brádler and C. Weedbrook, Security proof of continuous-variable quantum key distribution using three coherent states, *Phys. Rev. A* **97**, 022310 (2018).
- [29] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels, *Phys. Rev. A* **98**, 012340 (2018).
- [30] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, Implementation of continuous-variable quantum key distribution with discrete modulation, *Quantum Sci. Technol.* **2**, 024010 (2017).
- [31] Q. Liao, G. Xiao, C.-G. Xu, Y. Xu, and Y. Guo, Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source, *Phys. Rev. A* **102**, 032604 (2020).
- [32] E. Kaur, S. Guha, and M. M. Wilde, Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution, *Phys. Rev. A* **103**, 012412 (2021).
- [33] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Numerical approach for unstructured quantum key distribution, *Nat. Commun.* **7**, 11712 (2016).
- [34] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, *Quantum* **2**, 77 (2018).
- [35] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, *Phys. Rev. X* **9**, 041064 (2019).
- [36] 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).
- [37] 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).
- [38] 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).
- [39] 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).
- [40] 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).
- [41] W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance, *PRX Quantum* **2**, 040334 (2021).
- [42] S. Bäuml, C. P. García, V. Wright, O. Fawzi, and A. Acín, Security of discrete-modulated continuous-variable quantum key distribution, [arXiv:2303.09255](https://arxiv.org/abs/2303.09255).
- [43] 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).
- [44] Z.-P. Liu, M.-G. Zhou, W.-B. Liu, C.-L. Li, J. Gu, H.-L. Yin, and Z.-B. Chen, Automated machine learning for secure key rate in discrete-modulated continuous-variable quantum key distribution, *Opt. Express* **30**, 15024 (2022).
- [45] F. Kanitschar and C. Pacher, Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection, *Phys. Rev. Appl.* **18**, 034073 (2022).
- [46] 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).
- [47] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM, in *2021 European Conference on Optical Communication (ECOC)* (IEEE, New York, 2021), pp. 1–4.
- [48] 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).
- [49] 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).
- [50] C. Lei, J. Zhang, Y. Li, Y. Zhao, K. Wang, S. Liu, B. Wang, H. Gao, and J. Li, 16 QAM quantum noise stream cipher coherent transmission over 300 km without intermediate amplifier, *IEEE Photonics Technol. Lett.* **33**, 1002 (2021).
- [51] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, <http://cvxr.com/cvx>.
- [52] M. Grant and S. Boyd, Graph implementations for nonsmooth convex programs, in *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag, New York, 2008), pp. 95–110.
- [53] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. A* **461**, 207 (2005).
- [54] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, *Nature (London)* **421**, 238 (2003).
- [55] R. García-Patrón and N. J. Cerf, Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution, *Phys. Rev. Lett.* **97**, 190503 (2006).
- [56] M. Navascués, F. Grosshans, and A. Acín, Optimality of gaussian attacks in continuous-variable quantum cryptography, *Phys. Rev. Lett.* **97**, 190502 (2006).
- [57] A. Leverrier and P. Grangier, Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a gaussian modulation, *Phys. Rev. A* **81**, 062314 (2010).
- [58] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian quantum states, *Phys. Rev. Lett.* **96**, 080502 (2006).
- [59] X. Wang, H. Wang, C. Zhou, Z. Chen, S. Yu, and H. Guo, Continuous-variable quantum key distribution with low-complexity information reconciliation, *Opt. Express* **30**, 30455 (2022).
- [60] X. Wang, M. Xu, Y. Zhao, Z. Chen, S. Yu, and H. Guo, Non-Gaussian reconciliation for continuous-variable quantum key distribution, *Phys. Rev. Appl.* **19**, 054084 (2023).