Chaos, Solitons and Fractals 196 (2025) 116331

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

journal homepage: www.elsevier.com/locate/chaos

High-rate discretely-modulated continuous-variable quantum key distribution using quantum machine learning

Qin Liao [a], Zhuoying Fei [a], Jieyu Liu [a], Anqi Huang [b], Lei Huang [a], Yijun Wang [c,*]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha, 410082, China
[b] Institute for Quantum Information and State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha, 410003, China
[c] Center for Optoelectronic Information Engineering, School of Automation, Central South University, Changsha, 410083, China

ARTICLE INFO

Keywords:
Quantum machine learning
Quantum key distribution
*k*NN classification

ABSTRACT

Continuous-variable quantum key distribution (CVQKD) is one of the promising ways to ensure information security. In this paper, we propose a high-rate scheme for discretely-modulated (DM) CVQKD using quantum machine learning technologies, which divides the whole CVQKD system into three parts, i.e., the initialization part that is used for training and estimating quantum classifier, the prediction part that is used for generating highly correlated raw keys, and the data postprocessing part that generates the final secret key string shared by Alice and Bob. To this end, a low-complexity quantum k-nearest neighbor (QkNN) classifier is designed for predicting the lossy discretely-modulated coherent states (DMCSs) at Bob's side. The performance of the proposed QkNN-based CVQKD especially in terms of machine learning metrics and complexity is analyzed, and its theoretical security is proved by using semi-definite program (SDP) method. Numerical simulation shows that the secret key rate of our proposed scheme is explicitly superior to that of the existing DM CVQKD protocols, and it can be further enhanced with the increase of modulation variance.

1. Introduction

Continuous-variable quantum key distribution [1] (CVQKD) is designed to implement point-to-point and point to multi-point [2–4] secret key distribution, its security is guaranteed by the fundamental laws of quantum physics [5]. In a basic version of CVQKD [6], the sender, called Alice, encodes secret key bits in the phase space of coherent states and sends them to an insecure quantum channel, while the receiver, called Bob, measures these incoming signal states with coherent detection [7]. After several steps of data post-processing, a string of secret keys can be finally shared by Alice and Bob. One of the advantages of CVQKD is that it is compatible with most existing commercial telecommunication technologies [8–10], making it easier to integrate into real-world communication links.

In general, a CVQKD system is mainly composed of quantum signal processing and data postprocessing. The former part corresponds to signal modulation, transmission, and measurement, aiming to generate raw keys, while the latter part corresponds to data reconciliation, parameter estimation, and privacy amplification, attempting to extract the final secret keys from the raw keys. In CVQKD, secret key rate and maximal transmission distance are generally a pair of crucial performance indicators. For a specific CVQKD system, however, there is a tradeoff between the secret key rate and the maximal transmission distance: the longer the transmission distance, the lower the secret key rate, and vice versa. The main reason is that the continuous-variable quantum signal used to carry the secret key is extremely weak. Channel loss and excess noise rise as transmission distance increases [11,12], resulting in a reduction of signal-to-noise ratio (SNR) [13]. This leads a coherent detector to hardly discriminate between the quantum signal and noise, decreasing the secret key rate. Although some solutions, such as adding an optical amplifier [14] and adopting non-Gaussian operation [15,16], can effectively improve the performance of the CVQKD system, its improvement seems limited as they are still largely constrained by the imperfect devices.

In recent years, CVQKD using machine learning technologies is becoming a research hotspot, as these technologies can be used for improving the performance of CVQKD without any extra device [17,18]. More importantly, machine learning technologies can automatically compensate for the negative effects caused by imperfect devices, effectively removing the performance restriction of the imperfect devices. For instance, Ref. [19] reported a state-discrimination detector based on a Bayesian classification algorithm. This detector has the ability to surpass the standard quantum limit, which can be only achieved by

* Corresponding author.
E-mail address: xxywyj@sina.com (Y. Wang).

https://doi.org/10.1016/j.chaos.2025.116331
Received 11 February 2025; Received in revised form 10 March 2025; Accepted 16 March 2025
Available online 30 March 2025

conventional ideal detectors [20], so that the maximum transmission distance of the CVQKD system can be significantly increased. Ref. [21] suggested a multi-label learning-based embedded classifier with the capability to precisely predict the location of the signal state in phase space, so that it can dramatically improve the performance of the CVQKD system as well.

Although these works do reveal that machine learning-based technologies can significantly improve the performance of CVQKD system, an underlying issue seems to be neglected. With an extremely large amount of signal data, the complexity of the majority of machine learning technologies is nearly unacceptable, and this situation is especially severe in high-speed CVQKD system [22]. For example, the core machine learning technology used in Ref. [21] is k-nearest neighbor (kNN) [23], which is one of the most mature classification algorithms. However, kNN has a very high complexity as each unlabeled instance has to calculate all the distances between all labeled instances and itself, rendering extraordinary consumption in both time and space. These heavy costs have to be well addressed, otherwise CVQKD using machine learning technologies is unpractical, especially for the high-speed and/or real-time secret key distribution scenarios.

In past few years, quantum machine learning, which is based on quantum algorithms such as Shor's algorithm [24] and Grover's algorithm [25], has been developed rapidly. For example, Ref. [26] proposed a quantum linear regression algorithm based on the quantum Harrow–Hassidim–Lloyd (HHL) algorithm [27], which can efficiently estimate the parameter of quantum states in case of pure quantum states input. Ref. [28] reported a quantum support vector machine (SVM) which used the high parallelism of quantum computing to improve the classical SVM, thus obtaining an exponential speedup. Refs. [29,30] showed that the classical K-means algorithm can be accelerated by quantum minimal finding method. The above studies indicate that quantum algorithms contribute to speeding up machine learning, thereby improving the computing efficiency.

Inspired by the merits of quantum algorithms, in this work, we propose a high-rate CVQKD scheme based on quantum machine learning. The proposed scheme is quite different from conventional discretely-modulated (DM) CVQKD [31–34], which divides the whole CVQKD system into three parts, initialization, prediction and data postprocessing. The initialization part is used for training and estimating quantum classifier, the prediction part is used for generating highly correlated raw keys, and the data postprocessing part generates the final secret key string shared by Alice and Bob. In particular, a quantum k-nearest neighbor (QkNN) algorithm is designed as a quantum classifier for distinguishing the lossy discretely-modulated coherent states (DMCSs) at Bob's side. Different from classical kNN algorithm, QkNN simultaneously calculates all similarities in parallel, and sorts them by taking advantages of Grover's algorithm, thereby greatly reducing the complexity. The performance of the proposed QkNN-based CVQKD especially in terms of machine learning metrics and complexity is analyzed, and its theoretical security is proved by using semi-definite program (SDP) method. Numerical simulation shows that the secret key rate of QkNN-based CVQKD is explicitly superior to that of the existing DM CVQKD protocols, and it can be further enhanced with the increase of modulation variance. It indicates that the proposed QkNN-based CVQKD is suitable for the high-speed metropolitan secure communication due to its advantages of high-rate and low-complexity.

This paper is structured as follows. In Section 2, we briefly introduce the CVQKD protocol and classical kNN algorithm. In Section 3, we detail the proposed QkNN-based CVQKD. Performance analysis and discussion are presented in Section 4 and conclusions are drawn in Section 5.

2. CVQKD protocol and classical kNN algorithm

In order to make the paper self-contained, in this section, we first retrospect the process of CVQKD protocol, and briefly introduce the classical kNN algorithm.

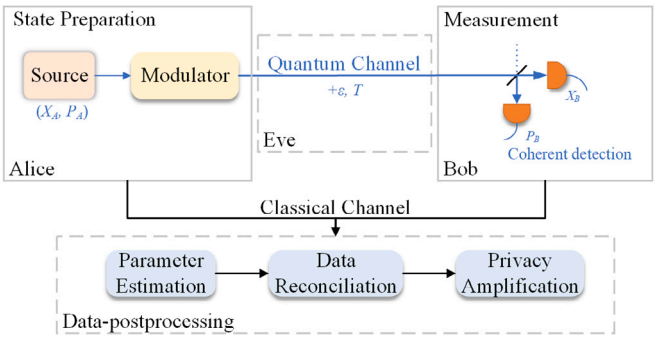

Fig. 1. The process of conventional CVQKD. Alice first prepares a modulated coherent state, and sends it to Bob through an untrusted quantum channel. Bob measures the incoming state with coherent detection so that Alice and Bob share two correlated sets variables, i.e. raw key. The final secret key can be obtained after data postprocessing, which includes parameter estimation, data reconciliation and privacy amplification.

2.1. Process of CVQKD protocol

In general, the whole process of one-way CVQKD protocol includes five steps, i.e., state preparation, measurement, parameter estimation, data reconciliation and privacy amplification. Fig. 1 shows the process of conventional CVQKD, and each step is explained as follows.

State Preparation. Alice prepares a train of coherent states whose quadrature values x and p obey a bivariate Gaussian distribution. Then the modulated coherent states are sent to Bob through an untrusted quantum channel.

Measurement. The pulses sent by Alice are received by Bob who measures these incoming signal states with coherent detector. After enough rounds, a string of raw keys can be shared between Alice and Bob.

Parameter Estimation. Alice and Bob disclose part of the raw keys to calculate the transmittance T and excess noise ε of the quantum channel. With these two parameters, the secret key rate can be estimated.

Data Reconciliation. If the estimated secret key rate is positive, the low density parity check (LDPC) code is applied to another part of the raw key, aiming to error correction.

Privacy Amplification. Finally, a privacy amplification algorithm is performed based on the hash function, so as to extract the final secret keys that are entirely unknown to the eavesdropper Eve.

2.2. Classical kNN algorithm

kNN is a traditional lazy learning algorithm that uses a majority vote to classify (predict) the grouping of unlabeled data points. For an unlabeled data point v_0 and a training set containing v_j $(j = 1, 2, \ldots, M)$ labeled data points, kNN first finds a set of labeled data points whose similarities with v_0 are the top k highest among all data points in training set, and then counts the number of each label, the label with the biggest number will be assigned as the label of data point v_0. Fig. 2 depicts an example of kNN algorithm in 2-dimensional feature space, in which a gray dot denotes an unlabeled data point and it is going to be labeled as green or blue. The gray dot will be assigned to the blue class when $k = 3$ due to there are two of the three-nearest labeled data points belong to the blue class while only one point belongs to the green class. Similarly, it will be labeled as green class for $k = 7$ as there are four of the seven-nearest labeled data points belong to the green class while only three points belong to the blue class.

The specific steps of kNN can be seen in Table 1. It is worth noting that the similarity is one of the crucial parameters of kNN algorithm. Assuming $\mathbf{v_0} = (v_{01}, v_{02}, \ldots, v_{0U})$ and $\mathbf{v_j} = (v_{j1}, v_{j2}, \ldots, v_{jU})$ are the respective feature vectors of unlabeled data point v_0 and labeled data point v_j, similarity can be measured by following ways.

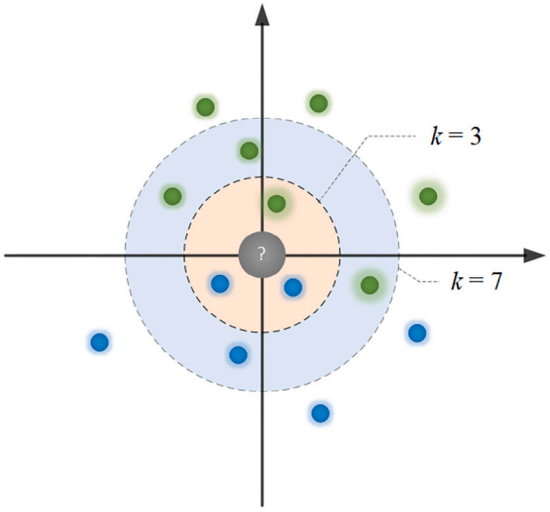

Fig. 2. An example of kNN algorithm in 2-dimensional feature space. The gray dot denotes an unlabeled data point. The green dots and blue dots are two classes of labeled data points. The gray dot will be assigned to the blue class when k=3, and it will be assigned to the green class when k=7. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

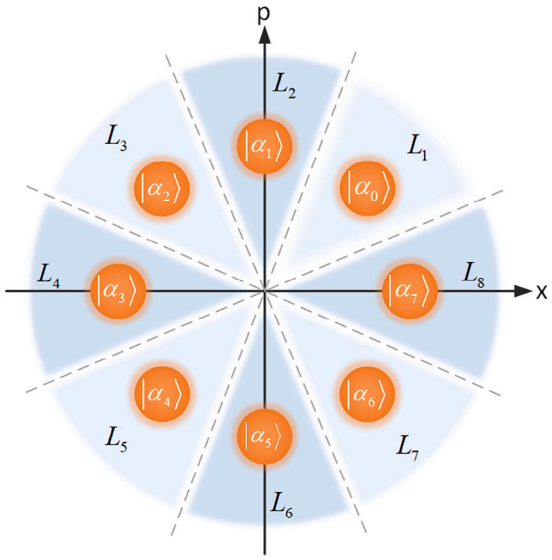

Fig. 3. Phase space representation of coherent states with 8PSK modulation. The orange dots $|\alpha_0\rangle$ to $|\alpha_7\rangle$ are standard 8PSK-modulated coherent states. Each coherent state is assigned to a label according to its location. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 1
kNN algorithm.

Input : training data points $V_j = \{\mathbf{v_1}, \mathbf{v_2}, ..., \mathbf{v_M}\}$ and their labels $V_j^L = \{v_1^L, v_2^L, ..., v_M^L\}$, unlabeled data point $\mathbf{v_0}$ and hyper-parameter k.
Output : predicted label v_0^L of data point $\mathbf{v_0}$.

function Predict
Load all training data points V_j and unlabeled data point $\mathbf{v_0}$ on the register.
for $j \leftarrow 1$ to M **do**
Compute $\mathrm{Sim}_{0j} = S(\mathbf{v_0}, \mathbf{v_j})$.
end for
Sort $S = \{\mathrm{Sim}_{01}, \mathrm{Sim}_{02}, ...\mathrm{Sim}_{0M}\}$ (descending or ascending).
Choose k neighbors which are nearest to $\mathbf{v_0}$.
Conduct majority voting and assign the label v_j^L of the majority to the data point $\mathbf{v_0}$.
return v_0^L
end function

Euclidean distance

$$\mathrm{Sim}_E(\mathbf{v_j}, \mathbf{v_0}) = \sqrt{\sum_{r=1}^{U}(v_{jr} - v_{0r})^2}. \tag{1}$$

Cosine similarity

$$\mathrm{Sim}_C(\mathbf{v_j}, \mathbf{v_0}) = \frac{\mathbf{v_j} \cdot \mathbf{v_0}}{|\mathbf{v_j}||\mathbf{v_0}|} = \frac{\sum_{r=1}^{U} v_{jr} v_{0r}}{\sqrt{\sum_{r=1}^{U} v_{jr}^2}\sqrt{\sum_{r=1}^{U} v_{0r}^2}}. \tag{2}$$

In the above two similarities, Euclidean distance counts the absolute distance of each data point, revealing the difference of each data point's location in the coordinate system [35]. Cosine similarity counts the cosine of an angle between two vectors, revealing the directional difference of each vector [36]. In addition, Manhattan distance [37], Hamming distance [38] and inner product also can be used as similarity in kNN, one should select a proper way according to different applications.

3. QkNN-based CVQKD

Before we detail the proposed QkNN-based CVQKD, several concepts need to be introduced. As shown in Fig. 3, the coherent states that Alice prepared are discretely modulated with 8 phase shift keying (8PSK). We equally divide the entire phase space into eight areas, and assign each area to a label L_i ($i = 1, 2, \ldots, 8$). By doing so, each coherent state can be classified into a certain label according to its position. For example, coherent state $|\alpha_0\rangle$ belongs to label L_1 and coherent state $|\alpha_7\rangle$ belongs to label L_8. Note that although our study is mainly based on 8PSK modulation strategy, other discrete modulation strategies can also be used for the proposed QkNN-based CVQKD. Fig. 4 shows the change of location in phase space of a modulated coherent state after passing an untrusted quantum channel. It depicts that the transmitted coherent state received by Bob is no longer identical with its initial signal state due to the phase drift ($\theta' \neq \theta$) and energy attenuation ($\sqrt{x'^2 + p'^2} < \sqrt{x^2 + p^2}$) caused by the imperfect channel noise and loss. To detailedly describe this difference, we construct a multi-dimensional feature vector for each received coherent state by calculating Euclidean distances between the received coherent state and each standard 8PSK-modulated coherent state. By extracting these distance features, the features of received coherent state can be extended from three dimensions (x', p', θ') to eight dimensions $(d_0, d_1, d_2, \ldots, d_7)$. For now, the Q$k$NN-based CVQKD can be detailed below.

As shown in Fig. 5, the whole QkNN-based CVQKD system can be divided into three parts, i.e., initialization, prediction and data postprocessing.

Initialization. Alice first prepares DMCSs with 8PSK modulation and labels each DMCS which follows the rule shown in Fig. 3. Both DMCSs and their respective labels are sent to Bob who measures the received signals with heterodyne detection [39], and these DMCSs are called training data. Bob subsequently extracts features from each measurement result to obtain an eight-dimensional feature vector. After collecting enough feature vectors, Bob locally prepares a quantum state $|\tau\rangle$ to carry the information of all feature vectors. Note that the aim of the initialization part is to prepare quantum state $|\tau\rangle$ which stores feature information of all labeled DMCSs, so that once the quantum state $|\tau\rangle$ has been successfully prepared, one does not need to perform this part repeatedly. To guarantee the security, the transmission of labels has to be done without eavesdropping. This can be implemented by multiple ways, for example, legitimate users can securely transmit information of labels by applying physical isolation or one-way transmission, and they can also prevent Eve from eavesdropping by monitoring the communication system when the labels are transmitting. Even if the information of labels is compromised, the initialization part can be rerun to prepare new DMCSs and their respective labels.

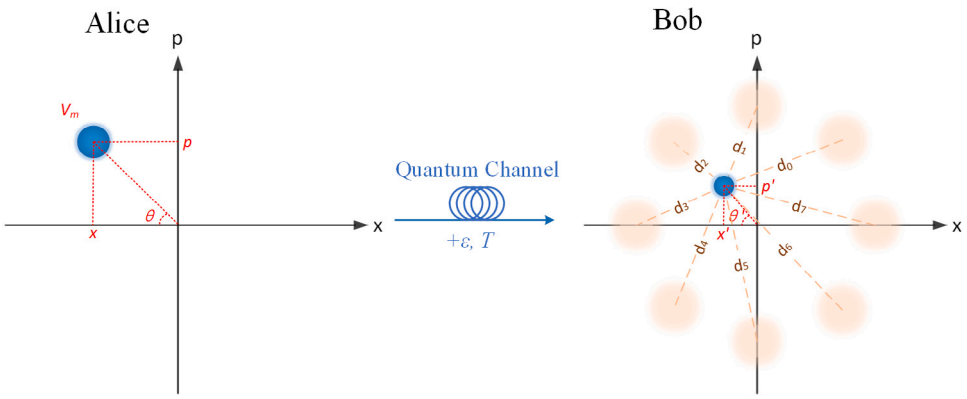

Fig. 4. Feature construction for coherent state in phase space. (Left) Alice randomly selects one of the 8PSK-modulated coherent states and sends it to the untrusted quantum channel. (Right) Bob receives the transmitted coherent state and extracts its eight-dimensional distance features $(d_0, d_1, d_2, \ldots, d_7)$.

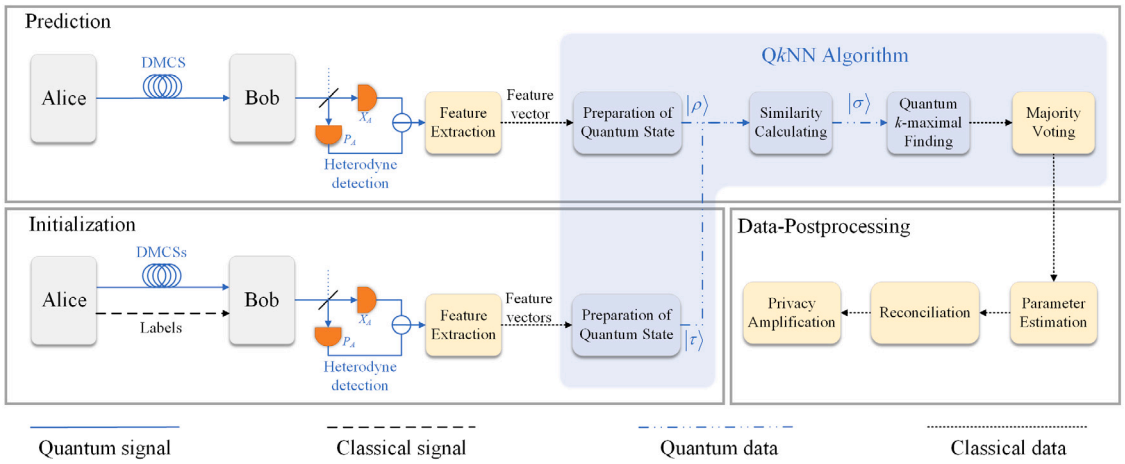

Fig. 5. The process of Q*k*NN-based CVQKD. It is divided into initialization, prediction and data postprocessing. Yellow boxes represent classical operation, and blue boxes represent quantum operation. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Prediction. Alice randomly prepares an unlabeled DMCS with 8PSK modulation and sends it to the untrusted quantum channel. Bob receives this incoming signal state and measures it with heterodyne detection. Similarly, an eight-dimensional feature vector for this signal state can be constructed according to its measurement result. Bob then locally prepares a quantum state $|\rho\rangle$ to carry the information of this feature vector. For now, Bob holds both quantum state $|\rho\rangle$ that stores the information of unlabeled DMCS and quantum state $|\tau\rangle$ that stores the information of labeled DMCSs. He subsequently calculates the similarities between these quantum states and stores them into quantum state $|\sigma\rangle$. After quantum k-maximal finding, k nearest neighbors of the unlabeled DMCS can be found. Finally, the label whose count is the biggest in k nearest neighbors is assigned to the unlabeled DMCS, so that Bob can precisely recover the bit information sent by Alice. After enough rounds, Alice and Bob can share a string of raw keys. Compared with the raw keys generated by conventional DM CVQKD, the raw keys generated by this part are more correlated.

data postprocessing. This part is similar to the postprocessing of conventional CVQKD, which includes parameter estimation, data reconciliation and privacy amplification. Details about these steps can be found in Ref. [40].

With these three parts, secret keys can be finally shared between Alice and Bob. In what follows, several critical steps of the proposed Q*k*NN-based CVQKD is detailed.

3.1. Preparation of quantum states

As we mentioned above, Bob needs to prepare quantum states ($|\tau\rangle$ or $|\rho\rangle$) in both initialization part and prediction part. The difference is that quantum state $|\tau\rangle$ is prepared in initialization part to carry the information of all feature vectors extracted from labeled DMCSs, while quantum state $|\rho\rangle$ is prepared in prediction part to carry the information of feature vector extracted from an unlabeled DMCS. Assuming the normalized feature vectors extracted from labeled DMCSs are $V = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_M}\}$ and the normalized feature vector extracted from an unlabeled DMCS is $\mathbf{v_0}$, the quantum states $|\tau\rangle$ and $|\rho\rangle$ can be respectively expressed by [41]

$$|\tau\rangle = \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle|1\rangle(\sqrt{1-v_{ji}^2}|0\rangle + v_{ji}|1\rangle), \tag{3}$$

and

$$|\rho\rangle = \frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle(\sqrt{1-v_{0i}^2}|0\rangle + v_{0i}|1\rangle)|1\rangle, \tag{4}$$

where v_{ji} (v_{0i}) is the ith feature value of feature vector $\mathbf{v_j}$ ($\mathbf{v_0}$), U is the dimension of the extracted features ($U = 8$ in our case) and M is the number of labeled DMCSs. Obviously, $|\tau\rangle$ is the superposition state that carries the information of all feature vectors for known (labeled) DMCSs, while $|\rho\rangle$ is the quantum state that carries the information of feature vector for an unknown (unlabeled) DMCS.

In what follows, we show how to obtain these two quantum states. To prepare quantum state $|\tau\rangle$, we first need to prepare an initial state

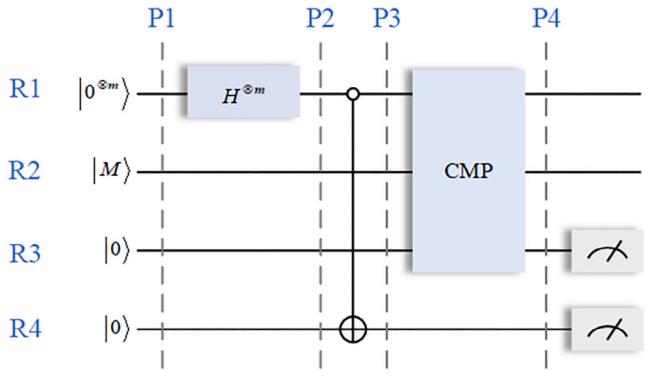

Fig. 6. The quantum circuit for preparing $\frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle$. $|M\rangle$ is the computational basis state that stores M as a binary string, and $m = \lceil \log_2(M+1) \rceil$. H is the Hadamard gate, CMP is a comparison operator.

$|\tau_{init}\rangle$ which can be expressed as

$$|\tau_{init}\rangle = \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle|0\rangle|0\rangle, \tag{5}$$

where state $\frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle$ (or state $\frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle$) can be obtained by a quantum circuit shown in Fig. 6. See Appendix A for the detailed derivation of initial state $|\tau_{init}\rangle$. Subsequently, an Oracle $\mathcal{O}|j\rangle|i\rangle|0\rangle = |j\rangle|i\rangle|v_{ji}\rangle$ is applied to this initial state so that the resultant state $|\tau_o\rangle$ can be expressed by

$$\begin{aligned}|\tau_o\rangle &= \mathcal{O}|\tau_{init}\rangle \\ &= \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle|v_{ji}\rangle|0\rangle.\end{aligned} \tag{6}$$

After that, a unitary operation

$$R_y(2\sin^{-1}v_{ji}) = \begin{bmatrix} \sqrt{1-v_{ji}^2} & -v_{ji} \\ v_{ji} & \sqrt{1-v_{ji}^2} \end{bmatrix} \tag{7}$$

is applied to the last quantum bit (qubit) of $|\tau_o\rangle$, so that the rotated state

$$\begin{aligned}|\tau_r\rangle &= R_y(2\sin^{-1}v_{ji})|\tau_o\rangle \\ &= \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle|v_{ji}\rangle(\sqrt{1-v_{ji}^2}|0\rangle + v_{ji}|1\rangle)\end{aligned} \tag{8}$$

can be obtained. Finally, the quantum state $|\tau\rangle$ can be obtained by removing the auxiliary qubit $|v_{ji}\rangle$ of $|\tau_r\rangle$ using Oracle $\mathcal{O}^\dagger$. Similarly, the quantum state $|\rho\rangle$ can be prepared in the same way with initial state $|\rho_{init}\rangle = \frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle|0\rangle|0\rangle$. As a result, the information of feature vectors can be stored in the amplitude of quantum states $|\tau\rangle$ and $|\rho\rangle$.

3.2. Similarity calculating

For now, Bob possesses both the quantum state $|\tau\rangle$ that carries the information of known DMCSs and the quantum state $|\rho\rangle$ that carries the information of unknown DMCS. He first calculates the fidelity, which can be used as a measure of the similarity, between these quantum states and stores it to the amplitude of qubit by performing a controlled-SWAP (c-SWAP) test shown in Fig. 7. The quantum circuit of c-SWAP test is composed of two Hadamard gates and a SWAP operation which obeys $\text{SWAP}|\rho\rangle|\tau_j\rangle = |\tau_j\rangle|\rho\rangle$, where

$$|\tau_j\rangle = \frac{1}{\sqrt{U}}\sum_{i=1}^{U}|i\rangle|1\rangle(\sqrt{1-v_{ji}^2}|0\rangle + v_{ji}|1\rangle). \tag{9}$$

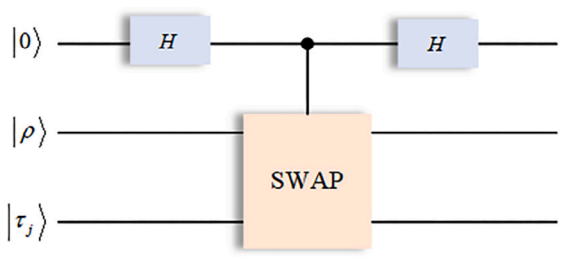

Fig. 7. The c-SWAP test quantum circuit.

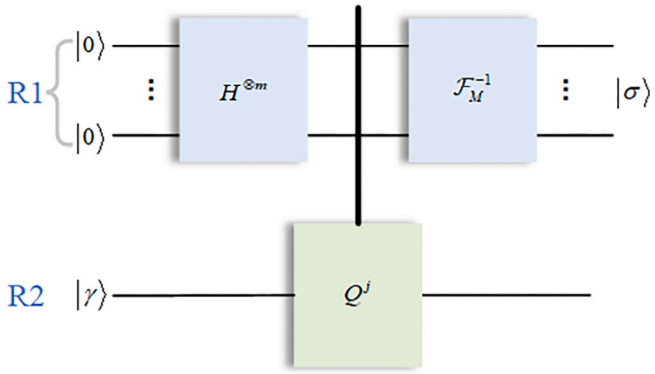

Fig. 8. The quantum circuit for amplitude estimation. It is used to obtain the estimate from the amplitude of a quantum state. Q is an unitary operator which obeys $Q = -\mathcal{A}S_0\mathcal{A}^\dagger S_\chi$ and $\mathcal{F}^{-1}$ is quantum inverse Fourier transform. Q^j denotes j applications of operator Q.

Therefore, the function of c-SWAP test is that the last two states will be swapped if the control qubit is $|1\rangle$ or they will not be swapped if the control qubit is $|0\rangle$.

After passing the c-SWAP test, the input state can be transformed to

$$\begin{aligned}|\gamma_j\rangle &= \text{c-SWAP}|0\rangle|\rho\rangle|\tau_j\rangle \\ &= \frac{1}{2}|0\rangle(|\rho\rangle|\tau_j\rangle + |\tau_j\rangle|\rho\rangle) + \frac{1}{2}|1\rangle(|\rho\rangle|\tau_j\rangle - |\tau_j\rangle|\rho\rangle) \\ &= \sqrt{P_j(0)}|0\rangle + \sqrt{1-P_j(0)}|1\rangle,\end{aligned} \tag{10}$$

where

$$P_j(0) = \frac{1+|\langle\rho|\tau_j\rangle|^2}{2}. \tag{11}$$

See Appendix B for the detailed derivation of $P_j(0)$. It is easy to find that $P_j(0)$ is directly proportional to the fidelity $|\langle\rho|\tau_j\rangle|^2$, so that $P_j(0)$ can be directly used for measuring the similarity between $|\rho\rangle$ and $|\tau_j\rangle$. After M times c-SWAP test, a superposition state whose amplitudes contain all similarities can be finally obtained as

$$|\gamma\rangle = \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle(\sqrt{P_j(0)}|0\rangle + \sqrt{1-P_j(0)}|1\rangle). \tag{12}$$

In order to facilitate the processing of follow-up quantum search algorithm, amplitude estimation [42] is further applied to this superposition state so that the amplitudes of $|\gamma\rangle$ can be stored as a qubit string. Fig. 8 shows the quantum circuit for implementing amplitude estimation, which includes two steps, i.e., amplitude amplification and phase estimation. Specifically, amplitude amplification is implemented by an unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^\dagger S_\chi$ where $\mathcal{A}$ performs $|0^{\otimes m}\rangle \to |\gamma\rangle$, S_0 obeys

$$S_0|x\rangle = \begin{cases} |x\rangle, x \neq 0 \\ -|x\rangle, x = 0 \end{cases}, \tag{13}$$

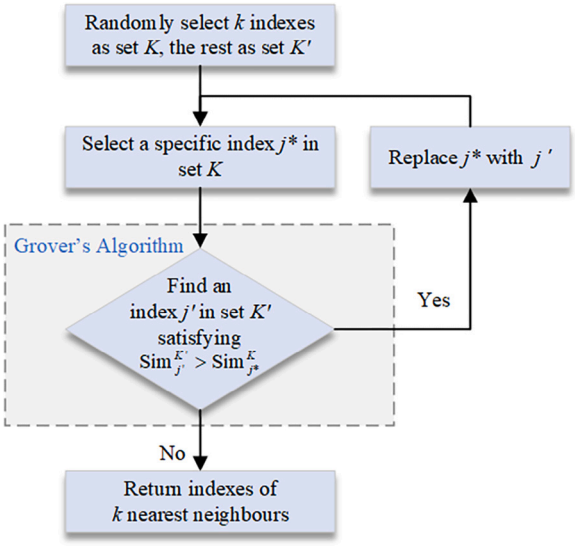

Fig. 9. The flow chart of the quantum k-maximal finding algorithm.

and S_χ obeys

$$S_\chi|x\rangle = \begin{cases} |x\rangle, \chi(x) = 0 \\ -|x\rangle, \chi(x) = 1 \end{cases}, \tag{14}$$

while phase estimation is implemented by an inverse quantum Fourier transform (IQFT) $\mathcal{F}^{-1}$ which is defined as

$$\mathcal{F}_M^{-1}|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} exp(-\iota\frac{2\pi}{M}xy)|y\rangle, \tag{15}$$

where $0 \le x < M$, $\iota = \sqrt{-1}$. After amplitude estimation, a quantum state

$$|\sigma\rangle = \frac{1}{\sqrt{M}} \sum_{j=1}^{M} |j\rangle \left|\mathrm{Sim}_j\right\rangle \tag{16}$$

can be prepared, where $\mathrm{Sim}_j = \frac{M}{\pi}\arcsin(\sqrt{\widetilde{P_j}(0)})$ and $\widetilde{P_j}(0)$ is the estimate of $P_j(0)$. See Appendix C for the detailed derivation of quantum state $|\sigma\rangle$. For now, the similarities can be deemed to have been stored as a qubit string due to Sim_j is also directly proportional to the fidelity $|\langle\rho|\tau_j\rangle|^2$.

3.3. Quantum k-maximal finding

Bob now holds the quantum state $|\sigma\rangle$ whose qubit string contains the information of similarities between all known DMCSs and the unknown DMCS. He then finds k nearest neighbors of the unknown DMCS by applying quantum k-maximal finding algorithm, which is detailed as follows.

As shown in Fig. 9, Bob first randomly selects k known DMCSs and records their corresponding indexes j into an initial set K, the rest indexes j' are recorded into a set K'. Then, the Grover's algorithm [25] is applied to $|\sigma\rangle$ to find an index j' whose corresponding $|\mathrm{Sim}_{j'}^{K'}\rangle$ satisfying $\mathrm{Sim}_{j'}^{K'} > \mathrm{Sim}_{j^*}^{K}$, where $j^* \in K$. In our case, the quantum circuit for implementing Grover's algorithm is shown in Fig. 10, which includes a number of Grover iterations and a final measurement. Each iteration is composed of a unitary operator S_F and a Grover diffusion operator $\mathcal{D}$. Specifically, S_F denotes conditional phase shift transformation which obeys

$$S_F|j\rangle = \begin{cases} -|j\rangle, F(j) = 1 \\ |j\rangle, \text{otherwise} \end{cases}, \tag{17}$$

Table 2
Confusion matrix.

	Predicted positive	Predicted negative
Actual positive	$\mathcal{N}_{TP}$	$\mathcal{N}_{FN}$
Actual negative	$\mathcal{N}_{FP}$	$\mathcal{N}_{TN}$

where the function F is defined as

$$F(j) = \begin{cases} 1, \ \mathrm{Sim}_j > \mathrm{Sim}_{j^*}^{K} \\ 0, \ \text{otherwise} \end{cases}. \tag{18}$$

The S_F operator can be implemented by a CMP operator and a CNOT gate. After passing the CMP operation, the fourth input qubit $|0\rangle$ is transformed to

$$\frac{1}{\sqrt{M}} \sum_{F(j)=1} |1\rangle + \frac{1}{\sqrt{M}} \sum_{F(j)\neq 1} |0\rangle. \tag{19}$$

Then, the CNOT gate is controlled by the above state so that the last input qubit $|0\rangle$ is transformed to

$$\begin{aligned} |0\rangle &\xrightarrow{X} |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\xrightarrow{CNOT} \frac{1}{\sqrt{2M}} \sum_{j=1}^{M} (-1)^{F(j)}(|0\rangle - |1\rangle). \end{aligned} \tag{20}$$

Therefore, the resultant state

$$\begin{aligned} &\frac{1}{\sqrt{M}} \sum_{j=1}^{M} |j\rangle(-1)^{F(j)} \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \left(-\frac{1}{\sqrt{M}} \sum_{F(j)=1} |j\rangle + \frac{1}{\sqrt{M}} \sum_{F(j)\neq 1} |j\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{21}$$

can be obtained after applying S_F operator. The Grover diffusion operator $D = W'S_0W'^{\dagger}$ is subsequently applied to the first qubit of the resultant state, so that its amplitude will be inversed about average [43]. After the first Grover iteration, the state

$$\frac{3M-4t}{M} \frac{1}{\sqrt{M}} \sum_{F(j)=1} |j\rangle + \frac{M-4t}{M} \frac{1}{\sqrt{M}} \sum_{F(j)\neq 1} |j\rangle, \tag{22}$$

where t is the number of solutions of Grover's algorithm, can be obtained. From Eqs. (21) and (22), we can easily find that the amplitude of $\sum_{F(j)=1}|j\rangle$ is amplified. After enough rounds of Grover iteration, the index j' can be obtained by the final measurement with a probability approaching 1 (Details about this iteration is presented in Appendix D). Bob then replaces j^* with j', and starts a new round of Grover's algorithm. Finally, the indexes of k nearest neighbors can be obtained from the final set K.

4. Performance analysis and discussion

In this section, we first present the performance of the proposed QkNN algorithm, followed by its complexity analysis. Subsequently, the security of the whole QkNN-based CVQKD scheme is detailedly analyzed.

4.1. Performance of QkNN algorithm

As the proposed QkNN can be deemed a quantum version of kNN algorithm, classical machine learning metrics can be used for evaluating its performance. In machine learning area, the confusion matrix is one of the most widely used concepts to analyze the performance of a certain classification algorithm. Table 2 shows the confusion matrix, in which the true positive ($\mathcal{N}_{TP}$) indicates the counts that actual positive data are predicted as positive, false positive ($\mathcal{N}_{FP}$) indicates the counts that actual negative data are predicted as positive, false negative ($\mathcal{N}_{FN}$) indicates the counts that actual positive data are predicted as negative,

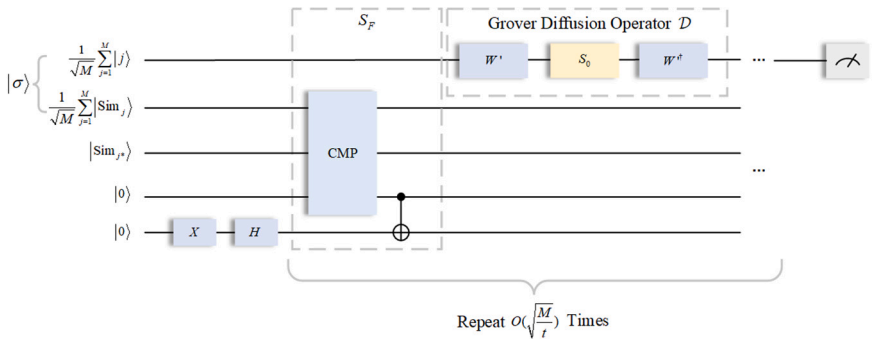

Fig. 10. Quantum circuit of Grover's algorithm. The Grover iteration is composed of a unitary transformation S_F and Grover diffusion operator D. S_F is a unitary transformation to realize phase inversion of the target quantum state, and Grover diffusion operator D is an operator to realize inversion about average of the quantum state. It needs to repeat $O(\sqrt{\frac{M}{t}})$ times of Grover iterations to complete Grover's algorithm.

and true negative ($\mathcal{N}_{TN}$) indicates the counts that actual negative data are predicted as negative.

With confusion matrix, a machine learning metric called **Precision** ($\mathcal{P}_{\mathrm{Prec}}$) can be defined as

$$\mathcal{P}_{\mathrm{Prec}} = \frac{\mathcal{N}_{TP}}{\mathcal{N}_{TP} + \mathcal{N}_{FP}}, \tag{23}$$

which indicates the proportion of actual positive data in all predicted positive data. This metric is important to our case as raw keys are generated from the correct labels in all the predicted labels. Since there are eight labels existing in phase space, we further calculate the precision of each label $\mathcal{P}_{\mathrm{Prec}_i}$ and average them to obtain a metric **Average Precision** $\bar{\mathcal{P}}_{\mathrm{Prec}}$, i.e.

$$\bar{\mathcal{P}}_{\mathrm{Prec}} = \frac{1}{8}\sum_{i=1}^{8}\mathcal{P}_{\mathrm{Prec}_i}. \tag{24}$$

Obviously, the higher the value of $\bar{\mathcal{P}}_{\mathrm{Prec}}$, the more correlated the raw key. Fig. 11 shows the average precision $\bar{\mathcal{P}}_{\mathrm{Prec}}$ of the proposed QkNN algorithm with different hyper-parameter k. By and large, it can be found that the value of $\bar{\mathcal{P}}_{\mathrm{Prec}}$ decreases as transmission distance increases, which indicates that the transmission distance is a crucial factor that impacts the performance of QkNN algorithm. This is in line with our expectation, as the increased transmission distance will lead to more channel losses, resulting in extremely lower SNR of the received DMCSs. In addition, we find that $\bar{\mathcal{P}}_{\mathrm{Prec}}$ fluctuates as the hyper-parameter k varies, and this situation exists in all distances. To select a proper k, we mark the peak value of each line out with a circle. It is observed that these peak values occur when k is set from 11 to 17, e.g. $\bar{\mathcal{P}}_{\mathrm{Prec}} = 0.9541$ at transmission distance of 5 km when $k = 15$, which suggests that the value of k should not be set too small or too large. This is because a small value of k may lead to overfitting problem and a large value of k may result in underfitting problem, while $\bar{\mathcal{P}}_{\mathrm{Prec}}$ will be decreased by either of the two problems [44].

For now, we have investigated the performance of QkNN in terms of precision. To comprehensively evaluate a classifier, however, a sole metric is inadequate. Therefore, an overall metric called macro-average **Receiver Operating Characteristic** (ROC) curve [45], which describes the average **True Positive Rate** ($\mathcal{P}_{\mathrm{TPR}}$) of a certain multi-class classifier as a function of its average **False Positive Rate** ($\mathcal{P}_{\mathrm{FPR}}$), is introduced. For each class, $\mathcal{P}_{\mathrm{TPR}}$ indicates the proportion of the data that is correctly predicted as positive in all actual positive data, and $\mathcal{P}_{\mathrm{FPR}}$ indicates the proportion of the data that is incorrectly predicted as positive in all actual negative data. Their formulas are given by

$$\mathcal{P}_{\mathrm{TPR}} = \frac{\mathcal{N}_{TP}}{\mathcal{N}_{TP} + \mathcal{N}_{FN}}, \tag{25}$$

$$\mathcal{P}_{\mathrm{FPR}} = \frac{\mathcal{N}_{FP}}{\mathcal{N}_{FP} + \mathcal{N}_{TN}}. \tag{26}$$

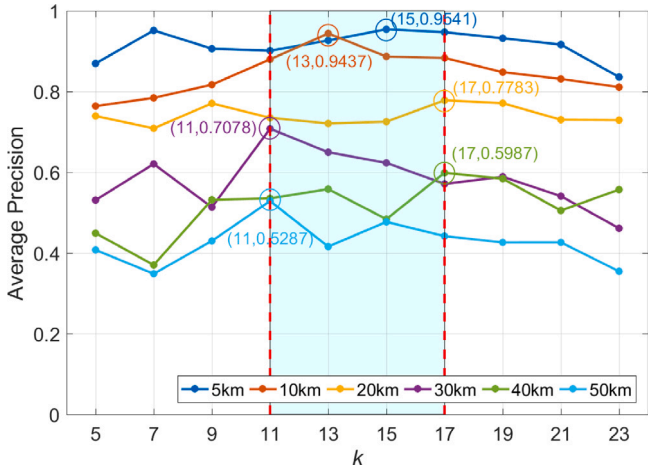

Fig. 11. The average precision $\bar{\mathcal{P}}_{\mathrm{Prec}}$ of QkNN algorithm as a function of k. From top to bottom, the broken lines represent the distance of 5 km, 10 km, 20 km, 30 km, 40 km and 50 km, respectively.

Fig. 12 shows the macro-average ROC curves of the proposed QkNN with hyper-parameter $k = 15$. The dashed line is the result of random guess, which illustrates that there is no performance improvement without using any classification algorithm. With macro-average ROC curve, one can explicitly tell the quality of the multi-class classifier: the curve closer to point $(0, 1)$, the better performance. Obviously, the proposed QkNN can dramatically improve the performance of predicting DMCSs. Moreover, it can be observed that these curves are away from the best point $(0, 1)$ as the transmission distance increases, this trend is identical with our previous analysis, which further illustrates that channel loss is important for the performance of QkNN algorithm. Besides, we further calculate the **area under curve** (AUC) [46] for each distance and thus obtain AUC value Λ_{Q}, which is a probability value range from 0 to 1. As a numerical value, Λ_{Q} can be directly used for quantitatively evaluating classifier's quality. It can be easily found that our proposed QkNN algorithm achieves extremely high overall performance ($\Lambda_{\mathrm{Q}} > 0.99$) with transmission distance is 5 km. It is worth noting that the AUC value of random guess is 0.5, while it exceeds 0.80 with the proposed QkNN even the transmission distance is increased to 50 km. This result demonstrates that the effectiveness of QkNN in CVQKD system, therefore, the AUC value Λ_{Q} can be used to describe the efficiency of quantum classifier in the following security analysis of the proposed QkNN-based CVQKD system.

It is worth mentioning that since the QkNN algorithm is the quantum version of the kNN algorithm, the core ideas of the two are identical. Therefore, the performance for both kNN and QkNN is identical if they calculate the similarity with same metric.

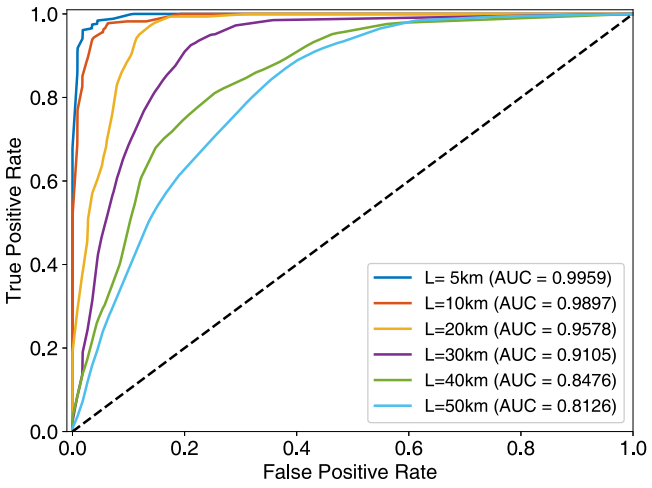

Fig. 12. The macro-average ROC curves of QkNN with hyper-parameter $k = 15$. Dashed line denotes the performance of random guess.

4.2. Complexity analysis for QkNN algorithm

Before presenting the complexity analysis of QkNN, let us briefly retrospect the complexity of classical kNN first. Assuming there are M training data points $V_j = \{\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_M}\}$ and each training data point is represented as an U dimensional feature vector $\mathbf{v_j} = (v_{j1}, v_{j2}, \ldots, v_{jU})$, the classical kNN algorithm first needs to calculate all similarities between the unlabeled data point $\mathbf{v_0}$ and each labeled data point $\mathbf{v_j}$, so that the complexity of this step is $O(UM)$. Then, the M similarities need to be sorted with a certain sorting algorithm such as quick sort, merge sort, heap sort, etc. In general, the complexity of above sorting algorithms is no less than $O(M \log_2 M)$ [47]. Finally, the majority voting requires $O(k)$ times to count the number of labels and assigns the label to $\mathbf{v_0}$. As a result, the total complexity of classical kNN can be expressed by

$$O(UM + M \log_2 M + k). \tag{27}$$

In what follows, let us discuss the complexity of the proposed QkNN algorithm in detail. As shown in Fig. 5, the whole QkNN is composed of four parts, i.e., preparation of quantum states, similarity calculating, quantum k-maximal finding and majority voting. For preparation of quantum states, as detailed in Section 3.1, both quantum states $|\tau\rangle$ and $|\rho\rangle$ are prepared by 3 Oracles (i.e. $\mathcal{O}$, R_y and $\mathcal{O}^\dagger$), so that the complexity of this part is $O(6)$. For similarity calculating, the two quantum states $|\tau\rangle$ and $|\rho\rangle$ are first passed through the c-SWAP test quantum circuit to obtain the quantum state $|\gamma_j\rangle$ that contains the similarity $P_j(0)$. Note that the complexity of calculating a $P_j(0)$ is $O(\log_2^2 U)$ [48]. To obtain the superposition state $|\gamma\rangle$ whose amplitudes contain all similarities, the c-SWAP test needs to be performed M times, the complexity is thereby increased to $O(M \log_2^2 U)$. Subsequently, the similarities need to be stored as a qubit string by amplitude estimation. Specifically, the Q operator is repeatedly performed to estimate the amplitude a (see details in Appendix C), and the error probability for estimating a satisfies [42]

$$|a - \widetilde{a}| \leqslant \frac{\pi}{R} + \frac{\pi^2}{R^2}, \tag{28}$$

where $\widetilde{a}$ is the estimation of a, and R is the iteration times of operator Q. Obviously, R needs to satisfy the following inequation, i.e.

$$R \geqslant \frac{\pi(\pi + 1)}{\delta}, \tag{29}$$

if the error probability $|a - \widetilde{a}| \leqslant \delta$. That is to say, the Q operator needs to be performed at least R times ($O(R)$) to ensure that the error probability is less than or equal to δ. Therefore, the total complexity of similarity calculating is $O(M \log_2^2 U + R)$. For quantum k-maximal finding, let $\mathcal{T}$ be a set whose elements do not belong to set K but are more similar to $\mathbf{v_0}$ than some points in set K, and the number of elements of set $\mathcal{T}$ is t. Obviously, to find out k maximal values, the Grover's algorithm and replacement need to be repeatedly performed until set $\mathcal{T}$ is empty, i.e., $t = 0$. Ref. [49] shows that t can be reduced to $\frac{t}{2}$ by performing $O(k)$ iterations of Grover's algorithm and replacement when $t > 2k$, i.e., the Oracle needs to perform $O(k\sqrt{\frac{M}{t}})$ times. Once t is reduced to $t \leq 2k$, $O(\sqrt{\frac{M}{t}})$ times Oracles in each round of Grover's algorithm are required to ensure $t = 0$. Therefore,

$$\begin{cases} k(\sqrt{\frac{M}{2k}} + \sqrt{\frac{M}{4k}} + \sqrt{\frac{M}{8k}} + \cdots), t > 2k \\ \sum_{i=1}^{2k} \sqrt{\frac{M}{i}}, t \leq 2k \end{cases} \tag{30}$$

times Oracles are required for reducing t to 0. From Eq. (30), we can easily find that the complexity of quantum k-maximal finding is $O(\sqrt{kM})$. Till now, we have presented the complexity analysis of the former three parts, note that the last part of QkNN, namely the majority voting, is similar to that of classical kNN, so that its complexity remains $O(k)$. Therefore, the total complexity of our proposed QkNN is

$$O(M \log_2^2 U + R + \sqrt{kM} + k). \tag{31}$$

Fig. 13 shows complexity comparisons between the proposed QkNN and classical kNN. As can be seen in Fig. 13(a), the total complexity of the proposed QkNN is much less than that of classical kNN, it illustrates that the proposed QkNN algorithm could offer a significant speedup over classical kNN algorithm. To figure out how the acceleration happens, we further mark each part with different colors and the result shows that the complexities of similarity calculating and k-maximal finding (corresponding to sorting in classical kNN algorithm) are dramatically decreased by the proposed QkNN. It illustrates that the quantum parts of QkNN are crucial for speedup. In addition, we find that the complexities for both QkNN and classical kNN algorithms are affected by several parameters, i.e., the dimension U, the number of training data M and the number of nearest neighbors k. We therefore plot Fig. 13(b), (c) and (d) to investigate the respective influence of each parameter on complexity. As shown in Fig. 13(b) and (c), the complexity of classical kNN rises quite sharply with the increase of U or M, while the complexity of QkNN rises very slowly. It illustrates that the proposed QkNN algorithm is of clear superiority in addressing high dimensional or large-size classification issues. Fig. 13(d) shows that although the complexity of classical kNN is apparently larger than that of QkNN, the complexities of both algorithms are not sensitive to the hyper-parameter k, which illustrates that k is not a crucial parameter that heavily affects the complexities of both classical kNN and QkNN algorithms. It is worthy noting that, to explicitly show the respective trends, the scale of labeled data point M is set to 128 in Fig. 13(a), (b) and (d). Actually, M is usually far more than 10^5 for a realistic CVQKD system [40]. In such a practical scenario, the complexity gap between QkNN and classical kNN will be extremely large.

4.3. Security analysis of QkNN-based CVQKD

Till now, we have demonstrated the performance of QkNN-based CVQKD in terms of machine learning metrics and have analyzed the complexity of QkNN algorithm, both results have shown the advantages of our scheme. In what follows, we present the theoretical security proof for QkNN-based CVQKD with SDP method [50], detailed calculations can be found in Appendix E. As known, the asymptotic secret key rate of the conventional DM CVQKD with reverse reconciliation is given by [51]

$$K_{\text{asym}} = \beta I_{\text{AB}} - \chi_{\text{BE}}, \tag{32}$$

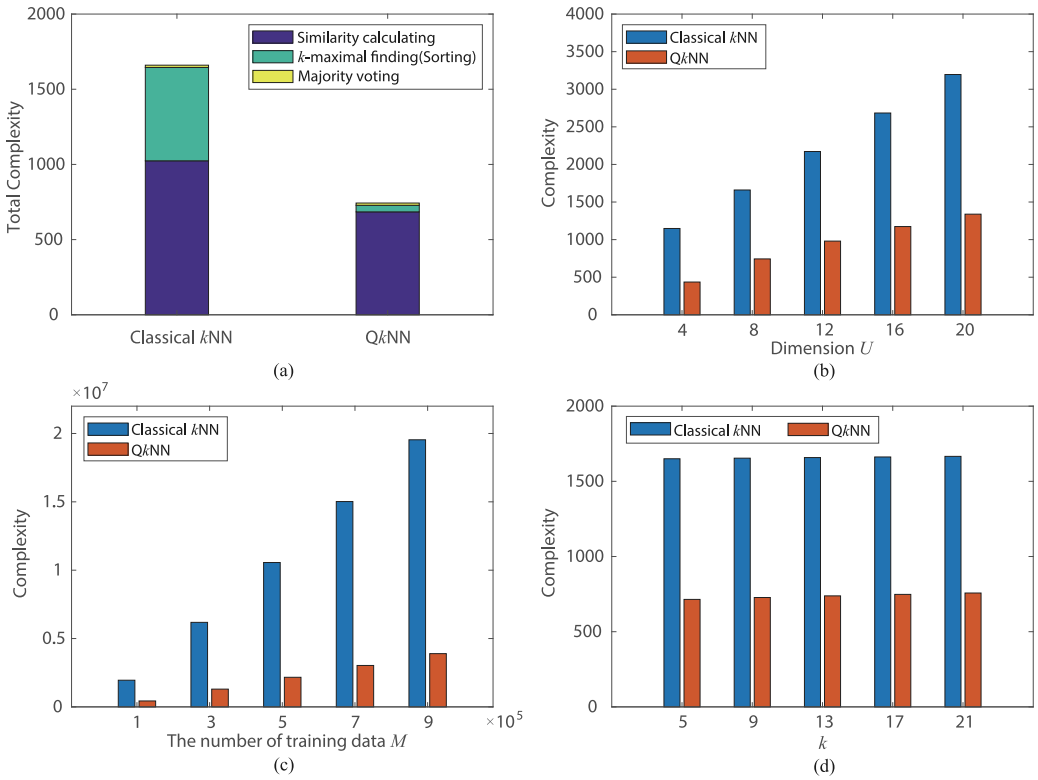

Fig. 13. Complexity comparisons. (a) Comparison of total complexity. Parameters are set to be as follows. $U = 8$, $R = 131$ ($\delta = 0.1$), $M = 128$ and $k = 15$; (b) Complexity comparison as a function of dimension U; (c) Complexity comparison as a function of M; (d) Complexity comparison as a function of hyper-parameter k. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

where β is the reconciliation efficiency, I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} is the Holevo bound of the mutual information between Eve and Bob. However, Eq. (32) does not consider the influence of the introduction of QkNN classifier for both legitimate users (Alice and Bob) and the eavesdropper (Eve), therefore, it has to be amended to suitable for evaluating quantum machine learning-based CVQKD. Due to the data processing is quite different, Eq. (32) can be rewritten as the following form

$$K_{\mathrm{asym}}^{\mathrm{Q}} = \beta \Lambda_{\mathrm{Q}} I_{\mathrm{AB}} - p(y_i)\chi_{\mathrm{BE}}, \tag{33}$$

where $p(y_i) = 1/N$ is the probability of discrete uniform distribution when variable $Y = y_i (i = 1, 2, \ldots, N)$.

The difference between Eqs. (32) and (33) lies in two parts. First, the AUC value Λ_{Q} has to be considered as it describes the efficiency of quantum classifier. Higher AUC value implies higher correlation of raw keys between Alice and Bob. Second, term χ_{BE}, which represents the Holevo quantity for Eve's maximum accessible information, is reduced to $p(y_i)\chi_{\mathrm{BE}}$. This is because Eve is no longer able to acquire as much information as before, due to some relationships being no longer fixed and public. To be specific, in conventional DM CVQKD, the relationship between each DMCS and its binary presentation is fixed and public. For instance, the key bits of state $|\alpha_0\rangle$ in QPSK CVQKD is always (0, 0) (see Figure 1 in Ref. [52]), so that Eve can precisely recover the correct key bits (0, 0) when she successfully intercepts the coherent state $|\alpha_0\rangle$. Similarly for 8PSK CVQKD, Eve can precisely recover the correct key bits (0, 0, 0) when she successfully intercepts the coherent state $|\alpha_0\rangle$. However, due to the special-designed process of QkNN-based CVQKD, the above relationship is no longer fixed and public. Although each DMCS is assigned to a fixed label, such as the label of $|\alpha_0\rangle$ is L_1 and the label of $|\alpha_7\rangle$ is L_8 shown in Fig. 3, the binary presentation for each label can be randomly assigned by Alice. That is to say, label L_1 can represent any binary bits from (0,0,0) to (1,1,1), as well as other labels. Since the initialization part is secure, Bob will learn the assignment by the transmitted DMCSs at the end of initialization. While Eve who does not participate in the initialization part is completely unaware of the assignment shared by Alice and Bob. She thus can only guess the correct label with a success probability of $1/N$ for N-PSK modulation. As can be seen in Fig. 14, in our proposed scheme, Eve's maximum accessible information is apparently reduced when compared with conventional DM CVQKD, and it can be further decreased by using higher dimensional PSK modulation. This is opposite to the trend in conventional DM CVQKD in which Eve's maximum accessible information will increase with higher dimensional PSK modulation. This is because the number of classes of DMCSs increases as the modulation dimension increases, so that the binary representations that can be selected by the label of

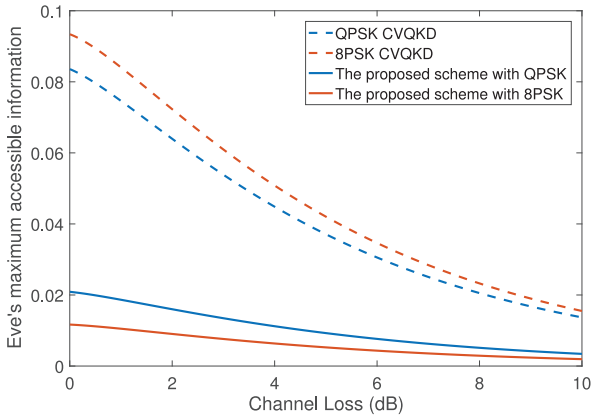

Fig. 14. Eve's maximum accessible information as a function of channel loss (0.2 dB/km). Solid lines denote the proposed scheme with different QPSK and 8PSK, respectively. Dashed lines denote the conventional DM CVQKD with QPSK and 8PSK, respectively. Modulation variance V_m are set to 0.33 for QPSK and 0.38 for 8PSK.

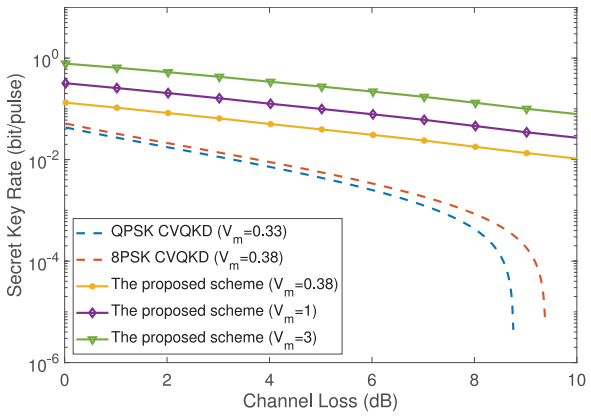

Fig. 15. Asymptotic secret key rate as a function of channel loss (0.2 dB/km). Solid lines denote the proposed QkNN-based CVQKD with different modulation variances, blue dashed line denotes QPSK CVQKD, and red dashed line denotes 8PSK CVQKD. The parameters are set to be as follows. Detector efficiency $\eta = 0.6$, electronic noise $\upsilon_{el} = 0.05$, excess noise $\varepsilon = 0.01$, reconciliation efficiency $\beta = 0.98$ and $k = 15$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

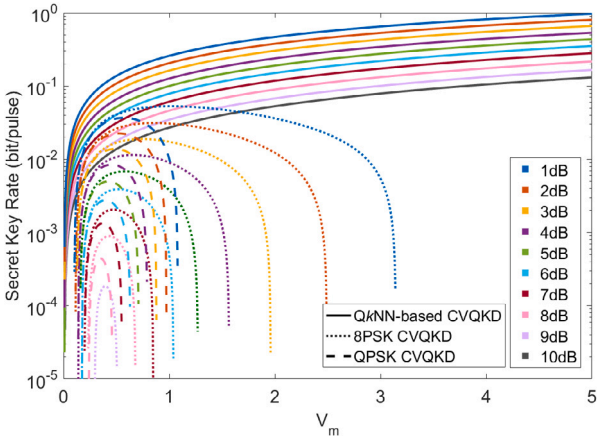

Fig. 16. Asymptotic secret key rate as a function of modulation variance V_m. Solid lines denote the QkNN-based CVQKD, dotted lines denote 8PSK CVQKD, and dashed lines denote QPSK CVQKD. Different channel losses are marked with different colors. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

DMCS increase. Therefore, the probability that Eve can correctly guess the binary bits of the intercepted coherent state is smaller, so that her maximum accessible information is getting less. It illustrates that the proposed scheme can efficiently prevent eavesdropper from obtaining more useful information, thereby contributing to the increase of final secret key rate.

Fig. 15 shows the performance comparison between QkNN-based CVQKD and two conventional DM CVQKD protocols in asymptotic limit. The results demonstrate that the secret key rate of QkNN-based CVQKD outperforms other DM CVQKD protocols at all channel losses. In addition, we find that the secret key rate of the proposed scheme can be further increased with the risen modulation variance V_m. This is inconsistent with conventional DM CVQKD whose security has to be guaranteed by small modulation variance [52,53]. To investigate what caused this inconsistency, we plot Fig. 16, which shows the asymptotic secret key rates of above-mentioned schemes as a function of modulation variance. It can be easily found that the curves of both QPSK CVQKD and 8PSK CVQKD are arched and located in certain ranges of small modulation variance, and the ranges are getting narrower as channel loss increases. Meanwhile, curves of QkNN-based CVQKD keep rising with the increase of modulation variance, which illustrates that small modulation variance is no longer needed for guaranteeing the security, so that the secret key rate of our proposed scheme can be further increased by setting proper larger modulation variance.

5. Conclusion

In this work, we have proposed a high-rate continuous-variable quantum key distribution scheme based on quantum machine learning, called QkNN-based CVQKD. The proposed scheme divides the whole process of conventional DM CVQKD protocol into three parts, i.e., initialization, prediction and data postprocessing. The initialization part is used for training and estimating quantum classifier, the prediction part is used for generating highly correlated raw keys, and the data postprocessing part generates the final secret key string shared by Alice and Bob. To this end, a specialized QkNN algorithm was elegantly designed as a quantum classifier for distinguishing the incoming DMCSs. We then introduced several related machine learning-based metrics to estimate the performance of QkNN, and compared its complexity with classical kNN algorithm. The asymptotic security proof of QkNN-based CVQKD was finally presented with SDP method.

We have comprehensively analyzed the performance of QkNN-based CVQKD, the results indicate that our proposed scheme is suitable for the high-speed metropolitan secure communication due to its advantages of high-rate and low-complexity. Besides, it is worthy noticing that the quantum classifier is not limited to the proposed QkNN, any other well-behaved quantum classifier can be used for improving CVQKD with the proposed processing framework.

In summary, QkNN-based CVQKD is not only an improvement of CVQKD protocol, but also provides a novel thought for introducing various (quantum) machine learning-based methodologies (e.g., quantum neural network [54]) to CVQKD field. In future studies, the experimental implementation of the proposed scheme will be investigated within the quantum Internet [55,56].

CRediT authorship contribution statement

Qin Liao: Writing – review & editing, Writing – original draft, Supervision, Resources, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Zhuoying Fei:** Writing – review & editing, Writing – original draft, Visualization, Formal analysis. **Jieyu Liu:** Writing – review & editing, Writing – original draft, Validation, Methodology. **Anqi Huang:** Writing – review & editing. **Lei Huang:** Writing – review & editing, Visualization, Validation. **Yijun Wang:** Writing – review & editing, Supervision, Project administration.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Qin Liao reports financial support was provided by National Natural Science Foundation of China. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We would like to thank the anonymous referees for their constructive suggestions. This work was supported by the National Natural Science Foundation of China (Grant No. 62101180), the Hunan Provincial Natural Science Foundation of China (Grant No. 2022JJ30163), and the Open Research Fund Program of the State Key Laboratory of High Performance Computing, National University of Defense Technology (Grant No. 202101-25).

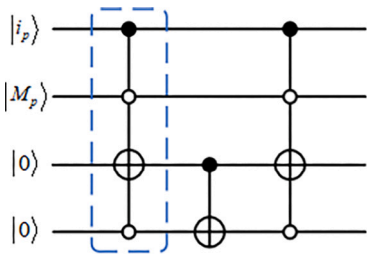

Fig. A.17. The quantum circuit to implement CMP. i_p $(p = 0, 1, \ldots, m-1)$ and M_p $(p = 0, 1, \ldots, m-1)$ are the single binary bit of $(i)_{10} = (i_{m-1} i_{m-2} \ldots i_1 i_0)_2$ and $(M)_{10} = (M_{m-1} M_{m-2} \ldots M_1 M_0)_2$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Appendix A. Derivation of the initial state

To clearly describe the preparation of initial state, the quantum circuit shown in Fig. 6 is divided into four phases P1-P4. Thereinto, H is Hadamard gate which is defined by

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}, \tag{A.1}$$

we therefore have $H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. CMP is a unitary operation which obeys

$$\mathrm{CMP}|i\rangle|M\rangle|0\rangle = \begin{cases} |i\rangle|M\rangle|0\rangle & i \leqslant M \\ |i\rangle|M\rangle|1\rangle & i > M \end{cases}, \tag{A.2}$$

where $|M\rangle$ is the computational basis state that stores M as a binary string.

The CMP operation can be implemented by a quantum circuit shown in Fig. A.17, which is composed of three controlled NOT (CNOT) gates and four inverted controlled NOT (ICNOT) gates. The CNOT gate flips the controlled qubit if its control qubit is $|1\rangle$, while the ICNOT gate flips the controlled qubit if the control qubit is $|0\rangle$. By properly combining these quantum control gates, the controlled qubits can be flipped under certain conditions. For example, after passing the first combined control gate (blue dashed box shown in Fig. A.17), the third qubit will be flipped when the other three control qubits are $|100\rangle$. To implement CMP operation, the quantum circuit of Fig. A.17 needs to perform m times, where $m = \lceil \log_2(M+1) \rceil$.

In what follows, we present the derivation of preparing the quantum state $\frac{1}{\sqrt{M}} \sum_{j=1}^{M} |j\rangle$. Assuming there are n $(0 \leq n < 2^{m-1})$ qubits' binary value larger than M, we have $M = 2^m - n - 1$. The states of qubits in different phases (P1-P4) and registers (R1-R4) are presented in Table A.3. Let us start the derivation with the input quantum state $|0^{\otimes m} M 00\rangle$. At first, a $H^{\otimes m}$ gate is applied to R1, the input quantum state is therefore transformed to

$$\frac{1}{\sqrt{2^m}}(|0M00\rangle + |1M00\rangle + \cdots + |(2^m-1)M00\rangle). \tag{A.3}$$

Then, an ICNOT gate is applied to R1 and R4, so that the resultant state can be expressed by

$$\frac{1}{\sqrt{2^m}}(|0M01\rangle + |1M00\rangle + |2M00\rangle + \cdots + |(2^m-1)M00\rangle). \tag{A.4}$$

After that, the CMP operation is applied to R1, R2 and R3, the quantum state is finally transformed to

$$\frac{1}{\sqrt{2^m}}(|0M01\rangle + |1M00\rangle + |2M00\rangle + \cdots + |MM00\rangle + |(M+1)M10\rangle + \cdots + |(2^m-1)M10\rangle). \tag{A.5}$$

From Eq. (A.5), it is easy to find that the probability of measurement outcome of (0,0) is $\frac{2^m-n-1}{2^m} = \frac{M}{2^m}$. Therefore, the quantum state

$$\frac{1}{\sqrt{M}}(|1\rangle + |2\rangle + \cdots + |M\rangle) = \frac{1}{\sqrt{M}} \sum_{j=1}^{M} |j\rangle \tag{A.6}$$

can be obtained with the probability $\frac{M}{2^m}$ from R1.

Similarly, we can prepare the quantum state $\frac{1}{\sqrt{U}} \sum_{i=1}^{U} |i\rangle$ by replacing the input qubit $|M\rangle$ with $|U\rangle$. Then, the initial state

$$|\tau_{init}\rangle = \frac{1}{\sqrt{M}} \sum_{j=1}^{M} |j\rangle \frac{1}{\sqrt{U}} \sum_{i=1}^{U} |i\rangle|0\rangle|0\rangle \tag{A.7}$$

can be prepared.

Appendix B. Derivation of the probability of measuring the top qubit of c-SWAP test

As shown in Fig. 7, the top qubit $|0\rangle$ is firstly transformed to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ by a Hadamard gate. After passing the SWAP gate, the whole quantum system turns to $\frac{1}{\sqrt{2}}(|0\rangle|\rho\rangle|\tau_j\rangle + |1\rangle|\tau_j\rangle|\rho\rangle)$. The top qubit is subsequently operated by another Hadamard gate, resulting in the final quantum state

$$|\gamma_j\rangle = \frac{1}{2}|0\rangle(|\rho\rangle|\tau_j\rangle + |\tau_j\rangle|\rho\rangle) + \frac{1}{2}|1\rangle(|\rho\rangle|\tau_j\rangle - |\tau_j\rangle|\rho\rangle). \tag{B.1}$$

If we measure the top qubit of quantum state $|\gamma_j\rangle$, the probability of outcome of 0 is $P_j(0) = (1 + |\langle\rho|\tau_j\rangle|^2)/2$. The detailed derivation is as follows.

Let $\{M_i\} = \{M_0, M_1\}$ be measurement operator set, where

$$\begin{aligned} M_0 &= |0\rangle\langle 0| \quad M_0^\dagger M_0 = M_0, \\ M_1 &= |1\rangle\langle 1| \quad M_1^\dagger M_1 = M_1, \end{aligned} \tag{B.2}$$

and $\{M_i\}$ obeys

$$\begin{aligned} \sum_i M_i^\dagger M_i &= M_0^\dagger M_0 + M_1^\dagger M_1 \\ &= M_0 + M_1 = I, \end{aligned} \tag{B.3}$$

where I is identity matrix. $P_j(0)$ can be derived by

$$\begin{aligned} P_j(0) &= \langle\gamma_j|M_0^\dagger M_0|\gamma_j\rangle \\ &= \langle\gamma_j|M_0|\gamma_j\rangle \\ &= \langle\gamma_j||0\rangle\langle 0||\gamma_j\rangle \\ &= \left[\frac{1}{2}(\langle\tau_j|\langle\rho| + \langle\rho|\langle\tau_j|)\langle 0| + \frac{1}{2}(\langle\tau_j|\langle\rho| - \langle\rho|\langle\tau_j|)\langle 1|\right| \\ &\quad |0\rangle\langle 0|\left[\frac{1}{2}|0\rangle(|\rho\rangle|\tau_j\rangle + |\tau_j\rangle|\rho\rangle) + \frac{1}{2}|1\rangle(|\rho\rangle|\tau_j\rangle - |\tau_j\rangle|\rho\rangle)\right] \\ &= \left[\frac{1}{2}(\langle\tau_j|\langle\rho| + \langle\rho|\langle\tau_j|)\langle 0|\right]|0\rangle\langle 0|\left[\frac{1}{2}|0\rangle(|\rho\rangle|\tau_j\rangle + |\tau_j\rangle|\rho\rangle)\right] \\ &= \left[\frac{1}{2}(\langle\tau_j|\langle\rho| + \langle\rho|\langle\tau_j|)\right]\langle 0|0\rangle\langle 0|0\rangle|\left[\frac{1}{2}(|\rho\rangle|\tau_j\rangle + |\tau_j\rangle|\rho\rangle)\right] \\ &= \left[\frac{1}{2}(\langle\tau_j|\langle\rho| + \langle\rho|\langle\tau_j|)\right]\left[\frac{1}{2}(|\rho\rangle|\tau_j\rangle + |\tau_j\rangle|\rho\rangle)\right] \\ &= \frac{1}{4}(\langle\tau_j|\langle\rho||\rho\rangle|\tau_j\rangle + \langle\rho|\langle\tau_j||\rho\rangle|\tau_j\rangle + \langle\tau_j|\langle\rho||\tau_j\rangle|\rho\rangle + \\ &\quad \langle\rho|\langle\tau_j||\tau_j\rangle|\rho\rangle) \\ &= \frac{1}{4}(2 + 2|\langle\rho|\tau_j\rangle|^2) \\ &= \frac{1}{2}(1 + |\langle\rho|\tau_j\rangle|^2), \end{aligned} \tag{B.4}$$

where $\langle\rho|\rho\rangle = 1$ and $\langle\tau_j|\tau_j\rangle = 1$.

Appendix C. Derivation for obtaining quantum state $|\sigma\rangle$ by amplitude estimation

After M times c-SWAP test, Bob now holds a superposition state $|\gamma\rangle$ (Eq. (12) in the main text) whose amplitudes contain all similarities between all known DMCSs and the unknown DMCS. The aim of amplitude

Table A.3
The states of qubits passing quantum circuit shown in Fig. 6.

	P1	P2	P3	P4
R1	$\|0^{\otimes m}\rangle$	$\frac{1}{\sqrt{2^m}}(\|0\rangle+\|1\rangle)^{\otimes m}$ $=\frac{1}{\sqrt{2^m}}(\|0\rangle+\|1\rangle+...+\|2^m-1\rangle)$	$\frac{1}{\sqrt{2^m}}(\|0\rangle+\|1\rangle+...+\|2^m-1\rangle)$	$\frac{1}{\sqrt{2^m}}(\|0\rangle+\|1\rangle+...+\|2^m-1\rangle)$
R2	$\|M\rangle$	$\|M\rangle$	$\|M\rangle$	$\|M\rangle$
R3	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\frac{1}{\sqrt{2^m}}(\underbrace{\|0\rangle+...+\|0\rangle}_{2^m-n}+\underbrace{\|1\rangle+...+\|1\rangle}_{n})$
R4	$\|0\rangle$	$\|0\rangle$	$\frac{1}{\sqrt{2^m}}(\|1\rangle+\underbrace{\|0\rangle+...+\|0\rangle}_{2^m-1})$	$\frac{1}{\sqrt{2^m}}(\|1\rangle+\underbrace{\|0\rangle+...+\|0\rangle}_{2^m-1})$

estimation is to store these similarities from amplitudes to a quantum bit string, which is convenient for the processing of follow-up quantum search algorithm.

In fact, the superposition state $|\gamma\rangle$ can be decomposed as $|\gamma\rangle = |\gamma_g\rangle + |\gamma_b\rangle$, where $|\gamma_g\rangle = \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\sqrt{P_j(0)}|0\rangle$ denotes good state that we needed and $|\gamma_b\rangle = \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\sqrt{1-P_j(0)}|1\rangle$ denotes bad state that we do not need. Let $a = \langle\gamma_g|\gamma_g\rangle = \frac{1}{M}\sum_{j=1}^{M}P_j(0)$ denotes the probability that measuring $|\gamma\rangle$ produces a good state, amplitude amplification is first performed to the state $|\gamma\rangle$ by repeatedly applying the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^\dagger S_\chi$, where $\mathcal{A}S_0\mathcal{A}^\dagger = I - 2|\gamma\rangle\langle\gamma|$ and $-S_\chi = I - \frac{2}{1-a}|\gamma_b\rangle\langle\gamma_b|$ [42]. We therefore can derive that

$$\begin{aligned} Q|\gamma_g\rangle &= (1-2a)|\gamma_g\rangle - 2a|\gamma_b\rangle, \\ Q|\gamma_b\rangle &= 2(1-a)|\gamma_g\rangle + (1-2a)|\gamma_b\rangle. \end{aligned} \tag{C.1}$$

From Eqs. (C.1), the Q operator can be further expressed as a matrix form

$$Q = \begin{bmatrix} 1-2a & -2\sqrt{a(1-a)} \\ 2\sqrt{a(1-a)} & 1-2a \end{bmatrix}. \tag{C.2}$$

Assuming $\sin^2\theta_a = a = \langle\gamma_g|\gamma_g\rangle$, the matrix Q can be rewritten as

$$Q = \begin{bmatrix} \cos(2\theta_a) & -\sin(2\theta_a) \\ \sin(2\theta_a) & \cos(2\theta_a) \end{bmatrix}, \tag{C.3}$$

so we have

$$\begin{aligned} Q &= \cos(2\theta_a)I - \imath\sin(2\theta_a)Y \\ &= exp(-2\imath\theta_a Y), \end{aligned} \tag{C.4}$$

where $\imath = \sqrt{-1}$ and Y is Pauli Y operator that defined as

$$Y = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}. \tag{C.5}$$

Therefore, we can derive that the eigenvalues of Q are $exp(\pm\imath 2\theta_a)$ and the eigenstates of Q are

$$\begin{aligned} |\Phi_+\rangle &= \frac{1}{\sqrt{2}}\left(\frac{|\gamma_b\rangle}{\sqrt{1-a}} + \imath\frac{|\gamma_g\rangle}{\sqrt{a}}\right), \\ |\Phi_-\rangle &= \frac{1}{\sqrt{2}}\left(\frac{|\gamma_b\rangle}{\sqrt{1-a}} - \imath\frac{|\gamma_g\rangle}{\sqrt{a}}\right), \end{aligned} \tag{C.6}$$

so that the quantum state $|\gamma\rangle$ can be expanded on the eigenstates basis of Q as

$$\begin{aligned} |\gamma\rangle &= |\gamma_b\rangle + |\gamma_g\rangle \\ &= \sqrt{1-a}\frac{1}{\sqrt{2}}(|\Phi_+\rangle + |\Phi_-\rangle) + \imath\sqrt{a}\frac{1}{\sqrt{2}}(|\Phi_+\rangle - |\Phi_-\rangle) \\ &= \frac{1}{\sqrt{2}}(exp(\imath\theta_a)|\Phi_+\rangle + exp(-\imath\theta_a)|\Phi_-\rangle). \end{aligned} \tag{C.7}$$

As shown in Fig. 8, the Hadamard gates are first applied to m $|0\rangle$ qubits, so that a quantum state $\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|j\rangle$ can be produced. Then the operator Q^j is controlled by this state to apply j times of operator Q to quantum state $|\gamma\rangle$, the resultant state is transformed to

$$\begin{aligned} &\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|j\rangle Q^j|\gamma\rangle \\ &= \frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|j\rangle\left[\frac{1}{\sqrt{2}}exp(\imath(2j+1)\theta_a)|\Phi_+\rangle + \frac{1}{\sqrt{2}}exp(-\imath(2j+1)\theta_a)|\Phi_-\rangle\right] \\ &= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}exp(\imath 2\theta_a j)|j\rangle\right]exp(\imath\theta_a)|\Phi_+\rangle + \\ &\quad \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}exp(-\imath 2\theta_a j)|j\rangle\right]exp(-\imath\theta_a)|\Phi_-\rangle. \end{aligned} \tag{C.8}$$

After amplitude amplification, phase estimation is subsequently used for estimating the phase information θ_a of the resultant state. Thus, after applying IQFT $\mathcal{F}_M^{-1}$ on register R1, the quantum state is transformed to

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left|M\frac{\widetilde{\theta}_a}{\pi}\right\rangle exp(\imath\theta_a)|\Phi_+\rangle + \frac{1}{\sqrt{2}}\left|M(1-\frac{\widetilde{\theta}_a}{\pi})\right\rangle exp(-\imath\theta_a)|\Phi_-\rangle, \tag{C.9}$$

where $\widetilde{\theta}_a$ is the estimate of θ_a. Let us define $\sigma_1 = M\frac{\widetilde{\theta}_a}{\pi}$ and $\sigma_2 = M(1-\frac{\widetilde{\theta}_a}{\pi})$, so that $\sin^2(\widetilde{\theta}_a) = \sin^2(\pi\frac{\sigma_1}{M})$ and $\sin^2(\widetilde{\theta}_a) = \sin^2(\pi - \pi\frac{\sigma_2}{M}) = \sin^2(\pi\frac{\sigma_2}{M})$. Thus, $\sin^2(\pi\frac{\sigma_1}{M}) = \sin^2(\pi\frac{\sigma_2}{M})$, so we have $\sigma_1 = \sigma_2 = \sigma$. Therefore, the state $|\Phi\rangle$ can be rewritten as

$$|\Phi\rangle = \frac{1}{\sqrt{2}}|\sigma\rangle exp(\imath\theta_a)|\Phi_+\rangle + \frac{1}{\sqrt{2}}|\sigma\rangle exp(-\imath\theta_a)|\Phi_-\rangle, \tag{C.10}$$

where

$$\begin{aligned} |\sigma\rangle &= \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\left|\frac{M}{\pi}\arcsin(\sqrt{\widetilde{P_j}(0)})\right\rangle \\ &= \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle\left|\mathrm{Sim}_j\right\rangle. \end{aligned} \tag{C.11}$$

As a result, the similarities between all known DMCSs and the unknown DMCS are stored as a qubit string after amplitude estimation. Note that the quantum state $|\sigma\rangle$ can always be obtained from R1.

Appendix D. Grover iteration of grover's algorithm

As we mentioned in the main text, the Grover's algorithm includes a number of Grover iterations and a final measurement. The Grover iteration is defined as

$$G_F = DS_F = W'S_0W'^{\dagger}S_F, \tag{D.1}$$

where $W'|0\rangle = \frac{1}{\sqrt{M}}\sum_{j=1}^{M}|j\rangle$ and $S_0 = 2|0^m\rangle\langle 0^m| - I_m$ [57]. Assuming there are t different values of j satisfying $F(j) = 1$, the initialized quantum state can be expressed as

$$|\Psi_0\rangle = |\Psi(q_0, s_0)\rangle = \sum_{F(j)=1}q_0|j\rangle + \sum_{F(j)\neq 1}s_0|j\rangle, \tag{D.2}$$

where $tq^2+(M-t)s^2=1$ and $q_0=s_0=\frac{1}{\sqrt{M}}$. After applying the Grover operator G_F to the $|\Psi(q_0,s_0)\rangle$, it is transformed to

$$\begin{aligned}|\Psi_1\rangle &= |\Psi(q_1,s_1)\rangle \\ &= |\Psi(\frac{M-2t}{M}q_0+\frac{2(M-t)}{M}s_0, \frac{M-2t}{M}s_0-\frac{2t}{M}q_0)\rangle.\end{aligned} \tag{D.3}$$

Extending to the general situation, the quantum state $|\Psi_l\rangle=|\Psi(q_l,s_l)\rangle$ can be obtained after l iterations, where

$$\begin{aligned}q_l &= \frac{M-2t}{M}q_{l-1}+\frac{2(M-t)}{M}s_{l-1}, \\ s_l &= \frac{M-2t}{M}s_{l-1}-\frac{2t}{M}q_{l-1}.\end{aligned} \tag{D.4}$$

Let $\sin^2\theta=t/M$ where $\theta\in(0,\pi/2]$, we have

$$\begin{aligned}q_l &= \frac{1}{\sqrt{t}}\sin[(2l+1)\theta], \\ s_l &= \frac{1}{\sqrt{M-t}}\cos[(2l+1)\theta],\end{aligned} \tag{D.5}$$

which can be verified by mathematical induction.

The task of the Grover iterations is to continuously amplify the amplitude q, so that the probability of obtaining $\sum_{F(j)=1}|j\rangle$ is infinitely close to 1, i.e., we have the following equation

$$\begin{aligned}t*q_l^2 &= t*\frac{1}{t}\sin^2[(2l+1)\theta] \\ &= \sin^2[(2l+1)\theta] \\ &= 1.\end{aligned} \tag{D.6}$$

From Eq. (D.6), we can derive that

$$\begin{aligned}&\sin[(2l+1)\theta]=1, \\ \Rightarrow\ &(2l+1)\theta=\frac{\pi}{2}, \\ \Rightarrow\ &l=\frac{\pi-2\theta}{4\theta}.\end{aligned} \tag{D.7}$$

Since l can only be an integer, thus we have $l=\lfloor\frac{\pi}{4\theta}\rfloor$. In addition, we have $\theta\approx\sin\theta=\sqrt{\frac{t}{M}}$ when M is large enough. Therefore, it needs $\frac{\pi}{4}\sqrt{\frac{M}{t}}$ Grover iterations to find the target index j'.

Appendix E. Calculation of secret key rate for DM CVQKD protocol

In this section, we present the calculation of secret key rate for DM CVQKD protocol with SDP method [50]. As presented in Section 4.3, the asymptotic secret key rate of CVQKD protocol with reverse reconciliation and heterodyne detection under collective attack obeys

$$K_{\text{asym}}=\beta I_{\text{AB}}-\chi_{\text{BE}}. \tag{E.1}$$

In the heterodyne detection case, the Shannon mutual information between Alice and Bob I_{AB} is given by

$$I_{\text{AB}}=\log_2\frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}, \tag{E.2}$$

where $V=V_{\text{m}}+1$ is the variance of one half of a two-mode squeezed vacuum state, V_{m} is the modulation variance of Alice, $\chi_{\text{tot}}=\xi-1+2(1+v_{\text{el}})/(\eta T)$ is the total noise referred to the channel input, T is the transmission efficiency, ξ is the excess noise, η is efficiency of the detector and v_{el} is noise due to detector electronics.

The Holevo bound of mutual information between Eve and Bob χ_{BE} is given by

$$\chi_{\text{BE}}=\sum_{i=1}^{2}G(\frac{\lambda_i-1}{2})-\sum_{i=3}^{5}G(\frac{\lambda_i-1}{2}), \tag{E.3}$$

where $G(x)=(x+1)\log_2(x+1)-x\log_2 x$, and $\lambda_i(i=1,2,3,4,5)$ are symplectic eigenvalues of states' covariance matrices, which is given by

$$\lambda_{1,2}=\frac{1}{2}[A\pm\sqrt{A^2-4B}], \tag{E.4}$$

with

$$\begin{aligned}A &= V^2+T^2(V+\chi_{\text{line}})^2-2TZ^2, \\ B &= T^2(V^2+V\chi_{\text{line}}-Z^2)^2;\end{aligned} \tag{E.5}$$

and

$$\lambda_{3,4}=\frac{1}{2}[C\pm\sqrt{C^2-4D}], \tag{E.6}$$

with

$$\begin{aligned}C &= \frac{1}{(T(V+\chi_{\text{tot}}))^2}(A\chi_{\text{het}}^2+B+1 \\ &\quad+2\chi_{\text{het}}(V\sqrt{B}+T(V+\chi_{\text{line}}))+2TZ^2), \\ D &= (\frac{V+\sqrt{B}\chi_{\text{het}}}{T(V+\chi_{\text{tot}})})^2;\end{aligned} \tag{E.7}$$

and the last symplectic eigenvalue $\lambda_5=1$. In the above equations, $\chi_{\text{line}}=1/T-1+\xi$ is the channel-added noise, $\chi_{\text{het}}=[1+(1-\eta)+2v_{\text{el}}]/\eta$ is the detection-added noise, and Z is the correlation between Alice and Bob. In SDP method, Z is defined as

$$Z=2\sqrt{T}\text{tr}(\tau^{1/2}\hat{a}\tau^{-1/2}\hat{a}^\dagger)-\sqrt{2T\xi\omega}, \tag{E.8}$$

where $\hat{a}$ is the annihilation operator, $\hat{a}^\dagger$ is the creation operator, and

$$w=\sum_k p_k(\langle\alpha_k|\hat{a}_\tau^\dagger\hat{a}_\tau|\alpha_k\rangle-|\langle\alpha_k|\hat{a}_\tau|\alpha_k\rangle|^2), \tag{E.9}$$

where $\hat{a}_\tau=\tau^{1/2}\hat{a}\tau^{-1/2}$, and for an N-PSK modulation,

$$\tau=\frac{1}{N}\sum_{k=0}^{N-1}|\alpha exp(\imath k\theta)\rangle\langle\alpha exp(\imath k\theta)|, \tag{E.10}$$

with $\theta=2\pi/N$.

Data availability

Data will be made available on request.

References

[1] Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira JL, Razavi M, Shaari JS, Tomamichel M, Usenko VC, Vallone G, Villoresi P, Wallden P. Advances in quantum cryptography. Adv Opt Photon 2020;12:1012–236. http://dx.doi.org/10.1364/AOP.361502.

[2] Pan Y, Bian Y, Li Y, Xu X, Ma L, Wang H, Luo Y, Dou J, Pi Y, Yang J, et al. High-rate 16-node quantum access network based on passive optical network. 2024, arXiv preprint arXiv:2403.02585.

[3] Hajomer AA, Derkach I, Filip R, Andersen UL, Usenko VC, Gehring T. Continuous-variable quantum passive optical network. 2024, arXiv preprint arXiv:2402.16044.

[4] Chapman JC, Alshowkan M, Qi B, Peters NA. Entanglement-based quantum digital signatures over a deployed campus network. Opt Express 2024;32(5):7521–39. http://dx.doi.org/10.1364/OE.510787.

[5] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Modern Phys 2002;74:145–95. http://dx.doi.org/10.1103/RevModPhys.74.145.

[6] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett 2002;88:057902. http://dx.doi.org/10.1103/PhysRevLett.88.057902.

[7] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using Gaussian-modulated coherent states. Nature 2003;421(6920):238–41. http://dx.doi.org/10.1038/nature01289.

[8] Liao Q, Liu X, Ou B, Fu X. Continuous-variable quantum secret sharing based on multi-ring discrete modulation. IEEE Trans Commun 2023;71(10):6051–60. http://dx.doi.org/10.1109/TCOMM.2023.3299978.

[9] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Modern Phys 2009;81:1301–50. http://dx.doi.org/10.1103/RevModPhys.81.1301.

[10] Chen Z, Wang X, Yu S, Li Z, Guo H. Continuous-mode quantum key distribution with digital signal processing. NPJ Quantum Inf 2023;9:28. http://dx.doi.org/10.1038/s41534-023-00695-8.

[11] Gyongyosi L, Imre S. Multiple access multicarrier continuous-variable quantum key distribution. Chaos Solitons Fractals 2018;114:491–505. http://dx.doi.org/10.1016/j.chaos.2018.07.006.

[12] Gyongyosi L. Multicarrier continuous-variable quantum key distribution. Theoret Comput Sci 2020;816:67–95. http://dx.doi.org/10.1016/j.tcs.2019.11.026.
[13] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin SW, Grangier P. Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys Rev A 2007;76:042305. http://dx.doi.org/10.1103/PhysRevA.76.042305.
[14] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R, Grangier P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J Phys B: At Mol Opt Phys 2009;42(11):114014. http://dx.doi.org/10.1088/0953-4075/42/11/114014.
[15] Guo Y, Liao Q, Wang Y, Huang D, Huang P, Zeng G. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. Phys Rev A 2017;95:032304. http://dx.doi.org/10.1103/PhysRevA.95.032304.
[16] Li Z, Zhang Y, Wang X, Xu B, Peng X, Guo H. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. Phys Rev A 2016;93:012310. http://dx.doi.org/10.1103/PhysRevA.93.012310.
[17] Liao Q, Wang Z, Liu H, Mao Y, Fu X. Detecting practical quantum attacks for continuous-variable quantum key distribution using density-based spatial clustering of applications with noise. Phys Rev A 2022;106:022607. http://dx.doi.org/10.1103/PhysRevA.106.022607.
[18] Liu Z-P, Zhou M-G, Liu W-B, Li C-L, Gu J, Yin H-L, Chen Z-B. Automated machine learning for secure key rate in discrete-modulated continuous-variable quantum key distribution. Opt Express 2022;30(9):15024–36. http://dx.doi.org/10.1364/OE.455762.
[19] Liao Q, Guo Y, Huang D, Huang P, Zeng G. Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection. New J Phys 2018;20:023015. http://dx.doi.org/10.1088/1367-2630/aaa8c4.
[20] Becerra FE, Fan J, Baumgartner G, Goldhar J, Kosloski JT, Migdall A. Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination. Nat Photon 2013;7:147–52. http://dx.doi.org/10.1038/nphoton.2012.316.
[21] Liao Q, Xiao G, Zhong H, Guo Y. Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution. New J Phys 2020;22:083086. http://dx.doi.org/10.1088/1367-2630/abab3c.
[22] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein SL, Lloyd S, Gehring T, Jacobsen CS, Andersen UL. High-rate measurement-device-independent quantum cryptography. Nat Photon 2015;9:397–402. http://dx.doi.org/10.1038/nphoton.2015.83.
[23] Cover T, Hart P. Nearest neighbor pattern classification. IEEE Trans Inform Theory 1967;13:21–7. http://dx.doi.org/10.1109/TIT.1967.1053964.
[24] Ekert A, Jozsa R. Quantum computation and Shor's factoring algorithm. Rev Modern Phys 1996;68:733–53. http://dx.doi.org/10.1103/RevModPhys.68.733.
[25] Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing. 1996, p. 212–9.
[26] Wiebe N, Braun D, Lloyd S. Quantum algorithm for data fitting. Phys Rev Lett 2012;109:050505. http://dx.doi.org/10.1103/PhysRevLett.109.050505.
[27] Harrow AW, Hassidim A, Lloyd S. Quantum algorithm for linear systems of equations. Phys Rev Lett 2009;103:150502. http://dx.doi.org/10.1103/PhysRevLett.103.150502.
[28] Rebentrost P, Mohseni M, Lloyd S. Quantum support vector machine for big data classification. Phys Rev Lett 2014;113:130503. http://dx.doi.org/10.1103/PhysRevLett.113.130503.
[29] Aïmeur E, Brassard G, Gambs S. Quantum clustering algorithms. In: Proceedings of the 24th international conference on machine learning. 2007, p. 1–8.
[30] Aïmeur E, Brassard G, Gambs S. Quantum speed-up for unsupervised learning. Mach Learn 2013;90:261–87. http://dx.doi.org/10.1007/s10994-012-5316-5.
[31] Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys Rev Lett 2009;102:180504. http://dx.doi.org/10.1103/PhysRevLett.102.180504.
[32] Leverrier A, Grangier P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. Phys Rev A 2011;83:042312. http://dx.doi.org/10.1103/PhysRevA.83.042312.
[33] Liu W-B, Li C-L, Xie Y-M, Weng C-X, Gu J, Cao X-Y, Lu Y-S, Li B-H, Yin H-L, Chen Z-B. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. PRX Quantum 2021;2:040334. http://dx.doi.org/10.1103/PRXQuantum.2.040334.
[34] Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Phys Rev X 2019;9:041064. http://dx.doi.org/10.1103/PhysRevX.9.041064.
[35] Van Der Heijden F, Duin RP, De Ridder D, Tax DM. Classification, parameter estimation and state estimation: an engineering approach using MATLAB. John Wiley & Sons; 2005.
[36] Tan P-N, Steinbach M, Kumar V. Introduction to data mining. Pearson Education India; 2016.
[37] Stigler SM. The history of statistics: The measurement of uncertainty before 1900. Harvard University Press; 1986.
[38] Waggener B, Waggener WN, Waggener WM. Pulse code modulation techniques. Springer Science & Business Media; 1995.
[39] Ma X-C, Sun S-H, Jiang M-S, Liang L-M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. Phys Rev A 2013;87:052309. http://dx.doi.org/10.1103/PhysRevA.87.052309.
[40] Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states. Phys Rev Lett 2015;114:070501–5. http://dx.doi.org/10.1103/PhysRevLett.114.070501.
[41] Wiebe N, Kapoor A, Svore K. Quantum algorithms for nearest-neighbor methods for supervised and unsupervised learning. 2014, arXiv preprint arXiv:1401.2142.
[42] Brassard G, Hoyer P, Mosca M, Tapp A. Quantum amplitude amplification and estimation. Contemp Math 2002;305:53–74. http://dx.doi.org/10.1090/conm/305/05215.
[43] Grover LK. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett 1997;79:325–8. http://dx.doi.org/10.1103/PhysRevLett.79.325.
[44] Hastie T, Tibshirani R, Friedman JH, Friedman JH. The elements of statistical learning: data mining, inference, and prediction, vol. 2, Springer; 2001.
[45] Fawcett T. An introduction to ROC analysis. Pattern Recognit Lett 2006;27:861–74. http://dx.doi.org/10.1016/j.patrec.2005.10.010.
[46] Bradley AP. The use of the area under the ROC curve in the evaluation of machine learning algorithms. Pattern Recognit 1997;30:1145–59. http://dx.doi.org/10.1016/S0031-3203(96)00142-2.
[47] Cormen TH, Leiserson CE, Rivest RL, Stein C. Introduction to algorithms. MIT Press; 2022.
[48] Hai VT, Chuong PH, et al. New approach of KNN algorithm in quantum computing based on new design of quantum circuits. Informatica 2022;46(5):95–103. http://dx.doi.org/10.31449/inf.v46i5.3608.
[49] Durr C, Heiligman M, Høyer P, Mhalla M. Quantum query complexity of some graph problems. SIAM J Comput 2006;35:1310–28. http://dx.doi.org/10.1137/050644719.
[50] Denys A, Brown P, Leverrier A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum 2021;5:540. http://dx.doi.org/10.22331/q-2021-09-13-540.
[51] Liao Q, Xiao G, Xu C-G, Xu Y, Guo Y. Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source. Phys Rev A 2020;102(3):032604. http://dx.doi.org/10.1103/physreva.102.032604.
[52] Ghorai S, Grangier P, Diamanti E, Leverrier A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys Rev X 2019;9(2):021059. http://dx.doi.org/10.1103/physrevx.9.021059.
[53] Liao Q, Liu H, Zhu L, Guo Y. Quantum secret sharing using discretely modulated coherent states. Phys Rev A 2021;103(3):032410. http://dx.doi.org/10.1103/physreva.103.032410.
[54] Gyongyosi L, Imre S. Training optimization for gate-model quantum neural networks. Sci Rep 2019;9(1):12679. http://dx.doi.org/10.1038/s41598-019-48892-w.
[55] Gyongyosi L, Imre S. Advances in the quantum internet. Commun ACM 2022;65(8):52–63. http://dx.doi.org/10.1145/3524455.
[56] Gyongyosi L, Imre S, Nguyen HV. A survey on quantum channel capacities. IEEE Commun Surv Tutorials 2018;20(2):1149–205. http://dx.doi.org/10.1109/COMST.2017.2786748.
[57] Boyer M, Brassard G, Høyer P, Tapp A. Tight bounds on quantum searching. Fortsch Phys: Prog Phys 1998;46:493–505. http://dx.doi.org/10.1002/(SICI)1521-3978(199806)46:4/5<493::AID-PROP493>3.0.CO;2-P.