Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution

Qin Liao1,2,5, Gang Xiao1, Hai Zhong2,3 and Ying Guo2,4,5

1 College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, People’s Republic of China
2 Institute of Advanced Photoelectric Detection and Quantum System, Central South University, Changsha 410075, People’s Republic of China
3 School of Computer Science and Engineering, Central South University, Changsha 410083, People’s Republic of China
4 School of Automation, Central South University, Changsha 410083, People’s Republic of China
5 Authors to whom any correspondence should be addressed.
E-mail: llqqlq@hnu.edu.cn and yingguo@csu.edu.cn

Keywords: quantum key distribution, machine learning, quantum cryptography

Abstract
We propose a novel scheme for discretely-modulated continuous-variable quantum key distribution (CVQKD) using machine learning technologies, which called multi-label learning-based CVQKD (ML-CVQKD). In particular, the proposed scheme divides the whole quantum system into state learning process and state prediction process. The former is used for training and estimating classifier, and the latter is used for generating final secret key. Meanwhile, a multi-label classification algorithm (MLCA) is also designed as an embedded classifier for distinguishing coherent state. Feature extraction for coherent state and related machine learning-based metrics for the quantum classifier are successively suggested. Security analysis based on the linear bosonic channel assumption shows that MLCA-embedded ML-CVQKD outperforms other existing discretely-modulated CVQKD protocols, such as four-state protocol and eight-state protocol, as well as the original Gaussian-modulated CVQKD protocol, and it will be further enhanced with the increase of modulation variance.

1. Introduction
For decades, continuous-variable quantum key distribution (CVQKD) [1, 2] has been a hotspot in quantum communication and quantum cryptography. It provides an approach to allows two distant legitimate partners, Alice and Bob, to share a random secure key over insecure quantum and classical channels. One of the advantage of CVQKD protocol is that the most state-of-art telecommunication technologies can be compatible to CVQKD protocols, so that one may apply CVQKD system to the practical communication network in use. CVQKD protocols have been shown to be secure against arbitrary collective attacks, which are optimal in both the asymptotic limit [3–6] and the finite-size regime [7, 8]. Recently, CVQKD is further proved to be secure against collective attacks in composable security [9].

In general, there are two modulation approaches in CVQKD protocol, i.e., Gaussian-modulated CVQKD protocol [10, 11] and discretely-modulated CVQKD protocol [12, 13]. For the first approach, Alice usually encodes key bits in the quadratures (\(\hat{p}\) and \(\hat{q}\)) of optical field [14], while Bob can restore the secret key bits through high-speed and high-efficiency coherent detection techniques. This strategy usually has a repetition rate higher than that of single-photon detections so that Gaussian-modulated CVQKD could potentially achieve higher secret key rate. However, it seems unfortunately limited to much shorter distance due to the problem of quite low reconciliation efficiency in long-distance transmission. For the second approach, it generates several nonorthogonal coherent states and exploits the sign of the measured quadrature of each state to encode information. This modulation strategy has a discrete set of choices instead of a continuous set for the choice of \(\hat{p}\) and for the choice of \(\hat{q}\) quadratures, thereby validating most excellent error-correcting codes even at low signal-to-noise ratio (SNR). However, very small modulation variance is needed.
for discretely-modulated CVQKD to keep it safe, which largely restrains its further development [5]. For example, the optimal modulation variances in four-state protocol and eight-state protocol are approximately 0.3 [15] and 0.25 [16] under linear bosonic channel assumption.

On the other hand, most of the existing CVQKD protocols, both Gaussian-modulated protocols and discretely-modulated protocols, are based on information-theoretical techniques, and comply with the similar pattern in which raw key is firstly generated and followed by the post-processing including reconciliation, parameter estimation, error-correcting and privacy amplification [17]. Although a number of excellent CVQKD protocols have been proposed such as measurement-device-independent CVQKD protocols [18–22], plug-and-play CVQKD protocols [23, 24], unidimensional CVQKD protocols [25–27], entangled-source-in-middle CVQKD protocols [28, 29], phase-encoded and basis-encoded CVQKD protocols [30, 31] etc, one may hardly make a further breakthrough for CVQKD due to the limitation of its traditional pattern and techniques.

In recent years, multi-label learning, which is a kind of machine learning technology [32], has been widely applied and has shown its powerful impact upon diverse research fields such as artificial intelligence, image processing, data mining and so on. Multi-label learning allows each instance belongs multiple labels simultaneously, therefore it is more in line with the objective description of the real world. Meanwhile, some recent works about improving CVQKD using machine learning-based method [33–35] have shown the feasibility. In this paper, we further propose a novel scheme, called ML-CVQKD, for discretely-modulated CVQKD using multi-label learning technology. This scheme is quite different from conventional discretely-modulated CVQKD, it divides the whole quantum system into trusted state learning process and untrusted state prediction process. The former is used for training and estimating classifier, and the latter is used for generating final secret key. In the meantime, a well-behaved multi-label classification algorithm (MLCA) is designed as an embedded classifier, which is not only quite suitable for the proposed system, but also beneficial for improving CVQKD performance. Feature extraction for coherent state is also presented to better fit the input requirement of MLCA, and machine learning-based metrics for classifier are subsequently suggested. Numerical simulation based on the linear bosonic channel shows that the proposed scheme waives the necessity of small modulation variance in discretely-modulated CVQKD, so that MLCA can exploit larger and reasonable variance to more precisely predict unknown coherent state, thereby enhancing the performance of discretely-modulated CVQKD system. Moreover, the proposed scheme can be applied to the existing system without deploying any extra equipment, and it is more economic than other existing CVQKD protocols in terms of practicality.

This paper is structured as follows. In section 2, we demonstrate the proposed scheme for discretely-modulated CVQKD. In section 3, we elaborate the principle of embedded MLCA algorithm. Analysis and discussion are presented in section 4 and final conclusions are drawn in section 5.

2. Multi-label learning-based CVQKD

In this section, we first briefly retrospect the traditional process of CVQKD system, and then give detailed description of the proposed multi-label learning-based CVQKD (ML-CVQKD) scheme.

2.1. Traditional process of CVQKD

Since Grosshans and Grangier put forward the initial Gaussian-modulated coherent state (GG02) protocol [36], scholars have proposed plenty of improved schemes. Subsequently, Leverrier et al further modified the process by taking finite-size effect into account [37], rendering the traditional process become a standard for most CVQKD systems.

Figure 1(a) shows the basic prepare-and-measurement (PM) model for traditional CVQKD, and its process is shown in figure 1(b) [9], we now explain each step as follows.
Figure 2. Scheme for ML-CVQKD. It is composed of two parts, state learning for modeling and evaluation, and state prediction for classification.

**State preparation.** Alice first prepares a modulated coherent state, and sends it to Bob through an untrusted quantum channel.

**Measurement.** Bob then measures the incoming state with coherent detection so that Alice and Bob share two correlated sets variables, i.e. raw key.

**Reconciliation.** One first needs to discretize the yielded raw key if Gaussian modulation is used, and then a linear error correcting code, usually a low density parity check (LDPC) code [38], is exploited to automatically reconcile the data between Alice and Bob.

**Parameter estimation.** Bob sends a part of bits of information to Alice that allow her to infer the characteristic of the quantum channel and compute the covariance matrix of quantum system.

**Privacy amplification.** Alice and Bob apply a random hash function to their respective strings so that they can obtain two identical strings, i.e., secret key.

The above process is based on information theory, so that one needs to correct the erroneous code and evaluate the quality of quantum channel, which makes reconciliation and parameter estimation become the most crucial steps. Therefore, a part of resources such as the generated raw key, storage and computing of devices have to be inevitably sacrificed for these two steps. Moreover, small modulation variance is needed to keep discretely-modulated CVQKD protocol safe, otherwise eavesdropper may perfectly launch the intercept-resend attack without detection [6].

### 2.2. Process of ML-CVQKD

Multi-label learning involves three modules, i.e., training, testing and prediction. Each module is responsible for respective task, i.e. modeling, evaluation and classification. Specifically, to construct the classifier, a training set is first used for learning the classification rules. Subsequently, another set of data, called testing set, is exploited to evaluate the classifier’s performance. Finally, the trained classifier can be used for predicting unknown data if the evaluation is passed. Inspired by the process of multi-label learning, ML-CVQKD is proposed, which includes two parts: state learning and state prediction. As shown in figure 2, we explain each step as follows.

**State learning**

**Step 1.** Alice first prepares modulated coherent states, and sends them to Bob through noisy and lossy quantum channel. The label information of each state is also sent to Bob via auxiliary classical channel.

**Step 2.** Bob measures the incoming states with coherent detector thereby obtains the measurement results. Note that these results are similar to, but not identical to the modulated information sent by Alice, this is because the transmitted signals are inevitably distorted by several negative effects such as channel noise and loss.

**Step 3.** Bob then extracts features from the obtained labeled coherent states, these features are prepared to training and testing classifier.
Figure 3. The $k$-NN classification algorithm in feature space. Green circle denotes an unknown data point, triangles and rectangles belong to red class and yellow class, respectively. Blue dashed circle represents $k = 3$ while blue dotted circle represents $k = 7$.

Step 4. After collecting sufficient featured data, Bob divides them into two datasets, i.e. training set and testing set. The former is used for training classifier, and the latter is used to evaluate the classifier’s performance. Finally, a well-behaved classifier for ML-CVQKD is prepared if testing is passed. Once the classifier has been trained successfully, one does not need to perform state learning repeatedly. The system is ready for generating secret key.

State prediction
Step 1. Alice prepares modulated coherent states and sends them to Bob through untrusted quantum channel.
Step 2. Bob obtains the measurement results (unlabeled) by measuring the received states with coherent detector.
Step 3. Bob first extracts features from the obtained unknown data, these features are subsequently used as input data for the prepared classifier.
Step 4. Bob classifies the input data using the well-behaved classifier, so that he can predict the state that Alice sent to him. After many rounds of prediction, Alice and Bob share a string of key.
Step 5. A linear error correcting code, usually a LDPC code, is applied to automatically correct the data between Alice and Bob.
Step 6. Bob sends a part of bits of information to Alice that allow her to infer the characteristic of the quantum channel and compute the covariance matrix of quantum system.
Step 7. To further enhance the security, Alice and Bob apply a random hash function to their respective strings. Finally, they respectively obtain two identical strings, i.e. secret key.

Similar to the basic assumption of QKD in which both Alice’s side and Bob’s side cannot be compromised (device-independent-QKD excluded), the steps of state learning has to be done without eavesdropping. That is to say, assuming state learning is trusted, otherwise Eve may have the opportunity to learn the knowledges about the classifier, rendering information leakage. This assumption can be implemented through security monitoring of the communication system when initially deploying the proposed scheme. We do not intend to detail it, as the monitoring approach is not the key point of this paper. Even so, we point out that an efficient way for monitoring state learning is necessary, we leave this issue to our future study. On the other hand, the steps in state prediction look similar to conventional CVQKD process, however, it is quite different. First of all, the steps of feature extraction and classifier are added to the process, these two steps are the point of ML-CVQKD scheme. Secondly, the data format is different, coherent state is represented by several robust features rather than quadratures itself, these proper features are conducive to improve the performance of quantum classifier.

3. Multi-label classification algorithm

MLCA is derived from a traditional lazy learning approach called $k$-nearest neighbor ($k$NN) [39]. It selects $k$ NNs for each unknown data point. Based on the number of neighboring data belonging to each possible class, maximum $a$ posteriori principle can be exploited to allocate the label to the unknown data point. Figure 3 depicts an example of $k$NN approach in feature space. The green circle denotes an unknown data point, while triangles and rectangles represent the labeled data points which respectively belong to red class and yellow class. The green circle will be assigned to the red class for $k = 3$, since two of the three-nearest
Figure 4. (Top) phase space representation of coherent states with (a) QPSK and (b) 8PSK modulation. Each coherent state is assigned only one label in QPSK or multiple (at least one) labels in 8PSK. (Bottom) quantum machine learning model for (c) single-label learning and (d) multi-label learning.

labeled data points belong to the red class while only one point belongs to the yellow class. Similarly, the green circle will be labeled as yellow class for $k = 7$.

$k$NN classifies unknown data in feature space which enlightens us that coherent states can probably be classified in its phase space. As shown in figure 4(a), the phase space is divided into several regions, which are labeled as $L_i$ ($i = 1, 2, 3, 4$) according to their located quadrant. We find that each QPSK-modulated coherent state belongs to a single label, which can be deemed quantum single-label learning problem depicted in figure 4(c). However, with the development of modulation technique, single-label learning is not suitable to address high-dimensional modulation problem. As an example, figure 4(b) shows the phase space representation for coherent states with 8PSK modulation. Thereinto, some of 8PSK-modulated coherent states, such as $|\alpha_2\rangle$, $|\alpha_4\rangle$, $|\alpha_6\rangle$ and $|\alpha_8\rangle$, simultaneously belong to multiple labels, which can be generalized into multi-label learning problem depicted in figure 4(d).

In fact, single label is a special case of multiple labels, so that both can be described by the model of multi-label learning. In what follows, we detail the proposed MLCA for addressing the generalized multi-label CVQKD model. Without loss of generality, we consider the algorithm for the eight-state CVQKD since it is the simplest multi-label modulation scheme. We note that the proposed MLCA can also be extended for other complicated modulation schemes.

3.1. Feature extraction for coherent state

As known, feature extraction is an important data-preprocessing step in machine learning field, since a set of suitable features would significantly enhance classification performance. The more features are extracted, the more details about the object can be obtained. However, there is few apparent features to describe a modulated coherent state, except for a few attributes such as $p$-quadrature, $q$-quadrature and modulated variance $V_M$.

To solve the above-mentioned problem, we construct a set of distance features for each coherent state. As shown in figure 5, Alice sends a modulated coherent state through an untrusted quantum channel (usually a single mode fiber, SMF), and then the transmitted coherent state is received by Bob. Note that the transmitted state is no longer identical with its initial modulated state due to the phase drift ($\theta' \neq \theta$) and energy attenuation ($\sqrt{p'^2 + q'^2} < \sqrt{p^2 + q^2}$) caused by the imperfect channel noise and loss. Subsequently, a number of virtual states (we named them reference states) are set for calculating the similarities of the transmitted state and reference states. In particular, the similarity can be measured by Euclidean metric, which is the straight-line distance between two points in Euclidean space \cite{40}. In the Cartesian coordinates, we assume $y = (y_1, y_2, \ldots, y_n)$ and $z = (z_1, z_2, \ldots, z_n)$ are two points in Euclidean $n$-dimensional space, and the distance $d$ between $y$ and $z$ is given by

\[
d(y, z) = \sqrt{\sum_{i=1}^{n} (y_i - z_i)^2}.\]
Specifically, in the two-dimensional phase space we have
\[
d_w(t, r) = \sqrt{(p' - p)^2 + (q' - q)^2},
\]
where \( w \) is the number of reference state, \( t = (p', q') \) and \( r = (p, q) \) are the respective Cartesian points of transmitted state and \( r \)th reference state. After that, we can extract a set of feature vectors \( d = (d_1, d_2, \ldots, d_w) \) for better description of the transmitted states.

As mentioned above, reference states are a set of virtual states that do not really exist, and hence one does not need to prepare them at Bob’s side. In general, reference states are set to be identical with initial modulated states, which can help us to investigate the influence of imperfect channel on transmitted state.

3.2. Multi-label classifier for ML-CVQKD

After extracting robust features, these features are subsequently used as input data of classifier for state learning. Assuming \( X = \mathbb{R}^d \) is \( d \)-dimensional data space, and \( Y = \{y_1, y_2, \ldots, y_l\} \) is label space containing \( l \) categories. A training set is given by \( \mathcal{D} = \{ (x_i, y_i) | 1 \leq i \leq m \} \), where \( x_i \in X \) is \( d \)-dimensional attribute vector \( (x_{i1}, x_{i2}, \ldots, x_{id})^T \) and \( Y_i \subseteq Y \) is a set of labels to which \( x_i \) belongs.

The task of learning system is to find a multi-label classifier \( h(\cdot) : X \rightarrow 2^Y \), where \( 2^Y \) is the power set of set \( Y \). Namely, for a given threshold function \( t : X \rightarrow \mathbb{R} \), it renders \( h(x) = \{ y | f(x, y) > t(x), y \in Y \} \).

Let \( |x\rangle \) be an unlabeled coherent state, and \( \mathcal{N}(|x\rangle) \) denotes the subset of \( k \) nearest coherent states of \( |x\rangle \) in training set. The following statistic will be calculated as
\[
C_j = \sum_{(|x\rangle, y^+ \in \mathcal{N}(|x\rangle)} \{ y_j \in Y^+ \},
\]
where \((|x^+\rangle, Y^+)\) denotes the labeled coherent states in training set that belong to \( \mathcal{N}(|x\rangle) \), \( \| \bullet \| \) denotes the times of \( \bullet \) and thus \( C_j \) counts the number of neighbors of \( |x\rangle \) belonging to the \( j \)th category \( y_j | 1 \leq j \leq l \).

Assuming \( H_j \) represents the event that coherent state \( |x\rangle \) has label \( y_j \), then \( P(H_j|C_j) \) denotes the posteriori probability, where \( H_j \) is true under the condition that \( C_j \) is the labeled data in \( \mathcal{N}(|x\rangle) \) have label \( y_j \). Accordingly, \( P(H_j|C_j) \) denotes the posteriori probability which \( H_j \) is false under the condition that \( C_j \) labeled data in \( \mathcal{N}(|x\rangle) \) with label \( y_j \). Let \( f(|x\rangle, y_j) = P(H_j|C_j)/P(H_j|C_j) \), the quantum multi-label classifier can be expressed by
\[
h(|x\rangle) = \{ y_j | P(H_j|C_j)/P(H_j|C_j) > t(|x\rangle), \ 1 \leq j \leq l \}.
\]

In other words, unlabeled coherent state \( |x\rangle \) can be assigned to category \( y_j \) when posteriori probability \( P(H_j|C_j) \) is greater than \( t(|x\rangle) \cdot P(H_j|C_j) \).

Specifically, based on Bayesian theorem [34], function \( f(|x\rangle, y_j) \) can be rewritten as
\[
f(|x\rangle, y_j) = \frac{P(H_j|C_j)}{P(H_j|C_j)} = \frac{P(H_j) \cdot P(C_j|H_j)}{P(H_j) \cdot P(C_j|H_j)},
\]
where \( P(H_j) \) and \( P(H_j) \) respectively represent the prior probability that event \( H_j \) is true or false, \( P(C_j|H_j) \) and \( P(C_j|H_j) \) respectively represent the conditional probability of \( C_j \) labeled coherent states in \( \mathcal{N}(|x\rangle) \) with label \( y_j \) under the condition that event \( H_j \) is true or false.

Figure 5. Feature extraction for 8PSK-modulated coherent state. (Left) Alice sends the modulated coherent state through the noisy and lossy channel. (Right) Bob receives the transmitted coherent state and extracts its distance features. Green dot denotes signal state, and yellow dot denotes virtual state, i.e. reference state.
The probabilities in equation (5) can be estimated by frequency counting in training set. In particular, prior probabilities can be calculated by

\[ P(H_j) = \frac{s + \sum_{i=1}^{m} [y_i \in Y_j]}{s \times 2 + m} \quad (1 \leq j \leq l), \tag{6} \]

and

\[ P(H_j) = 1 - P(H_j) \quad (1 \leq j \leq l), \tag{7} \]

where \( s \) is a smoothing parameter controlling the weight of uniform prior distribution during probability estimates, and it usually set to 1 for Laplace smoothing.

Different from prior probability, the estimation of conditional probabilities in equation (5) is complicated. For the \( j \)th category \( y_j \) (1 \( \leq j \leq l \)), we calculate two arrays \( \varsigma_j \) and \( \varsigma_j \), each of which contains \( k + 1 \) elements given by

\[ \varsigma_j[r] = \sum_{i=1}^{m} [y_i \in Y_j] \cdot [\psi_j(|x_i|) = r] \quad (0 \leq r \leq k), \tag{8} \]

and

\[ \varsigma_j[r] = \sum_{i=1}^{m} [y_i \notin Y_j] \cdot [\psi_j(|x_i|) = r] \quad (0 \leq r \leq k), \tag{9} \]

where

\[ \psi_j(|x_i|) = \sum_{(|x_i|, y_j) \in N(|x_i|)} [y_j \in Y_j]. \tag{10} \]

\( \psi_j(|x_i|) \) counts the number of neighbors that belong to category \( y_j \) in \( k \) NNs of the \( j \)th coherent state. Correspondingly, \( \varsigma_j[r] \) counts the number of coherent states that belong to category \( y_j \) themselves and exactly have \( r \) neighbors which belong to category \( y_j \) in \( k \) neighbors, while \( \varsigma_j[r] \) counts the number of coherent states that does not belong to category \( y_j \) and exactly have \( r \) neighbors which belong to category \( y_j \) in \( k \) neighbors. Consequently, the conditional probabilities in equation (5) can be calculated by

\[ P(C_j|H_j) = \frac{s + \varsigma_j[C_j]}{s \times (k + 1) + \sum_{r=0}^{k} \varsigma_j[r]}, \tag{11} \]

and

\[ P(C_j|H_j) = \frac{s + \varsigma_j[C_j]}{s \times (k + 1) + \sum_{r=0}^{k} \varsigma_j[r]}, \tag{12} \]

where 1 \( \leq j \leq l \) and 0 \( \leq C_j \leq k \). Finally, a well-behaved multi-label classifier \( h(|x|) \) for ML-CVQKD is obtained by the successful state learning.

Comparing with state-discrimination detector reported by our previous work [34], the proposed MLCA has several advantages. The most obvious merit is that MLCA has the ability to address the model of multi-label learning, thereby it is suitable to the high dimensional modulation strategy. In essence, MLCA belongs a part of data-processing in ML-CVQKD, so that it can be ran without any extra device or component. Moreover, the MLCA-embedded ML-CVQKD can further improve the performance of quantum communication system, we give the detailed analysis in next section.

4. Analysis and discussion

In this section, we elaborate the performance and security of the proposed MLCA-embedded ML-CVQKD system. We first interpret the prepared data after feature extraction, and then show the performance analysis of MLCA with several machine learning-based metrics. Security and comparison are subsequently presented.

4.1. Data preprocessing

For simplicity, we limit the analysis to a linear quantum channel, so that the quantum channel of the fiber-based one-way quantum key distribution can be deemed a mapping function which can be described as [41]

\[ q' = \sqrt{T}(q \cos \varphi_0 + p \sin \varphi_0) + \varepsilon, \tag{13} \]

\[ p' = \sqrt{T}(p \cos \varphi_0 - q \sin \varphi_0) + \varepsilon, \tag{14} \]
where $\varphi_0 = |\theta - \theta'|$ is the phase drift during transmission and $\varepsilon$ is Gaussian $(0, N_0 + T \xi)$ distribution. Figure 6 shows $10^4$ data points of 8PSK-modulated coherent state in phase space after passing 20 km fiber-based quantum channel. Due to the impact of channel loss and noise, the transmitted states are distributed in phase space with a certain probability distribution. As can be seen, however, these chaotic points with initial format are hardly distinguished thereby cannot be directly used as input data for MLCA. After feature extraction, figure 7 shows that these coherent states are mapped into an eight-dimensional vector by calculating the Euclidean distance between each data point and each reference state. We observe that most distance values of feature vectors are located range from 0 to 9.5, while a few feature vectors contains high distance values. These high-value feature vectors are corresponding to the edge outliers in figure 6, which leads to performance reduction. Therefore, a threshold function can be used to filter the high-value feature vectors, feature vectors whose feature value beyond black line in figure 7 should be discarded for performance improvement.

4.2. Performance on machine learning-based metrics
ML-CVQKD takes advantage of multi-label learning-based technology to predict unknown signal state, so that the traditional information theory-based metrics used in GG02 are not enough to comprehensively estimate the performance of our scheme. Hence, several machine learning-based metrics need to be introduced.
Assuming there are three datasets, i.e., dataset A denotes samples which predicted as positive, dataset B denotes all positive samples, and dataset C denotes all samples. Figure 8 shows the relationship between these datasets and their corresponding metrics, which are listed below.

**Precision (Prec)** describes the rate of positive samples in the samples predicted as positive.

**Recall (Rec)** describes the rate of samples predicted as positive in all positive samples.

**False positive rate (FPR)** describes the rate of samples predicted as positive in all negative samples.

Actually, besides the above-listed metrics, there may be other metrics used in machine learning to estimate specific systems. The reason why we select these three is that the primary concern of our scheme is the correctness of the coherent state classification. We need to know how accurate MLCA can be and how many misclassifications it occurs. In addition, since MLCA is designed for solving multi-label classification problems, we deploy another metric called **average precision (AP)**, which evaluates the average fraction of labels ranked above a particular label $y \in Y$ which are in $Y$. It can be expressed as

$$AP = \frac{1}{g} \sum_{i=1}^{g} \frac{1}{|Y_i|} \sum_{y \in Y_i} \left| \left\{ y' \mid \text{rank}_Y(|x_i\rangle, y') \leq \text{rank}_Y(|x_i\rangle, y), y' \in Y_i \right\} \right|,$$

where $g$ is the number of data in testing set and $\text{rank}_Y(\cdot, \cdot)$ is ranking function related to labels [39]. The performance improves with the increased AP, and the maximum perfect value is $AP = 1$.

Figure 9 shows the performance of the MLCA-embedded ML-CVQKD system in terms of precision (a), recall (b), false positive rate (c) and average precision (d). According to the plots (a), (b) and (d), the performance of Prec/Rec/AP show the similar trend. Namely, it increases with the enlarged modulation variance and decreases with the risen channel loss. More specifically, the optimal performance can be achieved in both Prec and Rec when $V_m \geq 40$ regulated at a certain channel loss range. It illustrates that the MLCA-embedded ML-CVQKD has the ability to accurately predict unlabeled positive signal states. In the meanwhile, plot (d) shows that the AP has larger range of perfect performance area. It illustrates that MLCA is well qualified for handling the multi-label classification problem of coherent state. On the other hand, plot (c) shows the reduced FPR, and it illustrates that the level of misclassification is well acceptable.

Although Prec/Rec/FPR/AP have shown the respective performance from different aspects, we still hope that using only one metric to check the overall quality of the embedded MLCA. Therefore, **receiver operating characteristic curve (ROC)** [42], which describes the true positive rate of a certain classifier as a function of its FPR, is introduced. With ROC curve, one can explicitly tell the quality of the classifier: the curve more close to point (0, 1), the performance better. Figure 10 shows the ROC curves of MLCA. The gray line is the result of random guess, which illustrates that there is no performance improvement without using any classifier. For each label, however, the ROC curve is close to point (0, 1) with embedded MLCA, which
denotes the proposed classifier can dramatically improve the prediction performance of ML-CVQKD. We further calculate the area under curve (AUC) for each label and thus obtain AUC value, which is a probability value range from 0 to 1. As a numerical value, AUC can be directly used for evaluating classifier’s quality. Therefore, the efficiency of quantum classifier $\Lambda$ can be described by its AUC value, namely $\Lambda = \text{average AUC}$ in our case. Moreover, a threshold range from 0.5 to 1 can be set to monitor the effectiveness of classifier. The state learning must be interrupted and restarted if AUC value of current trained classifier less than a certain threshold.

### 4.3. Security and comparison

Till now, we have demonstrated the performance of MLCA-embedded ML-CVQKD system in terms of machine learning-based metrics. However, we still want to present a performance comparison for ML-CVQKD in traditional way so that researchers who do not familiar with machine learning can
immediately evaluate how much improvement of the proposed scheme can achieve. To this end, we first present the theoretical security proof for ML-CVQKD as follows.

To avoid redundant description, we here only focus on the analysis with reverse reconciliation, one can also obtain the direct reconciliation version by the following similar approach. As known in asymptotic limit, the secret key rate of the conventional discretely-modulated CVQKD with reverse reconciliation is given by

\[ K_{asym} = \beta I(A : B) - \chi_{BE}, \]  

(16)

where \( \beta \) is the reconciliation efficiency and \( I(A : B) \) is the Shannon mutual information between Alice and Bob. For heterodyne detection, we have

\[ I(A : B) = \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \]  

(17)

where \( V = V_m + 1 \) and the total noise referred to the channel input is \( \chi_{\text{tot}} = \xi - 1 + 2(1 + v_\text{el})/(\eta T), \eta \) and \( v_\text{el} \) are the practical detector’s efficiency and noise due to detector electronics, respectively. Term \( \chi_{BE} \) represents the Holevo bound [43] of the mutual information between Eve and Bob and needs to be calculated in parameter estimation. In ML-CVQKD, however, due to the data processing is quite different, equation (16) can be rewritten as the following form

\[ K_{asym}^{\text{ML}} = \beta \Lambda_{\text{MLCA}} I(A : B) - \chi_{E}^{\text{ML}}. \]  

(18)

The difference between equations (16) and (18) lies in two parts. First, the efficiency of embedded classifier \( \Lambda \) has to be considered since the classifier is necessary to the proposed ML-CVQKD. Note that the MLCA is one of embedded classifiers suggested in this paper, other excellent classifiers may also fit for ML-CVQKD. Second, term \( \chi_{BE} \) in equation (16) is substituted by term \( \chi_{E}^{\text{ML}} \), which denotes the Holevo quantity of the useful information Eve acquired by interacting with the quantum states under collective attacks, reads

\[ \chi_{E}^{\text{ML}} = S(\rho_E) - \sum_{y_i} p(y_i) S(\rho_{E|y_i}), \]  

(19)

where \( S(\rho) = -\text{Tr}(\rho \log \rho) \) is the von Neumann entropy, the logarithms are taken in base 2, \( y_i \) is the raw key obtained by Bob’s measurement with probability \( p(y_i) \), \( \rho_{E|y_i} \) is the corresponding state of Eve’s ancilla, and

\[ p_E = \sum_{y_i} p(y_i) \rho_{E|y_i}. \]  

(20)

In conventional discretely-modulated CVQKD protocol, \( p(y_i) = 1/m \) is the probability of discrete uniform distribution when variable \( Y = y_i (i = 1, 2, \ldots, m) \), since \( Y \) contains \( m \) finite and complete encoding events randomly chosen by Alice. Note that the relationship between each discretely-modulated coherent state and its binary presentation is fixed and public. For example, the key bits of state \( |\alpha_0\rangle \) in four-state protocol is always \((0, 0)\) (see figure 1 of reference [44]), so that Eve can precisely intercept the correct key bits \((0, 0)\) when she successfully intercepts the coherent state \( |\alpha_0\rangle \). Due to Eve knows all public encoding events of four-state protocol, the probability is \( p(y_i) = 1/4 \). Similarly, as Eve knows all encoding events of eight-state protocol, so the probability is \( p(y_i) = 1/8 \). However, due to the special-designed process of ML-CVQKD, the above relationship is no longer fixed and public. Although the label(s) of each discretely-modulated coherent state is fixed, such as the label of \( |\alpha_1\rangle \) is \( L_1 \) and the labels of \( |\alpha_2\rangle \) are \( L_3, L_2 \) shown in figure 4(b), the relationship between label(s) and binary key bits can be randomly assigned by Alice. Hence, only Alice knows this relationship at the beginning, and Bob will learn it by the labeled coherent state at the end of state learning. While eavesdropper who do not participate the state learning process actually does not know the correct encoding events shared by Alice and Bob. That is to say, the possible encoding events \( Y \) for Eve is infinite \((m \to \infty)\), so that an intercepted state could denote any bit(s) for Eve, which leading \( p(y_i) \to 0 \). Therefore, Eve can hardly obtain useful information from the intercepted state. The rest calculations are the same as eight-state protocol and can be found in appendix A.

Figure 11 shows the performance comparison between MLCA-embedded ML-CVQKD and several existing CVQKD protocols in asymptotic limit. The results show that MLCA-embedded ML-CVQKD outperforms other conventional CVQKD protocols in terms of the maximum transmission distance. We also find that the performance of our scheme can be further enhanced with the risen modulation variance. To investigate the cause, we further plot the asymptotic secret key rates of above-mentioned protocols with fixed distances of 50 km and 100 km. As shown in figure 12, curves of both four-state protocol and eight-state protocol are arched and are located in certain ranges of small modulation variance, which shows that small variance is required for ensuring the security of conventional discretely-modulated CVQKD.
Figure 11. Performance comparison. Solid lines denote the asymptotic secret key rates as a function of transmission distance, in which modulation variances $V_m$ of four-state protocol, eight-state protocol and Gaussian-modulated CVQKD are optimized for reasonable SNR [45]. Black dotted line denotes PLOB bound. The parameters are set to $\eta = 0.6$, $\nu_d = 0.05$, reconciliation efficiency $\beta = 0.98$, classification efficiency $\Lambda = 0.927$, excess noise $\xi = 0.01$.

Figure 12. Asymptotic secret key rates as a function of modulation variance $V_m$. The transmission distance in main figure and the inset are 50 km and 100 km, respectively. The parameters are same with those in figure 11.

Meanwhile, curves of Gaussian-modulated CVQKD and our scheme are keep rising with the increase of modulation variance, it illustrates that the small variance is no longer required for the security of ML-CVQKD, so that the proposed scheme can outperform conventional discretely-modulated CVQKD protocols in terms of both transmission rate and distance by setting proper larger modulation variance. However, we point out that although the secret key rate of ML-CVQKD is an increasing function of modulation variance in the view of mathematical calculation, it cannot surpass the Piradola–Laurenza–Ottaviani–Banchi (PLOB) bound [46]. Besides, it is worthy noticing that the security proof of our scheme is based on the security analysis of discretely-modulated CVQKD developed in reference [5], which considers the asymptotic security under a linear channel assumption. Very recently, references [44, 47] have proven the asymptotic security of discretely-modulated CVQKD without this assumption, so that one may obtain tighter security bound of ML-CVQKD by taking advantage of their approaches.

Finally, let us consider the practicality of ML-CVQKD. At the initial state learning, Alice and Bob are starting to establish a classification model, this process may be a little bit costly since numbers of coherent states and classical data should be communicated and computed. Despite that, the cost is acceptable because only four labels need to be considered, this magnitude is very small for addressing multi-label learning problem [48] (see the metric of coverage for multi-label learning). Once the process successfully completed, the system begin to enter the real quantum key distribution process, i.e. state prediction process. This process is more economic than other existing CVQKD protocols. In addition, ML-CVQKD can be applied
to the existing optical communication system without any extra equipment, leading to fast deployment and operation.

5. Conclusion

In this work, we have proposed a multi-label learning-based scheme for discretely-modulated CVQKD protocol, called ML-CVQKD. In particular, the proposed scheme divides the whole quantum system into two parts, which are trusted state learning process and untrusted state prediction process, respectively. State learning is used for training and estimating multi-label classifier, while state prediction is used for generating final secret key. To this end, feature extraction was suggested to better represent the characteristics of modulated coherent state. Subsequently, a specialized MLCA was elegantly designed as an embedded classifier for distinguishing the incoming signal state. We then introduced a series of related machine learning-based metrics to estimate the performance of MLCA, and presented the asymptotic security proof of ML-CVQKD under the linear bosonic channel assumption. The practicality of ML-CVQKD was also discussed.

Performance analysis shows that MLCA-embedded ML-CVQKD is well feasible and effective for predicting the unknown signal state. Numerical simulation shows that the proposed MLCA-embedded ML-CVQKD outperforms other existing CVQKD protocols specially in maximum transmission distance, and the performance of both transmission distance and secret key rate will be further increased with the increase of modulation variance. Besides, we notice that the finite-size composable proof of the security of discretely-modulated CVQKD under collective Gaussian attacks is finished by reference [49], thereby investigating the finite-size composable security of ML-CVQKD is the subject of our future work.

In summary, ML-CVQKD is not only a kind of variant of CVQKD protocol, but also provides a novel thought for introducing various machine learning-based methodologies to CVQKD field.

Acknowledgments

Q Liao would like to thank Professor X Fu, Professor X Wang, Dr T Wang and Dr C Wang for the helpful discussions. We would also like to thank anonymous referees for their constructive suggestions. This work is supported by the National Natural Science Foundation of China (Grants Nos. 61772191, 61871407), the National Key R & D Projects of China (Grants Nos. 2018YFB0704000 and 2017YFB0902904), Hunan Provincal Natural Science Foundation of China (Grant No. 2020JJ5088) and the Fundamental Research Funds for the Central Universities (Grant No. 531118010371).

Appendix A. Calculation for discretely-modulated CVQKD protocol

Here, we present the calculation of asymptotic secret key rate of discretely-modulated CVQKD protocol in linear bosonic channel.

The asymptotic key rate of CVQKD protocol where Bob performs heterodyne detection with reverse reconciliation under collective attack can be given by

\[ K_{\text{asym}} = \beta I(A : B) - \chi_{BE}, \]  

where the mutual information of Alice and Bob \( I(A : B) \) is already given by equation (17), and

\[ \chi_{BE} = \sum_{i=1}^{2} G \left( \frac{\lambda_{i} - 1}{2} \right) - \sum_{i=3}^{5} G \left( \frac{\lambda_{i} - 1}{2} \right), \]  

where \( G(x) = (x + 1) \log_{2}(x + 1) - x \log_{2}x \) is the von Neumann entropy, and the symplectic eigenvalues\n
\[ \lambda_{1,2}^{2} = \frac{1}{2} \left[ A \pm \sqrt{A^{2} - 4B} \right] \]  

with\n
\[ A = V^{2} + T^{2}(V + \chi_{\text{line}})^{2} - 2TZ^{2} \]  

and\n
\[ B = T^{2}(V^{2} + V\chi_{\text{line}} - Z^{2})^{2}, \]

\[ \lambda_{3,4}^{2} = \frac{1}{2} \left[ C \pm \sqrt{C^{2} - 4D} \right] \]
with
\[ C = \frac{1}{T^2(V + \chi_{\text{tot}})^2} \left[ A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}(V\sqrt{T} + T(V + \chi_{\text{line}}) + 2VT^2) \right] \] (A7)

and
\[ D = \left( \frac{V + \sqrt{T}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})} \right)^2, \] (A8)

\( \lambda_8 = 1 \), where the total channel-added noise referred to the channel input is defined as \( \chi_{\text{line}} = 1/T - 1 + \xi \) and the detection-added noise referred to Bob’s input for heterodyne detection is \( \chi_{\text{het}} = [1 + (1 - \eta) + 2\nu_2]/\eta \). The term \( Z \) is the correlation between Alice and Bob. In Gaussian-modulated CVQKD protocol, \( Z \) usually equals to \( Z_8 = \sqrt{V^2 - 1} \). However, in discretely-modulated CVQKD, \( Z \) is quite different. Specifically, \( Z_4 \) is the correlation between Alice and Bob in four-state CVQKD and \( Z_8 \) is the correlation between Alice and Bob in eight-state CVQKD, which can be expressed by [6]

\[ Z_4 = 2\alpha^2 \sum_{k=0}^{3} \frac{p_{k/2}}{p_{k/2}} \] (A9)

with
\[ l_{0,2} = \frac{1}{2} e^{-\alpha^2} \left[ \cosh(\alpha^2) \pm \cos(\alpha^2) \right], \] (A10)
\[ l_{1,3} = \frac{1}{2} e^{-\alpha^2} \left[ \sinh(\alpha^2) \pm \sin(\alpha^2) \right]. \] (A11)

and
\[ Z_8 = 2\alpha^2 \sum_{k=0}^{7} \frac{p_{k/2}}{p_{k/2}} \] (A12)

with
\[ l_{0,4} = \frac{1}{4} e^{-\alpha^2} \left[ \cosh(\alpha^2) + \cos(\alpha^2) \pm 2 \cos \left( \frac{\alpha^2}{\sqrt{2}} \right) \cosh \left( \frac{\alpha^2}{\sqrt{2}} \right) \right], \] (A13)
\[ l_{1,5} = \frac{1}{4} e^{-\alpha^2} \left[ \sinh(\alpha^2) + \sin(\alpha^2) \pm \sqrt{2} \cos \left( \frac{\alpha^2}{\sqrt{2}} \right) \sinh \left( \frac{\alpha^2}{\sqrt{2}} \right) \right] \pm \sqrt{2} \sin \left( \frac{\alpha^2}{\sqrt{2}} \right) \cosh \left( \frac{\alpha^2}{\sqrt{2}} \right), \] (A14)
\[ l_{2,6} = \frac{1}{4} e^{-\alpha^2} \left[ \cosh(\alpha^2) - \cos(\alpha^2) \mp 2 \sin \left( \frac{\alpha^2}{\sqrt{2}} \right) \sinh \left( \frac{\alpha^2}{\sqrt{2}} \right) \right], \] (A15)
\[ l_{3,7} = \frac{1}{4} e^{-\alpha^2} \left[ \sinh(\alpha^2) - \sin(\alpha^2) \mp \sqrt{2} \cos \left( \frac{\alpha^2}{\sqrt{2}} \right) \sinh \left( \frac{\alpha^2}{\sqrt{2}} \right) \right] \pm \sqrt{2} \sin \left( \frac{\alpha^2}{\sqrt{2}} \right) \cosh \left( \frac{\alpha^2}{\sqrt{2}} \right). \] (A16)

Figure 13 shows the comparison of different covariance coefficients as a function of modulation variance \( V_m \). We find that \( Z_4 \) and \( Z_8 \) are equal to \( Z_8 \) when the modulation variance is small enough. Hence, for a sufficiently low modulation variance the bound \( \chi_{\text{het}} \) for discrete modulation is almost identical to the one obtained for a Gaussian modulation.

Figure 14 depicts the optimal modulation variance for discretely-modulated CVQKD protocol as a function of transmission distance. As can be seen from the figure, the optical modulation variance is
Figure 14. Optimal modulation variance for discretely-modulated CVQKD protocol as a function of transmission distance. The parameters are set to $\eta = 0.6, v_e = 0.05$, reconciliation efficiency $\beta = 0.98$ and excess noise $\xi = 0.01$.

decreased with the increase of transmission distance, and the minimum optimal modulation variances are 0.3 for four-state CVQKD and 0.35 for eight-state CVQKD. This numerical simulation shows that small modulation variance is required to guarantee safety for discretely-modulated CVQKD protocol as it can prevent eavesdropper from intercepting the useful information.

**ORCID iDs**

Qin Liao [https://orcid.org/0000-0001-7692-7476](https://orcid.org/0000-0001-7692-7476)
Ying Guo [https://orcid.org/0000-0002-9306-2061](https://orcid.org/0000-0002-9306-2061)

**References**

[1] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers Systems and Signal Processing pp 175–9
[2] Pirandola S et al 2019 Advances in quantum cryptography (arXiv:1906.01645)
[3] Grosshans F 2005 Collective attacks and unconditional security in continuous variable quantum key distribution Phys. Rev. Lett. 94 020504
[4] Navascués M and Acín A 2005 Security bounds for continuous variables quantum key distribution Phys. Rev. Lett. 94 020505
[5] Leverrier A and Grangier P 2009 Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation Phys. Rev. Lett. 102 180504
[6] Leverrier A and Grangier P 2011 Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation Phys. Rev. A 83 042312
[7] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Werner R F 2012 Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks Phys. Rev. Lett. 109 100502
[8] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 Security of continuous-variable quantum key distribution against general attacks Phys. Rev. Lett. 110 030502
[9] Leverrier A 2015 Composable security proof for continuous-variable quantum key distribution with coherent states Phys. Rev. Lett. 114 070501
[10] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 No-switching quantum key distribution using broadband modulated coherent light Phys. Rev. Lett. 95 180503
[11] Ma X-C, Sun S-H, Jiang M-S, Gui M and Liang L-M 2014 Gaussian-modulated coherent-state measurement-device-independent quantum key distribution Phys. Rev. A 89 042355
[12] Zhao Y-B, Heid M, Rigas J and Lütkenhaus N 2009 Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks Phys. Rev. A 79 012307
[13] Brádler K and Weedbrook C 2018 Security proof of continuous-variable quantum key distribution using three coherent states Phys. Rev. A 97 022310
[14] García-Patrón R and Cerf N J 2006 Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution Phys. Rev. Lett. 97 190503
[15] Zhang H, Fang J and He G 2012 Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers Phys. Rev. A 86 022338
[16] Guo Y, Li R, Liao Q, Zhou J and Huang D 2018 Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier Phys. Lett. A 382 372
[17] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states Phys. Rev. Lett. 88 057902
[18] Liao Q, Guo Y, Wang Y and Huang D 2018 Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution Opt. Express 26 019907
[19] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 High-rate measurement-device-independent quantum cryptography Nat. Photon. 9 397
[20] Li Z, Zhang Y-C, Xu F, Peng X and Guo H 2014 Continuous-variable measurement-device-independent quantum key distribution Phys. Rev. A 89 052301
[21] Guo Y, Liao Q, Huang D and Zeng G 2017 Quantum relay schemes for continuous-variable quantum key distribution Phys. Rev. A 95 042326
[22] Lupo C, Ottaviani C, Papanastasiou P and Pirandola S 2018 Continuous-variable measurement-device-independent quantum key distribution: composability security against coherent attacks Phys. Rev. A 97 052327
[23] Choi Y, Kwon O, Woo M, Oh K, Han S-W, Kim Y-S and Moon S 2016 Plug-and-play measurement-device-independent quantum key distribution Phys. Rev. A 93 032319
[24] Huang D, Huang P, Wang T, Li H, Zhou Y and Zeng G 2016 Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol Phys. Rev. A 94 032305
[25] Usenko V C and Grosshans F 2015 Unidimensional continuous-variable quantum key distribution Phys. Rev. A 92 062337
[26] Wang P, Wang X, Li J and Li Y 2017 Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions Opt. Express 25 27995
[27] Liao Q, Guo Y, Xie C, Huang D, Huang P and Zeng G 2018 Composable security of unidimensional continuous-variable quantum key distribution Quantum Inf. Process. 17 1
[28] Weedbrook C 2013 Continuous-variable quantum key distribution with entanglement in the middle Phys. Rev. A 87 022308
[29] Guo Y, Liao Q, Wang Y, Huang D, Huang P and Zeng G 2017 Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction Phys. Rev. A 95 032304
[30] Papanastasiou P, Lupo C, Weedbrook C and Pirandola S 2018 Quantum key distribution with phase-encoded coherent states: asymptotic security analysis in thermal-loss channels Phys. Rev. A 98 012340
[31] Huang P, Huang J, Zhang Z and Zeng G 2018 Quantum key distribution using basis encoding of Gaussian-modulated coherent states Phys. Rev. A 97 042311
[32] Robert C 2014 Machine learning: a probabilistic perspective Chance 27 62
[33] Liu J-Y, Ding H-J, Zhang C-M, Xie S-P and Wang Q 2019 Practical phase-modulation stabilization in quantum key distribution via machine learning Phys. Rev. Appl. 12 014059
[34] Liao Q, Guo Y, Huang D, Huang P and Zeng G 2018 Long-distance continuous-variable quantum key distribution Phys. Rev. A 98 022305
[35] Liu W, Huang P, Peng J, Fan J and Zeng G 2018 Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution Phys. Rev. A 97 022316
[36] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states Phys. Rev. Lett. 88 057902
[37] Leverrier A, Grosshans F and Grangier P 2010 Finite-size analysis of a continuous-variable quantum key distribution Phys. Rev. A 81 062343
[38] Jiang X-Q, Huang P, Huang D, Lin D and Zeng G 2017 Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution Phys. Rev. A 95 052318
[39] Zhang M L and Zhou Z H 2007 ML-KNN: a lazy learning approach to multi-label learning Pattern Recognit. 40 2038
[40] Deza M M and Deza E 2005 Encyclopedia of Distances (Berlin: Springer) (https://doi.org/10.1007/978-3-642-00234-2_1)
[41] Qi B, Huang L L, Qian L and Lo H K 2007 Experimental study on the Gaussian-modulated coherent-state quantum key distribution systems by using optical preamplifiers J. Phys. B: At. Mol. Opt. Phys. 40 114014