IOP Publishing   *New J. Phys.* **27** (2025) 053201   https://doi.org/10.1088/1367-2630/adcf45

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics
Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

CrossMark

OPEN ACCESS

RECEIVED
11 December 2024

REVISED
24 February 2025

ACCEPTED FOR PUBLICATION
22 April 2025

PUBLISHED
7 May 2025

PAPER

Multidimensional reconciliation scheme using deep learning in continuous-variable quantum key distribution

Yan Feng[1], Jiangliang Jin[2], Kun Zhang[3], Zhipeng Chen[1], Xue-Qin Jiang[2,4,*], Peng Huang[4,5,*] and Guihua Zeng[4,5]

[1] School of Electronic and Information, Shanghai Dianji University, Shanghai 201306, People's Republic of China
[2] School of Information Science and Technology, Donghua University, Shanghai 201620, People's Republic of China
[3] School of Electronics and Information, Soochow University, Suzhou 215006, People's Republic of China
[4] Hefei National Laboratory, Hefei 230088, People's Republic of China
[5] State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Sensing and Information Processing (QSIP), Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China
[*] Authors to whom any correspondence should be addressed.

E-mail: xqjiang@dhu.edu.cn and huang.peng@sjtu.edu.cn

Keywords: multidimensional reconciliation, continuous-variable quantum key distribution, deep learning, low-density parity-check codes

Abstract

Information reconciliation is a significant stage in continuous-variable quantum key distribution (CV-QKD) systems as it directly affects the performance of the CV-QKD systems including secret key rate and secure transmission distance. This paper proposes a multidimensional reconciliation scheme using deep learning in CV-QKD systems. Firstly, different neural networks are constructed to obtain the norm information. Secondly, a multidimensional reconciliation scheme with deep learning assisted norm information is proposed which no longer needs to transmit the norm information through the authenticated classical public channel. Finally, simulation results and performance analysis show that, compared with the traditional multidimensional reconciliation scheme, the multidimensional reconciliation scheme with deep learning assisted norm information can decrease the communication traffic to a certain extent.

1. Introduction

Numerous cryptosystems ensure information security, which is becoming more and more crucial in the modern information society. With the rapid development of quantum computers and quantum algorithms, the computational complexity assumption based classical cryptography approach has been no longer unconditionally secure [1–3]. Quantum key distribution (QKD) is unconditionally secure and has aroused much attention as it can provide information theoretically secure keys exchange even in the era of quantum computers [4–6]. The two primary types of QKD that encode information on discrete and continuous variables, respectively, are discrete-variable (DV) QKD and continuous-variable (CV) QKD [7–11]. DV-QKD employs the single photon detection and has the advantages long transmission distance and relatively simple data post processing [12, 13]. In contrast, CV-QKD encodes information on the quadratures of quantized optical fields and can provide a high secret key rate over metropolitan areas. Furthermore, it has good compatibility with the current coherent optical communication technology and has rapid progress in recent years [14–17].

Currently, there are various representative CV-QKD schemes. e.g. coherent state CV-QKD , squeezed-states CV-QKD and rotation symmetric bosonic codes CV-QKD [18, 19]. Among these schemes, the coherent state scheme [14, 20] stands out as it has been theoretically validated as secure against both collective and coherent attacks. A typical CV-QKD system, which is shown in figure 1, mainly includes two phases: quantum information transmission and post-processing. In the quantum information transmission phase, Alice sends the prepared coherent states to Bob through a private quantum channel. Then Bob measures the received coherent states by utilizing heterodyne or homodyne detection techniques. In order to

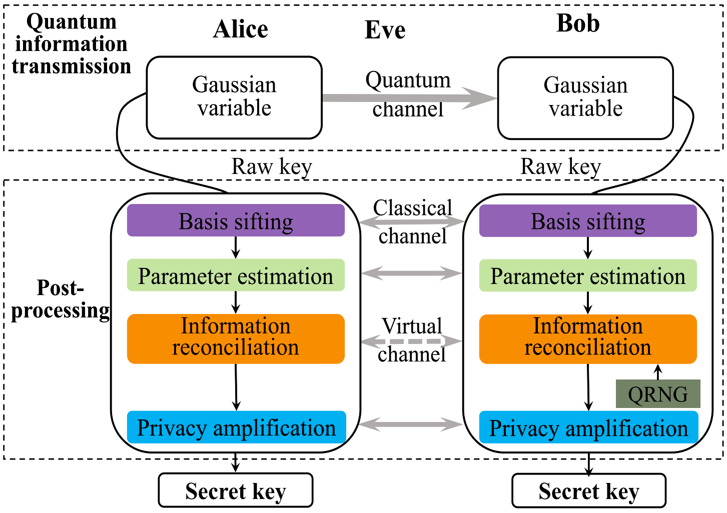

Figure 1. Schematic of a CV-QKD system. Alice transmits Gaussian quantum states to Bob over the private quantum channel. In the reverse multidimensional reconciliation scheme, Bob generates secret keys, and then both parties extract the secret keys over the authenticated classical public channel. QRNG: quantum random number generator.

obtain the secret keys for both legitimate parties, Alice and Bob subsequently perform the post-processing phase, which includes four stages: basis sifting, parameter estimation, information reconciliation [21] and privacy amplification [22]. It is generally known that the reconciliation efficiency is directly related to the secret key rate and the secure transmission distance of the involved CV-QKD system [23]. Therefore, information reconciliation is a crucial stage in the CV-QKD system to distill symmetric secret keys from the raw keys. To date, there have been mainly two information reconciliation schemes in CV-QKD systems: slice error-correcting reconciliation (SEC) [24] and multidimensional reconciliation [25]. The secure transmission distance of SEC reconciliation is limited by its poor quantization performance at the low signal-to-noise (SNR) of long-distance CV-QKD [26]. However, the multidimensional reconciliation can enhance the reconciliation efficiency, and therefore improve the secret key rate and secure transmission distance in case of low SNRs [27].

There are two types of multidimensional reconciliation, direct multidimensional reconciliation and reverse multidimensional reconciliation [28]. As the reverse multidimensional reconciliation can beat the 3 dB loss limit, it is optimum for CV-QKD systems [29]. In the reverse multidimensional reconciliation, a virtual channel which is often regarded approximately as a binary input additive white Gaussian noise (BI-AWGN) channel can be established [30]. Subsequently, the multidimensional reconciliation problem is successfully transformed into a channel coding problem that can be solved by error-correcting codes, theoretically extending the secure transmission distance from 30 to 50–100 km [31]. Afterward, to achieve higher reconciliation efficiency, the multidimensional reconciliation scheme has been employed in a series of works with different error-correcting codes [32–38].

However, to compute the initial iteration message, the multidimensional reconciliation scheme with error-correcting code requires the encoder to send norm information to the decoder. As we all know, all of the information shared during reconciliation must be authenticated using secure keys [39]. On the one hand, the extra norm in traditional multidimensional reconciliation scheme results in heavy consumption of communication traffic. On the other hand, when the repetition frequency of the quantum channel rapidly increases, the storage resources of post-processing devices are facing new hurdles [40]. Namely, the multidimensional reconciliation schemes which require the encoder providing norm information to the decoder may not be appropriate for the practical high-speed CV-QKD systems.

Here, we propose a multidimensional reconciliation scheme using deep learning in CV-QKD systems. Firstly, the decoding initialization formula for multidimensional reconciliation is analyzed. Based on deep learning, the related factors, e.g. the noisy version of the secret key, the SNRs obtained from parameter estimation, the Gaussian continuous variable of the decoder and the rotation matrix have been used to construct deep neural networks. Secondly, a multidimensional reconciliation scheme with deep learning assisted norm information is proposed, where the encoder no longer needs to transmit the norm information to the decoder. Finally, simulation results and performance analysis show that, compared with the traditional multidimensional reconciliation scheme, the multidimensional reconciliation scheme with deep learning assisted norm information can decrease the communication traffic to a certain extent. Moreover, compared with the scheme proposed in [41], the proposed multidimensional reconciliation scheme with deep learning assisted norm information can improve the reconciliation efficiency and secret key rate of CV-QKD systems.

This paper is organized as follows. In section 2, the technical preliminaries are briefly provided. In section 3, different neural networks are constructed to obtain the norm information and the multidimensional reconciliation scheme with deep learning assisted norm information is proposed. In section 4, the network training strategy, related simulation, and analysis of the proposed multidimensional reconciliation scheme with deep learning assisted norm information are provided. Finally, section 5 concludes the paper.

2. Preliminaries

In this section, we first briefly describe the multidimensional reconciliation in post-processing and then present the multidimensional reconciliation with low-density parity-check (LDPC) codes.

2.1. Multidimensional reconciliation

In CV-QKD, inevitable inconsistencies arise in the raw keys acquired by the legitimate parties, stemming from the inherent noises and attenuation within the quantum channel, as well as the intrinsic noise associated with the quantum states themselves. Information reconciliation is used to correct errors in raw keys, such that Alice and Bob can obtain the secret keys. However, the Gaussian distributed raw data that resulted from the quantum information transmission is not uniformly distributed. The raw data manipulations require the use of an authenticated classical public channel that only allows the transmission of uniformly distributed data. To this end, the nonuniform Gaussian distributed variable space has to be mapped into the uniform-distributed variable space in the multidimensional reconciliation stage.

To ensure security, Alice and Bob must partition the continuous variables with length N into successive d-dimensional vectors in multidimensional reconciliation. Then they can combine each group with d continuous variables in order and obtain $\boldsymbol{x} = (x_1, x_2, \cdots, x_d)$ obeying Gaussian distribution $\mathcal{N}(0, \sigma_x^2)^d$, $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z}$, where each continuous variable of z obeying $\mathcal{N}(0, \sigma_z^2)^d$ is the noise of the private quantum channel and d is the dimension of multidimensional reconciliation. The long distance CV-QKD systems require reverse multidimensional reconciliation, which is characterized as follows:

- The corresponding Gaussian vectors of Alice and Bob are normalized into $\boldsymbol{x}' = \boldsymbol{x}/||\boldsymbol{x}||$ and $\boldsymbol{y}' = \boldsymbol{y}/||\boldsymbol{y}||$ for each group with d continuous variables. Here, $||\boldsymbol{x}||$ and $||\boldsymbol{y}||$ are the Euclidean norms of Gaussian vectors $\boldsymbol{x}$ and $\boldsymbol{y}$, respectively. The normalized results $\boldsymbol{x}'$ and $\boldsymbol{y}'$ are uniform-distributed on the unit sphere S^{d-1}.
- A random binary sequence $\boldsymbol{c}$, which is considered as the secret key, with uniform distribution is generated by the quantum random number generator (QRNG) on Bob's side. Then, the secret key will be transformed into a codeword $\boldsymbol{c}'$ through error-correcting codes, e.g. LDPC codes. Meanwhile, the codeword $\boldsymbol{c}'$ needs to be converted into a binary spherical code $\boldsymbol{u}$ so as to guarantee the side information that will be transmitted over the authenticated classical public channel will not give any relevant information to Eve. For a subgroup of codeword denoted by $(c_1', c_2', \cdots, c_d')$, the corresponding spherical code is

$$\boldsymbol{u} = \left(\frac{(-1)^{c_1'}}{\sqrt{d}}, \frac{(-1)^{c_2'}}{\sqrt{d}}, \cdots, \frac{(-1)^{c_d'}}{\sqrt{d}} \right). \tag{1}$$

- Bob calculates the rotation matrix $\boldsymbol{M}(\boldsymbol{y}', \boldsymbol{u})$ according to the normalized result $\boldsymbol{y}'$ and the converted spherical code $\boldsymbol{u}$, where

$$\boldsymbol{M}(\boldsymbol{y}', \boldsymbol{u})\boldsymbol{y}' = \boldsymbol{u}. \tag{2}$$

Subsequently, the norm information $||\boldsymbol{y}||$, syndrome $\boldsymbol{S}$ and the rotation matrix $\boldsymbol{M}(\boldsymbol{y}', \boldsymbol{u})$ are sent from Bob to Alice. In such a case, Alice can generate a close approximation to $\boldsymbol{u}$ by performing rotation operation on $\boldsymbol{x}'$,

$$\begin{aligned} \boldsymbol{v} &= \boldsymbol{M}(\boldsymbol{y}', \boldsymbol{u})\boldsymbol{x}' \\ &= \frac{1}{||\boldsymbol{x}||}\boldsymbol{M}(\boldsymbol{y}', \boldsymbol{u})(\boldsymbol{y} - \boldsymbol{z}) \\ &= \frac{||\boldsymbol{y}||}{||\boldsymbol{x}||}\boldsymbol{u} - \frac{1}{||\boldsymbol{x}||}\boldsymbol{M}(\boldsymbol{y}', \boldsymbol{u})\boldsymbol{z}. \end{aligned} \tag{3}$$

Following the procedures above, a virtual channel with input $\boldsymbol{u}$ and output $\boldsymbol{v}$ is created. The Gaussian variable reconciliation problem is then turned into an error-correcting problem for the BI-AWGN channel [9]. To obtain the same key $\boldsymbol{u}$ as Bob's, Alice has to correct errors in $\boldsymbol{v}$ with error-correcting codes.

2.2. Multidimensional reconciliation with LDPC code

The meticulously designed LDPC codes, characterized by their well-crafted check matrices $\boldsymbol{H}$, exhibit performance levels that closely approximate the Shannon limit on BI-AWGN channels. By utilizing the belief propagation (BP) algorithm, specifically its log-likelihood ratio BP (LLR-BP), the LDPC codes achieve a substantial increase in decoding throughput. Consequently, we implement the LLR-BP algorithm in the context of multidimensional reconciliation, aiming to significantly reduce the frame error rate (FER), increase the secret key rate, and extend the secure transmission distance.

The LLR-BP algorithm stands as a highly efficient soft iterative decoding approach for LDPC codes. In the framework of this algorithm, variable nodes and check nodes engage in an iterative exchange of messages. Specifically, a check node receives messages from its adjacent variable nodes, processes them through a defined methodology, and then relays the processed messages back to its neighboring variable nodes. Similarly, a variable node receives messages emanating from its neighboring check nodes, processes these incoming messages, and subsequently transmits processed messages back to its adjacent check nodes. The iterative decoding procedure initiates at the variable nodes and terminates at the check nodes, marking a complete cycle. Furthermore, the iterative function maintains a precise one-to-one mapping with the check matrix $\boldsymbol{H}$. Once the check matrix $\boldsymbol{H}$ is established, the iterative function becomes deterministic, meaning that the decoding output is solely contingent upon the input information provided. Specifically, the decoding result is intricately tied to the initial iteration message alone. Consequently, it is imperative to first compute the initial iteration message m_i^0 for the variable nodes, serving as the foundation for initiating the iterative process.

To correct the errors between $\boldsymbol{u}$ and $\boldsymbol{v}$, equation (3) can be transformed as

$$||\boldsymbol{x}||\boldsymbol{v} - ||\boldsymbol{y}||\boldsymbol{u} = -\boldsymbol{M}(\boldsymbol{y}', \boldsymbol{u})\boldsymbol{z}. \tag{4}$$

Therefore, the condition probability $\Pr(v|u(c'))$ is given by

$$\Pr(v|u(c')) = \mathcal{K}\frac{1}{\sqrt{2\pi\sigma_z^2}}\mathrm{e}^{-\frac{(||\boldsymbol{x}||v - ||\boldsymbol{y}||u)^2}{2\sigma_z^2}}, \tag{5}$$

where $u(c') = \frac{(-1)^{c'}}{\sqrt{d}}$, $c' \in \{0,1\}$, and $\mathcal{K}$ is a normalization factor to make $\Pr(v|u(0)) + \Pr(v|u(1)) = 1$. $\Pr(u(c')|v)$ is the posterior probability, which is given by

$$\Pr(u(c')|v) = \frac{1}{1 + \mathrm{e}^{\frac{-2||\boldsymbol{x}||||\boldsymbol{y}||vu}{\sigma^2}}}. \tag{6}$$

Therefore, the initial iteration message can be calculated as

$$\begin{aligned} m_i^0 &= \ln\frac{\Pr(u_i(0)|v_i)}{\Pr(u_i(1)|v_i)} \\ &= \frac{2v_i}{\sigma_z^2}\frac{||\boldsymbol{x}||||\boldsymbol{y}||}{\sqrt{d}}, \end{aligned} \tag{7}$$

which can decide whether the multidimensional reconciliation succeeds or not.

Remark. It is evident from equation (7) that Alice needs to know the norm information including $||\boldsymbol{y}||$ and $||\boldsymbol{x}||$ when uses the traditional method to compute the initial iteration message. Since Alice does not have the norm information $||\boldsymbol{y}||$, Bob needs to send $||\boldsymbol{y}||$ to Alice for every $\boldsymbol{y}$. Furthermore, the norm information constitutes a continuous variable, necessitating its storage in the buffer as a floating-point number during implementation. Consequently, the transmission of norm information from the encoder to the decoder incurs significant consumption of communication traffic, posing an additional burden on the overall system.

3. Multidimensional reconciliation using deep learning

The better the decoding performance, the lower the FER and the higher the reconciliation efficiency. To obtain a high accuracy and decrease the communication traffic, the powerful data processing capability of the deep neural network can be used for multidimensional reconciliation in CV-QKD systems. Then, a multidimensional reconciliation scheme with deep learning assisted norm information is proposed, in which the encoder no longer needs to transmit the norm information through the authenticated classical public channel. In what follows, we will simply refer to the multidimensional reconciliation scheme with deep learning assisted norm information as the proposed deep learning scheme.

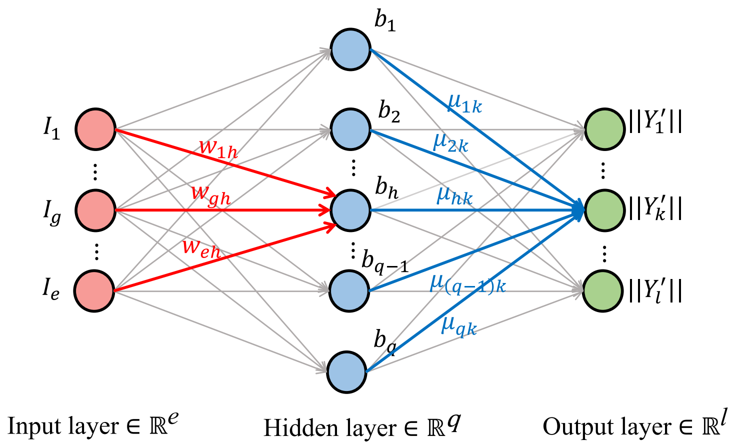

Figure 2. The structure diagram of a single hidden layer neural network.

3.1. Norm information assisted by deep neural network

The decoding initial iteration message of reverse multidimensional reconciliation directly affects the reconciliation performance. It can be inferred from equation (7) that Alice, as the decoder, requires $||\boldsymbol{x}||$, $\boldsymbol{v}$, σ_z^2, and $||\boldsymbol{y}||$ to calculate the initial iteration message. The norm information $||\boldsymbol{x}||$ of continuous variable $\boldsymbol{x}$ can be directly calculate by Alice. Then, the rotation function $\boldsymbol{M}(\boldsymbol{y}',\boldsymbol{u})$ and the norm information $||\boldsymbol{y}||$ can be transmitted from Bob to Alice through an authenticated classic public channel. The quantum channel noise variance σ_z^2 can be obtained from parameter estimation. By performing rotation operation on $\boldsymbol{x}'$, Alice obtains the estimated information $\boldsymbol{v}=\hat{\boldsymbol{u}}$. However, in the existing multidimensional reconciliation scheme, the quantum information transmission model is $\boldsymbol{y}=\boldsymbol{x}+\boldsymbol{z}$. The norm information $||\boldsymbol{y}||$ of the continuous variable $\boldsymbol{y}$ must be related to the continuous variable $\boldsymbol{x}$ transmitted by Alice and the SNR of the quantum channel. What is more, Alice needs to store the norm information $||\boldsymbol{y}||$ in the buffer until the iterative decoding finished. As the norm information is continuous variable, Alice needs much more storage resources to store it than the binary bits. Fortunately, the norm information $||\boldsymbol{y}||$ is related to $\boldsymbol{x}$, $\boldsymbol{v}$, σ_z^2 and $\boldsymbol{M}(\boldsymbol{y}',\boldsymbol{u})$. Naturally, we can think of a neural network with inputs $\boldsymbol{x}$, $\boldsymbol{v}$, σ_z^2 and $\boldsymbol{M}(\boldsymbol{y}',\boldsymbol{u})$, and the output $||\boldsymbol{y}||'$.

Deep learning refers to the method of training multi-layer neural networks, which includes the input layer, the output layer, and multiple hidden layers [42, 43]. The simplest multiple hidden layers, a three-layer network structure with only one-hidden layer is shown in figure 2. As illustrated in the figure, the layers of the neural network are fully interconnected, implying that neurons across different layers are all linked. Specifically, the neural network comprises e neurons in the input layer, q neurons in the hidden layer, and l neurons in the output layer. The vector $\boldsymbol{I}$ represents the network's inputs $\left(\boldsymbol{x};\boldsymbol{v};\sigma_z^2;\boldsymbol{M}(\boldsymbol{y}',\boldsymbol{u})\right)$. w and μ are the weight of hidden layers and the weight of output layers, respectively. g, h, and k represent the gth, hth, and kth neuron in the input layer, hidden layer, and output layer, respectively. b_h and $||\boldsymbol{y}_k||'$ are the outputs of the hth neuron in the hidden layer and the kth neuron in the output layer, respectively. Various types of activation functions serve distinct purposes. In this paper, we employ the tansig function, a prominent and frequently utilized activation function, within the hidden layers. The tansig function offers the advantage of being computable with reduced dimensionality, thereby enhancing computational efficiency. The linear activation function is frequently utilized in the output layer of neural networks tailored for regression tasks, enabling the output to encompass any continuous value within the real number domain. Therefore, the outputs corresponding to the hth neuron in the hidden layer and the kth neuron in the output layer are respectively given by

$$\begin{aligned} b_h &= f_{\text{tans}}\left(\sum_{g=1}^{e} w_{gh} I_g - \theta_h\right) \\ &= \frac{\exp\left(\sum_{g=1}^{e} w_{gh} I_g - \theta_h\right) - \exp\left(-\sum_{g=1}^{e} w_{gh} I_g + \theta_h\right)}{\exp\left(\sum_{g=1}^{e} w_{gh} I_g - \theta_h\right) + \exp\left(-\sum_{g=1}^{e} w_{gh} I_g + \theta_h\right)} \end{aligned} \quad (8)$$

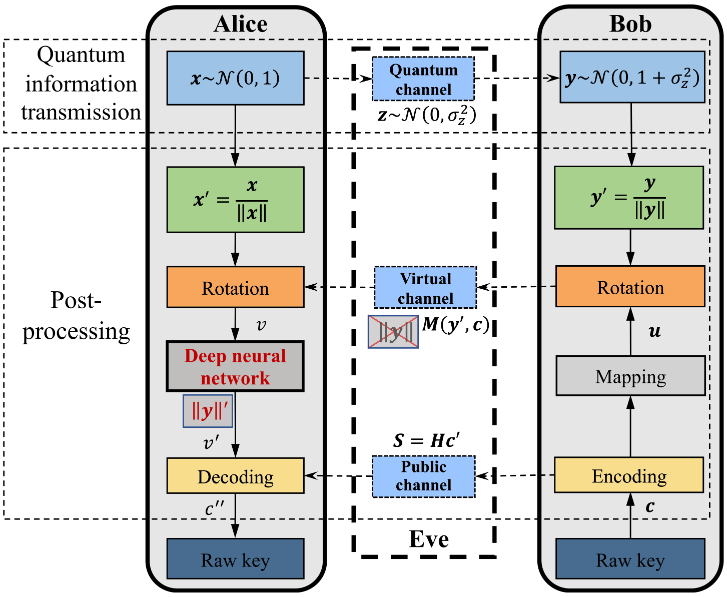
Alice
Bob
Quantum information transmission
$\boldsymbol{x}\sim\mathcal{N}(0,1)$
Quantum channel
$\boldsymbol{z}\sim\mathcal{N}(0,\sigma_z^2)$
$\boldsymbol{y}\sim\mathcal{N}(0,1+\sigma_z^2)$
Post-processing
$\boldsymbol{x}' = \frac{\boldsymbol{x}}{||\boldsymbol{x}||}$
$\boldsymbol{y}' = \frac{\boldsymbol{y}}{||\boldsymbol{y}||}$
Rotation
Virtual channel
Rotation
v
$||\boldsymbol{y}||$
$\boldsymbol{M}(\boldsymbol{y}',\boldsymbol{c})$
$\boldsymbol{u}$
Deep neural network
Mapping
$||\boldsymbol{y}||'$
v'
$\boldsymbol{S} = \boldsymbol{H}\boldsymbol{c}'$
Decoding
Public channel
Encoding
c''
$\boldsymbol{c}$
Eve
Raw key
Raw key

Figure 3. Schematic diagram of the multidimensional reconciliation scheme with deep neural network in CV-QKD.

and

$$||\boldsymbol{y}_k||' = f_{\text{line}}\left(\sum_{h=1}^{q}\mu_{hk}b_h - \theta_k\right), \tag{9}$$

where θ_h is the bias of the hth neuron in the hidden layer and θ_k is the bias of the kth neuron in the output layer.

Backpropagation neural network is currently one of the most widely used neural networks, which uses backpropagation algorithm to train the network [44]. The Levenberg–Marquardt (L–M) method is a representative backpropagation algorithm that combines the steepest descent method and Gaussian Newton method to quickly converge to the global optimal solution [45]. When the parameter estimation value of the steepest descent method is far from the optimal value at the beginning of the iteration, the L–M method has the advantage of stable descent. Additionally, the L–M method possesses the fast convergence speed characteristic of the Gaussian Newton method. After iterations, the L–M method can avoid falling into local extremes within the range of parameter estimation values close to the optimal value. The L–M method can adjust the gradient size: If the gradient descent progresses too rapidly, a smaller step size should be employed to approximate the Gaussian–Newton method; conversely, if the descent is too sluggish, a larger step size should be adopted to resemble the gradient descent method more closely. This adjustment ensures that the algorithm can promptly identify the appropriate direction and step size. Therefore, using the L–M method can more accurately find the relationship between inputs $\left(\boldsymbol{x};\boldsymbol{v};\sigma_z^2;\boldsymbol{M}(\boldsymbol{y}',\boldsymbol{u})\right)$ and the output $||\boldsymbol{y}||'$.

The mean square error (MSE) loss function is continuous and smooth at all points, making it convenient for differentiation. It can give appropriate penalty weights to gradients instead of treating them equally, which makes the direction of gradient updates more accurate and has a more stable solution. In light of the advantages of MSE, it can be used to train the network. The MSE is defined as

$$S^2 = \frac{1}{n}\sum_{k=1}^{p}\left[||\boldsymbol{y}_k||' - ||\boldsymbol{y}_k||\right]^2, \tag{10}$$

where n is the number of samples.

3.2. Multidimensional reconciliation with deep learning assisted norm information

With the assistance of norm information derived from a deep neural network, the encoder, Bob, can refrain from transmitting this norm information via the authenticated classical public channel to the decoder, Alice. In what follows, the proposed deep learning scheme which makes the initial iteration message computation free from the transmission of $||\boldsymbol{y}||$ is proposed. Considering the reverse multidimensional reconciliation process, the schematic diagram of the proposed deep learning scheme is depicted in figure 3. In the process of the proposed deep learning scheme, legitimate users also need to normalize the continuous variables $\boldsymbol{x}$ and $\boldsymbol{y}$. Then, the secret key can be transformed into a codeword $\boldsymbol{c'}$ through LDPC and the syndrome $\boldsymbol{S} = \boldsymbol{Hc'}$ will be transmitted by Bob. Subsequently, Alice and Bob execute a spherical rotation on the normalized vectors $\boldsymbol{x'}$ and $\boldsymbol{y'}$. During this spherical rotation, Bob randomly generates a spherical code u drawn from the set $\left\{\frac{-1}{\sqrt{d}}, \frac{1}{\sqrt{d}}\right\}$. Following this, Bob computes a rotation matrix $\boldsymbol{M}(\boldsymbol{y'}, \boldsymbol{u})$ such that $\boldsymbol{M}(\boldsymbol{y'}, \boldsymbol{u})\boldsymbol{y'} = \boldsymbol{u}$ and transmits the matrix $\boldsymbol{M}(\boldsymbol{y'}, \boldsymbol{u})$ to Alice. The result of the rotation operation is equation (3). To generate a close approximation to $\boldsymbol{u}$, Alice transforms equations (3) and (4). In order to be free from the transmission of $||\boldsymbol{y}||$ during calculating $-\boldsymbol{M}(\boldsymbol{y'}, \boldsymbol{u})\boldsymbol{z}$, Alice can obtain $||\boldsymbol{y}||'$ through the deep neural network. Then, the errors between $\boldsymbol{u}$ and $\boldsymbol{v'}$ can be calculated as

$$-\boldsymbol{M}(\boldsymbol{y'}, \boldsymbol{u})\boldsymbol{z} = ||\boldsymbol{x}||\boldsymbol{v'} - ||\boldsymbol{y}||'\boldsymbol{u}. \tag{11}$$

After the rotation, the output $||\boldsymbol{y}||'$ of the deep neural network can be obtained for decoding. Define M_j as the set of neighboring variable nodes associated with the jth check node, and $M_j \backslash i$ as the subset of M_j excluding the variable node i. Similarly, let N_i represent the set of neighboring check nodes linked to the ith variable node, with $N_i \backslash j$ denoting the subset of N_i that excludes the check node j. Next, Alice can compute the posterior probability $\Pr(u|v'(c))$ by equation (6) and compute m'^0_i by equation (7). Then, Alice implements the LLR-BP algorithm by substituting the received syndrome $\boldsymbol{S}$ and the initial message m'^0_i into the decoding iteration formulas as

$$r^l_{ji} = 2\tanh^{-1}\left[\left(1-2S_j\right)\prod_{i'\in M_j\backslash i}\tanh\left(\frac{m^{l-1}_{i'j}}{2}\right)\right] \tag{12}$$

and

$$m^l_{ij} = m'^0_i + \sum_{j'\in N_i\backslash j} r^l_{j'i}. \tag{13}$$

Here, $r^l_{j'i}$ represents the feedback message conveyed from the check node j' to the variable node i during the lth iteration, whereas m^l_{ij} signifies the message passed from the variable node i to the check node j in the same iteration. Additionally, m'^0_i represents the initial iteration message of the variable node i, which is computed utilizing norm information assisted by deep learning techniques. Following the completion of these iterations, each variable node decodes its associated bits by relying on all the information received from its neighboring check nodes,

$$m^l_i = m'^0_i + \sum_{j\in N_i} r^l_{ji}. \tag{14}$$

The decoding result of $c_i^{''}$ is

$$c_i^{''} = \begin{cases} 0, & m^l_i \geqslant 0 \\ 1, & m^l_i < 0, \end{cases} \tag{15}$$

and the iteration process terminates when the decoding result $\boldsymbol{c}''$ satisfies $\boldsymbol{Hc}'' = \boldsymbol{S}$ or when the maximum number of iterations has been reached.

4. Simulation and performance analysis

In this section, comparative simulation experiments are performed to analyze the performance of the proposed deep learning scheme. First, the network training strategy of the proposed deep learning scheme is provided. Subsequently, the performance analysis of the proposed deep learning scheme, including the comparing communication traffic and FER of different schemes are carried out. Finally, the reconciliation efficiency and secret key rate of the proposed deep learning scheme in CV-QKD systems are calculated and compared with that of the traditional multidimensional reconciliation schemes and the scheme proposed in [41]. In the simulations, we set $d = 8$ and apply the Advanced Television Systems Committee LDPC (ATSC-LDPC) codes to multidimensional reconciliation.

Table 1. Training samples.

Code rate R	SNRs									
2/15	0.20	0.21	0.22	0.23	0.24	0.25	0.26	0.27	0.28	0.29
5/15	0.70	0.71	0.72	0.73	0.74	0.75	0.76	0.77	0.78	0.79

Table 2. The network training settings.

Items	Settings
Epochs	1000
Network learning rate	0.01
Training goal	0.00 001
Data division	Random
Training algorithm	L–M

4.1. Network training strategy

In the existing schemes, Alice is required to store the norm information $||\boldsymbol{y}||$ of the continuous variable $\boldsymbol{y}$ in a buffer throughout the entire iterative decoding process. Notably, the norm information, being a continuous variable, occupies significantly more storage resources compared to binary bits. In our proposed deep learning scheme, Bob is no longer needed to transmit the norm information $||\boldsymbol{y}||$, leading to a substantial reduction in classical communication traffic and consequently, a notable savings in the secure key utilized for authentication purposes. Furthermore, Alice can significantly conserve storage resources, which contributes to the achievement of a high-speed CV-QKD system.

During the training iterations, the network continuously reduces the MSE value until the error reaches the expected value or the training frequency reaches the set maximum training frequency before stopping learning. Then, the trained neural network is saved for predicting the norm information in multidimensional reconciliation. In the iterative learning process of backpropagation neural network, the training data needs to be obtained first: the norm information of continuous variable $\boldsymbol{x}$ generated by Alice, the noise variance of the quantum channel σ_z^2, the rotation matrix $\boldsymbol{M}(\boldsymbol{y'},\boldsymbol{u})$, and the noisy information $\boldsymbol{v}$ are as feature attributes. The norm information of continuous variable $\boldsymbol{y}$ is the objective function. Since the CV-QKD system operates in extremely low SNR environments, it is necessary to use error-correcting codes with lower rates in multidimensional reconciliation to generate training data. In general, the rate of the error-correcting code used is not greater than 1/3 [46]. In addition, as the diversity of training samples is conducive to improving the universality of the neural network, the 16200 ATSC-LDPC codes under code rates 2/15 and 5/15 are generated as sample data to meet the channel diversity. The SNRs for training samples under code rates 2/15 and 5/15 are listed in table 1. Theoretically, several sets of different sample inputs I and the corresponding sample labels $||\boldsymbol{y}||$ can be obtained through the sample data. Finally, the samples are selected randomly from different SNRs to form a batch of samples.

In the proposed deep learning scheme, the length of each frame is set as 16 200, and 10 frames of data are generated for each SNR to train. Due to a total of 20 SNRs under two code rates, a total of 3240 000 data are generated for each feature attribute. In the simulation, we divide the total information into three parts: 70% training sample, 15% validation sample, and 15% test sample. Therefore, the training sample size for each feature input and output is 2268 000, each test sample size is 486 000, and each validation sample size is 486 000.

Based on the analysis of the basic principles of neural networks in the L–M algorithm, a neural network for predicting the norm $||\boldsymbol{y}||$ can be established. In terms of other settings for network training, the data division is random. Table 2 illustrates the neural network training setting.

4.2. Performance analysis of the proposed deep learning scheme

For the correlated raw key with length N in multidimensional reconciliation, the code rate is R, the dimension of the multidimensional reconciliation is d, and the size of the floating point number is f. In the traditional multidimensional reconciliation scheme, Bob needs to send the syndrome with size $(1-R)N$, rotation matrix $\boldsymbol{M}(\boldsymbol{y'},\boldsymbol{u})$ with size dfN, and norm information with size Nf/d. When Alice and Bob perform the multidimensional reconciliation once, the size of reconciliation data in the traditional multidimensional reconciliation scheme is

$$\begin{aligned} D_{\mathrm{t}} &= m+\frac{N}{d}\times d\times d\times f+\frac{N}{d}\times f \\ &= (1-R)N+dfN+\frac{Nf}{d}, \end{aligned} \tag{16}$$

Table 3. The size of reconciliation data in the traditional multidimensional reconciliation scheme, the proposed deep learning scheme and the scheme proposed in [41].

Code rates R	D_t	D_deep	$D_{[41]}$	$D_\text{t} - D_\text{deep}$	$\frac{D_\text{t}-D_\text{deep}}{D_\text{t}}$
2/15	4226 040	4161 240	416 1240	64 800	1.5334%
5/15	4222 800	4158 000	4158 000	64 800	1.5345%

while the size of reconciliation data in both the proposed deep learning scheme and the scheme proposed in [41] is

$$\begin{aligned} D_\text{deep} &= m + \frac{N}{d} \times d \times d \times f \\ &= (1-R)N + dfN. \end{aligned} \tag{17}$$

In comparison of equations (16) and (17), not only the traffic of the scheme proposed in [41] is $\frac{Nf}{d}$ less than the traditional multidimensional reconciliation scheme, but also our proposed deep learning scheme is $\frac{Nf}{d}$ less than the traditional multidimensional reconciliation scheme.

The length of each frame is set as 16200, and the size of a floating-point number is 32. Table 3 shows the size of reconciliation data D_t and D_deep in the traditional multidimensional reconciliation scheme and the proposed deep learning scheme, respectively. Compared with the traditional multidimensional reconciliation scheme, the proposed deep learning scheme can reduce 1.5334% and 1.5345% reconciliation data under code rate 2/15 and 5/15, respectively.

As we all know, the expression for the realistic secret key rate of a CV-QKD system can be expressed as

$$K = (1 - P_e)(\beta I_\text{AB} - \chi_\text{BE}). \tag{18}$$

where P_e is FER. If the error-correcting fails, the entire frame will be discarded. β is the reconciliation efficiency, and it can be calculated by $\beta = R/C$. R and C are the code rate of the error-correcting code and channel capacity, respectively. I_AB represents the mutual information shared by Alice and Bob, while χ_BE is the upper bound of the information and attacker Eve could have obtained (the so-called Holevo bound) [47, 48]. According to equation (18), FER is one of the main factors limiting the secret key rate [49].

We simulate the FERs of the traditional multidimensional reconciliation scheme [8], the proposed deep learning scheme, and the scheme proposed in [41] under code rates 2/15 and 5/15. Figures 4 and 5 show the FER of different multidimensional reconciliation schemes under code rates 2/15 and 5/15, respectively. It can be observed that the performance of the proposed deep learning scheme is close to that of the traditional multidimensional reconciliation scheme and better than the scheme proposed in [41]. The simulation results demonstrates that the proposed deep learning scheme is feasible in CV-QKD. The reason for this result is that a more accurate estimation of ||y|| leads to a more reliable initial message, which can improve the convergence of the LLR-BP decoding algorithm. In turn, the improvement of LLR-BP decoding algorithm reduces the likelihood of decoding errors and results in a lower FER. Furthermore, it has been proven that the proposed deep learning scheme can be effectively applied to channels with varying SNRs, showcasing its robust versatility and adaptability.

4.3. Reconciliation efficiency and secret key rate

From equation (18), it is evident that, for a specified FER, achieving a high secret key rate necessitates maximizing the reconciliation efficiency. For a given FER $= 0.9$ [50], the reconciliation efficiency of different schemes under code rates 2/15 and 5/15 are listed in table 4. Here, the subscripts t, deep, and [41] denote the traditional multidimensional scheme, the proposed deep learning scheme, and the scheme proposed in [41], respectively. The reconciliation efficiencies of the proposed deep learning scheme are higher than that of the scheme proposed in [41].

Then, relationships between the secret key rate and the transmission distance with various reconciliation efficiencies are shown in figures 6 and 7. Compared with the scheme proposed in [41] which also no longer requires the norm information from Bob, the secret key rate and the transmission distance of the proposed deep learning scheme are better.

In conclusion, the simulation results and their corresponding analyses demonstrate that the proposed deep learning scheme can significantly reduce communication traffic and storage resources, while maintaining nearly the same level of reconciliation efficiency as compared to the existing traditional multidimensional reconciliation schemes. What is more, simulation results show that the FER, reconciliation efficiency and secret key rate of the proposed deep learning scheme are superior to that of the scheme proposed in [41].

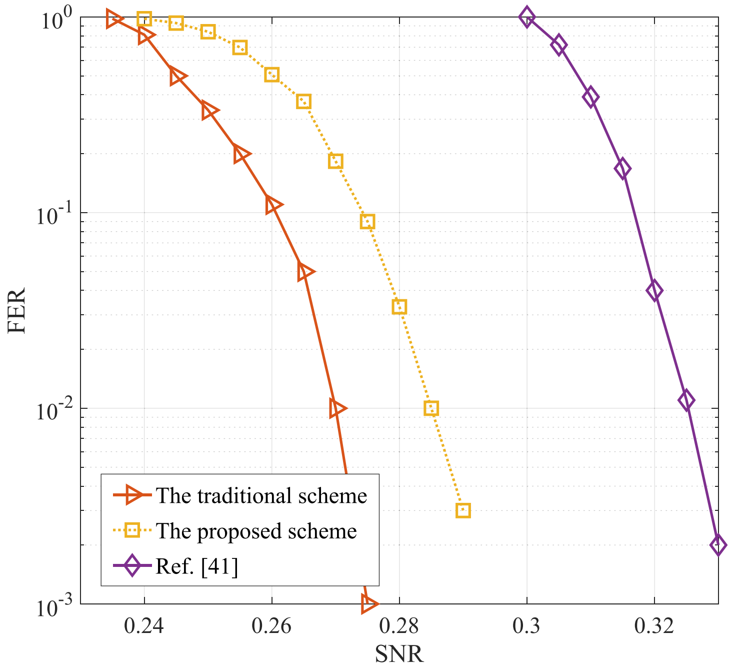

Figure 4. FER of different schemes under code rate 2/15.

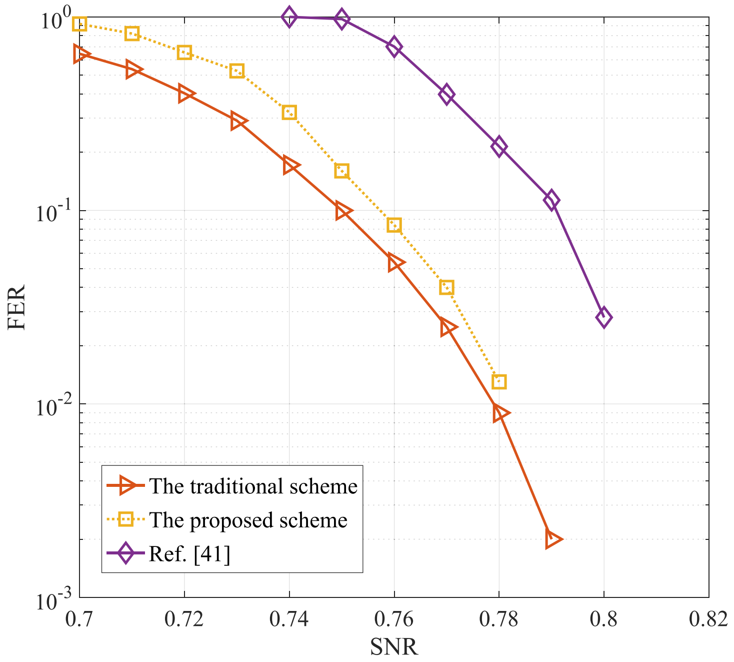

Figure 5. FER of the different schemes under code rate 5/15.

Table 4. Reconciliation efficiencies of the traditional multidimensional reconciliation scheme, the proposed deep learning scheme and the scheme proposed in [41] under different code rates.

FER = 0.9			
R	β_{t}	β_{deep}	β [41]
2/15	86.9%	84.1%	70.2%
5/15	88.6%	87.0%	82.4%

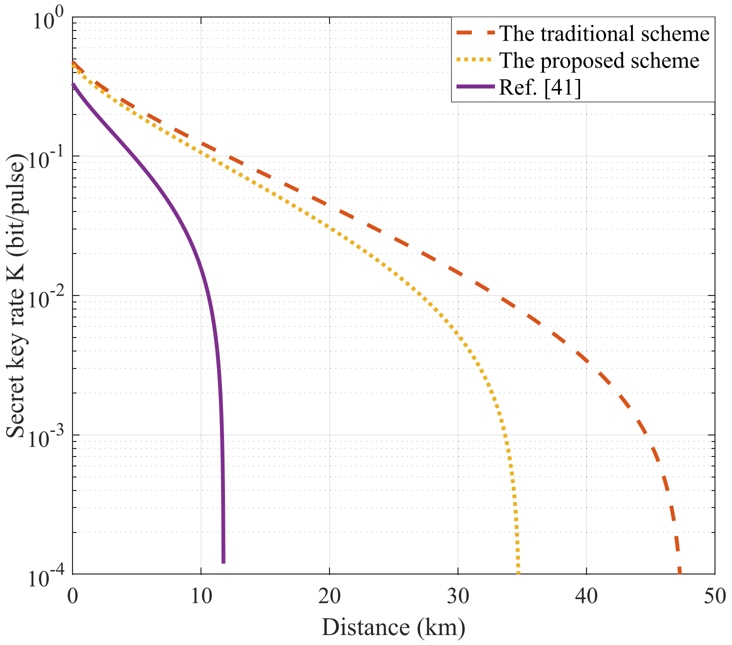

Figure 6. Secret key rate with respect to transmission distance under code rate 2/15. The parameters of the CV-QKD systems are as follows: excess noise $\xi = 0.001$, detection efficiency $\kappa = 0.9$, electronic noise $V_{\rm el} = 0.005$, and the attenuation factor of the quantum channel $\varphi = 0.2$ dB km^{-1}.

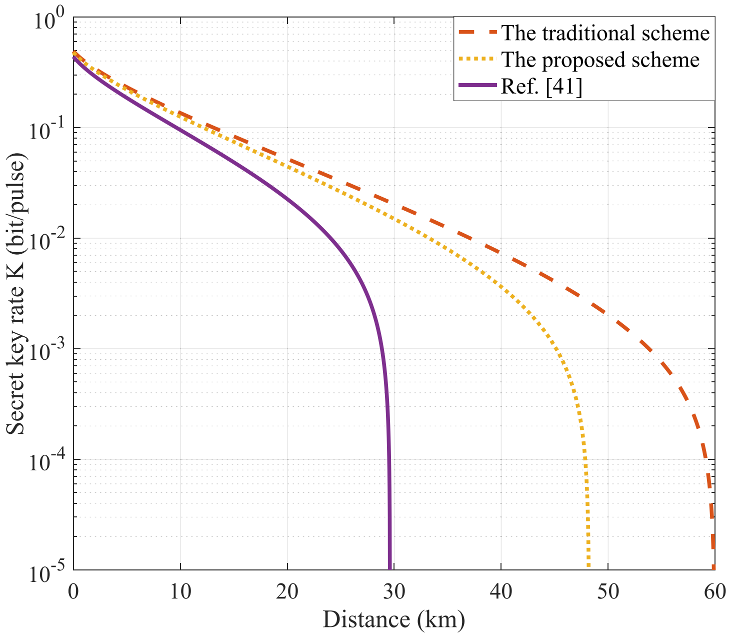

Figure 7. Secret key rate with respect to transmission distance under code rate 5/15. The parameters of the CV-QKD systems are as follows: excess noise $\xi = 0.001$, detection efficiency $\kappa = 0.9$, electronic noise $V_{\rm el} = 0.005$, and the attenuation factor of the quantum channel $\varphi = 0.2$ dB km^{-1}.

5. Conclusion

In this paper, the deep learning scheme was proposed to decrease the communication traffic and storage resources of the CV-QKD system. Both theoretical analysis and simulation results have unequivocally shown that the proposed deep learning scheme can substantially reduce communication traffic and storage resources, while experiencing virtually no degradation in reconciliation efficiency when compared to existing representative multidimensional reconciliation schemes. Compared with the scheme proposed in [41], which similarly eliminates the need for norm information from Bob, the proposed deep learning scheme achieves even higher reconciliation efficiency. Furthermore, by reducing the consumption of secure keys for authentication, the proposed deep learning scheme also enhances the secret key rate, thus facilitating the implementation of high-speed CV-QKD systems.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

This project is supported by the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300703), the Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), the State Key Laboratory of Advanced Optical Communication Systems and Networks (Grant No. 2024GZKF006), the Fundamental Research Funds for the Central Universities (Grant No. 2232023D-27), and Shanghai Pujiang Program (Grant No. 23PJ1400300).

ORCID iDs

Yan Feng https://orcid.org/0000-0002-0417-7191
Jiangliang Jin https://orcid.org/0000-0003-0077-8624
Kun Zhang https://orcid.org/0000-0002-4077-5922
Xue-Qin Jiang https://orcid.org/0000-0002-0414-4349
Peng Huang https://orcid.org/0000-0003-1449-1499

References

[1] Bennett C and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Comput. Syst. Signal* 175–9
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145
[3] Zhang H, Ji Z, Wang H and Wu W 2019 Survey on quantum information security *China Commun.* **16** 1–36
[4] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301
[5] Wang C, Huang P, Huang D, Lin D and Zeng G 2016 Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects *Phys. Rev. A* **93** 22315
[6] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[7] Braunstein S and Van Loock P 2006 Quantum information with continuous variables *Rev. Mod. Phys.* **77** 513
[8] Asp H, Bengtsson B and Jensen P 2011 Long distance continuous-variable quantum key distribution with a Gaussian modulation *Phys. Rev. A* **84** 6
[9] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Experimental demonstration of long-distance continuous-variable quantum key distribution *Nat. Photon.* **7** 378
[10] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S, Lloyd S, Gehring T, Christian S and Andersen U 2015 High-rate measurement-device-independent quantum cryptography *Nat. Photon.* **9** 6
[11] Zhou S, Xie Q and Zhou N 2024 Measurement-free mediated semi-quantum key distribution protocol based on single-particle states *Laser Phys. Lett.* **21** 6
[12] Liu Y *et al* 2023 Experimental twin-field quantum key distribution over 1000 km fiber distance *Phys. Rev. Lett.* **130** 210801
[13] Zhou L, Lin J, Jing Y and Yuan Z 2023 Twin-field quantum key distribution without optical frequency dissemination *Nat. Commun.* **14** 928
[14] Zhang M, Huang P, Wang P, Wei S and Zeng G 2023 Experimental free-space continuous-variable quantum key distribution with thermal source *Opt. Lett.* **48** 1184
[15] Chen Z, Wang X, Yu S, Li Z and Guo H 2023 *npj Quantum Inf.* **9** 28
[16] Bian Y, Pan Y, Xu X, Zhao L, Li Y, Huang W, Zhang L, Yu S, Zhang Y and Xu B 2024 Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip *Appl. Phys. Lett.* **124** 174001
[17] Zhang Y, Bian Y, Li Z, Yu S and Guo H 2024 Continuous-variable quantum key distribution system: past, present and future *Phys. Rev.* **11** 011318
[18] Li P-Z and Loock P 2023 Memoryless quantum repeaters based on cavity-QED and coherent states *Adv. Quantum Technol.* **6** 8
[19] Li P-Z, Dias J, Munro W J, Loock P, Nemoto K and Piparo N 2024 Performance of rotation-symmetric bosonic codes in a quantum repeater networ *Adv. Quantum Technol.* **7** 6
[20] Li L, Wang T, Li X, Huang P, Guo Y, Lu L, Zhou L and Zeng G 2023 *Photon. Res.* **11** 4
[21] Assche G, Cardinal J and Cerf N 2004 Reconciliation of a quantum-distributed Gaussian key *IEEE Trans. Inf. Theor.* **50** 394
[22] Bennett C, Brassard G, Crepeau C and Maurer U 1995 Generalized privacy amplification *IEEE Trans. Inf. Theor.* **41** 1915
[23] Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S and Guo H 2020 Long-distance continuous-variable quantum key distribution over 202.81 km of fiber *Phys. Rev. Lett.* **125** 010502
[24] Bai Z, Wang X and Yang S 2016 High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution *Sci. China Phys. Mech. Astron.* **59** 614201
[25] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 Multidimensional reconciliation for a continuous-variable quantum key distribution *Phys. Rev. A* **77** 042325
[26] Wen X, Li Q, Mao H, Wen X J and Chen N 2021 An improved slice reconciliation protocol for continuous-variable quantum key distribution *Entropy* **23** 1317

[27] Feng Y, Wang Y-J, Qiu R, Ge H, Shan Z and Jiang X-Q 2021 Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution *Phys. Rev. A* **103** 3

[28] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states *Phys. Rev. Lett.* **88** 057902

[29] Silberhorn C, Ralph T, Lutkenhaus N and Leuchs G 2002 Continuous variable quantum cryptography-beating the 3 dB loss limit *Phys. Rev. Lett.* **89** 16

[30] Zhou Y, Jiang X-Q, Liu W, Wang T, Huang P and Zeng G 2018 Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation *Chin. Phys. B* **27** 5

[31] Laudenbac F, Pacher C, Fung C, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P and Hübel H 2018 Continuous-variable quantum key distribution with Gaussian modulation - the theory of practical implementation *Adv. Quantum Technol.* **10** 1800011

[32] Lin D, Huang D, Huang P, Peng J and Zeng G 2016 High performance reconciliation for continuous-variable quantum key distribution with LDPC code *Int. J. Quantum Inf.* **13** 1550010

[33] Zhao S, Shen Z, Xiao H and Wang L 2018 Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding *Sci. China Phys. Mech. Astron.* **61** 09

[34] Wang X, Zhang Y, Yu S and Guo H 2018 High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code *Sci. Rep.* **8** 10543

[35] Zhou C, Wang X, Zhang Z, Yu S, Chen Z and Guo H 2021 Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes *Sci. China Phys. Mech. Astron.* **64** 6

[36] Fan X, Niu Q, Zhao T and Guo B 2022 Rate-compatible LDPC codes for continuous-variable quantum key distribution in wide range of SNRs regime *Entropy* **24** 1463

[37] Yang H, Liu S, Yang S, Lu Z, Li Y and Li Y 2024 High-efficiency rate-adaptive reconciliation in continuous-variable quantum key distribution *Phys. Rev. A* **109** 1

[38] Jiang X-Q, Xue S, Tang J, Huang P and Zeng G 2024 Low-complexity adaptive reconciliation protocol for continuous-variable quantum key distribution *Quantum Sci. Technol.* **9** 2

[39] Walenta N, Burg A, Caselunghe D, Constantin J, Gisin N, Guinnard O, Houlmann R, Junod P, Korzh B and Kulesza N 2014 A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing *New J. Phys.* **16** 1

[40] Mao H, Li Q, Han Q and Guo H 2019 High-throughput and low-cost LDPC reconciliation for quantum key distribution *Quantum Inf. Process.* **18** 232

[41] Li Q, Wen X, Mao H and Wen X 2019 An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution *Quantum Inf. Process.* **18** 1

[42] Hinton G, Osindero S and Teh Y-W 2006 A fast learning algorithm for deep belief nets *Neural Comput.* **18** 1527

[43] Gong L, Ding W, Li Z, Wang Y and Zhou N 2024 Quantum k-nearest neighbor classification algorithm via a divide and conquer strategy *Adv. Quantum Technol.* **7** 6

[44] Liang F, Shen C and Wu F 2018 An iterative BP-CNN architecture for channel decoding *IEEE J. Sel. Top. Signal Process.* **12** 144

[45] Ranganathan A 2004 The Levenberg-Marquardt algorithm

[46] Zhang K, Jiang X-Q, Feng Y, Qiu R and Bai E 2020 High efficiency continuous-variable quantum key distribution based on ATSC 3.0 LDPC codes *Entropy* **22** 1087

[47] Lodewyck J *et al* 2007 Quantum key distribution over 25 km with an all-fiber continuous-variable system *Phys. Rev. A* **76** 538

[48] Huang P, Wang T, Chen R, Wang P, Zhou Y and Zeng G 2021 Experimental continuous-variable quantum key distribution using a thermal source *New J. Phys.* **23** 113028

[49] Yang S, Yan Z, Yang H, Lu Q, Lu Z, Chen L, Miao X and Li Y 2023 Information reconciliation of continuous-variables quantum key distribution: principles, implementations and applications *EPJ Quantum Technol.* **10** 1

[50] Johnson S, Lance A, Ong L, Shirvanimoghaddam M, Ralph T C and Symul T 2017 On the problem of non-zero word error rates for fixed-rate error correction codes in continuous variable quantum key distribution *New J. Phys.* **19** 023003