



# Information reconciliation of continuous-variables quantum key distribution: principles, implementations and applications

Shenshen Yang<sup>1</sup>, Zhilei Yan<sup>1</sup>, Hongzhao Yang<sup>2,3</sup>, Qing Lu<sup>2,3</sup>, Zhenguo Lu<sup>2,3</sup>, Liuyong Cheng<sup>1</sup>, Xiangyang Miao<sup>1\*</sup> and Yongmin Li<sup>2,3,4\*</sup>

\*Correspondence:

[sxymiao@126.com](mailto:sxymiao@126.com);  
[yongmin@sxu.edu.cn](mailto:yongmin@sxu.edu.cn)

<sup>1</sup>College of Physics and Information Engineering, Shanxi Normal University, Taiyu Road, Taiyuan, 030031, Shanxi, China

<sup>2</sup>State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Wucheng Road, Taiyuan, 030006, Shanxi, China

Full list of author information is available at the end of the article

## Abstract

Quantum key distribution (QKD) can provide information-theoretically secure keys for two parties of legitimate communication, and information reconciliation, as an indispensable component of QKD systems, can correct errors present in raw keys based on error-correcting codes. In this paper, we first describe the basic knowledge of information reconciliation and its impact on continuous variable QKD. Then we introduce the information schemes and the corresponding error correction codes employed. Next, we introduce the rate-compatible codes, the hardware acceleration of the reconciliation algorithm, the research progress of information reconciliation, and its application in continuous variable QKD. Finally, we discuss the future challenges and conclude.

**Keywords:** Quantum key distribution (QKD); Continuous-variable; Information reconciliation; Error correction codes; Hardware acceleration; Rate-adaptive

## 1 Introduction

Quantum key distribution (QKD) [1–9] allows legitimate parties, Alice and Bob, to share secure keys through an insecure quantum channel. The fundamental theorems of the quantum physics guarantee that non-orthogonal quantum states transmit through a quantum channel cannot be replicated accurately. Furthermore, any measurements trying to discriminate the non-orthogonal quantum states will inevitably disturb them. Therefore, any eavesdropping behaviors against on QKD can be discovered.

According to the different carriers of the key, QKD can be divided into discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD) [10–14]. DV-QKD uses the polarization or phase of single photons to encode the key information, which can realize long-distance key distribution by using single photon detection technology. CV-QKD employs the quadrature components of quantum states to encode the key information, it is

© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

compatible with the existing coherent optical communication technology and can achieve high key rate in short and medium distance.

The first concept of CV-QKD was proposed in 1999 [15]. The Gaussian-modulated coherent states protocol was proposed in 2002 (GG02 protocol) [16] and experimentally verified in 2003 [17]. So far, a series of important advances have been reported in protocol design, experiment implementation, security analysis and field test. Novel theoretical protocols [18–23] are designed, security proofs are constantly improving [24–31], experiments [32–40] are gradually moving from proof-of-principle lab demonstrations to prototypes and in-field implementations. The transmission distance and the secret key rate (SKR) of systems continue to improve. The point-to-point transmission reaches 202.81 km of ultralow-loss optical fiber [33]. Measurement-device-independent CV-QKD has been successfully verified [19, 37]. Recently, some research teams have tried to integrate the sender and receiver of CV-QKD on silicon photonic chips [41–44]. Furthermore, the feasibility of establishing secure satellite-to-ground CV-QKD links is investigated [45, 46].

A typical CV-QKD system usually consists of four parts [11]: (1) Preparation, distribution and measurement of quantum states; (2) Key sifting and parameter estimation; (3) Information reconciliation (IR); and (4) Privacy amplification (PA). In the IR stage, Alice and Bob obtain the identical bit strings by correcting errors between their raw keys. As an indispensable step in CV-QKD system, IR must be able to match or surpass the clock rate of the system. However, the IR of CV-QKD is relatively complicated because it usually works at a low signal-to-noise ratio (SNR) regime, and digital signal processing technologies sometimes need to be introduced to improve the SNR [23, 47]. An overview of IR in DV-QKD has been presented in [48]. In this paper, we review the IR of CV-QKD including its principles, implementations, and applications.

The rest of the paper is organized as follows. In Sect. 2, we provide basic knowledge of IR and discuss the impact of IR performance on the CV-QKD system. It follows a summary of relevant reconciliation protocols, including slice reconciliation, multidimensional reconciliation, and other improved protocols in Sect. 3. In Sect. 4, we review the error correction codes (ECCs) that are used in IR, including low-density parity-check (LDPC) codes, polar codes, Raptor codes, and spinal codes. Section 5 presents the improvement of IR throughput based on hardware, such as field-programmable gate array (FPGA) or graphics processing unit (GPU). Next, we present the research progress of IR in Sect. 6. The typical applications of IR in CV-QKD systems are discussed in Sect. 7. In Sect. 8, we discuss the current challenges of IR. Finally, we give a conclusion in Sect. 9.

## 2 Preliminaries

In QKD, inconsistencies inevitably exist in the raw keys obtained by communication parties due to the noises and attenuation in quantum channel and the noises of quantum states themselves. The aim of IR is to share a set of completely consistent key bits by using classical ECCs for Alice and Bob.

### 2.1 Performance parameters of IR

The two most critical parameters of QKD are SKR and transmission distance, respectively. The multiple parameters of IR significantly affect the performance of QKD. Table 1 lists the three key parameters used for evaluating IR's performance. They are reconciliation efficiency ( $\beta$ ), frame error rate ( $FER$ ), and throughput ( $T$ ).

**Table 1** Key parameters used for evaluating IR performance

	Parameter	Symbol
1	Reconciliation efficiency	$\beta$
2	Frame error rate	$FER$
3	Throughput	$T$

The reconciliation efficiency  $\beta$  is the most important parameter for evaluating the quality of a key reconciliation scheme. Reconciliation efficiency is used to characterize the efficiency of the error correction. Throughput  $T$  tells the number of raw keys processed per unit of time. Notice that fast IR with throughput no less than the system clock rate is the prerequisite of a real-time QKD. Hardware acceleration, such as FPGA or GPU, can be used to improve the throughput. When ECCs are used for IR, they are carried out in the unit of code blocks, which is called a “frame”. The raw keys usually need to be divided into a series of frame and decoded. The FER represents the failure probability of IR. Obviously, the lower the FER, the better.

### 2.2 Effects of IR on CV-QKD systems

Ideally, the asymptotic SKR of CV-QKD systems can be expressed as:

$$K_{ideal} = I_{AB} - \chi_{BE}, \tag{1}$$

where  $I_{AB}$  is the Shannon mutual information between Alice and Bob,  $\chi_{BE}$  is the Holevo bound.

Considering the realistic reconciliation efficiency, FER, and throughput, the SKR of the CV-QKD system can be expressed as:

$$K_{prac} = \gamma(1 - FER)(\beta I_{AB} - \chi_{BE}), \tag{2}$$

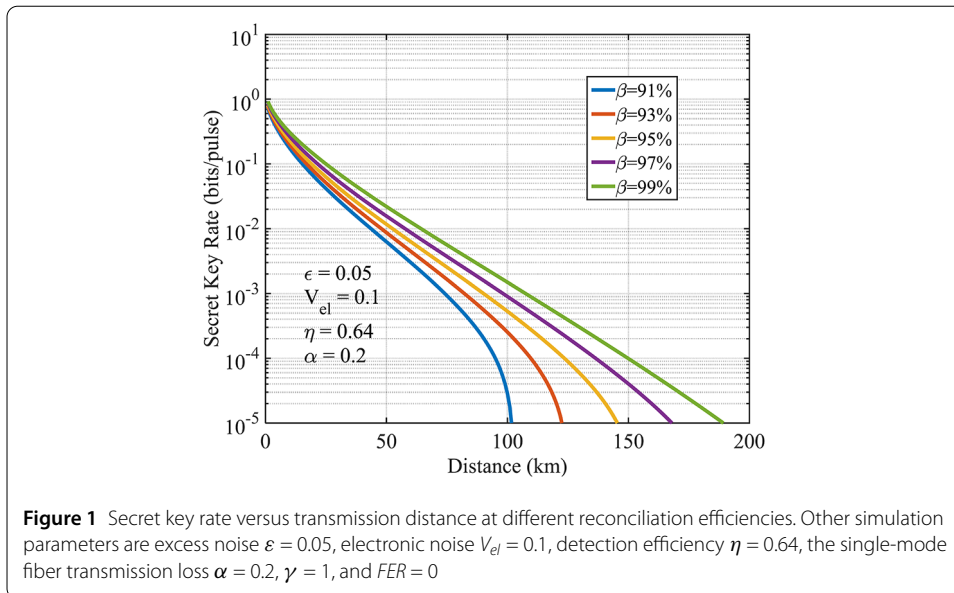
where  $\gamma = PP_{out}/PP_{in}$ ,  $PP_{out}$  and  $PP_{in}$  represent the post-processing (include IR and PA) output and input rates, respectively. The value of  $PP_{out}$  determines the maximum QKD clock rate that the post-processing can support and  $\gamma$  satisfies  $0 \leq \gamma \leq 1$ . When the speed of the post-processing is greater than or equal to the generation speed of the raw keys,  $\gamma = 1$ , that is, the raw keys can be fully utilized. The real throughput of IR will change the value of  $\gamma = PP_{out}/PP_{in}$ , and ultimately affects the SKR.

Figure 1 shows the SKR as a function of the transmission distance (standard single-mode fiber channel with loss of 0.2 dB/km) at different reconciliation efficiencies (91%-99%). As can be seen from Fig. 1, the higher the reconciliation efficiency, the farther the transmission distance. Given the transmission distance, higher reconciliation efficiency enables higher key rate.

When further consider the finite raw keys and consumed raw keys for parameter estimation, the practical secret key rate of the QKD system is given by [49]:

$$K_{prac} = \gamma(1 - FER) \left( \frac{n}{N} \right) (\beta I_{AB} - \chi_{BE} - \Delta(n)), \tag{3}$$

where  $n$  is the number of raw keys used to distill the secret key.  $N$  is the number of sifted raw keys after quantum transmission and measurement.  $\Delta(n)$  is the finite-size offset factor.



### 2.3 Direct and reverse reconciliation

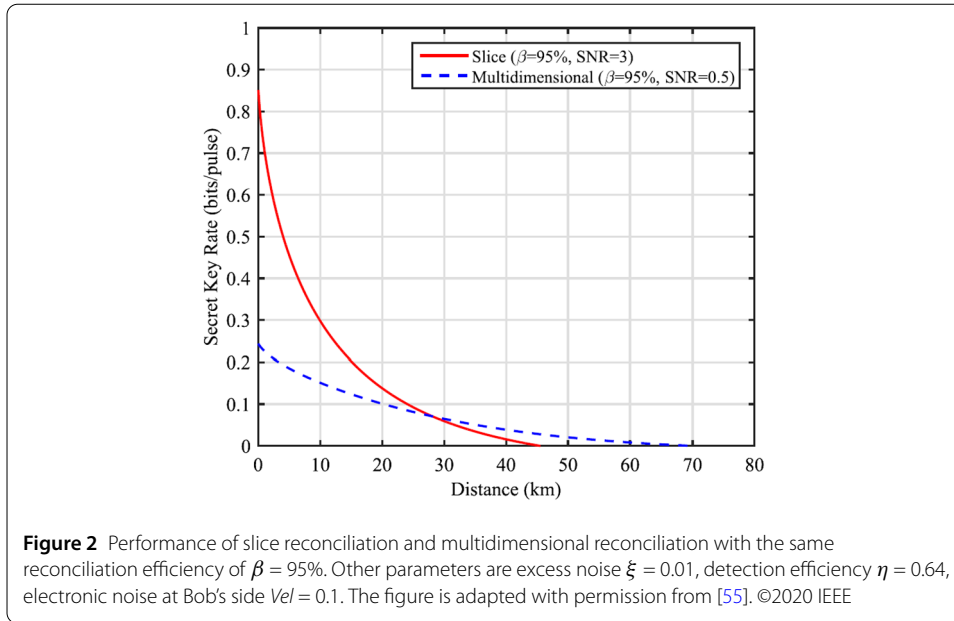
A CV-QKD system can be implemented in direct reconciliation (DR) or reverse reconciliation (RR), which have different performances. For DR, Alice sends the redundant information required for error correction to Bob, so that Bob can correct the errors of his data using the received information and obtain a bit string that is exactly the same as that of Alice. The ideal key rate of DR can be expressed as  $I_{AB} - \chi_{AE}$ . However, when the transmittance of the quantum channel is less than 1/2, it results in the inability to generate a secure key. For example, Eve can simulate a loss channel with a beam splitter and split the light emitted by Alice into two beams, then she keeping the larger part and sending the smaller part to Bob. In this case, Eve being able to extract more key information than Bob, which hinders legitimate parties to generate a secure key, called the 3 dB loss limit [50].

Two ways have been proposed to overcome the 3 dB limit, namely RR and post-selection, respectively. For RR, Bob’s raw keys is used as the benchmark, and he sends the information required for error correction to Alice, who correct her bit string to be the same as Bob’s bit string. The ideal SKR of RR can be expressed as  $I_{AB} - \chi_{BE}$ . RR can dramatically extend the transmission distance and generate security keys over longer distances, thus becoming a dominant scheme.

### 3 Reconciliation schemes

In CV-QKD systems, Alice and Bob obtain a set of correlated raw keys  $\mathbf{X}$  and  $\mathbf{Y}$  after the quantum states preparation, measurement, and key sifting phases. For Guassian modulated CV-QKD protocols, the raw keys are Gaussian variables.

Several schemes have been proposed for IR of Gaussian symbols, such as slice reconciliation [51], multidimensional reconciliation [52], sign reconciliation [50], and so on [53, 54], each scheme covers a certain range of SNRs. As shown in Fig. 2, the slice reconciliation is suitable for relatively high SNR of larger than 1 (short transmission distance), and the multidimensional reconciliation is suitable for low SNR from 0.01 to 1 (long transmission distance).



### 3.1 Slice reconciliation

The slice reconciliation was first proposed in 2004 [51]. It can correct the errors of Gaussian symbols using binary ECCs. For reverse reconciliation, Bob uses the quantizing function  $Q : \mathbb{R} \rightarrow \{0, 1\}^m$  to transform each Gaussian variable  $Y_i$  into an  $m$ -bit label  $\{B_j(Y_i)\}, j = 1, \dots, m$ . Next, Bob uses multi-level encoding (MLE) that encodes each individual level  $j$  of the label bits independently as the syndrome of an error correcting code with rate  $R_j (1 \leq j \leq m)$ . To recover Bob's  $m$ -bit label  $\{B_j\}$ , Alice employs multi-stage decoding (MSD) and uses her own source  $\mathbf{X}$  as side information. Finally, the two parties share identical keys. The principle of slice reconciliation is shown in Fig. 3(a).

To transform a Gaussian variable into a binary sequence, the real number axis is divided into a number of intervals and then a proper mapping is performed for the sliced Gaussian variables as shown in Fig. 3(c). The quantization efficiency of the Bob's Gaussian variables can be expressed as:

$$\beta_{\text{slice}} = \frac{I(X; Q(Y))}{I(X; Y)}, \tag{4}$$

where  $Q(Y)$  is the quantified Gaussian variable, and  $I(X; Y)$  is the mutual information between Alice and Bob. The quantization efficiency versus SNR for the optimal interval quantization and equal interval quantization is shown in Fig. 3(b).

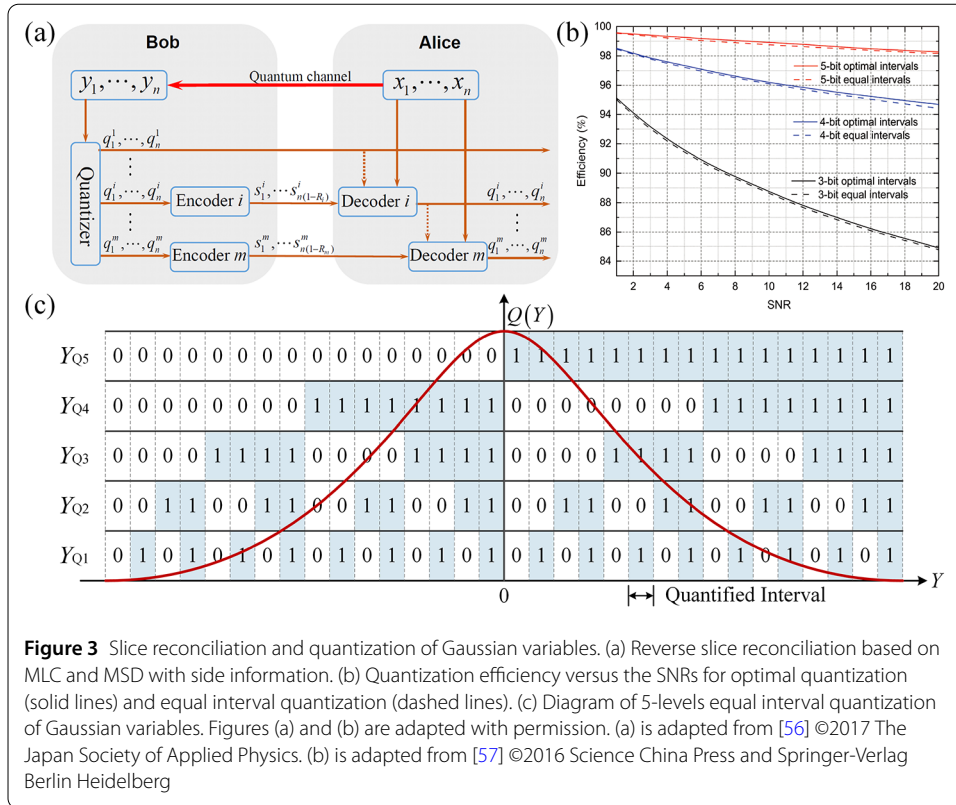
The mutual information  $I(X; Q(Y))$  can be expressed as:

$$I(X; Q(Y)) = H(X) + H(Q(Y)) - H(X, Q(Y)). \tag{5}$$

The terms on the rightside of Eq. (5) are defined as follows:

$$H(X) = \frac{1}{2} \log_2 2\pi \Sigma^2,$$

$$H(Q(Y)) = - \sum_a (P_a \log_2 P_a),$$



$$P_a = \frac{1}{2} \left( \operatorname{erf} \left( \frac{t_a}{\sqrt{2(\Sigma^2 + \sigma^2)}} \right) - \operatorname{erf} \left( \frac{t_{a-1}}{\sqrt{2(\Sigma^2 + \sigma^2)}} \right) \right),$$

$$H(X, Q(Y)) = - \sum_a \int_{-\infty}^{+\infty} dx f_a(x) \log_2 f_a(x),$$

$$f_a(x) = \int_{t_{a-1}}^{t_a} dy f_{X,Y}(x, y),$$

$$f_{X,Y}(x, y) = \frac{1}{2\pi \Sigma \sigma} \exp \left( -\frac{x^2}{2\Sigma^2} \right) \exp \left( -\frac{(x-y)^2}{2\sigma^2} \right),$$

where  $t_{a-1}$  and  $t_a$  denote the left and right endpoints of the interval  $a$ .

In Fig. 3(c), the raw key  $Y$  are quantified in to five levels. The information included in the first three levels is very small and disclosed directly, and the latter two levels are encoded and successively decoded. More precisely, Bob sends the quantized bit strings  $\{B_1(Y_i)\}$ ,  $\{B_2(Y_i)\}$ , and  $\{B_3(Y_i)\}$  of the first three levels and the syndromes  $S_4$  and  $S_5$  of the last two levels to Alice.

The reconciliation efficiency  $\beta$  of slice reconciliation is given by

$$\beta = \frac{H[Q(Y)] - m + \sum_{i=1}^m R_i}{I(X; Y)}, \tag{6}$$

where  $H[Q(Y)]$  is the information entropy of  $Q(Y)$ .

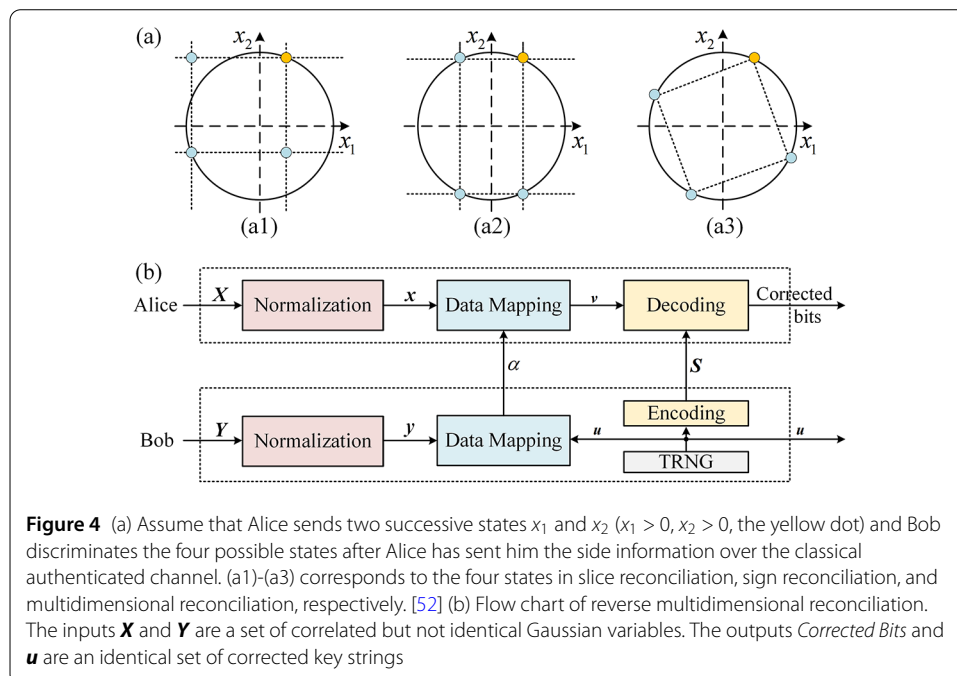
Bai *et al.* [56] and Mani *et al.* [58] explored the quantification scheme and analyzed the 4-levels, 5-levels, and 6-levels quantification and designed ECCs with better decoding performance to improve reconciliation efficiency. Wen *et al.* [59] proposed an improved slice

reconciliation protocol, named Rotated-SEC, which performs a random orthogonal rotation on the raw keys before quantization, and deduces a new estimator for the quantized sequences.

### 3.2 Multidimensional reconciliation

For CV-QKD protocols, the raw keys of Alice and Bob are correlated Gaussian variables and the SNR will be very low for long transmission distances. In this case, the raw keys have a small absolute value and are distributed around 0. Thus, it is difficult to discriminate the sign and realize the encoding and decoding. The multidimensional reconciliation algorithm provides a powerful encoding scheme for low SNR scenario and thus effectively extend the key distribution distance. By this way, the channel between Alice and Bob is converted into a virtual binary input additive white Gaussian noise (AWGN) channel and therefore efficient binary codes can be employed. The highest reconciliation efficiency achieves at  $d = 8$  because the ratio is highest between the capacities of the 8-dimensional channels and the binary input AWGN channel [60].

The basic principle of improving the discrimination in multidimensional reconciliation is the rotation of the raw keys, as shown in Fig. 4(a). Consider that Alice and Bob share a set of correlated Gaussian variables  $\mathbf{X}$  and  $\mathbf{Y}$  and  $x_1$  and  $x_2$  belong to  $\mathbf{X}$ . Figure 4(a) shows the four possible states that Bob needs to discriminate. (a1) represents the slice reconciliation: the four states are well separated, but the Gaussian symmetry is broken; (a2) represents the sign reconciliation: the symmetry is preserved but some states are difficult to discriminate because they are very close to each other; (a3) represents the multidimensional reconciliation, the states are well separated as well as the symmetry is preserved.





Both parties form a vector for each  $d$  elements of the Gaussian symbols, labeled  $\mathbf{X}'$  and  $\mathbf{Y}'$ , and then normalize each  $d$ -dimensional vector as follows:

$$\mathbf{x}' = \frac{\mathbf{X}'}{|\mathbf{X}'|}, \quad \mathbf{y}' = \frac{\mathbf{Y}'}{|\mathbf{Y}'|}, \tag{7}$$

where  $|\mathbf{X}'|$  and  $|\mathbf{Y}'|$  denote the modulo of vectors. After normalization, the random vectors are transformed into signal points on a unit sphere and the Gaussian variables are transformed into  $\mathbf{x}'$  and  $\mathbf{y}'$ . Then, a set of random bit strings  $\mathbf{u} = \{b_1, b_2, \dots, b_i\}$  of the same length as the Gaussian variables that obeying a uniform distribution is generated by a true random number generator (TRNG) at the receiver side, and each random bit string is transformed into a  $d$ -dimensional spherical vector as follows

$$\mathbf{u}' = \left( \frac{(-1)^{b_1}}{\sqrt{d}}, \frac{(-1)^{b_2}}{\sqrt{d}}, \dots, \frac{(-1)^{b_d}}{\sqrt{d}} \right). \tag{8}$$

The receiver performs a  $d$ -dimensional spatial rotation operation to compute  $\alpha$ , such that it satisfies  $\alpha \cdot \mathbf{y}' = \mathbf{u}'$ .  $\mathbf{u}$  is encoded to generate the syndrome  $\mathbf{S}$ . Then  $\alpha$  and  $\mathbf{S}$  are sent to Alice. Alice uses the received information to compute the mapping function  $M'$ . Then, she calculates  $\mathbf{v}$  using the equation  $M' \cdot \mathbf{x}' = \mathbf{v}$ . Finally, Alice uses the computed  $\mathbf{v}$  as side information to recover the exactly same  $\mathbf{u}$  as Bob by decoding.

The reconciliation efficiency  $\beta$  of the multidimensional reconciliation is defined as:

$$\beta = \frac{R}{I(X; Y)}, \tag{9}$$

where  $R$  is the rate of the ECC used in reconciliation scheme.

Recently, several works on optimization and modification of the multidimensional reconciliation and ECCs have been reported to further improve the performance of CV-QKD systems.

In 2019, Li *et al.* proposed an initial decoding message computation method for multidimensional reconciliation [61], which does not need the norm information from the encoder. They show that the improved scheme can decrease the communication traffic and storage resource consumption without significantly degrading in the reconciliation efficiency. What is more, the improved scheme can decrease the secure key consumption for classical channel authentication.

In 2021, Feng *et al.* studied the SNR of the virtual channel of multidimensional reconciliation and proved that the noise of the virtual channel follows the Student's  $t$ -distribution [62]. They proposed a novel  $t$ -BP (belief-propagation) decoding algorithm, whose FER is superior to the traditional BP decoding algorithm.

In 2023, Wang *et al.* applied the reverse multidimensional reconciliation to non-Gaussian modulation protocols [63], which can improve the performance of CV-QKD. In their work, the variables  $\mathbf{X}$  and  $\mathbf{Y}$  are obtained after non-Gaussian postselection [64] and  $\mathbf{X}$  follows non-Gaussian distribution and  $\mathbf{Y}$  follows Gaussian distribution. Alice normalizes her non-Gaussian distribution variables  $\mathbf{X}$  and rotates her normalized raw keys through the mapping function.

Table 2 shows the comparisons of the slice and multidimensional reconciliation schemes.



**Table 2** Comparisons of slice and multidimensional reconciliation scheme

	Slice reconciliation	Multidimensional reconciliation
Bits/pulse	> 1	= 1
Distance	< 30 km	> 30 km
Symmetry	Broken	Preserved
Encoding method	Quantization	Mapping
Decoding complexity	Low	High

### 3.3 Other schemes

Sign reconciliation [50] directly encode the continuous random variable to a key bit by using its sign. The sign reconciliation has the feature of simplicity and low complexity, however the performance is low. Jiang *et al.* proposed a new reconciliation scheme based on the punctured LDPC codes in 2017 [53]. Compared to the multidimensional reconciliation, their scheme has lower time complexity. Especially when the chosen punctured LDPC code achieves the Shannon capacity, there is no information leaked to the eavesdropper after IR stage. This indicates that the PA algorithm is no more required. Late [65], they proposed a new reconciliation scheme to decrease the FER. Gümüş *et al.* [54] proposed a multiple decoding attempts protocol that can be used in four-state CV-QKD and each attempt has fewer decoding iteration than the conventional protocol.

## 4 Error correction codes

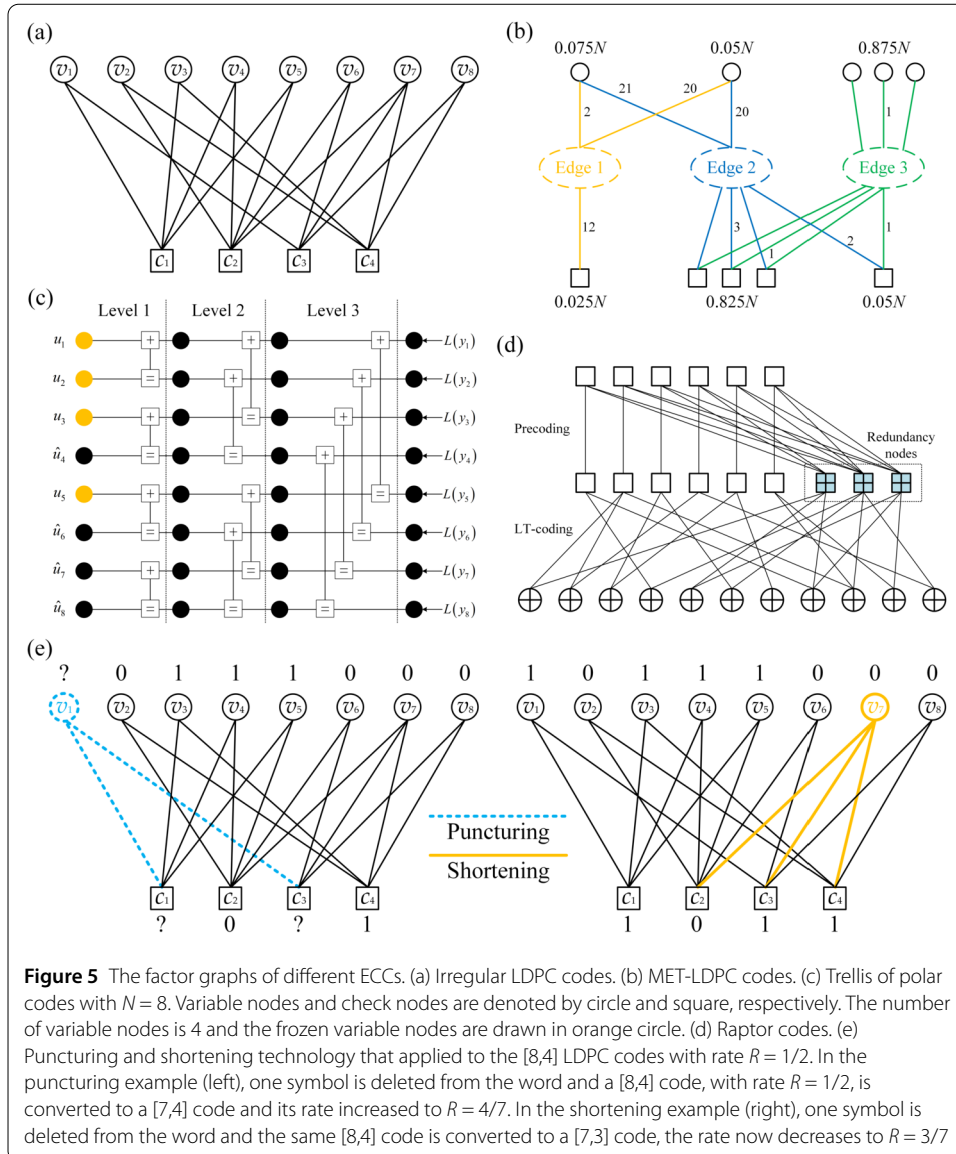
ECCs [66] allow for the detection and correction of errors occurred during the data transmission. Since a CV-QKD system usually works in a Gaussian channel with very low SNRs, typically below 0 dB, so that the initial bit error rate is very high, which requires that the ECC has very good decoding performance. Selecting an appropriate ECC with good decoding performance is the key to improve the reconciliation efficiency and reduce FER. A variety of ECCs with good decoding performance can be used to realize IR of CV-QKD, such as LDPC codes, Polar codes, Raptor codes, Spinal codes and so on. Next, we will introduce these ECCs in detail.

### 4.1 LDPC codes

LDPC codes [66] are a good performance ECC with low decoding complexity and can be used to achieve high-efficiency IR very close to the Shannon limit. They are usually represented using a sparse check matrix or a Tanner graph as shown in Fig. 5(a), in which edges are used to connect check nodes to variable nodes. Based on the information transfer between different variable nodes in the Tanner graph, LDPC codes use soft decision iterative decoding algorithm with posterior probability information. In addition, LDPC codes can be applied to almost all types of channels and parallel processing making them suitable for implementing hardware acceleration. LDPC codes are divided into different types, such as irregular LDPC codes [56, 57], multi-edge type LDPC (MET-LDPC) code [58, 60], non-binary LDPC codes [67], spatially coupled LDPC codes [65], and globally coupled LDPC code [68]. To achieve good performance, several aspects should be carefully considered, including decoding algorithms, message propagation schedule, and construction of the parity check matrix (PCM), etc.

#### 4.1.1 Degree distribution

The degree distribution is used in irregular codes to describe the degree of the nodes, that is, the distribution of non-zero elements in the PCM. Assume that the maximum degree of



the variable nodes and the check nodes are  $d_v$  and  $d_c$ , respectively, the degree distributions of the variable and check nodes can be expressed by

$$\begin{cases} \nu(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}, \\ \mu(x) = \sum_{i=2}^{d_c} \rho_i x^{i-1}, \end{cases} \quad (10)$$

where  $\lambda_i$  and  $\rho_i$  denotes the ratio of the number of edges connected to the variable or check nodes of the degree  $i$  to the total number of edges, respectively.

#### 4.1.2 Construction of parity check matrix

In addition to the size of PCMs and the degree distributions of their nodes, the position of the edges has also a significant impact on the error correction performance. A number of approaches have been proposed, such as random construction, the progressive edge growth (PEG) algorithm, and quasi-cyclic (QC) codes. The previous work showed that the

PEG algorithm has better performance at  $SNR \sim 3$ , while random construction exhibits better performance at  $SNR \sim 1$  [56]. QC codes are defined by a PCM constructed from an array of  $q \times q$  cyclically shifted identity matrices and  $q \times q$  zero matrices. It imposes a highly regular PCM structure with a sufficient degree of randomness offset to achieve near-Shannon-limit error correction performance while reducing the complexity of the decoder. It also reduces data permutation and memory access complexity by eliminating random, unordered memory access patterns.

#### 4.1.3 Decoding algorithms

LDPC codes are usually decoded using a belief propagation (BP) algorithm, in which messages typically in the form of a logarithmic-likelihood ratio (LLR) are iteratively passed in both directions along the edges between connected nodes. Two dominant LDPC decoding algorithms are the sum-product algorithm (SPA) and the min-sum algorithm (MSA). Note that two modifications of the MSA, called the normalized MSA and offset MSA [69], have been proposed to improve the performance.

The message propagation schedule [70] of the LDPC decoding process determines the order in which variable nodes and check nodes are processed, as well as whether multiple nodes are processed in parallel. Flooding, layered belief propagation (LBP) [71], and informed dynamic scheduling are three widely used schedules. LBP tends to converge to the correct code word with fewer iterations and therefore has lower computational complexity, and the memory size required for a LBP decoder is half of that required for a flooding decoder.

Although MSAs are easy to implement on FPGA, the sum-product decoding algorithm has better decoding performance where the layered message passing mechanism converges faster. It can reduce the number of iterations and the consumption of storage resources when applied to FPGAs [72].

The BP decoding algorithm consists of the following four main steps:

Step 1: Initialization: calculating the initial LLRs for each variable node:

$$LLR_i^{(0)} = LLR(P_i) = \ln \frac{P_i(0)}{P_i(1)}. \tag{11}$$

Step 2: Check nodes information processing:

$$L^{(l)}(r_{ji}) = \log \frac{1 + \prod_{i' \in R_j \setminus i} \tanh(\frac{1}{2}L^{(l-1)}(q_{i'}))}{1 - \prod_{i' \in R_j \setminus i} \tanh(\frac{1}{2}L^{(l-1)}(q_{i'}))}, \tag{12}$$

where  $l$  denotes the number of iterations.

Step 3: Variable nodes information processing:

$$L^{(l)}(q_{ij}) = LLR(P_i) + \sum_{j' \in C_i \setminus j} L^{(l)}(r_{j'i}). \tag{13}$$

Step 4: Decision. Computing hard-decision information for all variable nodes:

$$LLR_i^{(l)} = L(P_i) + \sum_{j \in C_i} L^{(l)}(r_{ji}). \tag{14}$$

If  $LLR_i^{(l)} \geq 0$ , then  $x_n = 1$ , otherwise  $x_n = 0$ . If  $\mathbf{H} \cdot \mathbf{X}^T = \mathbf{S}$ , the result  $\mathbf{X}$  is the decoded output, otherwise return to step 2. Repeat steps 2 and 3 until  $\mathbf{H} \cdot \mathbf{X}^T = \mathbf{S}$  is satisfied, or the number of iterations reaches the given maximum value.

In the LBP algorithm, step 2 and step 3 will be combined together. More precisely, the nodes in the PCM are processed row-by-row:

$$M_{ji} = LLR_i^{(l-1)} - E_{ji}^{(l-1)}, \tag{15}$$

$$E_{ji}^{(l)} = \prod_{i \in N(j)/i'} \text{sgn}(M_{ji}) \times \Psi \left[ \Psi(M_{ji}) - \sum_{i \in N(j)/i'} \Psi(M_{ji}) \right], \tag{16}$$

$$LLR_i^{(l)} = M_{ji} + E_{ji}^{(l)}, \tag{17}$$

where the function  $\Psi$  is defined as  $\Psi(x) = -\log[\tanh(|x|/2)]$ . From the node processing equation, the intermediate variables do not need to be cached into the next iteration process, thus effectively reducing the consumption of storage resources when implementing on FPGA.

#### 4.2 MET-LDPC codes

Richardson and Urbanke proposed the MET-LDPC code [73]. By introducing new constraints into the code design, the MET-LDPC code has the following advantages: (1) it shows better error correction performance on Gaussian noise channels; (2) the error correction performance at low code rates is closer to the Shannon limit than other ECCs, which can reduce the error floor at very low SNRs; (3) it also has good error correction performance at high code rates.

In 2011, Jougue *et al.* [60] used density evolution algorithm to find a set of degree distributions with code rate of 0.02, and then applied MET-LDPC codes to multidimensional reconciliation. They achieved a reconciliation efficiency of 96.9% when the code rate was 0.02 at the SNR of 0.029. In 2017, Wang *et al.* [74] used density evolution to find degree distributions at code rates of 0.05 and 0.10. In 2021, Mani *et al.* [58] used generalized external message passing graph method to find the best degree distributions at code rates of 0.01, 0.02, 0.05, and 0.10, respectively. Table 3 summarizes the optimal node degree distributions at different code rates.

#### 4.3 Polar codes

Polar codes are proposed by Arikan in 2009 [78]. Arikan proved that polar codes could achieve channel capacity in binary symmetric channels, and then Korada *et al.* showed that polar codes could also achieve channel capacity in arbitrary binary input discrete channels. Furthermore, the encoding/decoding of polar codes can be achieved with low complexity. Due to its good performance, it is applied to 5G communication [79, 80] and has also been applied to the IR of CV-QKD in recent years [49, 59, 81–85].

The basic idea of polar codes is the polarized subchannels exhibiting different properties by channel polarization at the encoding side. When the code length increases to a certain level, the channel capacity of some subchannels converges to 1 while the channel capacity of other subchannels converges to 0. Then, the information can be transmitted on the subchannels whose channel capacity is close to 1 to approach the channel capacity as much as possible. However, the coding subchannels of the finite code-length polar codes are not

**Table 3** Optimal node degree distribution of MET-LDPC codes at different code rates

Ref.	Code rate	Degree distribution
[58]	0.02	$\nu(\mathbf{r}, \mathbf{x}) = 0.0225r_1x_1^2x_2^{52} + 0.0175r_1x_1^3x_2^{57} + 0.96r_1x_3^1$ $\mu(\mathbf{x}) = 0.0165x_1^4 + 0.0035x_1^9 + 0.2475x_2^3x_3^1 + 0.7125x_2^2x_3^1$
[75]	0.025	$\nu(\mathbf{r}, \mathbf{x}) = 0.8711r_1x_1^1 + 0.0669r_1x_2^3x_3^2 + 0.0081r_1x_2^4x_3^2 + 0.0015r_1x_2^{27}x_3^3 + 0.0524r_1x_2^{28}x_3^3$ $\mu(\mathbf{x}) = 0.8711x_1^1x_2^2 + 0.1039x_3^3$
[76]	0.03	$\nu(\mathbf{r}, \mathbf{x}) = 0.0249r_1x_1^2x_2^{50} + 0.0219r_1x_1^3x_2^{50} + 0.9532r_1x_3^1$ $\mu(\mathbf{x}) = 0.0105x_1^5 + 0.0063x_1^{10} + 0.5196x_2^2x_3^1 + 0.4336x_2^3x_3^1$
[58]	0.05	$\nu(\mathbf{r}, \mathbf{x}) = 0.05625r_1x_1^2x_2^{20} + 0.04375r_1x_1^3x_2^{25} + 0.90r_1x_3^1$ $\mu(\mathbf{x}) = 0.0265625x_1^3 + 0.0234375x_1^7 + 0.48125x_2^2x_3^1 + 0.41875x_2^3x_3^1$
[76]	0.06	$\nu(\mathbf{r}, \mathbf{x}) = 0.0522r_1x_1^2x_2^{37} + 0.0291r_1x_1^3x_2^{21} + 0.9187r_1x_3^1$ $\mu(\mathbf{x}) = 0.0213x_1^9 + 0.2136x_2^2x_3^1 + 0.7051x_2^3x_3^1$
[76]	0.07	$\nu(\mathbf{r}, \mathbf{x}) = 0.0408r_1x_1^2x_2^{28} + 0.048r_1x_1^3x_2^{29} + 0.9112r_1x_3^1$ $\mu(\mathbf{x}) = 0.0188x_1^{12} + 0.1992x_2^2x_3^1 + 0.712x_2^3x_3^1$
[58]	0.10	$\nu(\mathbf{r}, \mathbf{x}) = 0.075r_1x_1^2x_2^{21} + 0.05r_1x_1^3x_2^{20} + 0.875r_1x_3^1$ $\mu(\mathbf{x}) = 0.025x_1^{12} + 0.825x_2^3x_3^1 + 0.05x_2^2x_3^1$
[77]	0.15	$\nu(\mathbf{r}, \mathbf{x}) = 0.0858r_1x_1^2x_2^{12} + 0.0996r_1x_1^3x_2^{14} + 0.8146r_1x_3^1$ $\mu(\mathbf{x}) = 0.0160x_1^{10} + 0.0194x_1^{16} + 0.0198x_2^2x_3^1 + 0.7948x_2^3x_3^1$
[35]	0.19	$\nu(\mathbf{r}, \mathbf{x}) = 0.1425r_1x_1^2x_2^{13} + 0.0950r_1x_1^3x_2^7 + 0.7625r_1x_3^1$ $\mu(\mathbf{x}) = 0.0475x_1^{12} + 0.5325x_2^3x_3^1 + 0.2300x_2^4x_3^1$

entirely polarized, and some of them are neither completely noise-free nor completely noisy, called the intermediate channels. The intermediate channels are protected by outer LDPC codes, called IC-LDPC Polar codes [84].

Since Arikan proposed the basic decoding algorithms: polarization codes-successive cancellation decoding algorithm, and belief propagation decoding algorithm [78], the decoding algorithms of polarization codes have been improved after more than ten years of efforts (for more details, please refer to Ref. [86]).

The main description tools of encoding and decoding for polar codes are “Trellis” and “Code Tree”, where the latter is a compressed form of the former. In general, given a polar code of code length  $N = 2n$ , the trellis contains  $n$  levels. The schematic diagram of trellis is shown in Fig. 5(c). The left side is the source side and the right side is the channel side.

#### 4.4 Rate-compatible codes

The rate-compatible codes are necessary for practical CV-QKD systems to deal with the time-varying channels. The methods to achieve rate-compatible are nodes puncturing, nodes shortening, and rateless codes. Typical rateless codes are Luby Transform (LT) codes [87], Raptor codes [88], and spinal codes [89]. The nodes puncturing and shortening (P&S) method, Raptor codes, and spinal codes that have been used in IR are elaborated in the following section.

##### 4.4.1 Puncturing and shortening

Puncturing [90] and shortening [91] are two rate-compatibility techniques that can increase and decrease the code rate, respectively. Using the two methods, we can achieve rate-compatible ECCs for channels with varying SNRs. P&S can be applied not only to LDPC codes, but also to polar codes. The advantage of P&S is that only one encoder/decoder pair is required for the entire SNR range, since the P&S positions are known in advance by the receiver, which effectively reduce the complexity of the CV-QKD system.

**Table 4** Comparisons of different ECCs

	Advantages	Disadvantages
LDPC codes	Construction of PCMs Low decoding complexity	High SNR
MET-LDPC codes	Low SNR	Construction of PCMs
Polar codes	Can achieve channel capacity	Low throughput
Raptors codes	Rate-compatible	High decoding complexity
Spinal codes	Rate-compatible	—

#### 4.4.2 Raptor codes

Raptor codes [88], a class of rateless codes with linear time encoding and decoding, have been used in the IR of CV-QKD [92–95]. The factor graph of Raptor code is shown in Fig. 5(d).

Raptor codes need to cascade another coding process, such as LDPC codes, on top of the LT codes to achieve good coverage of the source sequence. This so called pre-coding can effectively reduce the complexity of compiling codes and improve the success rate of decoding. However, Raptor codes require a higher decoding complexity and longer decoding latency than other types of ECCs.

Raptor-like codes [96] can be constructed if the structure of the PCM of Raptor codes is kept unchanged. The check matrix of Raptor-like codes is constructed by the common matrix construction method of LDPC codes. The Raptor-like codes have not only the code rate compatibility, but also better decoding performance than LDPC codes. Zhou *et al.* have applied Raptor-like LDPC codes to IR [97].

#### 4.4.3 Spinal codes

Spinal codes [89] are also rateless codes with a simple coding structure, it can adapt to time-varying channels without explicit bit rate selection. It have an efficient polynomial-time decoder, which achieves the Shannon capacity over both AWGN and BSC channels. In 2020, Wen *et al.* applied the spinal codes to IR and obtained good reconciliation performance [98].

### 4.5 Comparison of several ECCs

Table 4 shows the advantages and disadvantages of several ECCs compared with others.

## 5 Hardware acceleration

In a high-speed QKD system, the throughput of IR is one of the key factors governing the system key rate, as shown in Eq. (3). With the rapid development of experimental technology, the repetition rate of CV-QKD systems has grown from MHz to GHz [39]. Correspondingly, high-speed and real-time IR is required to match the high repetition rate. In this section, we will introduce how to use hardwares to accelerate the reconciliation algorithm and improve the throughput.

By increasing the code length, the decoding performance of ECCs can be improved effectively. However, increase of the code length will also increase the computational complexity. The code length in classical communication and DV-QKD is generally about 1k ~ 10k [70, 99], while CV-QKD often requires 100k ~ 1M. The throughput of encoding/decoding algorithms based on general central processing units (CPUs) for long code is very limited.

**Table 5** Comparison of FPGA and GPU

	FPGA	GPU
Parallel processing	✓	✓
Programmable	✓	✓
Computation	Fixed-point	Floating-point
Power consumption	Low	High
Development cycle	Long	Short

In order to solve this problem, the powerful parallel computing capability of hardware can be employed to improve the computing speed. Since, the structure of PCMs of the ECCs is readily parallelized [100]. This is an important factor for achieving high throughput, and also makes encoders and decoders suitable for implementation on FPGA and GPU to achieve very high throughput [101].

FPGAs can be used for both the algorithm acceleration and control tasks. It is ideal and attractive for designing prototypes and the manufacturing of small-production-run devices. FPGAs based platforms have been demonstrated to facilitate quantum information processing, DV-QKD prototypes [101–105], quantum algorithm [106, 107], and post-processing DV-QKD [108, 109]. The low power consumption makes FPGAs attractive for good integration ability. GPU provides floating-point computational precision with short development cycles and high-bandwidth on-chip memory. Table 5 compares the characteristics of FPGA and GPU.

### 5.1 FPGA-based acceleration

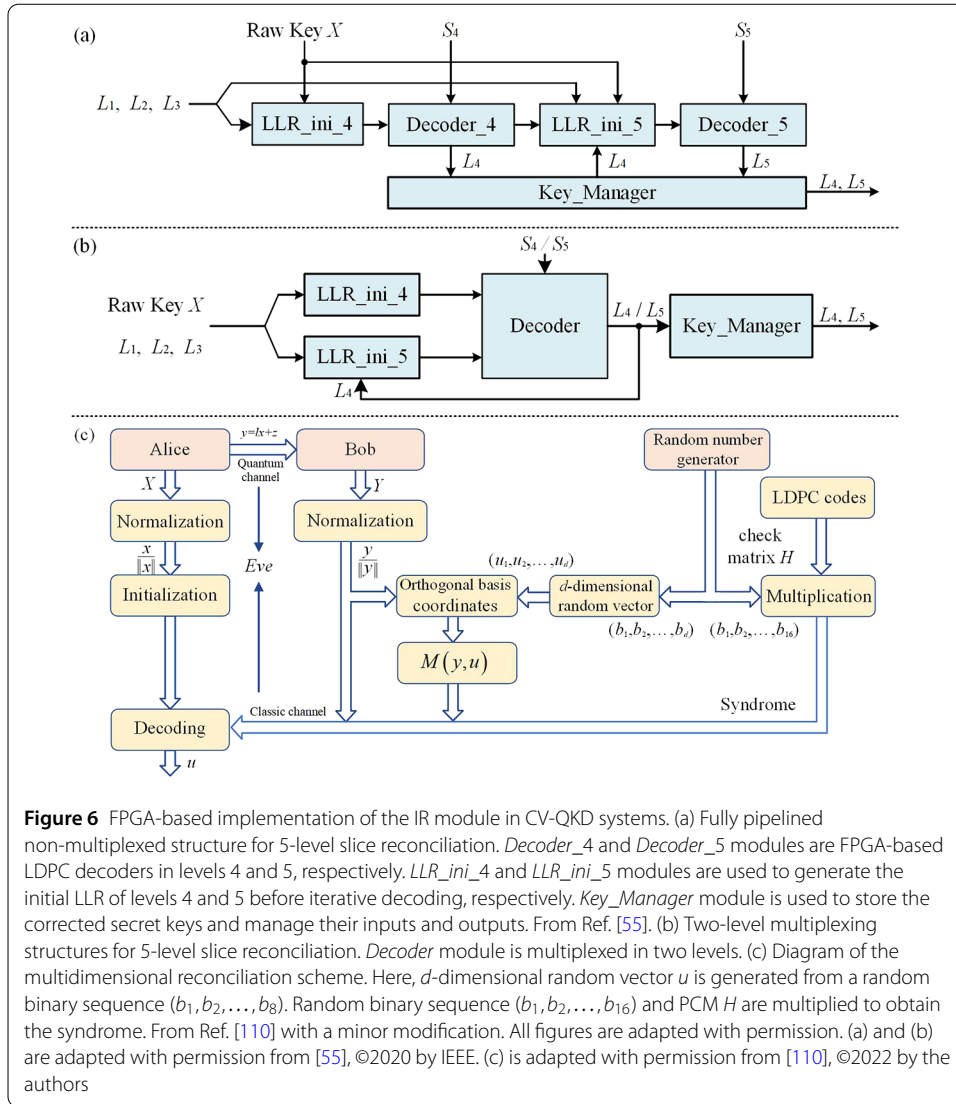
In 2020, Yang *et al.* achieved the high-speed hardware-accelerated IR procedure on a FPGA chip by taking advantage of its superior parallel processing ability [55]. As shown in Fig. 6(a) and (b). Two different structures including multiplexing and non-multiplexing are designed to achieve the trade-off between the speed and area of FPGAs, so that an optimal scheme can be adopted according to the requirement of a practical system. Many FPGA-based LDPC decoders have been developed over past few decades [70]. However, these decoders do not meet the decoding performance requirements of IR in CV-QKD systems. In 2021, Yang *et al.* proposed a high-speed layered SPA decoders with good performance and low-complexity for ultra-long quasi-cyclic LDPC codes [72]. To reduce the implementation complexity and hardware resource consumption, the messages in the iteration process are uniformly quantified and the function  $\Psi(x)$  is approximated with second-order functions. The decoder architecture improves the decoding throughput by using partial parallel and pipeline structures. A modified construction method of PCMs was applied to prevent read & write conflicts and achieve high-speed pipeline structure. The throughput of the LDPC decoder can be estimated by

$$T \approx \frac{f \cdot q}{(1 - R) \cdot N_{node} \cdot N_{iter}}, \tag{18}$$

where  $f$  is the clock frequency of FPGAs,  $q$  is the quasi-cyclic parameter,  $N_{node}$  is the average number of nodes in each row of a basic matrix, and  $N_{iter}$  is the average number of iterations to execute a decoding algorithm.

Recently, Lu *et al.* [110] designed an FPGA-based architecture for multidimensional reconciliation receiver module that can achieve high throughput according to system requirements with the top-level logic diagram shown in Fig. 6(c). To implement the sender





**Figure 6** FPGA-based implementation of the IR module in CV-QKD systems. (a) Fully pipelined non-multiplexed structure for 5-level slice reconciliation. *Decoder\_4* and *Decoder\_5* modules are FPGA-based LDPC decoders in levels 4 and 5, respectively. *LLR\_ini\_4* and *LLR\_ini\_5* modules are used to generate the initial LLR of levels 4 and 5 before iterative decoding, respectively. *Key\_Manager* module is used to store the corrected secret keys and manage their inputs and outputs. From Ref. [55]. (b) Two-level multiplexing structures for 5-level slice reconciliation. *Decoder* module is multiplexed in two levels. (c) Diagram of the multidimensional reconciliation scheme. Here,  $d$ -dimensional random vector  $u$  is generated from a random binary sequence  $(b_1, b_2, \dots, b_8)$ . Random binary sequence  $(b_1, b_2, \dots, b_{16})$  and PCM  $H$  are multiplied to obtain the syndrome. From Ref. [110] with a minor modification. All figures are adapted with permission. (a) and (b) are adapted with permission from [55], ©2020 by IEEE. (c) is adapted with permission from [110], ©2022 by the authors

of multidimensional reconciliation, FPGA-based MET-LDPC decoders still needs to be designed and implemented. To reduce the complexity of hardware implementation, we can simplify the matrix operation based on the characteristic of fewer non-zero elements in the matrix family.

In principle, the throughput based on FPGAs can be improved by instantiating multiple modules on a chip, and the throughput can be further improved by increasing the parallelism of iterative decoding, etc. Currently, integrated photonic technology is develops rapidly [111, 112], and some research teams have tried to implement the CV-QKD systems using silicon photonic chips [41, 43, 44]. To realize an overall integration, the IR module must also be able to be integrated and miniaturized. The advantages of easy integration and low power consumption of FPGAs make it a very competitive candidate.

### 5.2 GPU-based acceleration

GPUs are widely used in IR hardware acceleration for CV-QKD due to their easy programming and short development cycle [49, 113–118]. The main difficulty of GPUs also

lies in the implementation of storage and decoding algorithms. A GPU has many threads. If only one codeword is decoded at a time, the performance of the GPU cannot be fully utilized. Compute Unified Device Architecture (CUDA) can be utilized to implement multiple codewords parallel decoding algorithms, such as 64 codewords [115], 128 codewords [116], and 512 codewords [117]. Theoretically, the more parallel codewords, the greater throughput. However, the finite memory resources will limit the number of parallel codewords. The memory of GPUs is composed of global memory, constant memory, local memory, and so on. Due to the very large size of PCMs of IR, the developers need to optimize the memory structure of PCMs. To reduce latency, the iterative decoding messages are usually stored in global memory for coalesced access.

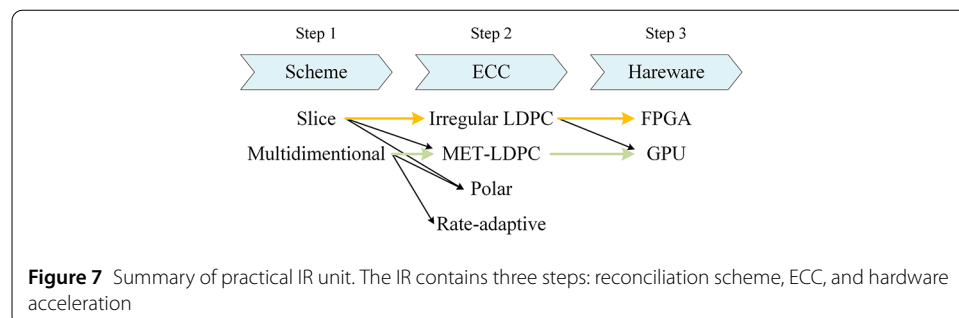
When selecting GPUs and according to the characteristics of IR, the main considerations are memory, threads, and clock frequency. Several models of GPUs have been employed in IR, such as NVIDIA GeForce GTX 1080/1650, TITAN Xp, and Tesla K40C accelerator card. With the advancement of technology, more and more on-chip resources will be available, which will further increase the parallelism of the IR algorithm. To avoid some operations that are not easy to perform on GPU, a hybrid CPU-GPU platform can be used [118].

### 6 Progress of IR

As shown in Fig. 7, a practical IR unit often contain three steps: designing a reconciliation scheme, selecting and optimizing the ECCs, and performing hardware acceleration. The early research on IR focused on improving the reconciliation efficiency to obtain high SKR per pulse, and after years of efforts, the reconciliation efficiency has now been able to reach more than 95%, which can meet most of the requirements of CV-QKD systems. In recent years, the research of IR has gradually focused on high-speed and practicality with the rapid increase of the system repetition rate. In this section, we summarize the research progress of IR including: slice reconciliation, multidimensional reconciliation, and rate-adaptive reconciliation.

#### 6.1 Slice reconciliation

In Table 6, we summarize the current research advances of slice reconciliation. The first reconciliation algorithm used for CV-QKD employs Turbo code [51] and its efficiency is less than 80%, which limits the maximum transmission distance to less than 20 km. By improving the LDPC based ECCs and optimizing the quantization of the Gaussian variable, the efficiency of the slice reconciliation gradually grows from less than 80% to above 95% [56, 119]. Recently, polar codes are employed in slice reconciliation with reconciliation efficiency of around 95% [83], notice that longer block length compared with that of



**Figure 7** Summary of practical IR unit. The IR contains three steps: reconciliation scheme, ECC, and hardware acceleration

**Table 6** Current research advances of slice reconciliation

Ref.	Year	ECC	Code length	SNR	$\beta$	FER	Throughput (M Symbols/s*)
[51]	2004	Turbo	—	—	—	—	—
[120]	2006	LDPC	$2 \times 10^5$	3	88.70%	—	—
				15	92.20%	—	—
[113]	2007	LDPC	$2 \times 10^5$	—	88.70%	$10^{-4}$	0.063
[121]	2010	LDPC	$2 \times 10^5$	—	89.00%	—	—
[122]	2014	LDPC	$1 \times 2^{20}$	1.0	94.20%	—	—
				3.0	94.10%	—	—
[119]	2016	NB-LDPC	$1 \times 10^5$	3.0	95.20%	—	—
[57]	2016	LDPC	$2 \times 10^5$	3.0	93.70%	—	—
[56]	2017	LDPC	$1 \times 10^6$	1.0	95.02%	19%	—
				3.0	95.26%	22%	—
[55]	2020	LDPC	349,952	1.0	93.02%	14%	14.83
			262,144	3.0	93.06%	11%	100.9
[59]	2021	Polar	$1 \times 2^{24}$	3.0	94.85%	< 10%	—
[83]	2022	Polar	$1 \times 10^9$	1.0	95.12%	< 20%	—
				3.0	95.16%	—	—
				10.0	95.82%	—	—

\*"Symbols/s" denotes the speed of processing raw keys in slice reconciliation.

LDPC are required. Yang *et al.* perform hardware acceleration of the slice reconciliation using FPGAs [55], the maximum throughput is higher than 100.9 M Symbols/s. However, the FER is relatively high (above 10%), and the rate-adaptive slice reconciliation has not been implemented. Due to the rapid growing of the system clock rate (above GHz), the throughput needs to be further improved.

## 6.2 Multidimensional reconciliation

Multidimensional reconciliation has gained much attentions because it can support CV-QKD systems over longer transmission distances. Table 7 shows a summary of multidimensional reconciliation research that have been reported. The reconciliation efficiency and throughput are gradually improving. Among them, the highest reconciliation efficiency can already reach 99%, at the cost of high FER. To reduce the FER, Feng *et al.* proposed a  $t$ -BP decoding algorithm [62]. Their simulation results show that FER with the new decoding algorithm is superior to that with the conventional BP algorithm. To improve the throughput, GPUs are employed for hardware acceleration and have made great progress [49, 114–116]. For example, the throughput is increased from 7.1 Mb/s [49] to 64.11 Mb/s [116] when the SNR is 0.161. In addition, Lu *et al.* has implemented the encoding module of multidimensional reconciliation based on FPGAs [110].

## 6.3 Rate-adaptive reconciliation

For practical QKD systems, the SNRs are not fixed and will inevitably fluctuate due to the transmission fluctuations of the quantum channel and variations of the QKD system itself. This requires that the optimal code rate of the ECCs used in the IR process should also be adjusted accordingly to guarantee the performance and security of the system.

**Table 7** Research progress of multidimensional reconciliation

Ref.	Year	ECC	Code length	SNR	$\beta$	FER	Throughput (Mbits/s)
[52]	2008	—	—	—	—	—	—
[60]	2011	MET-LDPC	$1 \times 2^{20}$	0.029	96.9%	1/3	—
[49]	2014	Polar	$1 \times 2^{24}$	1.097	95.20%	0.10	8.0
		LDPC	$1 \times 2^{20}$	1.097	96.90%	0.09	6.5
		LDPC	$1 \times 2^{20}$	0.161	93.10%	0.04	7.1
[93]	2017	Raptor	$1 \times 10^5$	-30 dB	96.00%	—	—
			$3.8 \times 10^4$	-5 dB	94.00%	—	—
[115]	2018	MET-LDPC	$1 \times 10^6$	0.029	96.99%	30.5%	16.41
				0.075	95.84%	31.4%	21.23
				0.160	93.40%	32.9%	30.39
[114]	2018	MET-LDPC	$1 \times 2^{20}$	$\sim 0.02$	99.00%	88.3%	1.807
				0.161	—	2.43%	9.17
[81]	2018	Polar	1,024	0.7	97.9%	4%	—
[116]	2020	MET-LDPC	$1 \times 10^6$	0.030	93.8%	32.81%	39.51
				0.076	94.63%	25%	48.65
				0.161	92.86%	17.97%	64.11
[123]	2020	SC-LDPC	$6.48 \times 10^6$	0.2157	$\sim 95.2\%$	0.001	—
		QC-LDPC	$6.48 \times 10^5$	0.635	—	—	
[118]	2022	LDPC	131,072	0.8	93.27%	$\sim 0.1$	26.7
[84]	2023	IC-LDPC Polar	8,192	-20.80 dB	98.06%	21%	—

The traditional LDPC codes and polar codes are sensitive to the number of error bits in the bit string, which is unsuitable for the fluctuating channel in practical applications. It is impossible to solve the problem by storing a large number of check matrices with different bit rates. To cope with the time-varying quantum channel, it is necessary to adjust the code rate of ECCs in real-time by rate-adaptive techniques (P&S) or rateless codes (Raptor codes and spinal codes).

Table 8 shows the reported rate-adaptive IR. Most of the current works use the multi-dimensional reconciliation scheme. Wang *et al.* [74] and Jeong *et al.* [75] adopted MET-LDPC codes, which can achieve high reconciliation efficiency, but the SNR range covered by a single PCM with the fixed code rate is very small. Zhang *et al.* [82] and Cao *et al.* [85] adopted polar codes to realize rate-adaptive reconciliation. Zhang *et al.* adopted the incremental freezing scheme of information bits in polar codes to fix the step size of frozen information bits, thus realizing the fixed-step code-rate adjustment. In Ref. [85], the channel state is estimated after IR to estimate the SNR and calculate the code rate. Then, the positions of the punctured and shortened bits are determined. Notice that, the schemes of Wen *et al.* [98] and Fan *et al.* [124] can be applied to larger SNRs.

### 7 Applications of IR in CV-QKD systems

At present, a number of teams have already applied IR to CV-QKD systems. Lodewyck *et al.* [113] implemented a coherent-state CV-QKD system with SKR of more than 2 kb/s on 25 km single mode fiber. In their QKD system, they used the slice reconciliation based on the LDPC codes and GPU. In 2009, they designed and realized a CV-QKD prototype [125] that employs sophisticated ECCs for reconciliation. Thereafter, they extended the trans-

**Table 8** Research progress of rate-adaptive reconciliation

Ref.	Year	ECC	Rang of SNR	$\beta$	FER
[74]	2017	MET-LDPC, P&S	0.0277 ~ 0.0314 0.069 ~ 0.081 0.143 ~ 0.176	96.36% ~ 96.59% 95.16% ~ 95.68% 93.21% ~ 93.64%	—
[94]	2019	Raptor	0.01 ~ 1.0 dB	95.00% ~ 98.00%	—
[98]	2020	Spinal	0 ~ 0.5	~ 95%	—
[82]	2021	Polar	0.01 ~ 1	> 95%	$0.04 \sim 9 \times 10^{-4}$
[97]	2021	Raptor-like LDPC	0.0229 ~ 0.0493	> 98%	—
[75]	2022	MET-LDPC, P	-15.6 ~ -15 dB	—	—
[124]	2022	LDPC, P	0.01 ~ 15	91.8%	—
[85]	2023	Polar, P&S	-4.5 ~ -0.5 dB	> 98%	$0.15 \sim 4 \times 10^{-4}$

"P", Puncturing; "P&S", Puncturing and Shortening.

mission distance to 80 km by using multidimensional reconciliation [126]. The multidimensional reconciliation is performed using MET-LDPC codes and achieved speeds up to several Mbps using an OpenCL implementation of BP decoding algorithm with flooding schedule on a GPU.

In 2015, Wang *et al.* [127] demonstrated CV-QKD over 50 km fiber. To generate the secret keys at low SNR regime, they adopted multidimensional reconciliation and the rate-adaptive LDPC code to perform key extraction offline. In 2021, they experimentally realized a passive-state-preparation CV-QKD scheme and a slice reconciliation based on slice-type polar codes is employed [34].

In 2019, Zhang *et al.* [128] combine multidimensional reconciliation and MET-LDPC codes to achieve high reconciliation efficiency at low SNRs. They implement multiple code words decoding simultaneously based on GPU and obtain throughput up to 30.39 Mbps on a GPU. In Ref. [33], the authors use slice reconciliation with polar codes at 27.27 km and 49.30 km, multidimensional reconciliation with MET-LDPC codes at 69.53 km, 99.31 km, and 140.52 km, and multidimensional reconciliation with Raptor codes at the longest distance of 202.81 km, respectively.

Zhang *et al.* [41] demonstrate an integrated CV-QKD system over a 2 m fiber link and generate secret keys with the slice reconciliation and LDPC codes. Furthermore, to prove the capability for long-distance CV-QKD, they developed a rate-adaptive reconciliation protocol based on multidimensional reconciliation and MET-LDPC codes.

In 2022, Wang *et al.* [76] designed three PCMs with code rates of 0.07, 0.06, and 0.03, which are suitable for transmission distances of 5, 10, 25 km in their QKD system, respectively. Jain *et al.* [35] obtained a reconciliation efficiency of  $\beta = 94.3\%$  and  $FER = 12.1\%$  for their experimental data (20 km long quantum channel) based on a multidimensional reconciliation scheme and MET-LDPC codes.

IR has applications not only in point-to-point CV-QKD systems, but also in CV-QKD network systems [129, 130].

## 8 Challenges

Although great progress has been made for IR, there are still several challenges for future work.

*Performance improvement.* On the one hand, we should continue to study more advanced ECCs for IR to improve the reconciliation efficiency and reduce the FER further. Furthermore, the hybrid platform such as FPGA-GPU should be investigated to give full play to the advantages of each platform. In this case, we can realize a better hardware acceleration performance and practicability (easy to use, low power consumption, and short development cycle) that are not attainable by using only a single platform. On the other hand, we know that several parameters of IR affect the performance of CV-QKD systems from previous sections. Currently, most of the existing research works focus on improving one or two parameters. To design an efficient and practical IR unit, it is crucial to consider (improve and optimize) the reconciliation scheme, ECCs, hardware acceleration, and other aspects from a global perspective. In addition, new methods, such as artificial intelligence can be introduced to IR to reduce the decoding complexity [118].

*Rate-adaptive reconciliation.* Most of the current research on rate-adaptive reconciliation concentrate on multidimensional reconciliation. The rate-adaptive slice reconciliation, which is suitable for short-range key distribution needs to be investigated. High throughput rate-adaptive reconciliation is critical for a high speed QKD system. To this end, the hardware structures need to be carefully designed according to the characteristics of the rate-compatible codes used. The main difficulties faced is how to improve the compatibility of codes in the hardware platform to make it compatible with different check matrices.

*Standardization.* With the rapid development of quantum information technology, its large-scale applications gradually become possible. The relevant scientific and technological progress has made the standards formulations available [131]. As a key part of QKD technique, the corresponding standards of IR is required. The existing error correction standards for classical communications are not well suited for CV-QKD. For example, ATSC 3.0 standard [123], an international broadcasting standard formulated by Advanced television systems committee (ATSC) in 2013, gives an encoding/decoding algorithm for LDPC codes. To establish the error correction standards for the CV-QKD, one should identify the types of codes and the encoding/decoding algorithms that are most suitable for the IR of CV-QKD.

## 9 Conclusions

In this paper, we have reviewed the IR in CV-QKD. The rapid development of CV-QKD technology has put forward growing requirements on IR. For future work, it is critical to further improve the overall performance of IR including throughput, efficiency, and FER. In this direction, various high-performance ECCs should be explored and developed to find the best candidate of IR. Furthermore, it is also necessary to efficiently adapt to time-varying channels for the IR. In terms of integration and miniaturization, special hardware architectures should be developed to dramatically accelerate the algorithm and reduce the power consumption. By taking the above measures, high performance and practical IR modules can be developed, which will pay the ways for large scale applications of CV-QKD technology in future.

### Funding

Innovation Program for Quantum Science and Technology (No. 2021ZD0300703), National Natural Science Foundation of China (NSFC) (No. 62175138, 62205188), Shanxi 1331KSC, Fundamental Research Program of Shanxi Province (No. 202203021222232, 202203021211260), Scientific and Technological Innovation Programs of Higher Education Institutions

in Shanxi Province (No. 2021L258) and Key Research and Development Program of Guangdong Province (No. 2020B0303040002).

### Abbreviations

ATSC, Advanced television systems committee; AWGN, Additive white Gaussian noise; BP, Belief propagation; BSC, Binary symmetric channel; CV-QKD, Continuous variable quantum key distribution; DR, Direct reconciliation; DV-QKD, Discrete variable quantum key distribution; ECC, Error correction code; FER, Frame error rate; FPGA, Field-programmable gate array; GPU, Graphics processing unit; IR, Information reconciliation; LBP, Layered belief propagation; LDPC, Low-density parity-check; LLR, Logarithmic-likelihood ratio; MLC, Multi-level coding; MSA, Min-sum algorithm; MSD, Multi-stage decoding; PA, Privacy amplification; PCM, Parity check matrix; PEG, Progressive edge growth; QKD, Quantum key distribution; RR, Reverse reconciliation; SKR, Secret key rate; SNR, Signal-to-noise ratio; TRNG, True random number generator.

### Availability of data and materials

Not applicable.

### Declarations

#### Ethics approval and consent to participate

Not applicable.

#### Consent for publication

The authors agree to publication in the journal. And, the work has not been published or presented elsewhere in part or in entirety.

#### Competing interests

The authors declare no competing interests.

#### Author contributions

SY and YL wrote the main manuscript text. XM checked the main manuscript. ZY prepared Fig. 5 and Table 6. HY, QL, and ZL wrote Sect. 5. LC was involved in the revision of the manuscript. All authors reviewed the manuscript.

#### Author details

<sup>1</sup>College of Physics and Information Engineering, Shanxi Normal University, Taiyu Road, Taiyuan, 030031, Shanxi, China.

<sup>2</sup>State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Wucheng Road, Taiyuan, 030006, Shanxi, China. <sup>3</sup>Collaborative Innovation Center of Extreme Optics, Shanxi University, Wucheng Road, Taiyuan, 030006, Shanxi, China. <sup>4</sup>Hefei National Laboratory, Hefei, 230088, China.

Received: 30 June 2023 Accepted: 20 September 2023 Published online: 06 October 2023

### References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: International conference on computer, system and signal processing; Bangalore, India; 1984. p. 175–9.
2. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. *Rev Mod Phys.* 2002;74(1):145–95.
3. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Rev Mod Phys.* 2009;81(3):1301–50.
4. Lo HK, Curty M, Tamaki K. Secure quantum key distribution. *Nat Photonics.* 2014;8(8):595–604.
5. Diamanti E, Lo HK, Qi B, Yuan Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* 2016;2:16025.
6. Bedington R, Arrazola JM, Ling A. Progress in satellite quantum key distribution. *npj Quantum Inf.* 2017;3:30.
7. Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. *Rev Mod Phys.* 2020;92(2):025002.
8. Lu CY, Cao Y, Peng CZ, Pan JW. Micius quantum experiments in space. *Rev Mod Phys.* 2022;94(3):035001.
9. Portmann C, Renner R. Security in quantum cryptography. *Rev Mod Phys.* 2022;94(2):025008.
10. Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy.* 2015;17(9):6072–92.
11. Li YM, Wang XY, Bai ZL, Liu WY, Yang SS, Peng KC. Continuous variable quantum key distribution. *Chin Phys B.* 2017;26(4):040303.
12. Laudenbach F, Pacher C, Fung CHF, Poppe A, Peev M, Schrenk B et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. *Adv Quantum Technol.* 2018;1(1):1800011.
13. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R et al. Advances in quantum cryptography. *Adv Opt Photonics.* 2020;12(4):1012–236.
14. Guo H, Li Z, Yu S, Zhang Y. Toward practical quantum key distribution using telecom components. *Fund Res.* 2021;1(1):96–8.
15. Ralph TC. Continuous variable quantum cryptography. *Phys Rev A.* 1999;61(1):010303.
16. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. *Phys Rev Lett.* 2002;88(5):057902.
17. Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using Gaussian-modulated coherent states. *Nature.* 2003;421(6920):238–41.
18. Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys Rev Lett.* 2009;102(18):180504.



19. Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein SL, Lloyd S et al. High-rate measurement-device-independent quantum cryptography. *Nat Photonics*. 2015;9(6):397–402.
20. Qi B, Loughovski P, Pooser R, Grice W, Bobrek M. Generating the local oscillator “locally” in continuous-variable quantum key distribution based on coherent detection. *Phys Rev X*. 2015;5(4):041009.
21. Soh DBS, Brif C, Coles PJ, Lütkenhaus N, Camacho RM, Urayama J et al. Self-referenced continuous-variable quantum key distribution protocol. *Phys Rev X*. 2015;5(4):041010.
22. Usenko VC, Grosshans F. Unidimensional continuous-variable quantum key distribution. *Phys Rev A*. 2015;92(6):062337.
23. Matsuura T, Maeda K, Sasaki T, Koashi M. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nat Commun*. 2021;12:252.
24. Leverrier A, García-Patrón R, Renner R, Cerf NJ. Security of continuous-variable quantum key distribution against general attacks. *Phys Rev Lett*. 2013;110(3):030502.
25. Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys Rev Lett*. 2015;114(7):070501.
26. Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys Rev Lett*. 2017;118(20):200501.
27. Ghorai S, Grangier P, Diamanti E, Leverrier A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys Rev X*. 2019;9(2):021059.
28. Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys Rev X*. 2019;9(4):041064.
29. Li C, Qian L, Lo HK. Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources. *npj Quantum Inf*. 2021;7:175.
30. Pereira D, Almeida M, Fação M, Pinto AN, Silva NA. Impact of receiver imbalances on the security of continuous variables quantum key distribution. *EPJ Quantum Technol*. 2021;8(1):22.
31. Pereira D, Almeida M, Pinto AN, Silva NA. Impact of transmitter imbalances on the security of continuous variables quantum key distribution. *EPJ Quantum Technol*. 2023;10(1):20.
32. Eriksson TA, Luis RS, Puttnam BJ, Rademacher G, Fujiwara M, Awaji Y et al. Wavelength division multiplexing of 194 continuous variable quantum key distribution channels. *J Lightwave Technol*. 2020;38(8):2214–8.
33. Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B et al. Long-distance continuous-variable quantum key distribution over 202.81 km fiber. *Phys Rev Lett*. 2020;125(1):010502.
34. Huang P, Wang T, Chen R, Wang P, Zhou Y, Zeng G. Experimental continuous-variable quantum key distribution using a thermal source. *New J Phys*. 2021;23(11):113028.
35. Jain N, Chin HM, Mani H, Lupo C, Nikolic DS, Kordts A et al. Practical continuous-variable quantum key distribution with composable security. *Nat Commun*. 2022;13:4740.
36. Pan Y, Wang H, Shao Y, Pi Y, Li Y, Liu B et al. Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. *Opt Lett*. 2022;47(13):3307–10.
37. Tian Y, Wang P, Liu J, Du S, Liu W, Lu Z et al. Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. *Optica*. 2022;9(5):492–500.
38. Zhang M, Huang P, Wang P, Wei S, Zeng G. Experimental free-space continuous-variable quantum key distribution with thermal source. *Opt Lett*. 2023;48(5):1184–7.
39. Tian Y, Zhang Y, Liu S, Wang P, Lu Z, Wang X et al. High-performance long-distance discrete-modulation continuous-variable quantum key distribution. *Opt Lett*. 2023;48(11):2953–6.
40. Du S, Wang P, Liu J, Tian Y, Li Y. Continuous variable quantum key distribution with a shared partially characterized entangled source. *Photon Res*. 2023;11(3):463–75.
41. Zhang G, Haw JY, Cai H, Xu F, Assad SM, Fitzsimons JF et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat Photonics*. 2019;13(12):839–42.
42. Wang X, Jia Y, Guo X, Liu J, Wang S, Liu W et al. Silicon photonics integrated dynamic polarization controller. *Chin Opt Lett*. 2022;20(4):041301.
43. Piétri Y, Vidarte LT, Schiavon M, Grangier P, Rhouni A, Diamanti E. CV-QKD receiver platform based on a silicon photonic integrated circuit. In: *Optical fiber communications conference and exhibition; San Diego, CA, USA; 2023*. p. 1–3.
44. Li L, Wang T, Li X, Huang P, Guo Y, Lu L et al. Continuous-variable quantum key distribution with on-chip light sources. *Photon Res*. 2023;11(4):504–16.
45. Hosseinihadj N, Babar Z, Malaney R, Ng SX, Hanzo L. Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook. *IEEE Commun Surv Tutor*. 2019;21(1):881–919.
46. Dequal D, Trigo Vidarte L, Roman Rodriguez V, Vallone G, Villoresi P, Leverrier A et al. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Inf*. 2021;7:3.
47. Chen Z, Wang X, Yu S, Li Z, Guo H. Continuous-mode quantum key distribution with digital signal processing. *npj Quantum Inf*. 2023;9(1):28.
48. Huth C, Guillaume R, Strohm T, Duplys P, Samuel IA, Güneysu T. Information reconciliation schemes in physical-layer security: a survey. *Comput Netw*. 2016;109:84–104.
49. Jouquet P, Kunz-Jacques S. High performance error correction for quantum key distribution using polar codes. *Quantum Inf Comput*. 2014;14(3&4):329–38.
50. Silberhorn C, Ralph TC, Lütkenhaus N, Leuchs G. Continuous variable quantum cryptography: beating the 3 dB loss limit. *Phys Rev Lett*. 2002;89(16):167901.
51. Van Assche G, Cardinal J, Cerf NJ. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans Inf Theory*. 2004;50(2):394–400.
52. Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys Rev A*. 2008;77(4):042325.
53. Jiang XQ, Huang P, Huang D, Lin D, Zeng G. Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution. *Phys Rev A*. 2017;95(2):022318.
54. Gümüş K, Eriksson TA, Takeoka M, Fujiwara M, Sasaki M, Schmalen L et al. A novel error correction protocol for continuous variable quantum key distribution. *Sci Rep*. 2021;11:10465.

55. Yang SS, Lu ZG, Li YM. High-speed post-processing in continuous-variable quantum key distribution based on FPGA implementation. *J Lightwave Technol.* 2020;38(15):3935–41.
56. Bai Z, Yang S, Li Y. High-efficiency reconciliation for continuous variable quantum key distribution. *Jpn J Appl Phys.* 2017;56(4):044401.
57. Bai Z, Wang X, Yang S, Li Y. High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution. *Sci China, Phys Mech Astron.* 2016;59(1):614201.
58. Mani H, Gehring T, Grabenweger P, Ömer B, Pacher C, Andersen UL. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. *Phys Rev A.* 2021;103(6):062419.
59. Wen X, Li Q, Mao H, Wen X, Chen N. An improved slice reconciliation protocol for continuous-variable quantum key distribution. *Entropy.* 2021;23(10):1317.
60. Jouguet P, Kunz-Jacques S, Leverrier A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys Rev A.* 2011;84(6):062317.
61. Li Q, Wen X, Mao H, Wen X. An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution. *Quantum Inf Process.* 2019;18(1):25.
62. Feng Y, Wang YJ, Qiu R, Zhang K, Ge H, Shan Z, et al. Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution. *Phys Rev A.* 2021;103(3):032603.
63. Wang X, Xu M, Zhao Y, Chen Z, Yu S, Guo H. Non-Gaussian reconciliation for continuous-variable quantum key distribution. *Phys Rev Appl.* 2023;19(5):054084.
64. Li Z, Zhang Y, Wang X, Xu B, Peng X, Guo H. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. *Phys Rev A.* 2016;93(1):012310.
65. Jiang XQ, Yang S, Huang P, Zeng G. High-speed reconciliation for CVQKD based on spatially coupled LDPC codes. *IEEE Photonics J.* 2018;10(4):7600410.
66. Richardson T, Urbanke R. *Modern coding theory.* Cambridge: Cambridge University Press; 2008.
67. Hirano T, Ichikawa T, Matsubara T, Ono M, Oguri Y, Namiki R et al. Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Sci Technol.* 2017;2(2):024010.
68. Shi JJ, Li BP, Huang D. Reconciliation for CV-QKD using globally-coupled LDPC codes. *Chin Phys B.* 2020;29(4):040301.
69. Chen J, Dholakia A, Eleftheriou E, Fossorier MPC, Hu XY. Reduced-complexity decoding of LDPC codes. *IEEE Trans Commun.* 2005;53(8):1288–99.
70. Hailes P, Xu L, Maunder RG, Al-Hashimi BM, Hanzo L. A survey of FPGA-based LDPC decoders. *IEEE Commun Surv Tutor.* 2016;18(2):1098–122.
71. Radosavljevic P, de Baynast A, Cavallaro JR. Optimized message passing schedules for LDPC decoding. In: *Asilomar conference on signals, systems and computers*; Pacific Grove, CA, USA; 30 Oct.-02 Nov. 2005; 2005. p. 591–5.
72. Yang SS, Liu JQ, Lu ZG, Bai ZL, Wang XY, Li YM. An FPGA-based LDPC decoder with ultra-long codes for continuous-variable quantum key distribution. *IEEE Access.* 2021;9:47687–97.
73. Richardson T, Urbanke R. Multi-edge type LDPC codes. In: *Workshop honoring prof. Bob McEliece 60th birthday*, California institute of technology, Pasadena, CA, USA. 2002. p. 24–5.
74. Wang X, Zhang Y, Li Z, Xu B, Yu S, Guo H. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *Quantum Inf Comput.* 2017;17(13&14):1123–34.
75. Jeong S, Jung H, Ha J. Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems. *npj Quantum Inf.* 2022;8:6.
76. Wang H, Li Y, Pi Y, Pan Y, Shao Y, Ma L et al. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. *Commun Phys.* 2022;5(1):162.
77. Ma L, Yang J, Zhang T, Shao Y, Liu J, Luo Y et al. Practical continuous-variable quantum key distribution with feasible optimization parameters. *Sci China Inf Sci.* 2023;66(8):180507.
78. Arıkan E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans Inf Theory.* 2009;55(7):3051–73.
79. Wang J, Jin A, Shi D, Wang L, Shen H, Wu D et al. Spectral efficiency improvement with 5G technologies: results from field tests. *IEEE J Sel Areas Commun.* 2017;35(8):1867–75.
80. Khan R, Kumar P, Jayakody DNK, Liyanage M. A survey on security and privacy of 5G technologies: potential solutions, recent advancements and future directions. *IEEE Commun Surv Tutor.* 2020;22(1):196–248.
81. Zhao S, Shen Z, Xiao H, Wang L. Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding. *Sci China, Phys Mech Astron.* 2018;61(9):90323.
82. Zhang M, Hai H, Feng Y, Jiang XQ. Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution. *Quantum Inf Process.* 2021;20(10):318.
83. Wang X, Wang H, Zhou C, Chen Z, Yu S, Guo H. Continuous-variable quantum key distribution with low-complexity information reconciliation. *Opt Express.* 2022;30(17):30455–65.
84. Cao Z, Chen X, Chai G, Peng J. IC-LDPC polar codes-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio. *Laser Phys Lett.* 2023;20(4):045201.
85. Cao Z, Chen X, Chai G, Liang K, Yuan Y. Rate-adaptive polar-coding-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio. *Phys Rev Appl.* 2023;19(4):044023.
86. Babar Z, Kaykac Egilmez ZB, Xiang L, Chandra D, Maunder RG, Ng SX et al. Polar codes and their quantum-domain counterparts. *IEEE Commun Surv Tutor.* 2020;22(1):123–55.
87. Luby M. LT codes. In: *The 43rd annual IEEE symposium on foundations of computer science*; Vancouver, BC, Canada; 2002. p. 271–80.
88. Shokrollahi A. Raptor codes. *IEEE Trans Inf Theory.* 2006;52(6):2551–67.
89. Perry J, Iannucci PA, Fleming KE, Balakrishnan H, Shah D. Spinal codes. In: *Proceedings of the ACM SIGCOMM 2012 conference on applications, technologies, architectures, and protocols for computer communication*; Helsinki, Finland; 2012. p. 49–60.
90. Ha J, Kim J, McLaughlin SW. Rate-compatible puncturing of low-density parity-check codes. *IEEE Trans Inf Theory.* 2004;50(11):2824–36.
91. Watanabe K, Kaguchi R, Shinoda T. Shortened LDPC codes accelerate OSD decoding performance. *J Wirel Commun Netw.* 2021;2021:22.

92. Shirvanimoghaddam M, Johnson SJ, Lance AM. Design of Raptor codes in the low SNR regime with applications in quantum key distribution. In: IEEE international conference on communications. 2016. p. 1–6.
93. Johnson SJ, Lance AM, Ong L, Shirvanimoghaddam M, Ralph TC, Symul T. On the problem of non-zero word error rates for fixed-rate error correction codes in continuous variable quantum key distribution. *New J Phys*. 2017;19(2):023003.
94. Zhou C, Wang X, Zhang Y, Zhang Z, Yu S, Guo H. Continuous-variable quantum key distribution with rateless reconciliation protocol. *Phys Rev Appl*. 2019;12(5):054013.
95. Asfaw MB, Jiang XQ, Zhan M, Hou J, Duan W. Performance analysis of Raptor code for reconciliation in continuous variable quantum key distribution. In: International conference on computing, networking and communications; Honolulu, HI, USA; 18-21 Feb. 2019; 2019. p. 463–7.
96. Park SI, Wu Y, Kim HM, Hur N, Kim J. Raptor-like rate compatible LDPC codes and their puncturing performance for the cloud transmission system. *IEEE Trans Broadcast*. 2014;60(2):239–45.
97. Zhou C, Wang X, Zhang Z, Yu S, Chen Z, Guo H. Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes. *Sci China, Phys Mech Astron*. 2021;64(6):260311.
98. Wen X, Li Q, Mao H, Luo Y, Yan B, Huang F. Novel reconciliation protocol based on spinal code for continuous-variable quantum key distribution. *Quantum Inf Process*. 2020;19(10):350.
99. Kiktenko EO, Malyshev AO, Fedorov AK. Blind information reconciliation with polar codes for quantum key distribution. *IEEE Commun Lett*. 2021;25(1):79–83.
100. Sarkis G, Giard P, Vardy A, Thibeault C, Gross WJ. Fast polar decoders: algorithm and implementation. *IEEE J Sel Areas Commun*. 2014;32(5):946–57.
101. Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe A et al. 10-Mb/s quantum key distribution. *J Lightwave Technol*. 2018;36(16):3427–33.
102. Zhang HF, Wang J, Cui K, Luo CL, Lin SZ, Zhou L et al. A real-time QKD system based on FPGA. *J Lightwave Technol*. 2012;30(20):3226–34.
103. Walenta N, Burg A, Caselunghe D, Constantin J, Gisin N, Guinnard O et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J Phys*. 2014;16(1):013047.
104. Paraíso TK, Roger T, Marangon DG, De Marco I, Sanzaro M, Woodward RI et al. A photonic integrated quantum secure communication system. *Nat Photonics*. 2021;15(11):850–6.
105. Sax R, Boaron A, Boso G, Atzeni S, Crespi A, Grünenfelder F et al. High-speed integrated QKD system. *Photon Res*. 2023;11(6):1007–14.
106. Li H, Pang Y. FPGA-accelerated quantum computing emulation and quantum key distillation. *IEEE MICRO*. 2021;41(4):49–57.
107. Li H, Wonfor A, Weerasinghe A, Alhussein M, Gong Y, Penty R. Quantum key distribution post-processing: a heterogeneous computing perspective. In: IEEE 35th international system-on-chip conference (SOCC); Belfast, United Kingdom; 2022. p. 1–6.
108. Zhou C, Li Y, Ma L, Luo Y, Huang W, Yang J et al. An efficient and high-speed two-stage decoding scheme for continuous-variable quantum key distribution system. *Proceedings of SPIE*. 12323. 2023.
109. Zhu M, Cui K, Li S, Kong L, Tang S, Sun J. A code rate-compatible high-throughput hardware implementation scheme for QKD information reconciliation. *J Lightwave Technol*. 2022;40(12):3786–93.
110. Lu Q, Lu Z, Yang H, Yang S, Li Y. FPGA-based implementation of multidimensional reconciliation encoding in quantum key distribution. *Entropy*. 2023;25(1):80.
111. Wang J, Sciarino F, Laing A, Thompson MG. Integrated photonic quantum technologies. *Nat Photonics*. 2020;14(5):273–84.
112. Feng L, Zhang M, Wang J, Zhou X, Qiang X, Guo G et al. Silicon photonic devices for scalable quantum information applications. *Photon Res*. 2022;10(10):A135–53.
113. Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys Rev A*. 2007;76(4):042305.
114. Milicevic M, Feng C, Zhang LM, Gulak PG. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *npj Quantum Inf*. 2018;4:21.
115. Wang X, Zhang Y, Yu S, Guo H. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code. *Sci Rep*. 2018;8:10543.
116. Li Y, Zhang X, Li Y, Xu B, Ma L, Yang J et al. High-throughput GPU layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems. *Sci Rep*. 2020;10:14561.
117. Guo D, He C, Guo T, Xue Z, Feng Q, Mu J. Comprehensive high-speed reconciliation for continuous-variable quantum key distribution. *Quantum Inf Process*. 2020;19(9):320.
118. Xie J, Zhang L, Wang Y, Huang D. Deep neural network based reconciliation for CV-QKD. *Photonics*. 2022;9(2):110.
119. Pacher C, Martinez-Mateo J, Duhme J, Gehring T, Furrer F. Information reconciliation for continuous-variable quantum key distribution using non-binary low-density parity-check codes. 2016. [arXiv:1602.09140](https://arxiv.org/abs/1602.09140).
120. Bloch M, Thangaraj A, McLaughlin SW, Merolla JM. LDPC-based Gaussian key reconciliation. In: IEEE information theory workshop; Punta del Este, Uruguay; 2006. p. 116–20.
121. Lu Z, Yu L, Li K, Liu B, Lin J, Jiao R et al. Reverse reconciliation for continuous variable quantum key distribution. *Sci China, Phys Mech Astron*. 2010;53(1):100–5.
122. Jouguet P, Elkouss D, Kunz-Jacques S. High-bit-rate continuous-variable quantum key distribution. *Phys Rev A*. 2014;90(4):042329.
123. Zhang K, Jiang XQ, Feng Y, Qiu R, Bai E. High efficiency continuous-variable quantum key distribution based on ATSC 3.0 LDPC codes. *Entropy*. 2020;22(10):1087.
124. Fan X, Niu Q, Zhao T, Guo B. Rate-compatible LDPC codes for continuous-variable quantum key distribution in wide range of SNRs regime. *Entropy*. 2022;24(10):1463.
125. Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouiri R, Grangier P. Field test of a continuous-variable quantum key distribution prototype. *New J Phys*. 2009;11(4):045023.
126. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photonics*. 2013;7(5):378–81.

127. Wang C, Huang D, Huang P, Lin D, Peng J, Zeng G. 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel. *Sci Rep.* 2015;5:14607.
128. Zhang Y, Li Z, Chen Z, Weedbrook C, Zhao Y, Wang X et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci Technol.* 2019;4(3):035006.
129. Xu Y, Wang T, Zhao H, Huang P, Zeng G. Round-trip multi-band quantum access network. *Photon Res.* 2023;11(8):1449–64.
130. Wang X, Chen Z, Li Z, Qi D, Yu S, Guo H. Experimental upstream transmission of continuous variable quantum key distribution access network. *Opt Lett.* 2023;48(12):3327–30.
131. van Deventer O, Spethmann N, Loeffler M, Amoretti M, van den Brink R, Bruno N et al. Towards European standards for quantum technologies. *EPJ Quantum Technol.* 2022;9(1):33.

### **Publisher's Note**

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Submit your manuscript to a SpringerOpen<sup>®</sup> journal and benefit from:**

- ▶ Convenient online submission
- ▶ Rigorous peer review
- ▶ Open access: articles freely available online
- ▶ High visibility within the field
- ▶ Retaining the copyright to your article

---

Submit your next manuscript at ▶ [springeropen.com](https://www.springeropen.com)

---