Chin. Phys. B Vol. 29, No. 4 (2020) 040301

Reconciliation for CV-QKD using globally-coupled LDPC codes*

Jin-Jing Shi(石金晶), Bo-Peng Li(李伯鹏), and Duan Huang(黄端)†

School of Computer Science and Engineering, Central South University, Changsha 410083, *China*

(Received 26 November 2019; revised manuscript received 13 January 2020; accepted manuscript online 20 January 2020)

Reconciliation is a necessary step in postprocessing of continuous-variable quantum key distribution (CV-QKD) system. We use globally coupled low-density parity-check (GC-LDPC) codes in reconciliation to extract a precise secret key from the raw keys over the authenticated classical public channel between two users. GC-LDPC codes have excellent performance over both the additive Gaussian white noise and binary-erasure channels. The reconciliation based on GC-LDPC codes can improve the reconciliation efficiency to 95.42% and reduce the frame error rate to 3.25×10^{-3}. Using distillation, the decoding speed can achieve 23.8 Mbits/s and decrease the cost of memory. Given decoding speed and low memory usage, this makes the proposed reconciliation method viable approach for high-speed CV-QKD system.

Keywords: continuous-variable quantum key distribution, globally coupled low-density parity-check, reconciliation efficiency, frame error rate

PACS: 03.67.–a, 03.67.Dd, 03.67.Hk, 03.67.Pp **DOI:** 10.1088/1674-1056/ab6d4f

1. Introduction

Quantum key distribution (QKD)[1] system allows two legitimate parties Alice and Bob, linked by a quantum channel and an authenticated classical channel, to share a common random binary key that is unknown to a potential eavesdropper, Eve.[2] The security of QKD is guaranteed by the no-cloning theorem of quantum mechanics. The no-cloning theorem considers that Eve measuring or observing quantum channels would disturb the coherent state which is transmitted from Alice to Bob.[3,4] There have been increased experimental efforts recently in QKD to prove the safety of QKD.[5–7] Continuous variable (CV) and discrete variable (DV) are two major types of QKD system. DV-QKD protocols encode information on the phase or the polarization of single photons.[8] Many schemes are proposed for DV-QKD systems,[9,10] and some of them have been explored to realize long distance and high secure key rate.[11,12] In information reconciliation process, we use low-density parity-check (LDPC) codes to reduce the information which Eve obtains from the honest parties Alice and Bob.[13,14] In CV-QKD system, Alice encodes her information in the amplitude and phase quadrature of coherent states[15,16] and sends it to Bob. On his side, Bob measures the quantum states using homodyne or heterodyne detector.[17,18] The CV-QKD provides a higher repetition rate, which provides a scheme to achieve a higher security key rate.[19]

In CV-QKD, the quantum channel used by Alice and Bob to create secret key is not deemed to be prefect. Noise will make the secret key different between Alice and Bob.[20,21] The information between Alice and Bob, along with the information which Eve gains by monitoring the reconciliation protocol, must then be corrected via post-processing. The post-processing of the CV-QKD system includes the following steps: sifting,[22] parameter estimation,[23,24] information reconciliation,[25] and privacy amplification.[26–29] The post-processing procedure is used to extract final secret key from the obtained raw key,[30] and the information reconciliation is used to correct the errors between Alice's and Bob's raw keys by exchanging error correcting messages through an authenticated classical channel.[31] We use LDPC codes to complete information reconciliation in our scheme. There are two types of information reconciliation, *i.e.*, direct reconciliation and reverse reconciliation.[32] Direct reconciliation is that Bob corrects its codeword based on Alice, while reverse reconciliation is that Alice corrects its codeword based on Bob. Due to the safe transmission distance cannot exceed the 3-dB limitation during direct reconciliation, only reverse reconciliation is considered in all safety considerations at this stage.

In order to improve the efficiency of information reconciliation[33,34] for the additive white Gaussian noise channel, we complete reverse reconciliation using check node-based quasi-cyclic globally coupled low-density parity-check (CN-based QC-GC-LDPC) codes which decrease the frame error rate (FER) of CV-QKD. Improving the efficiency can increase the secret key rate. CN-based QC-GC-LDPC codes have a different structure compared to the conventional LDPC block codes and the spatially coupled LDPC (SC-LDPC) codes. Reverse reconciliation[35–37] based on GC-LDPC codes can provide higher reconciliation efficiency than other block codes. After distillation, the decoding speed of reverse reconciliation can reach 23.8 Mbits/s. Through the simulation of our

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61801522, 61972418, and 61872390), the Natural Science Foundation of Hunan Province, China (Grant Nos. 2019JJ40352 and 2017JJ3415), and the Special Foundation for Distinguished Young Scientists of Changsha City, China (Grant No. kq1905058).

†Corresponding author. E-mail: duanhuang@csu.edu.cn

scheme, we obtain the reconciliation efficiency of CN-based QC-GC-LDPC codes can reach 95.42%. Reverse reconciliation using GC-LDPC codes also reduce the FER of CVQKD system, the FER can reach 3.25×10^{-3} and the bit error rate (BER) can be reduced to 5.45×10^{-7}. These will make the proposed scheme have high reconciliation performance.

The paper is arranged as follows: In Section 2, after brief introduction on GC-LDPC, we introduce the CN-based QC-GC-LDPC codes, and then we present the reconciliation scheme based on CN-based QC-GC-LDPC codes in Subsection 2.2. In Subsection 2.3, we discuss the decoding of CN-based QC-GC-LDPC code scheme in CV-QKD system. The performance of reverse reconciliation based on CN-based QC-GC-LDPC codes is given in Section 3, which includes high decoding speed method, low frame error rate, and high reconciliation efficiency. Finally, conclusion are drawn in Section 4.

2. Reconciliation based on CN-based QC-GC-LDPC codes

CN-based QC-GC-LDPC codes, which were proposed by Li *et al.* in Ref. [38], are a special type of LDPC codes with a structure related to but different from that of the SC-LDPC codes. From the perspective of Tanner graph, GC-LDPC codes are composed of a series of disjoint Tanner graphs which are connected together by a group of overall check-nodes (CNs), called global CNs. LDPC codes with this type are called CN-based QC-GC-LDPC codes, which have excellent performance in both the additive white Gaussian noise channel (AWGNC) and the binary erasure channel (BEC).

2.1. CN-based QC-GC-LDPC codes

CN-based QC-GC-LDPC codes are a kind of quasi-cyclic linear block codes. They are defined by their sparse parity check matrices $H = (h_{ij})_{m\times n}$ of size $m \times n$ where h_{ij} are elements of a binary Galois field GF(2) or non-binary Galois field GF(q) where $q > 2$. The construction method of CN-based QC-GC-LDPC codes has been introduced in detail in Ref. [39]. Here we briefly introduce the structural characteristics of CN-based QC-GC-LDPC codes. A CN-based QC-GC-LDPC codes are composed of base matrix B_{gc} which consists of two submatrices as shown:

$$B_{\mathrm{gc}} = \begin{pmatrix} R_1 & & & & & \\ & R_2 & & & & \\ & & \ddots & & & \\ & & & R_i & & \\ & & & & \ddots & \\ & & & & & R_t \\ - & - & - & - & - & - \\ & & X_{\mathrm{gc}} & & & \end{pmatrix}. \tag{1}$$

The above submatrix of B_{gc} is a diagonal matrix of size $t \times t$ and B_{gc} is consisted by diagonal array which includes $(m \times n)$-dimensional matrices R and the lower submatrix is matrix X_{gc}, where the form of R are derived from Reed–Solomon-based array and the matrix X_{gc} is an $(s \times nt)$-dimensional matrix. The matrix B_{gc} and X_{gc} represent “check node” and “global coupling”, respectively.

Denote the parity-check matrix of CN-based QC-GC-LDPC codes as $H_{\mathrm{qc,gc}}$ as shown in Eq. (2). $H_{\mathrm{qc,gc}}$ is made up of the base matrix B_{gc} and $(q-1)$-fold dispersion.[40] In B_{gc} matrix, if its element $b_{i,j} = 0$, we replace $b_{i,j}$ with a $(q-1) \times (q-1)$ zero matrix (ZM); otherwise, if $b_{i,j} \neq 0$, we replace $b_{i,j}$ by a $(q-1) \times (q-1)$ circulant permutation matrix (CPM).[41]

$$H_{\mathrm{qc,gc}} = \begin{pmatrix} CPM_{(R_1)} & & & \\ & CPM_{(R_2)} & & \\ & & \ddots & \\ & & & CPM_{R_k} \\ - & - & - & - \\ & & CPM_{(X_{\mathrm{gc}})} & \end{pmatrix}. \tag{2}$$

Same as other types of LDPC codes, CN-based QC-GC-LDPC codes can also be represented by Tanner graphs as shown in Fig. 1. Its Tanner graphs are divided into two parts, t disjoint copies of the local Tanner graphs g_{lo} and s global check nodes respectively. The s global check nodes provide the only connections between any two disjoint local Tanner graphs.

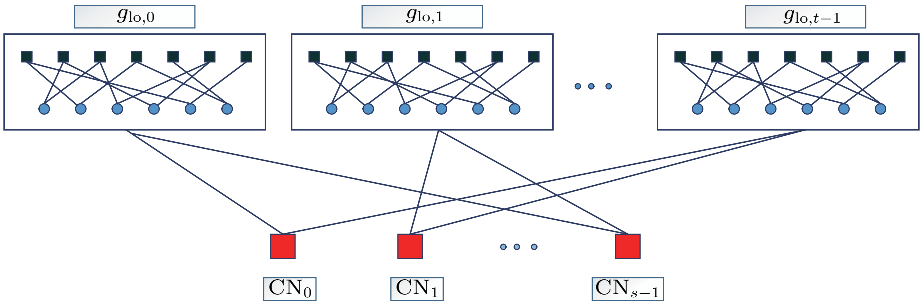

Fig. 1. The Tanner graphs of CN-based QC-GC-LDPC codes. The upper t disjoint copies are local Tanner graphs and the lower s check nodes are global check nodes which provide the only connections between the t disjoint local Tanner graphs.

2.2. Reconciliation based on CN-based QC-GC-LDPC codes

In CV-QKD system, Alice transmits N quantum coherent states to Bob through a quantum channel,[42] *i.e.*, $y_0 = t \times x_0 + z$, where $t = \sqrt{\eta_{\text{loss}}} \times T$, where η_{loss} is detection efficiency and T is the transmission efficiency, and z is the noise term subjecting to a centered normal distribution with a zero mean and noise variance of σ_z^2. Alice's and Bob's data are different due to imperfection of quantum channel. The main reason for imperfection is the existence of noise. After exchanging some quantum states on the quantum channel, Alice and Bob share some common data to complete the information reconciliation process. In order to complete the reverse reconciliation, Alice and Bob construct two new correlated Gaussian sequences from the sifted correlation sequences $X_0 = [x_1, x_2, \ldots, x_{\text{quantum}}]$ and $Y_0 = [y_1, y_2, \ldots, y_{\text{quantum}}]$ of length N_{quantum}. Alice and Bob select a set of elements U of length n, which $n < N_{\text{quantum}}$. In addition, n is equal to the LDPC codes block length.[15] The string U is selected as the secret key which will be transferred between Alice and Bob.[43]

As shown in Fig. 2, when Alice sends quantum information X_0 through a quantum channel, the string Y_0 received by Bob will be correlated to X_0 but not equal to X_0 due to the existence of channel noise. We correct the sequence X_0 according to the sequence Y_0 using the reverse reconciliation. Bob modulates the quantum information Y_0 to get M using random key U. Then Bob sends side information α to Alice to describe the method of obtaining M. Alice receives the side information α and applies α to X_0 to get U', where U' can be regarded as a noisy version of U. Alice and Bob reconstruct U' and U using the computationally intensive Sum-Product belief propagation decoding algorithm (BP algorithm) respectively.[44,45] The reverse reconciliation is described in detail in Subsection 2.3.

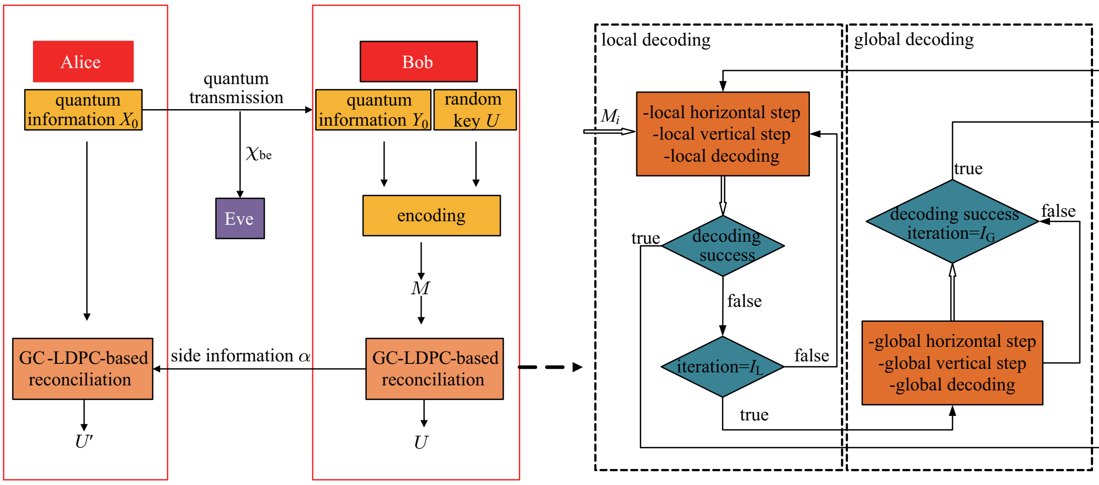

Fig. 2. The reverse reconciliation based on GC-LDPC codes provide the secondary reconciliation for the CV-QKD system, which can reduce the FER and BER. Using GC-LDPC codes can improve the performance of CV-QKD.

2.3. Decoding of CN-based QC-GC-LDPC codes in reverse reconciliation

We mentioned the BP algorithm in Subsection 2.2. In this section we will describe the decoding algorithm for the reverse reconciliation protocol[46,47] in detail. In CV-QKD system, Alice uses the BP algorithm to correct the classic messeage M over an optic fiber, where $M_i = (-1^{U_i} Y_{0_i})$. Considering structural characteristics of CN-based QC-GC-LDPC codes, the decoding process is divided into two parts: local decoding and global decoding. The received data M divides t sequences and decoded by t-independent decoders. If t sequences are decoded successfully and the locally decoded codeword U satisfies constraints of the parity-check $H_{\text{qc,gc}}$, *i.e.*, $U \times H_{\text{qc,gc}}^{\text{T}} = 0$, the codeword U could be delivered to remove the channel noise from her received message M, where $H_{\text{qc,gc}}^{\text{T}}$ is the transposed matrix of the matrix $H_{\text{qc,gc}}$. If local decoders encounter error during the decoding process, *i.e.*, $U \times H_{\text{qc,gc}}^{\text{T}} \neq 0$, we switch the decoding from the local part to global part through the global check nodes. In general, the global decoders are needed only when the amount of error in local decoding is large.

In the BP decoding algorithm, the quantities of non-zero elements in check nodes (CNs) and variable nodes (VNs) are constantly updated during the iteration. The operations of message passing can be described as follows:[48]

Step 1 Initialization

$$\begin{aligned} p_l^0 &= P, & x_l &= 0, \\ p_l^1 &= P = 1 - p_l^0, & x_l &= 1, \end{aligned} \tag{3}$$

where $x_l = 0$ means the prior probability of bit x_1 in received data is 0.

Step 2 Horizontal step

In the horizontal step, we calculate message $L(r_{ji})$ of each *CN* which passed from CNs to VNs. This step is used to update message of CNs.

$$L(r_{ji}) = 2 \times \tanh^{-1}\left(\prod_{i' \in R_{j\backslash i}} \tanh\left(\frac{1}{2} \times L(q_{i'j})\right)\right), \quad (4)$$

where r_{ji} is the message passed from CNs to VNs, $q_{i'j}$ is the message passed from VNs to CNs, $\tanh(\cdot)$ is the hyperbolic tangent function, and $\tanh^{-1}(\cdot)$ is the reverse hyperbolic tangent function. In addition, R_j is the set of column positions of element 1 in the j-th row of matrix H, $R_{j\backslash i}$ is the set of column positions of element 1 in the j-th row of matrix H excluding position i.

We depict the CN decoder situation in Fig. 3. Note that the CN$_j$ decoder receives message from the channel and the variable nodes connected to it, excluding the message from VN$_i$. After calculating these message using Eq. (4), CN$_j$ sends $L(r_{ji})$ to VN$_i$.

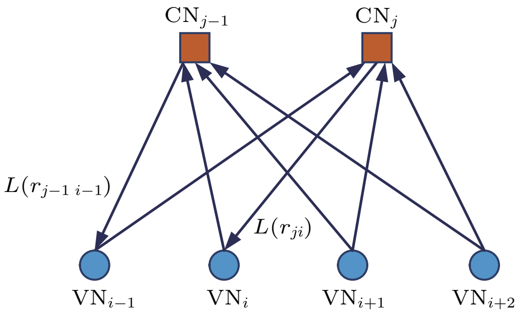

Fig. 3. Figure of the horizontal step. The message $L_{r_{ji}}$ is calculated based on information from all of its variable nodes, excluding message from VN$_i$, and message $L_{(r_{ji})}$ is sent to VN$_i$.

Step 3 Vertical step

In this step, we calculate message $L(q_{ij})$ of each VN which passed from VNs to CNs. In Fig. 4, we describe the process of information update about VNs in detail. This process includes calculating the message from the channel and the check nodes connected to it excluding the message from CN$_j$. After calculating these message using Eq. (5), VN$_i$ sends message $L(q_{ij})$ to CN$_j$.

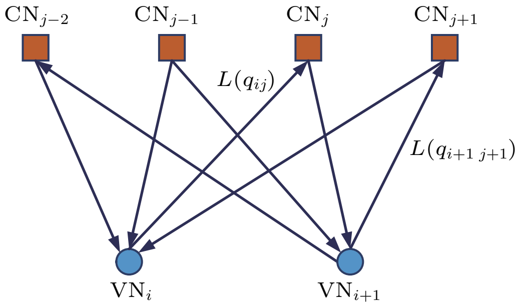

Fig. 4. This figure shows the vertical step. The message $L_{(q_{ij})}$ is calculated based on information from all of its check nodes, excluding message from CN$_j$, and message $L_{(q_{ij})}$ is sent to CN$_j$.

$$L(q_{ij}) = L(p_i) + \sum_{j' \varepsilon C_{i\backslash j}} L(r_{j'i}), \quad (5)$$

where P_i is initialized decoding information. $L(r_{ji})$, $L(q_{ij})$, and $L(P_i)$ are the log-domain versions of r_{ji}, q_{ij}, and P_i. Similarly, C_i is the set of row locations of element 1 in the i-th column, and $C_{i\backslash j}$ is the same as C_i, expect that location j is not included.

Step 4 Decoding

$$L(P_i) = L(p_i) + L(r_{ji}),$$
$$p_i = \begin{cases} 1 & \text{if} \quad L(Pi) < 0, \\ 0 & \text{otherwise.} \end{cases} \quad (6)$$

If $p_i \times H^t = 0$ or the number of iterations equals the maximum limit, stop; else, go to Step 2.

3. Performance of reverse reconciliation based on CN-based QC-GC-LDPC codes

In this section, we will introduce the performance of reverse reconciliation based on CN-based QC-GC-LDPC codes. There are some indicators that can reflect the performance of the reverse reconciliation, such as bit error rate, frame error rate, decoding speed, and reconciliation efficiency β.

3.1. The speed of decoding

In order to achieve high speed of the reverse reconciliation, it is necessary to analyze the factors which affect the reconciliation speed. Some factors will affect the reconciliation speed in different aspects, such as the decoding algorithm. The decoding algorithm is the most important factor affecting the reconciliation speed, and it is also the most important step of the reverse reconciliation. We use the BP algorithm to complete the reverse reconciliation. We apply the check matrix $H_{\text{qc,gc}}$ in the BP algorithm and the sparsity and irregularity of the check matrix bring the difficulty in calculation and decoding.

Considering the sparsity of the check matrix $H_{\text{gc,qc}}$, we apply "distillation" to reduce the complexity of the operation about the error correction.[4] Since the decoding process of BP algorithm is related to the column and row position of element 1 in $H_{\text{qc,gc}}$, we transform the sparse check matrix $H_{\text{qc,gc}}$ into two one-dimensional matrices, which contain the column and row positions of elements 1 in the $H_{\text{qc,gc}}$ matrix. For a clear expression, we use an example to illustrate the process of the matrix transformation. Assume that the matrix H is shown below

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \quad (7)$$

After the process of "distillation", we use one-dimensional vector row and col to represent the position of elements of 1 in matrix H.

$$\begin{aligned} M &= [1\ 1\ 1\ 2\ 2\ 2\ 2\ 3\ 3\ 3\ 4\ 4\ 4], \\ N &= [1\ 2\ 3\ 4\ 5\ 6\ 1\ 4\ 7\ 2\ 5\ 8]. \end{aligned} \tag{8}$$

The vector M represents the row position of each element 1 in the matrix H and the vector N represents the column position of each element 1 in the matrix H. Figure 5 presents the decoding speed of the BP algorithm and the BP algorithm using distillation with a code length range from 1000 bits to 14000 bits in a Intel Core i5-8400 CPU and an NVIDIA Tesla K80 GPU. In GPU-based decoding process, we first copy the message of row keys from CPU to GPU. Then we initialize the message of CNs and VNs. Next we update message of CNs and VNs using horizontal step and vertical step. After reaching the maximum number of iterations I or successful decoding, we get decoded data using Eq. (6) and copy them from GPU to CPU. In the reverse reconciliation process, we use the structural characteristics of CN-based QC-GC-LDPC code as shown in Fig. 1. First, we decode the received data in the local decoder. When the decoding fails and the number of iterations I_{L} of the local decoders is reached, the failed data are sent to the global decoder for secondary decoding, which can reduce FER and improve reconciliation efficiency. The decoding speed using distillation reaches 0.68 Mbits/s in an Intel Core i5-8400 CPU and reaches 23.8 Mbits/s in an NVIDIA Tesla K80 GPU. We know that the decoding speed of the BP algorithm will increase after using distillation.

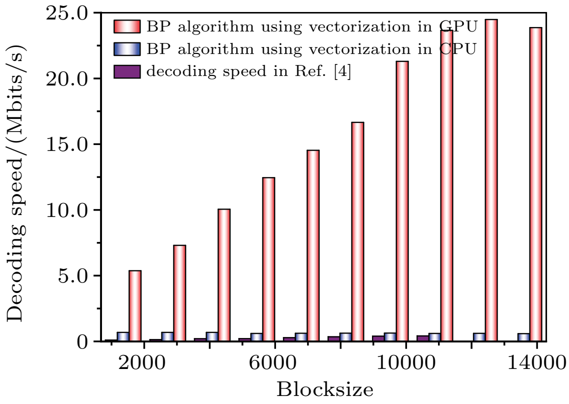

Fig. 5. The decoding speed about BP algorithm and BP algorithm using distillation. The decoding speed of BP algorithm using distillation reaches 0.68 Mbits/s in an Intel Core i5-8400 CPU, which is better than BP algorithm. The decoding speed reaches 23.8 Mbits/s in an NVIDIA Tesla K80 GPU. The blue columnar bar represents the decoding speed mentioned in Ref. [4].

Thus, using distillation will affect the decoding process, which means that the two-dimensional matrix is involved during decoding. The two-dimensional matrix is characterized by $L_{(r_{ji})}$ and $L_{(q_{ij})}$, respectively. After distillation, the $L_{(r_{ji})}$ and $L_{(q_{ij})}$ introduced in Subsection 2.3 are represented by $L_{(r_n)}$ and $L_{(q_n)}$.

$$L(r_n) = 2 \times \tanh^{-1}\left(\prod_{n' \varepsilon R_{M_{(n)}} \backslash N_{(n)}} \tanh\left(\frac{1}{2} \times L(q_{n'})\right)\right), \tag{9}$$

$$L(q_n) = L(p_{M_{(n)}}) + \sum_{n' \varepsilon C_{N_{(n)}} \backslash M_{(n)}} L(r_{n'}), \tag{10}$$

where $M_{(n)}$ and $N_{(n)}$ are the row and column position look-up tables.

We should notice that the range of subscripts i in Eq. (4) and Eq. (5) is different from subscripts n in Eq. (9) and Eq. (10). The size of $L_{(r_{ji})}$ and $L_{(q_{ij})}$ is $m \times n$ (the size of matrix H), while the size of $L_{(r_n)}$ and $L_{(q_n)}$ is P, where P is the number of element 1 in H. Distillation brings the benefit of improving the speed of decoding. Besides, distillation can decrease the cost of memory due to the sparsity of matrix H. The sparsity of H matrix leads to high complexity in the reverse reconciliation. We use distillation to reduce the computational complexity, which is used to extract 1 elements of H matrix. The decoding speed of the reverse reconciliation using distillation can achieve 23.8 Mbits/s in an NVIDIA Tesla K80 GPU.

3.2. Secret key rate and low frame error rate

As described in Subsection 2.3, in the reverse reconciliation, the codeword of Bob is sent to Alice the error correction in the form of frame U. if the result of the calculation is $U \times H_{\mathrm{qc,gc}}^{\mathrm{T}} \neq 0$, the decoding fails. In order to express the possibility of decoding failure, we introduce the frame error rate (FER). The FER is one of the most critical parameters of an error-correcting code, since decoding a message failure is usually associated with data loss in conventional data transmission scenarios, resulting in retransmission delays, that is, the original key blocks decoded incorrectly are discarded by Bob and Alice in the CV-QKD system. Based on base graph 1 in 5G standard, we construct a parity check matrix $H_{\mathrm{qc,gc}}$ of size 21712×32096 and code rate 0.3235.[49] Figure 6(a) shows the performance of the CN-based QC-GC-LDPC codes in terms of the BER, where the BER of code length 32096 can reach 5.45×10^{-7}. Figure 6(b) shows the performance of the FER about the CN-based QC-GC-LDPC codes, where the FER of code length 32096 can reach 3.25×10^{-3}. In Fig. 6(a), we can see that the performance of the BER increases as the code length increases of the same code. Figures 6(c) and 6(d) show the performances of BER and FER under different iterations. When the code length is infinite, the decoding speed will be slow due to the computing power of the CPU, so the code length we used is 32096. As a result, the finial key rate will be affected by $(1-FER)$, and the secret key rate[46,50,51] of the reverse reconciliation under collective attack can be represented as

$$K = (1-FER)(\beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}), \tag{11}$$

where β is the efficiency of the reverse reconciliation using CN-based QC-GC-LDPC codes, I_{AB} denotes the Shannon mutual information of Alice and Bob, which is numerically equal to the capacity of the channel. $\chi_{\rm BE}$ denotes the Holevo bound on the information between Bob and Eve.[52–54]

$$I_{\rm AB} = \frac{1}{2}\log_2(1+s) = \frac{1}{2}\log_2\left(\frac{V+\chi_{\rm total}}{1+\chi_{\rm total}}\right), \tag{12}$$

where $V = V_{\rm A}+1$, $V_{\rm A}$ is modulation variance of Alice, and $\chi_{\rm total}$ is the total noise between Alice and Bob. The Holevo bound $\chi_{\rm BE}$ is

$$\chi_{\rm BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{13}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, the $\lambda_{1,2,3,4,5}$ are given by $\lambda_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2-4B})$ and $\lambda_{3,4}^2 = \frac{1}{2}(C \pm \sqrt{C^2-4D})$, $\lambda_5 = 1$, where

$$\begin{aligned} A &= V^2(1-2T) + 2T + T^2(V+\chi_{\rm line})^2, \\ B &= T^2(V\chi_{\rm line}+1)^2, \\ C &= \frac{A\chi_{\rm h} + V\sqrt{B} + T(V+\chi_{\rm line})}{T(V+\chi_{\rm total})}, \\ D &= \frac{\sqrt{B}V + B\chi_{\rm h}}{T(V+\chi_{\rm total})}, \end{aligned} \tag{14}$$

where $\chi_{\rm h}$ is the additive noise of the detector which is attributed to the channel input. $\chi_{\rm h} = [(1-\eta)+v_{\rm el}]/\eta$, where η represents the quantum efficiency of detection of Bob, and $v_{\rm el}$ is the detector electrical noise. T is the transmittance of the CV-QKD system. The $\chi_{\rm line}$ is the channel additive noise which attributed to the input, $\chi_{\rm line} = 1/T - 1 + \xi$, where ξ is the system noise.

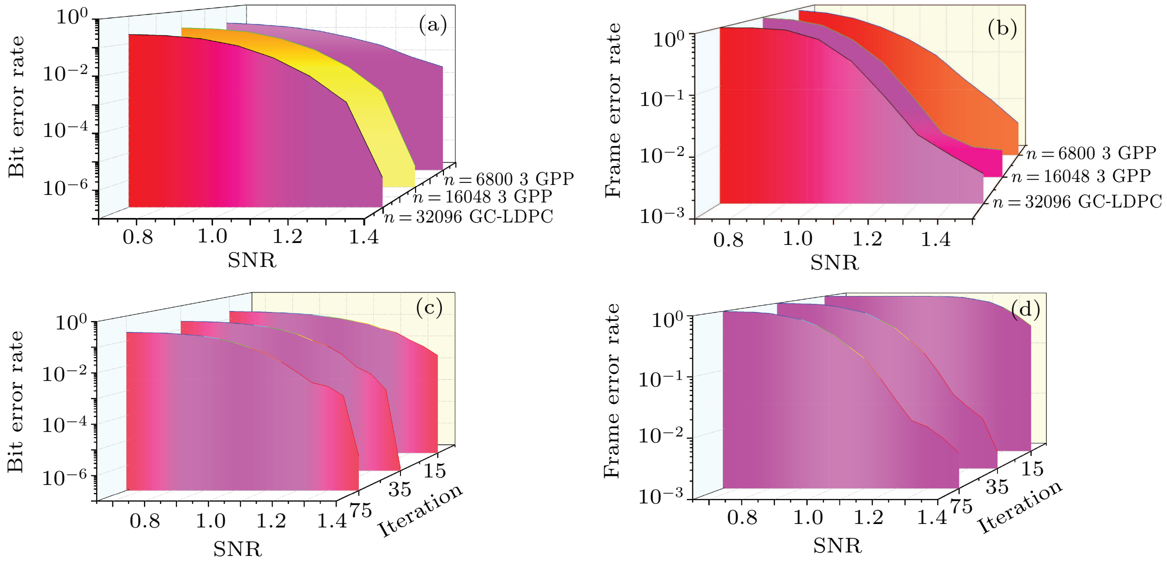

Fig. 6. (a) The BER performance of CN-based QC-GC-LDPC codes over AWGN channel. The BER can reach 10^{-7} using the Belief-propagation decoding algorithm. (b) The FER performance of CN-based QC-GC-LDPC codes over AWGN channel. The FER can reach 10^{-3} using the Belief-propagation decoding algorithm. (c) The performance of BER for different iterations. This figure shows the BER with 75, 35, and 15 iterations. As the number of iterations increases in the reverse reconciliation, the BER is more accurate. (d) The performance of FER under different iterations. This figure shows the FER with 75, 35, and 15 iterations. As the number of iterations increase in the reverse reconciliation, the FER is more accurate.

3.3. Reconciliation efficiency

Although the error correction problem has never been a critical issue for DV-QKD protocol, it only contains a small correction item, error correction is necessary for a CV-QKD protocol. For CV-QKD protocol, Alice and Bob need to extract their mutual information $I_{\rm AB}$ effectively. According to Eq. (11), the reconciliation efficiency affects the generation of the secret key rate. According to Eq. (15), the calculated reconciliation efficiency of our proposal is 95.42%, which is better than the one proposed in Refs. [46,50]. The reconciliation efficiency $\beta_{\rm qc,gc}$ can be expressed as

$$\beta_{\rm qc,gc} = \frac{R_{\rm code}}{C_{(s)}}, \tag{15}$$

where $R_{\rm code}$ is the code rate which is equal to k/n from the k-length information M and codeword U of length n, $C_{(s)}$ is the Shannon capacity and $C_{(s)} = 1/2\log_2(1+s)$ in which s is the SNR of the AWGNC[15,55] and $s = 1/\sigma^2$, σ^2 is the noise variance.

$$H = \begin{array}{|c|c|c|} \hline H_{\rm qc,gc} & A & 0 \\ \hline E & 0 & I \\ \hline \end{array} \tag{16}$$

The CN-based QC-GC-LDPC codes are descried in Ref. [40], the code rate is 0.4924 and the SNR Shannon limit is 1.12, using Eq. (15) we can gain the reverse reconciliation efficiency 90.8%. In order to improve the efficiency of the reconciliation, we need to reduce the code rate to increase the amount of redundant information. We briefly introduce the method of reducing the code rate via repetition coding mentioned in Ref. [56]. Starting with the repeat-accumulate (RA) code, additional rows and columns are appended as shown in Eq. (16). The matrix I is the identity matrix (ones on the diagonal, zeros elsewhere), and the matrix 0 is an all zero matrix. The matrix E can be formed from the first two columns of a truncated Vandermonde matrix. In our paper, we use repeat-accumulate codes[56] to reduce the GC-LDPC code rate to 0.3235 and SNR is 0.6 and we obtain the reverse reconciliation efficiency 95.42%. As shown in Table 1, using GC-LDPC codes provides higher efficiency of the reverse reconciliation.

Table 1. The efficiencies of the reverse reconciliation in the proposed and the previous reconciliation schemes.

Refs	Code type	SNR	Efficiency of reconciliation
Paul *et al.*[42]	LDPC	0.55	93.4%
		0.86	93.7%
		1.0	94.2%
Jérŏme *et al.*[46]	LDPC	2.0	86.7%
		3.25	89.8%
This work	GC-LDPC	0.6	95.42%

4. Conclusion

In this paper, we introduced the reverse reconciliation of CV-QKD system using CN-based QC-GC-LDPC codes. It was shown that the proposed scheme can provide more efficiencies and reduce the BER and FER in the reverse reconciliation. Given high complexity of the sparsity of check matrix in the reverse reconciliation, we use distillation to reduce the computational complexity, and the decoding speed of reconciliation can achieve 23.8 Mbits/s. Low FER and high decoding speed enable the CV-QKD system to quickly complete quantum key distribution. The excellent performance of CN-based QC-GC-LDPC codes can be applied in high-speed CVQKD system.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Wang X Y, Zhang Y C, Yu S and Guo H 2018 *Sci. Rep.* **8** 10543

[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[4] Lin D K, Huang D, Huang P, Peng J Y and Zeng G H 2015 *Int. J. Quantum. Inf.* **13.02** 100501

[5] Qian Y J, He D Y, Wang S, Chen W, Yin Z Q, Guo G C and Han Z F 2019 *Optica* **6** 1178

[6] Wang S, Chen W, Yin Z Q, He D Y, Hui C, Hao P L, Fan-Yan G J, Wang C, Zhang L J, Kuang J, Liu S F, Zhou Z, Wang Y G, Guo G C and Han Z F 2018 *Opt. Lett.* **43** 2030

[7] Wang S, Yin Z Q, Chau H F, Chen W, Wang C, Guo G C and Han Z F 2018 *Quantum Science and Technology* **3** 025006

[8] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C and Han Z F 2019 *Phys. Rev. X* **9** 021046

[9] Yin Z Q, Wang S, Chen W, Han Y G, Wang R, Guo G C and Han Z F 2018 *Nat. Commun.* **9** 457

[10] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat. Phoron.* **9.12** 832

[11] Wang S, Chen W, Guo J F, Yin Z Q, Li H W, Zhou Z, Guo G C and Han Z F 2012 *Opt. Lett.* **37** 1008

[12] Wang S, Chen W, Yin Z Q, Li H W, He D Y, Li Y H, Zhou Z, Song X T, Li F Y, Wang D, Chen H, Han Y G, Huang J Z, Guo J F, Hao P L, Li M, Zhang C M, Liu D, Liang W Y, Miao C H, Wu P, Guo G C and Han Z F 2014 *Opt. Express* **22** 21739

[13] Assche G V, Cardinal J and Cerf N J 2004 *IEEE Trans. Inf. Theory* **50** 394

[14] Furrer F 2014 *Phys. Rev. A* **90** 042325

[15] Milicevic M, Chen F, Zhang L M and Gulak P G 2018 *Npj. Quantum Inform.* **4** 21

[16] Diamanti E, Lo H K, Qi B and Yuan Z 2016 *Npj. Quantum Inform.* **2** 16025

[17] Huang D, Huang P, Li H S, Wang T, Zhou Y M and Zeng G H 2016 *Opt. Lett.* **41** 3511

[18] Huang D, Huang P, Wang T, Li H S, Zhou Y M and Zeng G H 2016 *Phys. Rev. A* **94** 032305

[19] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photon.* **7** 378

[20] Tang G Z, Sun S H and Li C Y 2019 *Chin. Phys. Lett.* **36** 70301

[21] Jiang X Q, Huang P, Huang D, Lin D K and Zeng G H 2018 *Phys. Rev. A* **95** 022318

[22] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, p. 175

[23] Guo Y, Su Y, Zhou J, Zhang L and Huang D 2019 *Chin. Phys. B* **28** 010305

[24] Wang C, Huang P, Huang D, Lin D K and Zeng G H 2016 *Phys. Rev. A* **93** 022315

[25] Lu Z X, Yu L, Li K, Liu B C, Lin J G, Jiao R Z and Yang B J 2010 *Sci. China-Phys., Mech. Astron.* **53** 100

[26] Zhang H, Mao Y, Huang D, Guo Y, Wu X and Zhang L 2018 *Chin. Phys. B* **27** 090307

[27] Li D W, Huang P, Zhou Y M, Li Y and Zeng G H 2018 *IEEE Photon. J.* **10.5** 1

[28] Jiang X Q, Huang P, Huang D, Lin D K and Zeng G H 2017 *Phys. Rev. A* **95** 022318

[29] Bacco D, Canale M, Laurenti N, Vallone G and Villoresi P 2013 *Nat. Commun.* **4** 2363

[30] Huang D, Lin D K, Wang C, Wei W Q, Fang S H, Peng J Y, Huang P and Zeng G H 2015 *Opt. Express* **23** 017511

[31] Bai Z L, Wang X Y, Yang S S and Li Y M 2016 *Sci. China-Phys. Mech. Astron.* **59** 614201

[32] Jouguet P, Kunz-Jacques S, Diamanti E and Leverrier A 2012 *Phys. Rev. A* **86** 032309

[33] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343

[34] Kiktenko E O, rushechkin A S, Lim TC C W, Kurochkin Y V and Fedorov A K 2017 *Phys. Rev. Appl.* **8** 044017

[35] Leverrier A and Grangier P 2011 *Phys. Rev. A* **83** 042312

[36] Jouguet P and Kunz-Jacques S 2012 arXiv: 1204.5882

[37] Li Y M, Wang X Y, Bai Z L, Liu W Y, Yang S S and Peng K C 2017 *Chin. Phys. B* **26** 040303

[38] Li J, Lin S, Abdel-Ghaffar K, Ryan W E and Costello D J 2016 *IEEE Inform. Theory Appl. Workshop* 16777097

[39] Phromsa-ard T, Sangwongngam P, Sripimanwat K, Kaemarungsri K, Vanichchanunt P and Wuttisittikulkij L 2014 *IEEE Electron., Comput., Telecommun. Inform. Technol.* 1–5

[40] Zhang J, Bai B, Mu X, Xu H, Liu Z and Li H 2018 *Wirel. Commun. Mob. Com.* **14** 4397671

[41] Diao Q, Huang Q and Lin S 2012 *IEEE Trans. Inf. Theory* **58** 4030

[42] Jouguet P, Elkouss D and Kunz-Jacques S 2014 *Phys. Rev. A* **90** 042329

[43] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238

[44] Fossorier M P C, Mihaljevic M and Imai H 1999 *IEEE Trans. Inf. Theory* **47.5** 673

[45] Gallager R 1962 *IEEE Trans. Inf. Theory* **8.1** 21

[46] Lodewyck J, Bloch M, Garciá-Patroán R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R and McLaughlin S W 2007 *Phys. Rev. A* **76** 042305

[47] Jiang X Q, Yang S Y, Huang P and Zeng G H 2018 *IEEE Photon. J.* **10.4** 1–10

[48] MacKay D J 1999 *IEEE Trans. Inf. Theory* **45** 399

[49] Document 3GPP *R*1 − 1711982 3GPP TSG RAN WG1 Meeting AH NR2, 3GPP, June 2017

[50] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 *Phys. Rev. A* **77** 042325

[51] Huang D, Huang P, Wang T, Li H S, Zhou Y M and Zeng G H 2016 *Phys. Rev. A* **94** 032305

[52] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R and Grangier P 2009 *J. Phys. B* **42** 114014

[53] Huang D, Huang P, Lin D K and Zeng G H 2016 *Sci. Rep.* **6** 19201

[54] Guo Y, Liao Q, Wang Y, Huang D, Huang P and Zeng G H 2017 *Phys. Rev. A* **95** 032304

[55] Jouguet P, Kunz-Jacques S and Leverrier A 2011 *Phys. Rev. A* **84** 062317

[56] Johnson S J, Chandrasetty V A and Lance A M 2016 *IEEE Australian Communications Theory Workshop* pp. 18–23