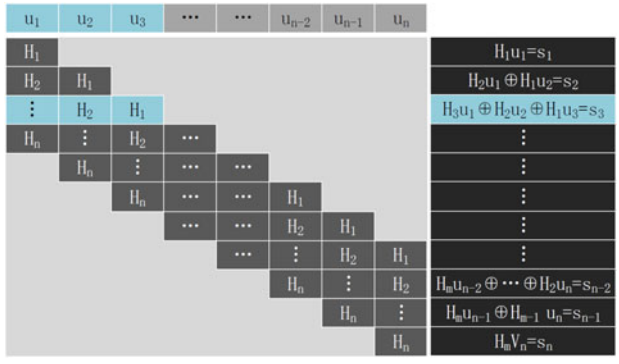
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

High-Speed Reconciliation for CVQKD Based on Spatially Coupled LDPC Codes

Volume 10, Number 04, August 2018

Xue-Qin Jiang, ***Member, IEEE***
Siyuan Yang
Peng Huang
Guihua Zeng



DOI: 10.1109/JPHOT.2018.2853736
1943-0655 © 2018 IEEE

IEEE photonics SOCIETY

IEEE

High-Speed Reconciliation for CVQKD Based on Spatially Coupled LDPC Codes

Xue-Qin Jiang,[1] ***Member, IEEE***, **Siyuan Yang**,[1] **Peng Huang**,[2] **and Guihua Zeng**[2]

[1]School of Information Science and Technology, Donghua University, Shanghai 201620, China
[2]State Key Laboratory of Advanced Optical Communication Systems and Networks, Center of Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China

DOI:10.1109/JPHOT.2018.2853736
1943-0655 © 2018 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Manuscript received April 19, 2018; revised June 6, 2018; accepted July 4, 2018. Date of publication July 11, 2018; date of current version July 24, 2018. This work was supported in part by the National Natural Science Foundation of China under Grants 61671143, 61332019, 61671287, and 61631014; and in part by the National Key Research and Development Program under Grant 2016YFA0302600.
Corresponding author: Xue-Qin Jiang (e-mail: xqjiang@dhu.edu.cn).

Abstract: The speed of continuous variable quantum key distribution is limited by the reconciliation efficiency and the reconciliation frame error rate (FER) in the reconciliation phase. In this paper, we propose an approach that may increase the reconciliation efficiency and decrease the FER. In detail, to increase the reconciliation efficiency, rather than using the block low-density parity-check (LDPC) codes, such as quasi-cyclic LDPC codes, multiedge-type LDPC codes, and punctured LDPC codes, this paper introduces spatially coupled (SC) LDPC codes to the reconciliation phase. To decrease the FER, we propose a new reconciliation scheme based on the special structure of SC-LDPC codes. To demonstrate the performance of the proposed approach, we construct the SC-LDPC codes based on quasi-cyclic repeat-accumulate codes. It is shown that the proposed scheme leads to higher reconciliation speed than that of the previous reconciliation schemes.

Index Terms: Continuous variable quantum key distribution (CVQKD), reconciliation efficiency, low-density parity-check (LDPC) code.

1. Introduction

In the processes of exchanging secret keys between two legitimate users Alice and Bob, it has been proved that quantum key distribution (QKD) is secured and also guaranteed by the laws of quantum physics. In QKD, cryptographic keys are encoded on photons, which is impossible for an eavesdropper, Eve, to attack without being detected [1]–[4]. Though discrete-variable QKD is commonly used [5]–[11], continuous-variable QKD (CVQKD) protocol is a better option allowing the implementation with standard telecom components with better security against eavesdropping [12]–[17]. The secret information is encoded on the quadratures X and P of a continuous variable quantum state in CVQKD. The single-photon detectors employed in discrete-variable QKD are replaced by homodyne or heterodyne detectors. Different types of CVQKD schemes have been proposed [18]–[21]. From the proposed, Gaussian-modulated coherent state (GMCS) QKD [18] has been found theoretically secure from collective [22], [23] and coherent attacks [24], [25].

Quantum transmission and post processing procedures are the two major components of a CVQKD scheme. To generate the raw keys, Alice and Bob first use the quantum transmission to prepare and measure while gaining advantage over Eve. The second stage is the post processing, which consists of two stages: reconciliation and privacy amplification. Reconciliation is a process that helps to correct errors and ensures similarity from the raw keys received over the quantum transmission. The second part of post processing procedure, privacy amplification, enables to achieve information theoretic security. This algorithm will allow to eliminate eavesdropped keys by Eve and produce the secret keys.

Since the reconciliation has a significant effect on the final secret key rate and maximal transmission distance of CVQKD systems, it has attracted much attentions. In CVQKD scheme, the reconciliation is performed using an error correction code design for the binary-input (BI)-AWGN channel and the efficiency of the reconciliation can be measured by $\beta = R/C(\eta)$, where R is the rate of the error correction code and $C(\eta)$ is the capacity at the signal-to-noise (SNR) η. Then, the final secret key rate K of the CVQKD system is given by

$$K = \beta I_{AB} - \chi_{BE} \ (bits/pulse). \tag{1}$$

where I_{AB} is the mutual information between Alice and Bob and χ_{BE} is the Holevo bound on the information leaked to Eve. It is easy to see that, in order to maximize the secret key rate K, β must be maximized. However, as Eq.(1) only provides an expression for the maximum achievable secret key rate and does not consider the speed of reconciliation. Considering the reconciliation frame error rate (FER) P_e, a more realistic expression for the secret key speed is given by [26], [27]

$$K_s = (1 - P_e)(\beta I_{AB} - \chi_{BE}). \tag{2}$$

Generally, a block low-density parity-check (LDPC) code with iterative decoding is always used in the reconciliation for the CVQKD [26], [28]. However, for a given LDPC code, achieving a high reconciliation efficiency requires a low SNR η, which results in a high FER. Hence, the change in reconciliation efficiency and the FER are opposite. Furthermore, due to the sub-optimality of iterative decoding, there is a gap between the (threshold) performance of iterative decoding and maximum a posteriori (MAP) probability decoding. Hence, to achieve the same performance, the LDPC code with iterative decoding requires higher SNR than that with MAP decoding, which leads to a reduced reconciliation efficiency for a given block LDPC code with iterative decoding. Spatially coupled LDPC (SC-LDPC) codes, introduced by Felström and Zigangirov [29], [30], provide a way to close this gap: SC-LDPC codes with iterative decoding have been shown to achieve the MAP threshold, making these codes attractive candidates for applications requiring near-capacity performance [30]–[32].

It is possible to increase the speed of reconciliation for the CVQKD by using SC-LDPC codes and their special structure. Instead of using block LDPC codes, such as repeat accumulate LDPC codes [26], multi-edge type LDPC codes [28], or punctured LDPC codes [33], in reconciliation, this work introduces SC-LDPC codes to increase the reconciliation efficiency for CVQKD scheme. We also propose a new reconciliation protocol based on the special structure of SC-LDPC codes to decrease the FER. The proposed reconciliation scheme has three advantages. First, the reconciliation efficiency based on SC-LDPC codes is higher than that of block LDPC codes. Second, for a given SC-LDPC codes and the corresponding reconciliation efficiency, the proposed reconciliation scheme has lower FER. Finally, the decoding complexity of LDPC iterative decoding in reconciliation can be reduced by using a windowed decoder (WD). These will lead the proposed scheme to a high reconciliation speed with a low reconciliation complexity.

This paper is arranged as follows. In Sec. 2, the SC-LDPC codes and a scheme to construct the SC-LDPC codes are introduced. A high efficiency reconciliation based on SC-LDPC codes is also presented in this section. In Sec. 3, a new reconciliation scheme based on the special structure of SC-LDPC codes is introduced, which leads to lower reconciliation FER. Then the security of the

proposed reconciliation scheme is investigated in Sec. 4. Finally, conclusions are drawn in Sec. 5.

$$\mathbf{H}_{SC} = \begin{bmatrix} \mathbf{H}_0(\mathbf{0}) & & & & & \\ \mathbf{H}_1(1) & \mathbf{H}_0(1) & & & & \\ \vdots & \vdots & \ddots & & & \\ \mathbf{H}_{m_s}(m_s) & \mathbf{H}_{m_s-1}(m_s) & \cdots & \mathbf{H}_0(m_s) & & \\ & \mathbf{H}_{m_s}(m_s+1) & \mathbf{H}_{m_s-1}(m_s+1) & \cdots & \mathbf{H}_0(m_s+1) & \\ & & & \ddots & \ddots & \ddots \end{bmatrix}. \tag{3}$$

2. High Efficiency Reconciliation Based on Spatially Coupled Codes

A SC-LDPC code is basically a LDPC code defined by a structured, infinitely extended parity-check matrix $\mathbf{H}_{SC}$ as shown in Eq.(3). In Eq.(3), $\mathbf{H}_i(t)$, $t \geq 0$, are sparse binary parity-check matrices of size $r \times n$ and m_s is the syndrome former memory of the code. If there is a positive integer T_s such that $\mathbf{H}_i(t) = \mathbf{H}_i(t + T_s)$ for all $i = 0, 1, \ldots, q$ and all $t \in \mathbb{Z}_{\geq 0}$, then $\mathbf{H}_{SC}$ is called time-varying. When $T_s = 1$, $\mathbf{H}_{SC}$ is called time-invariant, and the parity-check matrix can be simply written as

$$\mathbf{H}_{SC} = \begin{bmatrix} \mathbf{H_0} & & & & \\ \mathbf{H}_1 & \mathbf{H}_0 & & & \\ \vdots & \vdots & \ddots & & \\ \mathbf{H}_{m_s} & \mathbf{H}_{m_s-1} & \cdots & \mathbf{H}_0 & \\ & \mathbf{H}_{m_s} & \mathbf{H}_{m_s-1} & \cdots & \mathbf{H}_0 \\ & & & \ddots & \ddots & \ddots \end{bmatrix}. \tag{4}$$

In this paper, we will consider the time-invariant SC-LDPC codes. In practice, in order to construct codes of finite length, the infinitely extended matrix $\mathbf{H}_{SC}$ is terminated resulting in finite length code $N_c = Nn$, where N is a large positive integer [30]–[32], and the rate of the SC-LDPC code is

$$R = \frac{N(n-r) - (m_s - 1)r}{Nn}. \tag{5}$$

One advantage of SC-LDPC codes is that SC-LDPC codes with iterative decoding have been shown to achieve the MAP threshold of a block LDPC code. Another is that the long code words can conveniently be decoded with acceptable latency using a simple WD [34]. The WD works on subgraphs of the code and the window size W is defined as the number of sets of r check nodes of the parity-check matrix $\mathbf{H}_{SC}$ considered within each window. In the parity-check matrix $\mathbf{H}_{SC}$, the window thus consists of Wr rows of $\mathbf{H}_{SC}$ and all columns that are involved in the check equations.

Although iterative decoding of long LDPC codes can be practically implemented, encoding of these codes can be rather complex, since most of these codes, especially computer-generated random codes, do not have sufficient structure to allow simple encoding. One class of structured LDPC codes that allows low complexity encoding is the class of quasi-cyclic (QC)-LDPC codes [35]. It is known in coding theory that QC codes can be encoded with simple shift registers, with linear complexity based on their generators [35]–[37]. Compared to general LDPC codes, the design of a decoder for QC-LDPC codes can also be significantly simplified due to simplified routing of messages from memory to computation units. Therefore, QC-LDPC codes are favorable for hardware implementation. In this section, we present a scheme to construct the time-invariant parity-check matrix Eq.(4), which also has the quasi-cyclic structure.

Starting from the parity-check matrix $\mathbf{H}_{QC}$ of a block QC-LDPC code,

$$\mathbf{H}_{QC} = \begin{bmatrix} \mathbf{H}_{(0,0)} & \mathbf{H}_{(0,1)} & \cdots & \mathbf{H}_{(0,l-1)} \\ \mathbf{H}_{(1,0)} & \mathbf{H}_{(1,1)} & \cdots & \mathbf{H}_{(1,l-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{(r-1,0)} & \mathbf{H}_{(r-1,1)} & \cdots & \mathbf{H}_{(r-1,l-1)} \end{bmatrix}, \tag{6}$$

which consists of $r \times l$ cyclic permutation matrix or zero matrix of size $q \times q$, we aim at obtaining an unwrapped version of it, to form the parity-check matrix $\mathbf{H}_{SC}$ of a time-invariant SC-LDPC code. Following [38], we rearrange the rows and the columns of $\mathbf{H}_{QC}$ as follows: permute the rows according to the ordering 0, q, $2q$, ..., $(r-1)q$, 1, $q+1$, $2q+1$, ..., $(r-1)q+1$, 2, $q+2$, $2q+2$, ..., $rq-1$, and then permute the columns according to the ordering 0, q, $2q$, ..., $(l-1)q$, 1, $q+1$, $2q+1$, ..., $(l-1)q+1$, 2, $q+2$, $2q+2$, ..., $lq-1$. This way, we swap the inner and outer structures of the original matrix, which is a block of circulants, and obtain the parity-check matrix of an equivalent code in the form of a circulant of blocks, that is

$$\mathbf{H}_{BC} = \begin{bmatrix} \mathbf{H}_0 & \mathbf{H}_{q-1} & \cdots & \mathbf{H}_1 \\ \mathbf{H}_1 & \mathbf{H}_0 & \cdots & \mathbf{H}_2 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{q-1} & \mathbf{H}_{q-2} & \cdots & \mathbf{H}_0 \end{bmatrix} \tag{7}$$

where each block $\mathbf{H}_i$ is of size $r \times l$. As only row and column permutations are performed, $\mathbf{H}_{BC}$ in Eq.(7) still has quasi-cyclic structure and therefore the low encoding and decoding complexities.

Starting from $\mathbf{H}_{BC}$ in Eq.(7), we repeatedly move n positions to the right and then m positions down, we obtain the time-invariant parity-check matrix Eq.(4) with $q = m_s + 1$. Note that the constructing of quasi-cyclic parity-check matrix Eq.(6) and the selecting of q can be done by applying the methods in [36]

2.1 Reconciliation Scheme Based on Spatially Coupled LDPC Codes

In the quantum transmission phase, let $\mathbf{x}$ and $\mathbf{y}$ of length n be the classical random variables associated with the measured quantities of the legitimate parties Alice and Bob, and let $\mathbf{e}$ be the quantum state in possession of the eavesdropper. Once the quantum transmission phase has ended, Alice and Bob proceed with the reconciliation phase. The reconciliation is *direct* when Alice's data are used as a reference for establishing the key and *reverse* when the reference is Bob's data. Without lost of the generality, we consider the reverse reconciliation. However, the application of our scheme to the direct reconciliation is also immediate.

To demonstrate the benefit of using SC-LDPC codes, we consider the reverse reconciliation scheme of CVQKD which can be simply described as follows:

- A1 Bob chooses randomly an vector $\mathbf{u}$ of length n and generate $\alpha(\mathbf{y}, \mathbf{u})$ with $\mathbf{y}$ and $\mathbf{u}$.
- A2 Bob sends $\alpha(\mathbf{y}, \mathbf{u})$ to Alice on a public classical channel. Given a linear code $\mathbf{C}$ and its parity check matrix $\mathbf{H}$, Bob tells Alice the syndrome of $\mathbf{u}$, which is $\mathbf{H} \cdot \mathbf{u}^T = \mathbf{s}$, on the public channel, where $(\cdot)^T$ denotes the transpose operation.
- A3 Alice and Eve hence have the pairs $[\mathbf{x}, \alpha(\mathbf{y}, \mathbf{u})]$ and $[\mathbf{e}, \alpha(\mathbf{y}, \mathbf{u})]$, respectively, and the syndrome $\mathbf{s}$ of $\mathbf{u}$.
- A4 Alice recovers $\hat{\mathbf{u}}$ from $\mathbf{x}$, $\alpha(\mathbf{y}, \mathbf{u})$ and $\mathbf{s}$. If $\hat{\mathbf{u}} \cdot \mathbf{H} = \mathbf{s}$, Alice and Bob have extracted a common pair string $\hat{\mathbf{u}} = \mathbf{u}$, which is a raw key. Otherwise, the decoding fails, Alice and Bob discard their raw keys $\mathbf{u}$ and $\hat{\mathbf{u}}$, respectively.

The primary metric that defines the performance of a CVQKD system is the maximum rate at which Alice and Bob can securely generate and reconcile keys over a fixed-distance optical fiber in the presence of an eavesdropper that has access to both the quantum and classical channels.

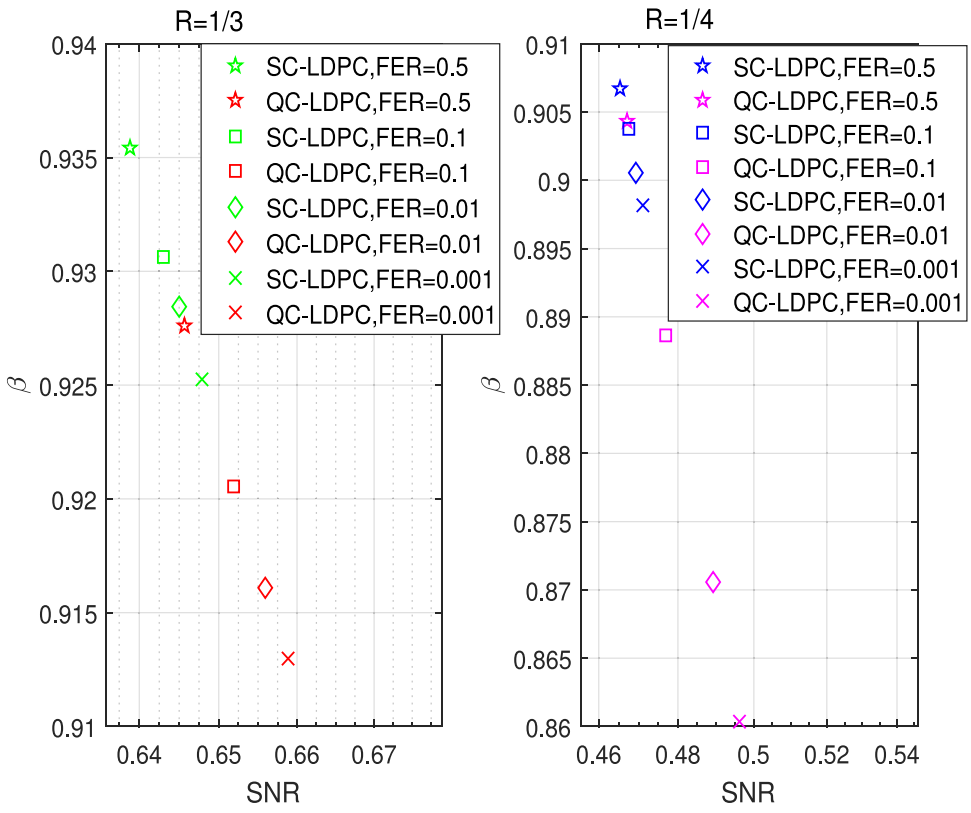


Fig. 1. Reconciliation efficiency of the SC-LDPC codes and QC-LDPC codes for FERs of 0.5, 0.1, 0.01 and 0.001.

The maximum secret key rate must be proven secure against a collective Gaussian attack and the man-in-the-middle attack.

In the following, we provide an example comparing the reconciliation efficiency and secret key rate of CVQKD based on block LDPC codes and SC-LDPC codes, respectively.

Example 1: Letting $N = 10$, we first construct the SC-LDPC codes of length 628000 based on the rate-1/3 and 1/4 QC-LDPC codes of length 62800, which are given in [39]. Then, we provide the β values corresponding to our constructed SC-LDPC codes and the QC-LDPC codes [39], respectively. The maximum allowed number of iterations is set to be 500. Fig. 1 shows the reconciliation efficiency of the SC-LDPC codes for FERs of 0.5, 0.1, 0.01 and 0.001, respectively. Also shown is the reconciliation efficiency of QC-LDPC codes. We can see from Fig. 1 that the reconciliation efficiency of the SC-LDPC codes is much higher than that of the QC-LDPC codes with the same rate. Furthermore, when the FER decrease exponentially from 0.5 to 0.001, the efficiency gaps increase approximately from 0.009 to 0.013, which indicates that the decrease of FER is faster than increase of the efficiency. However, the increase of efficiency leads to a longer transmission distance and higher secret key rate of the CVQKD scheme and the decrease of FER only leads to higher final key speed at a particular transmission distance.

Generally speaking, SC-LDPC codes provides higher reconciliation efficiency than the block LDPC codes, such as QC-LDPC codes, multi-edge typle LDPC codes, and punctured LDPC codes. Since higher reconciliation efficiency leads to the higher final secret key rate and therefore less leaked information to an eavesdropper, SC-LDPC codes will lead to higher compression ratios in the privacy amplification stage. However, as indicated by (2), the speed of reconciliation also depend on the FER of the reconciliation. Therefore, in the next section we will introduce a new reconciliation scheme to further reduce the FER of the reconciliation based on the special structure of the SC-LDPC codes.

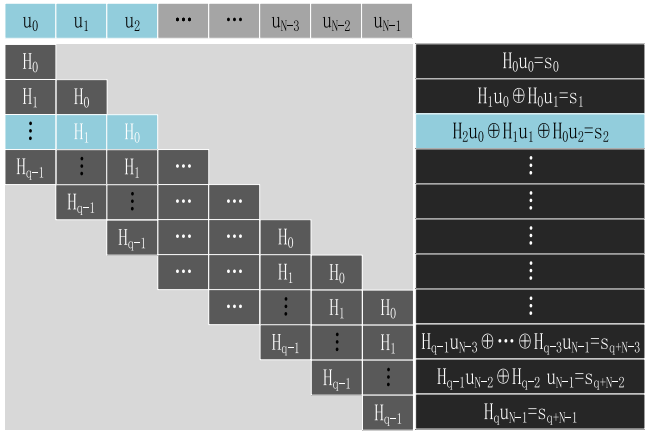


Fig. 2. Discarding erroneous sub-frames based on the special structure of the SC-LDPC codes.

3. Low FER Reconciliation Based on Spatially Coupled Codes

Note that in step **A4** If the decoding success, Alice has $\mathbf{H}_{SC} \cdot \hat{\mathbf{u}}^T = \mathbf{s}$. Then, Alice and Bob have the common reconciliation frame. If the decoding fails, Alice has $\mathbf{H}_{SC} \cdot \hat{\mathbf{u}}^T \neq \mathbf{s}$. Then, Alice and Bob discard their reconciliation frame. Based on the special structure of parity-check matrix Eq.(4), the frame $\mathbf{u}$ can be divided into sub-frames $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_{N-1}$ of length n. The corresponding syndrome $\mathbf{s}$ can also be divided into sub-syndromes $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{m_s+N-2}$ of length m. As shown in Fig. 2, $\mathbf{H}_{SC} \cdot \mathbf{u}^T = \mathbf{s}$ may lead to the constraints in Eq.(8)

$$\begin{cases} \mathbf{H_0 u_0^T} = \mathbf{s_0} \\ \mathbf{H}_1\mathbf{u}_0^T \oplus \mathbf{H}_0\mathbf{u}_1^T = \mathbf{s}_1 \\ \quad \vdots \\ \mathbf{H}_{q-1}\mathbf{u}_0^T \oplus \mathbf{H}_{q-2}\mathbf{u}_1^T \oplus \cdots \oplus \mathbf{H}_0\mathbf{u}_{q-1}^T = \mathbf{s}_{q-1} \\ \mathbf{H}_{q-1}\mathbf{u}_1^T \oplus \mathbf{H}_{q-2}\mathbf{u}_2^T \oplus \cdots \oplus \mathbf{H}_0\mathbf{u}_q^T = \mathbf{s}_q \\ \quad \vdots \\ \mathbf{H}_{q-1}\mathbf{u}_{N-1}^T = \mathbf{s}_{q+N-1} \end{cases} \tag{8}$$

where $\mathbf{0}$ is a zero vector of length m.

At the Alice side of the reverse reconciliation, comparing to the decoded frame $[\hat{\mathbf{u}}_i, \hat{\mathbf{u}}_{1+i}, \cdots, \hat{\mathbf{u}}_{m_s+i}]$ involved the ith constraint, the frame $[\hat{\mathbf{u}}_{1+i}, \cdots, \hat{\mathbf{u}}_{m_s+i+1}]$ involved the $(i+1)$th constraint include the new sub-frame $\hat{\mathbf{u}}_{q+i+1}$, which corresponds to the sequences $\mathbf{x}_i$ and $\mathbf{y}_i$. Based on the constraints Eq.(8), we proposed the following new reconciliation scheme in which Alice and Bob discard only sub-frames of $\mathbf{u}$ and $\hat{\mathbf{u}}$, respectively, even when $\mathbf{H}_{SC} \cdot \hat{\mathbf{u}}^T \neq \mathbf{s}$.

- B1 Bob chooses randomly an vector $\mathbf{u}$ of length Nn, divides it into N sub-frames $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_{N-1}$ of length n and generates $\alpha(\mathbf{y}, \mathbf{u})$ with $\mathbf{y}$ and $\mathbf{u}$.
- B2 Bob sends $\alpha(\mathbf{y}, \mathbf{u})$ to Alice on a public classical channel. Bob calculates the syndrome $\mathbf{s}$ of $\mathbf{u}$, divides $\mathbf{s}$ into sub-syndromes $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{m_s+N-2}$ of length m and tells Alice over the public channel.
- B3 Alice and Eve hence have the pairs $[\mathbf{x}, \alpha(\mathbf{y}, \mathbf{u})]$ and $[\mathbf{e}, \alpha(\mathbf{y}, \mathbf{u})]$, respectively, and the syndrome $\mathbf{s}$ of $\mathbf{u}$. Alice recovers $\hat{\mathbf{u}}$ from $\mathbf{x}$, $\alpha(\mathbf{y}, \mathbf{u})$ and $\mathbf{s}$.
- B4 For $i = 1, 2, ..., q + N - 1$, if ith constraint in Eq.(8) is satisfied, Alice and Bob have extracted a new common sub-frame $\hat{\mathbf{u}}_{q+i+1} = \mathbf{u}_{q+i+1}$ as the raw keys. Otherwise, Alice and Bob discard $\hat{\mathbf{u}}_{q+i+1}$ and $\mathbf{u}_{q+i+1}$, respectively.

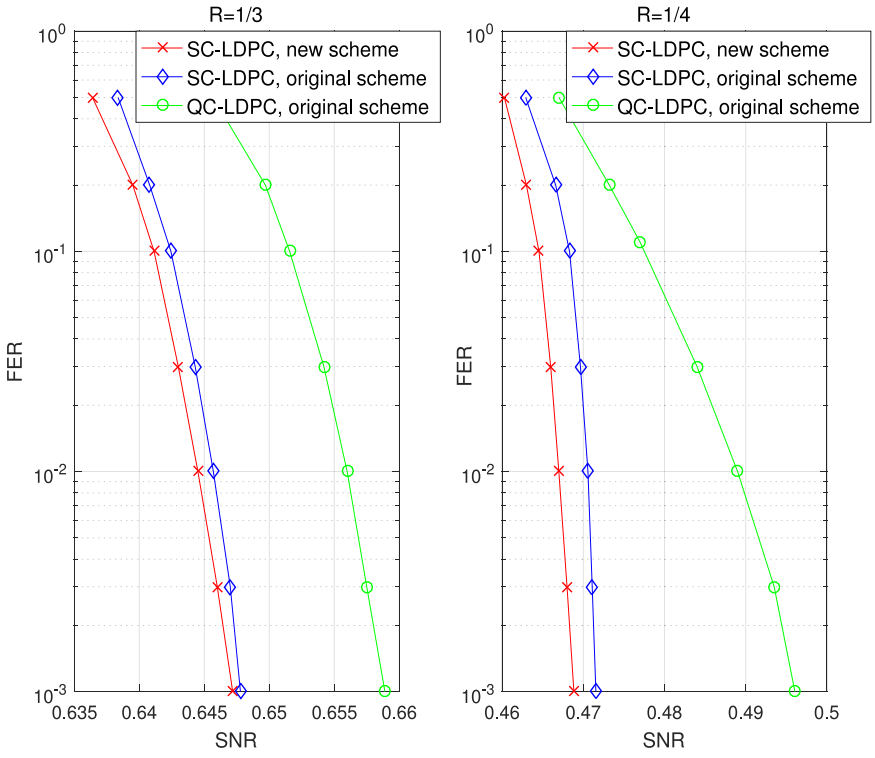


Fig. 3. FER values corresponding to SC-LDPC codes with the proposed reconciliation scheme and the original reconciliation scheme.

From **B4**, it is clear that even through $\mathbf{H}_{SC} \cdot \hat{\mathbf{u}}^T \neq \mathbf{s}$ and the decoding fails, Alice and Bob will not discard the whole frames $\mathbf{u}$ and $\hat{\mathbf{u}}$. Usually, they may extracted common pairs of sub-frames from $\mathbf{u}$ and $\hat{\mathbf{u}}$, respectively. Define F_{sub}^{j} as the number of erroneous discarded sub-frames in the j-th received frame, $1 \leq j \leq F_{total}$. Then, we redefine the FER as $\bar{P}_e$ calculated by

$$\bar{P}_e = \frac{\bar{F}_{dis}}{F_{total}}, \tag{9}$$

where

$$\bar{F}_{dis} = \frac{\sum_{i=1}^{F_{total}} F_{sub}^{i}}{N \times F_{total}}. \tag{10}$$

As $\bar{F}_{dis} \leq 1$, it is easy to see that $\bar{P}_e \leq P_e$, where the equality holds when all the sub-frames of an erroneous reconciliation frame are in error. Therefore, our proposed reconciliation scheme has lower FER than that of the previous reconciliation scheme **A1**–**A4** in [28].

Example 2: In this example, we consider the same SC-LDPC codes and QC-LDPC codes used in *Example 1*. We provide the FER values $\bar{P}_e$ corresponding to SC-LDPC codes with the proposed reconciliation scheme and SC-LDPC codes with previous reconciliation scheme, respectively. Also shown is the FER values P_e corresponding to QC-LDPC codes with the previous reconciliation scheme. The maximum allowed number of iterations is set to be 500. From Fig. 3, it is easy to see that our proposed reconciliation scheme has lower FER than that of the previous reconciliation scheme.

We also provide the reconciliation efficiency β, FER values P_e and $\bar{P}_e$ corresponding to *Example 1* and *Example 2* in Table 1, which verify that SC-LDPC codes provides higher β than the block LDPC codes and the new reconciliation scheme further reduce the FER of the reconciliation. Therefore, the proposed scheme lead to higher reconciliation speed than that of the previous reconciliation schemes.

TABLE I
Secret Key Speed (bps) of the Proposed and the Previous Reconciliation Schemes on a 25 km Optical Link

	R	η	β	P_e	$\bar{P}_e$	K_s
QC-LDPC, previous scheme	1/3	0.646	0.927	0.5		3.00×10^5
SC-LDPC, previous scheme	1/3	0.638	0.936	0.5		3.25×10^5
SC-LDPC, new scheme	1/3	0.638	0.936		0.25	4.88×10^5
QC-LDPC, previous scheme	1/3	0.651	0.921	0.1		5.07×10^5
SC-LDPC, previous scheme	1/3	0.642	0.931	0.1		5.57×10^5
SC-LDPC, new scheme	1/3	0.642	0.931		0.036	6.00×10^5
QC-LDPC, previous scheme	1/4	0.467	0.903	0.5		2.31×10^5
SC-LDPC, previous scheme	1/4	0.463	0.911	0.5		2.48×10^5
SC-LDPC, new scheme	1/4	0.463	0.911		0.23	3.82×10^5
QC-LDPC, previous scheme	1/4	0.476	0.890	0.1		3.65×10^5
SC-LDPC, previous scheme	1/4	0.468	0.903	0.1		4.16×10^5
SC-LDPC, new scheme	1/4	0.468	0.903		0.0032	4.60×10^5

4. Security Analysis

Since Eve may have collected information during her observations of the quantum transmission phase, Alice and Bob eliminate Eve's knowledge of the key by applying the privacy amplification to their raw keys, **u** and **û**, respectively, to extract the secret keys.

The objective of reconciliation is to extract a common sequence of raw keys of length N_c from observations of **x** and **y** so that privacy amplification can be used later on to extract the secret keys of K bits that is provably unknown to the eavesdropper Eve. From Eq.(1), we can see that the final secret key length K depends on I_{AB}, χ_{BE} and β. However, I_{AB}, χ_{BE} depend on the quantum transmission phase. The only thing related to K in the reconciliation phase is the reconciliation efficiency β. Therefore, we now proof that the reconciliation efficiency β of the proposed reconciliation scheme is the same as that of the original reconciliation scheme [28] for the given error-correcting code of rate R and the SNR η. As shown in [40], the reconciliation can be treated as a Slepian-Wolf coding problem, and the reconciliation efficiency is

$$\begin{aligned}\beta &\triangleq \frac{H(\mathbf{u}) - |\mathbf{s}|}{I(\mathbf{u};\hat{\mathbf{u}})} \\ &= \frac{\frac{1}{N_c}(H(\mathbf{u}) - |\mathbf{s}|)}{\frac{1}{N_c} I(\mathbf{u};\hat{\mathbf{u}})} \\ &= \frac{R}{C(\eta)} \\ &= \frac{N(n-r) - (q-1)r}{NnC(\eta)}.\end{aligned} \tag{11}$$

Here, the quantity $|\mathbf{s}|$ represents the number of bits in syndrome exchanged over the public channel.

Referring to Eq.(11), we define the reconciliation efficiency β_i corresponding to sub-frame $\mathbf{u}_i$ and sub-syndrome $\mathbf{s}_i$ as

$$\beta_i \triangleq \frac{H(\mathbf{u}_i) - |\mathbf{s}_i|}{I(\mathbf{u}_i; \hat{\mathbf{u}}_i)} = \frac{\frac{1}{n}(H(\mathbf{u}_i) - |\mathbf{s}_i|)}{\frac{1}{n} I(\mathbf{u}_i; \hat{\mathbf{u}}_i)} = \frac{R_i}{C(\eta)} = \frac{n-r}{nC(\eta)}. \tag{12}$$

Note that when $N \to \infty$, we have $\beta_i = \beta$. Therefore, the proposed reconciliation protocol does not change the reconciliation efficiency β and therefore the secret key rate K.

5. Conclusion

In conclusion, we introduced SC-LDPC codes to the reconciliation phase of the CVQKD. It was shown that the reconciliation efficiency of the SC-LDPC codes was much higher than that of the QC-LDPC codes of the same rate. Furthermore, we presented a new reconciliation scheme for the CVQKD, which reduced the FER of the reconciliation based on the special structure of the SC-LDPC codes. The proposed two ways increased the reconciliation efficiency and decrease the FER, respectively. Consequently, these two ways lead to higher reconciliation speed than that of the previous reconciliation scheme.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bangalore, India, 1984, pp. 175–179.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *"Quantum cryptography," Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.
[3] C. Weedbrook *et al.*, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, 2012.
[4] G. Zeng, *Quantum Private Communication*. Berlin, Germany: Springer-Verlag, 2010, ch. 3.
[5] S. Wang *et al.*, "Practical gigahertz quantum key distribution robust against channel disturbance," *Opt. Lett.*, vol. 43, pp. 2030–2033, 2018.
[6] S. Wang *et al.*, "Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme," *Quantum Sci. Technol.*, vol. 3, 2018, Art. no. 025006.
[7] Z.-Q. Yin *et al.*, "Improved security bound for the round-robin-differential-phase-shift quantum key distribution," *Nature Commun.*, vol. 9, 2018, Art. no. 457.
[8] C. Wang *et al.*, "Measurement-device-independent quantum key distribution robust against environmental disturbances," *Optica*, vol. 4, pp. 1016–1023, 2017.
[9] S. Wang *et al.*, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," *Nature Photon.*, vol. 9, pp. 832–836, 2015.
[10] S. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Exp.*, vol. 22, pp. 21739–21756, 2014.
[11] S. Wang *et al.*, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Opt. Lett.*, vol. 37, pp. 1008–1010, 2012.
[12] J. Lodewyck *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, 2007, Art. no. 042305.
[13] B. Qi, L. L. Huang, L. Qian, and H. K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A*, vol. 76, 2007, Art. no. 052323.
[14] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," *New J. Phys.*, vol. 11, 2009, Art. no. 045023.
[15] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photon.*, vol. 7, pp. 378–381, 2013.
[16] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.*, vol. 6, 2016, Art. no. 19201.
[17] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, "25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel," *Sci. Rep.*, vol. 5, 2015, Art. no. 14607.
[18] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, 2002, Art. no. 057902.
[19] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, 2003.
[20] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, 2004, Art. no. 170504.
[21] C. Weedbrook, "Continuous-variable quantum key distribution with entanglement in the middle," *Phys. Rev. A*, vol. 87, 2013, Art. no. 022308.
[22] R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," *Phys. Rev. Lett.*, vol. 97, 2006, Art. no. 190503.

[23] M. Navascué, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," *Phys. Rev. Lett.*, vol. 97, 2006, Art. no. 190502.
[24] R. Renner and J. I. Cirac, "De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, 2009, Art. no. 110504.
[25] F. Furrer *et al.*, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.*, vol. 109, 2012, Art. no. 100502.
[26] M. Milicevic, C. Feng, L. Zhang, and P. Gulak, "Key reconciliation with low-density parity-check codes for long-distance quantum cryptography," arXiv:1702.07740v2, 2017.
[27] S. Johnson, V. Chandrasetty, and A. Lance, "Repeat-accumulate codes for reconciliation in continuous variable quantum key distribution," in *Proc. Aust. Commun. Theory Workshop*, 2016, pp. 18–23.
[28] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A*, vol. 84, 2011, Art. no. 062317.
[29] A. J. Felstrom and K. S. Zigangirov, "Time-varying periodic convolutional codes with low-density parity-check matrix," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 2181–2191, Sep. 1999.
[30] S. Kudekar, T. Richardson, and R. Urbanke, "Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 803–834, Feb. 2011.
[31] S. Kudekar, C. Measson, T. Richardson, and R. Urbanke, "Threshold saturation on BMS channels via spatial coupling," ArXive-prints, Apr. 2010.
[32] M. Lentmaier, D. G. M. Mitchell, G. Fettweis, and D. J. Costello, Jr., "Asymptotically good LDPC convolutional codes with AWGN channel thresholds close to the Shannon limit," in *Proc. ISTC10*, Brest, France, 2010.
[33] X. Jiang, P. Huang, D. Huang, D. Lin, and G. Zeng, "Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 95, 2017, Art. no. 022318.
[34] M. Lentmaier, M. M. Prenda, and G. P. Fettweis, "Efficient message passing scheduling for terminated LDPC convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, Aug. 2011, pp. 1826–1830.
[35] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2004.
[36] X.-Q. Jiang, H. Hai, H.-M. Wang, and M. H. Lee, "Constructing large girth QC protograph LDPC codes based on PSD-PEG algorithm," *IEEE Access*, vol. 5, pp. 13489–13500, 2017.
[37] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2894–2901, Aug. 2005.
[38] M. Baldi, G. Cancellieri, and F. Chiaraluce, "Array convolutional low-density parity-check codes," *IEEE Commun.*, vol. 18, no. 2, pp. 336–339, Feb. 2014.
[39] "Digital video broadcasting (DVB)," ETSI, Sophia Antipolis, France, Tech. Rep. EN 302 307, Aug. 2009. [Online]. Available: http://www.dvb.org/
[40] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.