SCIENCE CHINA
Physics, Mechanics & Astronomy

• Article •

January 2016 Vol. 59 No. 1: 614201
doi: 10.1007/s11433-015-5702-7

High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution

ZengLiang Bai, XuYang Wang, ShenShen Yang, and YongMin Li*

State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China

Received March 31, 2015; accepted May 20, 2015

Efficient reconciliation is a crucial step in continuous variable quantum key distribution. The progressive-edge-growth (PEG) algorithm is an efficient method to construct relatively short block length low-density parity-check (LDPC) codes. The qua-si-cyclic construction method can extend short block length codes and further eliminate the shortest cycle. In this paper, by combining the PEG algorithm and quasi-cyclic construction method, we design long block length irregular LDPC codes with high error-correcting capacity. Based on these LDPC codes, we achieve high-efficiency Gaussian key reconciliation with slice recon-ciliation based on multilevel coding/multistage decoding with an efficiency of 93.7%.

Gaussian key reconciliation, irregular LDPC codes, progressive-edge-growth, quasi-cyclic construction method

PACS number(s): 03.67.Dd, 03.67.Hk, 84.40.Ua

Citation: Z. L. Bai, X. Y. Wang, S. S. Yang, and Y. M. Li, High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution, Sci. China-Phys. Mech. Astron. **59**, 614201 (2016), doi: 10.1007/s11433-015-5702-7

1 Introduction

Quantum key distribution (QKD) [1-3] enables two remote and legal parties (referred to as Alice and Bob) who are linked by a quantum channel and a classical authenticated public channel to share a secure key, which is unknown completely to the potential eavesdropper (Eve). The unconditional security provided by the QKD root in the basic principles of the quantum physics includes the uncertainty principle and the quantum no-cloning principle. In QKD, discrepancies inevitably occur between the correlated raw keys shared by Alice and Bob because of the added noises of the quantum state preparation, detection, and the potential eavesdropping behaviors. The transmission losses induced by the quantum channel, which simply decrease the photon counting rate in discrete variable (DV) QKD schemes, can introduce vacuum noise and decrease the signal-to-noise ratio (SNR) in homodyne-detection-based continuous variable (CV) QKD protocols [4,5]. To distill a common binary string out of a set of partially correlated random variables, an error correction mechanism (information reconciliation) [6] is exploited, which is performed over a public channel by exchanging reconciliation messages. Finally, the leaked key information gained by Eve is wiped out using privacy amplification [7,8], and a secure shorter key is extracted.

In comparison with DV QKD, CV QKD operates in the regime of low SNRs due to the vacuum noise that is induced by the transmission losses of the quantum channel. The corresponding reconciliation is more demanding, and its efficiency plays a key role in the achievable secret key rate and the limiting transmission distance. Slice reconciliation [9] is a useful method to extract mutual information from correlated continuous variables. Based on the coded modulation techniques (multilevel coding/multistage decoding, MLC/MSD) [10,11] with LDPC codes, higher effi-

*Corresponding author (email: yongmin@sxu.edu.cn)

ciency than that of slice error correction can be achieved. LDPC codes belong to the class of linear error correcting codes and perform at rates extremely close to the Shannon capacity. Decoding for LDPC codes can be fully parallelizable and can potentially be accomplished at significantly greater speeds. An LDPC code is described by a sparse parity check matrix, and its design is crucial to the error-correcting performance.

Progressive-edge-growth (PEG) algorithm [12-14] is a powerful algorithm to generate good sparse parity-check matrixes of LDPC codes at short block length. To extend the short block length codes to longer ones, a quasi-cyclic construction method can be utilized [15,16]. In this paper, with the aid of the above two methods, we efficiently construct good irregular LDPC codes with long block length (200000) and apply them to MLC/MSD slice reconciliation. By optimizing over the number of slices, the quantization step, and the rates for each slice, high-efficiency Gaussian key reconciliation is achieved with an efficiency of 93.7% for an SNR of 4.77 dB.

In sect. 2, we detail the reverse reconciliation for CV QKD and discuss the quantization efficiency of the Gaussian-distributed variable and error correction scheme with MLC/MSD slice reconciliation. In sect. 3, we describe the PEG algorithm. In sect. 4, we elaborate the quasi-cyclic construction method and compare the error-correcting performance of the LDPC codes that are constructed by different methods. In sect. 5, we present the Gaussian key reconciliation results.

2 Reverse reconciliation for CVQKD based on MLC/MSD slice reconciliation

In CV QKD, two types of reconciliation are investigated [17]: direct reconciliation and reverse reconciliation, in the light of the classical information flow (correction information) has the same direction as the initial quantum information flow or not. In the direct reconciliation scenario, Bob corrects its errors with respect to Alice; in the reverse reconciliation scenario, Alice corrects its errors with respect to Bob. The secret key produced is expressed as $\beta I_{AB}-I_{AE}$ with direct reconciliation and $\beta I_{AB}-I_{BE}$ with reverse reconciliation, where I_{AB} is the amount of information Alice and Bob share, I_{AE} and I_{BE} are the information the eavesdropper Eve can have about their results, and β is the reconciliation efficiency. It is known that the reverse reconciliation protocol can overcome the 3 dB loss limit of the quantum channel and may distill the secret key for very low value of the line transmission.

The reverse reconciliation for Gaussian-modulated coherent-state CV QKD can be divided into the following steps. The first step is the quantization of continuous Gaussian-distributed variables. Bob first divides the set of real variables $(-\infty, \infty)$ into intervals of 2^m and takes the Gaussian-distributed variable to the index (m bits) of the interval. This process is known as $Q(Y)$. For the given number of discretization intervals, we try to maximize the amount of information Alice and Bob share $I(X;Q(Y))$. In other words, the quantization losses $I(X;Y)-I(X;Q(Y))$ should be minimized. We consider here two different quantization algorithms for Gaussian-distributed variables: equal interval quantization and Lloyd-Max quantization [18]. The first interval starts from $-\infty$, and the last interval tends to $+\infty$. The quantization efficiency of a Gaussian-distributed variable is given by

$$\beta_{\text{slice}}=\frac{I\left(X;Q(Y)\right)}{I\left(X;Y\right)}. \tag{1}$$

For m=3 to m=5, we show in Figure 1 the optimal quantization efficiencies versus the SNRs for the above two types of quantization algorithms. The efficiencies have similar trends, and the efficiency improvement using Lloyd-Max quantization is not significant. Very high quantization efficiency can be obtained using 5-bit slice (32 intervals) equal interval quantization at SNRs ranging from 1 to 20. Therefore, in the following, we utilize the equal interval quantization and 5-bit slice scheme (m=5) to discretize Gaussian-distributed variables.

The second step of the reverse reconciliation is channel coding with side information [19] based on MLC/MSD. The principle of the MLC/MSD reconciliation scheme is shown in Figure 2. Once Bob's Gaussian-distributed variables have been transformed into a binary sequence, Bob converts them into m levels; then, each level is encoded and a set of parity bits (so called syndromes) are calculated and sent to Alice via the public channel. Usually, the levels corresponding to less information are completely disclosed and not encoded. Alice decodes each level jointly and retrieves

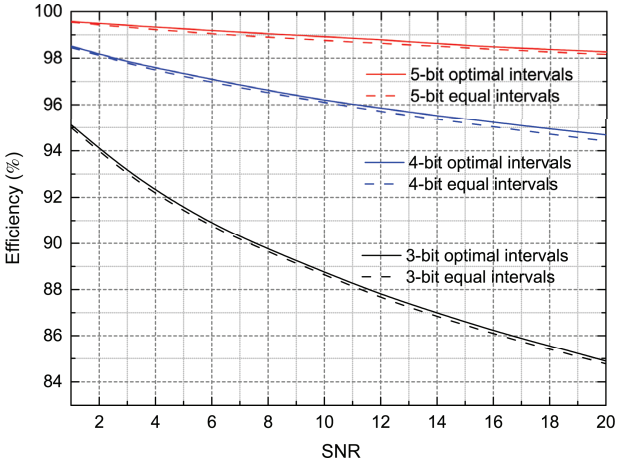

Figure 1 (Color online) Optimal quantization efficiency versus the SNRs for Lloyd-Max quantization (solid lines) and equal interval quantization (dashed lines).

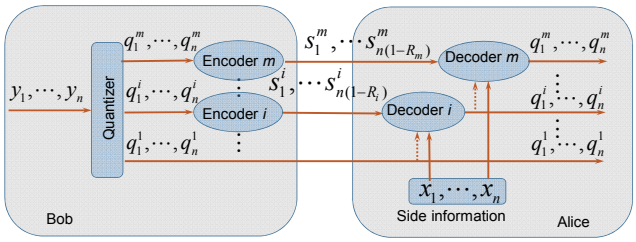

Figure 2 MLC/MSD with side information for reverse reconciliation.

Bob's bit sequence using her Gaussian-distributed variables (known as side information) and the syndromes sent by Bob. As illustrated in Figure 2, the least significant level is decoded first because it has less information, and the result is then passed to the following levels for further decoding. Finally, Alice can correct all errors with LDPC codes and obtain a bit sequence that is identical to Bob's bit sequence.

3 Progressive-edge-growth algorithm

An LDPC code is a linear block code defined by a sparse parity-check matrix H with dimensions $m \times n$. Usually, the matrix H is described as a Tanner graph consisting of a symbol and check nodes. Irregular LDPC codes with good degree distributions and long block length have better performance than regular LDPC codes. Good degree distributions with thresholds close to capacity can be designed using density evolution analysis. The PEG algorithm is a powerful algorithm to construct excellent parity-check matrixes having a large girth by placing edges or connections between symbol and check nodes in an edge-by-edge manner.

A PEG algorithm generally consists of two basic procedures: a local graph expansion and a check node selection procedure. In the process of construction of a Tanner graph, both procedures are executed sequentially to add new connecting edges between the symbol and check nodes by means of edge-by-edge. In the first procedure, the local tree graph is expanded from a symbol node, and the small girths l are searched and avoided as far as possible when adding a new edge. In the selection procedure, the candidate check nodes are reduced to balance the degrees of check nodes according to the current graph setting. In this way, the shortest cycle connecting these new edges under the current graph is guaranteed to be no shorter than $2(l+2)$. Irregular LDPC codes constructed by this method exhibit good iterative-decoding performance [14].

To generate a Tanner graph with m check nodes and n symbol nodes, we use the same notations and definitions as in refs. [12-14] to describe the PEG algorithm.

Generic Progressive Edge-Growth Algorithm [12-14]

for j=0 to $n-1$

{for k=0 to $d_{s_j}-1$

{if k=0

{ $E_{s_j}^0 \leftarrow$ edge (c_i, s_j), where $E_{s_j}^0$ is the first edge incident to s_j and c_i is a check node such that it has the lowest check-node degree under the current graph setting $E_{s_0} \cup E_{s_1} \cup \ldots \cup E_{s_{j-1}}$.

}

else

{expand a subgraph form symbol node s_j up to depth l under the current graph setting such that the cardinality of $N_{s_j}^l$ stops increasing but is less than m, or $\overline{N}_{s_j}^l \neq \varnothing$ but $\overline{N}_{s_j}^{l+1} \neq \varnothing$, then $E_{s_j}^k \leftarrow$ edge (c_i, s_j), where $E_{s_j}^k$ is the kth edge incident to s_j and c_i is a check node picked from the set $\overline{N}_{s_j}^l$ having the lowest check-node degree.

}

}

}

4 Long block length irregular LDPC codes by quasi-cyclic construction method

For CV QKD, good irregular LDPC codes with relatively long block length are required for the reconciliation. This is because the LDPC codes can only operate close to their ideal limit (Shannon limit) in the regime of large block length, usually over 100000 bits. Although the PEG algorithm is efficient for the construction of good short block length codes, it is difficult to generate long block length codes directly. In this section, we show that one can construct good irregular LDPC codes with block length of several hundred using the PEG algorithm and successively extend the codes to a relatively long block length (200000) with the quasi-cyclic construction method [20].

The sparse matrix of quasi-cyclic low-density parity-check (QC-LDPC) code consists of some small square circulant matrices with the same dimensions. The shift-times i represents that each column of a square matrix is moved i columns to the right. The identity matrix represents a circulant permutation matrix of shift 0. An $L \times L$ circulant matrix of shift-times 1 can be represented as follows:

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}. \quad (2)$$

The parity-check matrix H of the QC-LDPC code can be

put in the form below:

$$H=\begin{bmatrix} A^{P_{00}} & A^{P_{01}} & \cdots & A^{P_{0(t-2)}} & A^{P_{0(t-1)}} \\ A^{P_{10}} & A^{P_{11}} & \cdots & A^{P_{1(t-2)}} & A^{P_{1(t-1)}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ A^{P_{(c-2)0}} & A^{P_{(c-2)1}} & \cdots & A^{P_{(c-2)(t-2)}} & A^{P_{(c-2)(t-1)}} \\ A^{P_{(c-1)0}} & A^{P_{(c-1)1}} & \cdots & A^{P_{(c-1)(t-2)}} & A^{P_{(c-1)(t-1)}} \end{bmatrix}, \quad (3)$$

where H is a sparse matrix of dimension $cL\times tL$, $A^{P_{ij}}$ is an $L\times L$ circulant or all-zeros matrix, p_{ij} is the shift-times of the circulant matrix A, and c and t are two positive integers with $c<t$.

The matrix M of dimensions $c\times t$ is called the mother matrix, which can be generated by the PEG algorithm. This matrix M has the merit of large cycle girth. The parity-check matrix H can further be constructed by replacing each element "0" in matrix M with an all-zeros matrix of dimensions $L\times L$ and replacing each element "1" in matrix M with a circulant permutation matrix of dimensions $L\times L$.

The shift-times p_{ij} of the circulant permutation matrix A can be gained randomly, but it must violate the following cycle condition [21] to eliminate the cycle girth $2t$ (the length of shortest cycle) of the Tanner graph.

$$\sum_{i=1}^{2t}(-1)^{i+1}p_{\alpha_i,\beta_i}=0 \mod L, \quad (4)$$

where $p_{\alpha_1,\beta_1},\ldots,p_{\alpha_{2t},\beta_{2t}}$ are $2t$ corners of any closed path of length $2t$ in the shift-times matrix P.

Because each row (column) in a cyclic-shift sub-matrix has only one nonzero element, the degree distribution of irregular LDPC code constructed by the quasi-cyclic construction method is not changed. At the same time, we can eliminate the shortest cycle and improve the performance of error correction. To further eliminate the shortest cycle, we use multiple extensions based on the circulant matrix to construct irregular LDPC codes with longer length and higher error-correcting performance.

Figure 3 shows the simulation results with different construction methods of LDPC codes for a binary-input additive white Gaussian noise (BIAWGN) channel. In this simulation, all LDPC codes have the same code rate of R=0.5. (1) the irregular LDPC code of block length 2000 constructed by the PEG algorithm; (2) the PEG-based QC-LDPC code with the length of 2000 constructed by extending PEG-based irregular LDPC code; (3) the PEG-based QC-LDPC code of block length 200000. Performance was measured under iterative decoding using belief propagation. The maximum number of iterations for the decoder was set to 100. Comparing the three different LDPC codes, we conclude that the performance of PEG-based QC-LDPC code is better than PEG-based irregular LDPC code, and longer block length LDPC code has a lower error floor.

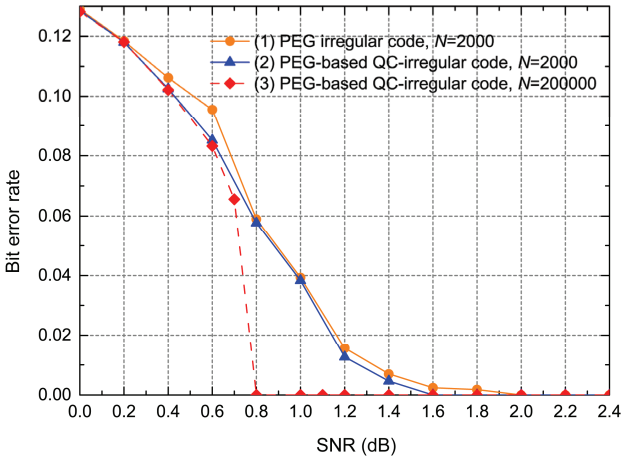

Figure 3 (Color online) The bit error rates of LDPC codes using different construction methods; all have a code rate of R=0.5.

The above results verify that good irregular LDPC codes with large block length can be efficiently constructed by exploiting the PEG algorithm based quasi-cyclic construction method. In sect. 5, we demonstrate that these LDPC codes can be applied to MLC/MSD slice reconciliation with high reconciliation efficiency.

5 Gaussian key reconciliation

In information reconciliation for CV QKD, the equal interval quantization and 5-bit slice scheme are used to generate the bit sequence. For an SNR of 4.77 dB, an optimal quantization efficiency up to 99.32% ($H(Q(Y))$=4.5271) is obtained, as shown in Figure 1. Each of the 5 levels is encoded independently, and the syndrome of X is calculated ($S=XH^{\mathrm{T}}$) and transmitted with the appropriate rate. The reconciliation efficiency β is given by

$$\beta=\frac{H\left(Q(Y)\right)-m+\sum_{i=1}^{m}R_i}{I(X;Y)}. \quad (5)$$

Eq. (5) shows that β is highly dependent on the rates of the LDPC codes. Rates close to the channel capacities should be chosen to maximize the reconciliation efficiency. To construct good irregular LDPC codes, we compute the capacity of LDPC codes under message-passing decoding with density evolution [22-24] and find good degree distribution pairs with differential evolution [25]. For the code rate of 0.4 and 0.9, we show good degree distribution pairs in Table 1. These code parameters were obtained under belief propagation for the BIAWGN channel.

Given the code parameters, the PEG algorithm is used to construct short block length irregular LDPC codes, whose length can be selected. In our simulation, the length of the short block codes is 400, and the girth is 8. Then, the short block length codes are extended to the length of 200000 with the dimensions of the circulant permutation matrix L=500 based on the quasi-cyclic construction method. For an SNR of 4.77 dB, using the chain rule of mutual information, we can obtain that the ideally requiring code rates

Table 1 Good degree distribution pairs of code rate 0.4 and 0.9. σ^* represents the maximum allowed value of noise for the BIAWGN channel

Rate	λ_2	λ_3	λ_7	λ_8	λ_{10}	ρ_5	ρ_6	ρ_{42}	ρ_{43}	σ^*
0.4	0.2998	0.2848	0.1866	–	0.2288	0.2981	0.7019	–	–	1.086
0.9	0.1741	0.2740	–	0.1652	0.3867	–	–	0.9284	0.0716	0.505

are 0.0006/0.0010/0.0124/0.4665/0.9823. Because the contribution of the first three levels is very small, bit strings at these levels are not encoded and are sent directly to Alice, which reduces the decoding complexity of Alice greatly. Finally, the Gaussian key reconciliation efficiency of 93.7% can be reached with the five practical codes with rates 0/0/0/0.43/0.98.

6 Conclusions

In this paper, irregular LDPC codes with large block length are constructed efficiently by the PEG algorithm and quasi-cyclic construction method. These codes are then applied to MLC/MSD slice reconciliation, and Gaussian key reconciliation is successfully achieved with an efficiency of 93.7% for an SNR of 4.77 dB. In the future, to improve the reconciliation efficiency, it is necessary to construct error-correcting codes with higher performance. For SNRs much less than 1, multi-edge LDPC codes using multidimensional reconciliation schemes can be used, which exhibit superior performance [26,27] at very low SNRs.

This work was supported by the National Natural Science Foundation of China (Grant No. 61378010), and the Natural Science Foundation of Shanxi Province (Grant No. 2014011007-1).

1 C. H. Bennett, and G. Brassard, in *Quantum cryptography: Public key distribution and coin tossing: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, 1984), pp. 175–179.
2 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
3 V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
4 F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
5 P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
6 U. M. Maurer, IEEE Trans. Inform. Theor. **39**, 733 (1993).
7 C. H. Bennett, G. Brassard, and J. M. Robert, SIAM J. Comput. **17**, 210 (1988).
8 C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inform. Theor. **41**, 1915 (1995).
9 G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inform. Theor. **50**, 394 (2004).
10 M. Bloch, A. Thangaraj, S. W. Mclaughlin, and J. M. Merolla, in *LDPC-based Gaussian key reconciliation: Proceedings of IEEE Information Theory Workshop* (Punta del Este, 2006), pp. 116-120.
11 J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).
12 X. Y. Hu, E. Eleftheriou, and D. M. Arnold, in *Progressive edge-growth Tanner graphs: Proceedings of IEEE Global Telecommunications Conference* (San Antonio, 2001), pp. 995-1001.
13 X. Y. Hu, E. Eleftheriou, and D. M. Arnold, in *Irregular progressive edge-growth (PEG) Tanner graphs: Proceedings of IEEE International Symposium on Information Theory* (Zurich Research Laboratory, Ruschlikon, 2002), pp. 480.
14 X. Y. Hu, E. Eleftheriou, and D. M. Arnold, IEEE Trans. Inform. Theor. **51**, 386 (2005).
15 M. P. C. Fossorier, IEEE Trans. Inform. Theor. **50**, 1788 (2004).
16 T. Okamura, in *Designing LDPC codes using cyclic shifts: Proceedings of IEEE International Symposium on Information Theory* (Yokohama, 2003), pp. 151.
17 F. Grosshans, and P. Grangier, arXiv: quant-ph/0204127v1.
18 J. Max, IRE Trans. Inform. Theor. **6**, 7 (1960).
19 A. D. Liveris, Z. X. Xiong, and C. N. Georghiades, IEEE Commun. Lett. **6**, 440 (2002).
20 Z. Y. Fan, W. B. Zhang, X. C. Liu, and H. H. Cheng, in *An improved algorithm for constructing QC-LDPC codes based on the PEG algorithm: Proceedings of IEEE 4th International Conference on Communications and Networking* (Xi'an, 2009), pp. 1-4.
21 J. Lu, and J. M. F. Moura, IEEE Trans. Magn. **42**, 208 (2006).
22 T. J. Richardson, and R. L. Urbanke, IEEE Trans. Inform. Theor. **47**, 599 (2001).
23 T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, IEEE Trans. Inform. Theor. **47**, 619 (2001).
24 S. Y. Chung, T. J. Richardson, and R. L. Urbanke, IEEE Trans. Inform. Theor. **47**, 657 (2001).
25 R. Storn, and K. Price, J. Global Optim. **11**, 341 (1997).
26 A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
27 P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).