High efficiency continuous-variable quantum key distribution based on QC-LDPC codes

Ying Guo (郭 迎)[1], Kangshuai Wang (汪康帅)[1], Duan Huang (黄 端)[1,*], and Xueqin Jiang (蒋学芹)[2]

[1]*School of Computer Science and Engineering, Central South University, Changsha 410083, China*
[2]*School of Information Science and Technology, Donghua University, Shanghai 201620, China*
**Corresponding author: duanhuang@csu.edu.cn*

Received April 8, 2019; accepted June 26, 2019; posted online September 12, 2019

Seeking good error correcting codes to improve the efficiency of continuous-variable quantum key distribution (CVQKD) reconciliation is a concerning issue. Due to the introduction of multidimensional reconciliation, the error correcting techniques in the classical binary-input additive white Gaussian noise channel are applicable to CVQKD. In this Letter, we apply the quasi-cyclic low-density parity-check (QC-LDPC) codes, which are specified in 5G protocol, to the reconciliation process. Simulation results show that the reconciliation efficiency can reach 92.6% when the code rate is 22/68 and the signal-to-noise ratio is 0.623. Such a new error correcting code points out a new direction for the development of CVQKD.

OCIS codes: 270.5565, 270.5568, 270.5585.
doi: 10.3788/COL201917.112701.

Quantum key distribution (QKD) is a truly secure communication technology that allows two distant parties, conventionally called Alice and Bob, to extract a string of secret keys even in the presence of a potential eavesdropper (Eve). Two major approaches to QKD include discrete variable (DV) QKD and continuous-variable (CV) QKD. Both of them were developed from the BB84 protocol, which was invented by Bennett and Brassard[1]. In DVQKD, a single-photon or weak coherent state is considered to be the carrier of information, and DV protocols allow one to distribute secret keys over a long distance. But, the practical application is limited by the preparation of the single-photon source and the low-efficiency single-photon detector. Hence, someone proposed a new scheme by encoding the information on CVs, such as the phase or amplitude quadratures of coherent states, to get rid of these limitations. This scheme not only removes the limitation of low detection efficiency, but also shows a higher secret key rate under the same signal-to-noise ratio (SNR)[2].

Although CVQKD based on the coherent state has many advantages, the interference introduced by quantum channel noise or the possible Eve will make the data obtained by the receiver inconsistent with that in the sender. So, it requires error correction for the received sequence. Considering that the efficiency of the error correcting code is an important factor limiting the range of CVQKD[3], researchers have begun to design more efficient codes for the reconciliation process of the CVQKD system. In this regard[4], low-rate multi-edge-type (MET) low-density parity-check (LDPC) codes are proposed, which can achieve high efficiencies above 93.1% for multiple code rates. While the high efficiency is only available with large block lengths, this makes the hardware implementations unrealistic. Thereupon[2], the repeat accumulate (RA) codes are designed with a block lengths of 64,800 bits, which are sufficient to achieve efficiencies above 85% over a wide range of SNRs and advisably reduce the implementation complexity. In this Letter, we first introduce and study the performance of quasi-cyclic (QC) LDPC codes in the 5G protocol, then carry out an expansion operation and apply it to the reconciliation step of the CVQKD system. Our motivation is low implementation complexity and high reconciliation efficiency in the waterfall region of digital video broadcasting satellite second generation (DVB-S2) QC-LDPC codes.

The International Telecommunication Union (ITU) has specified enhanced mobile broadband (eMBB) scenarios for mass data transmission[5], and it also finally determined that 5G communication would use LDPC codes as the long code block coding scheme for the eMBB service. In reality, the code used above is in fact a rediscovery[6] of the LDPC codes developed years earlier by Gallager[7]. It can be defined by a sparse parity check matrix. Furthermore, the matrix can be mapped to a bipartite/tanner graph composed of check nodes and variable nodes, as shown in Fig. 1.

The LDPC code used in the 5G protocol is a type of code with a special structure, which is named the QC-LDPC code[8]. The structure of QC-LDPC codes is depicted in Fig. 2, whose parity check matrix H is generated by expanding each element in the base matrix H_b.

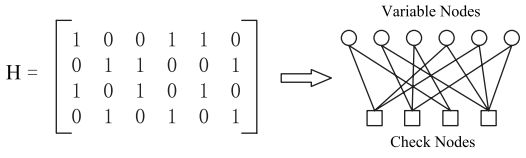

Fig. 1. H matrix and the corresponding tanner graph of (6,4) LDPC code.

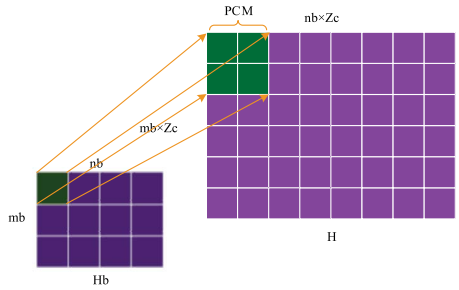

Fig. 2. Schematic diagram of base matrix expansion.

In other words, the H matrix of the QC-LDPC code can be divided into multiple square matrices of equal size, and each square matrix is filled with a cyclic right shift matrix of the identity matrix or the all-zero matrix. Setting the shift parameter $L = 1$, the circular permutation matrix (CPM) based on an identity matrix can be presented as

$$\mathrm{CPM} = I_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{bmatrix}_{Z\times Z}, \tag{1}$$

where Z is the dimension of the matrix, and it has the following characteristics:

- Each CPM is a square matrix;
- Each row (column) of the CMP is obtained by moving the previous row (column) one bit to the right;
- The CPM can be completely determined by its first row or first column.

Thereupon, we can start constructing the QC-LDPC code by defining a binary base matrix H_b,

$$H_b = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}_{m\times n}, \tag{2}$$

where $a_{ij} \in (0, 1)$, $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$. Following the rules presented above, each element in the base matrix H_b is expanded by a square matrix of size $Z \times Z$, and the 0 element and the 1 element are replaced by an all-zero matrix or a CPM, respectively.

The specific value of shift parameter L of each element in H_b is represented by the element in matrix P (same size as the binary base matrix) as follows:

$$P = \begin{bmatrix} P_{11} & P_{12} & \dots & P_{1n} \\ P_{21} & P_{22} & \dots & P_{2n} \\ \vdots & \vdots & & \vdots \\ P_{m1} & P_{m2} & \dots & P_{mn} \end{bmatrix}_{m\times n}. \tag{3}$$

Especially, the circle shift matrix can be defined as an all-zero matrix when $P_{ij} = +\infty$. Finally, we can obtain the H matrix of QC-LDPC codes in this form:

$$H = H_b^{(P_{ij})} = \begin{bmatrix} H_b^{(P_{11})} & H_b^{(P_{12})} & \dots & H_b^{(P_{1n})} \\ H_b^{(P_{21})} & H_b^{(P_{22})} & \dots & H_b^{(P_{2n})} \\ \vdots & \vdots & & \vdots \\ H_b^{(P_{m1})} & H_b^{(P_{m2})} & \dots & H_b^{(P_{mn})} \end{bmatrix}_{mZ\times nZ}. \tag{4}$$

In Ref. [9], two types of matrix P, corresponding to base graph (BG) #1 and BG #2, are given in Table 1, for a total of eight different P-matrices in each BG.

Here, k_b refers to the information bit in the two BGs, and p_b means the number of punctured information nodes. The core size is the selected matrix size when constructing the maximum code rate. The matrix size means the full size of the lowest rate matrix, and it is a crucial ingredient in the two BGs.

Now we assume that the number of bit in each block is K^*, and thus we can find the minimum value of Z in all sets of lifting sizes in Table 2 (denoted as Z_c) that satisfies the inequality

$$k_b \times Z_c \geq K^*. \tag{5}$$

Accordingly, the information length can be calculated by $K = 22Z_c$ for BG #1 and $K = 10Z_c$ for BG #2.

After calculating the value of Z_c, we can find the index i_{LS} corresponding to the row of Z_c according to Table 2. We then select one of the eight P-matrices that are mentioned above to generate the final H matrix.

Given that we already know how the code length, code rate[10], decoding algorithm, and other factors[11] affect the performance of LDPC codes, we are not going to enumerate the two BGs below. In addition, we find that it is not

Table 1. Two Types of BGs Given in the 5G Protocol

Family	k_b	p_b	Core Size	Matrix Size	r_{max}	r_{min}
BG #1	22	2	5×27	46×68	22/25	1/3
BG #2	10	2	7×17	42×52	2/3	1/5

Table 2. Sets of LDPC Lifting Size Z

Set Index (i_{LS})	Set of Lifting Size (Z)
0	2, 4, 8, 32, 64, 128, 256
1	3, 6, 12, 24, 48, 96, 192, 384
2	5, 10, 20, 40, 80, 160, 320
3	7, 14, 28, 56, 112, 224
4	9, 18, 36, 72, 144, 288
5	11, 22, 44, 88, 176, 352
6	13, 26, 52, 104, 208
7	15, 30, 60, 120, 240

easy to obtain an H matrix supporting the same code length at different code rates. Therefore, it is difficult to analyze the performance of the H matrix on a single parameter like code rate. But, fortunately, our focus is not on analyzing how one factor affects error correction performance, but finding the lowest SNR that can be achieved at a given frame error rate (FER). In order to make the CVQKD system work at the lowest possible SNR, the full base matrices of 46×68 and 42×52 are used to obtain the lowest code rate as possible.

Figures 3 and 4 depict the FER curves of the constructed LDPC codes under the same simulation parameters. As can be seen from Fig. 3, code expanding can significantly improve the performance of this code. This phenomenon becomes evident at the points where the SNR is 1.375 dB, and the FER drops markedly when the code length is increased from 8704 to 13,056. This sharp drop phenomenon of FER also occurs at the points where the channel SNR is 0.75 dB in Fig. 4.

Looking from the top to the bottom, the second (green), fourth (purple), and fifth (blue) curves in Fig. 3 and the first (red), third (tan), and fifth (purple) curves in Fig. 4

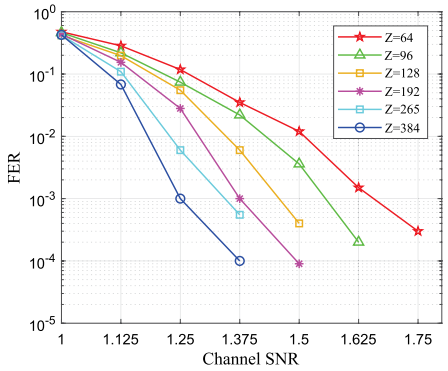

Fig. 3. Performance of constructed LDPC codes with $R = 22/68$, $Z = 64\backslash 96\backslash 128\backslash 192\backslash 256\backslash 384$. Code length $= 4325\backslash 6528\backslash 8704\backslash 13,056\backslash 17,408\backslash 26,612$ bits, binary phase-shift keying (BPSK) modulation, max iteration num $= 50$.

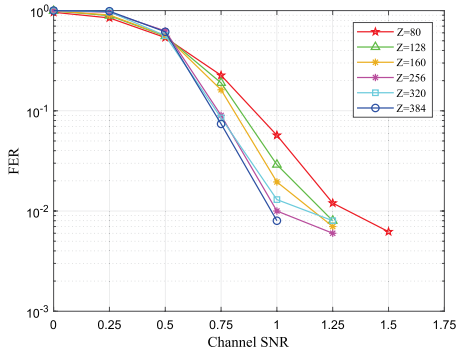

Fig. 4. performance of constructed LDPC codes with $R = 10/52$, $Z = 80\backslash 128\backslash 160\backslash 256\backslash 320\backslash 384$. Code length $= 4160\backslash 6656\backslash 8320\backslash 13,312\backslash 16,640\backslash 19,968$ bits, binary phase-shift keying (BPSK) modulation, max iteration num $= 50$.

depict the performance when the same base matrix is expanded to different code lengths. It can be clearly seen that the larger the expansion factor, the better the error correction performance will be, which indicates that increasing the expansion factor is an effective way to improve error correction performance of this code subset[12], rather than using repetition strategy.

Considering that the performance of this QC-LDPC code is expanded to be greatly improved, we now plan to introduce them into the reconciliation process of CVQKD. Figure 5 shows the coherent states CVQKD system, which utilizes homodyne detection and reverse reconciliation. The Eve is assumed to utilize collective attacks, and we assume asymptotic code length and finite key-size effects[13,14] are not considered.

The first, to the best of our knowledge, CVQKD protocol based on Gaussian modulated coherent states is the Grosshans and Grangier in 2002 (GG02) protocol[15], which is the most widely studied protocol in CVQKD. Similarly, our scheme is based on this protocol. We thoroughly describe the four pivotal steps (see Figure 5 for serial numbers) of how Alice and Bob interact below.

Alice prepares a continuous laser by a CW laser[16,17] and modulates it into pulsed light. Then, the pulsed light is separated into strong local oscillator (LO) light and weak signal light by a beam splitter (BS). Alice executes the first step of reconciliation straight after the generated weak signal light.

Step 1. Alice prepares an eight-dimensional random variable $X = (X_1, X_2, \ldots, X_8)^T$, which obeys the Gaussian distribution centered at zero with variance V_A in the units of shot-noise variance N_0. X can be normalized to x, namely $x = (X_1, X_2, \ldots, X_8)^T / \|X\| = (x_1, x_2, \ldots, x_8)^T$; so, the normalized random vector x has a uniform distribution on the unit sphere S^{d-1}[18] to prove that the side information that Alice sends to Bob on the public channel does not give any relevant information to Eve. For each generated weak signal pulse, Alice modulates the variable x to the quadrature X_A or the orthogonal quadrature P_A of the pulse by the modulator. Afterward, the signal light is attenuated to a suitable intensity by a variable ATT. The LO is designed to propagate in a relatively long optical fiber to reduce the interference of it on the signal light. The two beams are then coupled into a single fiber and transmitted to Bob through the quantum channel with a transmission efficiency $T = 10^{-\alpha L/10}$ and an excess

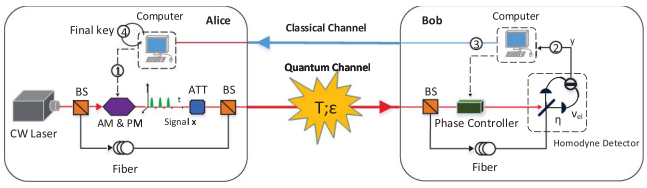

Fig. 5. Experimental setup of CVQKD scheme based on GG02 protocol. CW laser, continuous-wave laser; BS, beam splitter; AM, amplitude modulator; PM, phase modulator; ATT, attenuator.

noise ξ_c. Bob divides the received beam into signal light and an LO and inputs the signal light into the same length of the delay fiber, so that the signal light has the same time of delay as the LO. Further, the LO introduces a phase difference of zero or $\pi/2$ through a phase controller controlled by Bob and interferes with the signal light at the BS. In this way, a homodyne detector features an electronic noise υ_{el}, and an efficiency η can randomly select the quadrature X_A or the orthogonal quadrature P_A for the measurement. Therefore, in such a practical homodyne scheme, the total noise[19] referred to the channel input can be expressed as $\chi_{tot} = \chi_{line} + \chi_h / T$, where $\chi_{line} = \chi_c / T - 1$, $\chi_h = [(1-\eta) + \upsilon_{el}]/\eta$. We then go to the remaining step of reconciliation.

Step 2. Bob gets the eight-dimensional random variable $y = (y_1, y_2, \ldots, y_8)^T = x + \varepsilon$, where $x \sim N(0,1)^8$ and $\varepsilon \sim N(0, \sigma^2)^8$. According to the central limit theorem, it can be derived that y obeys a Gaussian distribution[20], namely $y \sim N(0, 1+\sigma^2)^8$.

Step 3. A binary string U is chosen randomly as the secret key that will be encoded into a linear error correcting code, such as the QC-LDPC code we proposed above, to generate u in Bob's side and map $u \in F_2^8$ onto an isomorphic image in the eight-dimensional sphere:

$$F_2^8 \to S^7 \subset R^8, \tag{6}$$

$$u = (b_1, b_2, \ldots, b_8) \mapsto \left(\frac{(-1)^{b_1}}{\sqrt{8}}, \frac{(-1)^{b_2}}{\sqrt{8}}, \ldots, \frac{(-1)^{b_8}}{\sqrt{8}} \right), \tag{7}$$

where $(b_1, b_2, \ldots, b_8)$ corresponds to the binary code word. Then, Bob can calculate the rotation matrix M according to the lemma 4 in Ref. [18],

$$M(x, y) = \sum \alpha_i(x, y) A_i, \tag{8}$$

and he sends matrix M and syndrome $S = Hu$ to Alice via the public channel, where $\alpha_i(x, y) = (A_i x | y)$, H is the parity check matrix of the proposed LDPC code, M satisfies $M(x, y)\, x = y$, and specific orthogonal matrix A_i can be referred to Ref. [18].

Step 4. Alice calculates the vector v based on the rotation matrix, where vector v is the noisy version of vector u, and the H matrix is used to correct the v vector. Finally, we can perform a standard privacy amplification[21] to agree on a final secret key.

Theoretically, the mutual information I_{AB} between Alice and Bob can be derived from the total noise referred to the channel as

$$I_{AB} = \frac{1}{2} \log_2 (1 + \mathrm{SNR}) = \frac{1}{2} \log_2 \left(\frac{V + \chi_{tot}}{1 + \chi_{tot}} \right), \tag{9}$$

where $V = V_A + 1$. To achieve the security constraint proposed in Ref. [22], the theoretical secret key rate is

$$R = I_{AB} - I_E, \tag{10}$$

where I_E denotes the maximum information that Eve can obtain from Bob's side, which is limited by the Holevo bound χ_{BE}[23] for collective attacks as

$$\chi_{BE} = S(\rho_E) - \int \mathrm{d} m_B p(m_B) S(\rho_E^{m_B}), \tag{11}$$

where m_B is the measurement of Bob, and it takes the form $m_B = x_B$ for the homodyne detector. $p(m_B)$ is the probability density of the measurement, $\rho_E^{m_B}$ is Eve's state conditional on Bob's measurement result, and S is the Neumann entropy. Since it has been shown that Gaussian attacks are optimal for collective attacks[24,25], and both Eve's system and Bob's measurement purify the system of CVQKD, the Holevo bound χ_{BE} can be calculated as in Ref. [26].

In the practical case, we have to take the reconciliation efficiency β and FER into consideration. The former is used to describe the efficiency of the mutual information extraction, and the latter is used to calculate the number of correct frames that we can obtain. They are closely related to the performance of the error correcting codes, so the secret key rate can be rewritten as[27]

$$K = (1 - \mathrm{FER})(\beta I_{AB} - \chi_{BE}), \tag{12}$$

where the efficiency of reconciliation is measured by $\beta = \frac{R}{C(s)}$ for a given SNR s, R is the rate of the code, and $C(s)$ is the capacity of the channel when the SNR is s.

For a given FER, the lowest SNR that can complete the correction is different, depending on the error correcting codes. When the lowest SNR is less than or equal to the SNR of the actual quantum channel, then the CVQKD system is feasible. However, in order to pursue longer transmission distances and higher key rates, the SNR of the quantum channel will be extremely low. Therefore, it is necessary to decrease the FER in Figs. 3 and 4.

A typical approach to operate this high performance QC-LDPC code over a low SNR is to use an expansion strategy. This strategy can maintain the excellent characteristics of the basic matrix given in the 5G protocol, and the decoding complexity can be acceptable by using two one-dimensional arrays to represent the LDPC codes. We just need to increase the maximum expansion factor in Table 2 from 384 to a suitable value, such as 1000. This means that the basic matrix we choose is the matrix corresponding to $i_{LS} = 1$ in Table 2.

We first construct 10/52 5G codes with a length of 52,000 ($i_{LS} = 1, Z = 1000$) and 1/4 DVB-S2 codes with a length of 62,800. The curves in Fig. 6(a) illustrate that the 10/52 5G code performs poorly in the waterfall region of the DVB-S2 code. In reality, we set more than one value for i_{LS}, namely $i_{LS} \in \{0, 1, 2, 3, 4, 5, 6, 7\}$, and the performance presents the same horizontal line over a wide range of SNRs. This means that to make better use of BG #2, we need to adopt other strategy for it. Figure 6(b) shows the performance of the 22/68 5G code with a length of 68,000 ($i_{LS} = 1, Z = 1000$) and 1/3 DVB-S2 code with a length

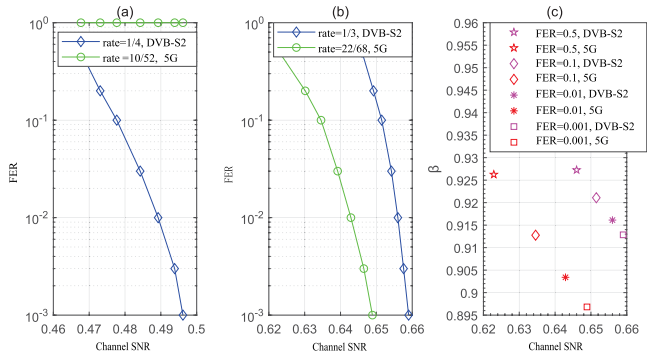

Fig. 6. (a) FER values of constructed QC-LDPC codes with rates 1/4 and 10/52. (b) FER values of constructed QC-LDPC codes with rates 1/3 and 22/68. Both (a) and (b) are binary phase-shift keying (BPSK) modulation, max iteration num = 500, frame num = 10,000. (c) Reconciliation efficiency of the QC-LDPC codes for FERs of 0.5, 0.1, 0.01, and 0.001.

of 62,800. Simulation results show that the former has a lower FER curve under similar code length and code rate conditions. In Fig. 6(c), we find the expanded QC-LDPC code in the 5G protocol provides comparable efficiency to that of the DVB-S2 protocol despite being a lower rate.

We emphasize the loss in the reconciliation efficiency caused by the multidimensional modulation, which has been studied in Ref. [3] and shows to be negligible in the low SNR regime for the eight-dimensional reconciliation scheme. On this basis, we set several free parameters for the CVQKD model we described: the signal variance encoded by Alice V_A, the transmission efficiency T of the quantum channel, the channel excess noise ϵ, the homodyne efficiency η, and the electronic noise V_{el} in Bob's station. As can be seen in Fig. 7, the expanded QC-LDPC code in the 5G protocol provides equivalent secret key rates to that of DVB-S2 protocol.

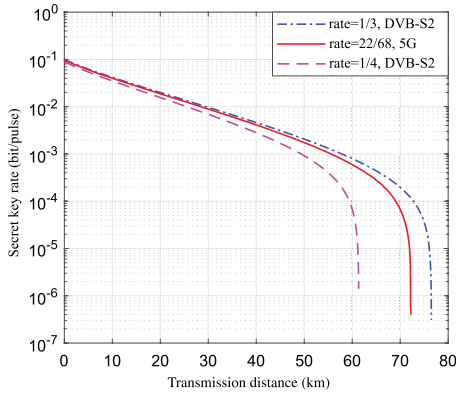

Fig. 7. Secret key rate as a function of distance for a CVQKD system with a homodyne detector, excess noise $\epsilon = 0.01$, detection efficiency $\eta = 0.6$, electronic noise $V_{el} = 0.01$, and the attenuation factor α of the quantum channel set to be 0.2 dB/km. Pinkish-red dashed curve and blue dashed curve show the QC-LDPC codes (length 62,800, rates 1/4 and 1/3) in the DVB-S2 protocol, respectively. Red solid curve shows the QC-LDPC code (length 68,000, rate 22/68) in the 5G protocol.

In this Letter, we investigate the performance of introducing the QC-LDPC codes specified in the 5G protocol into a common CVQKD system. In general, this code can provide reasonable performance just by increasing the expansion factor, as the maximum expansion factor given in the protocol is only 384. Given the QC-LDPC codes' commercial maturity, and the optimization strategy based on the expansion factor has low implementation complexity, these make the application of this code in CVQKD promising.

This work is supported by the National Natural Science Foundation of China (Nos. 61801522 and 61871407).

References

1. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference Computers, Systems and Signal Processing* (1984), p. 175.
2. S. J. Johnson, V. A. Chandrasetty, and A. M. Lance, in *Proceedings of 2016 Australian Communications Theory Workshop* (2016), p. 18.
3. A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
4. P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
5. H. Gamage, N. Rajatheva, and M. Latva-aho, in *Proceedings of 2017 European Conference on Networks and Communications* (2017), p. 1.
6. D. J. C. MacKay and R. M. Neal, Electron. Lett. **32**, 1645 (1996).
7. R. Gallager, IRE Trans. Inf. Theory **8**, 21 (1962).
8. M. P. C. Fossorier, IEEE Trans. Inf. Theory **50**, 1788 (2004).
9. J. M. Meredith, "5G; NR; Multiplexing and channel coding," Technical Specification ETSI TS 138 212 (V15.2.0) (2018).
10. D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, Int. J. Quantum. Inf. **13**, 1550010 (2015).
11. H. Zhang and J. M. F. Moura, in *Proceedings of IEEE Global Telecommunications Conference* (2003), p. 4022.
12. http://www.3gpp.org/ftp/TSG-RAN/WG1-RL1/TSGR1-89/Docs/.
13. A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
14. H. Zhang, Y. Mao, D. Huang, Y. Guo, X. Wu, and L. Zhang, Chin. Phys. B **27**, 090307 (2018).
15. F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
16. N. Zhou, Chin. Opt. Lett. **15**, 010002 (2017).
17. S. Zhou, P. Gu, X. Li, and S. Liu, Chin. Opt. Lett. **15**, 071401 (2017).
18. A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
19. D. Huang, P. Huang, T. Wang, H. Li, Y. Zhou, and G. Zeng, Phys. Rev. A **94**, 032305 (2016).
20. M. Shirvanimoghaddam, S. J. Johnson, and A. M. Lance, in *Proceedings of 2016 IEEE International Conference on Communications* (2016), p. 1.
21. G. Brassard and L. Salvail, Lect. Notes Comput. Sci. **765**, 411 (1994).
22. X.-Q. Jiang, P. Huang, D. Huang, D. Lin, and G. Zeng, Phys. Rev. A **95**, 022318 (2017).
23. R. Renner, Int. J. Quantum. Inf. **6**, 1 (2008).
24. M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).
25. R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
26. S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B: At. Mol. Opt. Phys. **42**, 114014 (2009).
27. X.-Q. Jiang, S. Yang, P. Huang, and G. Zeng, IEEE Photon. J. **10**, 7600410 (2018).