Japanese Journal of Applied Physics **56**, 044401 (2017)
https://doi.org/10.7567/JJAP.56.044401

REGULAR PAPER

High-efficiency reconciliation for continuous variable quantum key distribution

Zengliang Bai[1,2], Shenshen Yang[1,2], and Yongmin Li[1,2*]

[1]*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*
[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*

*E-mail: yongmin@sxu.edu.cn

Received November 24, 2016; accepted January 16, 2017; published online March 13, 2017

Quantum key distribution (QKD) is the most mature application of quantum information technology. Information reconciliation is a crucial step in QKD and significantly affects the final secret key rates shared between two legitimate parties. We analyze and compare various construction methods of low-density parity-check (LDPC) codes and design high-performance irregular LDPC codes with a block length of 10^6. Starting from these good codes and exploiting the slice reconciliation technique based on multilevel coding and multistage decoding, we realize high-efficiency Gaussian key reconciliation with efficiency higher than 95% for signal-to-noise ratios above 1. Our demonstrated method can be readily applied in continuous variable QKD.

1. Introduction

Quantum key distribution (QKD),[1–8] which can offer unconditional security, is the most practical branch of quantum information technology. On the basis of the basic principles of quantum physics, including the uncertainty principle and the quantum no-cloning principle, QKD can enable the sharing of random secret bits between two distant and legitimate parties (Alice and Bob) using an untrusted quantum channel with the help of an auxiliary authenticated classical channel. Two types of QKD protocols are currently investigated, i.e., discrete-variable QKD (DVQKD)[1,2] and continuous-variable QKD (CVQKD).[9–17] In DVQKD, one can encode information on discrete variables of quantum systems, such as the phase or polarization of single photons, which can be detected by single-photon detectors, and the raw keys are binary bit strings. In contrast, the CVQKD protocols employ the quadratures of a quantized electromagnetic field to encode the key information, and the signals measured by Bob are continuously distributed. Recently, the CVQKD protocols have been proven to be unconditionally secure against arbitrary attack in the asymptotic limit and in the finite-size regime.[18,19] The CVQKD protocols have the merits of requiring only standard optical communication technology and are expected to achieve higher secret key rates at a relatively short distance. Moreover, they are robust to the noisy photons in the quantum channel owing to the mode selection of the local oscillator.

When a QKD system is running, various noises are introduced owing to the nonideal preparation of quantum states, the dark noises of photoelectric detection, and potential eavesdropping behaviors, which unavoidably cause the raw keys of the two parties to be different from each other and the leakage of secret key information. Therefore, a key distillation process including information reconciliation and privacy amplification is necessary. Information reconciliation is an error-correcting protocol to correct the errors between Alice's and Bob's raw keys, and is implemented by exchanging error-correcting messages through an authenticated classical channel.[20] The privacy amplification procedure is used to filter out the potential leakage of information to an eavesdropper (Eve) with two-universal hash functions and extract secure keys. So far, the main reconciliation schemes for Gaussian-modulated CVQKD include slice reconciliation[21–23] and multidimensional reconciliation.[24,25] At a very low signal-to-noise ratio (SNR), the capacity of a binary input additive white Gaussian noise (BIAWGN) channel is approximately equivalent to the capacity of the physical Gaussian channel. A multidimensional reconciliation scheme that relies on a d-dimensional rotation operation to build a virtual channel very close to the BIAWGN channel, when combined with low-rate multiedge-type low-density parity-check (LDPC) codes, can achieve high-efficiency information reconciliation. However, because the capacity gap of the two channels increases gradually with the increase in SNR, the above approximation is no longer valid at high SNRs. Sliced error correction (SEC)[21] is an effective approach for correcting errors of correlated Gaussian-distributed continuous variables between Alice and Bob. Code-modulated techniques [multilevel coding (MLC) and multistage decoding (MSD)][26] with LDPC codes were proposed for channel coding and error correction in SEC, and the reconciliation efficiency of SEC was improved significantly.[22] At relatively high SNR, the slice reconciliation protocol has higher efficiency than the multidimensional reconciliation protocol. It is known that higher reconciliation efficiency means one can extract more secret keys. To improve the reconciliation efficiency, it is necessary to construct high-efficiency error-correcting LDPC codes.

In this paper, we propose an efficient construction method to design high-performance irregular LDPC codes for different code rates with a block length of 10^6. To this end, we investigate various construction methods for LDPC codes in detail and construct high-error-correcting-performance LDPC codes with different code rates. A discretized density evolution algorithm[27] is used to obtain good node degree distributions of irregular LDPC codes for the BIAWGN channel. These LDPC codes are further applied to correct errors of the Gaussian raw keys between Alice and Bob through MLC/MSD-based slice reconciliation schemes. Simulation results show that the reconciliation efficiency can reach more than 95% for an SNR from 1 to 3 with frame error rates (FERs) below 24%. The achieved reconciliation efficiency is higher than previously reported values, to the best of our knowledge.

The rest of this paper is organized as follows. In Sect. 2, we theoretically analyze the reconciliation protocol and secret key rate for CVQKD. In Sect. 3, we search for good node

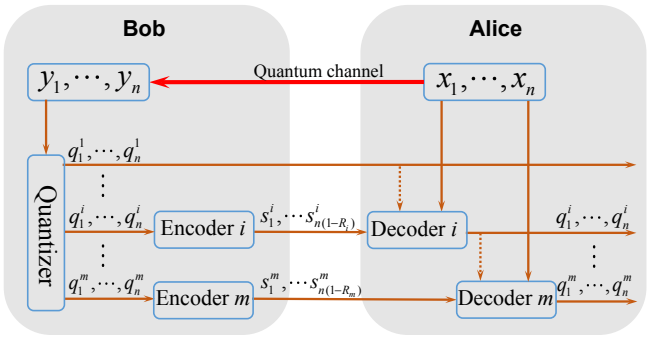

Fig. 1. (Color online) Reverse slice reconciliation based on MLC and MSD with side information.

degree distributions by discretized density evolution and differential evolution. Comparing the progressive-edge-growth (PEG) algorithm and the random construction method, we propose an effective method of constructing high-performance LDPC codes for different code rates. In Sect. 4, the results of our high-efficiency slice reconciliation based on MLC and MSD are described in detail. In Sect. 5, we give a brief conclusion.

2. Reconciliation protocol and secret key rate

Figure 1 depicts a schematic diagram of reverse slice reconciliation based on MLC and MSD with side information. The MLC scheme is a high-efficiency coding modulation technique and encodes the binary sequence at each level with a channel capacity rule. In MSD, the decoder of each level employs the results of the decoders of its previous levels, and such a joint iterative scheme is employed to improve the performance of decoding.

Usually, Gaussian states normally distributed in the phase space are used for CV-QKD schemes. After quantum transmission, Alice and Bob have two correlated Gaussian-distributed continuous variable sequences. Using mutual information theory, the final secret key rate can be written as $\Delta I = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}$, where β is the reconciliation efficiency, I_{AB} is the classical mutual information between Alice and Bob, and χ_{BE} is the Holevo information between Bob and Eve, which is also called leakage information for reverse reconciliation. In comparison with the direct reconciliation scheme, reverse reconciliation, in which Alice and Bob use Bob's data to establish the secret key, can break the 3 dB channel loss limit[11,28] and has been exploited for long-distance CVQKD systems. From the above formula, we can see that the efficiency β directly affects the final number of secret keys.

As shown in Fig. 1, the slice reconciliation scheme is divided into two parts: quantization of Gaussian-distributed variables and error correction based on MLC and MSD. The efficiency β of a practical MLC/MSD slice reconciliation protocol can be expressed as the following product:

$$\beta_{\mathrm{rec}} = \beta_{\mathrm{slice}} \cdot \beta_{\mathrm{code}}, \tag{1}$$

where the quantization efficiency of Gaussian-distributed variables, β_{slice}, is given by

$$\beta_{\mathrm{slice}} = \frac{I[X;Q(Y)]}{I(X;Y)}, \tag{2}$$

where $Q(Y)$ is the quantization of variable Y and $I(X;Y)$ is the mutual information between Alice and Bob. The efficiency of error correction, β_{code}, is given by

$$\beta_{\mathrm{code}} = \frac{H[Q(Y)] - m + \sum_{i=1}^{m} R_i}{I[X;Q(Y)]}, \tag{3}$$

where $H[Q(Y)]$ is the information entropy of $Q(Y)$. Hence, the efficiency of slice reconciliation can be calculated as

$$\beta_{\mathrm{rec}} = \frac{H[Q(Y)] - m + \sum_{i=1}^{m} R_i}{I(X;Y)}, \tag{4}$$

where R_i is the code rate for each level. The quantizer $Q(Y)$ divides the real line $(-\infty,+\infty)$ into 2^m disjoint intervals by $2^m - 1$ equally spaced points. The quantization efficiency β_{slice} is maximized by maximizing $I[X;Q(Y)]$ through the selection of an optimal interval step for the chosen number of intervals 2^m. With 32-interval ($m = 5$) quantization, the efficiency β_{slice} can reach above 99.4% for an SNR from 0.86 to 3. The second step is the reverse error correction with side information[29] based on MLC and MSD. After the discretization of Gaussian-distributed continuous variables, Bob classifies them into m levels, each of which corresponds to a bit sequence. Each level is encoded independently as a syndrome by the error-correcting code with a rate R_i ($1 \le i \le m$). Then, Bob sends the syndromes of the m levels to Alice through an authenticated classical channel. On the basis of the syndromes and her own Gaussian variables (side information), Alice can recover Bob's key.

It is known that the code rate of each level is bounded above by the channel capacity. Here, we use R_i^{opt} to represent the optimal code rate, and the following relation can be obtained:

$$I[X;Q(Y)] = H[Q(Y)] - m + \sum_{i=1}^{m} R_i^{\mathrm{opt}}. \tag{5}$$

From Eqs. (3) and (5), the efficiency of error correction can also be rewritten as

$$\beta_{\mathrm{code}} = \frac{H[Q(Y)] - m + \sum_{i=1}^{m} R_i}{H[Q(Y)] - m + \sum_{i=1}^{m} R_i^{\mathrm{opt}}}. \tag{6}$$

Equation (6) shows that the efficiency β_{code} is highly dependent on the rates of the error-correcting codes in MLC and MSD. To improve the efficiency of slice reconciliation, high-performance LDPC codes that perform at rates extremely close to the Shannon capacity should be designed.

3. Construction of high-performance long-length LDPC codes

Some studies have indicated that irregular LDPC codes with good node degree distributions exhibit a higher error-correcting capacity than regular codes. Discretized density evolution is an improved algorithm of density evolution[30] and has a low operation complexity. It uses a quantization operation to discretize input and output messages of sum-product decoding. Using this algorithm, we can calculate the threshold values of message-passing decoding and obtain

Table I. Optimal variable node degree distributions for two different code rates.

Code rate	Variable node degree distributions
0.120	$\lambda(x) = 0.3379x + 0.1952x^2 + 0.2338x^6 + 0.1160x^{30} + 0.1171x^{59}$
0.836	$\lambda(x) = 0.0970x + 0.2734x^2 + 0.2832x^9 + 0.0440x^{23} + 0.3024x^{39}$

very good node degree distributions of irregular LDPC codes by differential evolution. In Table I, we show the optimal node degree distribution pairs with code rates of 0.12 and 0.836 obtained under belief propagation for the BIAWGN channel. Starting with the good node degree distribution pairs, high-efficiency LDPC codes can be constructed.

It is well known that the performance of LDPC codes gradually improves with increasing block length. Unfortunately, the construction of the parity-check matrix of long irregular LDPC codes is not straightforward. In the following, four different construction methods are investigated and compared: the PEG algorithm, random construction (RC), quasi-cyclic extension based on RC (QC-RC), and quasi-cyclic extension based on PEG (QC-PEG). In all cases of QC extension,[31] the length of the mother matrix is 10^5. To assess the performance of the codes, the log-likelihood ratio belief propagation algorithm with side information is employed to decode LDPC codes over a BIAWGN channel, and the maximum number of iterations is set to be 100.

For the rates of 0.12 and 0.836, we show the results of the decoding performance of irregular LDPC codes with block lengths of 10^5 and 10^6 in Figs. 2 and 3, respectively. In QKD protocols, the privacy amplification requires that whole blocks of bits are the same between Alice and Bob after information reconciliation. To this end, the frame error rate (FER) is adopted to evaluate the decoding performance. Because it is difficult to construct LDPC codes with length $N = 10^6$ by the PEG algorithm, the decoding performance is not included (using an i7 CPU at 3.4 GHz for a rate of 0.12, the time consumed for the PEG algorithm is more than 5 days). From Fig. 2, we can conclude that the RC and QC-RC methods have better performance than the QC-PEG algorithm, and the performances of RC and QC-RC only show a small difference. The runtimes of the RC and QC-RC methods with 4-cycle-free are ∼50 and ∼10 s, respectively. From Fig. 3, we can see that the LDPC codes constructed on the basis of the three methods (QC-PEG, QC-RC, and RC) have similar error-correcting performance characteristics for a rate of 0.836. The time consumed for the QC-PEG, QC-RC, and RC algorithms are 5195, 3813, and 54322 s, respectively. As a result, on the basis of the performance and consumed time, the RC method is considered superior at low rate codes, while QC-RC is better for high rate codes.

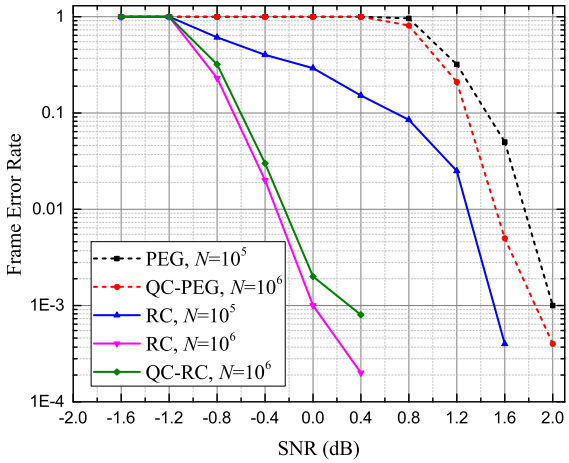

Fig. 2. (Color online) Decoding performance characteristics of irregular LDPC codes with code rate of 0.12 for different block lengths. QC-PEG and QC-RC represent QC extensions based on the PEG algorithm and RC method, respectively.

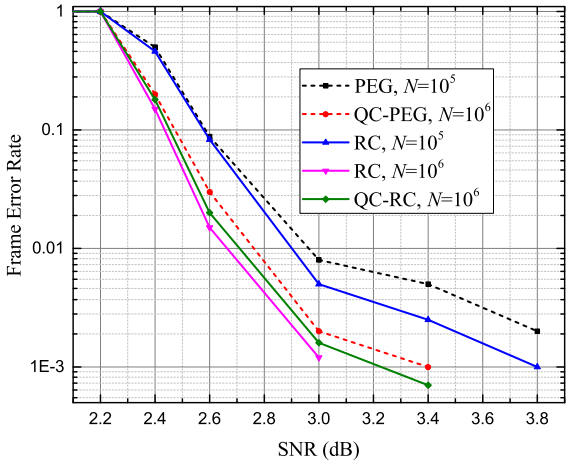

Fig. 3. (Color online) Decoding performance characteristics of irregular LDPC codes with code rate of 0.836 for different block lengths.

4. High-efficiency reconciliation for Gaussian key

In the following, we apply the techniques developed in the previous sections to the information reconciliation of a Gaussian-modulated CVQKD system. Using an equal-interval quantizer, the Gaussian-distributed continuous variables are divided into five discretization layers each of which forms a binary sequence. This operation maps the channel into five virtual BIAWGN channels. In accordance with the chain rule of mutual information, the optimal code rate corresponding to the ith level for a given SNR can be calculated as

$$R_i^{\text{opt}} = 1 - [I(\infty) - I(s)], \tag{7}$$

where $I(s)$ is the mutual information of the ith virtual BIAWGN channel for SNR $= s$.

The optimal rates for SNRs between 0.86 and 3 are shown in Table II. Because the optimal rates of error-correcting codes at levels 1, 2, and 3 are very low, the binary sequences at these levels are not encoded and are directly sent to Alice, which greatly reduces the decoding complexity of Alice and the time consumed for information reconciliation. The practical rates of the LDPC codes at levels 4 and 5 are bounded above by their optimal code rates. To increase the practical rate of each level, it is necessary to design high-performance irregular LDPC codes.

On the basis of the techniques developed above, two different strategies are adopted to construct large-block (10^6) LDPC codes with different rates. For code rates below 0.8, the RC method is utilized, while for rates above 0.8, the construction is implemented through two steps. We first construct a mother matrix using the RC method, and then

Table II. Optimal code rates for given SNRs.

SNR	R_1^{opt}	R_2^{opt}	R_3^{opt}	R_4^{opt}	R_5^{opt}
0.86	0.00015	0.00027	0.00054	0.11154	0.81343
1.0	0.00018	0.00032	0.00067	0.13505	0.84184
1.2	0.00022	0.00039	0.00093	0.16932	0.87419
1.4	0.00026	0.00046	0.00129	0.20444	0.89965
1.8	0.00035	0.00061	0.00248	0.27482	0.93565
2.2	0.00043	0.00075	0.00458	0.34337	0.95853
2.6	0.00051	0.00088	0.00782	0.40715	0.97297
3.0	0.00059	0.00101	0.01239	0.46650	0.98234

Table III. Parameters of slice reconciliation.

SNR	$H(Q(Y))$	$R_1/R_2/R_3/R_4/R_5$	β	FER
0.86	4.5191	0/0/0/0.0990/0.8025	93.96%	18%
1.0	4.5191	0/0/0/0.1200/0.8360	95.02%	19%
1.2	4.5213	0/0/0/0.1550/0.8650	95.17%	23%
1.4	4.5220	0/0/0/0.1900/0.8900	95.33%	19%
1.8	4.5249	0/0/0/0.2550/0.9300	95.58%	16%
2.2	4.5271	0/0/0/0.3220/0.9500	95.24%	24%
2.6	4.5299	0/0/0/0.3870/0.9650	95.44%	18%
3.0	4.5321	0/0/0/0.4480/0.9725	95.26%	22%

extend the mother matrix to large-block LDPC codes by the QC extension. These irregular LDPC codes are further applied to the error correction encoding and decoding of levels 4 and 5, which enables us to achieve high-efficiency information reconciliation with efficiency above 95% and an FER below 24%. Table III shows the achieved reconciliation efficiencies for SNRs from 0.86 to 3.0 and the related parameters used in reconciliation. The maximum numbers of decoding iterations at levels 4 and 5 are set to 180 and 60, respectively.

By considering decoding failures with the FER p_{fail}, the effective secret key rate for a QKD system can be rewritten as

$$\Delta I_{\text{eff}} = (\beta I_{\text{AB}} - \chi_{\text{BE}})(1 - p_{\text{fail}}). \tag{8}$$

In a CVQKD system, to achieve a long-distance transmission (high channel loss), the reconciliation efficiency β is more crucial than the FER. This is due to the special characteristics of CVQKD: each signal pulse sent by Alice will be detected by Bob and used to extract a secret key, and in the case of high channel loss, χ_{BE} will be very close to I_{AB}: $\chi_{\text{BE}} \to I_{\text{AB}}$. Therefore, typical β values of at least above 0.9 are required to ensure a positive secret key rate according to Eq. (1). To reach such a high β at a low SNR, the FER will increase to the order of 10%[25,32] unlike its counterpart in DVQKD, where the FER can be as low as 0.1%. It note that one can still achieve a high secret key rate even at a relatively high FER.

Table IV shows our information reconciliation results for CVQKD and those reported previously. There are two reconciliation schemes: reconciliation based on binary codes and that based on nonbinary codes. Using high-performance binary irregular LDPC codes, we can achieve higher reconciliation efficiency. Note that reconciliation based on nonbinary LDPC codes also exhibits good efficiency at an SNR of 3,[32] while it has a higher computational complexity.

Table IV. Reconciliation efficiencies.

SNR	β_{MSD1}	β_{MSD2}	$\beta_{\text{non-binary}}$	β
0.86		93.7%		93.96%
1	79.4%	94.2%		95.02%
3.0	88.7%	94.1%	94.3–95.2%	95.26%
N (bits)	2×10^5	$2^{20} \approx 10^6$	2×10^5	10^6
	Ref. 22	Ref. 23	Ref. 32	Our work

Note that information reconciliation can affect the security analysis for QKD.[33–36] For CVQKD, the error correction leakage $l_{\text{LE}} = H[Q(Y)] - \beta_{\text{rec}} I(X;Y)$, which depends on the reconciliation efficiency, is an important parameter for security analysis.[18,19,37–39] It has been shown that the one-way slice reconciliation technique based on a linear error-correcting code discussed in this paper is compatible with the composable security proof for CVQKD with coherent states.[19]

5. Conclusions

In this study, for SNRs between 0.86 and 3, we achieved high-efficiency information reconciliation for CVQKD based on the slice reconciliation protocol. Using a discretized density evolution algorithm, we acquired very good node degree distribution pairs of irregular LDPC codes. As a result of investigating and comparing various code construction methods, including the PEG algorithm, random construction, quasi-cyclic extension based on random construction, and quasi-cyclic extension based on PEG, we proposed a convenient and efficient construction method for designing high-performance irregular LDPC codes with a block length of 10^6. As a result, high-efficiency Gaussian key reconciliation was successfully realized with an efficiency above 95% and an FER below 24% for SNRs above 1.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (NSFC) (61378010, 11504219), the Key Project of the Ministry of Science and Technology of China (2016YFA0301403), the Natural Science Foundation of Shanxi Province (2014011007-1), and the Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi.

1) C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, 1984, p. 175.
2) N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
3) S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
4) X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Phys. Rep. **448**, 1 (2007).
5) V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
6) C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
7) H. K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
8) E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).
9) T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).
10) M. Hillery, Phys. Rev. A **61**, 022309 (2000).
11) C. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
12) F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P.

Grangier, Nature **421**, 238 (2003).
13) 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).
14) B. Qi, W. Zhu, L. Qian, and H. K. Lo, New J. Phys. **12**, 103042 (2010).
15) C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
16) P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
17) B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).
18) F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
19) A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
20) U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
21) G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).
22) M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, Proc. IEEE Information Theory Workshop, 2006, p. 116.
23) P. Jouguet, D. Elkouss, and S. Kunz-Jacques, Phys. Rev. A **90**, 042329 (2014).
24) A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
25) P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
26) U. Wachsmann, R. F. H. Fischer, and J. B. Huber, IEEE Trans. Inf. Theory **45**, 1361 (1999).
27) S. Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, IEEE Commun. Lett. **5**, 58 (2001).
28) F. Grosshans and P. Grangier, arXiv:quant-ph/0204127.
29) A. D. Liveris, X. Zixiang, and C. N. Georghiades, IEEE Commun. Lett. **6**, 440 (2002).
30) T. J. Richardson and R. L. Urbanke, IEEE Trans. Inf. Theory **47**, 599 (2001).
31) Z. Bai, X. Wang, S. Yang, and Y. Li, Sci. China Phys. Mech. Astron. **59**, 614201 (2016).
32) C. Pacher, J. Martinez-Mateo, J. Duhme, T. Gehring, and F. Furrer, arXiv:1602.09140.
33) M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
34) M. Hayashi and T. Tsurumaru, New J. Phys. **14**, 093014 (2012).
35) M. Hayashi and R. Nakayama, New J. Phys. **16**, 063009 (2014).
36) A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New J. Phys. **17**, 093011 (2015).
37) R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
38) A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
39) F. Furrer, Phys. Rev. A **90**, 042325 (2014).