Spherical reconciliation for a continuous-variable quantum key distribution*

Zhao Lu(卢钊)[1], Jian-Hong Shi(史建红)[1,2,†], and Feng-Guang Li(李风光)[1]

[1] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450004, *China*
[2] *Science and Technology on Information Assurance Laboratory, Beijing* 100072, *China*

(Received 6 August 2016; revised manuscript received 10 November 2016; published online 10 March 2017)

Information reconciliation is a significant step for a continuous-variable quantum key distribution (CV-QKD) system. We propose a reconciliation method that allows two authorized parties to extract a consistent and secure binary key in a CV-QKD protocol, which is based on Gaussian-modulated coherent states and homodyne detection. This method named spherical reconciliation is based on spherical quantization and non-binary low-density parity-check (LDPC) codes. With the suitable signal-to-noise ratio (SNR) and code rate of non-binary LDPC codes, spherical reconciliation algorithm has a high efficiency and can extend the transmission distance of CV-QKD.

Keywords: continuous-variable quantum key distribution, quantization, spherical reconciliation

PACS: 03.67.Dd, 03.67.Hk, 84.40.Ua **DOI:** 10.1088/1674-1056/26/4/040304

1. Introduction

Quantum key distribution (QKD)[1,2] allows two authorized parties (Alice and Bob) to obtain raw keys after quantum signal generation, transmission and detection Since BB84 protocol[1] was proposed in 1984, quantum key distribution (QKD) has been greatly developed[3–11] and can be used in data encryption.[12–14] Because of imperfection of experimental equipment, disturbance of external environment and eavesdropping from attacker Eve, some errors appear in raw keys and part of raw keys are revealed to Eve. To avoid these disadvantages, classical post-processing,[15–17] such as authentication information reconciliation and privacy amplification, must be used to generate errorless secure key.

According to the difference in transmitted quantum state, QKD protocols are divided into discrete-variable (DV) QKD protocol and CV-QKD protocol. In DV- QKD protocol,[1] the transmitted information is encoded with discrete variables[18] and the raw keys are binary bit strings. So the information reconciliation for DV-QKD protocol is an error correction step principally. In CV-QKD protocol,[2,19] the transmitted information is encoded with continuous variables and the raw keys are values of continuous variables. In this paper, we focus on information reconciliation of CV-QKD[20] by using Gaussian-modulated coherent states and homodyne detection.

CV-QKD is expected to achieve higher secret key rates than DV-QKD due to the possibility of encoding more than 1 bit per pulse, while the difficult point of CV-QKD lies in information reconciliation. Up to now, there have been mainly two information reconciliation methods for CV-QKD: slice reconciliation[21,22] and multidimensional reconciliation.[23] Slice reconciliation method consists of slice quantization step and error correction step. This method encodes a Gaussian variable (symbol) into several bits and is applied to the SNR range 0.5–15.[11] Multidimensional reconciliation method consists of transformation and error correction. This method encodes a symbol into only one bit and is used for SNRs below 0.5. Because slice reconciliation can quantify a continuous variable into several bits, the complexity of slice reconciliation is higher than that of multidimensional reconciliation. The reverse reconciliation,[24] which was proposed in 2003, can reach longer transmission distance (with more than 3-dB losses) than the direct reconciliation.[19] The efficiency and complexity of information reconciliation method are significant for the performance of CV-QKD system.

In this paper, we propose a new information reconciliation method named spherical reconciliation, which is based on spherical quantization and non-binary LDPC codes. In spherical reconciliation, firstly Alice or Bob's symbols are transformed into the points on the unit sphere completely. Then the points on the unit sphere are quantified into discrete variables with quantization function. Later part bits of discrete variables are discarded to reduce the bit error rate. Finally non-binary LDPC codes[25] are used to encode and decode remaining discrete variables and symbols, and Alice and Bob obtain consistent and secure binary keys.[26] Compared with slice reconciliation, the spherical reconciliation encodes more than 1 bit per pulse, in addition, spherical quantization can reduce leaked information. The performance of information reconciliation is influenced by quantization method, error correction method and corresponding signal-to-noise ratio (SNR) ranges. Reverse reconciliation is used in the following discussion. The simulation result indicates that spherical recon-

*Project supported by the National Natural Science Foundation of China (Grant Nos. U1304613 and 11204379).
†Corresponding author. E-mail: shijianhong2011@163.com
© 2017 Chinese Physical Society and IOP Publishing Ltd

ciliation can achieve a high efficiency nearly 97%, and obviously extend the transmission distance of CV-QKD systems to 80 km with a group of suitable parameters.

The rest of the paper is organized as follows. In Section 2, the spherical quantization theory is presented. In Section 3, the details of spherical reconciliation are described. In Section 4, the performances of two-dimensional spherical (2DS) reconciliation are analyzed.

2. Information theory and spherical quantization

The first step of spherical reconciliation is to perform the spherical quantization. Spherical quantization is based on the unit sphere S^{n-1} of $\mathbb{R}^n$, and all the symbols belong to reconciliation range and are quantified reasonably. Gaussian variables are mapped to uniform variables on the unit sphere, then the uniform variables are quantified into discrete variables. Quantization method determines the suitable SNR range of reconciliation method, and quantization efficiency influences the reconciliation efficiency.

2.1. Information theory of Gaussian variables

After the quantum process of CV-QKD, Alice owns a symbol $X \sim N(0,\sigma_X^2)$, Bob obtains a corresponding symbol $Y \sim N(0,\sigma_Y^2)$ and the noise random variable obeys Gaussian distribution with $N \sim N(0,\sigma_N^2)$. According to the characteristics of Gaussian channel, the SNR is defined as σ_X^2/σ_N^2. The relationships among X, Y, and N is determined by $\sigma_Y^2 = \sigma_X^2+\sigma_N^2$, $Y = X+N$.

The mutual information between Alice and Bob is defined as

$$I(X;Y) = h(Y) - h(Y|X) = h(Y) - h(N), \tag{1}$$

where $h(Z)$ is the differential entropy with $h(Z) = -\int p(z)\log_2 p(z)\mathrm{d}z$, Z is a continuous random variable with probability density function $p(z)$, $h(Y|X)$ is the differential conditional entropy of symbol Y for a given symbol X, and $h(Y) = \log_2\sqrt{2\pi\mathrm{e}\sigma_Y^2}$ and $h(N) = \log_2\sqrt{2\pi\mathrm{e}\sigma_N^2}$ are the differential entropies of symbols Y and N respectively. Hence the mutual information between Alice and Bob is also denoted as

$$\begin{aligned} I(X;Y) &= \log_2\sqrt{2\pi\mathrm{e}\sigma_Y^2} - \log_2\sqrt{2\pi\mathrm{e}\sigma_N^2} \\ &= \frac{1}{2}\log_2\left(1+\frac{\sigma_X^2}{\sigma_N^2}\right) \\ &= \frac{1}{2}\log_2(1+\mathrm{SNR}). \end{aligned} \tag{2}$$

2.2. Spherical quantization method

Quantization is a process in which the symbols are mapped into binary bits. In spherical quantization, Bob's symbols should be mapped into the points on the unit sphere S^{n-1}. Alice builds n-dimensional vector $\boldsymbol{X}^n = (X_1, X_2, \ldots, X_n)$ with her symbols X_i sequentially, with the same method Bob builds n-dimensional vector $\boldsymbol{Y}^n = (Y_1, Y_2, \ldots, Y_n)$. Hence the normalized vector $\boldsymbol{y}^n = \boldsymbol{Y}^n/|\boldsymbol{Y}^n|$ obeys uniform distribution on S^{n-1} with $|\boldsymbol{Y}^n| = \sqrt{Y_1^2+Y_2^2+\cdots+Y_n^2}$.

Assuming that Bob quantifies the normalized vector $\boldsymbol{y}^n$ to r bits, so there should be 2^r quantization ranges. Bob divides the unit sphere S^{n-1} into 2^r ranges $I_0, I_1, \ldots, I_{2^r-1}$ equally, and the probability of normalized vector falling in each quantization range $I_k, (k \in \{0,1,\ldots,2^r-1\})$ is

$$p(\boldsymbol{y}^n \in I_k) = \frac{1}{2^r}. \tag{3}$$

Each quantization range corresponds to one binary bit string. The normalized vector $\boldsymbol{y}^n$ will be quantified into this binary bit string if $\boldsymbol{y}^n$ belongs to the corresponding quantization range. The quantization function Q is defined as

$$Q(\boldsymbol{y}^n) = l_k \quad \text{if} \quad \boldsymbol{y}^n \in I_k. \tag{4}$$

Here, $k = \sum_{i=0}^{r-1} t_i 2^i$. $l_k = t_{r-1}\cdots t_1 t_0$ $(t_i \in \{0,1\})$ is the binary bit string of corresponding quantization range I_k. The quantization efficiency is denoted as

$$\beta_Q = \frac{I(\boldsymbol{X}^n; Q(\boldsymbol{y}^n))}{n \times I(X;Y)}. \tag{5}$$

Based on the elements of information theory, the mutual information between $\boldsymbol{X}^n$ and $Q(\boldsymbol{y}^n)$ is

$$I(\boldsymbol{X}^n; Q(\boldsymbol{y}^n)) = h(Q(\boldsymbol{y}^n)) - h(Q(\boldsymbol{y}^n)|\boldsymbol{X}^n). \tag{6}$$

The entropy of $Q(\boldsymbol{y}^n)$ is $h(Q(\boldsymbol{y}^n)) = -2^r \times p(Q(\boldsymbol{y}^n) = l_k)\log_2 p(Q(\boldsymbol{y}^n) = l_k)$ with $p(Q(\boldsymbol{y}^n) = l_k) = p(\boldsymbol{y}^n \in I_k)$. The differential conditional entropy $h(Q(\boldsymbol{y}^n)|\boldsymbol{X}^n)$ is defined as

$$\begin{aligned} &h(Q(\boldsymbol{y}^n)|\boldsymbol{X}^n) \\ &= \sum_{k=0}^{2^r-1} -p(Q(\boldsymbol{y}^n) = l_k|\boldsymbol{X}^n)\log_2 p(Q(\boldsymbol{y}^n) = l_k|\boldsymbol{X}^n), \end{aligned} \tag{7}$$

and the probability $Q(\boldsymbol{y}^n) = l_k$ is conditioned on the fact that Alice measures $x_1, x_2, \ldots, x_n$ and obtains

$$\begin{aligned} &p(Q(\boldsymbol{y}^n) = l_k|\boldsymbol{X}^n) \\ &= p(\boldsymbol{y}^n \in I_k | X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n) \\ &= \int_{I_k} p(\boldsymbol{y}^n | X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n)\mathrm{d}\boldsymbol{y}^n. \end{aligned} \tag{8}$$

Spherical quantization is different from symbol quantization of Slice reconciliation. An imperfection of slice quantization is that a few symbols are out of the quantization intervals and assigned to the corresponding adjacent intervals. This way changes quantization efficiency and reconciliation efficiency necessarily. While in spherical quantization, all the symbols are mapped into the points on the unit sphere, which satisfies all the symbols in the corresponding quantization ranges.

When the number of dimension is 2 or 3, the unit spheres can be divided equally through angle division or gridding division. A necessary problem is that it is difficult to divide the unit sphere S^{n-1} equally when the dimension n is larger than 3. Hence Bob should do this job in advance. In Section 4 spherical reconciliation will be simulated when the dimension is 2.

3. Details of spherical reconciliation

Spherical reconciliation contains spherical quantization, bits sifting and error correction. We have introduced the spherical quantization method in Section 2. Non-binary LDPC codes are used to correct errors constantly with high decoding efficiency.[27,28] After quantifying the symbols, bits sifting step and error correction step will be allowed to proceed.

3.1. Bits sifting

Bob's symbols $Y_1, Y_2, \ldots, Y_n$ were quantified into a binary bit string $l_k = t_{r-1}\cdots t_1 t_0$ in the spherical quantization step. Because of the structure characteristics of quantization function, part bits of l_k are strongly correlated with Alice's measured values $x_1, x_2, \ldots, x_n$, and the remaining bits of l_k are weakly correlated with Alice's measured values $x_1, x_2, \ldots, x_n$. Hence the bits in binary bit string l_k consist of strongly correlated bits and weakly correlated bits.[29] The weakly correlated bits distribute at the end of bit string with high probability. Hence the bit string l_k can be divided into two parts, i.e., the strongly correlated bit string $l_{\mathrm{a}} = t_{r-1}\cdots t_{q+1}t_q$ and the weakly correlated bit string $l_{\mathrm{b}} = t_{q-1}\cdots t_1 t_0$ with $q \in (0, r-1)$.

The bit string l_{b} contains weakly correlated bits so that it will be send to Alice entirely.[21] The remaining bit string l_{a} is used to correct error and generate secure keys. The parameter q influences the reconciliation efficiency immediately. If parameter q is too large, part of serviceable bits will be disclosed. If parameter q is too small, some extra errors will appear in l_{a}. The value of parameter q is determined by actual conditions, such as the length of l_k. In bits sifting step q bit information is discarded.

3.2. Error correction with non-binary LDPC codes

The purpose of error correction is that Alice and Bob share the same keys with high probability. They process the error correction via non-binary LDPC codes over Galois fields GF(2^s) with $(1 \le s \le 16)$, which are based on belief propagation (BP) decoding algorithm. Code rate of non-binary LDPC codes, R_{LDPC} is a parameter to influence decoding efficiency and reconciliation efficiency. The wasting information in error correction step is $(r-q)\times(1-R_{\mathrm{LDPC}})$.

At first, Bob generates a parity-check matrix $\boldsymbol{H}$ with a suitable size. Then Bob computes the syndrome $l_{\mathrm{a}}\boldsymbol{H}^{\mathrm{T}}$ and sends it to Alice via a noiseless channel. Later, Alice decodes her symbols by the sum-product algorithm,[29] which is based on BP decoding algorithm. The computational complexity is $O(s2^s)$ when a symbol is decoded. Finally, Alice obtains the bit string l_{a} with high probability $p_{\mathrm{succeed}} = 1 - p_{\mathrm{fail}}$, where p_{fail} is the probability that the error correction fails to decode and it is determined by the frame error rate of LDPC codes.

The total efficiency of bits sifting and error correction is given by

$$\begin{aligned}\beta_{\mathrm{SE}} &= \frac{h(Q(\boldsymbol{y}^n)) - q - (r-q)\times(1-R_{\mathrm{LDPC}})}{I(\boldsymbol{X}^n; Q(\boldsymbol{y}^n))} \\ &= \frac{h(Q(\boldsymbol{y}^n)) - r + (r-q)\times R_{\mathrm{LDPC}}}{I(\boldsymbol{X}^n; Q(\boldsymbol{y}^n))}.\end{aligned} \tag{9}$$

3.3. Reconciliation efficiency

Details of spherical reconciliation are finished, and the structure is shown in Fig. 1. The reconciliation efficiency can be defined as

$$\beta = \beta_Q \beta_{\mathrm{SE}}. \tag{10}$$

From formulas (5), (9), and (10), the efficiency of spherical reconciliation is given by

$$\beta = \frac{h(Q(\boldsymbol{y}^n)) - r + (r-q)\times R_{\mathrm{LDPC}}}{n \times I(X;Y)}. \tag{11}$$

From formula (11), SNR and code rate of non-binary LDPC codes are two important parameters, which can determine the reconciliation efficiency. By adjusting the SNR and code rate of non-binary LDPC codes, the optimal reconciliation efficiency can be obtained. Alice and Bob need transmit information twice in spherical reconciliation. One is that Bob sends weakly correlated bit string l_{b} to Alice (l_{b} is not used to generate keys), and the other is that Bob sends $l_{\mathrm{a}}\boldsymbol{H}^{\mathrm{T}}$ to Alice to be decoded.

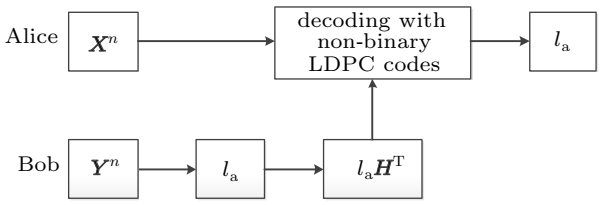


Fig. 1. Structure of spherical reconciliation.

4. Simulation analysis

We analyze the spherical reconciliation with a CV-QKD protocol based on Gaussian-modulated coherent states,[20] homodyne detection and reverse reconciliation. We simulate the performance of 2DS reconciliation now.

Alice and Bob build their respective two-dimensional vectors $\boldsymbol{X}^2 = (X_1, X_2)$ and $\boldsymbol{Y}^2 = (Y_1, Y_2)$. Bob normalizes $\boldsymbol{Y}^2$ and obtains $\boldsymbol{y}^2 = \boldsymbol{Y}^2/\sqrt{Y_1^2 + Y_2^2}$. According to different conditions, Bob quantifies the normalized value $\boldsymbol{y}^2$ into a bit string l_k with r bit length, and discards a bit string with q bits length. Considering the SNR of the transmission, Bob chooses a suitable non-binary LDPC codes and sends $l_a \boldsymbol{H}^{\mathrm{T}}$ to Alice to be decoded. Efficiency of spherical reconciliation is influenced by the performance of non-binary LDPC codes, especially code rate and corresponding frame error rate. Success rate of spherical reconciliation is determined by the frame error rate of LDPC codes. According to the performance of non-binary LDPC codes,[29] figure 2 shows the efficiency of 2DS reconciliation method. In the remaining part of simulation Bob chooses non-binary LDPC codes over GF(2^5) for frame length $n_1 = 10^3$ with code rate $R_{\mathrm{LDPC}} = 0.5$.

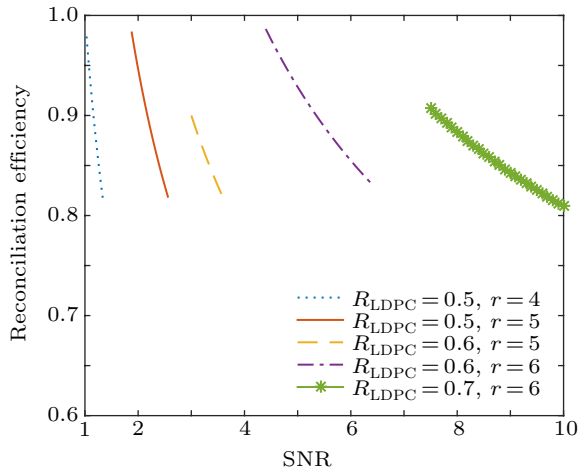


Fig. 2. (color online) Efficiencies of 2DS reconciliation method with different code rates of non-binary LDPC codes and length of quantified bit strings. The non-binary LDPC codes are over GF(2^5) for frame length $n_1 = 10^3$.

When the normalized value $\boldsymbol{y}^2$ is quantified into 5 bits, the number of quantization intervals is 32. As figure 3 shows, Bob divides the two-dimensional sphere into 32 ranges, i.e., $I_0, I_1, \ldots, I_{31}$. According to quantization function (4), Bob can compute the corresponding quantified value l_k. Its quantization efficiency can be calculated by formulas (5)–(8), and figure 4 shows the efficiency of 2DS quantization and efficiency of slice quantization with optimal intervals.[22] For 2DS quantization, $\boldsymbol{y}^2$ is quantified into 5 bits, which is similar to the case that a symbol is quantified into 2.5 bits. Compared with slice quantization, the efficiency of 2DS quantization is higher when slice quantization quantifies a symbol into 4 bits.

For the infinite-size condition, the secret key rate proven secure against individual attack is given by[23]

$$\Delta I_{\mathrm{infinite}} = (\beta I(X;Y) - I(Y;E))(1 - p_{\mathrm{fail}}), \qquad (12)$$

where β is the reconciliation efficiency, $I(X;Y)$ denotes the Shannon mutual information between Alice and Bob, $I(Y;E)$ is the mutual information between Bob and Eve, p_{fail} is the probability that error correction fails to be decoded.

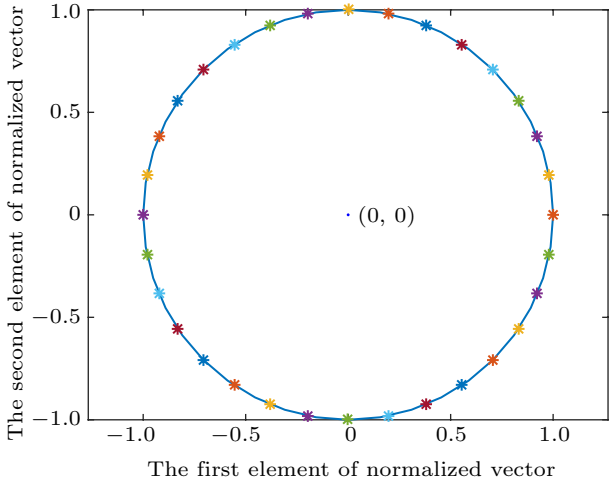


Fig. 3. (color online) When $r = 5$, the unit circle is divided into 32 ranges by the points, and the 32 ranges correspond to quantization intervals. The normalized random vector $\boldsymbol{y}^2$ has a uniform distribution on the unit circle.

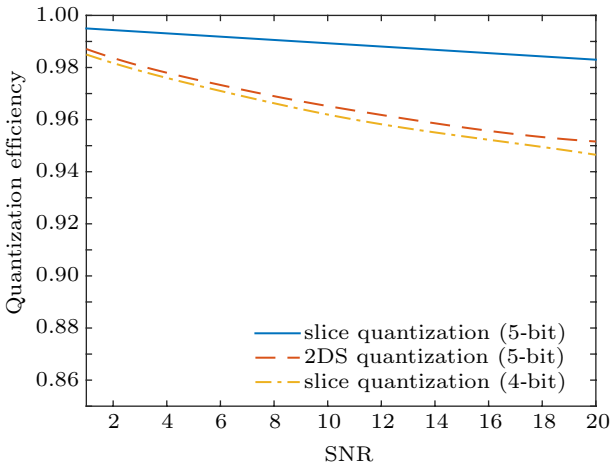


Fig. 4. (color online) Efficiencies of 2DS quantization and slice quantization with optimal intervals.

As figure 5 shows, when $r = 5$ and $q = 2$, 2DS reconciliation is optimal for an SNR of about 2, this new reconciliation method can extend the transmission distance of CV-QKD protocols to over 60 km when the SNR is 1.92. Figure 6 shows that the suitable SNR range varies with the length of quantified bit string l_k. For different lengths of quantified bit strings $r = 4$, $r = 5$, $r = 6$ and the suitable SNRs, reconciliation efficiency can reach 97%. Especially, the transmission distance of CV-QKD protocols is over 70 km when $r = 4$.

To compare spherical reconciliation with slice reconciliation in the same SNR case, we assume that the SNR is 3.25 and Bob quantifies a symbol into 4 bits, for slice reconciliation Bob should discard 2 bits, the efficiency is 90%.[30] In order to embody fairness, for 2DS reconciliation Bob quantifies $\boldsymbol{y}^2$ into 8 bits and discards 4 bits, which is equivalent to Bob's quantifying a symbol into 4 bits and discards 2 bits. As

figure 7 shows, under the same conditions the performance of 2DS reconciliation is superior.

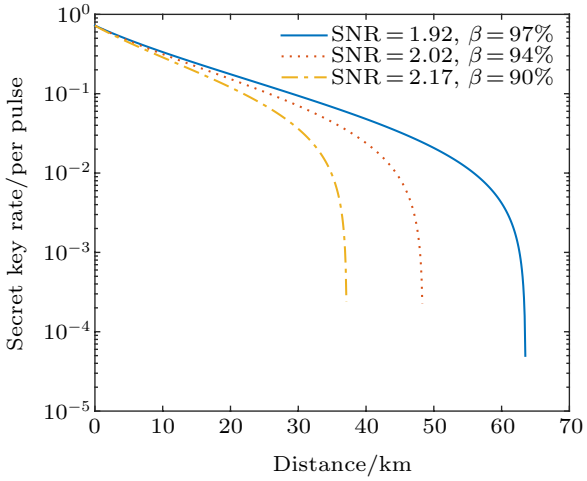


Fig. 5. (color online) Performances of 2DS reconciliation with different SNRs when $r = 5$, $q = 2$ and experimental parameters:[31] $\alpha = 0.2$ dB/km, $\eta = 0.6$, $\varepsilon = 0.01$, and $v_{\text{el}} = 0.01$.

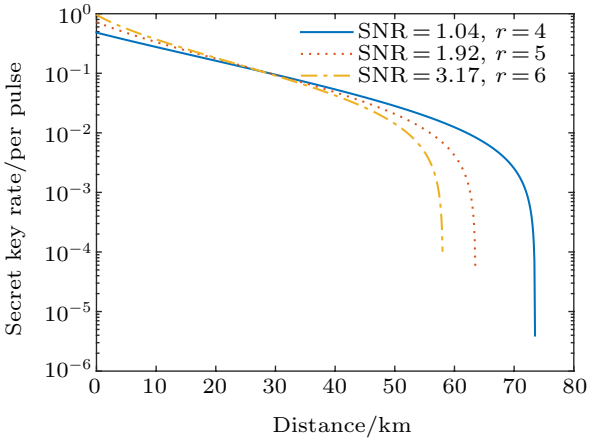


Fig. 6. (color online) Performances of 2DS reconciliation with different SNRs when $r = 4$, $r = 5$, $r = 6$ and $q = 2$. The reconciliation efficiencies in three cases are all 97%. The experimental parameters are as follows:[31] $\alpha = 0.2$ dB/km, $\eta = 0.6$, $\varepsilon = 0.01$, and $v_{\text{el}} = 0.01$.

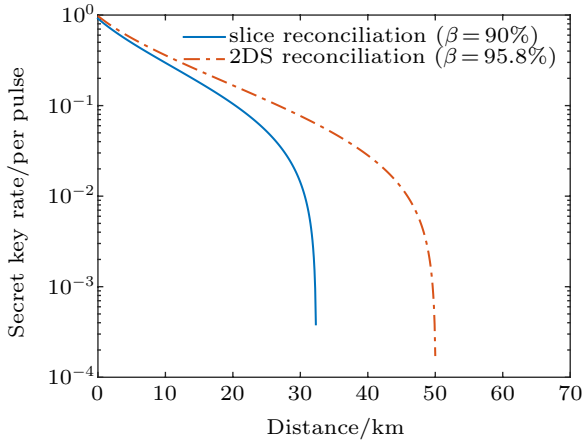


Fig. 7. (color online) Performances of 2DS reconciliation with $r = 8$, $q = 4$, and experimental parameters:[30] $\alpha = 0.2$ dB/km, $\eta = 0.606$, $\varepsilon = 0.005$, and $v_{\text{el}} = 0.041$.

For the finite-size condition, the secret key rate proven secure against collective attack is given by[32]

$$\Delta I_{\text{finite}} = \frac{KN_2}{N_1}[\beta I(X;Y) - \chi(Y;E) - \Delta(N_2)], \qquad (13)$$

where $I(X;Y)$ is the Shannon mutual information between Alice and Bob, $\chi(Y;E)$ is the Holevo bound on the information between Bob and Eve, and $\Delta(N_2)$ is related to the security of the privacy amplification.[33] The involved parameters are the repetition rate of CV-QKD system K, the number of the total signal pulses N_1, the number of the signals pulses for key generation N_2, and the reconciliation efficiency β.

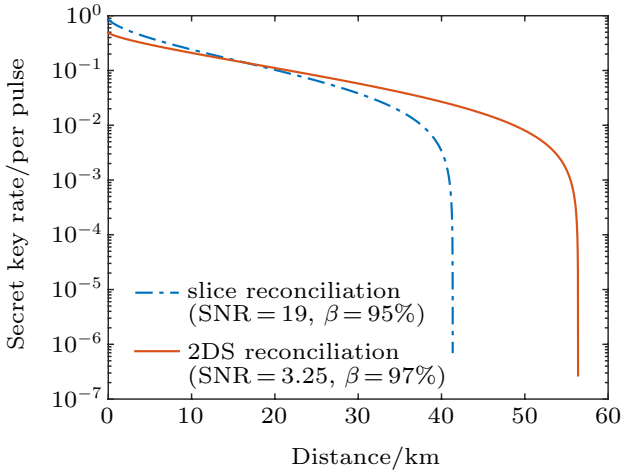


Fig. 8. (color online) Performances of 2DS reconciliation with $r = 8$, $q = 4$, and the experimental parameters:[11] $\alpha = 0.2$ dB/km, $\eta = 0.85$, $\varepsilon = 0.0015$, and $v_{\text{el}} = 0.001$.

Figure 8 shows the comparison of the performance between 2DS reconciliation method and slice reconciliation method[11] in the finite-size case with the corresponding SNR values being 3.25 and 19; the 2DS reconciliation method can extend the transmission distance to over 55 km when the SNR is 3.25 in the same CV-QKD system. As figure 9 shows, the performance of the spherical reconciliation is still better than that of multidimensional reconciliation when the size is finite. The distance of this CV-QKD system can be extend to 80 km when the modulation variance $V_{\text{A}} = 5.7$.

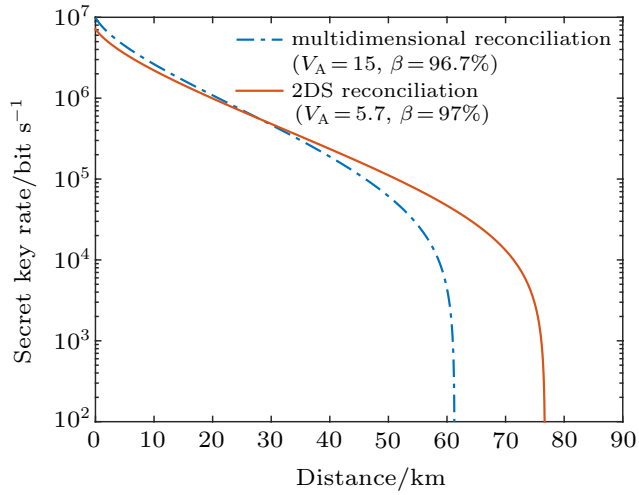


Fig. 9. (color online) Performances of 2DS reconciliation when $r = 4$, $q = 2$, and experimental parameters:[32] $\alpha = 0.2$ dB/km, $\eta = 0.6$, $\varepsilon = 0.07$, $v_{\text{el}} = 0.05$, $K = 25$ MHz, $N_1 = 10^9$, and $N_2/N_1 = 0.5$.

5. Conclusions

Information reconciliation is an indispensable part for CV-QKD system. In this paper we propose a new information reconciliation method named spherical reconciliation. Because of using no post-selection,[34,35] the spherical reconciliation can be proven secure against general attacks. Spherical quantization method is a high-efficiency quantization method. The performance of spherical reconciliation is restricted by the compatibility and performance of non-binary LDPC codes. We analyze the performance of 2DS reconciliation method, which has high efficiency and can extend the transmission distance of infinite-size and finite-size CV-QKD protocols. It is valuable to discuss spherical reconciliation in the case of high dimensions.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing,* December 10–12, 1984, New York, USA, p. 175

[2] Ralph T C 1999 *Phys. Rev. A* **61** 103031

[3] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595

[4] Gu Y B, Bao W S, Wang Y and Zhou C 2016 *Chin. Phys. Lett.* **33** 040301

[5] Li J, Chen Y H, Pan Z S, Sun F Q, Li N and Li L L 2016 *Acta Phys. Sin.* **65** 030302 (in Chinese)

[6] Yin Z Q, An X B and Han Z F 2015 *Acta Phys. Sin.* **64** 140303 (in Chinese)

[7] Chen H, An X B, Wu J, Yin Z Q, Wang S, Chen W and Han Z F 2016 *Chin. Phys. B* **25** 020305

[8] Li Y, Bao W S, Li H W, Zhou C and Wang Y 2016 *Chin. Phys. B* **25** 010305

[9] Wang L, Zhao S M, Gong L Y and Cheng W W 2015 *Chin. Phys. B* **24** 120307

[10] Li Y, Bao W S, Li H W, Zhou C and Wang Y 2015 *Chin. Phys. B* **24** 110307

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

[12] Xia Z H, Wang X H, Sun X M and Wang Q 2015 *IEEE Transactions on Parallel and Distributed Systems* **27** 340

[13] Fu Z J, Sun X M, Liu Q, Zhou L and Shu J G 2015 *IEICE Transactions on Communications* **98** 190

[14] Fu Z J, Wu X L, Guan C W, Sun X M and Ren K 2016 *IEEE Transactions on Information Forensics and Security* **11** 2706

[15] Elkouss D, Martinez-Mateo J and Martin V 2011 *Quantum Inform. Comput.* **11** 226

[16] Du P Y, Bai Z L, Wang X Y and Li Y M 2013 *Acta Sin. Quantum Opt.* **19** 129

[17] Li Y, Liao S K, Liang F T, Shen Q, Liang H and Peng C Z 2016 *Chin. Phys. Lett.* **33** 30303

[18] Buttler W T, Torgerson J R and Lamoreaux S K 2002 *Phys. Lett. A* **299** 38

[19] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

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

[21] Van Assche G, Cardinal J and Cerf N J 2004 *IEEE Transactions on Information Theory* **50** 394

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

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

[24] Grosshans F and Grangier P 2002 *Physics* **3** 4

[25] Davey M C, Mackay D 1998 *IEEE Commun. Lett.* **2** 70

[26] Ankan E, Ul Hassan N, Lentmaier M and Montorsi G 2015 *Journal of Communications and Networks* **17** 328

[27] Voicila A, Declercq D, Verdier F Fossorier M and Urard P 2010 *IEEE Trans. Commun.* **58** 1365

[28] Sayir J 2014 *Non-binary "LDPC decoding using truncated messages in the Walsh-Hadamard domain". International Symposium on Information Theory and ITS Applications, IEEE*, p. 16–20

[29] Pacher C, Martinez-Mateo J, Duhme J, Gehring T and Furrer F 2016 arXiv: 1602.09140v1 [quant-ph]

[30] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov, E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin W and Grangier P 2007 *Phys. Rev. A* **76** 042305

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

[32] Wang C, Huang D, Huang P, Lin D K, Peng J Y and Zeng G H 2015 *Sci. Rep.* **5** 14607

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

[34] Silberhorn C, Ralph T C, Lütkenhaus N and Leuche G 2002 *Phys. Rev. Lett.* **89** 167901

[35] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502