ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation

Yingming Zhou(周颖明), Xue-Qin Jiang(蒋学芹), Weiqi Liu(刘维琪), Tao Wang(王涛), Peng Huang(黄鹏), Guihua Zeng(曾贵华)
Citation: Chin. Phys. B . 2018, 27(5): 050301. **doi:** 10.1088/1674-1056/27/5/050301

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Entangled-photons generation with quantum dots

Yuan Li(李远), Fei Ding(丁飞), Oliver G Schmidt
Chin. Phys. B . 2018, 27(2): 020307. **doi:** 10.1088/1674-1056/27/2/020307

Improving continuous-variable quantum key distribution under local oscillator intensity attack using entanglement in the middle

Fang-Li Yang(杨芳丽), Ying Guo(郭迎), Jin-Jing Shi(石金晶), Huan-Li Wang(王焕礼), Jin-Jin Pan(潘矜矜)
Chin. Phys. B . 2017, 26(10): 100303. **doi:** 10.1088/1674-1056/26/10/100303

Spherical reconciliation for a continuous-variable quantum key distribution

Zhao Lu(卢钊), Jian-Hong Shi(史建红), Feng-Guang Li(李风光)
Chin. Phys. B . 2017, 26(4): 040304. **doi:** 10.1088/1674-1056/26/4/040304

Quantum hacking of two-way continuous-variable quantum key distribution using Trojan-horse attack

Hong-Xin Ma(马鸿鑫), Wan-Su Bao(鲍皖苏), Hong-Wei Li(李宏伟), Chun Chou(周淳)
Chin. Phys. B . 2016, 25(8): 080309. **doi:** 10.1088/1674-1056/25/8/080309

Rise of quantum correlations in non-Markovian environments in continuous-variable systems

Liu Xin, Wu Wei
Chin. Phys. B . 2014, 23(7): 070303. **doi:** 10.1088/1674-1056/23/7/070303

Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation*

Yingming Zhou(周颖明)[1], Xue-Qin Jiang(蒋学芹)[3], Weiqi Liu(刘维琪)[2], Tao Wang(王涛)[1], Peng Huang(黄鹏)[1,†], and Guihua Zeng(曾贵华)[1,3,‡]

[1] *State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Laboratory on Navigation and Location-based Service, and Center of Quantum Information Sensing and Processing (QSIP), Shanghai Jiao Tong University, Shanghai* 200240, *China*

[2] *College of Information Science and Technology, Northwest University, Xi'an* 710127, *China*

[3] *School of Information Science and Technology, Donghua University, Shanghai* 201620, *China*

(Received 15 January 2018; revised manuscript received 10 February 2018; published online 26 April 2018)

The well-known multi-dimensional reconciliation is an effective method used in the continuous-variable quantum key distribution in the long-distance and the low signal-to-noise-ratio scenarios. The virtual channel employed to exchange data is generally established by using a finite-dimensional rotation in the reconciliation procedure. In this paper, we found that the finite dimension of the multi-dimensional reconciliation inevitably leads to the mismatch of the signal-to-noise-ratio between the quantum channel and the virtual channel, which may be called the finite-dimension effect. Such an effect results in an overestimation on the secret key rate, and subsequently induces vital practical security loopholes.

Keywords: multi-dimensional reconciliation, finite-dimensional effect, continuous-variable, quantum key distribution

PACS: 03.67.Hk, 03.67.–a, 03.67.Dd **DOI:** 10.1088/1674-1056/27/5/050301

1. Introduction

Quantum key distribution is a vital practical application in quantum information science.[1,2] It enables two legitimate parties, which are always called Alice and Bob, to produce a shared random secure secret key via a quantum channel, even in the existence of an eavesdropper, generally called Eve, who possesses limitless ability. Its security is guaranteed by the quantum mechanics laws, e.g., the Heisenberg uncertainty principle and the quantum no-cloning theorem. Currently two implementation methods, i.e., the discrete variable quantum key distribution and the continuous variable quantum key distribution (CVQKD), are often referenced. The CVQKD scheme usually encodes information on the position and momentum quadratures of quantum states.[3] It has the merits of a potentially high bit rate and compatibility with classical optical communication. In the past few years, the CVQKD have made a great number of achievements in both theories[3–5] and experiments.[6–8] One of the most notable achievements is that the Gaussian modulated coherent state (GMCS) scheme[6] has been proven to be secure against collective attacks[9–12] and coherent attacks.[13–16] Its practical securities with imperfection of the deployed devices in the CVQKD system have also been investigated.[17–24] In order to defend against practical attacks, real-time monitoring technologies are extensively adopted to prevent both attacks and signal disturbance.[25–28] Recently, field tests based on the GMCS scheme in telecommunication optical networks have been successfully implemented by several groups.[29–31]

A standard CVQKD system commonly consists of three phases, i.e., the quantum communication, the reconciliation, and the privacy amplification. In the quantum communication phase, Alice sends a string of X through a quantum channel. After performing a measurement of quadrature states by using a balanced homodyne detector, Bob obtains a string of Y which is correlated to X. Then, Alice and Bob obtain a string called the raw key. After that, with the purpose of checking the existence of Eve, the parameter estimation is indispensable and it determines whether they should abort or reserve the subset of remaining strings. In the reconciliation step, Alice and Bob achieve the same fix-length secret key strings by correcting errors between the secret key strings obtained by Alice and Bob. After the reconciliation step, Alice and Bob extract the secure secret key with a privacy amplification algorithm.

As is well-known, the reconciliation efficiency and speed are directly related to the transmission distance and the secret key rate of the involved CVQKD system. Generally, a high reconciliation efficiency improves the secure transmission distance and the secret key rate, while a high reconciliation speed is necessary to realize the high bit-rate CVQKD. Currently, the reconciliation has become a main bottleneck for the CVQKD implementation in the high-rate and long-distance scenarios. By far, several typical reconciliation schemes have been pro-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61332019, 61671287, and 61631014) and the National Key Research and Development Program of China (Grant No. 2016YFA0302600).

†Corresponding author. E-mail: huang.peng@sjtu.edu.cn

‡Corresponding author. E-mail: ghzeng@sjtu.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd

posed. The proposed slice reconciliation scheme[32] quantifies the continuous variables to several layers, and then decodes them with correct-codes such as LDPC codes or BCH codes to obtain the same bit strings at both Alice and Bob's sides. This scheme has low decoding complexity, but its reconciliation efficiency is low and needs to be improved in a practical application. Because the raw keys follow a Gaussian distribution, it is more difficult to distinguish the signal in the presence of noise. In light of such a case, the post-selection scheme[33–37] was proposed to remove the small values and keep the big ones. Unfortunately, its security against arbitrary general attacks has not yet been proved. A most useful scheme called multi-dimensional reconciliation[38] was put forward to validly enhance the reconciliation efficiency and transmission distance in case of low signal-to-noise (SNR). With the assistance of multi-edge LDPC codes, such kinds of schemes[39,40] have achieved transmission distances up to 150 km[41] and decoding speeds up to 25 Mb/s.[42]

We note that all of the available multi-dimensional reconciliation schemes are essentially finite dimensions,[40] which actually deviates from the theoretical requirements of the reconciliation procedure. This deviation results in the so-called finite-dimensional effect (FDE), i.e., giving rise to the SNR mismatch between the quantum channel and the introduced virtual channel, subsequently, inducing the practical security loopholes. In this paper, we investigate the FDE of the multi-dimensional reconciliation scheme and its influences on the practical security of the involved CVQKD system. Since the multi-dimensional reconciliation scheme has finite dimensions, we find that the virtual channel follows a student's t-distribution but not a Gaussian distribution, even if not the binary input additive white Gaussian noise channel (BI-AWGNC), which is an approximation of the Gaussian channel at low SNR situation. Particularly, we find that the FDE may lead to the SNR mismatch between the quantum channel and the virtual channel. Consequently, it results in overestimation on the secret key rate, and then introduces practical security issues.

This paper is organized as follows. In Section 2, the multi-dimensional reconciliation scheme is reviewed briefly, then the FDE of the multi-dimensional reconciliation is investigated in Section 3. The influence of the FDE on the CVQKD is explored in Section 4. In Section 5, we investigate the practical loopholes in the involved CVQKD system induced by the FDE. Finally, the conclusions are drawn in Section 6.

2. Review of multi-dimensional reconciliation scheme

Different from the previously practical security issues due to imperfections of devices deployed in the CVQKD system, the practical security loopholes studied in this work are induced by imperfections of the employed algorithm but not the devices. In other words, in this paper we focus on the imperfections of the multi-dimensional reconciliation scheme. For clarity, we review briefly the multi-dimensional reconciliation scheme in this section.

Generally, in the GMCS scheme, Alice's information is encoded with a bivariate Gaussian distribution in phase space, and then Alice sends the information to Bob via a quantum channel interfered by the eavesdropper and channel noise. After Bob's measurement with a balanced homodyne detector, Alice and Bob share N couples of correlated variables $\{(x_i, y_i)|i = 1, 2, \ldots, N\}$, i.e., the raw key data, where x_i is the quadrature modulated by Alice, and y_i is the quadrature measured by Bob. Here N is the total number of transmitted data, $N = m+n$. Then, m couples of variables are randomly selected to estimate the quantities that are required to compute the secret key rate, and the remaining n pairs of variables are used for the key establishment. In the wake of these steps, the data are exchanged through a public authenticated channel so that one may execute the reconciliation procedure which distills an identical binary bit string between two parties. Thus the virtual channel which is used to exchange data is built. The schematic of the CVQKD with multi-dimensional reconciliation scheme is shown in Fig. 1.

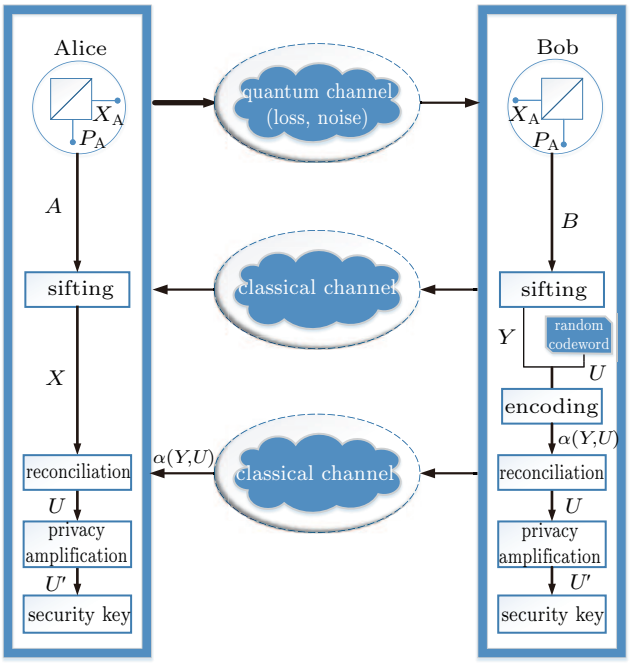


Fig. 1. (color online) Schematic of the CVQKD system based on the multi-dimensional reconciliation scheme with reverse reconciliation procedure.

The basic idea of the multi-dimensional reconciliation scheme is as follows. Firstly, map the non-uniform Gaussian-distributed variable space generated by the quantum communication into a uniform-distributed variable space. Then, ran-

domly choose a stochastic code words space whose prior probability meets a uniform distribution. After that, the chosen code words are transmitted over a public authenticated classical channel. In such a case, the two legitimated parties who share the key will not leak any side information about the code words so that Eve cannot obtain any extra key information. The multi-dimensional reconciliation scheme executes the following steps.

Step 1 Alice and Bob have to divide the obtained continuous variables into consecutive d-dimensional vectors in the multi-dimensional reconciliation scheme for the purposes of security. A common tactic is straightforward to assemble every d successive continuous variables into a d-dimensional vector. One may also recombine those elements after rearranging the continuous sequences such that $x=\{x_1,x_2,\ldots,x_d\}$, $y=\{y_1,y_2,\ldots,y_d\}$, and $n=d\times l$.

Step 2 Bob generates a uniform distribution random binary string S of length d (in the reverse reconciliation scheme) via a quantum random number generator. The total size $n=d\times l$ of the code S is bounded by the mutual information between Alice and Bob, i.e., $\log_2(n)\leq I(A;B)$. Then, Bob randomly chooses d-dimensional vector $u\in\left\{\frac{-1}{\sqrt{d}},\frac{1}{\sqrt{d}}\right\}^d$ according to the binary phase shift keying (BPSK) encoding, and sends the side information expressed by function f satisfying $f(y)=u$ and the generated syndrome to Alice. After that, Alice computes $f(x)=v$ with the function transmitted over a public authenticated classic channel.

Step 3 Alice receives the noisy version of u. In this way, the two parties, i.e., Alice and Bob, build a virtual channel with input u and output v. Afterwards, Alice tries to reconstruct u by utilizing the intensive sum-product belief propagation algorithm for decoding the LDPC code.[43,44] The virtual channel noise is eliminated and Alice shares the same key with Bob.

3. Finite-dimensional effect of multi-dimensional reconciliation

According to the multi-dimensional reconciliation scheme described in the above section, the function f rotates the quadrature measure y into binary codeword u. In practice, one may choose a function M so that $M(y,u)\cdot y=u$ for every word $y\sim N(0,1)^d$ sent by Bob and every codeword $u\in S^{d-1}$ in the regime of reverse reconciliation. Then, Bob sends $M=u\cdot y^{-1}$ to Alice through a public authenticated channel (the multiplication and division operators are defined in $M(y,u)\cdot y=u$ and $M=u\cdot y^{-1}$).[40] Assume the quantum communication procedure to be a standard linear model, the following relationship can be obtained:[11] $x=\ell y+z$ with $y\sim N(0,1)^d$ and $z\sim N(0,\sigma^2)^d$, where $\ell=\sqrt{\eta T}$, and η, T, z are the detection efficiency, the transmission efficiency, and the quantum channel noise term, respectively. In order to derive the virtual channel model with input u and output v more explicitly, we set $\ell=1$, i.e., without considering channel loss in the reverse reconciliation. Then, the noisy version of u is deduced as follows:

$$\begin{aligned} v &= M\cdot x \\ &= u\cdot y^{-1}(y+z) \\ &= u\cdot y\cdot y^{-1}+u\cdot y^{-1}\cdot z \\ &= u+u\cdot\frac{z}{y}. \end{aligned} \tag{1}$$

The multi-dimensional noise in the virtual channel is given by the term $u\cdot z/y$, such that $v=u+\varepsilon$ which is the rotated version of quantum channel noise. Due to the spherical symmetry and independence of the distribution on z and x, the noise of the virtual channel follows the distribution

$$u\cdot\frac{z}{y}\sim u\cdot\frac{z}{\|y\|}. \tag{2}$$

Hereto we have established a virtual channel and succeeded in reducing the reconciliation problem to a channel coding problem. In this way, one can graft the post-processing procedure of CVQKD on searching for a good code which has been developed maturely in the traditional communication system.

The noise of the virtual channel with input u and output v is given by

$$\epsilon = v-u=u\cdot\frac{z}{y}\sim u\cdot\frac{z}{\|y\|}. \tag{3}$$

According to the multi-dimensional reconciliation scheme, the continuous variable x and quantum noise z are decomposed into d-dimensional vectors, and u satisfies $u\in\left\{\frac{-1}{\sqrt{d}},\frac{1}{\sqrt{d}}\right\}^d$. So the noise ϵ_i $(i=1,2,\ldots,d)$, which is the element of vector ϵ, can be rewritten as

$$\begin{aligned} \epsilon_i &\propto \frac{\frac{1}{\sqrt{d}}(z_1\pm z_2\pm\cdots\pm z_d)}{\sqrt{y_1^2+y_2^2+\cdots+y_d^2}} \\ &= \frac{\frac{1}{d}(z_1\pm z_2\pm\cdots\pm z_d)-0}{\frac{\sqrt{y_1^2+y_2^2+\cdots+y_d^2}}{\sqrt{d}}}. \end{aligned} \tag{4}$$

Let $\bar{Z}=\frac{1}{d}(z_1\pm z_2\pm\cdots\pm z_d)$. Clearly, $\bar{Z}$ has zero mean and σ^2/d variance. Subsequently, $\bar{Z}-0/(\sigma/\sqrt{d})$ follows a normal distribution and $y_1^2+y_2^2+\cdots+y_d^2\sim\chi^2(d)$. Then, equation (4) may be expressed in a simplified form

$$\epsilon_i\propto\frac{\frac{\sigma}{\sqrt{d}}\left(\frac{\bar{Z}-0}{\frac{\sigma}{\sqrt{d}}}\right)}{\sqrt{\frac{y_1^2+y_2^2+\cdots+y_d^2}{d}}}. \tag{5}$$

In the probability theory,[45] the student's t-distribution is defined as follows. Let Q be a standard normal distribution, i.e., $Q\sim N(0,1)$, and P be a chi-squared distribution, i.e., $P\sim\chi^2(k)$. Meanwhile, Q and P are independent. Then let

$$t=\frac{Q}{\sqrt{P/k}}\sim t(k). \tag{6}$$

The t satisfies the student's t-distribution with k degrees of freedom. In terms of the above definition of the student's t-distribution, the distribution of noise over the virtual channel $\epsilon = (\epsilon_1, \epsilon_2, \cdots, \epsilon_d)$ can be expressed as follows:

$$\epsilon_i \sim \frac{\sigma}{\sqrt{d}} t(d). \tag{7}$$

That is, the noise of the virtual channel follows the student's t-distribution with d degrees of freedom. The noise ϵ has a zero mean and a noise variance of $\sigma^2/(d-2)$. Clearly, such a channel does not follow the Gaussian distribution.

Now we study the SNR of the virtual channel. According to the above calculation, the SNR of the virtual channel may be calculated by

$$S_{\mathrm{V}} = \frac{d-2}{d} \cdot \frac{1}{\sigma^2} = \frac{d-2}{d} S_{\mathrm{Q}}, \tag{8}$$

where $S_{\mathrm{Q}} = 1/\sigma^2$ is the SNR of the quantum channel (physical channel).

Apparently, the SNR of the virtual channel is associated with the reconciliation dimension d. The FDE of the multi-dimensional reconciliation will be eliminated when $d \to \infty$. Actually, since the norm of d-dimensional vector x follows the $\chi(d)$ distribution, when d approaches to infinity, $\chi(d)$ is approximately close to the Dirac distribution. In this way, the small absolute value coordinates benefit the final key extraction and become abundant. In addition, with the dimension d becoming larger, the virtual channel becomes closer to the BIAWGN channel, even the AWGN channel in the practical CVQKD system.

4. Influences of finite-dimensional effect on CVQKD system

In this section, we investigate the impacts of the FDE on the channel capacity, reconciliation efficiency, secure secret key rate, and secure transmission distance of the CVQKD system.

First, we consider the impacts of the FDE on the channel capacity. The capacity of the Gaussian channel, i.e., the AWGN channel, is given by

$$C_{\mathrm{A}} = \frac{1}{2} \log_2(1 + S_{\mathrm{G}}), \tag{9}$$

where S_{G} refers to the SNR which is equal to $1/\sigma^2$. However, this channel capacity cannot be reached since the multi-dimensional reconciliation scheme employs the BPSK encoding. Previously, the virtual channel is often regarded approximately as a BIAWGN channel, which uses a random variable $U \in \{-1, +1\}$ as its input and outputs a random variable $V = U + \epsilon$, where ϵ is a zero mean Gaussian random variable with variance σ^2. The capacity of BIAWGN is

$$C_{\mathrm{B}} = -\int_{-\infty}^{+\infty} \Phi(v, S_{\mathrm{B}}) \log_2(\Phi(v, S_{\mathrm{B}}))\, \mathrm{d}v - \frac{1}{2}\log_2(2\pi e) + \frac{1}{2}\log_2(S_{\mathrm{B}}), \tag{10}$$

where

$$\Phi(v, S_{\mathrm{B}}) = \sqrt{\frac{S_{\mathrm{B}}}{8\pi}} \left\{ \exp\left(-\frac{(v-1)^2 S_{\mathrm{B}}}{2}\right) + \exp\left(-\frac{(v+1)^2 S_{\mathrm{B}}}{2}\right) \right\}, \tag{11}$$

and S_{B} corresponds to the SNR of the BIAWGN channel.

Since the practical virtual channel actually follows the student's t-distribution, the capacity of the virtual channel is given by

$$C_{\mathrm{V}}^{d} = -\int_{-\infty}^{+\infty} \Phi(x, S_{\mathrm{V}}) \log_2(\Phi(x, S_{\mathrm{V}}))\, \mathrm{d}x + \log_2 \frac{\sqrt{d}}{\sigma} - H_d^t, \tag{12}$$

where

$$\Phi(x, S_{\mathrm{V}}) = \sqrt{\frac{S_{\mathrm{V}}}{8\pi}} \left\{ \exp\left(-\frac{(x-1)^2 S_{\mathrm{V}}}{2}\right) + \exp\left(-\frac{(x+1)^2 S_{\mathrm{V}}}{2}\right) \right\}, \tag{13}$$

S_{V} refers to the SNR of the virtual channel which is equal to $\frac{d-2}{d} \cdot \frac{1}{\sigma^2}$, and

$$H_d^t = \left(\frac{d+1}{2}\right)\left[\phi\left(\frac{d+1}{2}\right) - \phi\left(\frac{d}{2}\right)\right] + \log_2\left\{\sqrt{d} \cdot B\left[\frac{1}{2}, \frac{d}{2}\right]\right\}. \tag{14}$$

Here $\phi(\cdot)$ and $B(\cdot)$ are the Beta function and Digamma function, respectively. The Beta function is given by

$$B\left[\frac{1}{2}, \frac{d}{2}\right] = \frac{\sqrt{\pi}\Gamma(\frac{d}{2})}{\Gamma(\frac{d+1}{2})}, \tag{15}$$

and the Digamma function is expressed as

$$\phi(q) = \frac{\Gamma'(q)}{\Gamma(q)}. \tag{16}$$

In the multi-dimensional reconciliation scheme, the dimension is only restricted to $d = 1, 2, 4, 8$ according to the Hurwitz theorem of composition algebras,[38] or the dimension is restricted to $d = 16$.[40] Figure 2 demonstrates the influences of the FDE on the channel capacity when $d = 8$. As a comparison, we also plot the AWGN channel capacity and the BIAWGN channel capacity. As one may see from Fig. 2, the channel capacities of the Gaussian channel and BIAWGN channel are approximately equal in the low SNR situation. However when $d = 8$, the 8-dimensional channel capacity is much lower than that of the BIAWGN channel. Obviously, this deviation will influence inevitably the performance and practical security of the involved CVQKD system.

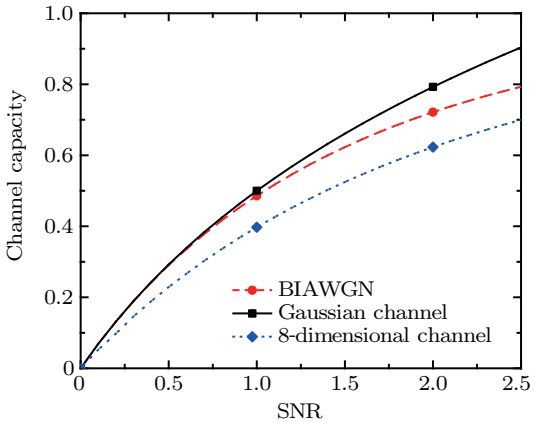


Fig. 2. (color online) Channel capacity with respect to the SNR. The red dash line represents the Gaussian channel capacity. The black solid line represents the BIAWGN channel capacity. The blue dotted line represents the octonian channel capacity. The octonian channel capacity is lower than the Gaussian channel capacity in the low SNR scenario.

Now we investigate the impacts of the FDE on the reconciliation efficiency. Generally, the reconciliation efficiency β is defined as

$$\beta(s) = \frac{R}{C(S)}, \tag{17}$$

where R is the code rate used for the reconciliation procedure, and $C(S)$ is the channel capacity when S corresponds to the SNR. Consider the impacts of the FDE, based on Eqs. (10), (12), and (17), the reconciliation efficiency $\tilde{\beta}$ in the virtual channel is given by

$$\tilde{\beta}_d = \frac{C_{\mathrm{B}}}{C_{\mathrm{V}}^d}\beta, \tag{18}$$

where β in Eq. (18) represents the reconciliation efficiency of the CVQKD system over the BIAWGN channel. The $S_{\mathrm{DE}}^{\mathrm{BIAWGN}}$ which enters to the C_{B} is the SNR threshold on the BIWAGN channel for the LDPC codes (size 2^{20}) predicted by the density evolution. The $S_{\mathrm{DE}}^{\mathrm{t}}$ which enters to the C_{V}^d is the threshold on the student's t-distribution channel for the LDPC codes (size 2^{20}) predicted by the density evolution. Based on the density evolution,[43] $S_{\mathrm{DE}}^{\mathrm{BIAWGN}}$ is smaller than $S_{\mathrm{DE}}^{\mathrm{t}}$ which enters the C_{V}^d. There is no definite numerical relationship between $S_{\mathrm{DE}}^{\mathrm{BIAWGN}}$ and $S_{\mathrm{DE}}^{\mathrm{t}}$. Clearly, the SNR between the quantum channel and virtual channel would match when d trends to infinity. Then the reconciliation efficiency $\tilde{\beta}_d$ approximates β in the AWGN channel.

In Table 1, we list the reconciliation efficiency $\tilde{\beta}_8$ in the virtual channel based on Eqs. (12), (17), and (18), which corresponds to the 8-dimensional reconciliation. The code rate R is set as 0.02 and 0.05 quoted from Refs. [40] and [39]. Apparently, since the virtual channel is not exactly a BIAWGN channel, the efficiency is lower than the reconciliation efficiency predicted by the density evolution on the BIAWGN channel. It is shown that the reconciliation efficiency descends from 96.9% to 91.3% when the FDE is considered.

Table 1. Reconciliation efficiency of BIAWGN versus rotation in 8-dimensions. The SNR is 0.0492 on Bob's side at 93 km (18.6 dB losses). The code rate R is set as 0.02 and 0.05. The exact reconciliation efficiencies $\tilde{\beta}_8$ on the virtual channel are lower than the efficiencies β without considering FDE. When the code rate $R = 0.02$, $\beta = 96.9\%$, and $\tilde{\beta}_8 = 91.3\%$ are obtained.

R	β/%	$\tilde{\beta}_8$/%	$S_{\mathrm{DE}}^{\mathrm{BIAWGN}}$	$S_{\mathrm{DE}}^{\mathrm{t}}$
0.05	95.8	89.7	0.075	0.083
0.02	96.9	91.3	0.029	0.042

Finally, we consider the influence of the FDE on the secret key rate. According to Ref. [11], the secret key rate K with n received pulses used for key establishment can be represented as follows:

$$K = \frac{n}{N}\left[\beta I_{\mathrm{AB}} - S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}} - \Delta(n)\right], \tag{19}$$

where $n = N - m$, $\beta \in (0,1)$ is the efficiency of the reverse reconciliation, I_{AB} represents the mutual information[46] between Alice and Bob, which can be derived from Bob's measured variance V_{B} and the conditional variance $V_{\mathrm{B|A}}$, i.e.,

$$I_{\mathrm{AB}} = \frac{1}{2}\log_2\frac{V_{\mathrm{B}}}{V_{\mathrm{B|A}}} = \frac{1}{2}\log_2\frac{V_{\mathrm{B}}}{\hat{\sigma}^2}, \tag{20}$$

and $S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}}$ represents the maximal value of the Holevo information compatible with statistics except with probability ϵ_{PE}. Since Bob's detector is calibrated before the experiment and cannot be controlled by Eve, $S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}}$ is determined by the following covariance matrix between Alice and Bob with finite-size effect:

$$\Gamma_{\mathrm{AB}} = \begin{bmatrix} (V_{\mathrm{A}}+1)\mathbb{I}_2 & \sqrt{T_{\min}(V_{\mathrm{A}}^2+2V_{\mathrm{A}})}\sigma_z \\ \sqrt{T_{\min}(V_{\mathrm{A}}^2+2V_{\mathrm{A}})}\sigma_z & [T_{\min}(V_{\mathrm{A}}+\varepsilon_{\max})+1]\mathbb{I}_2 \end{bmatrix}, \tag{21}$$

where matrices $\mathbb{I}_2 = \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$ and $\sigma_z = \left[\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right]$, $T_{\min}$ and $\varepsilon_{\max}$ correspond to the lower bound of the transmission efficiency T and the upper bound of the excess noise ε, respectively. When m is large enough (e.g., $> 10^6$), we could compute $T_{\min}$ and $\varepsilon_{\max}$ as follows:[11]

$$\begin{aligned} T_{\min} &= (\ell_{\min})^2, \\ \varepsilon_{\max} &= \frac{\sigma_{\max}^2 - 1}{T}. \end{aligned} \tag{22}$$

Furthermore, when m is large enough, $\ell_{\min}$ and $\sigma_{\max}^2$ can be calculated by

$$\begin{aligned} \ell_{\min} &\approx \sqrt{T} - z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{1+\varepsilon}{mV_{\mathrm{A}}}}, \\ \sigma_{\max} &\approx 1 + T\varepsilon + z_{\epsilon_{\mathrm{PE}}/2}\frac{(1+T\varepsilon)\sqrt{2}}{\sqrt{m}}, \end{aligned} \tag{23}$$

where $z_{\epsilon_{\mathrm{PE}}/2}$ follows

$$1 - \frac{1}{2}\mathrm{erf}\left(z_{\epsilon_{\mathrm{PE}}/2}/\sqrt{2}\right) = \frac{1}{2}\epsilon_{\mathrm{PE}}, \tag{24}$$

and $\mathrm{erf}(\cdot)$ is the error function defined as

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\mathrm{d}t. \tag{25}$$

Meanwhile, $S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}}$ is calculated as follows:

$$S_{\mathrm{BE}}^{\epsilon_{\mathrm{PE}}} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{26}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$, and λ_i are symplectic eigenvalues derived from the covariance matrices

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \\ \lambda_{3,4}^2 &= \frac{1}{2}(C \pm \sqrt{C^2 - 4D}), \\ \lambda_5 &= 1, \end{aligned} \tag{27}$$

with

$$\begin{aligned} A &= (V_{\mathrm{A}}+1)^2 - 2T_{\min}(V_{\mathrm{A}}^2 + 2V_{\mathrm{A}}) + [T_{\min}(V_{\mathrm{A}} + \varepsilon_{\max}) + 1]^2, \\ B &= [(T_{\min}\varepsilon + 1)(V_{\mathrm{A}}+1) - T_{\min}V_{\mathrm{A}}]^2, \\ C &= \frac{A(1-\eta+v_{\mathrm{el}}) + (V_{\mathrm{A}}+1)\sqrt{B} + T_{\min}(V_{\mathrm{A}} + \varepsilon_{\max}) + 1}{\eta T_{\min}(V_{\mathrm{A}} + \varepsilon_{\max} + 1 + v_{\mathrm{el}})}, \\ D &= \frac{\sqrt{B}(V_{\mathrm{A}} + 1 + \sqrt{B}(1-\eta+v_{\mathrm{el}})/\eta)}{\eta T_{\min}(V_{\mathrm{A}} + \varepsilon) + 1 + v_{\mathrm{el}}}. \end{aligned} \tag{28}$$

In Eq. (19), $\Delta(n)$ is a linear function of n and related to the security of privacy amplification. For a CVQKD system, $\Delta(n)$ can be expressed as[11]

$$\Delta(n) = 7\sqrt{\frac{\log_2(1/\hat{\epsilon})}{n}} + \frac{2}{n}\log_2\frac{1}{\epsilon_{\mathrm{PA}}}, \tag{29}$$

where parameters $\hat{\epsilon}$ and ϵ_{PA}, which are virtual parameters and can be optimized in computation, denote the smoothing parameter and the failure probability of the privacy amplification, respectively. In calculation, $\hat{\epsilon}$ and ϵ_{PA} are usually set to be equal to ϵ_{PE}, i.e., $\hat{\epsilon} = \epsilon_{\mathrm{PA}} = \epsilon_{\mathrm{PE}}$, because it is observed that the value of $\Delta(n)$ mainly depends on n instead of these two parameters.

Based on Eqs. (27) and (28), one may evaluate the secret key bit rate with finite-size effects under collective attacks. For a practical pulsed CVQKD system, the bit rate of the secret key is given by

$$R = f_{\mathrm{rep}}K, \tag{30}$$

where the secret key rate K is defined in Eq. (19) and f_{rep} represents the repetition frequency. Let m be the typical value $m = N/2 = 10^{10}$, the secret key rate may be regarded as a function $K = K(V_{\mathrm{A}}, T, \varepsilon, v_{\mathrm{el}}, N_0)$.

Figure 3 demonstrates the relationship between the secret key rate and the transmission distance with various reconciliation efficiencies. It shows that the change of the reconciliation efficiencies dramatically decreases the secret key rate, while the secure transmission distance is approximately 20 km shorter than the original one when we have not accounted for the FDE. It is shown that the value with FDE is lower than that without FDE at transmitted distance $d = 93$ km. If the FDE is not considered, it would lead to the misevaluation of the secret key rate, and then introduce a potential safety risk. Thus we can see that the FDE is significant for a practical CVQKD system.

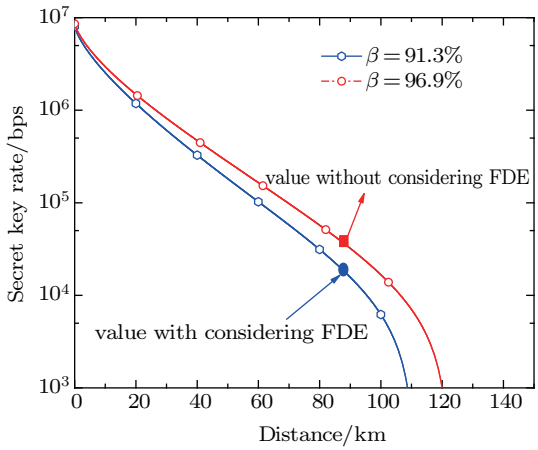


Fig. 3. (color online) Secret key rate under collective attacks in finite-size scenario. The blue solid line is the accurate secret key rate based on the finite-size security. The red solid line is the secret key rate based on the same finite-size scenario without considering the FDE. The block length N is set as 2×10^{10} and the security parameter $\epsilon = 1 \times 10^{-10}$. The modulation variance V_{A} is 6, and the excess noise is set as $\xi = 0.01$. The electronic noise at Bob's side is $v_{\mathrm{el}} = 0.04$.

5. Practical security loopholes

Commonly, the information characteristic of the introduced virtual channel should accord with that of the quantum channel in a CVQKD scheme. However, if they are not matching, for example, the SNRs between the quantum channel and the virtual channel are not the same, miscalculations on the secret key rate are generated. Consequently, such kinds of imperfections will inevitably degrade the practical security of the CVQKD system. The above section has demonstrated clearly the difference of SNRs between the quantum channel and the introduced virtual channel. Such difference, which is generated by the imperfections of the multi-dimensional reconciliation scheme, will lead to loopholes for the practical security. Actually, figure 3 has shown that the CVQKD system is insecure beyond about 100 km.

In the above section, we have demonstrated the influences of the FDE on the secure secret key rate and secure transmission distance. The most significant factor is that the FDE leads to the SNR mismatch between the quantum channel and the virtual channel. For example, the noise variation of the virtual channel is $4/3$ times of the one of the physical channel (Gaussian channel) when $d = 8$. Correspondingly, the SNR of the virtual channel is $3/4$ times of that of the quantum channel. Such change will decrease the actual reconciliation efficiency, which has a significant influence on the secret key rate.

Figure 4 plotted, respectively, for different reconciliation efficiency β and modulation variation V_{A} shows that the se-

cure secret key rates will drastically decrease and the secure transmitted distances will become shorter when considering the FDE. In addition, the FDE would be greater as the modulation V_A becomes larger. This explains that there is a gap between the secret key rate considering FDE and the one without considering FDE. In this way, Eve can utilize such a gap to engage in attack, such as intercept-resend attacks. Then Eve can gain access to some of the information on the legitimate parties. Thus the FDE can induce significant practical security issues.

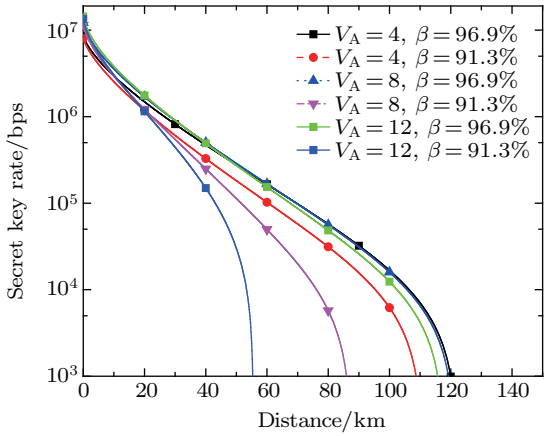


Fig. 4. (color online) Secret key rate under collective attacks in finite-size scenario. The block length N is set as 2×10^{10} and the security parameter $\epsilon = 1 \times 10^{-10}$. The excess noise ξ is set as 0.01. The balanced homodyne detection efficiency is set to $\eta = 0.6$, and the electronic noise at Bob's side is $v_{el} = 0.04$.

6. Conclusion

We have investigated the imperfections of the multi-dimensional reconciliation scheme and the induced practical security loopholes. Such kinds of imperfections come from the algorithm but are not induced by the devices of the CVQKD system, which has been investigated previously. We find that the binary input virtual channel is different from the BIAWGN channel due to the FDE. In particular, the FDE leads to SNR mismatch between the quantum channel and the virtual channel, and subsequently results in significant influences on the channel capacity, the reconciliation efficiency, and the secure secret key rate. Consequently, it leads to overestimation on the secret key rate, and then introduces practical security loopholes.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[3] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[4] Huang D, Huang P, Wang T, Li H S, Zhou Y M and Zeng G H 2016 *Phys. Rev. A* **94** 032305
[5] Xiao H and Zhang Z 2017 *Quantum Information Processing* **16** 13
[6] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[7] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photon.* **7** 378
[8] Gehring T, Händchen V, Duhme J, Furrer F, Franz T, Pacher C, Werner R F and Schnabel R 2015 *Nat. Commun.* **6** 8795
[9] Navascués M, Grosshans F and Acin A 2006 *Phys. Rev. Lett.* **97** 190502
[10] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[11] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343
[12] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501
[13] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
[14] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502
[15] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 *Phys. Rev. Lett.* **110** 030502
[16] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501
[17] Filip R 2008 *Phys. Rev. A* **77** 022310
[18] Jouguet P, Kunz-Jacques S, Diamanti E and Leverrier A 2012 *Phys. Rev. A* **86** 032309
[19] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **88** 022339
[20] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev. A* **87** 062313.
[21] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C and Han Z F 2013 *Phys. Rev. A* **87** 062329
[22] Huang J Z, Kunz-Jacques S, Jouguet P, Weedbrook C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2014 *Phys. Rev. A* **89** 032304
[23] Qin H, Kumar R and Alléaume R 2016 *Phys. Rev. A* **94** 012325
[24] Wang C, Huang P, Huang D, Lin D K and Zeng G H 2016 *Phys. Rev. A* **93** 022315
[25] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Han Z F and Guo G C 2015 *Nature Photonics* **9** 832
[26] Wang S, Chen W, Yin Z Q, *et al.* 2014 *Opt. Express* **22** 21739
[27] Wang S, Chen W, Guo J F, Yin Z Q, Li H W, Zhou Z, Guo G C and Han Z F 2012 *Opt. Lett.* **37** 1008
[28] Xu F X, Wang S, Han Z F and Guo G C 2010 *Chin. Phys. B* **19** 10
[29] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 *New J. Phys.* **11** 045023
[30] Jouguet P, Kunz-Jacques S, Debuisschert T, Fossier S, Diamanti E, Alléaume R, Tualle-Brouri R, Grangier P, Leverrier A, Pache P and Painchault P 2012 *Opt. Express* **20** 14030
[31] Huang D, Huang P, Li H S, Wang T, Zhou Y M and Zeng G H 2016 *Opt. Lett.* **41** 3511
[32] Van Assche G, Cardinal J and Cerf N J 2004 *IEEE Transactions on Information Theory* **50** 394
[33] Ralph T C 1999 *Phys. Rev. A* **61** 010303
[34] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
[35] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[36] Heid M and Lütkenhaus N 2007 *Phys. Rev. A* **76** 022313
[37] Xuan Q D, Zhang Z S and Voss P L 2009 *Opt. Express* **17** 24244
[38] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 *Phy. Rev. A* **77** 042325
[39] Richardson T and Urbanke R 2002 in *Workshop Honoring Prof. Bob McEliece on His 60th Birthday, California Institute of Technology, Pasadena, California* pp. 24–25
[40] Jouguet P, Kunz-Jacques S and Leverrier A 2011 *Phys. Rev. A* **84** 062317
[41] Huang D, Huang P, Lin D K and Zeng G H 2016 *Sci. Rep.* **6** 19201
[42] Lin D K, Huang D, Huang P, Peng J Y and Zeng G H 2015 *International Journal of Quantum Information* **13** 1550010
[43] Gallager R 1962 *IRE Transactions on information theory* **8** 21
[44] Richardson T J, Shokrollahi M A and Urbanke R L 2001 **47** 619
[45] Grinstead C M and Snell J L 2012 *Introduction to Probability* (New York: American Mathematical Soc.)
[46] Cover T M and Thomas J A 2012 *Elements of Information Theory* (New York: John Wiley & Sons)