Vol 16 No 5, May 2007
1009-1963/2007/16(05)/1364-06

Chinese Physics

Security analysis of continuous-variable quantum key distribution scheme*

Zhu Jun(朱 俊)†, He Guang-Qiang(何广强), and Zeng Gui-Hua(曾贵华)

The State Key Laboratory on Fiber-Optic Local Area Networks and Advanced Optical Communication Systems, Electronic Engineering Department, Shanghai Jiaotong University, Shanghai 200240, China

(Received 26 July 2006; revised manuscript received 27 October 2006)

In this paper security of the quantum key distribution scheme using correlations of continuous variable Einstein–Podolsky–Rosen (EPR) pairs is investigated. A new approach for calculating the secret information rate ΔI is proposed by using the Shannon information theory. Employing an available parameter F which is associated with the entanglement of the EPR pairs, one can detect easily the eavesdropping. Results show that the proposed scheme is secure against individual beam splitter attack strategy with a proper squeeze parameter.

Keywords: continuous variable EPR entanglement pairs, quantum key distribution, Shannon information theory, security analysis

PACC: 4250, 4230Q, 0365

1. Introduction

Quantum key distribution (QKD)[1] makes it possible for two remote parties, Alice and Bob, to agree on secret information that could later be distilled into a secret key for encrypting messages. The security of which is guaranteed by the fundamental laws of quantum mechanics.[2−4] Thus far many discrete variable (DV) QKD schemes,[1,5] generally based on the phase or polarization modulation of single photon pulses, have been proposed. However, besides having very low communicating rates, these schemes require specifically advanced devices such as single photon sources and single photon counters which are very difficult to fabricate. In contrast, the canonical quantum quadratures of light beams are customarily used in continuous variable (CV) QKD schemes[6−13] to encode information, which are easier to produce and detect comparatively. Therefore the CV QKD schemes associated with the canonical quantum quadratures of light beams become a more favourable candidate in the quantum cryptography.

At present, a very important problem in the active field of CV QKD schemes is the security analysis of the quantum cryptographic scheme. Although much researches have been done, the security analysis of the CV QKD schemes is still far from maturity, especially using Shannon information theory. In this paper, we study a CV QKD scheme using Einstein–Podolsky–Rosen (EPR) correlations. Detailed proof based on Shannon information theory has been given, which illustrates the security of this scheme against the individual beam splitter (BS) eavesdropping attack.

This paper is organized as follows. In Section 2, the scheme is specified so that the analysis about its security by calculating the secret information rate ΔI and the entanglement parameter F could be carried on more conveniently in Section 3. And the conclusions are drawn in Section 4.

2. Scheme description

For describing clearly our approach for the security analysis of the CV QKD scheme, we suggest a simple QKD scheme by using CV EPR correlations. The scheme is composed of two independent parties. Alice, the sender, has to prepare the CV EPR entanglement pairs by using a nondegenerate optical parametric amplifier (NOPA). Bob, the receiver, has to randomly select to measure a quadrature of the receiving signal (see Fig.1). The scheme can be described by the following steps:

Step 1 Alice prepares a state $|\psi_0\rangle = |0\rangle_1 \otimes |0\rangle_2$, where the subscripts 1 and 2 denote input modes $\hat{a}_1$

*Project supported by the National Natural Science Foundation of China (Grant No 60472018).

†E-mail: bierhoff_24@sjtu.edu.cn

and $\hat{a}_2$ respectively. Let the input modes enter into the NOPA, a pair of EPR entanglement light beams is generated with a proper squeezed parameter r. Thus, the output mode $\hat{a}_3$ correlates with the output mode $\hat{a}_4$, and this correlation increases with large r. The entanglement degree of the generated two-mode state, i.e., the state consisting of modes $\hat{a}_3$ and $\hat{a}_4$, may be characterized by using an available parameter F defined as,[14]

$$F = \left\langle \left[\Delta(X^1_{\text{out1}} - k_1 X^1_{\text{out2}})\right]^2 \right\rangle_{\min} \times \left\langle \left[\Delta(X^2_{\text{out1}} - k_2 X^2_{\text{out2}})\right]^2 \right\rangle_{\min}, \quad (1)$$

where k_1 and k_2 are coefficients giving F the minimal value, X^1 and X^2 are the canonical quantum quadratures of the light beams, and the subscripts out1 and out2 refer to the modes $\hat{a}_3$ and $\hat{a}_4$.

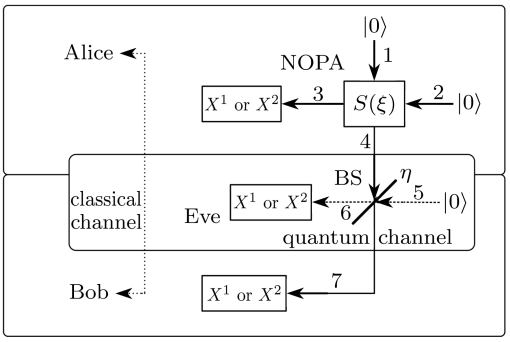

Fig.1. Schematic representation of the QKD scheme based on CV EPR correlations. NOPA: nondegenerate optical parametric amplifier. $S(\xi)$: two-mode squeezing operator of NOPA. BS: beam splitter. η: the transmission coefficient of BS. The Arabic numerals denote the modes.

Step 2 Alice calculates the entanglement parameter F_{a} and the corresponding threshold F_{th}. Then the mode $\hat{a}_4$ is sent to Bob, while $\hat{a}_3$ is preserved by Alice.

Step 3 Alice and Bob prepare random bit strings a and b respectively, where $a = a_1a_2a_3\cdots a_n$, $a_i \in \{0,1\}$, $\forall i$, $b = b_1b_2b_3\cdots b_n$, $b_i \in \{0,1\}$. According to a_i and b_i, Alice and Bob choose basis to measure X^1 or X^2 respectively. For instance, if $a_i = 0$, Alice measures X^1; otherwise, Alice measures X^2.

Step 4 Alice and Bob write down their measurement results and the corresponding time slots, respectively.

Step 5 After the transmission is finished, Alice and Bob compare their random sequences a and b through a classical channel. The measurement results are held when $a_i = b_i$, and the others are discarded. When Eve does not exist, the quantum channel is perfect and the squeezing parameter of CV EPR pairs is infinite, the remaining measurement results of both Alice and Bob would have the same absolute value.

Step 6 Alice tells Bob some of her remaining measurement results and the corresponding time slots through the classical channel. Bob then estimates the parameter F_{b} by comparing Alice's measurement results with his own measurement results with the corresponding time slots. If $F_{\text{b}} \geq F_{\text{th}}$, then he goes to Step 1, and restarts the protocol, since Eve gets more information than Bob in this situation. Otherwise proceeds with next step.

Step 7 By employing reconciliation and privacy amplification, Alice and Bob can distill secure key from the remaining measurement results.

3. Security analysis

In this section, the security of the proposed scheme is investigated in details by employing the Shannon information theory. The secret information rate defined by[15]

$$\Delta I = I(\alpha,\beta) - I(\alpha,\varepsilon) \quad (2)$$

is a very important parameter for showing the security, where $I(\alpha,\beta)$ denotes the mutual information between Alice and Bob, and $I(\alpha,\varepsilon)$ denotes the mutual information between Alice and Eve. Generally, if $\Delta I > 0$ the QKD protocol must be secure with the techniques of reconciliation and privacy amplification. To detect the eavesdropping, the entanglement parameter F defined in Eq.(1) is available. The condition $F \geq F_{\text{th}}$ may be employed to judge the influence of Eve's disturbance on the quantum channel.

3.1. Secret information rate

With the aim of calculating $I(\alpha,\beta)$ and $I(\alpha,\varepsilon)$, we first determine the probability distribution of the quadratures X^1 and X^2 in all modes as depicted in Fig.1. Applying a two-mode squeezed operator $S(\xi)$, we get the output modes, $\hat{a}_3$ and $\hat{a}_4$ of the NOPA:

$$\begin{aligned} X^1_3 &= X^1_1\cosh(r) + X^1_2\sinh(r), \\ X^2_3 &= X^2_1\cosh(r) - X^2_2\sinh(r), \\ X^1_4 &= X^1_2\cosh(r) + X^1_1\sinh(r), \\ X^2_4 &= X^2_2\cosh(r) - X^2_1\sinh(r), \end{aligned} \quad (3)$$

where $r = \kappa t$ is the squeezed parameter. Suppose Eve eavesdrops on the quantum channel individually by

using a BS with the transmission coefficient η, then we have the output modes of the BS

$$X_6^1 = \sqrt{\eta}X_5^1 - \sqrt{1-\eta}X_4^1,$$
$$X_6^2 = \sqrt{\eta}X_5^2 - \sqrt{1-\eta}X_4^2,$$
$$X_7^1 = \sqrt{\eta}X_4^1 + \sqrt{1-\eta}X_5^1,$$
$$X_7^2 = \sqrt{\eta}X_4^2 + \sqrt{1-\eta}X_5^2. \quad (4)$$

Combining Eqs.(3) and (4) we obtain,

$$X_6^1 = \sqrt{\eta}X_5^1 - \sqrt{1-\eta}X_2^1\cosh(r) - \sqrt{1-\eta}X_1^1\sinh(r),$$
$$X_6^2 = \sqrt{\eta}X_5^2 - \sqrt{1-\eta}X_2^2\cosh(r) + \sqrt{1-\eta}X_1^2\sinh(r),$$
$$X_7^1 = \sqrt{\eta}X_2^1\cosh(r) + \sqrt{\eta}X_1^1\sinh(r) + \sqrt{1-\eta}X_5^1,$$
$$X_7^2 = \sqrt{\eta}X_2^2\cosh(r) - \sqrt{\eta}X_1^2\sinh(r) + \sqrt{1-\eta}X_5^2. \quad (5)$$

Since random variables $X_i^1, X_i^2 (i = 1, 2, 5)$ are independent of each other with the Gaussian distribution

$$X_i^1, X_i^2 : N\left(0, \frac{1}{4}\right) (i = 1, 2, 5) \quad (6)$$

the random variables $X_i^1, X_i^2 (i = 3, 6, 7)$ also follow the Gaussian distribution.

According to the Shannon information theory,[16] we can simply calculate the mutual information between random variables $(X_3^1; X_6^1)$, $(X_3^2; X_6^2)$, $(X_3^1; X_7^1)$ and $(X_3^2; X_7^2)$:

$$I(X_3^1; X_6^1) = I(X_3^2; X_6^2) = \frac{1}{2}\log_2\left\{1 + \frac{4(1-\eta)\cosh^2(r)\sinh^2(r)}{(1-\eta) + \eta[\cosh^2(r) + \sinh^2(r)]}\right\},$$
$$I(X_3^1; X_7^1) = I(X_3^2; X_7^2) = \frac{1}{2}\log_2\left\{1 + \frac{4\eta\cosh^2(r)\sinh^2(r)}{\eta + (1-\eta)[\cosh^2(r) + \sinh^2(r)]}\right\}. \quad (7)$$

Since Alice and Bob randomly choose measurement basis and preserve their measurement only when their bases are compatible, half of their measurement results are discarded. Hence the actual mutual information between Alice and Bob is just half of that between $(X_3^1; X_7^1)$ and $(X_3^2; X_7^2)$, which is

$$I(\alpha, \beta) = \frac{1}{4}\log_2\left\{1 + \frac{4\eta\cosh^2(r)\sinh^2(r)}{\eta + (1-\eta)[\cosh^2(r) + \sinh^2(r)]}\right\}. \quad (8)$$

Similarly, the actual mutual information between Alice and Eve is

$$I(\alpha, \varepsilon) = \frac{1}{4}\log_2\left\{1 + \frac{4(1-\eta)\cosh^2(r)\sinh^2(r)}{(1-\eta) + \eta[\cosh^2(r) + \sinh^2(r)]}\right\}. \quad (9)$$

Employing Eqs.(2), (8) and (9), one obtains

$$\Delta I = I(\alpha, \beta) - I(\alpha, \varepsilon) = \frac{1}{4}\log_2\left\{\frac{[\eta(1+4M) + (1-\eta)N][(1-\eta) + \eta N]}{[(1-\eta)(1+4M) + \eta N][\eta + (1-\eta)N]}\right\}, \quad (10)$$

where

$$M = \cosh^2(r)\sinh^2(r),$$
$$N = \cosh^2(r) + \sinh^2(r).$$

To distill a secret final key by employing the techniques of reconciliation and privacy amplification, one may let $\Delta I = I(\alpha, \beta) - I(\alpha, \varepsilon) > 0$. Since the complexity of Eq.(10), we analyse the security via number simulations. The relationship between ΔI and η is plotted in Fig.2.

One may find that ΔI increases with the increase of η, and ΔI reaches its maximal value with $\eta = 1$. Besides, whatever value r has been given, there is always the result that $\Delta I = 0$ with $\eta = 0.5$. Physically, this can be explained as follows. Since Eve uses BS to eavesdrop the quantum channel individually, according to Eq.(4), the smaller the transmission coefficient η of BS is, the more information beam Eve would get

and the less Bob would get. When $\eta = 0.5$, the information beam that Eve obtains is as much as that Bob obtains.

In addition, Fig.2 shows that the absolute value of ΔI increases with the increase of squeezed parameter r. That means we could improve the mutual information between authorized communicators by consummating the EPR entanglement pairs. Particularly, when $r = 0$, i.e., the output modes of the NOPA are mutually independent, we have $\Delta I \equiv 0$. Under this circumstance, no one can obtain any information.

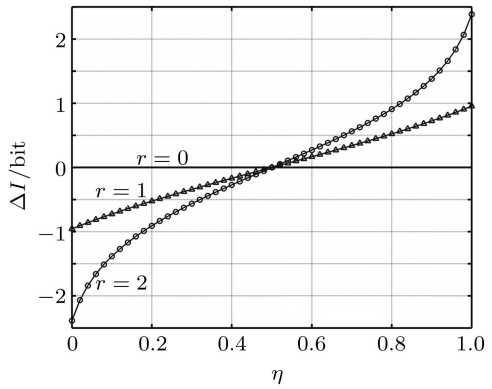

Fig.2. Secret information rate ΔI versus transmission coefficient η with squeezed parameter $r = 0, 1, 2$.

3.2. Detecting eve

In classical communication, an eavesdropper can obtain perfect copies of the beams without making any disturbance. However, in quantum theory, the eavesdropping inevitably disturbs the transmitting beam, which will destroy the correlations between EPR pairs. In addition, the information got by Eve is limited by the imperfection in the copies. Thus, Eve's intervention can be detected by calculating the entanglement parameter F due to the disturbance. Firstly the entanglement parameters $F_{\rm a}$, $F_{\rm th}$ and $F_{\rm b}$ are calculated. Then detailed circumstances are discussed.

Define

$$\delta X^1_{\rm Eve} = X^1_7 - k_1 X^1_3, \quad \delta X^2_{\rm Eve} = X^2_7 + k_2 X^2_3. \tag{11}$$

When $\eta = 0.5$ which corresponds to $\Delta I = 0$, combining Eqs.(4) and (11) we obtain

$$\begin{aligned} \delta X^1_{\rm Th} &= \frac{\sqrt{2}}{2}(X^1_4 + X^1_5) - k_1 X^1_3, \\ \delta X^2_{\rm Th} &= \frac{\sqrt{2}}{2}(X^2_4 + X^2_5) + k_2 X^2_3. \end{aligned} \tag{12}$$

When $\eta = 1$ which corresponds to no eavesdropping, from Eqs.(4) and (11) we have

$$\begin{aligned} \delta X^1_{\rm no-Eve} &= X^1_4 - k_1 X^1_3, \\ \delta X^2_{\rm no-Eve} &= X^2_4 + k_2 X^2_3. \end{aligned} \tag{13}$$

According to Eqs.(3) and (13), we have

$$\left\langle [\Delta(\delta X^j_{\rm no-Eve})]^2 \right\rangle = \frac{1}{4}[\cosh(r) - k_j \sinh(r)]^2 + \frac{1}{4}[\sinh(r) - k_j \cosh(r)]^2 \quad (j = 1, 2). \tag{14}$$

Equation (14) gives the minimal values of $\langle [\Delta(\delta X^1_{\rm no-Eve})]^2 \rangle$ and $\langle [\Delta(\delta X^2_{\rm no-Eve})]^2 \rangle$

$$\langle [\Delta(\delta X^1_{\rm no-Eve})]^2 \rangle_{\min} = \langle [\Delta(\delta X^2_{\rm no-Eve})]^2 \rangle_{\min} = \frac{1}{4\cosh^2(r) + 4\sinh^2(r)}, \tag{15}$$

when

$$k_1 = k_2 = \frac{2\cosh(r)\sinh(r)}{\cosh^2(r) + \sinh^2(r)}. \tag{16}$$

Employing Eq.(1) we obtain,

$$F_{\rm a} = \langle [\Delta(\delta X^1_{\rm no-Eve})]^2 \rangle_{\min} \langle [\Delta(\delta X^2_{\rm no-Eve})]^2 \rangle_{\min} = \frac{1}{16[\cosh^2(r) + \sinh^2(r)]^2}. \tag{17}$$

Similarly, Eqs.(3) and (12) give

$$\langle [\Delta(\delta X^j_{\rm Th})]^2 \rangle = \frac{1}{4}\left\{ \left[\frac{\sqrt{2}}{2}\cosh(r) - k_j \sinh(r)\right]^2 + \left[\frac{\sqrt{2}}{2}\sinh(r) - k_j \cosh(r)\right]^2 + (1 - \eta) \right\} \quad (j = 1, 2). \tag{18}$$

Substituting Eq.(16) into Eq.(18) we have

$$F_{\rm Th} = \langle[\Delta(\delta X^1_{\rm Th})]^2\rangle\langle[\Delta(\delta X^2_{\rm Th})]^2\rangle. \tag{19}$$

Similarly, combining Eqs.(5) and (11) we get

$$\langle[\Delta(\delta X^j_{\rm Eve})]^2\rangle = \frac{1}{4}\left\{[\sqrt{\eta}\cosh(r) - k_j\sinh(r)]^2 + [\sqrt{\eta}\sinh(r) - k_j\cosh(r)]^2 + (1-\eta)\right\} \quad (j=1,2). \tag{20}$$

Substituting Eq.(16) into Eq.(20) we have

$$F_{\rm b} = \langle[\Delta(\delta X^1_{\rm Eve})]^2\rangle\langle[\Delta(\delta X^2_{\rm Eve})]^2\rangle. \tag{21}$$

Obviously, there is always $F_{\rm b} \geq F_{\rm a}$, and the lower bound of $F_{\rm b}$ can be reached when $\eta = 1$. Also we have $F_{\rm b} = F_{\rm th}$ when $\eta = 0.5$.

The relationship between parameter $F_{\rm b}$ and disturbance coefficient $D(D = 1-\eta)$ is plotted in Fig.3.

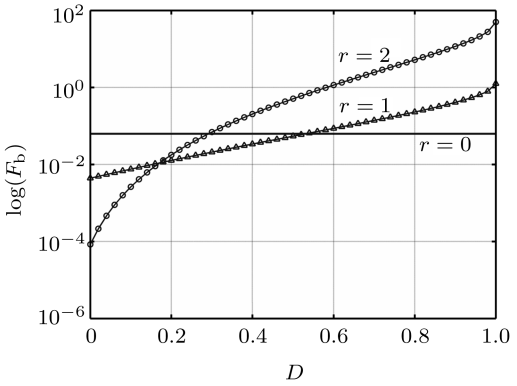

Fig.3. The entanglement parameter $F_{\rm b}$ versus disturbance coefficient D $(D = 1-\eta)$ with squeezed parameter $r = 0, 1, 2$. ($F_{\rm b}$ is drawn in logarithmic scale).

We see that $F_{\rm b}$ increases rapidly when D increases. Suppose the quantum channel is perfect, we can deduce as follows. When $F_{\rm b} \geq F_{\rm th}$, then we have $D \geq 0.5$. Thereby we have to restart the QKD process since Eve exists and $\Delta I \leq 0$. When $F_{\rm a} < F_{\rm b} < F_{\rm th}$, then we have $0 < D < 0.5$. Although Eve exists, we have no need to re-distribute the key because $\Delta I > 0$ in this situation. When $F_{\rm b} = F_{\rm a}$, then we have $D = 0$, which means that Eve does not exist. Consequently the information shared by Alice and Bob are absolutely secure. Specially, it has no practical meaning that $F_{\rm b}$ remains constant when $r = 0$, because the authorized communicators cannot share any information as mentioned in Section 3.1.

3.3. The relationship between ΔI and $F_{\rm b}$

According to the discussion above, the relationship between secret information rate ΔI and the entanglement parameter $F_{\rm b}$ is extremely significant. In principle, the relationship between ΔI and $F_{\rm b}$ may be obtained by combining Eqs.(10) and (21). However, the analytical expression is very complex. Therefore we illustrate the results by numerical simulations which are shown in the Fig.4 with a squeezed parameter $r = 2$.

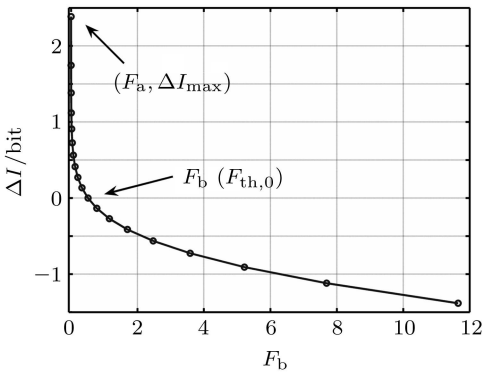

Fig.4. Secret information rate ΔI versus the entanglement parameter $F_{\rm b}$ with squeezed parameter $r = 2$.

In Fig.4, $F_{\rm b}$ increases quickly with the decrease of ΔI, especially when $\Delta I \leq 0$. It predicates that the more information Eve obtain, the easier she would be detected. For $r = 2$, $\Delta I_{\max} = 2.386$ bit when $F_{\rm b}$ reaches its lower bound $F_{\rm b\ min} = F_{\rm a} = 8.38 \times 10^{-5}$, and $\Delta I \leq 0$ when $F_{\rm b} \geq F_{\rm th} = 0.51$. Apparently these numerical solutions accord with the discussion in Section 3.2.

According to the above, one has the following results. When $F_{\rm b} = F_{\rm a}$, there is no eavesdropping in the QKD process which is actually an ideal case. In this case Alice and Bob may generate a secret key without any classic supplements such as privacy amplification. When $F_{\rm a} < F_{\rm b} < F_{\rm th}$, one may find that the secret information rate still satisfies $\Delta I > 0$ despite of the eavesdropper's existence. In this situation,

Alice and Bob may obtain an secure key by using the techniques of reconciliation and privacy amplification. When $F_{\rm b} \geq F_{\rm th}$, the eavesdropper's existence leads to the secret information rate $\Delta I \leq 0$ and Alice and Bob cannot obtain a secure key. The security of the QKD scheme can be guaranteed only by restarting the QKD process.

4. Conclusion

The security of the QKD scheme using correlations of CV EPR pairs is elaborately investigated by employing the Shannon information theory. The proposed approach for the security analysis of the CV QKD may be applied in other kinds of schemes which use CV. Using this approach the proposed scheme has been proven to be secure against the individual BS eavesdropping attack strategy. In addition, an approach for detecting eavesdropper by using the entanglement parameter F is presented. Physically, the squeezed parameter r plays important role in the proposed scheme. The larger squeezed parameter r benefits the perfection of the CV EPR entanglement pairs, subsequently, the higher key distributing rate and the channel capability.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Lo H K and Chau H F 1999 *Science* **283** 2050

[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[4] Mayers D 2001 *J. ACM* **48** 351

[5] Liang C, Fu D H, Liang B, Liao J, Wu L An, Yao D Ch and Lv Sh W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese)

[6] Braunstein S L and Loock P V 2005 *Rev. Mod. Phys.* **77** 513

[7] Ralph T C 1999 *Phys. Rev.* A **61** 010303(R)

[8] Hillery M 2000 *Phys. Rev.* A **61** 022309

[9] Gottesman D and Preskill J 2001 *Phys. Rev.* A **63** 022309

[10] Cerf N J, Lévy M and van Assche G 2001 *Phys. Rev.* A **63** 052311

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

[12] Silberhorn Ch, Korolkova N and Leuchs G 2002 *Phys. Rev. Lett.* **88** 167902

[13] He G Q and Zeng G H 2006 *Chin. Phys.* **15** 1284

[14] He G Q, Zhu J and Zeng G H 2006 *Phys. Rev.* A **73** 012314

[15] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733

[16] Jiang D 2004 *Information Theory and Coding* (Hefei: University of Science and Technology of China)