Quantum Information and Computation, Vol. 13, No. 9&10 (2013) 0827–0832

A STUDY OF BB84 PROTOCOL IN A DEVICE-INDEPENDENT SCENARIO: FROM THE VIEW OF ENTANGLEMENT DISTILLATION

ZHEN-QIANG YIN, WEI CHEN[a], SHUANG WANG[b], HONG-WEI LI, GUANG-CAN GUO, ZHENG-FU HAN[c]
Key Laboratory of Quantum Information, University of Science and Technology of China
Hefei, 230026, China

Received February 11, 2012
Revised February 1, 2013

For the past few years, the security of practical quantum key distribution systems has attracted a lot of attention. Device-independent quantum key distribution was proposed to design a real-life secure quantum key distribution system with imperfect and untrusted quantum devices. In this paper, we analyzed the security of BB84 protocol in a device-independent scenario based on the entanglement distillation method. Since most of the reported loopholes are in receivers of quantum key distribution systems, we focus on condition that the transmitter of the system is perfectly coincident with the requirement of the BB84 protocol, while the receiver can be controlled by eavesdropper. Finally, the lower bound of the final secret-key rate was proposed and we explained why the secure-key rate is similar to the well-known result for the original entanglement distillation protocol.

Keywords: BB84, device-independent, quantum key distribution
Communicated by: S Braunstein & H Zbinden

1 Introduction

With the help of quantum key distribution (QKD) [1, 2, 3], two distant peers (Alice and Bob) can share secret random string of bits to fulfill unconditional secure communication. The most commonly used QKD protocol is BB84 [1]. In this protocol, Alice randomly encodes the classical bits 0 and 1 as two orthogonal quantum states $|0\rangle$ and $|1\rangle$ or $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, transmits these photons to Bob through a quantum channel which is accessed by an eavesdropper Eve. Then Bob projects these photons with measurements $M_0 = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ or $M_1 = \{|+\rangle\langle +|, |-\rangle\langle -|\}$. Finally, secret key bits may be generated after some classical communications. Many successful experiments of QKD [4, 5, 6, 7, 8, 9, 10] have been reported.

Although the security of BB84 protocol has been proven [11], implementations using real-life devices are still facing severe challenges. The eavesdroppers (Eve) can utilize the imperfections of the devices to get extra information about the key, even totally hack the system. Several comprehensive and successful attacks to experimental or commercial QKD systems have been demonstrated, such as the time-shift attack [12], bright illumination attack [13] and wavelength-dependent attack [14]. To enhance the security of practical QKD systems,

[a]kooky@mail.ustc.edu.cn
[b]wshuang@ustc.edu.cn
[c]zfhan@ustc.edu.cn

device-independent (DI) QKD [15, 16] protocols were proposed. In DIQKD protocols, entangled photon pairs are used as light source. Alice and Bob are both receivers with arbitrary measurement devices, which will output classical bits according to their own random classical input bits and the incoming photon. The security of DIQKD is based on true random number sources, well-shielded security zones, and some quantum correlations of Alice and Bob's inputs and outputs. DIQKD systems have higher security level than traditional ones since the quantum devices can be untrusted or even controlled by Eve in these systems. However, the applications of DIQKD protocols are limited due to the low key generation rate, very limited secure distance, and the low efficiency of entanglement light sources.

In this paper, we analyzed the security of a DIQKD protocol in a BB84-like scenario, in which Alice uses a perfect quantum states encoder to fulfill BB84 protocol, and the devices in Bob are treated as a black box. The only assumption to Bob's black box is there is no unexpected information leakage outside his secure zone. This scenario is selected since the imperfections of the QKD receives are essential in most of the reported attacking experiments [12, 13, 14]. The security analyses for this scenario have been given in Refs. [17, 18] with the uncertainty relation of entropies, while the methods used in this paper are mainly based on the entanglement distillation protocol (EDP). As a powerful technique to analyze the security of QKD, EDP has played an essential role in the security proof of BB84 and some other QKD protocols [11, 19, 20, 21, 22]. As far as we know, the work in this paper is the first attempt to analyze the security of DIQKD protocol using EDP method, which indicates the relationship between DIQKD and EDP.

2 Module

Now, we first module our protocol. For simplicity, we concern the entanglement version of BB84. Alice prepares N pairs of entanglement states of particles A, A_1 and B, and each of them is:

$$|\Psi_{ini}\rangle_{AA_1B} = \frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)|0\rangle_{A_1} + \frac{1}{\sqrt{2}}(|0\rangle_A|+\rangle_B + |1\rangle_A|-\rangle_B)|1\rangle_{A_1}], \quad (1)$$

in which, the particle A represents the Alice's classical bit, B represents the information carrier photon transmitted to Bob via quantum channel, and A_1 corresponds to Alice's choice of her basis. Then, Eve may apply any possible unitary transformation U_1 to the the particle B and her ancilla E. In the most general situation, the dimension of Eve's ancilla and the information carrier photon B can be arbitrary. When particle B enters into Bob's device, quantum measurement B_0 or B_1 corresponding to Bob's input 0 or 1 respectively is performed to particle B, and then Bob learns output 0 or 1. We can assume that particle B's Hilbert space is spanned by a set of orthogonal basis $\{|0_n\rangle_B, |1_n\rangle_B, |n = 0, 1, 2...\}$. Note that $\langle 0_n|0_m\rangle = \langle 1_n|1_m\rangle = \delta_{nm}$, $\langle 0_n|1_m\rangle = 0$ are always satisfied while the relations between $|0\rangle$, $|1\rangle$ and $|0_n\rangle$, $|1_n\rangle$ may be arbitrary. According to Lemma 1 in Ref. [16], the measurements B_0 and B_1 can be viewed as two Hermite operators with eigenvalues 0 and 1 since the dimension of information carrier B after Eve's attack is arbitrary. Next, Lemma 2 in Ref. [16] also proves that the receiver's operation can be considered as that Bob first projects the particle B into a two-dimensional subspace spanned by the orthogonal basis $|0_n\rangle_B$ and $|1_n\rangle_B$, consequently B_0 and B_1 can be viewed as two Hermite measurements in the $(x - z)$ plane of the Bloch

sphere. In the following discussion, we will concern the density matrix of particle B when B is projected into subspace spanned by $|0_n\rangle_B$ and $|1_n\rangle_B$.

Without loss of generality, we assume the state of Eve's ancilla can be spanned by a set of orthogonal and normalized basis $|\Gamma_m\rangle_E$, then we can define Eve's operation U_1 to B and E in the quantum channel,

$$\begin{aligned} U_1|0\rangle_B|0\rangle_E &= \sum_{n,m} \gamma_{00nm}|\Gamma_m\rangle_E|0_n\rangle_B + \gamma_{01nm}|\Gamma_m\rangle_E|1_n\rangle_B \\ U_1|1\rangle_B|0\rangle_E &= \sum_{n,m} \gamma_{10nm}|\Gamma_m\rangle_E|0_n\rangle_B + \gamma_{11nm}|\Gamma_m\rangle_E|1_n\rangle_B, \end{aligned} \tag{2}$$

where, $\sum_{n,m}|\gamma_{00nm}|^2 + |\gamma_{01nm}|^2 = \sum_{n,m}|\gamma_{11nm}|^2 + |\gamma_{10nm}|^2 = 1$. If particle B collapses into subspace spanned by $|0_n\rangle_B$ and $|1_n\rangle_B$, the density matrix of particle B is given by

$$\rho'^{(n)} = \frac{\sum_m P\{\gamma_{00nm}|0\rangle_A|0_n\rangle_B + \gamma_{11nm}|1\rangle_A|1_n\rangle_B + \gamma_{01nm}|0\rangle_A|1_n\rangle_B + \gamma_{10nm}|1\rangle_A|0_n\rangle_B\}}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2}, \tag{3}$$

in which, $P\{|x\rangle\} = |x\rangle\langle x|$. Next, following the Lemma 3 in Ref. [16], we can assume that with the probability of 1/2, Eve flips the $|0\rangle_B$ and $|1\rangle_B$ with the quantum operation $-i\sigma_y$, then applies U_1 to particle B, Bob's measurement device will flip the $|0_n\rangle_B$, $|1_n\rangle_B$ with $-i\sigma_y^{(n)}$ correspondingly. Since B_0 and B_1 are both in the $(x-z)$ plane, this operation can make sure that the probabilities of the 0 and 1 bits in the sifted key bits are same, and Eve does not lose anything in this assumption. Note that $-i\sigma_y|0\rangle = |1\rangle$, $-i\sigma_y|1\rangle = -|0\rangle$, $-i\sigma_y^{(n)}|0_n\rangle = |1_n\rangle$, and $-i\sigma_y^{(n)}|1_n\rangle = -|0_n\rangle$. The corresponding density matrix if Eve performs this operation is given by

$$\rho''^{(n)} = \frac{\sum_m P\{\gamma_{11nm}|0\rangle_A|0_n\rangle_B + \gamma_{00nm}|1\rangle_A|1_n\rangle_B - \gamma_{10nm}|0\rangle_A|1_n\rangle_B - \gamma_{01nm}|1\rangle_A|0_n\rangle_B\}}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2}. \tag{4}$$

Therefore, the final density matrix under 0 basis can be given by

$$\rho^{(n)} = \frac{\rho'^{(n)}}{2} + \frac{\rho''^{(n)}}{2}. \tag{5}$$

Consider Alice and Bob aim to get the maximally entangled state $|\phi^+\rangle = (|0\rangle_A|0_n\rangle_B + |1\rangle_A|1_n\rangle_B)/\sqrt{2}$, the phase error rate in this subspace is given by

$$\begin{aligned} e_p^{(n)} &= \langle\phi^-|\rho^{(n)}|\phi^-\rangle + \langle\psi^-|\rho^{(n)}|\psi^-\rangle \\ &= \frac{1}{2} - \frac{Re(\sum_m \gamma_{00nm}\gamma_{11nm}^* + \gamma_{01nm}\gamma_{10nm}^*)}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2}, \end{aligned} \tag{6}$$

in which $|\phi^-\rangle = (|0\rangle_A|0_n\rangle_B - |1\rangle_A|1_n\rangle_B)/\sqrt{2}$, $|\psi^-\rangle = (|0\rangle_A|1_n\rangle_B - |1\rangle_A|0_n\rangle_B)/\sqrt{2}$ and $Re(x)$ represents the real part of a complex number x. However, Alice and Bob's goal may be $|\phi^-\rangle$, then we can obtain

$$\begin{aligned} e_p^{(n)} &= \langle\phi^+|\rho^{(n)}|\phi^+\rangle + \langle\psi^+|\rho^{(n)}|\psi^+\rangle \\ &= \frac{1}{2} + \frac{Re(\sum_m \gamma_{00nm}\gamma_{11nm}^* + \gamma_{01nm}\gamma_{10nm}^*)}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2}, \end{aligned} \tag{7}$$

similarly, in which $|\psi^+\rangle = (|0\rangle_A|1_n\rangle_B + |1\rangle_A|0_n\rangle_B)/\sqrt{2}$. Therefore, we define the effective phase error rate as

$$e_p^{(n)} = \frac{1}{2} - \frac{\left|Re(\sum_m \gamma_{00nm}\gamma_{11nm}^* + \gamma_{01nm}\gamma_{10nm}^*)\right|}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2}. \tag{8}$$

In the following, we will set $v = \frac{Re(\sum_m \gamma_{00nm}\gamma_{11nm}^* + \gamma_{01nm}\gamma_{10nm}^*)}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2}$ for simplicity. To derive the upper-bound of $e_p^{(n)}$, we must rely on the error rate under 1 basis. Don't forget the $-i\sigma_y$ and $-i\sigma_y^{(n)}$ operations above mentioned, the density matrices when Alice emits $|+\rangle_B = (|0\rangle_B + |1\rangle_B)/\sqrt{2}$ and $|-\rangle_B = (|0\rangle_B - |1\rangle_B)/\sqrt{2}$ are given by:

$$\begin{aligned} \rho_+^{(n)} &= \frac{1}{2(\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2)} \times \\ &[\sum_m P\{(\gamma_{00nm} + \gamma_{10nm})|0_n\rangle_B + (\gamma_{01nm} + \gamma_{11nm})|1_n\rangle_B\} \\ &+ P\{(\gamma_{01nm} - \gamma_{11nm})|0_n\rangle_B - (\gamma_{00nm} - \gamma_{10nm})|1_n\rangle_B\}] \\ \rho_-^{(n)} &= \frac{1}{2(\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2)} \times \\ &[\sum_m P\{(\gamma_{00nm} - \gamma_{10nm})|0_n\rangle_B + (\gamma_{01nm} - \gamma_{11nm})|1_n\rangle_B\} \\ &+ P\{(\gamma_{01nm} + \gamma_{11nm})|0_n\rangle_B - (\gamma_{00nm} + \gamma_{10nm})|1_n\rangle_B\}] \end{aligned} \tag{9}$$

respectively. Note that $\rho^{(n)}$ and its conjugate $\rho^{*(n)}$ will be with same information for Eve and produce key bits with same statistical result by the measurements B_0 and B_1 in the $x-z$ plane. We can assume that $\rho_+^{(n)} \to \rho_+^{(n)}/2 + \rho_+^{*(n)}/2$ and $\rho_-^{(n)} \to \rho_-^{(n)}/2 + \rho_-^{*(n)}/2$, by which we have

$$\rho_+^{(n)} = \begin{pmatrix} \frac{1}{2}+u & v \\ c.c & \frac{1}{2}-u \end{pmatrix} \qquad \rho_-^{(n)} = \begin{pmatrix} \frac{1}{2}-u & -v \\ c.c & \frac{1}{2}+u \end{pmatrix}, \tag{10}$$

where $u = \frac{Re(\sum_m \gamma_{00nm}\gamma_{10nm}^* - \gamma_{01nm}\gamma_{11nm}^*)}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2}$.

Actually, we can simplify above matrices by choosing some proper two orthogonal states $|0'_n\rangle_B$ and $|1'_n\rangle_B$ in the $(x-z)$ plane as z axis instead of $|0_n\rangle_B$ and $|1_n\rangle_B$. Indeed, we can introduce a rotation along y axis, which will lead to relabel $|0_n\rangle_B \to a|0'_n\rangle_B + b|1'_n\rangle_B$, $|1_n\rangle \to b|0'_n\rangle_B - a|1'_n\rangle_B$ where $a^2+b^2=1$, a and b are both real numbers. Note that the coefficients γ should be replaced by γ' in this rotated representation, satisfying $\gamma'_{00nm} = a\gamma_{00nm} + b\gamma_{01nm}$ and etc.. We verify that

$$\begin{aligned}&\frac{Re(\sum_m \gamma'_{00nm}\gamma'^{*}_{10nm} - \gamma'_{01nm}\gamma'^{*}_{11nm})}{\sum_m \left|\gamma'_{00nm}\right|^2 + \left|\gamma'_{11nm}\right|^2 + \left|\gamma'_{01nm}\right|^2 + \left|\gamma'_{10nm}\right|^2} \rightarrow \\ &(a^2-b^2)\frac{Re(\sum_m \gamma_{00nm}\gamma^{*}_{10nm} - \gamma_{01nm}\gamma^{*}_{11nm})}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2} \\ &+ 2ab\frac{Re(\sum_m \gamma_{00nm}\gamma^{*}_{11nm} + \gamma_{01nm}\gamma^{*}_{10nm})}{\sum_m \left|\gamma_{00nm}\right|^2 + \left|\gamma_{11nm}\right|^2 + \left|\gamma_{01nm}\right|^2 + \left|\gamma_{10nm}\right|^2},\end{aligned} \tag{11}$$

which can be 0 by choosing proper a and b. Thus, we conclude that by choosing relevant rotation along y axis, the density matrices when Alice emits $|+\rangle_B$ and $|-\rangle_B$ are simplified as

$$\rho_+^{(n)} = \begin{pmatrix} \frac{1}{2} & v \\ c.c & \frac{1}{2} \end{pmatrix} \quad and \quad \rho_-^{(n)} = \begin{pmatrix} \frac{1}{2} & -v \\ c.c & \frac{1}{2} \end{pmatrix} \tag{12}$$

respectively. In above density matrices and the remaining part of this paper, we only consider this relevant rotated representation, and omit all $'$ notations in γ', $|0'_n\rangle_B$ and $|1'_n\rangle_B$ for simplicity. If the bit error rate in this subspace under 1 basis is $e_{b1}^{(n)}$, according to Holevo bound we have

$$\begin{aligned}&S(\rho_+^{(n)}/2 + \rho_-^{(n)}/2) - S(\rho_+^{(n)})/2 - S(\rho_-^{(n)})/2 \\ &= 1 - H_2(\frac{1}{2} - \left|v\right|) \geqslant 1 - H_2(e_{b1}^{(n)}),\end{aligned} \tag{13}$$

in which S is the von Neumann entropy, H_2 is the Shannon's binary entropy function. Hence, we obtain that

$$\left|v\right| \geqslant \frac{1}{2} - e_{b1}^{(n)}. \tag{14}$$

Note that in this rotated representation, the phase error rate under 0 basis is still written as the form like (8). It reads

$$e_p^{(n)} = \frac{1}{2} - \left|v\right| \leqslant e_{b1}^{(n)}. \tag{15}$$

Hence we have obtained that for any two-dimensional subspace, the upper bound of the phase error under 0 basis is given by the corresponding bit error rate $e_{b1}^{(n)}$ under 1 basis.

Under 0 basis, Bob's measurement B_0 on $\rho^{(n)}$ will output sifted key bits 0 or 1. Recall that the phase error rate $e_p^{(n)}$ decides the Eve's information on Alice's key bits, while the information leakage in the post precessing step relies on the bit error rate $e_{b0}^{(n)}$. For any orthogonal and distinguishable subspace of particle B's Hilbert space, we can conclude that the secure-key rate under 0 basis is given by $R^{(n)} \geqslant 1 - H_2(e_p^{(n)}) - H_2(e_{b0}^{(n)}) = 1 - H_2(e_{b1}^{(n)}) - H_2(e_{b0}^{(n)})$, according to Ref.[11]. Since these subspaces are distinguishable and assuming the probability for successful projection into subspace spanned by $|0_n\rangle_B$ and $|1_n\rangle_B$ is p_n, the overall secure-key rate $R = \sum_n p_n R^{(n)} = 1 - \sum_n p_n H_2(e_{b1}^{(n)}) - p_n H_2(e_{b0}^{(n)}) \geqslant 1 - H_2(e_{b1}) - H_2(e_{b0})$, in which $e_{b1} = \sum_n p_n e_{b1}^{(n)}$ and $e_{b0} = \sum_n p_n e_{b0}^{(n)}$ are the mean bit error rates under 1 basis and 0 basis respectively.

3 Conclusion

Quite interestingly, we have given that the secure-key rate of BB84 protocol with a device-independent receiver, which is the same as the result given in Ref. [17]. However, the uncertainty relation plays the essential role in Ref. [17] while our methods are mainly based on EDP and some lemmas introduced in Ref. [16]. Our discussions elucidate the relation between the DIQKD and the EDP, explain why the secure-key rate in DI context is quite similar to the one in ordinary BB84 protocol and may shed lights on the understanding and future research on quantum key distribution.

Acknowledgements

This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grant No. 60921091 and No. 61101137).

References

1. C. H. Bennett, G.Brassard, Proceedings of *IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, (IEEE, New York, 1984), pp. 175-179.
2. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod.Phys. **74**, 145 (2002).
4. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. 96, 070502 (2006).
5. C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. 98, 010505 (2007).
6. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. 98, 010503 (2007).
7. T. Schmitt-Manderbach et al. Phys.Rev.Lett 98, 010504 (2007).
8. Y. Zhao, B. Qi, X.-F. Ma, H.-K. Lo and L. Qian, Proceedings of IEEE International Symposium on Information Theory 2006, pp. 2094-2098 Z.
9. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
10. Z.-Q. Yin et al., Chin. Phys. Lett. **25**, 3547 (2008).
11. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
12. Y. Zhao, C.-H.F. Fung, B. Qi, C. Chen, and H.-K. Lo, Physical Review A, **78**, 042333 (2008).
13. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 - 689 (2010).
14. H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Physical Review A, **84**, 062308 (2011).
15. A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
16. S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
17. M. Tomamichel, C.C.W. Lim, N. Gisin, and Renato Renner, Nature Communications, **3**, 634 (2012).
18. C. Branciard, E.G. Cavalcanti, S.P. Walborn, V. Scarani, H.M. Wiseman, Physical Review A, **85**, 010301(R) (2012).
19. J.-C. Boileau et al., Phys. Rev. Lett. **94**, 040503 (2005).
20. K. Wen, K. Tamaki, Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009).
21. Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han, and G.-C. Guo, Physical Review A, **82**, 042335 (2010).
22. Z.-Q. Yin, H.-W. Li, Y. Yao, C.-M. Zhang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Physical Review A, **86**, 022313 (2012).