Decoy-state reference-frame-independent quantum key distribution with both source errors and statistical fluctuations

Kang Liu(刘康)[1,2,†], Jian Li(李剑)[1,3,†], Jian-Rong Zhu(朱建荣)[1,2], Chun-Mei Zhang(张春梅)[1,2,‡], and Qin Wang (王琴)[1,2,§]

[1] *Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology of the Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[3] *Department of Physics, Southeast University, Nanjing* 211189, *China*

(Received 6 April 2017; revised manuscript received 2 June 2017; published online 20 October 2017)

Reference-frame-independent quantum key distribution (RFI QKD) can generate secret keys without the alignment of reference frames, which is very robust in real-life implementations of QKD systems. However, the performance of decoy-state RFI QKD with both source errors and statistical fluctuations is still missing until now. In this paper, we investigate the performance of decoy-state RFI QKD in practical scenarios with two kinds of light sources, the heralded single photon source (HSPS) and the weak coherent source (WCS), and also give clear comparison results of decoy-state RFI QKD with WCS and HSPS. Simulation results show that the secret key rates of decoy-state RFI QKD with WCS are higher than those with HSPS in short distance range, but the secret key rates of RFI QKD with HSPS outperform those with WCS in long distance range.

Keywords: quantum key distribution, reference-frame-independent, statistical fluctuations, source errors

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/26/12/120302

1. Introduction

Based on the laws of quantum physics, quantum key distribution (QKD)[1] allows two distant legitimate parties (typically called Alice and Bob) to share unconditionally secure keys, in the presence of the eavesdropper (Eve).[2] Since the first Bennett–Brassard-1984 (BB84) QKD protocol was proposed,[1] many successful QKD works have been achieved during the past decades.[3–15] In most of these experiments, a feedback setup is needed to align the reference frames between Alice and Bob, which will undoubtedly increase the complexity and time cost of QKD systems. Otherwise, the high quantum bit error rate (QBER) will prevent the generation of net secret keys.

Fortunately, reference-frame-independent QKD (RFI QKD) was proposed by Laing *et al.*[16] to avoid the active alignment of reference frames, which can obviously increase the whole communication efficiency between Alice and Bob. After that, a series of theoretical[17–19] and experimental[20–23] works on RFI QKD have been reported. However, none of them considered the practical scenarios including both source errors and statistical fluctuations.

In this paper, we investigate the performance of decoy-state RFI QKD in practical scenarios with two kinds of light sources, the heralded single photon source (HSPS) and the weak coherent source (WCS). The widely used vacuum + weak decoy-state method[24–28] is adopted to combat the photon-number-splitting (PNS) attack[29,30] caused by the multi-photons in the practical sources. Moreover, clear comparison results of decoy-state RFI QKD with WCS and HSPS are given, and simulation results show that the decoy-state RFI QKD even with both source errors and statistical fluctuations is very practical and robust.

2. Decoy-state RFI QKD with both source errors and statistical fluctuations

RFI QKD employs three mutually unbiased bases (Z, X, and Y) to encode the information,[16] which is very similar to the six-state protocol.[31] During the quantum communication phase, Alice randomly prepares quantum states with her local bases X_A, Y_A, and Z_A, and sends them to Bob. Bob randomly measures the received states with his local bases X_B, Y_B, and Z_B. In RFI QKD, the stability of the Z basis can be well maintained, which is also the case in most other QKD systems, while the X and Y bases are allowed to vary slowly.

*Project supported by the National Key Research and Development Program of China (Grant No. 2017YFA0304100), the National Natural Science Foundation of China (Grant Nos. 61475197, 61590932, 11774180, and 61705110), the Natural Science Foundation of the Jiangsu Higher Education Institutions (Grant Nos. 15KJA120002 and 17KJB140016), the Outstanding Youth Project of Jiangsu Province, China (Grant No. BK20150039), the Natural Science Foundation of Jiangsu Province, China (Grant No. BK20170902), and the Science Fund from the Nanjing University of Posts and Telecommunications, China (Grant No. NY217006).

† Kang Liu and Jian Li contributed equally to this work.
‡Corresponding author. E-mail: cmz@njupt.edu.cn
§Corresponding author. E-mail: qinw@njupt.edu.cn

© 2017 Chinese Physical Society and IOP Publishing Ltd

That is, Alice and Bob's Z, X, and Y bases satisfy $Z_B = Z_A$, $X_B = \cos\beta X_A + \sin\beta Y_A$, and $Y_B = \cos\beta Y_A - \sin\beta X_A$, where β is the relative rotation between Alice and Bob's reference frames and may drift with time slowly. After the quantum communication phase, Alice and Bob can distill secret keys from the data in Z_AZ_B basis, and estimate Eve's information from the data in X_AX_B, X_AY_B, Y_AX_B, and Y_AY_B bases. According to the decoy-state method,[26] the total gain and quantum bit error rate (QBER) that Alice sends in ξ_A ($\xi_A \in \{X_A, Y_A, Z_A\}$) and Bob measures them in ξ_B ($\xi_B \in \{X_B, Y_B, Z_B\}$) in the decoy-state RFI QKD can be calculated by

$$Q^{\varepsilon}_{\xi_A\xi_B} = \sum_{i=0}^{\infty} Y^i_{\xi_A\xi_B} P_{\varepsilon}(i), \tag{1}$$

$$E^{\varepsilon}_{\xi_A\xi_B} Q^{\varepsilon}_{\xi_A\xi_B} = \sum_{i=0}^{\infty} e^i_{\xi_A\xi_B} Y^i_{\xi_A\xi_B} P_{\varepsilon}(i), \tag{2}$$

where ε refers to the signal states μ, the decoy states ν, or the vacuum states ω, i denotes the i-photon states, $P_{\varepsilon}(i)$ corresponds to the photon-number distribution for the ε intensity. $e^i_{\xi_A\xi_B}$ ($Y^i_{\xi_A\xi_B}$) denotes the QBER (the yield) of the i-photon states. According to Eqs. (1) and (2), Alice and Bob can estimate the yields (error rates) of single-photon contributions $Y^1_{Z_AZ_B}$, $Y^1_{X_AX_B}$, $Y^1_{X_AY_B}$, $Y^1_{Y_AX_B}$, and $Y^1_{Y_AY_B}$ ($e^1_{Z_AZ_B}$, $e^1_{X_AX_B}$, $e^1_{X_AY_B}$, $e^1_{Y_AX_B}$, and $e^1_{Y_AY_B}$) with the three-intensity decoy-state method. Then, they can estimate the quantity $C = (1-2e^1_{X_AX_B})^2 + (1-2e^1_{X_AY_B})^2 + (1-2e^1_{Y_AX_B})^2 + (1-2e^1_{Y_AY_B})^2$. Finally, Eve's information can be bounded by

$$I_E = (1-e^1_{Z_AZ_B})h\Big(\frac{1+\phi}{2}\Big) + e^1_{Z_AZ_B} h\Big(\frac{1+\varphi}{2}\Big), \tag{3}$$

where

$$\phi = \min\Big[\frac{1}{1-e^1_{Z_AZ_B}}\sqrt{C/2}, 1\Big],$$

and

$$\varphi = \sqrt{C/2 - (1-e^1_{Z_AZ_B})^2\phi^2}\Big/ e^1_{Z_AZ_B}.$$

After the post-processing phase, the final key generation rate in the case of phase-randomized light sources with three-intensity decoy-state method can be calculated by[20]

$$R = Q^{1,\mu}_{Z_AZ_B}(1-I_E) - Q^{\mu}_{Z_AZ_B} f h(E^{\mu}_{Z_AZ_B}), \tag{4}$$

where $Q^{\mu}_{Z_AZ_B}$ ($E^{\mu}_{Z_AZ_B}$) represents the gain (QBER) of the signal states in Z_AZ_B basis, $Q^{1,\mu}_{Z_AZ_B}$ denotes the counting rate of the single-photon pulses from the signal states, h is the binary Shannon information function, and f is the error correction efficiency.

In practice, source errors and statistical fluctuations are inevitable issues in the security analysis of practical decoy-state RFI QKD systems. When considering source errors (for simplicity, we assume the vacuum source is precise which has no source errors), due to the imperfection of practical sources, the intensity of the pulses is not stable. That is to say, ε ranges from $\varepsilon_L(\delta)$ to $\varepsilon_U(\delta)$, where δ refers to the intensity fluctuations. Then, we can obtain the upper bound ($P^U_{\varepsilon}(i)$) and the lower bound ($P^L_{\varepsilon}(i)$) of the i-photon number distribution with intensity fluctuations. Take the WCS for example,

$$\begin{cases} P^U_{\varepsilon}(i) = \mathrm{e}^{-\varepsilon(1-\delta)}, & i = 0, \\ P^L_{\varepsilon}(i) = \mathrm{e}^{-\varepsilon(1+\delta)}, & i = 0, \end{cases} \tag{5}$$

$$\begin{cases} P^U_{\varepsilon}(i) = \dfrac{\mathrm{e}^{-\varepsilon(1+\delta)}(\varepsilon(1+\delta))^i}{i!}, & i \geq 1, \\ P^L_{\varepsilon}(i) = \dfrac{\mathrm{e}^{-\varepsilon(1-\delta)}(\varepsilon(1-\delta))^i}{i!}, & i \geq 1. \end{cases} \tag{6}$$

Then, the upper bounds (the lower bounds) of the total gain and QBER can be obtained respectively as follows:

$$\begin{cases} Q^{\varepsilon}_{\xi_A\xi_B,U} = \sum\limits_{i=1}^{\infty} Y^i_{\xi_A\xi_B} P^U_{\varepsilon}(i) + Y^0_{\xi_A\xi_B} P^U_{\varepsilon}(0), \\ Q^{\varepsilon}_{\xi_A\xi_B,L} = \sum\limits_{i=1}^{\infty} Y^i_{\xi_A\xi_B} P^L_{\varepsilon}(i) + Y^0_{\xi_A\xi_B} P^L_{\varepsilon}(0), \end{cases} \tag{7}$$

$$\begin{cases} E^{\varepsilon}_{\xi_A\xi_B,U} Q^{\varepsilon}_{\xi_A\xi_B,U} = \sum\limits_{i=1}^{\infty} e^i_{\xi_A\xi_B} Y^i_{\xi_A\xi_B} P^U_{\varepsilon}(i) \\ \qquad\qquad + e^0_{\xi_A\xi_B} Y^0_{\xi_A\xi_B} P^U_{\varepsilon}(0), \\ E^{\varepsilon}_{\xi_A\xi_B,L} Q^{\varepsilon}_{\xi_A\xi_B,L} = \sum\limits_{i=1}^{\infty} e^i_{\xi_A\xi_B} Y^i_{\xi_A\xi_B} P^L_{\varepsilon}(i) + e^0_{\xi_A\xi_B} Y^0_{\xi_A\xi_B} P^L_{\varepsilon}(0). \end{cases} \tag{8}$$

Finally, according to Ref. [32], the yield (error rate) of single-photon contributions inZ_AZ_B can be estimated by

$$Y^{1,L}_{Z_AZ_B} = \frac{P^L_{\mu}(2)Q^{\nu}_{Z_AZ_B,L} - P^U_{\nu}(2)Q^{\mu}_{Z_AZ_B,U} - (P^U_{\mu}(2)P^U_{\nu}(0) - P^L_{\nu}(2)P^L_{\mu}(0))Q^{\omega}_{Z_AZ_B}}{P^U_{\nu}(1)P^U_{\mu}(2) - P^L_{\mu}(1)P^L_{\nu}(2)}, \tag{9}$$

$$e^{1,U}_{Z_AZ_B} = \frac{E^{\nu}_{Z_AZ_B,U} Q^{\nu}_{Z_AZ_B,U} - e^0_{Z_AZ_B} P^L_{\nu}(0) Q^{\omega}_{Z_AZ_B}}{P^L_{\nu}(1) Y^{1,L}_{Z_AZ_B}}. \tag{10}$$

The other parameters $Y^{1,L}_{X_AX_B}$, $Y^{1,L}_{X_AY_B}$, $Y^{1,L}_{Y_AX_B}$, and $Y^{1,L}_{Y_AY_B}$ ($e^{1,U}_{X_AX_B}$, $e^{1,U}_{X_AY_B}$, $e^{1,U}_{Y_AX_B}$, and $e^{1,U}_{Y_AY_B}$) can be obtained analogously by applying the same method. According to the statistical fluctuations analysis theory,[33–35] the total gain and quantum bit error should be modified as follows:

$$Q^{\varepsilon,U}_{\xi_A\xi_B} = Q^{\varepsilon}_{\xi_A\xi_B}\left(1 + \frac{\gamma}{\sqrt{NP_{\varepsilon}P_{\xi_A|\varepsilon}P_{\xi_B}}}\right), \tag{11}$$

$$Q^{\varepsilon,L}_{\xi_A\xi_B} = Q^{\varepsilon}_{\xi_A\xi_B}\left(1 - \frac{\gamma}{\sqrt{NP_{\varepsilon}P_{\xi_A|\varepsilon}P_{\xi_B}}}\right), \tag{12}$$

$$E^{\nu,U}_{\xi_A\xi_B} Q^{\nu,U}_{\xi_A\xi_B} = E^{\nu}_{\xi_A\xi_B} Q^{\nu}_{\xi_A\xi_B}$$

$$\cdot\left(1+\frac{\gamma}{\sqrt{E^{\nu}_{\xi_A\xi_B}Q^{\nu}_{\xi_A\xi_B}NP_{\varepsilon}P_{\xi_A|\varepsilon}P_{\xi_B}}}\right), \quad (13)$$

where P_{ε} represents the probability that Alice randomly modulates pulses into the ε intensity, $P_{\xi_A|\varepsilon}$ denotes the conditional probability that Alice sends the states to Bob in ξ_A basis with the ε intensity, P_{ξ_B} refers to the probability that Bob chooses the ξ_B basis for his measurement, γ is the number of standard deviation, and N refers to the total number of pulses.

3. Numerical simulations

In order to explore the performance of the above decoy-state RFI-QKD scheme under practical experimental conditions, we use two kinds of light sources, e.g., WCS[3,4] and HSPS,[27,28] as examples and carry out the corresponding numerical simulations.

For the WCS, it has a Poisson distribution: $P^i_{\varepsilon} = (\varepsilon^i/i!)\mathrm{e}^{-\varepsilon}$, $(i \in (1,2,3,\ldots))$, while for the HSPS, it follows a sub-Poisson distribution: $P^i_{\varepsilon} = [1-(1-d_A)(1-\eta_A)^i](\varepsilon^i/i!)\mathrm{e}^{-\varepsilon}$, where η_A and d_A each correspond to the detection efficiency and the dark count rate of the local detector at Alice's side.

In all the simulation results presented below, we use the following parameters: $\nu = 0.01$, $\omega = 0$, $P_{\mu} = 1/2$, $P_{\nu} = P_{\omega} = 1/4$, and $P_{X_A} = P_{Y_A} = P_{Z_A} = P_{X_B} = P_{Y_B} = P_{Z_B} = 1/3$. Moreover, we set the misalignment of the reference frames as $\beta = \pi/7$ (in fact, β is unknown and we just use it to simulate a practical RFI-QKD system). Other parameters used in the simulation are listed in Table 1. For each line, the intensity of the signal states is optimized at each distance to maximize the final key rate.

Table 1. Simulation parameters for the three-intensity decoy-state RFI QKD with both source errors and statistical fluctuations. η_d (Y_0) is the detection efficiency (the dark count rate) of Bob's single photon detectors, e_d is the probability that Bob's single-photon detector is clicked incorrectly. α denotes the loss coefficient of the standard fiber link, γ is the number of the standard deviation when considering statistical fluctuations (here 5.3 corresponds to a failure probability of 10^{-7}), and f is the error correction efficiency. η_A (d_A) is the detection efficiency (the dark count rate) of Alice's single photon detector with HSPS.

η_d	e_d	Y_0	α/(dB/km)	η_A	d_A	γ	f
14.5%	1.5%	3×10^{-6}	0.2	0.75	1×10^{-6}	5.3	1.16

First, we study the performance of the decoy-state RFI QKD with standard statistical fluctuations, and the corresponding results are shown in Fig. 1. In Fig. 1, W (H) denotes WCS (HSPS), and the solid (dashed) curves from left to right correspond to the secret key rates of the decoy-state RFI QKD with WCS (HSPS) at $N = 10^9$, 10^{10}, and 10^{11}, respectively. From Fig. 1, it can be easily seen that the secret key rates of WCS are higher than those of HSPS in short distance range, but the key rates of HSPS outperform WCS in long distance range.

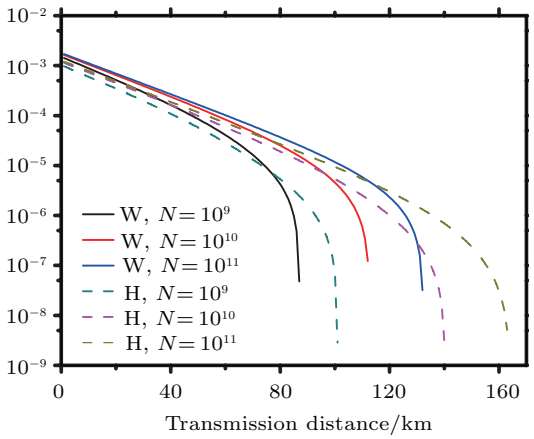


Fig. 1. (color online) Comparison results of the decoy-state RFI QKD with WCS and HSPS when considering statistical fluctuations. The solid (dashed) curves from left to right refer to the secret key rates of the decoy-state RFI QKD using WCS (HSPS) with $N = 10^9$, 10^{10}, and 10^{11}, respectively.

Then, we consider the effect of different source errors in the decoy-state RFI QKD with statistical fluctuations ($N = 10^{10}$), and the simulation results are shown in Fig. 2. Here, W (H) denotes WCS (HSPS), and the solid (dashed) curves from left to right in Fig. 2 denote the key rates of WCS (HSPS) with source errors $\delta = 0.04$, 0.02, and 0, individually. From Fig. 2, we find that the secret key rate declines with the increasing of source errors for both HSPS and WCS. Moreover, RFI QKD with WCS shows better performance than the one using HSPS at short distance range (< 80 km), and presents lower secret key rate than the one using HSPS at long distance range (> 110 km).

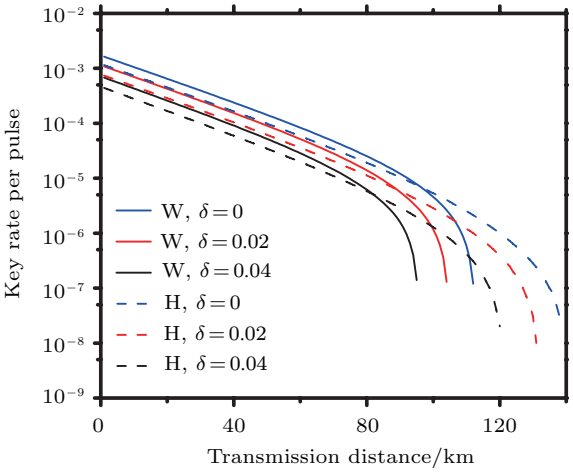


Fig. 2. (color online) Comparison results of the decoy-state RFI QKD with source errors when the number of sent pulses is $N = 10^{10}$. The solid (dashed) curves from left to right denote the secret key rates of the decoy-state RFI QKD with WCS (HSPS) with $\delta = 0.04$, 0.02, and 0, respectively.

Finally, the optimal intensities of signal states and the corresponding key rates at 60 km with statistical fluctuations and with both statistical fluctuations and source errors are shown in Table 2 and Table 3.

Table 2. The optimal intensities of signal states and corresponding key rates at 60 km with statistical fluctuations.

Par	W			H		
	$N = 10^9$	$N = 10^{10}$	$N = 10^{11}$	$N = 10^9$	$N = 10^{10}$	$N = 10^{11}$
μ	0.539	0.653	0.684	0.482	0.596	0.629
R	4.080×10^{-5}	8.327×10^{-5}	1.017×10^{-4}	2.873×10^{-5}	5.858×10^{-5}	7.182×10^{-5}

Table 3. The optimal intensities of signal states and corresponding key rates at 60 km with both statistical fluctuations and source errors.

Par	W			H		
	$\delta = 0$	$\delta = 0.02$	$\delta = 0.04$	$\delta = 0$	$\delta = 0.02$	$\delta = 0.04$
μ	0.653	0.626	0.566	0.596	0.554	0.482
R	8.327×10^{-5}	5.163×10^{-5}	2.855×10^{-5}	5.858×10^{-5}	3.598×10^{-5}	1.981×10^{-5}

4. Conclusions

In conclusion, RFI QKD can generate secret keys without alignment of reference frames, which exhibits obvious superiority in real-life QKD systems. Considering both source errors and statistical fluctuations, we studied the performance of the decoy-state RFI QKD with two kinds of practical sources, e.g., WCS and HSPS. Simulation results demonstrate that the secret key rates of the decoy-state RFI QKD with WCS are higher than those with HSPS in a short distance range, but the secret key rates of RFI QKD with HSPS outperform those with WCS in a long distance range. Our work will provide useful guidance in practical implementations of RFI QKD systems.

References

[1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–79
[2] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[4] Peng C Z, Zhang J, Yang D, Gao W B, Ma H X, Yin H and Pan J W 2007 *Phys. Rev. Lett.* **98** 010505
[5] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503
[6] Schmitt M T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T and Zeilinger A 2007 *Phys. Rev. Lett.* **98** 010504
[7] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[8] Yuan Z L, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **90** 011118
[9] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L and Guo G C 2008 *Chin. Phys. Lett.* **25** 3547
[10] Fröhlich B and Yuan Z L 2015 *Nat. Photon.* **9** 781
[11] Wang S, Chen W and Yin Z Q 2014 *Opt. Express* **22** 21739
[12] Wang S, Chen W and Guo J F 2012 *Opt. Lett.* **37** 1008
[13] Li F Y, Wang D, Wang S, Li M, Yin Z Q, Li H W, Chen W and Han Z F 2014 *Chin. Phys. B.* **23** 124201
[14] Zhang Y, Wang S, Yin Z Q, Chen W, Liang W Y, Li H W, Guo G C and Han Z F 2012 *Chin. Phys. B* **21** 100307
[15] He D Y, Wang S and Chen W 2017 *Appl. Phys. Lett.* **110** 111104
[16] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev. A* **82** 012304
[17] Wang C, Sun S H, Ma X C, Tang G Z and Liang L M 2015 *Phys. Rev. A* **92** 042319
[18] Yin Z Q, Wang S, Chen W, Li H W, Guo G C and Han Z F 2014 *Quantum Inf. Process.* **13** 1237
[19] Zhang C M, Zhu J R and Wang Q 2017 *Phys. Rev. A.* **95** 032309
[20] Liang W Y, Wang S, Li H W, Yin Z Q, Chen W, Yao Y and Han Z F 2014 *Sci. Rep.* **4** 3617
[21] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502
[22] Zhang P, Aungskunsiri K, Martín-López E, Wabnig J, Lobino M, Nock R W and Laing A 2014 *Phys. Rev. Lett.* **112** 130501
[23] Wabnig J, Bitauld D, Li H W, Laing A, O'Brien, J L and Niskanen A O 2013 *New J. Phys.* **15** 073001
[24] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[25] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[26] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[27] Wang Q, Wang X B and Guo G C 2007 *Phys. Rev. A* **75** 012312
[28] Wang Q, Wang X B, Björk G and Karlsson A 2007 *Europhys. Lett.* **79** 40001
[29] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863
[30] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[31] Bruss D 1998 *Phys. Rev. Lett.* **81** 3018
[32] Zhou Y H, Yu Z W and Wang X B 2014 *Phys. Rev. A* **89** 052325
[33] Wang X B, Peng C Z and Zhang J 2008 *Phys. Rev. A* **77** 042311
[34] Wang X B, Yang L, Peng C Z and Pan J C 2009 *New J. Phys.* **11** 075006
[35] Wang S, Zhang S L, Li H W, Yin Z Q, Zhao Y B, Chen W, Han Z F and Guo G C 2009 *Phys. Rev. A* **79** 062309