Lower bound for the security of differential phase shift quantum key distribution against a one-pulse-attack*

Li Hong-Wei(李宏伟)[a)b)], Yin Zhen-Qiang(银振强)[a)†], Wang Shuang(王 双)[a)], Bao Wan-Su(鲍皖苏)[b)], Guo Guang-Can(郭光灿)[a)], and Han Zheng-Fu(韩正甫)[a)‡]

[a)] *Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei* 230026, *China*

[b)] *Electronic Technology Institute, Information Engineer University, Zhengzhou* 450004, *China*

(Received 11 February 2011; revised manuscript received 28 April 2011)

Quantum key distribution is the art of sharing secret keys between two distant parties, and has attracted a lot of attention due to its unconditional security. Compared with other quantum key distribution protocols, the differential phase shift quantum key distribution protocol has higher efficiency and simpler apparatus. Unfortunately, the unconditional security of differential phase shift quantum key distribution has not been proved. Utilizing the sharp continuity of the von Neuman entropy and some basic inequalities, we estimate the upper bound for the eavesdropper Eve's information. We then prove the lower bound for the security of the differential phase shift quantum key distribution protocol against a one-pulse attack with Devatak–Winter's secret key rate formula.

Keywords: lower bound, differential phase shift, quantum key distribution

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/20/10/100306

1. Introduction

Since the unconditional security of quantum key distribution (QKD) can be guaranteed by the physical principle, it has attracted much attention. The QKD protocol can be divided into discrete-variable protocols, continuous-variable protocols, and distributed-phase reference protocols, all of which have made rapid progress both theoretically and experimentally.[1−3] The differential phase shift QKD (DPS-QKD) protocol was proposed by Inoue, Waks, and Yamamoto in 2002.[4,5] Since the DPS-QKD protocol has high communication efficiency and simple apparatus,[6] it has attracted much attention in recent years. In practical experiments, Takesue *et al.* have reported experimental realization over 200 km with superconducting single-photon detectors.[7] However, the unconditional security of the DPS-QKD protocol with a weak coherent source under the most general coherent attack has not been proved. The unconditional security of the DPS-QKD protocol against individual attacks was proved by Waks *et al.*,[8] and that of a single-photon-source DPS-QKD protocol against the most general coherent attack was proved by Wen *et al.*[9] More recently, upper bounds for the security of a weak coherent source DPS-QKD protocol against a one-pulse attack were analysed by Branciard *et al.*,[10] but the security analysis can only be satisfied in the long-distance case. In this paper, we will give the lower bound for the security of a weak coherent source DPS-QKD protocol against a one-pulse attack with photon-number-resolved detectors.

In the DPS-QKD protocol, the transmitter, Alice, generates a train of weak coherent pulses, which are randomly modulated by 0 or π phases and sent over the quantum channel to the receiver, Bob. After passing through Bob's interferometer, the detector records a detection depending on consecutive pulse interference. In the one-pulse-attack protocol, the eavesdropper, Eve, will interact with each pulse with the same strategy. We suppose that Bob has a photon-number-resolved detector; then only a single-photon state on Bob's side can be used to generate the final secret key in our security analysis.

Applying Devetak–Winter's secret key rate bound,[11] we will analyse the security of the DPS-

*Project supported by the National Fundamental Research Program of China (Grant No. 2006CB921900), National Natural Science Foundation of China (Grant Nos. 60537020 and 60621064), and the Innovation Funds of the Chinese Academy of Sciences.

†Corresponding author. E-mail: yinzheqi@mail.ustc.edu.cn

‡Corresponding author. E-mail: zfhan@ustc.edu.cn

© 2011 Chinese Physical Society and IOP Publishing Ltd

QKD protocol against a one-pulse attack,

$$R = r_{\rm sift}[1 - h(Err) - \chi_{AE}], \tag{1}$$

where

$$\begin{aligned} &r_{\rm sift} = (1 - {\rm e}^{-\mu t\eta}),\\ &\chi_{AE} = S(\rho_E) - \frac{1}{2}S(\rho_E^{A=0}) - \frac{1}{2}S(\rho_E^{A=1}), \end{aligned} \tag{2}$$

$r_{\rm sift}$ is the sift efficiency of the protocol, χ_{AE} is the Holevo bound, which estimates the upper bound of the eavesdropper's information, μ is the mean photon number of the weak coherent photon source on Alice's side, t is the transmission coefficient about the quantum channel, η is the detection efficiency on Bob's side, h is the binary entropy function, Err is the quantum bit error rate estimated by Alice and Bob, $\rho_E^{A=0}$ ($\rho_E^{A=1}$) is Eve's quantum state in the case of Alice's classical bit being 0(1), and $\rho_E = \frac{1}{2}\rho_E^{A=0} + \frac{1}{2}\rho_E^{A=1}$ is Eve's quantum state without considering Alice's classical bit.

2. Lower bound for the security of the DPS-QKD protocol against a one-pulse attack with photon-number-resolved detectors

The most general unitary transformation considering the one-pulse attack can be given as follows:

$$\begin{aligned} &U|\sqrt{\mu}\rangle_A|0\rangle_E\\ &= \sqrt{\sigma_1}(\sqrt{Q}|0\rangle_B|v_0\rangle_E + \sqrt{1-Q}|1\rangle_B|p_0\rangle_E)\\ &\quad + \sqrt{1-\sigma_1}\sum_{i=2}^{\infty}\sqrt{q_i}|i\rangle_B|q_i\rangle_E,\\ &U|-\sqrt{\mu}\rangle_A|0\rangle_E\\ &= \sqrt{\sigma_2}(\sqrt{Q}|0\rangle_B|v_1\rangle_E - \sqrt{1-Q}|1\rangle_B|p_1\rangle_E)\\ &\quad + \sqrt{1-\sigma_2}\sum_{i=2}^{\infty}\sqrt{t_i}|i\rangle_B|t_i\rangle_E, \end{aligned} \tag{3}$$

where, $|v_{0/1}\rangle_E$, $|p_{0/1}\rangle_E$, $|q_i\rangle_E$, and $|t_i\rangle_E$ are quantum states to which Eve attaches Bob's system, and $0 \le \sigma_1 \le 1$ ($0 \le \sigma_2 \le 1$) is the probability that Bob obtains the vacuum or single photon state when the quantum state $|\sqrt{\mu}\rangle_A$ ($|-\sqrt{\mu}\rangle_A$) has been transmitted by Alice. The $q_i, t_i \quad i = 2, \ldots, \infty$ are positive real numbers, which should be satisfied by $\sum_{i=2}^{\infty} q_i = \sum_{i=2}^{\infty} t_i = 1$. After this unitary transformation, the quantum state transmitted in the quantum channel can be given as the following four cases:

$$\begin{aligned} &|\sqrt{\mu},\sqrt{\mu}\rangle_A|0,0\rangle_E\\ &\to |0,1\rangle_B|v_0,p_0\rangle_E + |1,0\rangle_B|p_0,v_0\rangle_E\\ &= (|0,1\rangle_B + |1,0\rangle_B)|D_0\rangle_E + (|0,1\rangle_B - |1,0\rangle_B)|D_1\rangle_E, \end{aligned} \tag{4a}$$

$$\begin{aligned} &|-\sqrt{\mu},-\sqrt{\mu}\rangle_A|0,0\rangle_E\\ &\to |0,1\rangle_B|v_1,p_1\rangle_E + |1,0\rangle_B|p_1,v_1\rangle_E\\ &= (|0,1\rangle_B + |1,0\rangle_B)|D_0'\rangle_E + (|0,1\rangle_B - |1,0\rangle_B)|D_1'\rangle_E, \end{aligned} \tag{4b}$$

$$\begin{aligned} &|\sqrt{\mu},-\sqrt{\mu}\rangle_A|0,0\rangle_E\\ &\to |0,1\rangle_B|v_0,p_1\rangle_E - |1,0\rangle_B|p_0,v_1\rangle_E\\ &= (|0,1\rangle_B + |1,0\rangle_B)|E_0\rangle_E + (|0,1\rangle_B - |1,0\rangle_B)|E_1\rangle_E, \end{aligned} \tag{4c}$$

$$\begin{aligned} &|-\sqrt{\mu},\sqrt{\mu}\rangle_A|0,0\rangle_E\\ &\to |0,1\rangle_B|v_1,p_0\rangle_E + |1,0\rangle_B|p_1,v_0\rangle_E\\ &= (|0,1\rangle_B + |1,0\rangle_B)|E_0'\rangle_E + (|0,1\rangle_B - |1,0\rangle_B)|E_1'\rangle_E, \end{aligned} \tag{4d}$$

where,

$$|D_0\rangle_E = \frac{1}{2}(|v_0,p_0\rangle_E + |p_0,v_0\rangle_E), \tag{5a}$$

$$|D_1\rangle_E = \frac{1}{2}(|v_0,p_0\rangle_E - |p_0,v_0\rangle_E), \tag{5b}$$

$$|D_0'\rangle_E = \frac{1}{2}(|v_1,p_1\rangle_E + |p_1,v_1\rangle_E), \tag{5c}$$

$$|D_1'\rangle_E = \frac{1}{2}(|v_1,p_1\rangle_E - |p_1,v_1\rangle_E), \tag{5d}$$

$$|E_0\rangle_E = \frac{1}{2}(|v_0,p_1\rangle_E - |p_0,v_1\rangle_E), \tag{5e}$$

$$|E_1\rangle_E = \frac{1}{2}(|v_0,p_1\rangle_E + |p_0,v_1\rangle_E), \tag{5f}$$

$$|E_0'\rangle_E = \frac{1}{2}(|v_1,p_0\rangle_E - |p_1,v_0\rangle_E), \tag{5g}$$

$$|E_1'\rangle_E = \frac{1}{2}(|v_1,p_0\rangle_E + |p_1,v_0\rangle_E). \tag{5h}$$

Utilizing the photon-number-resolved detector, Bob can discard the vacuum state and multi-photon state in Eqs. (4a)–(4d). Suppose that Alice's quantum states $|\sqrt{\mu},\sqrt{\mu}\rangle_A$, $|-\sqrt{\mu},-\sqrt{\mu}\rangle_A$, $|\sqrt{\mu},-\sqrt{\mu}\rangle_A$, and $|-\sqrt{\mu},\sqrt{\mu}\rangle_A$ have the same quantum bit error rate in the classical step (Alice and Bob can discard other cases), we can obtain the following condition by considering Eqs. (5a)–(5h)

$$||D_0\rangle_E|^2 = \frac{1}{2}(1 + |\langle p_0|v_0\rangle|^2) = 1 - Err, \tag{6a}$$

$$||D_1\rangle_E|^2 = \frac{1}{2}(1 - |\langle p_0|v_0\rangle|^2) = Err, \tag{6b}$$

$$||D_0'\rangle_E|^2 = \frac{1}{2}(1 + |\langle p_1|v_1\rangle|^2) = 1 - Err, \tag{6c}$$

$$||D_1'\rangle_E|^2 = \frac{1}{2}(1 - |\langle p_1|v_1\rangle|^2) = Err, \quad (6d)$$

$$||E_0\rangle_E|^2 = \frac{1}{2}(1 - \mathrm{Re}\langle v_0|p_0\rangle\langle p_1|v_1\rangle) = Err, \quad (6e)$$

$$||E_1\rangle_E|^2 = \frac{1}{2}(1 + \mathrm{Re}\langle v_0|p_0\rangle\langle p_1|v_1\rangle) = 1 - Err, \quad (6f)$$

$$||E_0'\rangle_E|^2 = \frac{1}{2}(1 - \mathrm{Re}\langle v_1|p_1\rangle\langle p_0|v_0\rangle) = Err, \quad (6g)$$

$$||E_1'\rangle_E|^2 = \frac{1}{2}(1 + \mathrm{Re}\langle v_1|p_1\rangle\langle p_0|v_0\rangle) = 1 - Err. \quad (6h)$$

Estimating the upper bound of Eve's information is the main difficulty in our security analysis. We can suppose that Alice and Bob have two raw key sets about the measurement outcomes. The first set is the raw key generated by quantum states $|\sqrt{\mu}, \sqrt{\mu}\rangle_A$ and $|\sqrt{\mu}, -\sqrt{\mu}\rangle_A$, and the second set is the raw key generated by quantum states $|-\sqrt{\mu}, -\sqrt{\mu}\rangle_A$ and $|-\sqrt{\mu}, \sqrt{\mu}\rangle_A$. Further, Alice and Bob will choose different classical protocols (error correction and privacy amplification) by considering two respective sets. In this paper, we will only consider the first set in our security analysis; the second set can be analysed similarly. More precisely, we will give Eve's density matrix by considering the unitary transformation in Eqs. (4a)–(4d) as follows:

$$\rho_E^{A=0} = (1 - Err)|\tilde{D}_0\rangle\langle\tilde{D}_0| + Err|\tilde{D}_1\rangle\langle\tilde{D}_1|, \quad (7a)$$

$$\rho_E^{A=1} = (1 - Err)|\tilde{E}_1\rangle\langle\tilde{E}_1| + Err|\tilde{E}_0\rangle\langle\tilde{E}_0|, \quad (7b)$$

$$\rho_E = \frac{1}{2}[(1 - Err)|\tilde{D}_0\rangle\langle\tilde{D}_0| + Err|\tilde{D}_1\rangle\langle\tilde{D}_1| + (1 - Err)|\tilde{E}_1\rangle\langle\tilde{E}_1| + Err|\tilde{E}_0\rangle\langle\tilde{E}_0|], \quad (7c)$$

where,

$$|D_0\rangle = \sqrt{1 - Err}|\tilde{D}_0\rangle, \quad |D_1\rangle = \sqrt{Err}|\tilde{D}_1\rangle, \quad (8a)$$

$$|E_0\rangle = \sqrt{Err}|\tilde{E}_0\rangle, \quad |E_1\rangle = \sqrt{1 - Err}|\tilde{E}_1\rangle. \quad (8b)$$

For estimating the upper bound of Eve's information $S(\rho_E)$, we will define a new quantum density matrix ρ_E',

$$\rho_E' \equiv \frac{1}{2}|\tilde{D}_0\rangle\langle\tilde{D}_0| + \frac{1}{2}|\tilde{E}_1\rangle\langle\tilde{E}_1|. \quad (9)$$

Utilizing the strong convexity of the trace distance,[12] we can obtain the upper bound of the trace distance between the density matrix ρ_E and ρ_E',

$$D(\rho_E, \rho_E') \leq Err. \quad (10)$$

Applying the sharp continuity of the von Neumann entropy,[13] we can obtain the information distance between the von Neuman entroy $S(\rho_E)$ and $S(\rho_E')$,

$$\begin{aligned} &|S(\rho_E) - S(\rho_E')| \\ &\leq D(\rho_E, \rho_E')\log_2(d-1) + h(D(\rho_E, \rho_E')), \end{aligned} \quad (11)$$

where $d = 16$ is the dimension of Eve's density matrix. With the definition of the von Neumann entropy and some of its basic properties,[12] $S(\rho_E^{A=0})$ and $S(\rho_E^{A=1})$ can be simply estimated by

$$S(\rho_E^{A=0}) = h(Err), \quad (12a)$$

$$S(\rho_E^{A=1}) \geq 0. \quad (12b)$$

Similarly, the von Neumann entropy $S(\rho_E')$ can be calculated by

$$\begin{aligned} S(\rho_E') &= h\left(\frac{1 - |\langle\tilde{D}_0|\tilde{E}_1\rangle|^2}{2}\right) \\ &= h\left(\frac{1 - |\langle D_0|E_1\rangle|^2/(1 - Err)^2}{2}\right), \end{aligned} \quad (13)$$

where,

$$\begin{aligned} \langle D_0|E_1\rangle &= \frac{1}{4}(\langle p_0|p_1\rangle + \langle v_0|v_1\rangle + \langle v_0|p_0\rangle\langle p_0|v_1\rangle \\ &\quad + \langle v_0|p_1\rangle\langle p_0|v_0\rangle). \end{aligned} \quad (14)$$

To estimate the lower bound of $|\langle D_0|E_1\rangle|$, we will give some conditions for which the unitary transformation should be satisfied. Applying the unitary requirement in Eq. (3), we can obtain the following condition:

$$\begin{aligned} &\langle\mu|UU^\dagger|\sqrt{-\mu}\rangle \\ &= \mathrm{e}^{-2\mu} \\ &\leq \sqrt{\sigma_1\sigma_2}(Q|\langle v_0|v_1\rangle| + (1 - Q)|\langle p_0|p_1\rangle|) \\ &\quad + \sqrt{(1 - \sigma_1)(1 - \sigma_2)}. \end{aligned} \quad (15)$$

More precisely, this equation can be transformed into the following expression:

$$\begin{aligned} &|\langle p_0|p_1\rangle|_{\min} \\ &\geq \frac{[\mathrm{e}^{-2\mu} - \sqrt{(1 - \sigma_1)(1 - \sigma_2)}]/\sqrt{\sigma_1\sigma_2} - Q}{1 - Q}. \end{aligned} \quad (16)$$

Applying Eq. (6), we can obtain the following expression:

$$\begin{aligned} &|\langle v_0|p_0\rangle| = |\langle v_1|p_1\rangle| = \sqrt{1 - 2Err}, \\ &Re\langle v_0|p_0\rangle\langle p_1|v_1\rangle = 1 - 2Err. \end{aligned} \quad (17)$$

Applying Eqs. (16) and (17), we can estimate the lower bound of $|\langle D_0|E_1\rangle|$ in Eq. (14); a detailed analysis will be given in Appendix A. Correspondingly, combining Eqs. (1), (10)–(13) with Eq. (14), we can obtain the lower bound for the final secret key rate as

$$\begin{aligned} &R \\ &= (1 - \mathrm{e}^{-\mu t\eta}) \end{aligned}$$

$$\times \left[1 - \frac{3}{2}h(Err) - h\left[\frac{1 - |\langle D_0|E_1\rangle|^2/(1-Err)^2}{2}\right] - Err\log_2(15)\right]. \quad (18)$$

Utilizing the security analysis result, we will give, in Fig. 1, the final secret key rate with different quantum bit error rate by considering some special security parameters, and the optimal mean photon number μ with different quantum bit error rate will be given in Fig. 2.

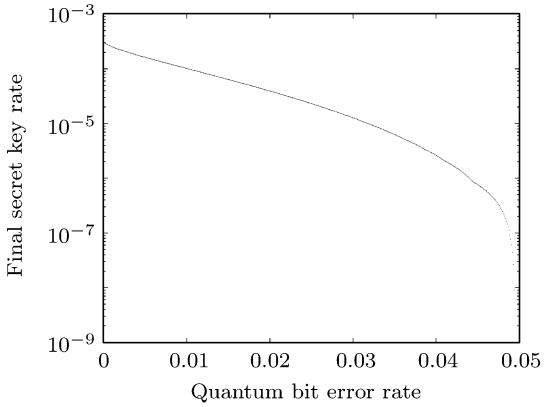


Fig. 1. Lower bound for the security of the differential phase shift quantum key distribution protocol against a one-pulse attack with optimal mean photon number μ. The parameters in our calculation are $t = 0.1$, $\eta = 0.1$, $Q = 0.1$, $\sigma_1 = \sigma_2 = 0$.

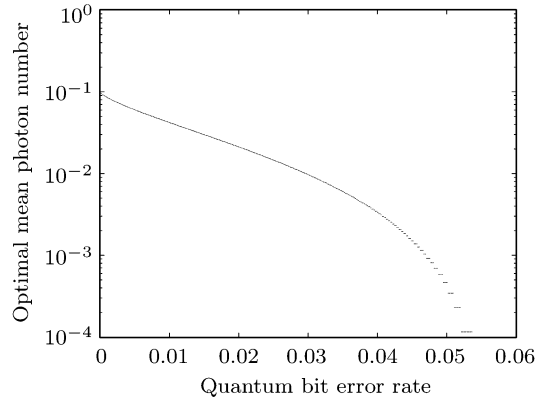


Fig. 2. Optimal mean photon number μ with different quantum bit error rate. The parameters in our calculation are $t = 0.1$, $\eta = 0.1$, $Q = 0.1$, $\sigma_1 = \sigma_2 = 0$.

3. Conclusion

We have analysed the unconditional security of differential phase shift quantum key distribution against a one-pulse attack by considering that there are photon-number-resolved detectors on the receiver's side. The security analysis result can be applied in practical experiments. Future work will attemot to prove the unconditional security of the DPS-QKD protocol against the most general coherent attack.

Appendix A

Applying Eq. (17), we can give the following expression:

$$\begin{aligned} |v_0\rangle &= x|p_0\rangle + y|p_0^{\perp}\rangle, \\ |v_1\rangle &= x'|p_1\rangle + y'|p_1^{\perp}\rangle, \end{aligned} \quad (A1)$$

where, x, x', y, and y' are complex numbers, which can be satisfied by the following equations:

$$\begin{aligned} &|x| = |x'| = \sqrt{1-2Err}, \\ &|y| = |y'| = \sqrt{2Err}, \\ &\mathrm{Re}(x'x^*) = 1 - 2Err, \\ &x^* = \sqrt{1-2Err}(\cos(\theta) + \mathrm{i}\sin(\theta)), \\ &x' = \sqrt{1-2Err}(\cos(\varphi) + \mathrm{i}\sin(\varphi)), \end{aligned} \quad (A2)$$

where, $0 \le \theta \le \pi$ and $0 \le \varphi \le \pi$ are arbitrary real values; then we can obtain

$$\begin{aligned} \mathrm{Re}(x'x^*) &= (1-2Err)(\cos(\theta\cos(\varphi) \\ &\quad + \sin(\theta)\sin(\varphi))), \\ \theta &= \varphi, \\ x^* &= x'. \end{aligned} \quad (A3)$$

Combining Eq. (14) with Eq. (A3), we can obtain

$$\begin{aligned} |\langle D_0|E_1\rangle| &= \frac{1}{4}|(\langle p_0|p_1\rangle + \langle v_0|v_1\rangle + \langle v_0|p_0\rangle\langle p_0|v_1\rangle + \langle v_0|p_1\rangle\langle p_0|v_0\rangle)| \\ &= \frac{1}{4}|\langle p_0|p_1\rangle + x^*x'\langle p_0|p_1\rangle + x^*y'\langle p_0|p_1^{\perp}\rangle + y^*x'\langle p_0^{\perp}|p_1\rangle + y^*y'\langle p_0^{\perp}|p_1^{\perp}\rangle + x^*x'\langle p_0|p_1\rangle + x^*y'\langle p_0|p_1^{\perp}\rangle \\ &\quad + xx^*\langle p_0|p_1\rangle + xy^*\langle p_0^{\perp}|p_1\rangle| \\ &\ge (1+3|x|^2)|\langle p_0|p_1\rangle|_{\min} - |x^*y'\langle p_0|p_1^{\perp}\rangle + y^*x'\langle p_0^{\perp}|p_1\rangle + x^*y'\langle p_0|p_1^{\perp}\rangle + xy^*\langle p_0^{\perp}|p_1\rangle| \\ &\quad + |y^*y'\langle p_0^{\perp}|p_1^{\perp}\rangle| \\ &\ge \frac{1}{4}\{\ge (1+3(1-2Err))|\langle p_0|p_1\rangle|_{\min} - (4\sqrt{1-2Err}\sqrt{2Err})\sqrt{1-|\langle p_0|p_1\rangle|_{\min}^2} - 2Err\} \end{aligned}$$

$$\geq \frac{1}{4}\Bigg\{(1+3(1-2Err))\left\{\frac{[\mathrm{e}^{-2\mu}-\sqrt{(1-\sigma_1)/(1-\sigma_2)}]/\sqrt{\sigma_1\sigma_2}-Q}{1-Q}\right\}$$
$$-(4\sqrt{1-2Err}\sqrt{2Err})\sqrt{1-\left\{\frac{[\mathrm{e}^{-2\mu}-\sqrt{(1-\sigma_1)(1-\sigma_2)}]/\sqrt{\sigma_1\sigma_2}-Q}{1-Q}\right\}^2}-2Err\Bigg\}, \quad \text{(A4)}$$

where we utilize the triangle inequality and the following inequalities:

$$|\langle p_0|p_1^{\perp}\rangle|^2+|\langle p_0|p_1\rangle|^2\leq 1,$$
$$|\langle p_0^{\perp}|p_1\rangle|^2+|\langle p_0|p_1\rangle|^2\leq 1,$$
$$|\langle p_0^{\perp}|p_1^{\perp}\rangle|^2\leq 1. \quad \text{(A5)}$$

References

[1] Xu F X, Wang S, Han Z F and Guo G C 2010 *Chin. Phys.* B **19** 100312

[2] Liu Y, Wu Q L, Han Z F, Dai Y M and Guo G C 2010 *Chin. Phys.* B **19** 080308

[3] Wang H, Yan L S, Pan W, Luo B, Guo Z and Xu M F 2011 *Acta Phys. Sin.* **60** 020304 (in Chinese)

[4] Inoue K, Waks E and Yamamoto Y 2003 *Phys. Rev. Lett.* **89** 037902

[5] Inoue K, Waks E and Yamamoto Y 2003 *Phys. Rev.* A **68** 022317

[6] Jiao R Z, Feng C X and Ma H Q 2009 *Chin. Phys.* B **18** 915

[7] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nature Photonics* **1** 343

[8] Waks E, Takesue H and Yamamoto Y 2006 *Phys. Rev.* A **73** 012344

[9] Wen K, Tamaki K and Yamamoto Y 2009 *Phys. Rev. Lett.* **103** 170503

[10] Branciard C, Gisin N and Scarani V 2008 *New J. Phys.* **10** 013031

[11] Devetak I and Winter A 2005 *Proc. R. Soc. Lond.* A **461** 207

[12] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) pp. 510–518

[13] Audenaert K M R 2007 *J. Phys.* A: *Math. Theor.* **40** 8127