Round-robin differential quadrature phase-shift quantum key distribution*

Chun Zhou(周淳)[1,2,†], Ying-Ying Zhang(张莹莹)[1,2,†], Wan-Su Bao(鲍皖苏)[1,2,‡], Hong-Wei Li(李宏伟)[1,2], Yang Wang(汪洋)[1,2], and Mu-Sheng Jiang(江木生)[1,2]

[1] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450001, *China*

[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 1 September 2016; revised manuscript received 17 October 2016; published online 20 December 2016)

Recently, a round-robin differential phase-shift (RRDPS) protocol was proposed [*Nature* **509**, 475 (2014)], in which the amount of leakage is bounded without monitoring the signal disturbance. Introducing states of the phase-encoded Bennett–Brassard 1984 protocol (PE-BB84) to the RRDPS, this paper presents another quantum key distribution protocol called round-robin differential quadrature phase-shift (RRDQPS) quantum key distribution. Regarding a train of many pulses as a single packet, the sender modulates the phase of each pulse by one of $\{0, \pi/2, \pi, 3\pi/2\}$, then the receiver measures each packet with a Mach–Zehnder interferometer having a phase basis of 0 or $\pi/2$. The RRDQPS protocol can be implemented with essential similar hardware to the PE-BB84, so it has great compatibility with the current quantum system. Here we analyze the security of the RRDQPS protocol against the intercept-resend attack and the beam-splitting attack. Results show that the proposed protocol inherits the advantages arising from the simplicity of the RRDPS protocol and is more robust against these attacks than the original protocol.

Keywords: round-robin differential phase-shift protocol, quantum key distribution, intercept-resend attack, beam-splitting attack

PACS: 03.67.Dd, 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/26/2/020303

1. Introduction

Quantum key distribution (QKD) allows two legitimate parties (typically called Alice and Bob) to generate a common string of secret key bits in the presence of eavesdroppers. In principle, the laws of quantum mechanics guarantee the unconditional security of QKD.[1,2] Since the Bennett–Brassard 1984 (BB84) protocol was proposed in 1984,[3] QKD has attracted public attention and many protocols are presented for both discrete variable[4–10] and continuous variable.[11,12] In most protocols, the information leakage of quantum communication needs to be estimated by monitoring signal disturbance, which sacrifices signals for sampling and decreases the efficiency of the protocols.

Different from many protocols such as BB84, a new approach named round-robin differential phase-shift (RRDPS) quantum key distribution was proposed.[13] It has attracted intensive attention from theoretical works[14–16] and has been implemented in optical fibers using readily available optical telecommunication tools.[17–20] Due to its distinctive measurement scheme, privacy amplification of this protocol depends on the states preparation instead of the signal disturbance. This property causes the protocol to have a better tolerance of bit errors and finite-length effects. Furthermore, there is an obvious indication that RRDPS is largely insensitive to multi-photon states. This protocol allows communication parties to transmit much brighter states obtaining higher communication rates and longer distance.

Inheriting the benefit of the RRDPS protocol, we introduce the states of PE-BB84 into the RRDPS protocol, where each pulse is randomly phase modulated by one of $\{0, \pi/2, \pi, 3\pi/2\}$. We call it the round-robin differential quadrature phase-shift (RRDQPS) QKD. Combining the superiorities of BB84 and the RRDPS protocol, the security of this scheme is based on the fact that a secure key can be obtained only when the basis of the signal state matches that of the measurement system, in addition to measuring the phase difference between pulses at different intervals in a packet. The RRDQPS protocol can be implemented with essential similar hardware to the PE-BB84 except adding a variable optical delay line.

The most general attacks in QKD are coherent and joint attacks, in which Eve treats the entire key as a system and utilizes the information leaked in error correction and privacy amplification. Needing a probe of large dimensionality with infinite coherence time, these attacks are beyond the domain of the current technology. In addition, the proof of security against coherent attacks may be quite difficult, one can restrict eavesdropping to individual attacks, in which Eve entangles each photon with an independent probe and measures these

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61505261 and 11304397) and the National Basic Research Program of China (Grant No. 2013CB338002).

† The first two authors contributed equally to this work.

‡Corresponding author. E-mail: 2010thzz@sina.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

probes independently. The restriction to individual attacks is regarded as a practical assumption for the foreseeable future.

This paper is organized as follows. In Section 2, we describe detailed procedures of the RRDQPS protocol and present the alternative protocol of the RRDQPS protocol. After presenting the configuration, in Section 3, we quantitatively analyze the security of the proposed protocol against typical eavesdropping, intercept-resend attack and beam-splitting attack. In Section 4, we summarize this paper.

2. Round-robin differential quadrature phase-shift QKD

2.1. RRDQPS protocol

In round-robin differential quadrature phase-shift (RRDQPS) quantum key distribution protocol, we employ a train of pulses with block-wise phase randomization and utilize the relative phases between two pulses of the packet. Since secret keys are encoded on pairs of pulses and the whole train of pulses is linked together by the phase relations, it is no use for eavesdroppers to work on each pulse separately. Despite this notable simplicity in the implementation, because of the non-deterministic collapse of a wavefunction in a quantum measurement, it has been expected that the protocol should be robust against many strong attacks by eavesdroppers, including photon-number-splitting (PNS) attacks and intercept-and-resend (IR) attack.

Figure 1 shows the basic idea of the proposed RRDQPS protocol. A transmitter (Alice) uses a laser source to emit a long train of coherent pulses, each of which is phase modulated randomly and attenuated to be less than one photon per pulse on average. A variable delay Mach–Zehnder interferometer followed by two photon detectors is used at the site of a receiver (Bob). Using this setup, Alice and Bob proceed the RRDQPS protocol as follows.

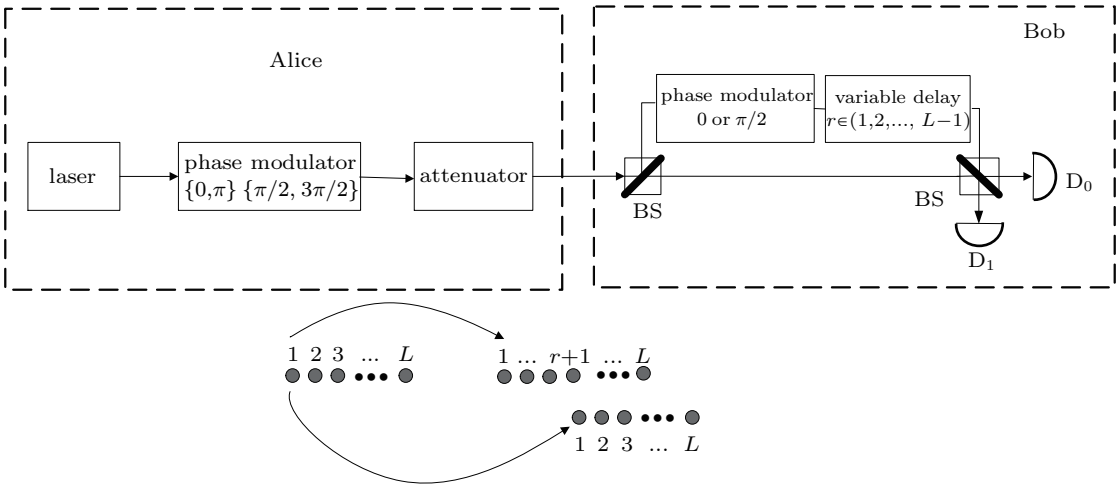


Fig. 1. Setup of RRDQPS protocol. Alice's laser emits a train of L pulses with interval T. She chooses one of $\{0,\ \pi/2,\ \pi,\ 3\pi/2\}$ with an equal probability as phase shift and applies on each pulse. Bob splits the received train into two beams, and the longer arm of the interferometer passes through a phase modulator that incurs phase shift 0 or $\pi/2$.

Step 1 Alice chooses the phases $\phi_x = (\pi/2)a_x + b_x\pi + \phi$ where $a_x \in \{0,1\}$ represents the basis choice, $b_x \in \{0,1\}$ is the random bit and $\phi \in [0,2\pi)$ is a common random optical phase shift to all the L pulses in the same packet in order to improve the security key rate in the actual protocol. In detail, the phases $\phi_x \in \{0+\phi,\ \pi+\phi\}$ and $\phi_x \in \{\pi/2+\phi,\ 3\pi/2+\phi\}$ can be considered as the bit values $\{0,1\}$ in the "even" $(a_x = 0)$ and "odd" $(a_x = 1)$ basis respectively. Then, Alice generates the following encoded signal

$$|\psi\rangle = \bigotimes_{n=0}^{L-1} e^{i\phi_n}|n\rangle$$

and sends to Bob, where the photon is in the n-th pulse for state $|n\rangle$.

Step 2 After the possible intervention of an eavesdropper, Bob receives the signal and splits the incoming signal into two paths through a variable delay Mach–Zehner interferometer, the long arm of which has a phase shift, 0 or $\pi/2$, corresponding to his basis choice, and a variable delay. The variable delay is determined by a random value $r \in \{1,\ldots,L-1\}$. Utilizing the beam splitters and interferometer, the pulses are measured by two photon detectors corresponding to bit values "0" and "1". Interference between pulses belonging to adjacent blocks is invalid, and timing of valid detection is labeled by the pulse from the short arm. Bob records the valid detection timing k, and the detection result, D_0 or D_1.

Step 3 Through an authenticated classical channel, Bob announces the choice of basis to Alice. Then Alice tells Bob whether their basis choices match. This is a sifting step. They discard where the basis fails to match. For the matched packet, Bob announces the photon interferometer time k, variable delay r publicly.

In detail, when the phase difference sent from Alice $\Delta\theta_A \in \{0,\pi\}$ and the phase shift in Bob is 0, Alice creates bit "0" from $\Delta\theta_A = 0$ and creates bit "1" from $\Delta\theta_A = \pi$, then

Bob creates bit "0" from the click of D_0 and bit "1" from the click of D_1. When $\Delta\theta_A \in \{\pi/2, 3\pi/2\}$ and phase shift is $\pi/2$, Alice creates bit "0" from $\Delta\theta_A = \pi/2$ and creates bit "1" from $\Delta\theta_A = 3\pi/2$. Then Bob creates bit "0" from the click of D_0 and bit "1" from the click of D_1. If the phase shift of Bob mismatches the phase difference in Alice, they discard the data.

Step 4 Alice and Bob repeat steps 1–3 to accumulate enough sifted keys. Communicating on an authenticated classical channel, they perform error correction and privacy amplification on the sifted keys to extract the final secure key.

2.2. Alternative protocol

Obviously, the model of the RRDQPS protocol can be considered containing two RRDPS measurements, as shown in Fig. 2.

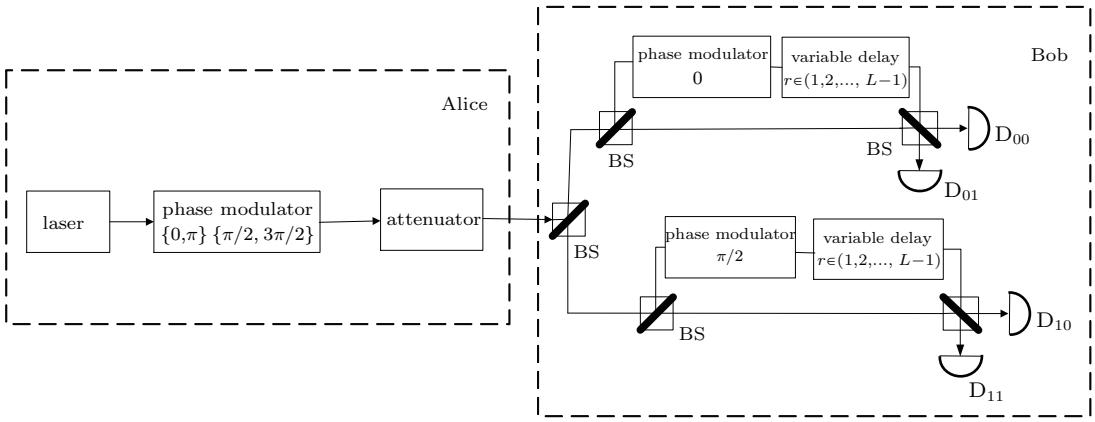


Fig. 2. Equivalent model of RRDQPS.

Here we consider equivalent ways of carrying out the RRDQPS protocol.[21]

(i) Alice prepares L auxiliary qubits and L optical pulses in state

$$|\Phi\rangle = 2^{-L/2} \bigotimes_{k=0}^{L-1} |a_k\rangle \left| e^{i\frac{\pi}{2}b}(-1)^{a_k}\alpha \right\rangle,$$

where b corresponds to the choice of basis, while a_k refers to a random bit. She measures, v, the total number of photons in the L pulses with projective measurement, and sends the encoded state to Bob.

(ii) Bob utilizes the beam splitter and interferometers, records the pair of valid timing $\{k, k+r\}$ and announces it through the public channel.

(iii) Alice operates a CNOT gate on the k-th qubit, as the control qubit, and the $(k+r)$-th qubit, as the target one.

(iv) Alice measures all the qubits but the $(k+r)$-th one on X basis $\{|+\rangle, |-\rangle\}$ and measures the $(k+r)$-th qubit on Z basis $\{|0\rangle, |1\rangle\}$ to determine the raw key bit.

(v) Alice and Bob repeat the above steps to accumulate enough raw keys.

(vi) After a sifting step, Alice and Bob share the sifted key bit. Then they conduct error correction and privacy amplification to extract the final key.

Since a CNOT gate on Z basis can be seen as a CNOT gate on X basis exchanging the target and control qubits, the alternative protocol measures all L qubits on X basis to obtain L bits and calculate the $s_k \oplus s_{k+r}$. This shows that the alternative protocol is identical to the previous one from the view of Eve.

3. Security analysis

In this section, we consider some typical attacks that Eve might perform. Two basic attacks including intercept-resend attack and beam-splitting attack are shown. Analyzing the performance of the protocol against these attacks in detail, we obtain an intuitive idea of the security of the protocol.

3.1. Intercept-resend attack

An intercept-resend attack is a typical individual attack, where the eavesdropper, Eve, cuts into the line, using the same apparatus as Bob. Eve measures the whole pulse train and resends a fake state to Bob according to her measurement result. Figure 3 shows the basic idea behind this attack. Since the four states sent from Alice are nonorthogonal, Eve cannot fully identify the transmitted states, but she can obtain information from the measurement.

The periodic train of attenuated laser pulses is sent out by Alice then received by Bob or Eve. Randomly choosing a variable delay for each packet, Bob or Eve measures the packet using an unbalance interferometer. We discuss what happens when Bob and Eve choose the same delay, and the probability of this case is $1/(L-1)$. Without loss of generality, we assume that the phase difference of the valid pulses in Alice is 0. When Eve measures the packet with a Mach–

Zehnder interferometer having a phase shift of 0, detector D_0 will click. When Eve measures with an interferometer having a phase shift of $\pi/2$, the probability of the detection at D_0 or D_1 is equal to 50%. In other words, from the detection of D_0, Eve cannot judge the differential phase $\Delta\theta = 0, \pi/2$ or $3\pi/2$. What she can do is randomly resend fake states with one of these phase differences to be 0, $\pi/2$ or $3\pi/2$, where the possibilities are 0.5, 0.25 and 0.25 respectively. Taking the first row for example, the probability of Eve choosing "0" is $1/2$ and D_0 is certain to click. Then the probability of Bob choosing "0" is also $1/2$. Thus, the ultimate probability of this case is $1/2 \times 1/2 = 1/4$. For the resent states, since Alice and Bob create a key bit only when their basis choices are matched, the possibility of the key generation is shown as Table 1.

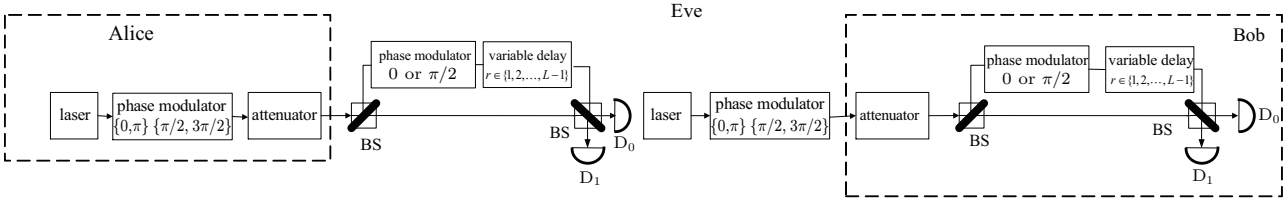


Fig. 3. Schematic diagram of intercept-resend attack.

Table 1. The intercept-resend attack when Alice sends $\Delta\theta_A = 0$, Bob and Eve choose the same delay. In the second to the fourth column, the basis choices of Eve, the measurement results and the phase differences resent by Eve are given. The next columns contain the basis chosen by Bob and the detection results. In the last two columns, the results of sifting and corresponding probabilities are given.

Alice	Eve			Bob		Result	
	Basis	Detection	Resend	Basis	Detection	Sifting	Probability
$\Delta\theta_A = 0$	0	D_0	$\Delta\theta_E = 0$	0	D_0	Keep	1/4
				$\pi/2$	D_0	Discard	1/8
					D_0	Discard	1/8
	$\pi/2$	D_0	$\Delta\theta_E = \pi/2$	0	D_0	Keep	1/16
					D_1	Bit error	1/16
				$\pi/2$	D_0	Discard	1/8
		D_1	$\Delta\theta_E = 3\pi/2$	0	D_0	Keep	1/16
					D_1	Bit error	1/16
				$\pi/2$	D_1	Discard	1/8

It is also easy to see from Table 1 that the key generation probability is $1/4 + 1/16 \times 4 = 1/2$, the probability that Eve obtains correct key is $1/4 + 1/16 = 5/16$ and the bit error rate is $1/16 + 1/16 = 1/8$. Thus, Eve can know the correct key with $\frac{5/16}{1/2} = 5/8$ probability, and results in bit error rate with $\frac{1/8}{1/2} = 1/4$ probability in total. A similar discussion is also made for the differential phase in Alice, which is $\Delta\theta = \pi/2\,, \pi$ or $3\pi/2$. Note that the intercept-resend attack induces no bit error in the RRDPS protocol, which indicates that the proposed protocol is more robust against the intercept-resend attack than the original one.

3.2. Beam-splitting attack

The basic idea behind the second attack strategy is shown in Fig. 4. In a beam-splitting attack, Eve inserts a beam splitter into the quantum channel to split part of the transmitted photons and store them, then sends the rest of the photons through a lossless channel. The fraction of the photons split should be equal to that of loss in the channel without beam-splitting attack, in order not to modify the communication rate. Finally, Eve measures the split states using an unbalanced interferometer with the same phase shift as Bob, after Alice and Bob announce the photon interferometer time and the basis choice. Because of the use of coherent states, Eve's detection events are independent of Bob. Based on this strategy, Eve can obtain detection results of the corresponding two pulses using appropriate phase bias without being revealed.

The amount of information Eve obtains per packet depends on the transmission between Alice and Bob η and the average photon number per packet $L\mu$, where L is the length of each packet. In each packet containing L pulses, Eve transmits $L\eta\mu$ photons to Bob and stores $L(1-\eta)\mu$ photons. After knowing the information of Bob, Eve delays her measurement and the probability of click from the packet is $2(1-\eta)\mu$, which can be considered as the information Eve obtains.

In RRDQPS, the amount of information leakage can be seen as a function of average photon number. Optimizing the choice of μ can decrease the information leakage and remove it by privacy amplification, indicating the robustness of the protocol against the beam-splitting attack. As for the photon-number-splitting (PNS) attack, it breaks the coherency of the pulses in a packet, then it will reveal the existence of the eavesdropper. The RRDQPS protocol can effectively be robust against photon-number-splitting attack.

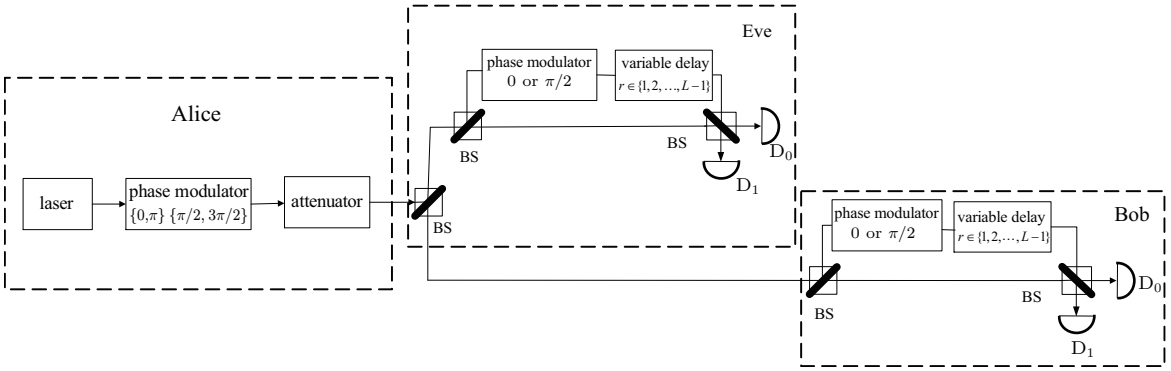


Fig. 4. Schematic diagram of beam-splitting attack.

4. Summary

In this paper, a new quantum key distribution protocol named round-robin differential quadrature phase-shift (RRDQPS) QKD has been proposed. A coherent pulse train phase modulated by $\{0,\ \pi/2,\ \pi,\ 3\pi/2\}$, for each pulse is transmitted and measured with a Mach–Zehnder interferometer having a phase basis of 0 or $\pi/2$. The RRDQPS protocol can be implemented with essential similar hardware to the PE-BB84, so it has great compatibility with an existing system. After describing the setup and procedure of this protocol in detail, we analyze the security of the protocol against the intercept-resend attack and the beam-splitting attack. There is a long way to go for strict proof of the security of the protocol, but we anticipate that this kind of protocol will be an outstanding candidate for practical long distance quantum cryptography.

References

[1] Lo H K and Chau H F 1999 *Science* **283** 2050
[2] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computer Systems and Signal Processing*, Banglore: India, p. 175
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[6] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[7] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[8] Gu Y B, Bao W S, Wang Y and Zhou C 2016 *Chin. Phys. Lett.* **33** 40301
[9] Yin Z Q, An X B and Han Z F 2015 *Acta Phys. Sin.* **64** 140303 (in Chinese)
[10] Li Y, Bao W S, Li H W, Zhou C and Wang Y 2016 *Chin. Phys. B* **25** 010305
[11] Braunstein S L and Loock P 2005 *Rev. Mod. Phys.* **77** 513
[12] 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
[13] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475
[14] Zhang Z, Yuan X, Cao Z and Ma X F 2015 arXiv: 1505.02481v1 [quant-ph]
[15] Mizutani A, Imoto N and Tamaki K 2015 *Phys. Rev. A* **92** 060303
[16] Zhang Y Y, Bao W S, Zhou C, Li H W, Wang Y and Jiang M S 2016 *Opt. Express* **24** 20763
[17] Guan J Y, Cao Z and Liu Y 2015 *Phys. Rev. Lett.* **114** 180502
[18] Li Y H, Cao Y, Dai H and Lin J 2015 arXiv: 1505.08142v1 [quant-ph]
[19] Takesue H, Sasaki T, Tamaki K and Koashi M 2015 *Nat. Photon.* **9** 827
[20] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat. Photon.* **9** 832
[21] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inform. Comput.* **4** 325
[22] Waks E, Takesue H and Yamanoto Y 2006 *Phys Rev. A* **73** 012344