CHIN. PHYS. LETT. Vol. 34, No. 8 (2017) 080302

Application of a Discrete Phase-Randomized Coherent State Source in Round-Robin Differential Phase-Shift Quantum Key Distribution *

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

[1]*Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Zhengzhou 450001*

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

(Received 31 March 2017)

Recently, a novel kind of quantum key distribution called the round-robin differential phase-shift (RRDPS) protocol was proposed, which bounds the amount of leakage without monitoring signal disturbance. The protocol can be implemented by a weak coherent source. The security of this protocol with a simply characterized source has been proved. The application of a common phase shift can improve the secret key rate of the protocol. In practice, the randomized phase is discrete and the secret key rate is deviated from the continuous case. In this study, we analyze security of the RRDPS protocol with discrete-phase-randomized coherent state source and bound the secret key rate. We fix the length of each packet at 32 and 64, then simulate the secret key rates of the RRDPS protocol with discrete-phase randomization and continuous-phase randomization. Our simulation results show that the performance of the discrete-phase randomization case is close to the continuous counterpart with only a small number of discrete phases. The research is practically valuable for experimental implementation.

PACS: 03.67.Dd, 03.67.Hk, 42.50.Ex DOI: 10.1088/0256-307X/34/8/080302

Quantum key distribution enables two authenticated users (typically called Alice and Bob) to share a common string of bits, secret key.[1,2] Secure keys can be used for secure communication and authentication. The security of the secret key has been proven to be unconditional, guaranteed by the laws of physics.[3–5] In the conventional QKD system, error correction and privacy amplification are both estimated from error rate, which lead to an upper bound of the bit error rate, limiting the application of quantum key distribution systems.

Recently, a round-robin different phase-shift (RRDPS) protocol was proposed.[6] It has been implemented using readily available optical tools[7–10] and has also attracted intensive attention from theoretical works.[11–14] It has also been used to develop a QKD-based quantum private query without a failure probability.[15] There is obvious indication that the RRDPS protocol is largely insensitive to multi-photon states. This allows communication parties to transmit much brighter states obtaining higher communication rate and longer distance.

In conventional protocols, the security often relies on several assumptions, one of which is that Alice has a perfect single photon source. Due to the great challenge to build a perfect single photon source, the coherent state source becomes the most common photon source for state-of-art quantum key distribution. The assumption of a single photon source can be removed at the cost of introducing another assumption: the phase of each signal is uniformly random. In practice, the assumption of continuous phase randomization may be dissatisfactory in practical implementations. In conventional protocols, there are valid attacks stealing key information the users cannot discover.[16–18]

To connect theory with practice, several approaches have been proposed. In practical implementation, there are two means randomizing the phase: passive and active. In the passive process, pulses are generated by switching a laser on or off. Due to residual correlation between the phases of adjacent pulses, this approach should be avoided.[19] As for the active process, Alice should modulate the global phase of each signal with an extra random value using phase modulator to implement phase randomization. However, the phase can only be modulated discretely. A recent work suggests that with a global phase chosen from a small number of possible values, security can also be achieved in the BB84 protocol.[20]

Like the existing QKD protocol, the RRDPS protocol can be implemented simply by a weak coherent laser pulse train as a light source. The security proof adopts the source with a simple characterization about the total photon number in a packet. Applying a common phase shift to a packet, the key rate can be improved. In some practical quantum systems, continuous phase randomization may not be satisfied in implementations. When the phase is not continuously randomized, the secret key rate of generating the secure key may deviate from the continuous case. It is still a question to analyze the security of the RRDPS protocol with discrete-phase randomization.

*Supported by the National Basic Research Program of China under Grant No 2013CB338002, and the National Natural Science Foundation of China under Grant Nos 11304397 and 61505261.

**Corresponding author. Email: 2010thzz@sina.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

In this Letter, considering the essence of the RRDPS protocol, we analyze the phase error rate of the RRDPS protocol using discrete-phase-randomized coherent states and provide a rigorous bound on the key rate without monitoring the disturbance. We show that as the number of discrete phases increases, secure key rate of discrete-phase-randomized source approaches that of the continuous one. In simulation, for only 4 phases, with typical parameters the secret key rate can be close to the continuous phase randomized case. Our result can be directly applied to the implementation of the RRDPS protocol, since coherent states are a major source of current experiment.

In the RRDPS protocol, we employ a train of pulses with block-wise phase randomization and utilize the relative phases between two pulses in a packet, and one of them is delayed by an optical line. 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. Since secret keys are encoding on every pair of pulses and the whole train of pulses is linked together by the phase relations, they are not used for eavesdroppers to work on each pulse separately and security of the protocol is guaranteed.

The ideal round-robin differential phase-shift protocol proceeds as follows: (1) Alice generates a random L-bit string $s = (s_0, s_1, \ldots, s_{L-1})$, $s_n \in \{0, 1\}$, $n \in \{0, 1, \ldots L-1\}$, and sends Bob the following encoded signal

$$|\psi\rangle = \frac{1}{\sqrt{L}} \sum_{n=0}^{L-1} (-1)^{s_n} |n\rangle,$$

where $|n\rangle$ denotes that the photon is in the nth pulse. (2) After the possible intervention of an eavesdropper, Bob receives the weak signal. Generating a random value $r \in \{1, \ldots L-1\}$, through an optical interference measurement, Bob determines the phase difference $s_i \oplus s_j$ of a pair of pulses with indices $i, j \in \{0, 1, \ldots L-1\}$ satisfying $j - i = \pm r (\mathrm{mod} L)$. The outcome of the measurement is recorded as the sifted key s_{B} of Bob. (3) Through an authenticated classical channel, Bob announces $\{i, j\}$ to Alice, then Alice records $s_{\mathrm{A}} = s_i \oplus s_j$ as her sifted key bit. (4) Alice and Bob repeat steps 1–3 to accumulate enough sifted key. Communicating on an authenticated classical channel, they perform error correction and privacy amplification on the sifted key to extract the final secure key.

Coherent state source is the major candidate of perfect single photon source in current technology. Coherent state can be described by[21]

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum \frac{\alpha^n}{\sqrt{n!}} |n\rangle.$$

When we assume that the phase of each pulse is totally randomized, the photon number of each pulse follows a Poisson distribution. The density matrix of a coherent state with intensity μ can be given by

$$\rho_\mu = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n|,$$

where $|0\rangle\langle 0|$ refers to the vacuum state, and $|n\rangle\langle n|$ stands for the density matrix of n-photon state.

Consider a coherent state source with discrete phase chosen from the set as follows:

$$\{\theta_i = \frac{2\pi i}{N} | i = 0, 1, \ldots, N-1\},$$

where the phases are distributed in $[0, 2\pi)$ evenly. Then the mixed state can be decomposed into a set of pure states,[20]

$$\begin{aligned} |\Psi_N\rangle &= \sum_{k=0}^{N-1} |k\rangle_{\mathrm{A}} |\sqrt{2}\alpha e^{2k\pi i/N}\rangle_{\mathrm{B}} \\ &= \sum_{n=0}^{N-1} |n\rangle_{\mathrm{A}} |\lambda_n\rangle_{\mathrm{B}}, \end{aligned}$$

where the phase of coherent state $\sqrt{2}\alpha$ is controlled by a quantum coin, $|n\rangle_{\mathrm{A}}$ can be seen as random outputs of a quantum coin, and $|\lambda_n\rangle_{\mathrm{B}}$ is pure states

$$\begin{aligned} |\lambda_n\rangle &= \sum_{k=0}^{N-1} e^{-2kn\pi i/N} |e^{2k\pi i/N} \sqrt{2}\alpha\rangle \\ &= \sum_{l=0}^{\infty} \frac{(\sqrt{2}\alpha)^{lN+n}}{\sqrt{(lN+n)!}} |lN+n\rangle. \end{aligned} \tag{1}$$

By this decomposition, the Hilbert space is divided into different number Fock state spaces, $H_{0 \bmod N} \oplus H_{1 \bmod N} \oplus \ldots \oplus H_{(N-1) \bmod N}$. We hope that one of these pure states can be closed to a single-photon state.[20]

Due to the quick increase of $\sqrt{(lN+n)!}$ when N is large, it is obvious that $|\lambda_n\rangle$ can approximate a Fock state. When N approaches infinity, $|\lambda_n\rangle$ becomes a Fock state, $|\lambda_n\rangle = |n\rangle$. With N discrete phases, the probability of n-photon state can be calculated by

$$P_n^{(N)}(\mu) = \sum_{l=0}^{\infty} \frac{\mu^{lN+n} e^{-\mu}}{(lN+n)!},$$

where $\mu = 2|\alpha|^2$ is the intensity of each small pulse. It can be seen as the probability summation of Fock states whose photon numbers are n module N. When N approaches infinity, it follows a Poisson distribution.

A practical schematic diagram of the RRDPS protocol using coherent state source is shown in Fig. 1. In the stage of state preparation, Alice prepares the coherent state with random phase modulated by the first phase modulator, namely, adding a random phase on each pulse train. Then, Alice encodes random phase 0 or π on each pulse via the second phase modulator.

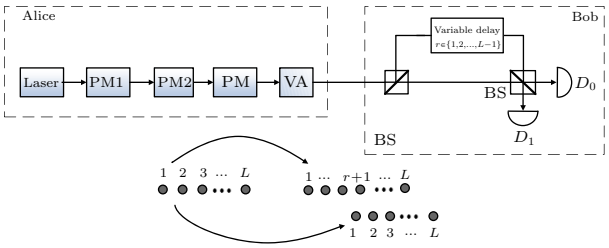


Fig. 1. Schematic diagram for the RRDPS protocol with coherent states. PM, phase modulator; VA, variable attenuator. Here, PM1 realizes phase randomization, which means to add a random phase on each pulse train, and PM2 is used for encoding random phase 0 or π on each pulse.

Alice generates coherent-state pulses with phase $\phi_n = \pi s_n + \phi$, where ϕ is a common random optical phase shift to all the L pulses in the same packet to improve the security key rate in the actual protocol. Here $s = (s_0, s_1, \ldots, s_{L-1})$ is random L-bit sequence. With intensity $\alpha(\alpha > 0)$, Alice generates the following encoded signal $|\psi\rangle$ and sends to Bob through an insecure quantum channel,

$$\begin{aligned}|\psi\rangle &= |\alpha e^{i\phi_0}\rangle \otimes |\alpha e^{i\phi_1}\rangle \otimes \ldots \otimes |\alpha e^{i\phi_{L-1}}\rangle \\ &= \otimes_{n=0}^{L-1} |\alpha e^{i\phi_n}\rangle.\end{aligned}$$

From there, they communicate in the same way as the ideal scheme.

In the RRDPS protocol, the random bit sequence $s = (s_0, s_1, \ldots, s_{L-1})$ can be seen as outcome of Z-basis ($\{|0\rangle, |1\rangle\}$). For each train, Alice prepares L ancillary qubits and an L-pulse state $|\psi\rangle$ in an entangled state

$$|\psi\rangle_{\text{Alice}} = 2^{-L/2} \otimes_{k=0}^{L-1} \sum_{s_k=0,1} |s_k\rangle (-1)^{s_k \hat{n}_k} |\psi\rangle,$$

where $\hat{n}_k$ is the photon number operator for the kth pulse, and $|s_k\rangle$ is the kth ancillary qubit. The measurement outcomes of the L ancillary qubits in the Z basis can be regarded as random bits to construct secret key bits. When Alice measures the L ancillary qubits in the X basis ($\{|+\rangle, |-\rangle\}$), where $|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)$, the possibility of qubits found in $|-\rangle$ is defined to be the phase error rate. It is determined by the number of photons contained in this pulse. If a pulse contains an odd number of photons, it has a phase error. Hence the number of $|-\rangle$ is no more than the total photon number.

One of the most important tasks in the security proof is to derive an upper bound on the information leakage to the eavesdropper, which means phase error rate. The phase error rate in the RRDPS protocol only relies on the state preparation. Generally speaking, it is equal to the probability of finding an odd number of photons in a pulse.

Without the random optical phase shift of each packet, the phase error rate is defined as[6]

$$e_{\text{ph}} = \frac{e_{\text{src}}}{Q} + \left(1 - \frac{e_{\text{src}}}{Q}\right) \frac{v_{\text{th}}}{L-1},$$

where Q is the rate of detection. The total photon number v in a packet satisfies $P(v > v_{\text{th}}) \leq e_{\text{src}}$, where v_{th} is an integer less than $(L-1)/2$ and e_{src} is a constant.

The cost of error correction is $f \cdot h(e_{\text{bit}})$, where f is the efficiency of error correction and $h(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary Shannon entropy function. The secret key rate is given by

$$R = \frac{Q}{L}[1 - f \cdot h(e_{\text{bit}}) - h(e_{\text{ph}})].$$

When the random optical phase is continuous, the coherence among different photon-number states is eliminated, and the quantum state emitted can be seen as a classical mixture of state with fixed photon numbers. Then the key rate can be improved to[6]

$$R = \frac{Q}{L}\left[1 - f \cdot h(e_{\text{bit}}) - \frac{e_{\text{src}}}{Q} - \left(1 - \frac{e_{\text{src}}}{Q}\right) h\left(\frac{v_{\text{th}}}{L-1}\right)\right].$$

In the scheme with discrete-phase-randomized coherent state source, $|\lambda_i\rangle (i = 0, 1, \ldots, N-1)$ contains the Fock states whose photon numbers of modulo, N, are the same as i, and it becomes close to i-photon state when N is large, $|\lambda_i\rangle = |i\rangle$.

Borrowing the security analysis of Gottesman–Lo–Lutkenhaus–Preskill (GLLP),[22] an imperfect source may tag some of the qubits and may reveal some information to an eavesdropper. Supposing that a fraction Δ of qubits are tagged, Eve may completely know the key bits of the tagged part and know slightly about the rest.

Then, packets with the total photon number v satisfying the form of $P(v > v_{\text{th}})$ can be considered as tagged by Alice and completely known by Eve. Here Δ consists of two parts in the scheme with a discrete-phase-randomized coherent state source, $\sum_{v > v_{\text{th}}} P_v^{(N)}(L\mu)$ and $\sum_{v=0}^{v_{\text{th}}} P_{lN+v}^{(N)}(L\mu)$, where $l = \min\{l | lN + v > v_{\text{th}}\}$ is the minimum value causing $lN + v > v_{\text{th}}$.

The former part refers to the summation of pure states $|\lambda_i\rangle (i = 0, 1, \ldots, N-1)$ with subscript greater than v_{th}, and in these pure states all the Fock states contain photons greater than v_{th}. The latter part denotes the summation of Fock states belonging to pure states $|\lambda_i\rangle (i = 0, 1, \ldots, N-1)$ with subscript less than v_{th} but containing photons greater than v_{th},

$$\begin{aligned}\Delta &= \sum_{v > v_{\text{th}}} P_v^{(N)}(L\mu) + \sum_{v=0}^{v_{\text{th}}} P_{lN+v}^{(N)}(L\mu) \\ &= 1 - \sum_{v=0}^{v_{\text{th}}} P_v^{(N)}(L\mu) + \sum_{v=0}^{v_{\text{th}}} P_{lN+v}^{(N)}(L\mu) \\ &= 1 - \sum_{v=0}^{v_{\text{th}}} (P_v^{(N)}(L\mu) - P_{lN+v}^{(N)}(L\mu). \qquad (2)\end{aligned}$$

Treating the untagged qubits as $e_{\text{src}} = 0$, the secure final key of discrete-phase-randomized scheme can be

extracted at the asymptotic rate

$$R = \frac{Q}{L}[1 - f \cdot h(e_{\rm bit}) - \Delta h(e_{\rm ph}^{\rm untagged}) - (1-\Delta)h(e_{\rm ph}^{\rm untagged})] = \frac{Q}{L}\left[1 - f \cdot h(e_{\rm bit}) - \Delta - (1-\Delta)h\left(\frac{v_{\rm th}}{L-1}\right)\right], \quad (3)$$

where Q and $e_{\rm bit}$ are the overall gain and quantum key error rate, respectively, and can be measured in experiments.

In our simulation, we adopt a widely used simulation model for QKD. The yield of i-photon state, Y_i, comes from background and signals, and can be given by[23]

$$Y_i = 1 - (1 - Y_0)(1 - \eta)^i,$$

where Y_0 is the background depending on the length of each packet L and background noise in each pulse y_0, and becomes $1 - (1 - y_0)^L$. The relationship between the transmission distance D and the overall transmittance η satisfies

$$\eta = 10^{-\alpha D/10}\eta_{\rm Bob},$$

where $\eta_{\rm Bob}$ is the detection efficiency, and α is the loss coefficient.

The bit error rate of the i-photon state is given by

$$e_i = \frac{e_0 Y_0 + e_{\rm d}(1 - Y_0)(1 - (1-\eta)^i)}{Y_i},$$

where the error rate of the background e_0 is 0.5, and a constant $e_{\rm d}$ characterizes the stability of the quantum system. Then the overall gain when using discrete-phase-randomized coherent state source is given by

$$Q_{L\mu} = \sum_{j=0}^{N-1} P_j^{(N)}(L\mu)Y_j = \sum_{j=0}^{N-1}\sum_{l=0}^{\infty}\frac{(L\mu)^{lN+j}e^{-L\mu}}{(lN+j)!}[1 - (1-Y_0)(1-\eta)^j]. \quad (4)$$

The overall quantum bit error rate is given by

$$E_{L\mu}Q_{L\mu} = \sum_{j=0}^{N-1} P_j^{(N)}(L\mu)e_j Y_j = \sum_{j=0}^{N-1}\sum_{l=0}^{\infty}\frac{(L\mu)^{lN+j}e^{-L\mu}}{(lN+j)!}[e_0 Y_0 + e_{\rm d}(1-Y_0)(1-(1-\eta)^j)]. \quad (5)$$

Based on the above formulas, using the data listed in Table 1, we simulate various cases of phase number N and compare the maximum transmission distance of each case. The length of each packet is fixed at 32 and 64, respectively. The rates are optimized over the choice of $v_{\rm th}$ and the mean photon number μ.

Table 1. Parameters of a typical QKD system.[24] Here α is the channel loss coefficient, $\eta_{\rm Bob}$ is the detection efficiency of Bob, y_0 is the background noise in each pulse, and $e_{\rm d}$ characterizes the stability of the quantum system.

Experiment	α	$e_{\rm d}$	$\eta_{\rm d}$	y_0	f
GYS	0.2	0.033	0.045	1.7×10^{-6}	1.2

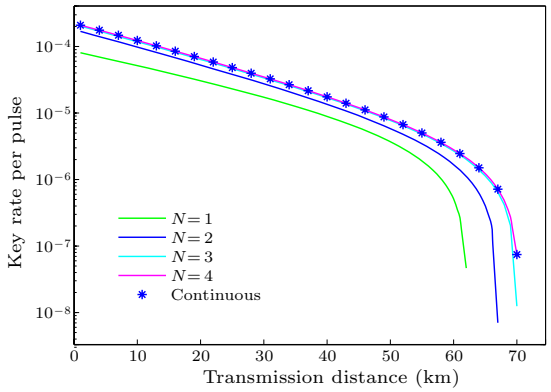


Fig. 2. Key rates versus the transmission distance for different numbers of random phase (N) when the length of each packet is 32. The solid lines from right to left correspond to the cases without random phase shift and N from 1 to 4, respectively. The case of $N = 1$ refers to the no phase randomization case. The asterisk line is the continuous phase randomization case.

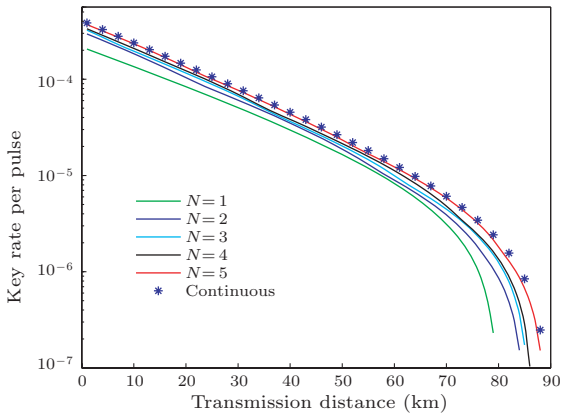


Fig. 3. Key rates versus the transmission distance for different numbers of random phase (N) when the length of each packet is 64. The solid lines from right to left correspond to the cases without random phase shift and N from 1 to 5, respectively.

The simulation results are shown in Figs. 2 and 3. When N is small, the secret key rate is less than that of the continuous case. The smaller the number of discrete phase N is, the larger the deviation is. Thus it is important to determine the need of phase before practical implementation. Since the amount of leaked information is bounded during the state-preparation stage, it is quite related to the length of each packet. The need of discrete phase is connected with the length of packet. As shown by the curves, when the length is fixed at 32, we can see that with four random phases, the performance of discrete phase randomization is close to that of the continuous case.

In conclusion, considering the essence of the protocol, we have analyzed the application of

discrete-phase-randomized coherent state source in the RRDPS protocol. With our simulation results, when the length of each packet is 32, only 4 random phases are needed for the discrete phase randomization, and the security key rate is close to the continuous case. Since two bits of random numbers per pulse, which gives $2^2 = 4$ possible phases, are enough, our scheme is highly practical. We note that a feasible solution of phase-randomized under current technology is offered. When the length of each packet is different, the need of discrete phases is also different. Compared with the BB84 protocol, the number of discrete phase needed is much fewer in the RRDPS protocol.

References

[1] Bennett C H and Brassard G 1984 *Int. Conf. Comput. Syst. Signal Process* (Banglore, India) (New York: IEEE) p 175
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[3] Lo H K and Chau H F 1999 *Science* **283** 2050
[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[5] Mayers D 2001 *J. ACM* **48** 351
[6] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475
[7] Guan J Y, Cao Z, Liu Y, Shen-Tu G L, Pelc J S, Fejer M M, Peng C Z, Ma X, Zhang Q and Pan J W 2015 *Phys. Rev. Lett.* **114** 180502
[8] Li Y H, Cao Y, Dai H, Lin J, Zhang Z, Chen W, Xu Y, Guan J Y, Liao S K, Yin J, Zhang Q, Ma X, Peng C Z and Pan J W 2016 *Phys. Rev.* A **93** 030302
[9] Takesue H, Sasaki T, Tamaki K and Koashi M 2015 *Nat. Photon.* **9** 827
[10] 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
[11] Zhang Z, Yuan X, Cao Z and Ma X F 2015 arXiv:1505.02481v1[quant-ph]
[12] Mizutani A, Imoto N and Tamaki K 2015 *Phys. Rev.* A **92** 060303
[13] Yin H L, Fu Y, Mao Y and Chen Z B 2016 *Phys. Rev.* A **93** 022330
[14] Zhang Y Y, Bao W S, Zhou C, Li H W, Wang Y and Jiang M S 2016 *Opt. Express* **24** 20763
[15] Liu B, Gao F, Huang W and Wen Q Y 2015 *Sci. Chin. Phys. Mech. Astron.* **58** 100301
[16] Sun S H, Gao M, Jiang M S, Li C Y and Liang L M 2012 *Phys. Rev.* A **85** 032304
[17] Tang Y L, Yin H L, Ma X, Fung C H F, Liu Y, Yong H L, Chen T Y, Peng C Z, Chen Z B and Pan J W 2013 *Phys. Rev.* A **88** 022308
[18] Sun S H, Jiang M S, Ma X C, Li C Y and Liang L M 2015 *Sci. Rep.* **4** 04759
[19] Xu F, Qi B, Ma X, Xu H, Zheng H and Lo H K 2012 *Opt. Express* **20** 12366
[20] Cao Z, Zhang Z, Lo H K and Ma X F 2015 *New J. Phys.* **17** 053014
[21] Glauber R J 1963 *Phys. Rev.* A **131** 2766
[22] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[23] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326
[24] Gobby C, Yuan Z L and Shield A J 2004 *Appl. Phys. Lett.* **84** 3762