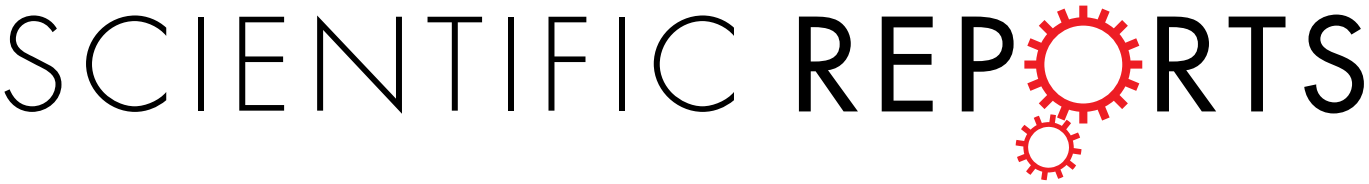

OPEN

Round-robin differential-phase-shift quantum key distribution with a passive decoy state method

Received: 12 October 2016
Accepted: 06 January 2017
Published: 13 February 2017

Li Liu[1,2], Fen-Zhuo Guo[1,2], Su-Juan Qin[1] & Qiao-Yan Wen[1]

Recently, a new type of protocol named Round-robin differential-phase-shift quantum key distribution (RRDPS QKD) was proposed, where the security can be guaranteed without monitoring conventional signal disturbances. The active decoy state method can be used in this protocol to overcome the imperfections of the source. But, it may lead to side channel attacks and break the security of QKD systems. In this paper, we apply the passive decoy state method to the RRDPS QKD protocol. Not only can the more environment disturbance be tolerated, but in addition it can overcome side channel attacks on the sources. Importantly, we derive a new key generation rate formula for our RRDPS protocol using passive decoy states and enhance the key generation rate. We also compare the performance of our RRDPS QKD to that using the active decoy state method and the original RRDPS QKD without any decoy states. From numerical simulations, the performance improvement of the RRDPS QKD by our new method can be seen.

Quantum key distribution (QKD) enables two distant parties (Alice and Bob) to share a key, which is secret from any eavesdropper (Eve)[1]. It has been proved to be unconditional secure theoretically[2]. QKD has been widely studied in both theoretical and experimental research[3,4] since its initial proposal. Moreover, QKD has entered the commercial market[5] and small QKD networks have been realized[6].

Since the rise of the BB84 protocol[1], many QKD protocols have been proposed[7–11]. The security proofs of QKD focus on how much the information is leaked to Eve. The information leakage generally can be estimated through monitoring some statistics by Alice and Bob[2,12–16]. The conventional QKD protocols inherently rely on the original version of Heisenberg's uncertainty principle, which dictates that the more information Eve has obtained, the more disturbance she should have caused on the signal. Recently, a new type of protocol, called round-robin differential-phase-shift (RRDPS) QKD protocol[17], was proposed and surprisingly, the information leakage of this protocol is estimated without any monitoring, but depends only on the state prepared by Alice. The RRDPS QKD protocol has higher stability and lower loss, it can also tolerate more noisy channels[18,19]. Since the RRDPS QKD was proposed, it has been studied both theoretically[18–20] and experimentally[20–23].

Unfortunately, due to the imperfections of devices, there is still a big gap between the theory and practice of QKD. The decoy state method has been used in the general BB84 protocol[24–29] to defeat the photon-number-splitting (PNS) attack[29,30] and guarantee the security against imperfect sources, such as weak coherent pulses (WCPS)[27]. Recently, a tight bound on the key rate of RRDPS QKD was given in ref. 18, in which it was also proposed that the infinite decoy state method for RRDPS QKD would improve the key rate. Ying-Ying Zhang *et al.*[31] extended it to the practical case with a finite number of decoy states and got the performance close to the infinite decoy state method. These approaches are all related to the active decoy state selection, which is based on the assumption that Eve can not distinguish decoy and signal states. However, this assumption may not stand in real active decoy state experiments, for which it may open up to side channel attacks and even break the security of the system when one actively modulates the intensities of pulses[32,33]. The passive decoy state method[34–37] can reduce the side channel information in the decoy state preparation procedure. Different from the active decoy state method, the passive one only uses one intensity signal, and Alice post-selects the signal state and the decoy state according to the response of Alice's own detector. The method in ref. 36 extended passive decoy state to practical unstable light sources including phase-randomized WCPs, which inspired its application to practical QKD.

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [2]School of Science, Beijing University of Posts and Telecommunications, Beijing, 100876, China. Correspondence and requests for materials should be addressed to F.-Z.G. (email: gfenzhuo@bupt.edu.cn)

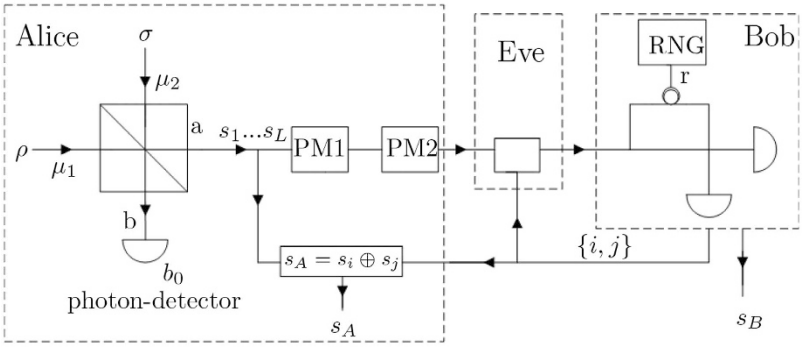

Figure 1. Basic setup of a passive decoy state RRDPS QKD scheme: interference of two Fock diagonal states, ρ and σ, at a beam splitter (BS) of transmittance t; a and b represent the two output modes. Signals flow through lines. PM 1 adds a random phase on each pulse train, and PM 2 encodes random phases 0 or π on each pulse. Eve tries to guess Alice's bit $s_A = s_i \oplus s_j$ in the figure, where indices $\{i, j\}$ are announced by Bob. According to the random number generator RNG, Bob conducts measurement to guess s_A.

In this paper, we apply the passive decoy state method to the RRDPS QKD protocol. Alice uses weak coherent sources with random phases to passively generate signal states or decoy states. Not only can the more environment disturbance be tolerated, but also one can avoid the side channel attacks on sources, which may be generated by active modulation of source intensities. Most of all, we apply a strategy that gives the accurate probability of having 0, 1, 2 photons and omits the other multiphoton occurrences. Our method is accordant with practical systems. we also show the performance comparison between our method, the active decoy state method and the original RRDPS protocol in our paper. A performance improvement of our RRDPS QKD using passive decoy state method can be seen in numerical simulations. It shows that under the same key generation rate, our protocol will have longer transmission distance.

Results

RRDPS QKD with passive decoy state strategy. In this section, we apply the passive decoy state method to the RRDPS QKD protocol[17], as shown in Fig. 1.

The protocol proceeds as follows:

1. Alice uses two weak coherent pulses with random phases to passively generate signal or decoy states. In this way she can prepare a series of pulse trains with each contains L pulses, and each train encodes a random L-bit sequence $s = (s_1 s_2 ... s_L)$ on a weak signal. Then she applies phase modulation $\{0, \pi\}$ to each optical mode according to s and obtains the state $|\psi\rangle_s$ as in Eq. (1),
$$|\psi_s\rangle = \frac{1}{\sqrt{L}} \sum_{k=1}^{L} (-1)^{s_k} |k\rangle, \tag{1}$$
where the photon is in the k-th pulse for state $|k\rangle$, s_k is the encoded bit sequence. She sends $|\psi\rangle_s$ to Bob.
2. Bob splits the received signal with a 50/50 beam splitter to obtain two L-pulse trains, uses RNG to generate a random number $r \in \{-L+1, \ldots, -2, -1, 1, 2, \ldots, L-1\}$, and shifts one of the L-pulse trains forward ($r > 0$) or backward ($r < 0$) by $|r|$ pulses.
3. Bob measures the interference between two L-pulse trains. If he obtains a detection on position i in the unshifted pulse train, corresponding to position j in the shifted pulse train, and $0 \le j = i + r \le L - 1$, Bob records a raw key bit according to the relative phase $s_B = s_i \oplus s_j$. Otherwise, Bob regards the transmission as a failure.
4. Bob announces $\{i, j\}$ so that Alice can obtain the sifted key, $s_A = s_i \oplus s_j$.

Alice generates phase-randomized pulses using two weak coherent sources with intensities μ_1 and μ_2 per pulse, respectively. It passively generates signal and decoy states, which is a joint-distribution state according to the result of detector b_0. ρ and σ denote the coherent states of two phase-randomized WCP sources states, respectively,

$$\begin{aligned} \rho &= e^{-\mu_1} \sum_{n=0}^{\infty} \frac{(\mu_1)^n}{n!} |n\rangle\langle n|, \\ \sigma &= e^{-\mu_2} \sum_{n=0}^{\infty} \frac{(\mu_2)^n}{n!} |n\rangle\langle n|, \end{aligned} \tag{2}$$

with μ_1 and μ_2 denoting the mean photon number of the two signals. The joint probability of having n photons in output mode a and m photons in output mode b can be written as ref. 38

$$p_{n,m} = \frac{\upsilon^{n+m}e^{-\upsilon}}{n!m!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n(1-\gamma)^m d\theta, \tag{3}$$

where the parameters υ, γ and θ are given by

$$\begin{aligned} \upsilon &= L(\mu_1+\mu_2), \\ \gamma &= \frac{L\mu_1 t + L\mu_2(1-t) + \xi\cos\theta}{\upsilon}, \\ \xi &= 2L\sqrt{\mu_1\mu_2(1-t)t}, \end{aligned} \tag{4}$$

and L denotes the number of pules, t denotes the transmittance of a beam splitter. This result differs from the one expected from the interference of two pure coherent states with fixed phase relation, $\left|\sqrt{\mu_1}e^{i\phi_1}\right\rangle$ and $\left|\sqrt{\mu_2}e^{i\phi_2}\right\rangle$, at a BS of transmittance t. In this last case, $p_{n,m}$ is just the product of two Poissonian distributions.

When Alice ignores the outcome of the measurement in mode b, the probability of having n photons in mode a can be written as

$$p_n^{(T)} = \sum_{m=0}^{\infty} p_{n,m} = \frac{\upsilon^n}{n!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n e^{-\upsilon\gamma}d\theta, \tag{5}$$

which is proven to be a non-Poissonian probability distribution[38] and $l \in \{c, \bar{c}\}$.

For Alice's detector b_0, the joint probability of having n photons in mode a and no click in the threshold detector b_0 has now the form

$$\begin{aligned} p_n^{(\bar{c})} &= (1-\varepsilon)\sum_{m=0}^{\infty}(1-\eta_{b_0})^m p_{n,m} \\ &= (1-\varepsilon)\frac{\upsilon^n e^{-\eta_{b_0}\upsilon}}{n!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n e^{-(1-\eta_{b_0})\upsilon\gamma}d\theta, \end{aligned} \tag{6}$$

where the parameter ε denotes dark count and η_{b_0} denotes the single photon detection efficiency of the detector. $\bar{c}$ indicates the detector b_0 has no click. Then, the probability of having n photons in mode a and producing a click in Alice's threshold detector b_0 is

$$p_n^{(c)} = p_n^{(T)} - p_n^{(\bar{c})}, \tag{7}$$

where c indicates the detector b_0 has a click.

Estimation of the key generation rate. We modify the Gottesman-Lo-Lutkenhaus-Preskill (GLLP) formula[39] according to the RRDPS QKD security analysis[18]. From the GLLP formula, we have

$$LR^{(l)} = Q^{(l)}(1 - fh(E^{(\bar{c})}) - h(e_n^{(ph)})), \tag{8}$$

where $R^{(l)}, l \in \{c, \bar{c}\}$ indicates the key generation rate of RRDPS QKD with passive decoy state between Alice and Bob. $e_n^{(ph)}$ denotes the phase error rate of n-photon pulses. f is the efficiency of the error correction protocol, $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. $Q^{(l)}$ and $E^{(l)}$ indicate the total gain and the quantum bit error rate (QBER) corresponding to setting l, respectively. Thus, combine with $Q^{(l)} = \sum_{n=0}^{\infty} p_n^{(l)} Y_n$, we get the new key generation rate formula

$$LR^{(l)} = Q^{(l)} - Q^{(l)}fh(E^{(\bar{c})}) - \sum_{n=0}^{V_{th}} Y_n p_n^{(l)} h(e_n^{(ph)}), \tag{9}$$

where we denote the output that cause no click of Alice's detector b_0 as signal states. The ones that cause a click of Alice's detector b_0 are decoy states. As for RRDPS protocol, the phase error rate depends on the preparation of quantum states rather than the transmission process. When the number of photons in a train is no more than an integer $V_{th}\left(V_{th} < \frac{L-1}{2}\right)$, the phase error rate $e_n^{(ph)}$ can be bounded by $V_{th}/L - 1$[13]. So we can get R, the final key generation rate per pulse of RRDPS QKD with passive decoy state between Alice and Bob, it's the main parameter to evaluate the performance of protocol,

$$R = R^{(c)} + R^{(\bar{c})}. \tag{10}$$

Next, we give how to obtain the parameters $Q^{(l)}$ and $E^{(l)}$ corresponding to setting l. The gain $Q^{(l)}$ corresponding to setting l is the probability that Bob obtains a click in his measurement apparatus when Alice sends him a state prepared with setting l. It can be written as

$$Q^{(l)} = \sum_{n=0}^{\infty} p_n^{(l)} Y_n, \tag{11}$$

where Y_n denotes the yield of an n-photon state. Similarly, the quantum bit error rate (QBER) associated to setting l, which we shall denote as $E^{(l)}$, is given by

$$Q^{(l)}E^{(l)} = \sum_{n=0}^{\infty} p_n^{(l)} Y_n e_n, \tag{12}$$

with e_n representing the error rate of an n-photon state.

The yields Y_n can be expressed as refs 34,35

$$Y_n = 1 - (1 - Y_0)(1 - \eta)^n, \tag{13}$$

where Y_0 is the background rate, η represents the overall transmittance of the system. This quantity can be written as

$$\eta = \eta_c \eta_B, \tag{14}$$

where η_c is the transmittance of the quantum channel, and η_B denotes the overall transmittance of Bob's detection apparatus; that is, η_B includes the transmittance of any optical component within Bob's measurement device and the detector efficiency. The parameter η_c can be related with a transmission distance D measured in km for the given QKD scheme as

$$\eta_c = 10^{-\frac{\alpha D}{10}}, \tag{15}$$

where α represents the loss coefficient of the channel measured in dB/km.

The n-photon error rate e_n is given by refs 25,26

$$e_n = \frac{Y_0 e_0 + (Y_n - Y_0) e_d}{Y_n}, \tag{16}$$

where e_d is the probability that a signal hits the wrong detector on Bob's side due to the misalignment in the quantum channel and in his detection setup. As usual, we also consider that the background is random (i.e. $e_0 = 1/2$).

$Q^{(c)}$ and $Q^{(\bar{c})}$ denote the overall gains in the case of Alice's detector producing a click and no click, respectively. $Q^{(T)}$ denotes the overall gain that Alice ignores the result of her measurement in mode b, i.e. the sum of the gains $Q^{(c)}$ and $Q^{(\bar{c})}$. After substituting Eqs (5), (6) and (13–15) into the gain formulas Eq. (11) we obtain:

$$Q^{(T)} = 1 - (1 - Y_0) e^{-\eta_{b_0}\omega} I_{0,\eta\xi}, \tag{17}$$

$$Q^{(\bar{c})} = p^{(\bar{c})} - (1 - \varepsilon)(1 - Y_0) e^{(\eta_{b_0} - \eta)\omega - \eta_{b_0} v} I_{0,(\eta_{b_0} - \eta)\xi}, \tag{18}$$

$$Q^{(c)} = Q^{(T)} - Q^{(\bar{c})}, \tag{19}$$

where $I_{q,z}$ represents the modified Bessel function of the first kind, $\omega = L\mu_1 t + L\mu_2(1-t)$. From the Eqs (11), (12), (16) we can get:

$$\begin{aligned} Q^{(T)}E^{(T)} &= \sum_{n=0}^{\infty} p_n^{(T)} Y_n \left[\frac{Y_0(e_0 - e_d)}{Y_n} + e_d\right] = \sum_{n=0}^{\infty} p_n^{(T)} Y_0(e_0 - e_d) + \sum_{n=0}^{\infty} p_n^{(T)} Y_n e_d \\ &= Y_0(e_0 - e_d) + Q^{(T)} e_d, \end{aligned}$$

thus

$$E^{(T)} = \frac{(e_0 - e_d) Y_0}{Q^{(T)}} + e_d. \tag{20}$$

Then, in a similar way, we can get

$$E^{(\bar{c})} = \frac{(e_0 - e_d) Y_0 p^{(\bar{c})}}{Q^{(\bar{c})}} + e_d, \tag{21}$$

$$E^{(c)} = E^{(T)} - E^{(\bar{c})}. \tag{22}$$

And from the Eq. (6) we have

$$p^{(\bar{c})} = \sum_{n=0}^{\infty} p_n^{(\bar{c})} = (1 - \varepsilon) e^{-\eta_d \omega} I_{0,\eta\xi}. \tag{23}$$

For practical implementations, large photon numbers are negligible comparing with those from small photon numbers. So we only consider the photon numbers for $n = 0, 1, 2$. The expressions of $p_n^{(T)}$ with $n = 0, 1, 2$ in Eq. (5) are ref. 37:

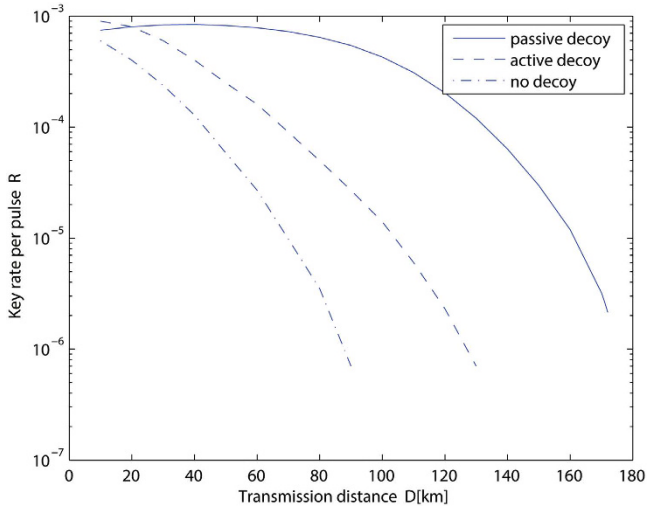

Figure 2. Key generation rate vs the transmission distance in RRDPS QKD with the passive decoy state method (solid line), the active decoy state method (dashed line; ref. 31) and no decoy state (dot-dashed line; ref. 17).

$$p_0^{(T)} = I_{0,\xi} e^{-\omega}, \tag{24}$$

$$p_1^{(T)} = (\omega I_{0,\xi} - \xi I_{1,\xi}) e^{-\omega}, \tag{25}$$

$$p_2^{(T)} = \frac{1}{2}\left[\omega^2 I_{0,\xi} + (1-2\omega)\xi I_{1,\xi} + \xi^2 I_{2,\xi}\right] e^{-\omega}. \tag{26}$$

The probabilities $p_n^{(\bar{\epsilon})}$ with $n = 0, 1, 2$ in Eq. (6) have the form ref. 37

$$p_0^{(\bar{\epsilon})} = \tau I_{0,(1-\eta_{b_0})\xi}, \tag{27}$$

$$p_1^{(\bar{\epsilon})} = \tau [\omega I_{0,(1-\eta_{b_0})\xi} - \xi I_{1,(1-\eta_{b_0})\xi}], \tag{28}$$

$$p_2^{(\bar{\epsilon})} = \frac{\tau}{2}\left[\omega^2 I_{0,(1-\eta_{b_0})\xi} + \left(\frac{1}{1-\eta_{b_0}} - 2\omega\right)\xi I_{1,(1-\eta_{b_0})\xi}\right] + \frac{\tau}{2}\xi^2 I_{2,(1-\eta_{b_0})\xi}, \tag{29}$$

where $\tau = (1-\varepsilon) e^{[-\eta_{b_0}\upsilon + (1-\eta_{b_0})\omega]}$.

Numerical Simulation. According to the security analysis in above section, we can get the key generation rate Eq. (8) plotted in Fig. 2.

The parameters used in our method are the misalignment error rate $e_d = 1.5\%$, the background rate $Y_0 = 3 \times 10^{-6}$, $\eta_d = 0.12$, and $f = 1$, $t = 1/2$, which are the same as those in the original proposal for the active decoy state method in ref. 40. Then we can get

$$\begin{aligned} \upsilon &= L(\mu_1 + \mu_2), \\ \gamma &= \frac{\frac{L}{2}(\mu_1 + \mu_2) + \xi \cos\theta}{\upsilon}, \\ \xi &= L\sqrt{\mu_1 \mu_2}, \\ \omega &= \frac{L}{2}(\mu_1 + \mu_2). \end{aligned} \tag{30}$$

We show the relations between key generation rate and the transmission distance in RRDPS QKD protocol in Fig. 2. Given the certain transmission distance, we optimize the intensity of sources to maximize the key generation rate. According to the practical system, the key generation rate had better not lower than 10^{-7}. Thus we can obtain the maximal transmission distance as shown in 2.

From Fig. 2, we can see that the longer the transmission distance D is, the smaller the key generation rate R will be. We also show the performance comparison between our method, the active decoy state method[31] and the

original protocol RRDPS[17]. It can clearly be seen that the passive decoy state method can provide a performance improvement over the active one and the original one. That is, under the same key generation rate, our protocol will have longer transmission distance. Furthermore, it can defeat the photon-number-splitting (PNS) attack and guarantee the security against the imperfect sources compared to the original RRDPS QKD protocol[17]. It can also eliminate side channel attacks on sources, which may be caused by actively modulating decoy states[31].

Discussion

In summary, we apply the passive decoy state method in the RRDPS QKD which was proposed recently, and give a security analysis of this protocol. Using the passive decoy state method, the RRDPS QKD protocol provides a secure way to exchange private information without monitoring conventional disturbances and still maintains a high tolerance of noise. And it can also exclude the source side channel attacks, which the active source modulation method may bring. According to the RRDPS QKD security analysis, we modify the GLLP formula and derive a new key generation rate formula for our RRDPS protocol using passive decoy state method. Most importantly, we enhance the key generation rate. From the numerical simulations, we find that the RRDPS QKD with the passive decoy state method can have a performance improvement to the protocol with the active decoy state method and the original RRDPS protocol without decoy states.

The active decoy state method itself may introduce another loophole while closing the loophole of multiphoton pulses. As is well known, the active decoy state method is demonstrated based on the assumption that Eve can never distinguish the decoy state and the signal state. Unfortunately, this assumption is invalid in certain conditions, and Eve can beat the decoy state method due to the property of the intensity modulator. ref. 32 demonstrates that Eve can get full information about the key generated between the legitimate parties in QKD with active decoy state method. Compared with active selection, the passive decoy state method can reduce the side channel information in the decoy state preparation procedure. Thus, the passive signal and decoy state selection can avoid the side channel attacks on sources, which may be generated by active modulation of source intensities. Although the passive decoy state method can not remove all side channel attacks on sources, it can still avoid more attacks than the protocol with no decoy states and the active decoy states. Similar to the active decoy state method, the passive one can also defeat PNS attack. So we apply the passive decoy state method to the RRDPS QKD protocol, this strategy is very promising for applications of practical systems.

References

1. Bennett, C. H. & Brassard. G. Quantum cryptography: public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* 175–179 (1984).
2. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441 (2000).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
4. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 2050 (1999).
5. Shields, A. & Yuan, Z. Key to the quantum industry. *Phys. World* **20,** 24 (2007).
6. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19,** 10387–10409 (2011).
7. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661 (1991).
8. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68,** 3121 (1992).
9. Bruß, D. Optimal Eavesdropping in Quantum Cryptography with Six States. *Phys. Rev. Lett.* **81,** 3018 (1998).
10. Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89,** 037902 (2002).
11. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92,** 057901 (2004).
12. Tamaki, K., Koashi, M. & Imoto, N. Unconditionally secure key distribution based on two nonorthogonal states. *Phys. Rev. Lett.* **90,** 167904 (2003).
13. Boileau, J. C., Tamaki, K., Batuwantudawe, J., Laflamme, R. & Renes, J. M. Unconditional security of a three state quantum key distribution protocol. *Phys. Rev. Lett.* **94,** 040503 (2005).
14. Tamaki, K. & Lo, H. K. Unconditionally secure key distillation from multiphotons. *Phys. Rev. A* **73,** 010302(R) (2006).
15. Wen, K., Tamaki, K. & Yamamoto, Y. Unconditional security of single-photon differential phase shift quantum key distribution. *Phys. Rev. Lett.* **103,** 170503 (2009).
16. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3,** 634 (2012).
17. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature (London)* **509,** 475 (2014).
18. Zhang, Z., Yuan, X., Cao, Z. & Ma, X. Round-robin differential-phase-shift quantum key distribution. arXiv:1505.02481 (2015).
19. Mizutani, A., Imoto, N. & Tamaki, K. Robustness of the round-robin differential-phase-shift quantum-key-distribution protocol against source flaws. *Phys. Rev. A* **92,** 060303(R) (2015).
20. Guan, J. Y. *et al.* Experimental passive round-robin differential phase-shift quantum key distribution. *Phys. Rev.Lett.* **114,** 180502 (2015).
21. Takesue, H., Sasaki, T., Tamaki, K. & Koashi, M. Experimental quantum key distribution without monitoring signal disturbance. *Nat. Photonics* **9,** 827 (2015).
22. Wang, S. *et al.* Experimental demonstration of a quantum key distribution without signal disturbance monitoring. *Nat. Photonics* **9,** 832 (2015).
23. Li, Y. H. Experimental round-robin differential phase-shift quantum key distribution. *Phys. Rev. A* **93,** 030302(R) (2016).
24. Hwang, W. Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
25. Ma, X. F., Qi, B., Zhao, Y. & Lo, H. K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72,** 012326 (2005).
26. Lo, H. K., Ma, X. F. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
27. Wang, X. B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
28. Song, T. T., Zhang, J., Qin, S. J., Gao, F. & Wen, Q. Y. Finite-key analyses for quantum key distribution with decoy-states. *Quant. Inf. Comp.* **11,** 374–389 (2011).
29. Lin, S., Wen, Q. Y., Gao, F. & Zhu, F. C. Eavesdropping on secure deterministic communication with qubits through photon-number-splitting attacks. *Phys. Rev. A* **79,** 054303 (2009).
30. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys.Rev. Lett.* **85,** 1330 (2000).
31. Zhang, Y. Y. *et al.* Practical round-robin differential phase-shift quantum key distribution. *Opt. Express* **24.** 020763 (2016).

32. Jiang, M. S., Sun, S. H., Li, C. Y. & Liang, L. M. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. *Phys. Rev. A* **86,** 032310 (2012).
33. Ma, X. F. & Lo, H. K. Quantum key distribution with triggering parametric down-conversion sources. *New J. Phys.* **10,** 073018 (2008).
34. Mauerer, W. & Silberhorn, C. Quantum key distribution with passive decoy state selection. *Phys. Rev. A* **75,** 050305(R) (2007).
35. Adachi, Y., Yamamoto, T., Koashi, M. & Imoto, N. Simple and efficient quantum key distribution with parametric down-conversion. *Phys. Rev.Lett.* **99,** 180503 (2007).
36. Song, T. T., Qin, S. J., Wen, Q. Y., Wang, Y. K. & Jia, H. Y. Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources. *Scientific Reports* **5,** 15276 (2015).
37. Curty, M., Ma, X., Qi, B. & Moroder, T. Passive decoy-state quantum key distribution with practical light sources. *Phys. Rev. A* **81,** 022310 (2010).
38. Curty, M., Moroder, T., Ma, X. & Lütkenhaus, N. Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution. *Opt. Lett.* **34,** 3238 (2009).
39. Gottesman, D., Lo, H. K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4,** 325 (2004).
40. Sun, S. H., Gao, M., Li, C. Y. & Liang, L. M. Practical decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **87,** 052329 (2013).

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant Nos 61572081, 61672110, 61671082).

Author Contributions

L.L. proposed the theoretical method. L.L. and F.Z.G. wrote the main manuscript text. S.J.Q. and Q.Y.W. reviewed the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Liu, L. *et al.* Round-robin differential-phase-shift quantum key distribution with a passive decoy state method. *Sci. Rep.* **7**, 42261; doi: 10.1038/srep42261 (2017).

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.