www.nature.com/scientificreports

SCIENTIFIC REPORTS

OPEN

Received: 15 January 2015
Accepted: 17 September 2015
Published: 14 October 2015

An improved scheme on decoy-state method for measurement-device-independent quantum key distribution

Dong Wang[1,2,3,4], Mo Li[1,2,3,4], Guang-Can Guo[1,2,3,4] & Qin Wang[1,2,3]

Quantum key distribution involving decoy-states is a significant application of quantum information. By using three-intensity decoy-states of single-photon-added coherent sources, we propose a practically realizable scheme on quantum key distribution which approaches very closely the ideal asymptotic case of an infinite number of decoy-states. We make a comparative study between this scheme and two other existing ones, i.e., two-intensity decoy-states with single-photon-added coherent sources, and three-intensity decoy-states with weak coherent sources. Through numerical analysis, we demonstrate the advantages of our scheme in secure transmission distance and the final key generation rate.

Quantum key distribution (QKD) entails two legitimate parties, Alice and Bob, to distribute secure keys in the presence of an eavesdropper, Eve[1]. The security of QKD has been established theoretically by virtue of the principle of quantum mechanics[2–4]. However, the security claims are based on theoretical and idealized assumptions, such as some convenient models on the photon sources or the detectors, which are not necessarily met by experimental implementations. In experiment, one usually adopts the weak coherent state (WCS) generated from attenuated lasers to replace the ideal single-photon source, which is unavailable at present. Nevertheless, there are non-negligible multi-photon components in WCS, which can be exploited by Eve via the photon-number-splitting (PNS) attack[5–7].

To combat the PNS attack, the powerful decoy-state method is proposed[8–17]. Then more work about the decoy-state method with an arbitrary number of intensities and related security analysis for finite key length have been discussed[18–20]. The decoy-state method can be further combined with the newly proposed measurement-device-independent quantum key distribution (MDI-QKD) to fight all other potential detector side-channel attacks[21–27]. Through the decoy-state method, one can estimate the lower bound of the counting rate and the upper bound of the quantum-bit error-rate (QBER) caused by two-single-photon pulses, and thus obtain a lower bound for the secure key rate. In order to get more precise estimations, one can use better light sources with negligible vacuum component and multi-photon probabilities[15,16], or use more intensities of decoy-states[11,25]. Large number of intensities of decoy-states will cause experimental difficulties and larger statistical fluctuations. In this report, by using single-photon-added coherent sources (SPACS)[28,29], we propose a scheme involving only three intensities of decoy-states which nevertheless can approach very closely the asymptotic case involving infinite number of intensities.

[1]Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China. [2]Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China. [3]Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China. [4]Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China. Correspondence and requests for materials should be addressed to Q.W. (email: qinw@njupt.edu.cn)

SPACS has a relatively high probability of single-photon and no vacuum component. In principle, the state $|\alpha, 1\rangle$ of SPACS can be generated by the elementary one-photon excitation on a coherent state[28–30], and is theoretically described by applying the photon creation operator $\hat{a}^\dagger$ to a coherent state $|\alpha\rangle$:

$$|\alpha, 1\rangle := \frac{\hat{a}^\dagger|\alpha\rangle}{\sqrt{1+|\alpha|^2}} = \frac{e^{-|\alpha|^2/2}}{\sqrt{1+|\alpha|^2}}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\sqrt{n+1}\,|n+1\rangle.$$

It is clear that there is no vacuum term contribution in the state of SPACS. The probability of finding n photons is

$$P_n(\mu) = \frac{n}{\lambda+1}e^{-\lambda}\frac{\lambda^{n-1}}{(n-1)!},\quad n = 1, 2, \cdots$$

where $\lambda := -\frac{1}{2}(\sqrt{\mu^2 - 2\mu + 5} + \mu - 3)$ and μ is the mean photon number. SPACS has been experimentally created with high efficiency and fidelity[29–34]. In particular, Zavatta *et al.* prepared the SPACS by a conditional technique through parametric down-conversion process[30,34], where a piece of LBO crystal is pumped with a Ti:sapphire laser working at 393 nm, and the generated SPACS is working at 786 nm, the overall efficiency obtained is 60%, and the corresponding state fidelity is up to 99.5%. In general, almost all the conditions required for QKDs had been matched except for the signal wavelength. Nevertheless, we find no in-principle difficulty in generating the SPACS at telecommunication wavelength since what we need is only to change the phase-match conditions inside nonlinear crystals, e.g., replacing LBO with PPKTP. Therefore, it is feasible to apply SPACS to QKD under present technology.

In this report, we apply SPACS to MDI-QKD by using three-intensity and combining the method proposed by Zhou *et al.*[25]. Due to the absence of vacuum component in SPACS, we need not take the contribution of vacuum pulses into account as in other schemes. Using only three non-zero intensities (two decoy-states and one signal state) of SPACS, we can get precise estimation of the counting rate and the quantum bit error rate (QBER) caused by single-photon pulses, which leads to significantly improved final key generation rate and secure transmission distance.

For our scheme, we will need the following results. First, when $n \geqslant 2$ and $1 \le \mu_x < \mu_y$, the photon number distribution in a state of SPACS has the following property

$$\frac{P_n(\mu_y)}{P_n(\mu_x)} \geqslant \frac{P_2(\mu_y)}{P_2(\mu_x)} \geqslant \frac{P_1(\mu_y)}{P_1(\mu_x)} \tag{1}$$

which follows from

$$\frac{P_{n-1}(\mu_x)}{P_n(\mu_x)} - \frac{P_{n-1}(\mu_y)}{P_n(\mu_y)} = \frac{(n-1)!}{n}\left(\frac{1}{\lambda_x^{n-1}} - \frac{1}{\lambda_y^{n-1}}\right) \geqslant 0,$$

where $\lambda_\xi = \frac{1}{2}(\sqrt{\mu_\xi^2 - 2\mu_\xi + 5} + \mu_\xi - 3)$, $\xi = x, y, z$. The last inequality is ensured by $\lambda_x < \lambda_y$ since $1 \le \mu_x < \mu_y$.

Next, when $i \le j \le k$ and $\mu_x \le \mu_y \le \mu_z$, it holds that

$$\begin{aligned} G(i, j, k) := {} & [g_i(\mu_x) - g_j(\mu_x)][g_j(\mu_y) - g_k(\mu_y)] \\ & - [g_i(\mu_y) - g_j(\mu_y)][g_j(\mu_x) - g_k(\mu_x)] \geqslant 0, \end{aligned} \tag{2}$$

where $g_l(\mu_\xi) := \frac{P_l(\mu_\xi)}{P_l(\mu_z)}$, $l \geqslant 1$, $\xi = x, y, z$. To prove this, note that

$$g_l(\mu_\xi) = e^{\lambda_z - \lambda_\xi}\left(\frac{1+\lambda_z}{1+\lambda_\xi}\right)\left(\frac{\lambda_\xi}{\lambda_z}\right)^{l-1},\quad l = i, j, k;\ \xi = x, y, z,$$

and $G(i, j, k)$ can be rewritten as

$$G(i, j, k) = \frac{1}{\lambda_x\lambda_y\lambda_z^{i+j+k-2}}\begin{vmatrix} \lambda_x^i & \lambda_x^j & \lambda_x^k \\ \lambda_y^i & \lambda_y^j & \lambda_y^k \\ \lambda_z^i & \lambda_z^j & \lambda_z^k \end{vmatrix}$$

which is positive due to the property of generalized Vandermonde determinant and the conditions $i \le j \le k$, $\lambda_x < \lambda_y < \lambda_z$.

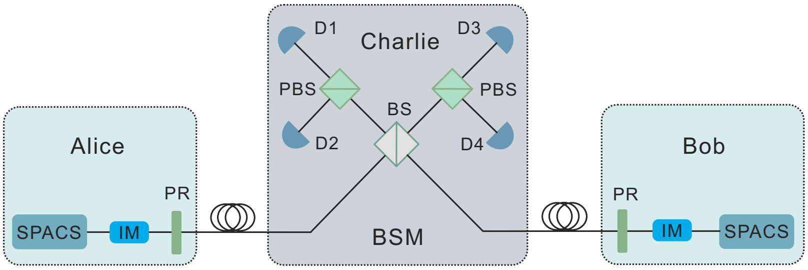

Figure 1. A schematic setup of MDI-QKD using the SPACSs. Alice and Bob randomly prepare SPACSs in a BB84 polarization state with a polarization rotator (PR). Intensity modulator (IM) is used to generate decoy-states. Charlie performs a partial BSM when the signal pulses from Alice and Bob arrive at a 50:50 beam splitter (BS). Four single-photon detectors (D1–D4) are employed to detect the results.

Improved 3-intensity decoy-state method for MDI-QKD

In MDI-QKD, Alice and Bob simultaneously send signals to an untrusted third party (UTP, possibly controlled by an eavesdropper Eve). The UTP performs a partial BSM and announces whether the measurement result is successful. According to the UTP's announcement, those successful events will be post-selected and further processed for the final key generation by Alice and Bob. A schematic setup of our three-intensity decoy-state MDI-QKD with SPACS is shown in Fig. 1. Alice and Bob need to randomly prepare the signals with intensities α, β, respectively, where $\alpha, \beta \in \{\mu_x, \mu_y, \mu_z\}$. Here μ_x and μ_y are the intensities of the two decoy-states, while μ_z is the intensity of the signal state, $\mu_x < \mu_y < \mu_z$. When Alice and Bob send signals with intensities α and β, respectively, the gain and QBER are given by

$$Q_{\alpha,\beta}^{W} = \sum_{n,m=1}^{\infty} P_n(\alpha) P_m(\beta) Y_{nm}^{W}, \quad E_{\alpha,\beta}^{W} Q_{\alpha,\beta}^{W} = \sum_{n,m=1}^{\infty} P_n(\alpha) P_m(\beta) e_{nm}^{W} Y_{nm}^{W},$$

respectively. Here W represents the Z- or X-basis, and n, m denote the number of photons sent by Alice and Bob, respectively. Y_{nm}^{W} denotes the yield, and e_{nm}^{W} denotes the error rate, when Alice sends an n-photon pulse and Bob sends an m-photon pulse to the UTP. The decoy-states and signal-state are prepared in different bases. Hereafter we shall omit the superscript W without causing any confusion.

As demonstrated in ref. 25, as long as inequalities (1) and (2) are satisfied, we can get the lower bound of Y_{11} by using the lowest two intensities (μ_x and μ_y) for Alice and Bob such that

$$\begin{aligned} Y_{11} \geq Y_{11}^{L} = {} & \frac{[P_1(\mu_x)P_2(\mu_y) + P_1(\mu_y)P_2(\mu_x)]Q_{\mu_x,\mu_x}}{P_1^2(\mu_x)[P_1(\mu_x)P_2(\mu_y) - P_1(\mu_y)P_2(\mu_x)]} \\ & - \frac{P_2(\mu_x)(Q_{\mu_x,\mu_y} + Q_{\mu_y,\mu_x})}{P_1(\mu_x)[P_1(\mu_x)P_2(\mu_y) - P_1(\mu_y)P_2(\mu_x)]}. \end{aligned} \tag{3}$$

Moreover, we can get an upper bound of e_{11} by inequalities (1) and (2) as[25]

$$e_{11} \leq e_{11}^{U} := \frac{1}{\gamma^2 Y_{11}^{L}} \begin{vmatrix} T_x & T_y & T_z \\ P_2(\mu_x) & P_2(\mu_y) & P_2(\mu_z) \\ P_3(\mu_x) & P_3(\mu_y) & P_3(\mu_z) \end{vmatrix}, \tag{4}$$

where $\gamma = P_1(\mu_z)P_2(\mu_z)P_3(\mu_z)G(1, 2, 3)$, and for $\xi \in (x, y, z)$,

$$\begin{aligned} T_{\xi} = {} & [g_2(\mu_y) - g_3(\mu_y)]E_{\mu_\xi,\mu_x}Q_{\mu_\xi,\mu_x} - [g_2(\mu_x) - g_3(\mu_x)]E_{\mu_\xi,\mu_y}Q_{\mu_\xi,\mu_y} \\ & + [g_3(\mu_y)g_2(\mu_x) - g_3(\mu_x)g_2(\mu_y)]E_{\mu_\xi,\mu_z}Q_{\mu_\xi,\mu_z}. \end{aligned}$$

In our protocol, the Z-basis is used as the key generation basis, and the X-basis is for error testing only. Then by inequalities (3) and (4), one can obtain the lower bound of the successful single-photon yield $Y_{11}^{Z,L}$ in the Z-basis and the upper bound of the single-photon error rate $e_{11}^{X,U}$ in the X-basis. The final secure key rate can be calculated with the observed total gains and error rates as

$$R \geqslant P_1^2(\mu_z) Y_{11}^{Z,L}[1 - H(e_{11}^{X,U})] - Q_{\mu_z,\mu_z}^{Z} f H\left(E_{\mu_z,\mu_z}^{Z}\right), \tag{5}$$

η_d	Y_0	e_d	e_0	α	f
14.5%	3.0×10^{-6}	1.5%	0.5	0.2 dB/km	1.16

Table 1. Parameters values for simulations. η_d and Y_0 are the transmittance and dark count rate; e_d is the probability that the survived photon hits a wrong detector, which is independent of the transmission distance, and e_0 is the error rate of dark count; α is the transmission fiber loss constant; f is the error correction efficiency. The UTP is located midway between Alice and Bob, and all detectors are identical.

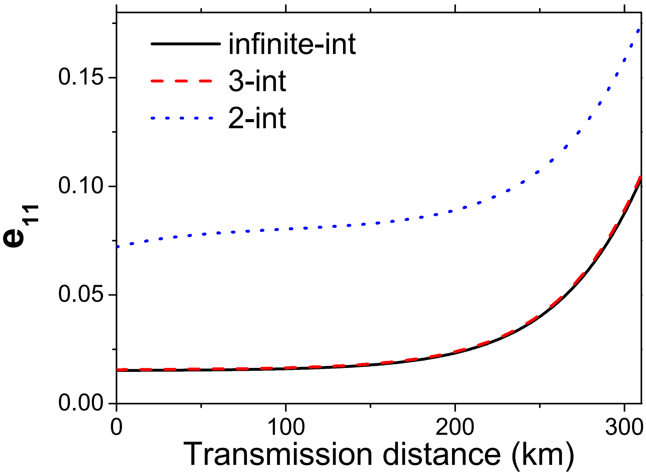

Figure 2. Comparison of the estimated values of e_{11} for MDI-QKD with SPACS by using different number of decoy states. The dashed curve represents the result of our three-intensity decoy-state method, the solid curve represents the result of using an infinite number of decoy-states, and the dotted curve corresponds to the result of two-intensity decoy-states method.

with f being the error correction efficiency and $H(p) := -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary Shannon entropy function.

Numerical Simulation

With inequalities (3–5) we can perform corresponding numerical simulation for our three-intensity MDI-QKD with SPACS. We further compare our scheme with the two-intensity MDI-QKD involving SPACS[35] and the conventional three-intensity MDI-QKD involving WCS[23]. For the total gains and error rates, which can be directly measured from the experiment, we use the channel model and method as in[27] to estimate these values. The relevant parameters are listed in Table 1 [21]. During the simulation, for the two-intensity or our three-intensity decoy-states with SPACS, we set reasonable intensities with $\mu_x = 1.05$, $\mu_y = 1.06$ for the decoy-states, and $\mu_z = 1.10$ for the signal-state. For the three-intensity decoy-states with WCS, we set $\mu_x = 0$, $\mu_y = 0.1$ for decoy-states, and optimize the intensity for the signal-state (μ_z) in each instance. Corresponding simulation results are shown in Figs 2 and 3.

In Fig. 2, we compare the estimation value of e_{11} between our three-intensity decoy-state method and the conventional two-intensity decoy-state method when both using SPACS. Obviously, by using our three-intensity decoy-state method, we can get significant improvement in the estimation of e_{11} over the conventional two-intensity decoy-state method. Moreover, our method approaches very closely the ideal value by using an infinite number of intensities of decoy-states.

In Fig. 3(a), we give the comparison of the key generation rates by using different methods, i.e., our three-intensity decoy-state with SPACS, the conventional two-intensity decoy-state with SPACS, and the three-intensity decoy-state with WCS. In each case the key generation rate has been normalized by the corresponding value of using an infinite number of intensities of decoy-states. We find from Fig. 3(a) that our scheme performs much better than the other two methods: Longer secure transmission distance and much higher key generation rate. In Fig. 3(b), the ratio of the key generation rate between our scheme and the other two methods have also been displayed. It can be seen that our scheme shows excellent behavior even at rather long distance (>200 km). It exhibits tens of times or even hundreds of times of enhancement in the key generation rate than the three-intensity decoy-state method with WCS at long distances (>150 km), see the left axis of Fig. 3(b). When compared with the conventional two-intensity decoy-state method with SPACS, our scheme obtains more than double enhancement in the key generation rate at very long distances (>200 km), see the right axis of Fig. 3(b).

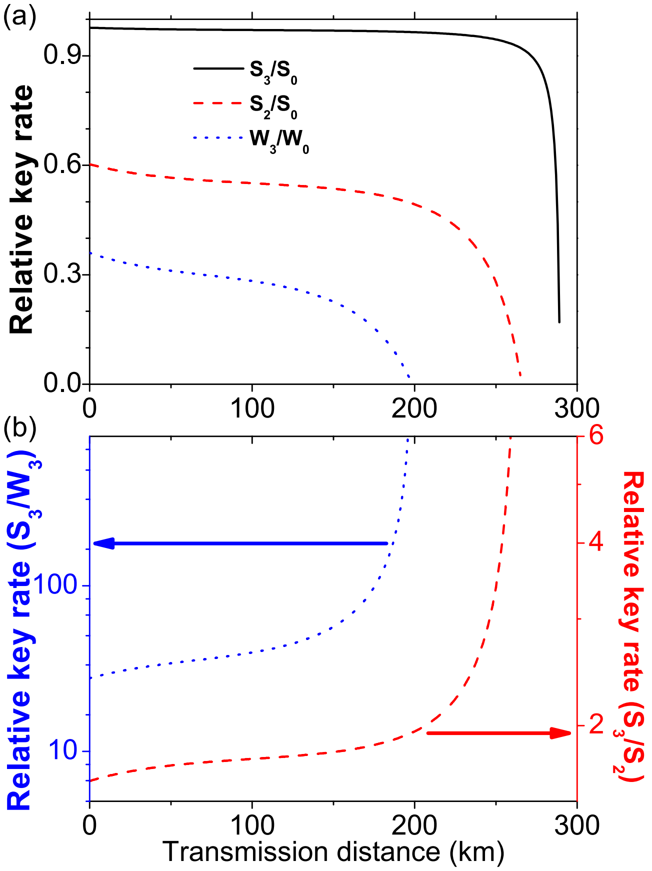

Figure 3. The relative key generation rates of different decoy-state MDI-QKD protocols, either with SPACS or WCS. S_3, S_2 or S_0 represents the key generation rate for MDI-QKD involving three-intensity, two-intensity or infinite decoy-state, with SPACS. W_3 and W_0 are the corresponding key generation rates with WCS. (**a**) Comparison of the normalized key generation rate for different methods, i.e., two- or three-intensity decoy-state SPACS, or the three-intensity decoy-state WCS. (**b**) The ratio of the key generation rates between our scheme and the conventional two-intensity decoy-state with SPACS or the three-intensity decoy-state with WCS.

Conclusion

We have introduced an improved scheme on MDI-QKD involving three-intensity decoy-state with SPACS, and have compared its performance with two existing methods. Through numerical simulation, we have demonstrated that our scheme shows excellent behavior in both the secure transmission distance and the final key generation rate. For example, when compared with the conventional two-intensity MDI-QKD with SPACS, the key generation rate is enhanced by several times. Compared with the three-intensity MDI-QKD with WCS, our scheme not only presents almost one hundred kilometers increasing in the secure transmission distance, but also shows tens of times enhancement in the final key generation rate. We emphasize that our scheme depends on SPACS which can be generated with current technology, although its present setup is relatively bulky and has higher technical requirements compared with the WCS system. We can expect that with the development of technology, the emergence of miniaturization and maturing of SPACS system will cause it to replace other sources and launches a wide implementation in quantum key distributions in the near future.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing* [175–179] (IEEE, New York, 1984).
2. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283,** 2050–2056 (1999).
3. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85,** 441–444 (2000).
4. Mayers D. Unconditional security in quantum cryptography, *J. ACM* **48,** 351–406 (2001).
5. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography, *Phys. Rev. Lett.* **85,** 1330–1333 (2000).
6. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution, *Phys. Rev. A* **61,** 052304 (2000).

7. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, *New J. Phys.* **4,** 44.1–44.9 (2002).
8. Hwang, W. Y. Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91,** 057901 (2003).
9. Wang, X. B. Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94,** 230503 (2005).
10. Lo, H. K., Ma, X. F. & Chen, K. Decoy state quantum key distribution, *Phys. Rev. Lett.* **94,** 230504 (2005).
11. Wang, X. B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light, *Phys. Rev. A* **72,** 012322 (2005).
12. Ma, X. F., Qi, B., Zhao, Y. & Lo, H. K. Practical decoy state for quantum key distribution, *Phys. Rev. A* **72,** 012326 (2005).
13. Zhao, Y., Qi, B., Ma, X. F., Lo, H. K. & Qian, L. Experimental quantum key distribution with decoy states, *Phys. Rev. Lett.* **96,** 070502 (2006).
14. Rosenberg, D. *et al.* Long-distance decoy-state quantum key distribution in optical fiber, *Phys. Rev. Lett.* **98,** 010503 (2007).
15. Wang, Q., Wang, X. B. & Guo, G. C. Practical decoy-state method in quantum key distribution with a heralded single-photon source, *Phys. Rev. A* **75,** 012312 (2007).
16. Wang, Q. & Karlsson, A. Performance enhancement of a decoy-state quantum key distribution using a conditionally prepared down-conversion source in the Poisson distribution, *Phys. Rev. A* **76,** 014309 (2007).
17. Wang, Q. *et al.* Experimental decoy-state quantum key distribution with a sub-Poissionian heralded single-photon source, *Phys. Rev. Lett.* **100,** 090501 (2008).
18. Hayashi, M. General theory for decoy-state quantum key distribution with an arbitrary number of intensities, *New Journal of Physics* **9,** 284 (2007).
19. Hayashi, M. Optimal decoy intensity for decoy quantum key distribution, arXiv:1311.3003 (2013).
20. Hayashi, M. Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths, *New Journal of Physics* **16,** 063009 (2014).
21. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108,** 130503 (2012).
22. Ma, X. F., Fung, C. H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution, *Phys. Rev. A* **86,** 052305 (2012).
23. Wang, X. B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, *Phys. Rev. A* **87,** 012320 (2013).
24. Wang, Q. & Wang, X. B. Efficient implementation if the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources, *Phys. Rev. A* **88,** 052332 (2013).
25. Zhou, Y. H., Yu, Z. W. & Wang, X. B. Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100%, *Phys. Rev. A* **89,** 052325 (2014).
26. Li, M. *et al.* Measurement-device-independent quantum key distribution with modified coherent state, *Opt. Lett.* **39,** 880–883 (2014).
27. Wang, Q. & Wang, X. B. Simulating of the measurement-device-independent quantum key distribution with phase randomized general sources, *Sci. Rep.* **4,** 04612 (2014).
28. Agarwal, G. S. & Tara, K. Nonclassical properties of states generated by the excitations on a coherent state, *Phys. Rev. A* **43,** 492 (1991).
29. Zavatta, A., Viciani, S. & Bellini, M. Quantum-to-classical transition with Single-photon-added coheret states of light, *Science* **306,** 660–662 (2004).
30. Zavatta, A., Viciani, S. & Bellini, M. Single-photon exciation of a coherent state: Catching the elementary step of stimulated light emission, *Phys. Rev. A* **72,** 023820 (2005).
31. Zavatta, A., Viciani, S. & Bellini, M. Non-classical field characterization by high-frequency, time-domain quantum homodyne tomography, *Laser Phys. Lett.* **3,** 3–16 (2005).
32. Barbieri, M. *et al.* Non-Gaussianity of quantum states: An experimental test on single-photon-added coherent states, *Phys. Rev. A* **82,** 063833 (2010).
33. Bellini, M., Coelho, A. S., Filippov, S. N., Manko, V. I. & Zavatta, A. Towards higher precision and operational use of optical homodyne tomograms, *Phys. Rev. A* **85,** 052129 (2012).
34. Filippov, S. N., Manko, V. I., Coelho, A. S., Zavatta, A. & Bellini, M. Single-photon-added coherent states: estimation of parameters and fidelity of the optical homodyne detection, *Phys. Scr.* **T153,** 014025 (2013).
35. Wang, D. *et al.* Quantum key distribution with the single-photon-added coherent source, *Phys. Rev. A* **90,** 062315 (2014).

Acknowledgments

Q.W. thanks S.L.L. and Y.H.Z. for useful discussion during this work. We gratefully acknowledge the financial support from the National Natural Science Foundation of China through Grants No. 11274178, No. 11311140250, No. 61475197, the Natural Science Foundation of the Jiangsu Higher Education Institutions through Grant No. 15KJA120002, and the Outstanding Youth Project of Jiangsu Province through Grant No. BK20150039.

Author Contributions

Q.W. proposed the idea, wrote the source code, analyzed the numerical results and did changes on the manuscript, D.W. did numerical simulation and wrote the manuscript, M.L. assisted in doing numerical simulation and drawing figures, G.C.G. did comments and changes on the manuscript.

Additional Information

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

How to cite this article: Wang, D. *et al.* An improved scheme on decoy-state method of measurement-device-independent quantum key distribution. *Sci. Rep.* **5**, 15130; doi: 10.1038/srep15130 (2015).