SCIENTIFIC REPORTS

OPEN

Measurement-device-independent quantum key distribution via quantum blockade

Received: 4 July 2017
Accepted: 18 December 2017
Published online: 07 March 2018

Yi-Heng Zhou[1,2], Zong-Wen Yu[1,3], Ao Li[1,2], Xiao-Long Hu[1,2], Cong Jiang[1,2] & Xiang-Bin Wang[1,2,4]

Efficiency in measurement-device-independent quantum key distribution(MDI-QKD) can be improved not only by the protocol, but also single-photon sources. We study the behavior of MDI-QKD with statistical fluctuation using quantum blockade source. Numerical simulation for a type of 4-intensity protocol shows that, after parameter optimization, this source can improve the final key rate by 100 times compared with traditional weak coherent state sources.

Quantum key distribution (QKD)[1–5] allows two remote parties to distribute secure keys through public channels. QKD can ensure unconditional security guaranteed by the laws of quantum physics[1–5]. However, in practical implementation, the imperfections of QKD system like imperfect single-photon sources will cause loopholes that eavesdropper may make use of. To overcome this insecurity, the decoy state method was proposed[6–26], and one can still keep the unconditional security of QKD with imperfect single-photon sources[27–31]. Then, to patch up the loophole caused by the limitation of detection efficiency as well as channel losses[32,33], the device independent QKD (DI-QKD)[34–37] and the measurement-device independent QKD (MDI-QKD)[38–40] were developed. The combination of the decoy-state method and MDI-QKD has been studied both experimentally[41–45] and theoretically[46–57].

Yet, because of the complexity of the system compared with the BB84 protocol, the key rate of the decoy-state MDI-QKD is rather lower than BB84. Taking into account the statistical fluctuation, the data size and the communication time become the great influence to the final key rate[47,48,50,56]. For example, the number of total pulses at each side N is usually larger than 10^{12} to generate keys. To overcome this difficulty, previously[58] we provided a very efficient 4-intensity protocol which can remarkably improve the key rate and communication distance. It can improve the key rate by almost 2 magnitude orders after parameter optimization. However, one should not counted on the unrealistic wish to further improve the efficiency unlimitedly by taking progress on the protocol only. We should also consider the path of improving the quality of the single-photon sources. Generally, at present the weak coherent state(WCS) sources are used for practical QKD. But the WCS pulses have a large vacuum component and significant fraction of multi-photon states, these will severely reduce the key rate and transmission distance. The situation is even worse in MDI-QKD because the large fraction of vacuum pulses(both vacuum decoy states and vacuum fraction in a Poisson pulse) at one side lead to a large observed value of the error rate in X basis. Fortunately, a quantum blockade source(QBS) can conspicuously enhance the signal photon component. The method of using quantum blockade source in QKD was proposed[59] with a simple simulation of asymptotic key rate. However, it considers only the traditional BB84 protocol, it has not studied the important MDI-QKD and the finite size effects for practical QKD. Here in this work, we study the application of quantum blockade source in practical decoy state method MDI-QKD with most high efficient protocol, the 4-intensity protocol. Our numerical results will verify the remarkable progress of about 100 times rise in key rate.

Results

The photon blocade. Photon blockade as a nonlinear quantum optical process can be realized experimentally with single atoms coupled to a resonator[60,61], solid-state with (quantum dot) QD coupled to dielectric resonators[62–65] and nonlinear Kerr medium[66,67]. Particularly, Kerr-type material has advantages in its controllability

[1]Department of Physics, State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing, 100084, People's Republic of China. [2]Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, 230026, China. [3]Data Communication Science and Technology Research Institute, Beijing, 100191, China. [4]Jinan Institute of Quantum technology, SAICT, Also a member of Center for Atomic and Molecular Nanosciences at Tsinghua University, Jinan, 250101, People's Republic of China. Yi-Heng Zhou and Zong-Wen Yu contributed equally to this work. Correspondence and requests for materials should be addressed to X.-B.W. (email: xbwang@mail.tsinghua.edu.cn)

	P_0	P_1	P_2	P_3
I	39.15%	47.38%	12.88%	0.06%
II	25.75%	67.92%	6.30%	0.03%
III	24.17%	71.37%	4.42%	0.05%

Table 1. The photon number probability of two typical different sets of system parameters in ref.[59].

and flexibility. To obtain a high quality single-photon sources, in our previous work(OL2016), we have calculated and simulated explicitly the photon-number distribution for pulses outside cavities. In the single-photon blockade using Kerr-type resonators under the condition of different parameters, it reveals an optimized single-photon state probability. In that work, we have simulated the system with quantum trajectory method[68–70]. In this method, for each single trajectory we simulate, we monitory the number of photons from the output of the resonantor. And the output light could be generally expanded in the Fock basis as: $|a_{out}\rangle = \sum_{n=0}^{\infty} c_n|n\rangle$ where $|c_n|^2$ is the probability of photon state $|n\rangle$. At last we can estimate the photon number probability $P_n = \frac{|c_n|^2}{\sum |c_i|^2}$ from the number of counted photons.

Obviously, when evaluating the superiority of certain sources in decoy state method QKD, the photon number probability is wanted. To obtain P_n, one needs to simulate the system using quantum trajectory method. For this, the calculation takes a lot of computation resource. And it is not likely to reach the continuous functions but discrete results (seen in Table 1) of the system parameters to P_n. This situation urges us to change the normal strategy of dealing with decoy state method MDI-QKD under the influence of statistical fluctuation, which will be discussed later in the work.

Protocol. We use subscript A or B to denote a source at Alice's side or Bob's side. In the protocol we proposed before[58], sources x_A and y_A (x_B and y_B) only emit pulses in X basis while source z_A (z_B) only emits pulses in Z basis. The protocol needs four different states $\rho_{o_A} = |0\rangle\langle 0|$, ρ_{x_A}, ρ_{y_A}, ρ_{z_A} ($\rho_{o_B} = |0\rangle\langle 0|$, ρ_{x_B}, ρ_{y_B}, ρ_{z_B}) respectively.

In photon number space, suppose

$$\rho_{x_A} = \sum_k a_k|k\rangle\langle k|, \quad \rho_{x_B} = \sum_k b_k|k\rangle\langle k|, \tag{1}$$

$$\rho_{y_A} = \sum_k a'_k|k\rangle\langle k|, \quad \rho_{y_B} = \sum_k b'_k|k\rangle\langle k|, \tag{2}$$

$$\rho_{z_A} = \sum_k a''_k|k\rangle\langle k|, \quad \rho_{z_B} = \sum_k b''_k|k\rangle\langle k|, \tag{3}$$

We call x_A, x_B as well as y_A, y_B the decoy sources; z_A, z_B the signal sources, and o_A, o_B the vacuum sources.

At each time, Alice will randomly choose source l_A with probability p_{l_A} for $l = o, x, y, z$. Similarly, Bob will randomly choose source r_B with probability p_{r_B} for $r = o, x, y, z$. The emitted pulse pairs (one pulse from Alice, one pulse from Bob) are sent to the un-trusted third party (UTP). We shall use notation lr to indicate the two-pulse source when Alice use source l_A and Bob use source r_B to general a pulse pair, e.g., source xy is the source that Alice uses source x_A and Bob uses source y_B. Also, here in our protocol, the intensity for pulses in Z basis can be different from those of X basis, this makes more freedom in choosing the intensities and hence further raises the key rate. Those effective events caused by pulse pairs from source zz will be used for key distillation, while the effective events caused by sources in X basis and vacuum sources will be used to estimate the yield and the phase-flip error rate of the single-photon pulse pairs.

The final key rate of per pulse pair can be calculated as[6,7]

$$R = p_{z_A}p_{z_B} \cdot \{a_1''^Z b_1''^Z \underline{s}_{11}[1 - H(\bar{e}_{11})] - fS_{zz}H(E_{zz})\}, \tag{4}$$

In which, $\underline{s}_{11}$ is the lower bound of the single photon counting rate s_{11}, and $\bar{e}_{11}$ is the upper bound of the single photon error rate e_{11}, H is the binary Shannon entropy, f is the factor of error correction inefficiency. S_{lr} note the counting rate in UTP while Alice choice the source l and Bob choice the source r, E_{lr} and T_{lr} note the error rate and error counting rate respectively. (Meaning $T_{lr} = E_{lr}S_{lr}$).

As S_{zz} and E_{zz} can directly get in UTP, to obtain the final key rate, one needs to know $\underline{s}_{11}$ as well as $\bar{e}_{11}$ by the decoy state method. As was shown in ref.[58], both $\underline{s}_{11}$ and $\bar{e}_{11}$ are functionals of a common variable $\mathcal{H}$ (See details in the appendix). The final key rate is then

$$R = \min_{\mathcal{H} \in \mathcal{I}} \mathcal{R}(\mathcal{H}). \tag{5}$$

And as shown in detail in the appendix, $\mathcal{I}$ is the range of values for $\mathcal{H}$.

Numerical simulation. With the protocol introduced above, we can numerically calculate the key rate and evaluate the performance of the MDI-QKD. In considering the finite-size effects, we shall take a failure probability of 10^{-7} with a normal distribution. Finite size effects are very important in the practical application of QKD,

	e_d	p_d	ηd	N
a	1.5%	6.02×10^{-6}	14.5%	10^{10}
b	1%	10^{-7}	40%	10^{13}

Table 2. Device parameters and data sizes used in numerical simulations. e_d: the alignment error. p_d: the dark count rate. η_d: the detection efficiency of all detectors. N: the total pulse pair emitted.

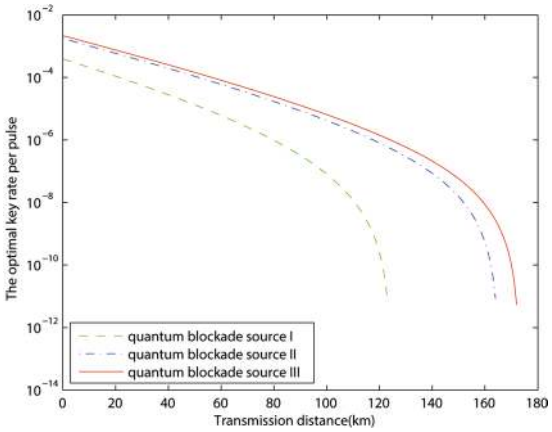

Figure 1. The optimized key rates (per pulse pair) versus transmission distance by different sources with device parameters and data size being given by line *a* of Table 2. The quantum blockade source is choice from Table 1.

because of the finite transition time and relatively small data size, especially when one needs communication with little delay, like generating fresh key.

For these purpose, to achieve a practical useful key rate, we need both the protocol introduced above and the optimization algorithm. There are variety parameters in the protocol (if using the traditional WCS sources, the parameters are the intensities and the emitting probabilities for each sources, which means six variables). Not like the situation without statistical fluctuation, globally optimization will make remarkable difference in the final key rates.

Usually, we describe the decoy state method system by several continuously parameters and optimiz them in computer program. But the case here makes this strategy difficult, because our quantum blockade source is described by the disperse P_n. Though these P_n are essentially based on several continuously parameters in quantum blockade system, but as discuss above, one have to implement Monte Carlo algorithm to conduct the photon number distribution, which takes a lot of time and the results are may not smooth enough for the farther optimization.

To solve the predicament, we no longer optimize the quantum blockade source itself, but add a linear attenuation device(optical fiber for example) right after each source. Equally obtain the continuously changing source as

$$P'_n = \sum_{k=n}^{\infty} P_k \eta^n (1-\eta)^{k-n} C_k^n \tag{6}$$

here η is the penetration rate, and $\eta \in [0, 1]$.

Through this treatment, we need only one kind of quantum blockade source to accomplish the whole decoy state method MDI-QKD. By choice three different η, two decoy sources and one signal source can be easily obtained. And we just need to optimize the three η and corresponding emittion probabilities, which would make the problem simpler and more calculable.

In the numerical simulation, we take a simple treatment using normal distribution to make a fair comparison with the prior art results[56–58], and uniformly set failure probability $\varepsilon = 10^{-7}$, and implement the global optimization for each method compared in our figures.

Table 2 shows the device parameters and data sizes used in numerical simulations. Except for the parameters listed, we also set error correction inefficiency $f_e = 1.16$ for all the simulation. The parameters choice is based on[58] to provide comprehensive and fair comparison and the two lines represent two typical experimental setup.

In Fig. 1, we compare the performances of quantum blockade source with different photon number distributions in Table 1. The result approximately declares that P_1 is the most important parameter to estimate the advantage of quantum blockade source in MDI-QKD. But we must point out that the key rate is also affect by the other P_n.

Based on this conclusion, in Figs 2 and 3, we chooses quantum blockade source III to compare with the traditional weak coherent source, and the advantage is observable with both case a and case b. In Fig. 4, we plot the single photon pulse pair error rates of the two sources discussed above in the calculation of case a in Fig. 2. And it clearly shows that the remarkable reduction of single photon pulse pair error rate for the quantum blockade source comparing with the traditional weak coherent source, which is the main contribution to the improvement of key rate.

We also give some typical key rates in certain distance points in Table 3. In that table, the key rates in lines 2 and 3 are obtained with parameters of case a, and the other two lines are calculated with parameters of case b in

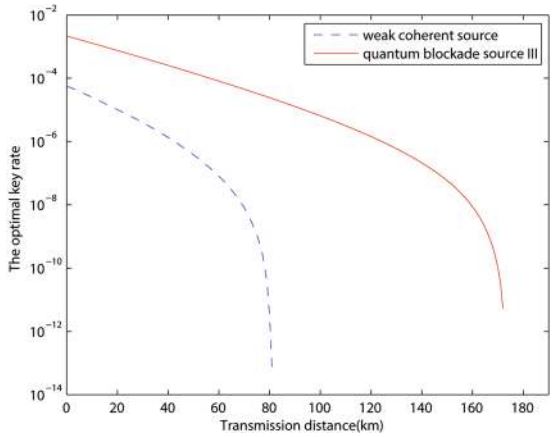

Figure 2. The optimized key rates (per pulse pair) versus transmission distance by different sources with device parameters and data size being given by line *a* of Table 2.

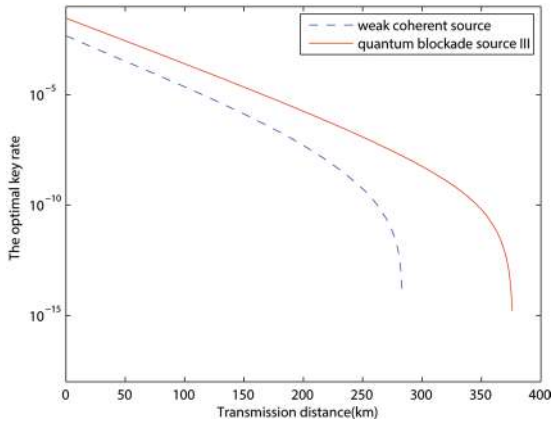

Figure 3. The optimized key rates (per pulse pair) versus transmission distance by different sources with device parameters and data size being given by line *b* of Table 2.

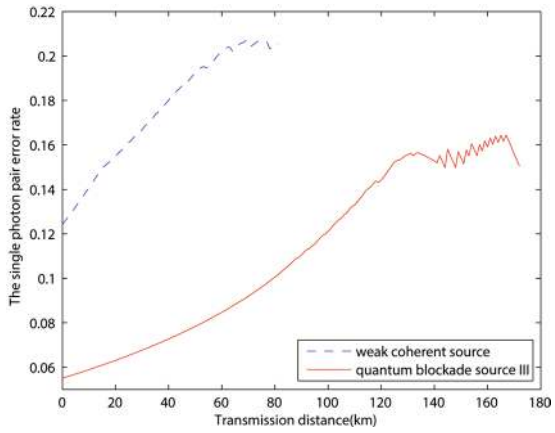

Figure 4. The single photon pair error rates versus transmission distance by different sources of the calculation in Fig. 1.

Table 2. It clearly shows the significantly increasing of the key rate due to the quantum blockade sources used, and we also explain that this advantage is mainly due to the reduction of single photon pair error rate.

And here we also compare the secure key rate of our numerical simulation with an existing MDI-QKD experiment[71]. Given the same detector parameters, alignment errors and pulse number, at the distance of 259 *km*,

	50 *km*	70 *km*
weak coherent source	3.78×10^{-7}	8.10×10^{-9}
quantum blockade source	1.45×10^{-4}	4.49×10^{-5}
weak coherent source	3.31×10^{-4}	1.15×10^{-4}
quantum blockade source	2.77×10^{-3}	1.07×10^{-3}

Table 3. The key rates of some typical distance points. The line two and line three are the simulation of Fig. 2, the line four and line five are the simulation of Fig. 3.

the key rate of the MDI-QKD experiment with weak coherent state is 3.48×10^{-9} and the key rate of quantum blockade sources is 1.88×10^{-7}.

Discussion

In summary, we have investigated the performance of quantum blockade source in practical MDI-QKD. Although the previous work[59] obtain the similar simulations to prove the advantage of quantum blockade source comparing with the WCS, but the statistical fluctuation and global optimization are not included there. Even the finite data size reduces the key rate, one can still reach the irresistibly superiority of quantum blockade source by the efficient decoy state method considering statistical fluctuation[58] and global optimization strategy. It demonstrates that by implementing the scheme above, the quantum blockade source can greatly improve the key rate and communication distance of practical MDI-QKD, which is nearly tens of or hundreds of times.

Methods

When statistical fluctuation is considered, the estimation will be tougher, but as mentioned above, using our newly developed strategy[58], those two parameters of great importance can be estimated easily and tight.

To deal with the decoy state method with statistical fluctuation, we need bring in the expected value of observed variable S_{lr}, T_{lr}, as the form of $\langle S_{lr}\rangle$ and $\langle T_{lr}\rangle$, so the estimation equations are:

$$\begin{aligned} s_{11} &\geq \underline{s}_{11}(\mathcal{H}) = \frac{[a_1'b_2'\langle S_{xx}\rangle + a_1b_2a_0'\langle S_{oy}\rangle + a_1b_2b_0'\langle S_{yo}\rangle] - [a_1b_2\langle S_{yy}\rangle + a_1b_2a_0'b_0'\langle S_{oo}\rangle] - a_1'b_2'\mathcal{H}}{a_1a_1'(b_1b_2' - b_1'b_2)}, \\ e_{11} &\leq \bar{e}_{11}(\mathcal{H}) = \frac{\langle T_{xx}\rangle - \mathcal{H}/2}{a_1b_1\mathcal{H}_{11}}, \\ \text{and } \mathcal{H} &= a_0\langle S_{ox}\rangle + b_0\langle S_{xo}\rangle - a_0b_0\langle S_{oo}\rangle. \end{aligned} \tag{7}$$

In these two estimations, we choice s_{11} and e_{11} as the functions of $\mathcal{H}$, which is the common part of them. (The detail prove of this method can be seen in our previous work[58]). By using this kinds of estimations, the final key rate is also the functions of $\mathcal{H}$. Then through scanning $\mathcal{H}$ in the interval giving by the statistical fluctuation of certain failure probability, the minimum value of $R(\mathcal{H})$ is final key rate. And it's much better than the result of treat statistical fluctuation in s_{11} and e_{11} respectively.

So we have,

$$R = \min_{\mathcal{H} \in \mathcal{I}} \mathcal{R}(\mathcal{H}). \tag{8}$$

And $\mathcal{I} = [h - \delta,\ h + \delta]$ with

$$\begin{aligned} h &= a_0S_{ox} + b_0S_{xo} - a_0b_0S_{oo} \\ \delta &= a_0\gamma\sqrt{\frac{S_{ox}}{N_{ox}}} + b_0\gamma\sqrt{\frac{S_{xo}}{N_{xo}}} + a_0b_0\gamma\sqrt{\frac{S_{oo}}{N_{oo}}} \end{aligned} \tag{9}$$

This result is obtained by the theory of statistical fluctuation, γ is the parameter decided by the failure probability.(For example, if we choice the failure probability as $1e-7$, then $\gamma = 5.3$)

The other advantage of our method propose in refs[58,72] is the joint-treatment of the statistical fluctuation, which allow us to get the expect values in the estimations of $\underline{s}_{11}$ and $\bar{e}_{11}$ by the following constraints:

$$\begin{aligned} &N_{lr}S_{lr} + \gamma\sqrt{N_{lr}S_{lr}} \geq N_{lr}\langle S_{lr}\rangle \geq N_{lr}S_{lr} - \gamma\sqrt{N_{lr}S_{lr}};\ \text{for any } lr \in \mathcal{D} \\ &N_{yo}\langle S_{yo}\rangle + N_{oy}\langle S_{oy}\rangle \geq N_{yo}S_{yo} + N_{oy}S_{oy} - \gamma\sqrt{N_{yo}S_{yo} + N_{oy}S_{oy}} \\ &N_{xx}\langle S_{xx}\rangle + N_{yo}\langle S_{yo}\rangle_+ N_{oy}\langle S_{oy}\rangle \\ &\quad \geq N_{xx}S_{xx} + N_{yo}S_{yo} + N_{oy}S_{oy} - \gamma\sqrt{N_{xx}S_{xx} + N_{yo}S_{yo} + N_{oy}S_{oy}} \\ &N_{yy}\langle S_{yy}\rangle + N_{oo}\langle S_{oo}\rangle \leq N_{yy}S_{yy} + N_{oo}S_{oo} + \gamma\sqrt{N_{yy}S_{yy} + N_{oo}S_{oo}} \end{aligned} \tag{10}$$

and

$$N_{ox}S_{ox} + N_{xo}S_{xo} + \gamma\sqrt{N_{ox}S_{ox} + N_{xo}S_{xo}} \geq N_{xo}\langle S_{xo}\rangle + N_{ox}\langle S_{ox}\rangle_{\mathcal{L}} \geq N_{ox}S_{ox} + N_{xo}S_{xo} - \gamma\sqrt{N_{ox}S_{ox} + N_{xo}S_{xo}} \tag{11}$$

References

1. Bennett, C. H. & Brassard, G. In *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing* (IEEE, New York), pp. 175–179 (1984).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
3. Gisin, N. & Thew, R. *Quantum communication Nature Photonics*. **1**, 165 (2006).
4. Dusek, M., Lütkenhaus, N. & Hendrych, M. In *Progress* in Optics V*VVX*, edited by E. Wolf (Elsevier, 2006).
5. Scarani, V. *et al*. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
6. Inamori, H., Lütkenhaus, N. & Mayers, D. *European Physical Journal D*. **41**, 599 (2007).
7. Gottesman, D. *et al*. *Quantum Inf. Comput.* **4**, 325 (2004).
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. Adachi, Y., Yamamoto, T., Koashi, M. & Imoto, N. Simple and efficient quantum key distribution with parametric down-conversion. *Phys. Rev. Lett*. **99**, 180503 (2007).
14. Hayashi, M. Practical evaluation of security for quantum key distribution. *Phys. Rev. A*. **75**, 022307 (2006).
15. Hayashi, M. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Phys. Rev. A*. **76**, 012329 (2007).
16. Rosenberg, D. *et al*. Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett.* **98**, 010503 (2007).
17. Schmitt-Manderbach, T. *et al*. xperimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).
18. Peng, C. Z. *et al*. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.* **98**, 010505 (2007).
19. Yuan, Z. L., Sharpe, A. W. & Shields, A. J. *Appl. Phys. Lett.* **90**, 011118 (2007).
20. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. *Opt. Express.* **16**, 18790 (2008).
21. 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).
22. Y. Zhao, *et al*. In *Proceedings of IEEE International Symposium on Information Theory, Seattle*, pp. 2094–2098 (IEEE, New York, 2006).
23. Wang, X. B., Peng, C. Z., Zhang, J., Yang, L. & Pan, J. W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A*. **77**, 042311 (2008).
24. Hu, J. Z. & Wang, X. B. Reexamination of the decoy-state quantum key distribution with an unstable source. *Phys. Rev. A*. **82**, 012331 (2010).
25. Wang, X. B. Hiroshima, T., Tomita, A. & Hayashi, M. Quantum information with gaussian states. *Physics Reports*. **448** (2007).
26. Wang, X. B., Yang, L., Peng, C. Z. & Pan, J. W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **11**, 075006 (2009).
27. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **85**, 1330 (2000).
28. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*. **61**, 052304 (2000).
29. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New J. Phys.* **4**, 44 (2002).
30. Huttner, B. B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A*. **51**, 1863 (1995).
31. Yuen, H. P. Quantum amplifiers, quantum duplicators and quantum cryptography. *Quantum Semiclassic. Opt.* **8**, 939 (1996).
32. Lyderson, L., Makarov, V. & Skaar, J. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics.* **4**, 686 (2010).
33. Gerhardt, I. *et al*. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Commu.* **2**, 349 (2011).
34. Mayers, D. & Yao, A. C.C. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)*, p. 503 (IEEE Computer Society, Washington, DC, 1998).
35. Acin, A. *et al*. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett*. **98**, 230501 (2007).
36. Scarani, V. & Renner, R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-Way postprocessing. *Phys. Rev. Lett*. **100**, 200501 (2008).
37. Scarani, V. & Renner, R. In *3rd Workshop on Theory of Quantum Computation, Communication and Cryptography* (*TQC 2008*), See also arXiv: **0806.0120** (University of Tokyo, Tokyo 30 Jan-1 Feb 2008).
38. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
39. Tamaki, K., Lo, H. K., Fung, C. H. F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A*. **85**, 042307 (2012).
40. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
41. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
42. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Proof-of-principle field test of quantum key distribution immune to detector attacks. arxiv: 1204.0738v1.
43. Ferreira da Silva, T. *et al*. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A*. **88**, 052303 (2013).
44. Tang, Z. *et al*. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
45. Tang, Y. L. *et al*. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).
46. Wang, X. B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A*. **87**, 012320 (2013).
47. Ma, X. F., Fred Fung, C. H. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A*. **86**, 052305 (2012).
48. Wang, Q. & Wang, X. B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. *Phys. Rev. A*. **88**, 052332 (2013).
49. Xu, F., Qi, B., Liao, Z. & Lo, H. K. Long distance measurement-device-independent quantum key distribution with entangled photon sources. *Appl. Phys. Lett*. 061101 (2013).
50. Curty, M. *et al*. *Finite-key analysis for measurement-device-independent quantum key distribution*. arXiv: 1307.1081v1.
51. Yu, Z. W., Zhou, Y. H. & Wang, X. B. Three-intensity decoy-state method for measurement-device-independent quantum key distribution. *Phys. Rev. A*. **88**, 062339 (2013).

52. Yu, Z. W., Zhou, Y. H. & Wang, X. B. *Decoy state method for measurement device independent quantum key distribution with different intensities in only one basis*. arXiv: 1309.0471v1.
53. Yu, Z. W., Zhou, Y. H. & Wang, X. B. *Generalized three-intensity decoy state method for measurement device independent quantum key distribution*. arXiv: 1309.5886v1.
54. 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).
55. Wang, Q. & Wang, X. B. Simulating of the measurement-device independent quantum key distribution with phase randomized general sources. *Scientific Reports.* **4**, 4612 (2014).
56. Xu, F., Xu, H. & Lo, H. K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A.* **89**, 052333 (2014).
57. Yu, Z. W., Zhou, Y. H. & Wang, X. B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Phys. Rev. A.* **91**, 032318 (2015).
58. Zhou, Y. H., Yu, Z. W. & Wang, X. B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A.* **93**, 042324 (2016).
59. Li, A., Chen, T., Zhou, Y. H. & Wang, X. B. Optics Letters, Vol.41, No.9 (2016). On-demand single-photon sources via quantum blockade and applications in decoy-state quantum key distribution. *Optics Letters*, **41**, No. 9 (2016).
60. Carmichael, H. J. Photon antibunching and squeezing for a single atom in a resonant cavity. *Phys. Rev. Lett.* **55**, 2790 (1985).
61. Birnbaum, K. M. *et al*. Photon blockade in an optical cavity with one trapped atom. *Nature.* **436**, 87 (2005).
62. Hennessy, K. *et al*. Quantum nature of a strongly coupled single quantum dot-cavity system. *Nature.* **445**, 896 (2007).
63. Faraon, A. *et al*. *Nat. Phys.* **4**, 859 (2008).
64. He, Y. M. *Nature Nanotechnology* **8**, 213 (2013).
65. He, Y. M. *et al*. On-demand semiconductor single-photon source with near-unity indistinguishability. *Nature Nanotechnology* **8**, 213 (2013).
66. Gullans, M., Chang, D. E., Koppens, F. H. L., Garcìa de Abajo, F. J. & Lukin, M. D. Single-photon nonlinear optics with graphene plasmons. *Phys. Rev. Lett.* **111**, 247401 (2013).
67. Smolyaninov, I. I., Zayats, A. V., Gungor, A. & Davis, C. C. Single-photon tunneling via localized surface plasmons. *Phys. Rev. Lett.* **88**, 187402 (2002).
68. Tian, L. & Carmichael, H. J. Quantum trajectory simulations of two-state behavior in an optical cavity containing one atom. *Phys. Rev. A.* **46**, R6801 (1992).
69. Carmichael, H. J. An Open Systems Approach to Quantum Optics, *Lecture Notes in Physics (Springer Science& Business Media)* (1993).
70. Plenio, M. B. & Knight, P. L. The quantum-jump approach to dissipative dynamics in quantum optics. *Rev. Mod. Phys.* **70**, 101 (1998).
71. Hua-Lei, Y. *et al*. Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
72. Liu., Y. *et al*. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).

Acknowledgements

We acknowledge the financial support in part by the 10000-Plan of Shandong province (Taishan Scholars), National High-Tech Program of China grant No. 2011AA010800 and 2011AA010803, NSFC grant No. 11474182, 11774198, U1738142, 11174177 and 60725416, and the key R&D Plan Project of Shandong Province, grant No. 2015GGX101035 and the National key R&D plan, grant No. 2017YFA0303901.

Author Contributions

Xiang-Bin Wang proposed this work, Zong-Wen Yu and Yi-Heng Zhou studied the QKD part, Ao Li studied the quantum blockade part. Xiao-Long Hu and Cong Jiang did the calculations and drew the figures. Zong-Wen Yu and Yi-Heng Zhou wrote the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

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