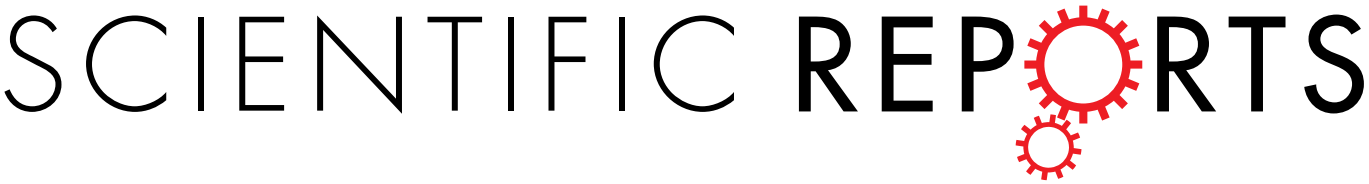

OPEN

Measurement-Device-Independent Quantum Key Distribution over asymmetric channel and unstable channel

Received: 6 August 2018
Accepted: 7 November 2018
Published online: 05 December 2018

Xiao-Long Hu[1], Yuan Cao[2,3], Zong-Wen Yu[1,5] & Xiang-Bin Wang[1,4,6]

We show that a high key rate of Measurement-Device-Independent Quantum Key Distribution (MDIQKD) over asymmetric and unstable quantum channel can be obtained by full optimization and compensation. Employing a gradient optimization method, we make the full optimization taking both the global optimization for the 12 independent parameters and the joint constraints for statistical fluctuations. We present a loss-compensation method by monitoring the channel loss for an unstable channel. The numerical simulation shows that the method can produce high key rate for both the asymmetric channel and the unstable channel. Compared with the existing results of independent constraints, our result here improves the key rate by 1 to tens of times in typical experimental conditions.

Quantum key distribution (QKD) provides the communication users with secure keys to encrypt their information. Bennett and Brassard proposed BB84 protocol[1] to realize QKD, but the lack of practical single-photon sources limited the use of origin BB84 protocol. BB84 protocol with imperfect single-photon sources would suffer from the photon-number-splitting (PNS) attack[2–4]. This loophole can be fixed by the decoy-state method[5–8]. With the decoy-state method, QKD can be used in the practical system between users with longer distace[9–11]. After that, measurement-device-independent QKD (MDIQKD) was proposed to avoid any loophole from the imperfect detection devices[12–15]. Combined with decoy-state method, MDIQKD can also avoid the loophole from the imperfect single-photon sources[15,16]. Nowadays, the decoy-state MDIQKD has become the mainstream of the studies of quantum key distribution both theoretically[16–29] and experimentally[30–43]. Various numerical models and optimization methods[21–24] have improved the key rate and secure distance a lot. The numerical model by Xu *et al.*[21] can apply to the case of asymmetrical channel rather precisely. The maximum distance of MDIQKD has been experimentally increased to 404 kilometers[38] using the 4-intensity protocol[24] with joint constraints for statistical fluctuations[23]. Another experiment exceeding 400-kilometer distance applying the decoy-state method but not using MDIQKD scheme was reported recently[43].

In the scheme of decoy-state MDIQKD, at each time the user Alice (Bob) randomly chooses her (his) basis, bit value and intensity to send a pulse in a corresponding state, e.g. BB84 state in a polarization-coding MDIQKD, to an untrusted third party (UTP) Charlie. Charlie performs a collective measurement on each pulse pair and announces the measurement result in the public channel. After Charlie announces the measurement results, Alice and Bob announce the bases and intensities they use. Based on all announcement, Alice and Bob can calculate the yield and the error rate of single-photon pulse pairs, and then distill the secure key.

[1]State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing, 100084, People's Republic of China. [2]National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, 230026, China. [3]CAS Center for Exellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai, 201315, China. [4]Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, 230026, China. [5]Data Communication Science and Technology Research Institute, Beijing, 100191, China. [6]Shenzhen Institute for Quantum Science and Engineering, and Department of Physics, Southern University of Science and Technology, Shenzhen, 518055, China. Xiao-Long Hu and Yuan Cao contributed equally. Correspondence and requests for materials should be addressed to X.-B.W. (email: xbwang@mail.tsinghua.edu.cn)

For the practical applications, the asymmetric and unstable channels are common cases both in fiber and free space. For example, when we consider the quantum network, due to the different geographical locations of users, the channel losses can be largely different. And if we want implement MDIQKD in free space, the channels are always asymmetric and unstable too, due to the atmospheric turbulence or moving sites (such as the satellite). Although the security of MDIQKD doesn't make any assumption to the channel, the unstable and/or asymmetric quantum channel decreases the key rate quite a lot. Therefore, directly applying the optimized parameters for symmetric channel does not give a good performance in an asymmetric channel or an unstable channel. Here, we propose full optimization of four-intensity decoy-state MDIQKD protocol to largely increase the key rate in asymmetric channels than existing results of partial optimization. For full optimization, we mean: (1) Using 12 independent parameters, (2) Applying joint constraints[23,24] for statistical fluctuations. If one only use one of the above two operations, that is partial optimization. Moreover, a loss-compensation method is presented with optimization to increase the performance of MDIQKD in unstable channels.

Results

Four-intensity decoy-state MDIQKD. Among all existing protocols of decoy-state MDIQKD, the 4-intensity protocol seems to be the most efficient one[24] which has been extensively verified experimentally[37–40]. As was stated in the four-intensity decoy-state method in Ref.[24], Alice and Bob each uses 4 different intensities, including one vacuum. This means in general, there are 7 different intensities for both sides with 6 independent parameters for non-vacuum intensities. Together with the frequencies of using each intensities, there are 12 independent parameters in general in the protocol. Also, the four-intensity protocol suggests using the joint constraints in statistical fluctuation of different observable[23,24]. A full implementation of the four-intensity protocol means doing optimization among all those 12 parameters with joint constraints fully.

Explicitly, in the four-intensity decoy-state method in ref.[24], Alice (Bob) uses a source z_A (z_B) with intensity μ_{az} (μ_{bz}) that only emits photons in the Z basis, two sources x_A and y_A (x_B and y_B) with intensities μ_{ax} and μ_{ay} (μ_{bx} and μ_{by}) that only emit photons in the X basis and a vacuum source o_A (o_B) that only emits vacuum pulses. At each time, Alice (Bob) randomly chooses a source in the four sources above to send a pulse, with probability p_{al_A}, $l = z, x, y, o$ (p_{br_B}, $r = z, x, y, o$). So we call it "four-intensity protocol".

The key rate of the decoy-state MDIQKD is given by:

$$R = p_{az}p_{bz}\{a_{z1}b_{z1}\underline{\langle s_{11}\rangle}\,[1 - H\,(\overline{\langle e_{11}^{ph}\rangle})] - fS_{zz}H(E_{zz})\} \tag{1}$$

where a_{z1} and b_{z1} are the fraction of single photons of sources z_A and z_B, $\langle s_{11}\rangle$ and $\overline{\langle e_{11}^{ph}\rangle}$ are the bound of yield and phase-flip error rate of single-photon pulse pairs which can be obtained by the decoy-state method, S_{zz} and E_{zz} are yield and bit-flip error rate when Alice and Bob both send pulses with source z_A/z_B, $H(p) = -p\log_2 p - (1 - p)\log_2(1 - p)$ is the binary entropy function and f is the correction efficiency.

Details for calculation of the key rate can be found in the appendix.

Optimization of source parameters. In the numerical simulation, we will estimate what values we would observe for the yields and error rates in a certain model and use these values to calculate the key rate. Given the properties of the channel and the detection devices, we can regard the key rate as a function of source parameters:

$$\widetilde{R} = \widetilde{R}(\mu_{ax}, \mu_{ay}, \mu_{az}, p_{ax}, p_{ay}, p_{az}, \mu_{bx}, \mu_{by}, \mu_{bz}, p_{bx}, p_{by}, p_{bz}) = \widetilde{R}(\vec{x}). \tag{2}$$

If we use weak coherent state sources, the relation between the intensity μ and the photon number distribution $\rho = \sum_k a_k|k\rangle\langle k|$ is $a_k = e^{-\mu}\frac{\mu^k}{k!}$.

In the calculation of the key rate, we need to take the joint fluctuation and the scan of $\mathcal{H}$ (the definition of $\mathcal{H}$ is in the appendix) into consideration. In addition, the number of parameters we need to optimize is large, which means the parameter space is very huge. Therefore, normal optimization method costs a lot of time. We should improve the optimization method to get the optimal parameters quickly. Firstly, we consider the "gradient" of the key rate function[29]:

$$\frac{\Delta\widetilde{R}}{\Delta x_k} = \frac{\widetilde{R}(x_k + \Delta x_k, x_i) - \widetilde{R}(x_k - \Delta x_k, x_i)}{2\Delta x_k}. \tag{3}$$

In the case that both $\widetilde{R}(x_k + \Delta x_k, x_i)$ and $\widetilde{R}(x_k - \Delta x_k, x_i)$ are less than $\widetilde{R}(x_k, x_i)$, we set $\frac{\Delta\widetilde{R}}{\Delta x_k} = 0$. With

$$\frac{\Delta\widetilde{R}}{\Delta\vec{x}} = \left(\frac{\Delta\widetilde{R}}{\Delta x_1}, \ldots, \frac{\Delta\widetilde{R}}{\Delta x_{12}}\right) \tag{4}$$

we can find the direction that key rate increases the fastest and get close to the optimal parameters quickly.

To avoid the case that the optimal parameters are the local optimal point, which satisfies $\widetilde{R}(x_k + \Delta x_k, x_i) \le \widetilde{R}(x_k, x_i)$ for any k but is not the maximum point in the whole area, we search the points in the nearby area to see whether there is higher key rate. Accurately, we calculate the key rate $\widetilde{R}(x_k + \delta_k\Delta l)$; $\delta_k = -1, 0, 1$; $k = 1, \ldots, 12$ with a certain Δl. If there are some points with higher key rate, we jump to the point with highest key rate in the nearby area and execute the above procedure again.

In our simulation, we found that in most cases, the gradient method brings us to the optimal point. But in some cases, it brings us to the local optimal point.

Loss-compensation method. For the case of unstable channel, according to our MDIQKD protocol, all source parameters should be determined before the QKD process and fixed during the QKD process. Even though we can detect the channel transmittance η at any time, we cannot change the source parameters to optimize the key rate at real time. The decoy state method requests that the intensities of pulses must be fixed. Say, switching among 3 fixed intensities. If one change the intensities beyond these 3 intensities, or change the intensities non-randomly, the result of the decoy-state method will be invalid. With the fixed source parameters μ_A and μ_B and unstable channel transmittance $\eta_A(t)$ and $\eta_B(t)$, which means the transmittance changes dependently on time, there are always some cases that the intensities at the two sides of Charlie's beam splitter deviate a lot, saying that at some time t_i, $\mu_A\eta_A(t_i)$ and $\mu_B\eta_B(t_i)$ deviate a lot. These cases will give a quite high error rate that decreases the key rate a lot.

First we consider the case with stable channel that satisfies $\mu_A\eta_A > \mu_B\eta_B$. In an asymmetric channel, if one attenuates one path, the channel will become symmetric and the detected error rate will be small. However, in such a case, the amount of detected bits is also decreased and the final key rate is not necessarily improved. If we add extra loss $\frac{\mu_B\eta_B}{\mu_A\eta_A} \le \tilde{\eta}_A \le 1$ to the channel between Alice and Charlie, we can get a better key rate. Given the transmittance and the intensities of sources, the specific value of $\tilde{\eta}_A$ can be determined by numerical simulation.

Then we come to the case with unstable channel. Technically, the channel loss cannot be changed too fast. Otherwise the physical compensation cannot be made instantaneously. We assume that the transmittance remains unchanged during each time window, which means the transmittance doesn't fluctuate too rapidly. Suppose that we are given the transmittance distribution $\{\eta_A^{(1)}, \cdots, \eta_A^{(i)}, \cdots\}$ and $\{\eta_B^{(1)}, \cdots, \eta_B^{(i)}, \cdots\}$ and fixed μ_A, μ_B. A general loss-compensation method is to add different extra loss $\tilde{\eta}^{(ij)} < 1$ to Alice's or Bob's channel for different transmittance pair $\eta_A^{(i)} \otimes \eta_B^{(j)}$ and we can determine the optimal value of each $\tilde{\eta}^{(ij)}$ for each $\eta_A^{(i)} \otimes \eta_B^{(j)}$ pair. But in practice, the optimization of so many variables is out of any computer's ability. So we keep only one extra loss $\tilde{\eta}$ and raise a variable δ. When the transmittance pair $\eta_A^{(i)} \otimes \eta_B^{(j)}$ satisfies $\eta_A^{(i)}/\eta_B^{(j)} > \delta$, Charlie should add the extra loss $\tilde{\eta}$ to the channel between Alice and Charlie. When the transmittance pair $\eta_A^{(i)} \otimes \eta_B^{(j)}$ satisfies $\eta_B^{(j)}/\eta_A^{(i)} > \delta$, Charlie should add the extra loss $\tilde{\eta}$ to the channel between Bob and Charlie. In other cases, Charlie doesn't have to add any extra loss to the channel. We can use numerical simulation, combined with optimization of source parameters, to determine the values of $\tilde{\eta}$ and δ to get the best key rate when given a specific transmittance distribution.

In the simulation of the unstable channel, suppose that we have the transmittance distribution $\{\eta_A^{(1)}, \cdots, \eta_A^{(i)}, \cdots\}, \{\eta_B^{(1)}, \cdots, \eta_B^{(j)}, \cdots\}$ and the corresponding probability $\{p_A^{(1)}, \cdots, p_A^{(i)}, \cdots\}, \{p_B^{(1)}, \cdots, p_B^{(j)}, \cdots\}$. We can calculate the "transmittance pair distribution" $\{\eta_A^{(1)} \otimes \eta_B^{(1)}, \cdots, \eta_A^{(i)} \otimes \eta_B^{(j)}, \cdots\}$ and the corresponding probability $\{p_A^{(1)} * p_B^{(1)}, \cdots, p_A^{(i)} * p_B^{(j)}, \cdots\}$. With a certain source pair lr and a certain transmittance pair $\eta_A^{(i)} \otimes \eta_B^{(j)}$, the observed yield $S_{lr}(\eta_A^{(i)} \otimes \eta_B^{(j)})$ and the observed error rate $E_{lr}(\eta_A^{(i)} \otimes \eta_B^{(j)})$ can be calculated as in ref.[44] theoretically. Then the yield and the error rate in the whole process can be calculated by

$$S_{lr} = \sum_{i,j} p_A^{(i)} p_B^{(j)} S_{lr}(\eta_A^{(i)} \otimes \eta_B^{(j)}) \tag{5}$$

and

$$E_{lr} = \sum_{i,j} p_A^{(i)} p_B^{(j)} E_{lr}(\eta_A^{(i)} \otimes \eta_B^{(j)}). \tag{6}$$

When the loss-compensation is performed, we can calculate the S_{lr}, E_{lr} in the same way except the (ij)-th transmittance pair is changed into $\eta_A^{(i)}\tilde{\eta} \otimes \eta_B^{(j)}$ if $\frac{\eta_A^{(i)}}{\eta_B^{(j)}} > \delta$, or $\eta_A^{(i)} \otimes \eta_B^{(j)}\tilde{\eta}$ if $\frac{\eta_B^{(j)}}{\eta_A^{(i)}} > \delta$.

Numerical simulation. First we consider the case that the channel is stable but asymmetric. We shall estimate what values would be probably observed for the yields in the normal cases by the linear models[15,21,22] and the errors in X basis by the useful model for misalignment error under asymmetric channel in ref.[21]. We show the optimized key rate in some asymmetric cases in Fig. 1 and some results in certain distances in Table 1, in comparison with the results of independent bounds in ref.[45], with device parameters in Table 2. From Fig. 1, we can find that with full implementation of the four-intensity MDIQKD and full optimization of the source parameters, quite good key rate can be achieved. In particular, we have taken the joint constraints[23,24] for statistical fluctuations, this affects the key rate significantly. Taking joint constraints will consume some more computational time. The computation can be done very fast if we apply formulas of refs[23,24] rather than the linear programming. In our numerical simulation, we have already overcome the problem of unpredictable behavior such as jitters[45]. Actually, the computational time seems not to be a major issue for the practical application. In the application for the unstable channel, one can choose to test the channels and do the optimization for the major loss values of the changing channel before running the protocol.

Then for the unstable channel, we consider a simple case that $\eta_A^{(i)} = (3 + 2i)\,\mathrm{dB}$, $\eta_B^{(j)} = (13 + 2j)\,\mathrm{dB}$ with probability $p_A^{(i)} = p_B^{(j)} = 0.2$ for $i, j = 1, \ldots, 5$ (Here the detector's efficiency is contained in the total loss). We show the key rate with different δ and $\tilde{\eta}$ with source parameters optimized in Table 3.

The case that $\delta = \tilde{\eta}' = 0\,\mathrm{dB}$ is equal to that we don't perform the loss-compensation method. In the second line of Table 3, we can see that an improper loss-compensation ($\delta = -7\,\mathrm{dB}$ and $\tilde{\eta}' = 5\,\mathrm{dB}$) will decrease the key rate. We can find that in this transmittance distribution, setting $\delta = -8.75\,\mathrm{dB}$ and $\tilde{\eta}' = 4.5\,\mathrm{dB}$ can maximize the key rate in our loss-compensation method.

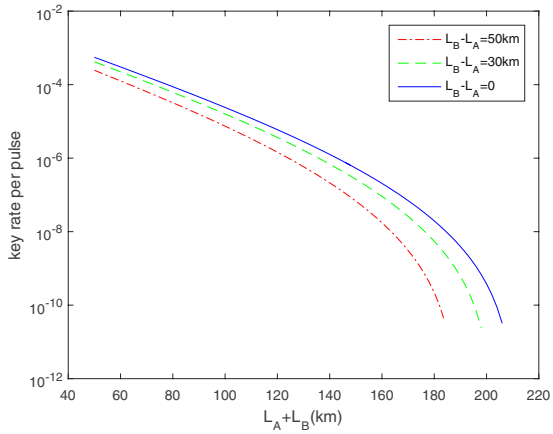

Figure 1. Optimized key rate versus the total distance between Alice and Bob in asymmetric channel with the device parameters in Table 2.

L_A(km)	L_B(km)	Optimized key rate per pulse pair	
		ours	Ref.[45]
10	60	6.299×10^{-5}	3.106×10^{-5}
43	93	3.151×10^{-7}	1×10^{-8}
50	100	6.576×10^{-8}	4.786×10^{-11}
30	60	3.117×10^{-5}	1.445×10^{-5}
59.3	89.3	2.972×10^{-7}	1×10^{-8}
70	100	2.490×10^{-8}	0

Table 1. Optimized key rate at different distances in asymmetric channel with the parameters in Table 2.

N_t	η_d	d	E_d^X	E_d^Z	f	ε
10^{11}	65%	8×10^{-7}	0.5%	0.5%	1.16	10^{-7}

Table 2. Device parameters for Table 1. N_t: total number of pulse pairs; η_d: detection efficiency of the detectors; d: dark count rate of the detectors; E_d^X/E_d^Z: misalignment error rate in the X/Z basis; f: correction efficiency; ε: failure probability for statistical fluctuation evaluation between observable and the mean value.

δ(dB)	$\tilde{\eta}'$(dB)	Optimized key rate per pulse pair
0	0	1.7747×10^{-6}
−7	5	1.5229×10^{-6}
−8.5	4.5	2.2279×10^{-6}
−8.75	4	2.2217×10^{-6}
−8.75	4.5	2.2283×10^{-6}
−8.75	5	2.2184×10^{-6}
−9	4.5	2.2278×10^{-6}

Table 3. Optimized key rate with different δ and $\tilde{\eta}'$ in unstable channel with the parameters in Table 2.

Discussion

We propose a full implementation of four-intensity decoy-state MDIQKD. Even if the channels between the users and UTP are asymmetric, our four-intensity protocol still has a good performance. We also propose a loss-compensation method. This method can improve the key rate a lot in unstable channel.

Method: calculation of the key rate. *Asymptotic case.* We define the yield, the error yield and the error rate as follow. Consider a pulse pair set $\mathcal{C}$, which contains $N_{\mathcal{C}}$ pulse pairs totally. These pairs cause $M_{\mathcal{C}}$ effective counts and $W_{\mathcal{C}}$ error counts. In this case, the yield $S_{\mathcal{C}} = M_{\mathcal{C}}/N_{\mathcal{C}}$, the error yield $T_{\mathcal{C}} = W_{\mathcal{C}}/N_{\mathcal{C}}$ and the error rate $E_{\mathcal{C}} = W_{\mathcal{C}}/M_{\mathcal{C}}$.

In photon number space, the density matrices of the pulses from the sources can be written as

$$\rho_{l_A} = \sum_{k=0}^{\infty} a_{lk}|k\rangle\langle k|, \quad l = x, y, z \tag{7}$$

and

$$\rho_{r_B} = \sum_{k=0}^{\infty} b_{rk}|k\rangle\langle k|, \quad r = x, y, z. \tag{8}$$

We assume that the states above satisfy these conditions:

$$\frac{a_{yk}}{a_{xk}} \geq \frac{a_{y2}}{a_{x2}} \geq \frac{a_{y1}}{a_{x1}}, \quad \frac{b_{yk}}{b_{xk}} \geq \frac{b_{y2}}{b_{x2}} \geq \frac{b_{y1}}{b_{x1}} \tag{9}$$

for $k > 2$, so that the decoy-state results can apply. Familiar sources used in practice, such as weak-coherent-state sources and heralded single-photon sources out of the parametric-down conversion, satisfy the conditions above.

In the following, we will omit the subscript A and B in l_A and r_B if it doesn't cause confusion. A pulse pair of lr is a pair where Alice's pulse is from l and Bob's pulse if from r. The two-mode source lr emits all lr pairs.

The main idea of decoy state is that the yield of $|m\rangle|n\rangle$ photon pairs from different source pairs should be the same in the asymptotic case, which means

$$\langle s_{mn}^{lr}\rangle = \langle s_{mn}\rangle, \quad l, r = x, y, z. \tag{10}$$

Using Eq. (10) and the convex form of yield of lr source pairs

$$\langle S_{lr}\rangle = \sum_{m,n=0}^{\infty} a_{lm}b_{rn}\langle s_{mn}\rangle, \tag{11}$$

we can calculate the lower bound of the yield of single-photon pairs:

$$\langle s_{11}\rangle \geq \underline{\langle s_{11}\rangle} = \frac{S_+ - S_- - a_{y1}b_{y2}\mathcal{H}}{a_{x1}a_{y1}(b_{x1}b_{y2} - b_{x2}b_{y1})} \tag{12}$$

where

$$S_+ = a_{y1}b_{y2}\langle S_{xx}\rangle + a_{x1}b_{x2}a_{y0}\langle S_{oy}\rangle + a_{x1}b_{x2}b_{y0}\langle S_{yo}\rangle, \tag{13}$$

$$S_- = a_{x1}b_{x2}\langle S_{yy}\rangle + a_{x1}b_{x2}a_{y0}b_{y0}\langle S_{oo}\rangle \tag{14}$$

and

$$\mathcal{H} = a_{x0}\langle S_{ox}\rangle + b_{x0}\langle S_{xo}\rangle - a_{x0}b_{x0}\langle S_{oo}\rangle. \tag{15}$$

Eq. (12) holds when

$$K_a = \frac{a_{y1}a_{x2}}{a_{x1}a_{y2}} \leq \frac{b_{y1}b_{x2}}{b_{x1}b_{y2}} = K_b. \tag{16}$$

In the case of $K_a > K_b$, the lower bound of s_{11} can be calculated with Eqs (12–15) by making exchange between a_{xk} and b_{xk}, and exchange between a_{yk} and b_{yk}, for $k = 1, 2$.

Similarly, we can calculate the upper bound of phase-flip error rate of single-photon pairs:

$$\langle e_{11}^{ph}\rangle \leq \overline{\langle e_{11}^{ph}\rangle} = \frac{\langle T_{xx}\rangle - \mathcal{H}/2}{a_{x1}b_{x1}\underline{\langle s_{11}\rangle}}. \tag{17}$$

With $\underline{\langle s_{11}\rangle}$ and $\overline{\langle e_{11}^{ph}\rangle}$, we can calculate the key rate with Eq. (1).

Nonasymptotic case. In the nonasymptotic regime, we should consider the statistical fluctuation of the observable, e.g. the difference between observed values and mean values. Given a failure probability ε, the observed value $S_{\mathcal{C}}$ of an observable of a set $\mathcal{C}$ and its mean value $\langle S_{\mathcal{C}}\rangle$ satisfy:

$$-\Delta_- \leq S_{\mathcal{C}} - \langle S_{\mathcal{C}}\rangle \leq \Delta_+. \tag{18}$$

If we perform a standard error analysis, Δ can be given by

$$\Delta_- = \Delta_+ = \gamma\sqrt{\frac{S_{\mathcal{C}}}{N_{\mathcal{C}}}} \tag{19}$$

where $N_{\mathcal{C}}$ is the number of elements in set $\mathcal{C}$ and $\gamma = 5.3$ given the failure probability $\varepsilon = 10^{-7}$.

According to the idea of joint constraints of statistical fluctuation[23], the set $\mathcal{C}$ can be either all pulse pairs from a source pair, or the combination of all pulse pairs from different source pairs. Taking all these joint constraints into consideration, the bound of $\langle s_{11}\rangle$ and $\langle e_{11}^{ph}\rangle$ can be calculated tighter.

As a joint term in $\underline{\langle s_{11}\rangle}$ and $\overline{\langle e_{11}^{ph}\rangle}$, $\mathcal{H}$ should fluctuate jointly in Eq. (12) and Eq. (17), instead of taking the worst case independently[24]. We regard R as a function of $\mathcal{H}$, scan $\mathcal{H}$ in its possible range and take the minimum R as the final key rate:

$$\widetilde{R} = \min_{\mathcal{H}\in[\underline{\mathcal{H}},\overline{\mathcal{H}}]} R(\mathcal{H}) \tag{20}$$

Method: verifying the global optimization. When we search the points in the nearby area in our optimization algorithm, we can change the parameter Δl in our programme. In the cases with different Δl, e.g. $\Delta l = 0.1, 0.001, 0.0001\ldots$, we obtain almost the same optimized results.

We make another test that to each point, we start from many sets of different initial values of parameters. We then obtain almost the same results for the optimized parameters.

These strongly indicate that our result is indeed the globally optimized result.

References

1. Bennett, C. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (1984).
2. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Physical Review A* **51**, 1863 (1995).
3. Yuen, H. P. Quantum amplifiers, quantum duplicators and quantum cryptography. *Quantum and Semiclassical Optics: Journal of the European Optical Society Part B* **8**, 939 (1996).
4. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Physical Review Letters* **85**, 1330 (2000).
5. Inamori, H., Lütkenhaus, N. & Mayers, D. Unconditional security of practical quantum key distribution. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics* **41**, 599–627 (2007).
6. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters* **91**, 057901 (2003).
7. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters* **94**, 230503 (2005).
8. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Physical review letters* **94**, 230504 (2005).
9. Wang, Q. *et al*. Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source. *Physical review letters* **100**, 090501 (2008).
10. Xu, F. *et al*. Experimental demonstration of counteracting imperfect sources in a practical one-way quantum-key-distribution system. *Physical Review A* **80**, 062309 (2009).
11. Zhang, C.-H., Luo, S.-L., Guo, G.-C. & Wang, Q. Approaching the ideal quantum key distribution with two-intensity decoy states. *Physical Review A* **92**, 022332 (2015).
12. Lydersen, L. *et al*. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics* **4**, 686–689 (2010).
13. Gerhardt, I. *et al*. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature communications* **2**, 349 (2011).
14. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Physical review letters* **108**, 130502 (2012).
15. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Physical review letters* **108**, 130503 (2012).
16. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A* **87**, 012320 (2013).
17. Wang, Q. & Wang, X.-B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. *Physical Review A* **88**, 052332 (2013).
18. Curty, M. *et al*. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature communications 5* (2014).
19. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Three-intensity decoy-state method for measurement-device-independent quantum key distribution. *Physical Review A* **88**, 062339 (2013).
20. 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%. *Physical Review A* **89**, 052325 (2014).
21. Xu, F., Curty, M., Qi, B. & Lo, H.-K. Practical aspects of measurement-device-independent quantum key distribution. *New Journal of Physics* **15**, 113007 (2013).
22. Xu, F., Xu, H. & Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Physical Review A* **89**, 052333 (2014).
23. 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. *Physical Review A* **91**, 032318 (2015).
24. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Physical Review A* **93**, 042324 (2016).
25. Wang, Q., Zhou, X.-Y. & Guo, G.-C. Realizing the measure-device-independent quantum-key-distribution with passive heralded-single photon sources. *Scientific reports* **6** (2016).
26. Jiang, C., Yu, Z.-W. & Wang, X.-B. Measurement-device-independent quantum key distribution with source state errors in photon number space. *Physical Review A* **94**, 062323 (2016).
27. Jiang, C., Yu, Z.-W. & Wang, X.-B. Measurement-device-independent quantum key distribution with source state errors and statistical fluctuation. *Physical Review A* **95**, 032325 (2017).
28. Zhou, X.-Y., Zhang, C.-H., Zhang, C.-M. & Wang, Q. Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources. *Physical Review A* **96**, 052337 (2017).
29. Hu, X.-L., Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Practical measurement-device-independent quantum key distribution without vacuum sources. *Physical Review A* **95**, 032331 (2017).
30. 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. *Physical review letters* **111**, 130501 (2013).
31. Chan, P., Slater, J. A., Lucio-Martinez, I., Rubenok, A. & Tittel, W. Modeling a measurement-device-independent quantum key distribution system. *Optics express* **22**, 12716–12736 (2014).

32. Liu, Y. *et al*. Experimental measurement-device-independent quantum key distribution. *Physical review letters* **111**, 130502 (2013).
33. da Silva, T. F. *et al*. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A* **88**, 052303 (2013).
34. Tang, Z. *et al*. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical review letters* **112**, 190503 (2014).
35. Tang, Y.-L. *et al*. Measurement-device-independent quantum key distribution over 200 km. *Physical review letters* **113**, 190501 (2014).
36. Wang, C. *et al*. Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Physical review letters* **115**, 160502 (2015).
37. Comandar, L. C. *et al*. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics* **10**, 312 (2016).
38. Yin, H.-L. *et al*. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters* **117**, 190501 (2016).
39. Wang, C. *et al*. Measurement-device-independent quantum key distribution robust against environmental disturbances. *Optica* **4**, 1016–1023 (2017).
40. Roberts, G. L. *et al*. Experimental measurement-device-independent quantum digital signatures. *Nature Communications* **8**, 1098 (2017).
41. Pirandola, S. *et al*. High-rate measurement-device-independent quantum cryptography. *Nature Photonics* **9**, 397 (2015).
42. Wang, C.-Y. *et al*. Integrated server for measurement-device-independent quantum key distribution network. *arXiv preprint arXiv:1808.08586* (2018).
43. Boaron, A. *et al*. Secure quantum key distribution over 421 km of optical fiber. *arXiv preprint arXiv:1807.03222* (2018).
44. Wang, Q. & Wang, X.-B. Simulating of the measurement-device independent quantum key distribution with phase randomized general sources. *Scientific reports* **4** (2014).
45. Wang, W., Xu, F. & Lo, H.-K. Enabling a scalable high-rate measurement-device-independent quantum key distribution network. *arXiv preprint arXiv:1807.03466* (2018).

Acknowledgements

We acknowledge the financial support in part by The National Key Research and Development Program of China grant No. 2017YFA0303901; NSFC grant No. 11474182, 11774198 and U1738142; the key Research and Development Plan Project of Shandong Province, grant No. 2015GGX101035; Shandong Peninsula National Innovation Park Development Project; Taishan Scholars of Shandong Province. Yuan Cao was supported by the Youth Innovation Promotion Association of CAS.

Author Contributions

X.B.W. and Y.C. proposed this work. X.L.H. and Z.W.Y. did the calculations and drew the figures. X.L.H. and Y.C. 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.