communications physics

ARTICLE

https://doi.org/10.1038/s42005-022-00831-4 OPEN

Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology

Hong-Wei Li[1]✉, Chun-Mei Zhang[2]✉, Mu-Sheng Jiang[1] & Qing-Yu Cai[3]✉

Quantum key distribution (QKD) provides a promising solution for sharing information-theoretic secret keys between two remote legitimate parties. To improve the maximal transmission distance and the maximal error rate tolerance, we apply the advantage distillation technology to analyze the security of practical decoy-state QKD systems. Based on the practical experimental parameters, the device-dependent QKD protocols and the measurement-device-independent QKD protocols have been respectively analyzed, and our analysis results demonstrate that the advantage distillation technology can significantly improve the performance of various QKD protocols. In the four-state and six-state device-dependent QKD protocols, we prove that the maximal transmission distance can be improved from 142 km to 180 km and from 146 km to 187 km respectively. In the four-state and six-state measurement-device-independent QKD protocols, we prove that the maximal transmission distance can be improved from 195 km to 273 km and from 200 km to 282 km respectively.

[1] Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450000, China. [2] Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China. [3] School of Information and Communication Engineering, Hainan University, Haikou 570228, China. ✉email: lihow@ustc.edu.cn; cmz@njupt.edu.cn; qycai@wipm.ac.cn

Quantum key distribution (QKD)[1,2] is the art of sharing the information-theoretic secure key between two different remote parties Alice and Bob, while the eavesdropper Eve cannot get the secret key information even if she has unlimited computation and storage power[3–5]. The practical QKD system includes four steps to generate the final secret key. In the first step, Alice randomly chooses two classical bits to modulate a single-photon quantum state in two bases, which will be sent to Bob through a public quantum channel. In Bob's side, he randomly chooses a basis to measure the received quantum states. In the second step, Alice and Bob publicly exchange the basis information with an authenticated classical channel, and they only retain those events with the same basis, which is called the raw key. In the third step, they apply the advantage distillation technology to increase the correlation between their raw key, thus they can get an advantage over Eve. In the fourth step, they perform the error correction and privacy amplification to generate the final secret key. Note that the third step may be omitted if the quantum bit error rate (QBER) is small in practical QKD systems, where the advantage distillation technology may have no advantage to increase the correlation. However, in the case of eavesdropping or long transmission distance, QBER will become higher, which will severely reduce the final secret key. Luckily, the advantage distillation technology can be adopted to improve the secret key rate in QKD.

The advantage distillation technology was firstly proposed in the classical cryptography theory[6], which was then utilized in the device-dependent QKD (DD-QKD) protocol[7–9] and device-independent (DI) QKD protocol[10] respectively. By considering the single-photon state modulation, the security of different QKD protocols has been proved with and without the advantage distillation technology respectively[7,8,11,12], and the analysis results demonstrate that the advantage distillation technology can improve the error tolerance of different QKD protocols. However, practical QKD systems are usually based on weak coherent sources, the multi-photon events of which may introduce the photon number splitting attack[13,14]. Fortunately, the decoy-state method[15–17] can be applied to detect this attack, which has been a routine in practical QKD systems. More recently, some statistical fluctuation analysis methods have been proposed to account for the finite-size key effects on the achievable secret key generation rate[18–21].

In practical decoy-state QKD implementations, there are two important questions to be solved. One is how to increase the transmission distance without quantum repeaters, and the other is how to increase the tolerable background error rate. Since the practical quantum repeater technology is still immature until now, measurement-device-independent-QKD (MDI-QKD) protocols[22,23] have been proposed to increase the transmission distance, which require the optical interference device in the middle of the quantum channel. More recently, to beat the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound[24], twin-field QKD[25] was proposed. However, new QKD protocols usually need to change the hardware devices in the first step, which cannot be directly applied in the established QKD systems.

In this paper, to solve these questions, we apply the repetition-code based advantage distillation technology in decoy-state DD-QKD and MDI-QKD protocols respectively. By applying the practical DD-QKD experimental parameters[26], we prove that, for the four-state and six-state DD-QKD protocols, the maximal transmission distance can be improved from 142 km to 180 km and from 146 km to 187 km respectively, and the maximal tolerable background error rate can be improved from 6.2% to 16.4% and from 7% to 21.8% respectively. By applying the practical MDI-QKD experimental parameters[18,27], we prove that, for the four-state and six-state MDI-QKD protocols, the maximal transmission distance can be improved from 195 km to 273 km and from 200 km to 282 km respectively, and the maximal tolerable background error rate can be improved from 4.5% to 14% and from 4.9% to 18% respectively. The analysis results demonstrate that the advantage distillation technology can significantly improve the maximal transmission distance and the maximal tolerable background error rate in different QKD systems. More importantly, the advantage distillation technology does not change the hardware devices about the quantum state preparation and measurement, which can be directly applied to current QKD systems[28–30].

Results

Decoy-state device-dependent QKD with advantage distillation. In practical DD-QKD systems, phase-randomized weak coherent sources, which can be seen as a mixture of photon-number states, are usually applied to modulate quantum states. However, the multi-photon states can be utilized by Eve to launch the photon number splitting attack. Fortunately, the decoy-state method can be applied to estimate the single-photon counting rate and error rate. By considering the weak coherent pulse with the mean photon number μ, the secret key rate can be estimated with the GLLP (Gottesman-Lo-Lütkenhaus-Preskill)[31] formula

$$R_{\text{decoy}} \geq Q_\mu \left[\frac{Y_1 P_1}{Q_\mu} S(A|E)_{\text{single photon}} - H(A|B) \right], \quad (1)$$

where P_1 is the single-photon probability in Alice's signal states, Y_1 is the single-photon counting rate and Q_μ is the total counting rate of signal states. E is Eve's ancillary state, $S(A|E) = S(A,E) - S(E)$, $H(A|B) = H(A,B) - H(B)$, $H(x) = -x\log(x) - (1-x)\log(1-x)$ and $S(\rho) = -\operatorname{tr}(\rho\log\rho)$ are the entropy functions. $S(A|E)_{\text{single photon}}$ is the conditional entropy by considering the single-photon state preparation in Alice's side.

Based on the entanglement distillation and purification technology, $S(A|E)_{\text{single photon}}$ can be restricted by $S(A|E)_{\text{single photon}} \geq 1 - H(e_1)$, where e_1 is the single-photon error rate. Note that $S(A|E)_{\text{single photon}}$ can also be analyzed with the information-theoretical security analysis method, where the detailed explanation is given in the Methods section. Since only the single-photon pulses can be used to generate the final secret key, we can apply the entanglement based QKD protocol to analyze the final secret key rate. In the entanglement based QKD protocol, Alice prepares quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends the second particle to Bob. After quantum channel transmission, Alice and Bob share quantum state $\sigma_{AB} = \sum_{i=0}^{3}\lambda_i|\Phi_i\rangle\langle\Phi_i|$ $(\sum i = 0^3\lambda_i = 1)$, where $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $|\Phi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ (see the Methods section for details). Correspondingly, the relationship between $\lambda_i (i = 0,1,2,3)$ and the single-photon error rate in different bases can be analyzed, where the four-state DD-QKD protocol satisfies $\lambda_1 + \lambda_3 = e_1^x$, $\lambda_2 + \lambda_3 = e_1^z$, and the six-state DD-QKD protocol satisfies $\lambda_1 + \lambda_3 = e_1^x$, $\lambda_2 + \lambda_3 = e_1^z$, $\lambda_1 + \lambda_2 = e_1^y$. e_1^z, e_1^x and e_1^y are the single-photon error rates in the Z basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, the X basis $\{|0\rangle\langle 0|_x, |1\rangle\langle 1|_x\}$, and the Y basis $\{|0\rangle\langle 0|_y, |1\rangle\langle 1|_y\}$, where $|0\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $|0\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, and $|1\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. Based on decoy-state technology, e_1^z, e_1^x and e_1^y can be accurately estimated, so that the constraints of $\lambda_i (i = 0,1,2,3)$ can be obtained.

In the advantage distillation protocol[5], Alice and Bob split their raw key into blocks of b bits $\{x_0, x_1, \ldots x_{b-1}\}$ and $\{y_0, y_1, \ldots y_{b-1}\}$ respectively. Alice privately generates a random bit $c \in \{0,1\}$, and sends the message $m = \{m_0, m_1, \ldots, m_{b-1}\} = \{x_0 \oplus c, x_1 \oplus c, \ldots x_{b-1} \oplus c\}$ to Bob through an authenticated classical channel. They accept the block if and only if $\{m_0 \oplus y_0, m_1 \oplus y_1, \ldots, m_{b-1} \oplus y_{b-1}\}$ equals $\{0,0,\ldots,0\}$ or $\{1,1,\ldots,1\}$, and then keep the first bit x_0 and y_0 as the raw key. Note that if Eve knows any measurement outcome $m_i (0 \leq i \leq b-1)$, she can get all of the b measurement outcomes.

Thus, only the events that all of the b pulses are single-photon states can be used to generate the final secret key, the probability of which is given by $\left(\frac{Y_1P_1}{Q_\mu}\right)^b$. Combining this advantage distillation technology with the information-theoretical security analysis method, the GLLP secret key rate formula can be modified with the following inequality

$$\tilde{R}_{\text{decoy}} \geq \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} q_{\text{succ}} Q_\mu \left[\left(\frac{Y_1P_1}{Q_\mu}\right)^b S(A|E)_{\text{single photon}} - H(A|B) \right], \quad (2)$$

where $q_{\text{succ}} = E_\mu^b + (1-E_\mu)^b$ is the successful probability of the advantage distillation protocol, E_μ is the error rate of signal states, $S(A|E)_{\text{single photon}}$ can be estimated with the following inequality

$$S(A|E)_{\text{single photon}} \geq 1 - (\tilde{\lambda_0}+\tilde{\lambda_1}) H\left(\frac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}}\right) - (\tilde{\lambda_2}+\tilde{\lambda_3}) H\left(\frac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}}\right), \quad (3)$$

where $\tilde{\lambda_0} = \frac{(\lambda_0+\lambda_1)^b+(\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}$, $\tilde{\lambda_1} = \frac{(\lambda_0+\lambda_1)^b-(\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}$, $\tilde{\lambda_2} = \frac{(\lambda_2+\lambda_3)^b+(\lambda_2-\lambda_3)^b}{2p_{\text{succ}}}$, $\tilde{\lambda_3} = \frac{(\lambda_2+\lambda_3)^b-(\lambda_2-\lambda_3)^b}{2p_{\text{succ}}}$, $p_{\text{succ}} = (\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b$ (see the Methods section for details). The modified key rate formula can be explained from two aspects. First, since the quantum channel can be controlled by Eve, she can choose the optimal parameters $\lambda_i (i = 0, 1, 2, 3)$ to reduce the key rate. Secondly, the advantage distillation protocol can be controlled by Alice and Bob, so they can choose the optimal advantage distillation parameter b to increase the key rate.

In the error correction step, all of errors should be corrected by Alice and Bob, thus $H(A|B)$ can be estimated by the following inequality

$$H(A|B) \leq fH(\tilde{E_\mu}), \quad (4)$$

where $\tilde{E_\mu} = \frac{E_\mu^b}{E_\mu^b+(1-E_\mu)^b}$ is the error rate value after the advantage distillation step, $f > 1$ is the error correction efficiency. Since Eve can get all of the classical information transmitted in the classical channel, $fH(\tilde{E_\mu})$ demonstrates the maximal key information leaked to Eve in the error correction step. Finally, the final secret key rate can be estimated with the following optimization method

$$\begin{aligned}
&\max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} q_{\text{succ}} Q_\mu \left[\left(\frac{Y_1P_1}{Q_\mu}\right)^b \left(1 - (\tilde{\lambda_0}+\tilde{\lambda_1}) H\left(\frac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}}\right) \right.\right. \\
&\left.\left. -(\tilde{\lambda_2}+\tilde{\lambda_3}) H\left(\frac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}}\right)\right) - fH(\tilde{E_\mu}) \right] \\
&\text{subject to} \\
&q_{\text{succ}} = E_\mu^b + (1-E_\mu)^b, \\
&\tilde{E_\mu} = \frac{E_\mu^b}{E_\mu^b + (1-E_\mu)^b}, \\
&\lambda_1 + \lambda_3 = e_1^x \text{ (four-state or six-state protocol)}, \\
&\lambda_2 + \lambda_3 = e_1^z \text{ (four-state or six-state protocol)}, \\
&\lambda_1 + \lambda_2 = e_1^y \text{ (six-state protocol)}, \\
&p_{\text{succ}} = (1-e_1^z)^b + (e_1^z)^b, \\
&\tilde{\lambda_0} = \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}, \\
&\tilde{\lambda_1} = \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}, \\
&\tilde{\lambda_2} = \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2p_{\text{succ}}}, \\
&\tilde{\lambda_3} = \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2p_{\text{succ}}},
\end{aligned} \quad (5)$$

where Y_1, e_1^x, e_1^y and e_1^z can be estimated with the decoy-state method (see the Methods section for details). By applying the DD-QKD experimental parameters[26] listed in Table 1, we analyze the secret key rate of the four-state DD-QKD protocol with and without advantage distillation technology, and the corresponding results are shown in Fig. 1.

As shown in Fig. 1, when the optimal b value satisfies $b > 1$, the advantage distillation technology can significantly improve the performance of practical QKD systems, which extends the maximal transmission distance from 142 km to 180 km. On the other side, the calculation results demonstrate that the maximal tolerable background error rate e_{Det} can be improved from 6.2% to 16.4% by adopting the advantage distillation technology. In particular, the maximal transmission distance can be improved from 0 km to 175 km when $e_{Det} = 6.3\%$.

At the same time, we adopt the DD-QKD parameters[26] listed in Table 1 to analyze the six-state DD-QKD protocol with and without advantage distillation technology, and the corresponding results are shown in Fig. 2.

From the calculation results, we find that the maximal transmission distance can be improved from 146 km to 187 km, the maximal tolerable background error rate e_{Det} can be improved from 7% to 21.8%, and the maximal transmission distance can be improved from 0 km to 182 km if the background error rate is $e_{Det} = 7.1\%$. The analysis results demonstrate that the advantage distillation technology can efficiently improve the transmission distance and error tolerance compared with the no advantage distillation case. Moreover, compared with the four-state DD-QKD protocol, the six-state DD-QKD protocol has more superiority both in the transmission distance and the background error rate tolerance.

Decoy-state measurement-device-dependent QKD with advantage distillation. More interestingly, the advantage distillation technology can also be applied to the MDI-QKD protocol. Different from the DD-QKD protocol, the MDI-QKD protocol requires both Alice and Bob to prepare the single-photon state to generate the secret key, and the secret key rate can be estimated with the following optimization method

$$\begin{aligned}
&\max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} q_{\text{succ}} Q_{\mu\mu} \left[\left(\frac{Y_{11}P_{11}}{Q_{\mu\mu}}\right)^b \left(1 - (\tilde{\lambda_0}+\tilde{\lambda_1}) \right.\right. \\
&\left.\left. H\left(\frac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}}\right) - (\tilde{\lambda_2}+\tilde{\lambda_3}) H\left(\frac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}}\right)\right) - fH(\tilde{E_{\mu\mu}}) \right] \\
&\text{subject to} \\
&q_{\text{succ}} = E_{\mu\mu}^b + (1-E_{\mu\mu})^b, \\
&\tilde{E_{\mu\mu}} = \frac{E_{\mu\mu}^b}{E_{\mu\mu}^b + (1-E_{\mu\mu})^b}, \\
&\lambda_1 + \lambda_3 = e_{11}^x \text{ (four-state or six-state protocol)}, \\
&\lambda_2 + \lambda_3 = e_{11}^z \text{ (four-state or six-state protocol)}, \\
&\lambda_1 + \lambda_2 = e_{11}^y \text{ (six-state protocol)}, \\
&p_{\text{succ}} = (1-e_{11}^z)^b + (e_{11}^z)^b, \\
&\tilde{\lambda_0} = \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}, \\
&\tilde{\lambda_1} = \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}, \\
&\tilde{\lambda_2} = \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2p_{\text{succ}}}, \\
&\tilde{\lambda_3} = \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2p_{\text{succ}}},
\end{aligned} \quad (6)$$

where P_{11} is the probability of both Alice and Bob's signal states

Table 1 Experimental parameters of numerical simulations for device-independent quantum key distribution (DD-QKD) and measurement-device-independent quantum key distribution (MDI-QKD) protocols, including the loss coefficient of the standard fiber link α, the detection efficiency of single-photon detectors η_D, the probability that a photon hit the erroneous detector e_{Det}, the dark count rate of single-photon detectors Y_0, and the error correction efficiency f, which are from Ref. [26] and Refs. [18,27] respectively.

Protocols	α	η_D	e_{Det}	Y_0	f	μ
DD-QKD	0.21 dB/km	4.5%	3.3%	1.7×10^{-6}	1.22	0.48
MDI-QKD	0.2 dB/km	14.5%	1.5%	6.02×10^{-6}	1.16	0.48

Moreover, the mean photon number of the signal states μ is also listed here.

emitting single-photon events, Y_{11} is the counting rate of both Alice and Bob transmitting single-photon states, $Q_{\mu\mu}$ ($E_{\mu\mu}$) is the counting rate (error rate) of Alice and Bob's signal states, e_{11}^z, e_{11}^x and e_{11}^y are the single-photon error rate in the Z, X and Y bases respectively. Note that, Y_{11}, e_{11}^x, e_{11}^y and e_{11}^z can be estimated with the decoy-state method (see the Methods section for details). By applying the MDI-QKD experimental parameters[18,27] listed in Table 1, we analyze the secret key rate of the four-state MDI-QKD protocol with and without advantage distillation technology, and the corresponding results are shown in Fig. 3.

As illustrated in Fig. 3, we find that the maximal transmission distance can be improved from 195 km to 273 km, the maximal tolerable background error rate e_{Det} can be improved from 4.5% to 14%, and the maximal transmission distance can be improved from 0 km to 260 km when $e_{Det} = 4.6\%$. The analysis results demonstrate that the advantage distillation technology can significantly improve

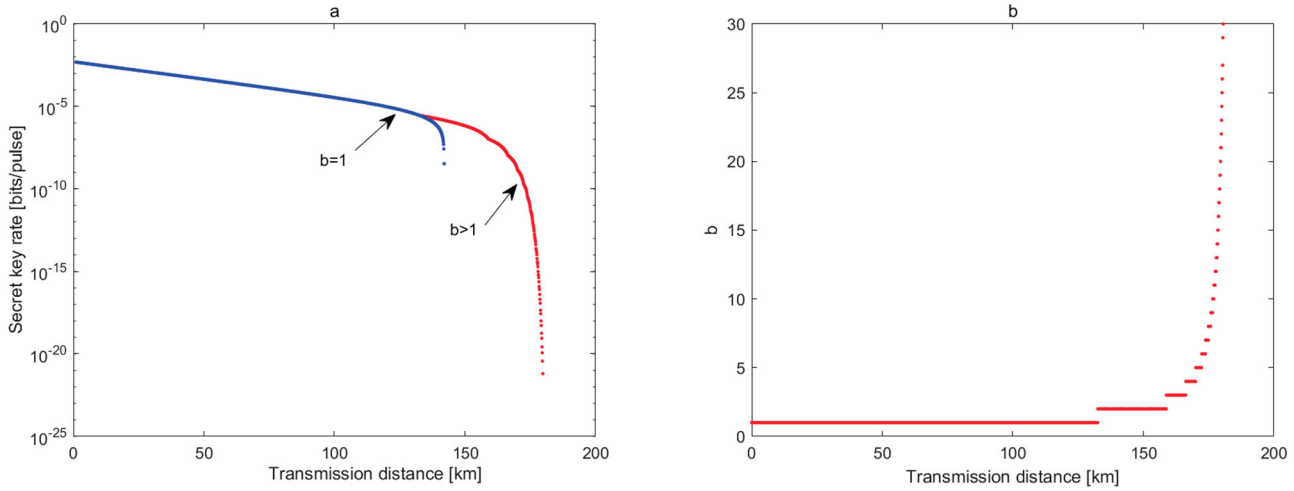

Fig. 1 Results of the four-state device-dependent quantum key distribution (DD-QKD) protocol with and without advantage distillation. a The relationship between the transmission distance and the secret key rate, the blue line is the secret key rate without advantage distillation ($b = 1$), while the red line is the secret key rate with the advantage distillation technology ($b > 1$). **b** The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b > 1$) can improve the secret key rate when the transmission distance is larger than 132 km.

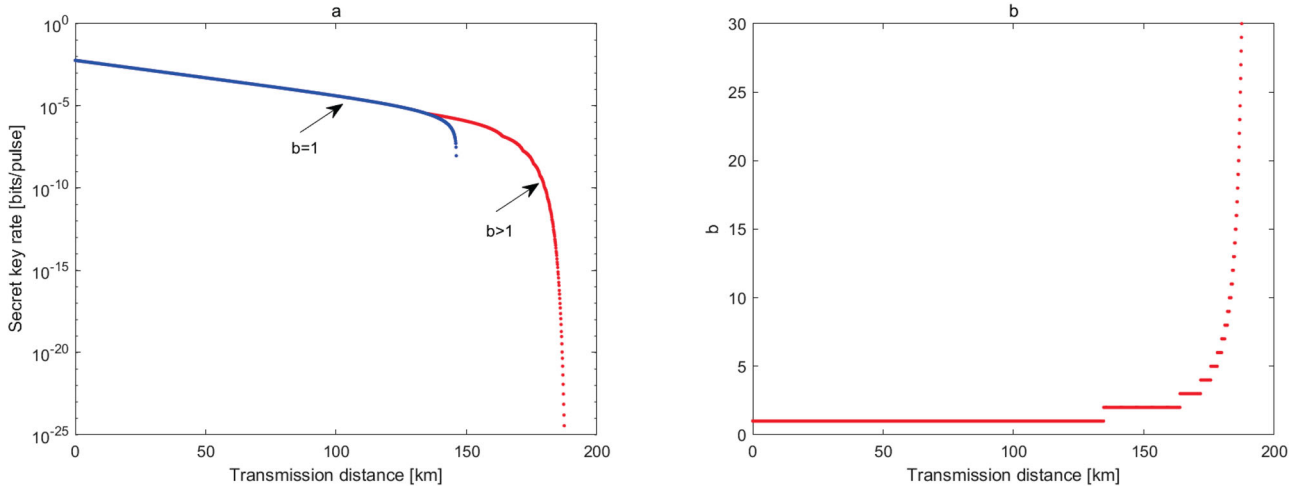

Fig. 2 Results of six-state device-dependent quantum key distribution (DD-QKD) protocol with and without advantage distillation. a The relationship between the transmission distance and the secret key rate, the blue line is the secret key rate without advantage distillation ($b = 1$), while the red line is the secret key rate with the advantage distillation technology ($b > 1$). **b** The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b > 1$) can improve the secret key rate when the transmission distance is larger than 134 km.

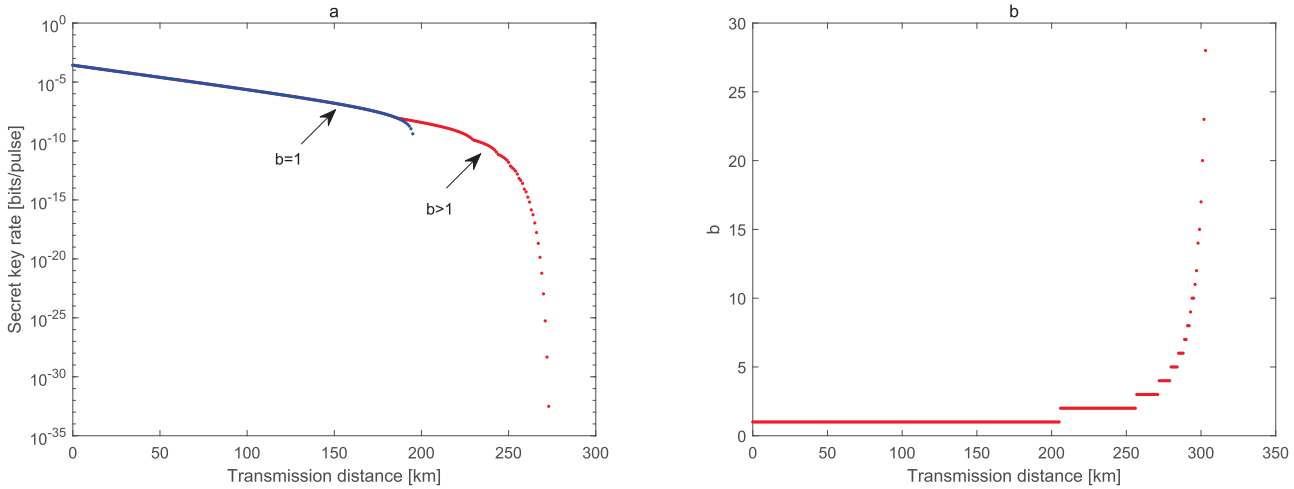

Fig. 3 Results of four-state measurement-device-independent quantum key distribution (MDI-QKD) protocol with and without advantage distillation. **a** The relationship between the transmission distance and the secret key rate, the blue line is the secret key rate without advantage distillation ($b = 1$), while the red line is the secret key rate with the advantage distillation technology ($b > 1$). **b** The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b > 1$) can improve the secret key rate when the transmission distance is larger than 185 km.

the transmission distance and error tolerance compared with the no advantage distillation case.

Similarly, we adopt the MDI-QKD experimental parameters[18,27] listed in Table 1 to analyze the six-state MDI-QKD protocol with and without advantage distillation technology, and the corresponding results are shown in Fig. 4.

From the calculation results, we find that the maximal transmission distance can be improved from 200 km to 282 km, and the maximal tolerable background error rate e_{Det} can be improved from 4.9% to 18%, and the maximal transmission distance can be improved from 0 km to 270 km when $e_{Det} = 5\%$. Compared with the four-state MDI-QKD protocol, the six-state MDI-QKD protocol has more advantage both in the transmission distance and the background error rate tolerance. Moreover, we also plot the PLOB bound[24] in Fig. 4, and the performance of six-state MDI-QKD with advantage distillation is obviously lower than the PLOB bound. Fortunately, the twin-field QKD protocol[25] proposed recently can surpass the PLOB bound. The advantage distillation method developed in this paper can also be extended to twin-field QKD[25] to further improve its performance, and we will leave this as future research.

Finite key security analysis. In practical QKD systems, the generated secret key is finite, thus how to prove security of QKD with the advantage distillation technology in finite-key scenarios is an important question. Since the advantage distillation technology only modifies the classical post-processing step, we can simply analyze the finite key length with the existed methods. More precisely, based on the quantum asymptotic equipartition property[32,33] and the leftover hash lemma[5,34], the secret key rate with the DD-QKD protocol can be given by

$$\begin{aligned}\widetilde{R}_{\mathrm{decoy}} &\geq \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} q_{\mathrm{succ}} Q_\mu [S^{\varepsilon_{min}}_{\mathrm{min}}(A|E)_{\mathrm{single\ photon}} - H(A|B)] \\ &\geq \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} q_{\mathrm{succ}} Q_\mu \left[\left(\frac{Y_1 P_1}{Q_\mu}\right)^b \left(1 - \left(\tilde{\lambda}_0 + \tilde{\lambda}_1\right) H \right.\right. \\ &\left.\left. \left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1}\right) - (\tilde{\lambda}_2 + \tilde{\lambda}_3) H\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3}\right)\right) - f H(\tilde{E}_\mu) - \Delta \right],\end{aligned} \tag{7}$$

where

$$\Delta = 4\sqrt{\frac{b}{n}} \log(2\sqrt{2^{H_{\max}(A|E)}} + 1) \sqrt{\log \frac{2}{\varepsilon^2_{\min}}} + \frac{2b}{n} \log \frac{1}{\varepsilon_{\mathrm{pa}}}, \tag{8}$$

n is the raw key length before the advantage distillation step, $H_{\max}(A|E)$ is the conditional max-entropy function[5], $H^{\varepsilon_{\min}}_{\min}(A|E) = \max_{\sigma_{AE} \in \mathcal{B}^{\varepsilon_{\min}}(\rho_{AE})} H_{\min}(A|E)$, $\mathcal{B}^{\varepsilon_{\min}}(\rho_{AE})$ is the set of sub-normalized states σ_{AE} with $D(\sigma_{AE}, \rho_{AE}) \leq \varepsilon_{\min}$, and the final secret parameter can be given by $\varepsilon \equiv \varepsilon_{\mathrm{pa}} + 2\varepsilon_{\min}$. Note that the the secret key rate with the MDI-QKD protocol can be analyzed similarly. In the practical experimental realization, the QBER value and the count rate value also have statistical fluctuations, which can be analyzed by applying the Chernoff bound and the Hoeffding inequality[20,21]. However, we should emphasize that the advantage distillation technology reduces the length of the raw key when $b > 1$, thus it has larger statistical error to analyze the security of QKD protocols with finite resources.

Conclusions

Improvements on the maximal transmission distance and the maximal error rate tolerance are two important topics of analyzing the security of practical QKD systems. By combining the advantage distillation technology with the decoy-state method, we prove that both the maximal transmission distance and the maximal tolerable error rate can be sharply improved in different DD-QKD and MDI-QKD protocols. More importantly, the advantage distillation technology does not change the quantum step of a practical QKD system. It only modifies the classical post-processing step, so it can be conveniently applied to various practical QKD systems. In the future research, it will be interesting to experimentally realize the advantage distillation technology in different QKD systems.

Methods

Single-photon QKD with advantage distillation. In the four-state or six-state DD-QKD protocol, Alice and Bob randomly prepare and measure the quantum state in the two-dimensional Hilbert spaces. By applying the entanglement based protocol, we assume that Alice prepares the quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends the second particle to Bob, then Alice and Bob take inputs from four-dimensional Hilbert spaces $H_A \otimes H_B$ to apply binary measurements. By considering the four-state and six-state QKD protocols, it has been proved that Eve's general attack can be reduced to the Pauli attack[5,11], which can be described by the classical probability theory. After quantum channel transmission, Alice and Bob

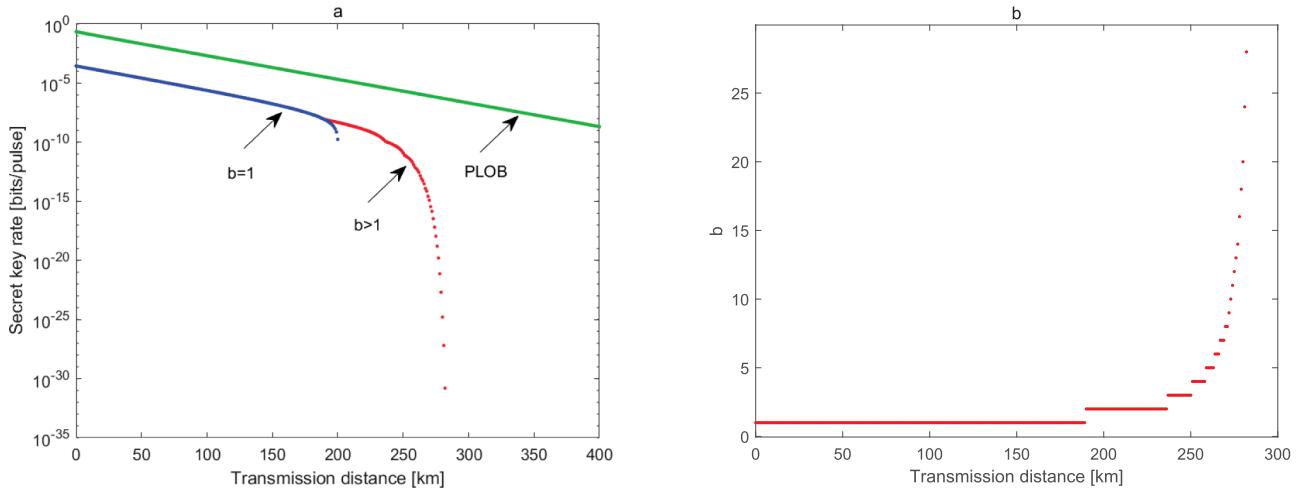

Fig. 4 Results of six-state measurement-device-independent quantum key distribution (MDI-QKD) protocol with and without advantage distillation. **a** The relationship between the transmission distance and the secret key rate, the blue line is the secret key rate without advantage distillation ($b = 1$), the red line is the secret key rate with the advantage distillation technology ($b > 1$), and the green line is the Pirandola- Laurenza-Ottaviani-Banchi (PLOB) bound. **b** The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b > 1$) can improve the secret key rate when the transmission distance is larger than 189 km.

share the following quantum state

$$\sigma_{AB} = \sum_{i=0}^{3} \lambda_i |\Phi_i\rangle\langle\Phi_i|, \quad \text{with} \quad \sum_{i=0}^{3} \lambda_i = 1, \tag{9}$$

where

$$\begin{aligned} |\Phi_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Phi_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\Phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{10}$$

Obviously, the single-photon error rates in the Z basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, the X basis $\{|0\rangle\langle 0|_x, |1\rangle\langle 1|_x\}$, and the Y basis $\{|0\rangle\langle 0|_y, |1\rangle\langle 1|_y\}$ are constrained by $\lambda_2 + \lambda_3 = e_1^z$, $\lambda_1 + \lambda_3 = e_1^x$, and $\lambda_1 + \lambda_2 = e_1^y$ respectively. Since Eve holds the purified system of σ_{AB}, we have the following pure state σ_{ABE} on $H_A \otimes H_B \otimes H_E$

$$\sigma_{ABE} = |\Psi\rangle\langle\Psi|_{ABE}, \text{with} |\Psi\rangle_{ABE} = \sum_{i=0}^{3} \sqrt{\lambda_i} |\Phi_i\rangle_{AB} \bigotimes |e_i\rangle_E, \tag{11}$$

where the reduced density operator σ_{AE} and σ_E can be respectively given by

$$\sigma_{AE} = \mathrm{tr}_B \sigma_{ABE}, \ \sigma_E = \mathrm{tr}_A \sigma_{AE}. \tag{12}$$

Note that the quantum channel can be controlled by Eve, she can choose the optimal parameters $\lambda_i (i = 0, 1, 2, 3)$ to reduce the secret key rate as long as λ_i is constrained by the QBER in different bases. Based on the this state preparation, the secret key rate can be given by[5]

$$\begin{aligned} R &\geq \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} [S(A|E) - H(A|B)] \\ &= \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \left[1 - (\lambda_0 + \lambda_1) H\left(\frac{\lambda_0}{\lambda_0 + \lambda_1}\right) - (\lambda_2 + \lambda_3) H\left(\frac{\lambda_2}{\lambda_2 + \lambda_3}\right) - H(\lambda_0 + \lambda_1)\right], \end{aligned} \tag{13}$$

where $H(A|B) = H(\lambda_0 + \lambda_1)$ demonstrates that Z basis is used for generating the final secret key.

To improve the maximal tolerable QBER, the advantage distillation technology based on the repetition code protocol has been proposed[5]. In the repetition code protocol, Alice and Bob split their raw key into blocks of b bits $\{x_0, x_1, \ldots x_{b-1}\}$ and $\{y_0, y_1, \ldots y_{b-1}\}$ respectively. Alice privately generates a random bit $c \in \{0, 1\}$, and sends the message $m = \{m_0, m_1, \ldots, m_{b-1}\} = \{x_0 \oplus c, x_1 \oplus c, \ldots x_{b-1} \oplus c\}$ to Bob through an authenticated classical channel. They accept the block if and only if $\{m_0 \oplus y_0, m_1 \oplus y_1, \ldots, m_{b-1} \oplus y_{b-1}\}$ equals $\{0, 0, \ldots, 0\}$ or $\{1, 1, \ldots, 1\}$, and then keep the first bit x_0 and y_0 as the raw key. That is, if all bits in $\{x_0, x_1, \ldots x_{b-1}\}$ and $\{y_0, y_1, \ldots y_{b-1}\}$ are completely the same or different, Alice and Bob will obtain a raw key bit, the corresponding successful probability of which is given by

$$p_{\mathrm{succ}} = (\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b. \tag{14}$$

We emphasize that the successful probability p_{succ} can be further improved if Alice and Bob iteratively repeat the advantage distillation protocol on very small blocks. Consequently, the practical QBER value in the Z basis can be reduced from $\lambda_2 + \lambda_3$ to $\frac{(\lambda_2+\lambda_3)^b}{p\mathrm{succ}}$, and the quantum state shared between Alice and Bob can be given by[5]

$$\tilde{\sigma}_{AB} = \tilde{\lambda_0} |\Phi_0\rangle\langle\Phi_0| + \tilde{\lambda_1} |\Phi_1\rangle\langle\Phi_1| + \tilde{\lambda_2} |\Phi_2\rangle\langle\Phi_2| + \tilde{\lambda_3} |\Phi_3\rangle\langle\Phi_3|, \tag{15}$$

where

$$\begin{aligned} \tilde{\lambda_0} &= \frac{(\lambda_0 + \lambda_1)^b + (\lambda_0 - \lambda_1)^b}{2p_{\mathrm{succ}}}, \\ \tilde{\lambda_1} &= \frac{(\lambda_0 + \lambda_1)^b - (\lambda_0 - \lambda_1)^b}{2p_{\mathrm{succ}}}, \\ \tilde{\lambda_2} &= \frac{(\lambda_2 + \lambda_3)^b + (\lambda_2 - \lambda_3)^b}{2p_{\mathrm{succ}}}, \\ \tilde{\lambda_3} &= \frac{(\lambda_2 + \lambda_3)^b - (\lambda_2 - \lambda_3)^b}{2p_{\mathrm{succ}}}. \end{aligned} \tag{16}$$

Based on the state preparation $\tilde{\sigma}_{AB}$ and the advantage distillation parameter b, the secret key rate $\tilde{R}$ can be modified as the following inequality

$$\begin{aligned} \tilde{R} \geq \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} p_{\mathrm{succ}} \Bigg[& 1 - (\tilde{\lambda_0} + \tilde{\lambda_1}) H\left(\frac{\tilde{\lambda_0}}{\tilde{\lambda_0} + \tilde{\lambda_1}}\right) \\ & - (\tilde{\lambda_2} + \tilde{\lambda_3}) H\left(\frac{\tilde{\lambda_2}}{\tilde{\lambda_2} + \tilde{\lambda_3}}\right) - H(\tilde{\lambda_0} + \tilde{\lambda_1}) \Bigg]. \end{aligned} \tag{17}$$

Note that the advantage distillation protocol can be controlled by Alice and Bob, so they can choose the optimal advantage distillation parameter b to improve the secret key rate.

Security analysis of decoy-state QKD. Firstly, we consider the security analysis of decoy-state QKD without advantage distillation. Combining Eq. (13) with the decoy-state method[15–17], the secret key rate with DD-QKD system can be given by

$$R'_{\mathrm{decoy}} \geq \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} Q_\mu \left[\frac{Y_1 P_1}{Q_\mu} S(A|E)_{\text{single photon}} - f H(E_\mu) \right], \tag{18}$$

where P_1 is the single-photon probability in Alice's signal states, Y_1 is the single-photon counting rate, Q_μ and E_μ denote the counting rate and error rate of signal states, Inspired by the information-theoretical security analysis method given by[5], $S(A|E)_{\text{single photon}}$ can be estimated with the following inequality

$$S(A|E)_{\text{single photon}} \geq 1 - (\lambda_0 + \lambda_1) H\left(\frac{\lambda_0}{\lambda_0 + \lambda_1}\right) - (\lambda_2 + \lambda_3) H\left(\frac{\lambda_2}{\lambda_2 + \lambda_3}\right), \tag{19}$$

where $\lambda_i (i = 0, 1, 2, 3)$ can be characterized with the following equations

$$\begin{aligned} \lambda_1 + \lambda_3 &= e_1^x, \\ \lambda_2 + \lambda_3 &= e_1^z, \\ \lambda_1 + \lambda_2 &= e_1^y, \end{aligned} \tag{20}$$

where e_1^z, e_1^x and e_1^y are the single-photon error rates in the Z, X and Y bases, which can be estimated with the decoy-state method.

Similarly, by considering the Bell state measurement outcome $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in Charlie's side, the secret key rate with decoy-state MDI-QKD system can be given by

$$R'_{\text{decoy}} \geq \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} Q_{\mu\mu}\left[\frac{Y_{11}P_{11}}{Q_{\mu\mu}} S(A|E)_{\text{single photon}} - fH(E_{\mu\mu})\right], \tag{21}$$

where P_{11} is the probability of both Alice and Bob's signal states emitting single-photon events, Y_{11} is the counting rate of both Alice and Bob transmitting single-photon states, and $Q_{\mu\mu}$ ($E_{\mu\mu}$) is the counting rate (error rate) of Alice and Bob's signal states. Similarly, $\lambda_i (i = 0, 1, 2, 3)$ can be characterized with the following equations

$$\begin{aligned} \lambda_1 + \lambda_3 &= e_{11}^x, \\ \lambda_2 + \lambda_3 &= e_{11}^z, \\ \lambda_1 + \lambda_2 &= e_{11}^y, \end{aligned} \tag{22}$$

where e_{11}^z, e_{11}^x and e_{11}^y are the single-photon error rates in the Z, X and Y bases, which can be estimated with decoy-state method. Note that the other three Bell states measurement outcomes can be analyzed similarly.

As for the security analysis of decoy-state with advantage distillation which has been given in Section II, we will not repeated it here.

Simulation method of decoy-state QKD with advantage distillation. To simulate the performance of decoy-state QKD with advantage distillation, we adopt infinite decoy states to precisely estimate channel parameters. Briefly, combining Eq. (18) with the advantage distillation method[7–9], the secret key rate with the DD-QKD system can be given in Eq. (5). Combining Eq. (21) with the advantage distillation method[7–9], the secret key rate with the MDI-QKD system can be given in Eq. (6). Compared with the secret key rate without advantage distillation, only the events that all of the b pulses are single-photon states can be used to generate the final secret key, thus the advantage distillation parameter b should be optimized to maximize the final secret key.

For the decoy-state DD-QKD with advantage distillation, the corresponding parameters Y_1, P_1, e_1^x, e_1^y, e_1^z, Q_μ and E_μ are given as $P_1 = \mu e^{-\mu}$, $\eta = 10^{\frac{-\alpha l}{10}}\eta_D$, $Y_1 = Y_0 + \eta$, $e_1^x = e_1^y = e_1^z = \frac{0.5Y_0 + e\text{Det}\eta}{Y_1}$, $Q_\mu = Y_0 + 1 - e^{-\eta\mu}$, $E_\mu = \frac{0.5Y_0 + e\text{Det}(1-e^{-\eta\mu})}{Q_\mu}$ [35]. By applying the practical DD-QKD experimental parameters[26] listed in Table 1, the secret key rate of decoy-state DD-QKD with advantage distillation can be easily estimated. Similarly, by adopting the simulation model in[36] (see Eqs. (2)–(7) in[36] for details), the secret key rate of decoy-state MDI-QKD with advantage distillation can be easily estimated.

Data availability

The data that support the findings of this study are available from the corresponding authors on request.

Code availability

Source codes of the plots are available from the corresponding authors on request.

Received: 26 July 2021; Accepted: 17 February 2022;
Published online: 11 March 2022

References

1. Charles H, B. & Gilles, B. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
2. Dagmar, Bruß Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018 (1998).
3. Hoi-Kwong, L. & Hoi Fung, C. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
4. Peter W, S. & John, P. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
5. Renato, R. Security of quantum key distribution. *Int. J. Quant. Inform.* **6**, 1–127 (2008).
6. Ueli M, M. Secret key agreement by public discussion from common information. *IEEE Trans Inform Theory* **39**, 733–742 (1993).
7. Barbara, K., Cyril, B. & Renato, R. Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses. *Phys. Rev. A* **75**, 012316 (2007).
8. Joonwoo, B. & Antonio, A. Key distillation from quantum channels using two-way communication protocols. *Phys. Rev. A* **75**, 012334 (2007).
9. Glaucia, M., Filip, R., Jeremy, R., David, E. & Stephanie, W. Key rates for quantum key distribution protocols with asymmetric noise. *Phys. Rev. A* **101**, 062321 (2020).
10. Ernest Y-Z, T., Charles C-W, L. & Renato, R. Advantage distillation for device-independent quantum key distribution. *Phys. Rev. Lett.* **124**, 020502 (2020).
11. Daniel, G. & Hoi-Kwong, L. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inform. Theory* **49**, 457–475 (2003).
12. Hoi Fung, C. Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. *Phys. Rev. A* **66**, 060302 (2002).
13. Bruno, H., Nobuyuki, I., Nicolas, G. & Tsafrir, M. Quantum cryptography with coherent states. *Phys. Rev. A* **51**, 1863 (1995).
14. Norbert, L. ütkenhaus & Mika, J. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *N. J. Phys.* **4**, 44 (2002).
15. Won-Young, H. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
16. Xiang-Bin, W. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
17. Hoi-Kwong, L., Xiongfeng, M. & Kai, C. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
18. Feihu, X., He, X. & Hoi-Kwong, L. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052333 (2014).
19. Geng, C. et al. Parameter estimation of atmospheric continuous-variable quantum key distribution. *Phys. Rev. A* **99**, 032326 (2019).
20. Marcos, C. et al. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 1–7 (2014).
21. Charles Ci Wen, L., Marcos, C., Nino, W., Feihu, X. & Hugo, Z. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
22. Samuel L, B. & Stefano, P. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
23. Hoi-Kwong, L., Marcos, C. & Bing, Q. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
24. Stefano, P., Riccardo, L., Carlo, O. & Leonardo, B. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 1–15 (2017).
25. Marco, L., Zhiliang L, Y., James F, D. & Andrew J, S. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
26. C, G., aZL, Y. & AJ, S. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84**, 3762–3764 (2004).
27. Rupert, U. et al. Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3**, 481–486 (2007).
28. Guan-Jie, Fan-Yuan et al. A universal simulating framework for quantum key distribution systems. *Sci. China Inf. Sci.* **63**, 1–15 (2020).
29. Liao, Sheng-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
30. Chen, Yu-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
31. Daniel, G., Hoi-Kwong, L., Norbert, L. ütkenhaus & John, P. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325–360 (2004).
32. Marco, T., A framework for non-asymptotic quantum information theory. Preprint https://arxiv.org/abs/1203.2142 (2012).
33. Rotem, Arnon-Friedman, Reductions to iid in device-independent quantum information processing. Preprint at https://arxiv.org/abs/1812.10922 (2018).
34. Jaikumar, R. & Amnon, Ta-Shma Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J Discrete Math.* **13**, 2–24 (2000).
35. Xiongfeng, M., Bing, Q., Yi, Z. & Hoi-Kwong, L. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
36. Xiongfeng, M., Chi-Hang Fred, F. & Mohsen, R. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).

Acknowledgements

The authors would like to thank Zhen-Qiang Yin for his helpful discussion. This work is supported by National Key Research and Development Program of China (Grant no. 2020YFA0309702), NSAF (Grant no. U2130205), National Natural Science Foundation of China (Grant no. 11725524), Natural Science Foundation of Henan (Grant no. 202300410532), and China Postdoctoral Science Foundation (2019T120446, 2018M642281).

Author contributions

H.-W.L. and Q.-Y.C. conceived the project. H.-W.L., C.-M.Z. and M.-S.J. performed the calculation and analysis. H.-W.L. and C.-M.Z. wrote the paper.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42005-022-00831-4.

Correspondence and requests for materials should be addressed to Hong-Wei Li, Chun-Mei Zhang or Qing-Yu Cai.

Peer review information *Communications Physics* thanks Yichen Zhang and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. Peer reviewer reports are available.

Reprints and permission information is available at http://www.nature.com/reprints

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