Improving the Performance of Practical Quantum Key Distribution With Advantage Distillation Technology

Hong-Wei Li (h.w.lee.roy@gmail.com)
Zhengzhou Information Science and Technology Institute
Chun-Mei Zhang
Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications
Mu-Sheng Jiang
Henan Key Laboratory of Quantum Information and Cryptography
Qing-Yu Cai
Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences

Article

Keywords: Quantum key distribution (QKD), practical, distillation technology, advantage, maximal transmission distance

Posted Date: August 3rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-753036/v1

Version of Record: A version of this preprint was published at Communications Physics on March 11th, 2022. See the published version at https://doi.org/10.1038/s42005-022-00831-4.

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

Hong-Wei Li[1*], Chun-Mei Zhang[2†], Mu-Sheng Jiang[1], Qing-Yu Cai[3‡]
[1] *Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou 450000, China*
[2] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[3] *Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071, China*

To improve the maximal transmission distance and the maximal error rate tolerance, we apply the advantage distillation technology to analyze security of the practical decoy-sate quantum key distribution system. Based on the practical experimental parameters, the device-dependent quantum key distribution protocols and the measurement-device-independent quantum key distribution protocols have been respectively analyzed, and our analysis results demonstrate that the advantage distillation technology can significantly improve the performance of different quantum key distribution protocols. In the four-state and six-state device-dependent quantum key distribution 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 quantum key distribution 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. More interestingly, the advantage distillation technology does not need to change the hardware devices about the quantum step, thus it can be conveniently to be applied in various practical quantum key distribution systems.

I. INTRODUCTION

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 can not 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 state. In the second step, Alice and Bob publicly exchanges the basis information with an authenticated classical channel, and they only retain those events with the same bases, which is called the raw key. In the third step, they apply an advantage distillation technology to increase the correlation, 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, QBER becomes higher in the case of eavesdropping by Eve or long transmission distance, thus we can utilize the advantage distillation technology to improve the secret key rate. 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, security of the QKD protocol 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.

In practical decoy-state QKD implementations, there are two important questions to be solved. The first question is how to increase the transmission distance without the quantum repeater, and the second question is how to increase the tolerable background error rate. More recently, measurement-device-independent-QKD (MDI-QKD) protocols [18, 19] have been proposed to increase the transmission distance, which require the optical interference device in the middle of the quantum channel. However, new QKD protocols usually need to change the hardware devices in the first step, and it can not be directly applied in the established QKD systems. In this paper, to solve the two important questions, we apply the the repetition-code based advantage distillation technology to improve the transmission distance and the error tolerance in decoy-state DD-QKD and MDI-QKD respectively. By applying the practical DD-QKD experimental parameters [20], 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 [21, 22], 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 with the four state and six state MDI-QKD protocols, and the maximal tolerate background error rate can be improved from 4.5% to 14% and from 4.9% to 18% with the four state and six state MDI-QKD protocol respectively. This analysis results demonstrate that the advantage distillation technology can significantly improve the maximal transmission distance and the maximal tolerable background error rate with different practical QKD systems. More importantly, the advantage distillation technology does not need to change the hardware devices in the first step, thus it can be directly applied in different QKD systems [23–25].

II. 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 and Bob take inputs from four-dimensional Hilbert spaces $H_A \otimes H_B$ to apply binary measurements. It has been proved that the QKD protocol can be illustrated with the following quantum state preparation [5],

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

where

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

Since Eve hold the purifying system of σ_{AB}, we have the following pure state σ_{ABE} on $H_A \otimes H_B \otimes H_E$

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

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

$$\sigma_{AE} = Tr_B \sigma_{ABE}, \quad \sigma_E = Tr_A \sigma_{AE}. \tag{4}$$

Based on the previous state preparation, the corresponding secret key rate can be given by [5]

$$\begin{array}{l} R \geq min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}[S(A|E) - H(A|B)] \\ \quad = min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}[1 - (\lambda_0+\lambda_1)H(\frac{\lambda_0}{\lambda_0+\lambda_1}) - (\lambda_2+\lambda_3)H(\frac{\lambda_2}{\lambda_2+\lambda_3}) - H(\lambda_0+\lambda_1)], \end{array} \tag{5}$$

where $H(x)$ and $S(\rho)$ are the entropy functions, $H(A|B) = H(\lambda_0 + \lambda_1)$ demonstrates that the rectilinear basis $\{|0\rangle\langle 0|_z, |1\rangle\langle 1|_z\}$ 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 $x_0, x_1, ...x_{b-1}$ and $y_0, y_1, ...y_{b-1}$ respectively. Alice privately generates a random bit $c \in \{0, 1\}$, and sends the message $m = m_0, m_1, ..., m_{b-1} = x_0 \oplus c, x_1 \oplus c, ...x_{b-1} \oplus c$ to Bob through an authenticated classical channel. Bob accepts the block if and only if $m_0 \oplus y_0, m_1 \oplus y_1, ..., m_{b-1} \oplus y_{b-1} \in \{0, 0, ...0 \ or \ 1, 1, ..., 1\}$. If Alice and Bob accept the block, they keep the first bit x_0 and y_0 as the raw key. Finally, Alice and Bob will apply the error correction and privacy amplification to get the final secret key.

In this advantage distillation protocol, Alice and Bob keep their bit in the case of the b bits having no error bit or having b error bits, thus the successful probability of this protocol can be given by

$$p_{succ} = (\lambda_0 + \lambda_1)^b + (\lambda_2 + \lambda_3)^b. \tag{6}$$

By applying the previous advantage distillation technology, the practical QBER value in the rectilinear basis can be reduced from $\lambda_2 + \lambda_3$ to $\frac{(\lambda_2+\lambda_3)^b}{p_{succ}}$, and the quantum state shared between Alice and Bob can be given by [5]

$$\tilde{\sigma}_{AB} = \tilde{\lambda_0}|\Phi_0\rangle\langle\Phi_0| + \tilde{\lambda_1}|\Phi_1\rangle\langle\Phi_1| + \tilde{\lambda_2}|\Phi_2\rangle\langle\Phi_2| + \tilde{\lambda_3}|\Phi_3\rangle\langle\Phi_3|, \tag{7}$$

where

$$\begin{array}{l} \tilde{\lambda_0} = \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2p_{succ}}, \\ \tilde{\lambda_1} = \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2p_{succ}}, \\ \tilde{\lambda_2} = \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2p_{succ}}, \\ \tilde{\lambda_3} = \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2p_{succ}}. \end{array} \tag{8}$$

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

$$\tilde{R} \geq max_b\ min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \tfrac{1}{b} p_{succ}[1-(\tilde{\lambda_0}+\tilde{\lambda_1})H(\tfrac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}})-(\tilde{\lambda_2}+\tilde{\lambda_3})H(\tfrac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}})-H(\tilde{\lambda_0}+\tilde{\lambda_1})], \tag{9}$$

where Alice and Bob can choose the optimal advantage distillation parameter b to improve the secret key rate.

III. DECOY-STATE QKD WITH ADVANTAGE DISTILLATION

In practical QKD systems, weak coherent sources are usually applied to modulate the quantum state, but the multi photon state may be attacked by Eve to apply the photon number splitting attack. Fortunately, the decoy-state method can be applied to exactly estimate the single-photon counting rate and error rate, thus the secret key rate can be estimated. Based on the advantage distillation technology and the decoy-state method, we can get the modified secret key rate with the following inequality

$$R_{decoy} \geq max_b\ min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \tfrac{1}{b} p_{succ} Q_\mu [S(A|E) - H(A|B)], \tag{10}$$

where Q_μ is the total counting rate of signal states, and p_{succ} is the successful probability of this protocol. Based on the secret key rate analysis result with the single photon state, the conditional entropy function $S(A|E)$ can be estimated by the following equation

$$S(A|E) \geq (\tfrac{Y_1 P_1}{Q_\mu})^b (1-(\tilde{\lambda_0}+\tilde{\lambda_1})H(\tfrac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}})-(\tilde{\lambda_2}+\tilde{\lambda_3})H(\tfrac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}})), \tag{11}$$

where P_1 is the single-photon probability in Alice's signal states, and Y_1 is the single-photon counting rate. In the advantage distillation protocol, Eve can get all of the b measurement outcomes if any measurement outcome m_i $(0 \leq i \leq b-1)$ is known by Eve, thus only the case that all of the b pulses are single-photon states can be used to generate the final secret key. In practical decoy state QKD systems with coherent sources, the probability of b rounds with single-photon pulses can be given by $(\frac{Y_1 P_1}{Q_\mu})^b$. Since only the single-photon pulse can be used to generate the final secret key, we consider the quantum state $\sigma_{AB} = \sum_{i=0}^{3} \lambda_i |\Phi_i\rangle\langle\Phi_i|$ with the single-photon state preparation in Alice's side. Correspondingly, the four-state DD-QKD protocol has the following restriction $\lambda_1+\lambda_3 = e_1^x, \lambda_2+\lambda_3 = e_1^z$, and the six-state DD-QKD protocol has the following restriction $\lambda_1+\lambda_3 = e_1^x,\ \lambda_2+\lambda_3 = e_1^z,\ \lambda_1+\lambda_2 = e_1^y$, where e_1^x, e_1^y and e_1^z are the single-photon error rate in the rectilinear basis, diagonal basis $\{|0\rangle\langle 0|_x, |1\rangle\langle 1|_x,\ where\ |0\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ and the circular basis $\{|0\rangle\langle 0|_y, |1\rangle\langle 1|_y,\ where\ |0\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |1\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$ respectively.

In the error correction step, all of errors should be corrected by Alice and Bob, thus the conditional entropy function $S(A|B)$ can be estimated by the following equation

$$H(A|B) \leq fh(\tilde{E_\mu}), \tag{12}$$

where $\tilde{E_\mu} = \frac{E_\mu^b}{E_\mu^b + (1-E_\mu)^b}$ is the error rate value after the advantage distillation protocol, f is the error correction efficiency. Based on the previous analysis result, the final secret key rate can be estimated with the following optimization method

$$\begin{aligned}
&max_b\ min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}\ \tfrac{1}{b} q_{succ} Q_\mu [(\tfrac{Y_1 P_1}{Q_\mu})^b (1-(\tilde{\lambda_0}+\tilde{\lambda_1})H(\tfrac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}})-(\tilde{\lambda_2}+\tilde{\lambda_3})H(\tfrac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}})) - fh(\tilde{E_\mu})] \\
&subject\ \ to \\
&\quad q_{succ} = E_\mu^b + (1-E_\mu)^b \\
&\quad \tilde{E_\mu} = \tfrac{E_\mu^b}{E_\mu^b + (1-E_\mu)^b} \\
&\quad \lambda_1+\lambda_3 = e_1^x \ \ (four-state\ or\ six-state\ protocol) \\
&\quad \lambda_2+\lambda_3 = e_1^z \ \ (four-state\ or\ six-state\ protocol) \\
&\quad \lambda_1+\lambda_2 = e_1^y \ \ (six-state\ protocol).
\end{aligned} \tag{13}$$

In the asymptotic case, infinite decoy states can be applied, the corresponding parameters Y_1, P_1, e_1, Q_μ and E_μ can be estimated by $P_1 = \mu e^{-\mu}$, $\eta = 10^{\frac{-\alpha l}{10}} \eta_D$, $Y_1 = Y_0 + \eta$, $e_1 = \frac{0.5Y_0 + e_{Det}\eta}{Y_1}$, $Q_\mu = Y_0 + 1 - e^{-\eta\mu}$, $E_\mu = \frac{0.5Y_0 + e_{Det}(1-e^{-\eta\mu})}{Q_\mu}$, where μ is the mean photon number of the signal states, α is the loss coefficient in the quantum channel, l is the length of the fiber, η_D is the detection efficiency in Bob's side, Y_0 is the background rate in Bob's side, e_{Det} is the

probability that a photon hit the erroneous detector. By applying the practical QKD experimental parameters [20] ($\mu = 0.48$, $\alpha = 0.21$ dB/km, $e_{Det} = 0.033$, $Y_0 = 1.7 \times 10^{-6}$, $\eta_D = 0.045$, $f = 1.22$), 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. From the calculation results, we find that the maximal transmission distance can be improved from 142 km to 180 km, thus the advantage distillation technology can significantly improve the transmission distance by comparing with the no advantage distillation case. 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%, and the maximal transmission distance can be improved from 0 km to 175 km if the background error rate is $e_{Det} = 6.3\%$.

At the same time, we adopt the practical experimental parameters [20] 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. Compared with the four-state DD-QKD protocol, the six-state DD-QKD protocol has the advantage both in the transmission distance and the back ground error rate tolerance.

More interestingly, the advantage distillation technology can also be applied to the MDI-QKD protocol. By applying the experimental parameters in [21, 22] ($\alpha = 0.2$ dB/km, $e_{Det} = 0.015$, $Y_0 = 6.02 \times 10^{-6}$, $\eta_D = 0.145$, $f = 1.16$) with the mean photon number $\mu = 0.48$, we analyze security of the four-state and six-state MDI-QKD protocols with the advantage distillation technology. Different from the 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

$$\begin{aligned}
&max_b\ min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}\ \tfrac{1}{b} p_{succ} Q_{\mu\mu}[(\tfrac{Y_{11}P_{11}}{Q_{\mu\mu}})^b(1-(\tilde{\lambda_0}+\tilde{\lambda_1})H(\tfrac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}})-(\tilde{\lambda_2}+\tilde{\lambda_3})H(\tfrac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}}))-fh(\tilde{E_{\mu\mu}})]\\
&subject\ \ to\\
&\quad p_{succ} = E_{\mu\mu}^b + (1-E_{\mu\mu})^b\\
&\quad \tilde{E_{\mu\mu}} = \tfrac{E_{\mu\mu}^b}{E_{\mu\mu}^b+(1-E_{\mu\mu})^b}\\
&\quad \lambda_1+\lambda_3 = e_{11}^x\ \ (four-state\ or\ six-state\ protocol)\\
&\quad \lambda_2+\lambda_3 = e_{11}^z\ \ (four-state\ or\ six-state\ protocol)\\
&\quad \lambda_1+\lambda_2 = e_{11}^y\ \ (six-state\ protocol).
\end{aligned} \tag{14}$$

where P_{11} is the probability of both Alice and Bob's signal states emitting single-photon events, $Q_{\mu\mu}$ ($E_{\mu\mu}$) is the counting rate (error rate) of Alice and Bob's signal states, e_{11}^x, e_{11}^z and e_{11}^y are the single-photon error rate in the rectilinear basis, diagonal basis and the circular basis respectively. Based on this optimization calculation method, 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. From the calculation results, we find that the maximal transmission distance can be improved from 195 km to 273 km, and 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 if the background error rate is $e_{Det} = 4.6\%$. The analysis results demonstrate that the advantage distillation technology can significantly improve the transmission distance and error tolerance compared with the no advantage distillation case.

Similarly, we adopt the experimental parameters [21, 22] 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 if the background error rate is $e_{Det} = 5\%$. Compared with the four-state MDI-QKD protocol, the six-state MDI-QKD protocol has the advantage both in the transmission distance and the back ground error rate tolerance.

In the practical QKD systems, the generated secret key is finite, thus how to prove the security of the QKD protocol with the advantage distillation technology in finite-key scenarios is an important question. Since the advantage distillation technology only modify the classical post processing step, we can simply analyze the finite key length with the existed method. More precisely, based on the quantum asymptotic equipartition property [26, 27] and the leftover hash lemma [5, 28], the secret key rate with the DD-QKD protocol can be given by

$$\begin{aligned}
\widetilde{R}_{decoy} &\geq max_b\ min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}\ \tfrac{1}{b} q_{succ} Q_\mu[S_{min}^{\varepsilon_{min}}(A|E) - H(A|B)]\\
&\geq max_b\ min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}\ \tfrac{1}{b} q_{succ} Q_\mu[(\tfrac{Y_1P_1}{Q_\mu})^b(1-(\tilde{\lambda_0}+\tilde{\lambda_1})H(\tfrac{\tilde{\lambda_0}}{\tilde{\lambda_0}+\tilde{\lambda_1}})-(\tilde{\lambda_2}+\tilde{\lambda_3})H(\tfrac{\tilde{\lambda_2}}{\tilde{\lambda_2}+\tilde{\lambda_3}}))-fh(\tilde{E_\mu})-\Delta]
\end{aligned} \tag{15}$$

where

$$\Delta = 4\sqrt{\frac{b}{n}} log(2\sqrt{2^{H_{max}(A|E)}} + 1)\sqrt{log\frac{2}{\varepsilon_{min}^2}} + \frac{2b}{n} log\frac{1}{\varepsilon_{pa}}, \tag{16}$$

n is the secret key length before the advantage distillation step, $H_{max}(A|E)$ is the conditional max-entropy function [5], $H_{min}^{\varepsilon_{min}}(A|E) = max_{\sigma_{AE}\in\mathcal{B}^{\varepsilon_{min}}(\rho_{AE})} H_{min}(A|E)$, $\mathcal{B}^{\varepsilon_{min}}(\rho_{AE})$ is the set of sub-normalised states σ_{AE} with $D(\sigma_{AE}, \rho_{AE}) \leq \varepsilon_{min}$, and the final secret parameter can be given by $\varepsilon \equiv \varepsilon_{pa} + 2\varepsilon_{min}$. 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 should be analyzed by applying the law of large number.

IV. CONCLUSION AND DISCUSSION

How to improve the maximal transmission distance and the maximal background error rate are two important questions to analyze the security of the practical QKD system. By combining the advantage distillation technology with the decoy-state method, we prove that both of the maximal transmission distance and the maximal tolerable background error rate have been sharply improved with different DD-QKD and MDI-QKD protocols. More importantly, the advantage distillation technology does not need to change the quantum step of a practical QKD system, and it only needs to modify the classical post processing step, which 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.

Code availability

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

Data availability

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

Acknowledgements

The authors would like to thank Zhen-Qiang Yin for his helpful discussion. This work is supported by National Natural Science Foundation of China (Grant Nos. 61675235 and 11725524), Natural Science Foundation of Henan (Grant No. 202300410532), National Key Research and Development Program of China (Grant Nos. 2016YFA0302600, 2020YFA0309702), and China Postdoctoral Science Foundation (2019T120446, 2018M642281). *,†,‡To whom correspondence should be addressed, Email: lihow@ustc.edu.cn, cmz@njupt.edu.cn, qycai@wipm.ac.cn.

Author Contributions

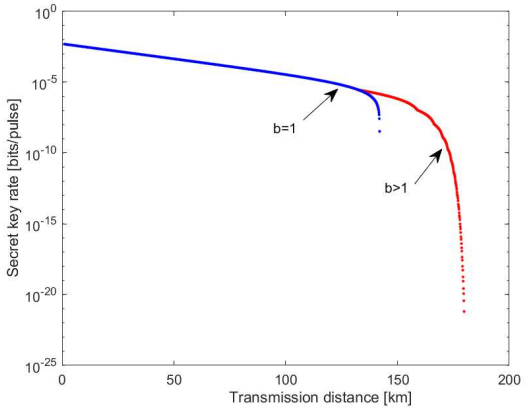
Hong-Wei Li and Qing-Yu Cai conceived the project. Hong-Wei Li, Chun-Mei Zhang and Mu-Sheng Jiang performed the calculation and analysis. Hong-Wei Li and Chun-Mei Zhang wrote the paper. *,†,‡To whom correspondence should be addressed, Email: lihow@ustc.edu.cn, cmz@njupt.edu.cn, qycai@wipm.ac.cn.

Competing Financial Interests

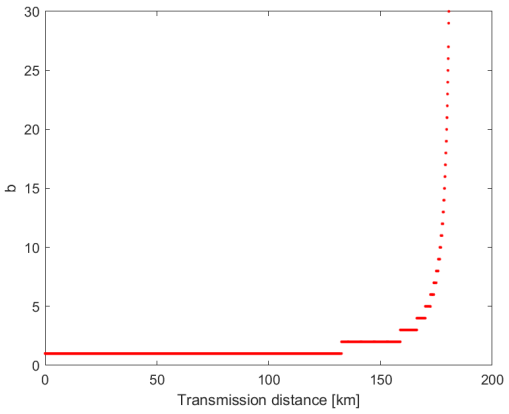
The authors declare no competing financial interests.

[1] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. New York: IEEE, 175-179 (1984).
[2] D. Bruss, Phys. Rev. Lett. 81, 3018 (1998).
[3] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).
[4] P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[5] R. Renner. International Journal of Quantum Information, 6(1), 1-127 (2008).
[6] U. Maurer, IEEE Trans. Inf. Theory 39, 733 (1993).
[7] B. Kraus, C. Branciard and R. Renner, Physical Review A 75(1), 2316 (2006).
[8] J. Bae and A. Acin, Physical Review A, 75(1), 2334 (2012).

[9] G. Murta, F. Rozpdek, J. Ribeiro, D. Elkouss, S. Wehner, Physical Review A, 101, 062321 (2020).
[10] E. Y.-Z. Tan, C. C.-W. Lim, R. Renner, Phys. Rev. Lett. 124, 020502 (2020).
[11] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory 49, 457 (2003).
[12] H. F. Chau, Phys. Rev. A 66, 060302 (2002).
[13] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A 51, 1863 (1995).
[14] N. Lutkenhaus and M. Jahma, New J. Phys. 4, 44 (2002).
[15] W. Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[16] X. B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[17] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[18] H. K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
[19] M. Lucamarini, Z. L. Yuan, J. F. Dynes and A. J. Shields, Nature 557.7705(2018).
[20] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004).
[21] F. Xu, H. Xu, and H. K. Lo, Phys. Rev. A 89(5), 3846-3855 (2014).
[22] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, et al., Nat. Phys. 3, 481 (2007).
[23] G. J. Fan-Yuan, W. Chen, F. Y. Lu, et al., Sciece China. Information Sciences, 63(8) (2020).
[24] S. K. Liao, W. Q. Cai, W. Y. Liu, et al., Nature 549, 43C47 (2017).
[25] Y. A. Chen, Q. Zhang, T. Y. Chen, et al., Nature 589, 214C219 (2021).
[26] R. Arnon-Friedman, PhD thesis, arXiv:1812.10922, (2018).
[27] M. Tomamichel, PhD thesis, arXiv:1203.2142, (2012).
[28] J. Radhakrishnan and A. Ta-Shma, Siam Journal on Discrete Mathematics, 13(1), 2-24 (2000).

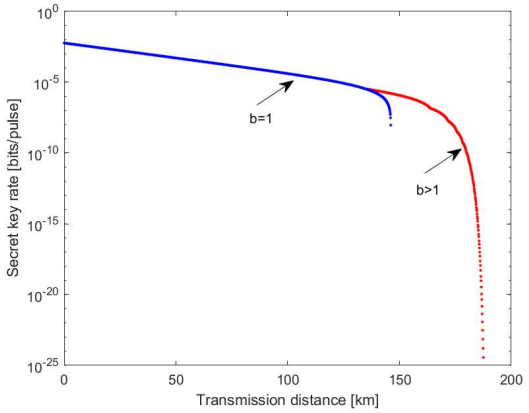


(a)The relationship between the transmission distance and the secret key rate, the blue line is the secret key rate without advantage distillation ($b = 1$), while the red line is the secret key rate with the advantage distillation technology ($b \geq 2$).

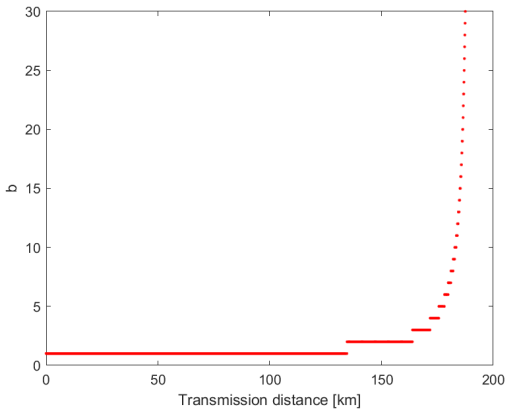


(b)The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b \geq 2$) can improve the secret key rate when the transmission distance is larger than 132 km.

FIG. 1: Results of the four-state DD-QKD protocol with and without advantage distillation.

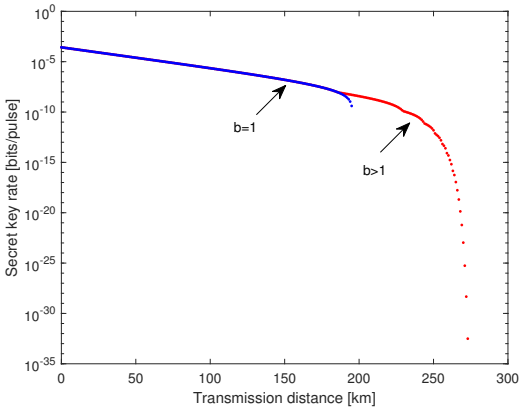


(a)The relationship between the transmission distance and the secret key rate, the blue line is the secret key rate without advantage distillation ($b = 1$), while the red line is the secret key rate with the advantage distillation technology ($b \geq 2$).

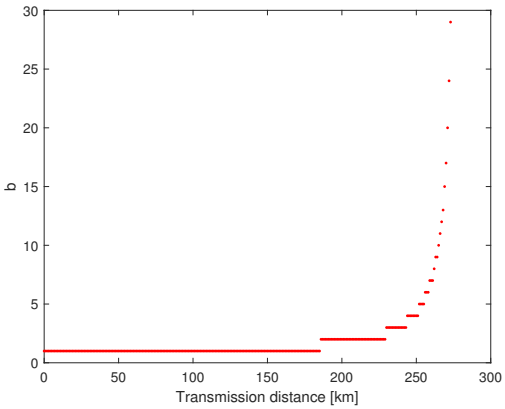


(b)The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b \geq 2$) can improve the secret key rate when the transmission distance is larger than 134 km.

FIG. 2: Results of six-state DD-QKD protocol with and without advantage distillation.

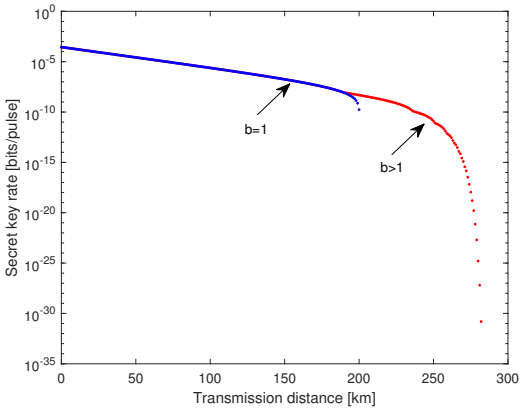


(a)The relationship between the transmission distance and the secret key rate, the blue line is the secret key rate without advantage distillation ($b = 1$), while the red line is the secret key rate with the advantage distillation technology ($b \geq 2$).

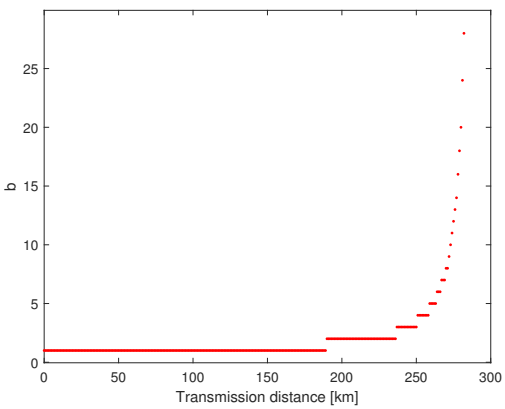


(b)The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b \geq 2$) can improve the secret key rate when the transmission distance is larger than 185 km.

FIG. 3: Results of four-state 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 ($b \geq 2$).



(b)The relationship between the transmission distance and the optimal b values, the advantage distillation technology ($b \geq 2$) can improve the secret key rate when the transmission distance is larger than 189 km.

FIG. 4: Results of six-state MDI-QKD protocol with and without advantage distillation.