Effect of weak randomness flaws on security evaluation of practical quantum key distribution with distinguishable decoy states

Yu Zhou(周雨)[1,2], Hong-Wei Li(李宏伟)[1,2,†], Chun Zhou(周淳)[1,2], Yang Wang(汪洋)[1,2], Yi-Fei Lu(陆宜飞)[1,2], Mu-Sheng Jiang(江木生)[1,2], Xiao-Xu Zhang(张晓旭)[1,2], and Wan-Su Bao(鲍皖苏)[1,2,‡]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou* 450001, *China*

[2] *Synergetic Innovation Centre of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 19 May 2022; revised manuscript received 20 July 2022; accepted manuscript online 5 August 2022)

Quantum key distribution provides an unconditional secure key sharing method in theory, but the imperfect factors of practical devices will bring security vulnerabilities. In this paper, we characterize the imperfections of the sender and analyze the possible attack strategies of Eve. Firstly, we present a quantized model for distinguishability of decoy states caused by intensity modulation. Besides, considering that Eve may control the preparation of states through hidden variables, we evaluate the security of preparation in practical quantum key distribution (QKD) scheme based on the weak-randomness model. Finally, we analyze the influence of the distinguishability of decoy state to secure key rate, for Eve may conduct the beam splitting attack and control the channel attenuation of different parts. Through the simulation, it can be seen that the secure key rate is sensitive to the distinguishability of decoy state and weak randomness, especially when Eve can control the channel attenuation.

Keywords: weak randomness, quantum key distribution, distinguishable decoy state

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/ac8730

1. Introduction

Quantum key distribution (QKD) provides a method of sharing secure key between Alice and Bob. Since the proposal of the first QKD protocol BB84,[1] QKD has attracted much interest and the unconditional security of which is guaranteed by the fundamental laws of quantum mechanics. The entanglement distillation and purification (EDP) technology,[2,3] and the von Neumann entropy theory[4] have provided a method of security analysis. However, the above security proves that all systems based devices are ideal, which is difficult to realize under the Eve's attack. QKD system with imperfect devices may not satisfy with the security assumptions, resulting in weak random problems and information disclosure. And the secure key rate obtained in theory will be overestimated compared with the actual value and some information may be extracted by Eve from the overestimated part from the information theory perspective. In the practical system, it is difficult to realize the ideal single photon source. Generally we use the weak coherent source (WCS) obtained by attenuating the laser. For the multiphoton part of the WCS may be exploited by the photon-number-splitting attack,[5] the mature decoy state protocol[6–9] has been proposed to estimate the proportion of the actual single photon part. In the decoy state protocol, we need to modulate the intensities of signal state and decoy state. The intensity modulation can be realized by using an external optical modulator located behind the laser diode[10,11] or directly modulating the injection current of the laser diode.[12,13] The external modulation requires an additional intensity modulator, which increases the system complexity, and the redundant intensity modulator will also bring additional security problems. Therefore, in this paper, we mainly discuss the security of internal intensity modulation by changing the injection current. The mainly problem of internal modulation method is that the states can be distinguished in time domain,[14] the attack strategies of Eve against this defect have also been discussed. However, the distinguishability of decoy states can be improved by setting the pre-bias current and adjusting the current excitation time,[15] which greatly improve the practicability of the internal modulation. Besides, the channel attenuation is also a non-negligible issue in the implementation of the protocol when we consider the distinguishability. Here, we assume that Eve can control the attenuation loss in quantum channel,[16] so that Eve can partially control the estimation of secure key rate by adjusting the attenuation of distinguishable states.

Recent years, the weak randomness of devices has been paid more and more attention. Several weak-randomness models have been proposed and improved.[17–19] In the practical BB84 protocol, due to the imperfection of preparation, the basis-choice and coding may be partially controlled by Eve, which bring weak-randomness issue. For example, if the generation of random numbers at the source is non ideal and the regular pattern of non ideal random numbers is mastered by Eve, the results of basis selection and coding in the prepara-

†Corresponding author. E-mail: lhw@qiclab.cn

‡Corresponding author. E-mail: bws@qiclab.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

tion process will be guessed by Eve with a greater probability. Eve can also introduce the weak randomness through attacking on non-ideal devices, such as Trojan-horse attack.[20,21] In order to prevent Trojan-horse attacks, Alice usually uses optical fiber loops, filters, isolators and other components to isolate external Trojan lights. However, the imperfect factors existing in these devices make them unable to completely isolate the external Trojan lights, which may lead to the leakage of some coding and basis selection information when the Trojan lights are reflected. Besides, the non ideality of the detectors may lead Eve to realize the weak control over the basis selection at Bob end, which affects the randomness of the overall basis selection, such as time shift attack,[22] wavelength attack,[23] spatial mismatch,[24] and probabilistic blinding attack.[25] The above attack takes advantage of the imperfection of the detectors, allowing Eve to guess the bases of both sides of the communication with a higher probability. By characterizing the weak randomness of bases selection and coding of protocol, the practical security of QKD is analyzed by the weak-randomness models. Combined with the existing weak-randomness models, this paper analyzes the practical security of QKD protocol. Firstly, the existing attack scheme to distinguishable decoy states is realized by implementing photon-number-splitting attack in specific time windows. Given that Eve controls the channel attenuation, she can influence the counting rate of photons to prevent the attack from being discovered by both sides of the communication.[14] However, the distinguishable probabilities of decoy states can be improved by setting the parameters of internal modulation.[15] Here, Eve's operation on the probability distinguishable part can not be completely hidden, we assume that Eve does not operate on the probably distinguishable states to ensure the protocol is executed. According to the probability distribution of states, we can divide the output of modulation and extract the completely distinguishable part. We mainly analyze Eve's attack on the indistinguishable states, in which the traces of operation will be found. And then we can estimate the influence of weak randomness when the states preparation is not perfect to the indistinguishable states.

In addition, the nonideality of decoy-state distinguishability and weak randomness we discussed is not limited to the decoy state BB84 protocol, but also can be analyzed for measurement-device-independent (MDI),[26,27] twin-field (TF),[28–30] and continuous-variable (CV)[31,32] protocols. Although the implementation methods may be different from BB84, considering the weak randomness caused by non ideal devices is critical for security analysis. There are also basis selection and coding in the preparation process of MDI, TF and CV protocols, in which we need to discuss the non ideality of specific systems and devices to evaluate the effect of weak randomness. Besides, the decoy state method is also used in MDI and TF protocols, which may also lead to the problem of distinguishing decoy states. The specific analysis of the above protocols is worthy of further study in the future. Here, we mainly analyze the weak randomness and decoy-state distinguishability of BB84 protocol in this paper. The specific arrangement of this paper is as follows. In Section 2, we give the characterization of distinguishing method and calculate the completely distinguishable probability. In Section 3, we analyse the finite-key security of the protocol based on the weak-randomness model, and then consider the effect that Eve may control the channel attenuation of different states. In Section 4, we simulate the secure key rate when Eve controls the attenuation under different distinguishable probability and weak-randomness parameters. Finally, we summarize the conclusions of the simulation and discuss the influence of the conclusions on the practical QKD in Section 5.

2. Distinguishing characterization of decoy states

In practical protocols, we choose the weak coherent source with internal modulation and decoy state method. Here, we will discuss the distinguishability of states and calculate the distinguishable probability. Huang *et al.* gave an attack scheme in which the decoy states can be probabilistically distinguished in time domain.[14] This method applies the inconsistency of the signal state and decoy state probability distribution in the time domain to distinguish states. Recently, Pranshu *et al.* adjusted the probability distribution of the decoy state in the time domain by changing the parameters of the internally modulated injection current.[15] The secondary oscillation peak of probability distribution in the time domain can be decreased by increasing the pre-bias current. And the delay between signal and decoy state can also be compensated by adjusting the time of injection current. However, the compensation of signal state cannot be perfect. Thus, we characterize the information leakage caused by the distinguishability of decoy state as follows.

As shown in the schematic diagram in Fig. 1, the imperfection of internal modulation makes the peak of the probability curve of the signal state in the time domain arriving earlier, for the current intensity of the modulated signal state is greater than that of the decoy state. Although there are improved methods for internal modulation, perfect modulation can not be guaranteed in practice. For convenience of explanation, we simplify the probability curves of signal state and decoy state in time domain in the figure above, and they are represented by f_{s} and f_{d}, respectively. According to the schematic diagram, we can analyze the distinguishability between signal states and decoy states. The previous attack scheme is realized by setting a time window in the area where the probability distribution does not coincide.[14] However, when Eve sets the

attacking windows in period $[d_0, s_1]$, although there are differences in the probability of response between signal states and decoy states, Eve may still misjudge the received states. In this case, Eve's PNS attack on the received states may be found by both sides of the communication through the decoy state protocol. When Eve attacks in period $[s_0, d_0]$, she can completely distinguish the signal state and the decoy state. That is, no information obtained in $[s_0, d_0]$ is safe and Eve can obtained the same states by implementing the PNS attack. Also, Eve's operation cannot be discovered at this time. So we assume that Eve only implements PNS attack in $[s_0, d_0]$ and does nothing to the received states in $[d_0, s_1]$. Based on the analysis above, we can calculate the probability that the signal state carries secure information as

$$p_{\mathrm{s}} = \int_{d_0}^{s_1} f_{\mathrm{s}}\,\mathrm{d}t, \tag{1}$$

where $\int_{s_0}^{s_1} f_{\mathrm{s}}\,\mathrm{d}t = \int_{d_0}^{d_1} f_{\mathrm{d}}\,\mathrm{d}t = 1$, and we assume that the indistinguishable probability of the output is $p = p_{\mathrm{s}}$. And the distinguishable probability can be expressed as $p_{\mathrm{c}} = \int_{s_0}^{d_0} f_{\mathrm{s}}\,\mathrm{d}t$. By characterizing the distinguishable probability of signal states and decoy states, we can divide the quantum states from the source into two parts, the indistinguishable part S_1 and the distinguishable part S_2.

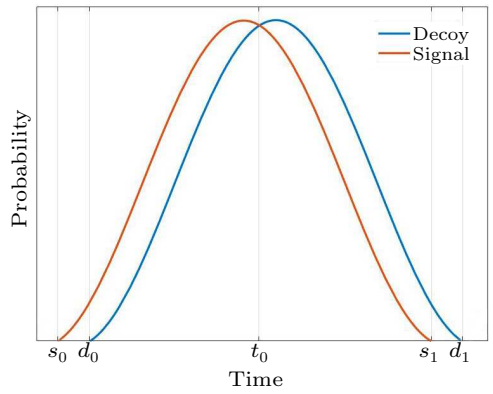


Fig. 1. Probability distribution diagram of the signal state and the decoy state in the time domain of Eve. Here we assume that Eve can obtain the probability distributions of the two states after the preparation of Alice.

3. Security analysis based on the weak-randomness model

In this section, we will analyze the security of the indistinguishable part S_1 based on the weak random model. For the sake of illustration, we adopt the weak decoy state protocol to simplify the discussion of distinguishability. Suppose Alice performs internal modulation on the WCS, using the signal states and the decoy states with the average number of photons of μ and ν, respectively. Firstly, we briefly describe the weak-randomness model.[17] After the intensity modulation, Alice requires two random bits for each quantum state in preparation, and we assume x_0 for bit coding and x_1 for basis-choice. After Bob receives a quantum state, he needs one random bit y to select the measurement bases and the final key is distilled only when Alice and Bob choose the same basis $x_1 = y$. In practical QKD system, since the imperfections of devices, x_0 (x_1) may be weakly controlled by Eve with hidden variables λ_1 and λ_2 as follows:

$$p(x_0) = \sum\nolimits_i p_{\lambda_0=i} p(x_0|\lambda_0 = i), \tag{2}$$

$$p(x_1) = \sum\nolimits_j p_{\lambda_1=j} p(x_1|\lambda_1 = j). \tag{3}$$

Here two hidden variables should satisfy $\sum_i p_{\lambda_0=i} = \sum_j p_{\lambda_0=j} = 1$. Since the λ_1 and λ_2 can be used to influence the preparation, we cannot guarantee $p(x_0|\lambda_0 = i) = p(x_1|\lambda_1 = j) = 1/2$. To quantify the deviations from hidden variables, we introduce parameters ε_0 and ε_1 as follows:

$$|p(x_0|\lambda_0 = i) - \frac{1}{2}| \le \varepsilon_0, \tag{4}$$

$$|p(x_1|\lambda_1 = j) - \frac{1}{2}| \le \varepsilon_1, \tag{5}$$

where $0 \le \varepsilon_0, \varepsilon_1 \le 1/2$.

we can calculate the secure key rate[19]

$$R \ge -Q_\mu f(E_\mu) H(E_\mu) + Q_{\mu,1}[1 - H(e_{1,\mathrm{phase}})], \tag{6}$$

$$Q_\mu = Y_0 + 1 - \mathrm{e}^{-\mu\eta}, \tag{7}$$

$$E_\mu = \frac{e_0 Y_0 + e_{\mathrm{det}}(1 - \mathrm{e}^{-\mu\eta})}{Q_\mu}, \tag{8}$$

where $\eta = \eta_{\mathrm{Bob}} 10^{-\alpha/10}$ is the total transmittance and α is the channel loss. Q_μ and E_μ are the total gain and bit error of the signal states, respectively. $Q_{\mu,1}$ and $e_{1,\mathrm{phase}}$ are the yield and the phase error of the single photon pulse of the signal state, respectively. Considering the finite key may lead to statistical fluctuation, we estimate the fluctuation of the count rate and bit error rate under the finite key as follows. Let N and $p_\mu = p_\nu$ are the total number of pulses emitted by source and the probability of selecting intensity μ or ν. We assume that the bases selection is balanced. According to the finite-key effect,[33,34] we limit the range of statistical fluctuations using the Azuma's inequality[35]

$$N_\mu^* = \frac{1}{2} N p_\mu Q_\mu, \tag{9}$$

$$|N_\mu^* - N_\mu| \le \delta_{\mathrm{A}}(N_\mu, \varepsilon_{\mathrm{A}}), \tag{10}$$

with probability being at least $1 - 2\varepsilon_{\mathrm{A}}$, where $\delta_{\mathrm{A}}(x, y) = \sqrt{2}x(\ln(1/y))$, N_μ^* and N_μ are the expected value and the actual value of the detected states with intensity μ. Then we can calculate the fluctuation range of the counting rate

$$\frac{2(N_\mu^* - \delta_{\mathrm{A}}(N_\mu, \varepsilon_{\mathrm{A}}))}{N p_\mu} \le Q_\mu \le \frac{2(N_\mu^* + \delta_{\mathrm{A}}(N_\mu, \varepsilon_{\mathrm{A}}))}{N p_\mu}, \tag{11}$$

and we express the upper and lower bounds of Q_μ as Q_μ^+ and Q_μ^- and the bit error of the signal states can be expressed as

$$E_\mu^+ = \frac{e_0 Y_0 + e_{\mathrm{det}}(1 - \mathrm{e}^{-\mu\eta})}{Q_\mu^-},$$

$$E_\mu^- = \frac{e_0 Y_0 + e_{\rm det}(1-{\rm e}^{-\mu\eta})}{Q_\mu^+}. \tag{12}$$

Similarly, the upper and lower bounds of counting rate Q_ν and E_ν can be obtained. The gain and quantum bit error rate of a single photon can be expressed as[8]

$$Y_1^{\rm L} \geq \frac{\mu}{\mu\nu-\nu^2} Q_\nu^- {\rm e}^\nu - Q_\mu^+ {\rm e}^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2} Y_0, \tag{13}$$

$$Q_{\mu,1} \geq Q_{\mu,1}^{\rm L} = \frac{\mu^2 {\rm e}^{-\mu}}{\mu\nu-\nu^2}$$

$$\times \left(Q_\nu^- {\rm e}^\nu - Q_\mu^+ {\rm e}^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2} Y_0 \right), \tag{14}$$

$$e_{1,{\rm bit}} \leq e_{1,{\rm bit}}^{\rm U} = \frac{E_\nu^+ Q_\nu^+ {\rm e}^\nu - e_0 Y_0}{\nu Y_1^{\rm L}}, \tag{15}$$

where Y_0 is the background counting rate, $e_0 = 0.5$ for dark counts occur randomly.

For $\lambda_0 = i$ and $\lambda_1 = j$, the final quantum state under the Pauli quantum channel can be written as

$$\begin{aligned} \rho_{\rm AB}^{i,j} = & \sum\nolimits_{u,v} q_{u,v} \Big\{ p(x_1=0|\lambda_1=j) \boldsymbol{I}\otimes\boldsymbol{X}^u\boldsymbol{Z}^v |\varphi\rangle\langle\varphi|_{\lambda_0=i} \boldsymbol{Z}^v\boldsymbol{X}^u\otimes\boldsymbol{I} \Big\} \\ & + \Big\{ p(x_1=1|\lambda_1=j) \boldsymbol{I}\otimes\boldsymbol{H}\boldsymbol{X}^u\boldsymbol{Z}^v\boldsymbol{H} |\varphi\rangle\langle\varphi|_{\lambda_0=i} \boldsymbol{H}\boldsymbol{Z}^v\boldsymbol{X}^u\boldsymbol{H}\otimes\boldsymbol{I} \Big\}, \end{aligned} \tag{16}$$

with

$$\begin{aligned} |\varphi\rangle_{\lambda_0=i} = & \sqrt{p(x_0=0|\lambda_0=i)}|00\rangle \\ & + \sqrt{p(x_0=1|\lambda_0=i)}|11\rangle, \end{aligned} \tag{17}$$

where $u,v \in \{0,1\}$, $\sum_{u,v} q_{u,v} = 1$, $q_{u,v}$ is the probability that Eve performs different operators on the quantum state $|\varphi\rangle_{\lambda_0=i}$. $\boldsymbol{I}$ is the unity matrix, $\boldsymbol{X}$ and $\boldsymbol{Z}$ are Pauli matrices, $\boldsymbol{H}$ is the Hadmard matrices. We can estimate the phase error based on the bit error above model,[17] and Sun *et al.* have improved this method as follows:[19]

$$e_{\rm phase}^{i,j} \leq \frac{1+2\varepsilon_1}{1-2\varepsilon_1} e_{\rm bit}^{i,j} + \frac{1}{2} - \sqrt{\frac{1}{4}-\varepsilon_0^2}. \tag{18}$$

As partial states are distinguishable, the optimal attack strategy for Eve is that she only attacks the states of the indistinguishable part S_1 and does nothing to other part. In the worst case, total bit errors come from S_1 while both sides of the communication can only detect the global error rate. The actual bit error of the S_1 is

$$e_{1,{\rm bit}}^{S_1,i,j} = \frac{e_{1,{\rm bit}}^{i,j}}{p} \leq \frac{e_{1,{\rm bit}}^{U,i,j}}{p}, \tag{19}$$

where p is the indistinguishable probability. Combined with the weak-randomness model and Eq. (14), we can calculate the phase error of S_1 as

$$e_{1,{\rm phase}}^{S_1,i,j} \leq \frac{1+2\varepsilon_1}{1-2\varepsilon_1} e_{1,{\rm bit}}^{S_1,i,j} + \frac{1}{2} - \sqrt{\frac{1}{4}-\varepsilon_0^2}. \tag{20}$$

Combined with Eq. (6), the final secret key rate can be given by[19]

$$\begin{aligned} R \geq & \sum\nolimits_{i,j} p_{\lambda_0=i} p_{\lambda_1=j} R^{i,j} \\ \geq & \sum\nolimits_{i,j} p_{\lambda_0=i} p_{\lambda_1=j} \Big(-Q_\mu^{i,j} f\left(E_\mu^{i,j}\right) H\left(E_\mu^{i,j}\right) \\ & + Q_{\mu,1}^{S_1,i,j} \left(1 - H\left(e_{1,{\rm phase}}^{S_1,i,j}\right)\right) \Big) \\ \geq & -Q_\mu f(E_\mu) H(E_\mu) + p Q_{\mu,1} \left(1 - H\left(e_{1,{\rm phase}}^{S_1}\right)\right), \end{aligned} \tag{21}$$

where $R^{i,j}$ is the secure key rate when $\lambda_0 = i$ and $\lambda_1 = j$. $Q_\mu^{i,j}$ and $E_\mu^{i,j}$ are the total gain and bit error of the signal states, respectively. And $Q_{\mu,1}^{S_1,i,j}$ and $e_{1,{\rm phase}}^{S_1,i,j}$ are the yield and phase error of single photon pulse of the signal state of S_1, respectively.

Then, we assume that Eve can control channel attenuation with ultra-low loss or even lossless fibers. In the practical QKD system, Eve can distinguish the signal states from S_2 and control the decay of transmission states through low loss optical fibers. Therefore, the best strategy[16] for Eve is to use low-loss optical fibers for the distinguishable states of S_2 and allow the states of S_1 to be transmitted over normal channels. In this case, we can make further amendments to

$$\begin{aligned} R \geq & p_1 Q_{\mu,1}^L \left[1 - H\left(\frac{1+2\varepsilon_1}{1-2\varepsilon_1} \frac{e_{1,{\rm bit}}^U}{p_1} + \frac{1}{2} - \sqrt{\frac{1}{4}-\varepsilon_0^2} \right) \right] \\ & - Q_\mu^+ f(E_\mu^+) H(E_\mu^+), \end{aligned} \tag{22}$$

$$p_1 = \frac{p(1-q_1)}{p(1-q_1)+p_{\rm c}(1-q_2)}, \tag{23}$$

where q_1 and q_2 are the probability loss of S_1 and the distinguishable part of S_2, respectively. The transmission loss of ordinary optical fiber is $\alpha_1 = 0.2$ dB/km, while the ultra-low loss optical fiber with a transmission loss of $\alpha_2 = 0.14$ dB/km[36] can be used by Eve. If Eve uses ultra-low loss fiber transmission for the distinguishable part of S_2 and ordinary optical fiber for S_1, we can characterize q_1 and q_2 by

$$1-q_1 = 10^{-\alpha_1 l}, \quad 1-q_2 = 10^{-\alpha_2 l}, \tag{24}$$

where l is the transmission distance of the optical fiber.

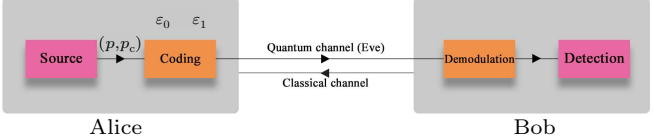


Fig. 2. BB84 system diagram. p and $p_{\rm c}$ are the indistinguishable probability and the distinguishable probability of signal states. The ε_0 and ε_1 are the deviation parameters of coding and basis-choice when the preparation is weakly controled by Eve.

4. Simulation and discussion

In this section, we simulate the effect of distinguishing states and the weak randomness on secure key rate. Alice and Bob choose the signal and decoy states with expected photon number μ and ν. Since Eve can partially distinguish the states, she can transfer the distinguishable part with the ultra-low loss optical fiber or even lossless fibers.

The experimental parameters are shown in the Table 1.

Table 1. Simulation parameters.

Variable	Parameter	Simulation value
N	number of pulses emitted from the source	10^8
μ	expected photon numbers of signal states	0.48
ν	expected photon numbers of decoy states	0.05
α_1	fiber loss coefficient	0.2
α_2	ultra-low loss fiber (lossless fiber) loss coefficient	0.14(0)
Y_0	the background rate	10^{-6}
η_{Bob}	detection efficiency of Bob	0.0045
e_{det}	the response probability of erroneous detector	3.3%
f	efficiency of error correction	1.22

After the expected photon numbers of decoy states and signal states are set, we can calculate the normalized probability distribution of signal states and decoy states in time domain by pretreatment. For Eve, the optimal attack opportunity is when the states just enter the channel. Moreover, the distribution can be adjusted by setting the parameters of internal modulation.[15] By analyzing the adjusted probability distributions in time domain, we can get the indistinguishable probability p and the distinguishable probability p_c of the source. Considering that Eve can control channel attenuation and there are statistical fluctuations caused by finite-key effect, we simulate the effect on the secure key rate. Here, we firstly simulate the effect of decoy state methods and statistical fluctuation on practical QKD protocol. As shown in Fig. 3, we can see that the finite-key effect has a significant impact on the secure key rate, especially in long-distance transmission. Simulation results show that the smaller the size of the data sent, the greater the impact of statistical fluctuations on the secure key rate. When the size of the data gradually increases, the secure key rate will eventually tend to a rate of wireless data scale. Besides, we also simulate secure key rate using different kinds of decoy methods when the data are limited in Fig. 4. In our simulation, the statistical fluctuations caused by finite-key will enable the one decoy protocol to perform better than the vacuum + weak protocol when data size is small, although it will flip when the data size is large.[8] The same conclusion can also be found in Ref. [37]. In summary, limited data size is worth considering in the practical protocols, for it has a significant impact on the security of the key. In this paper, we mainly adopt the one decoy protocol with $N = 10^8$ in the later simulation to explore the effect of weak randomness and distinguishability on practical security.

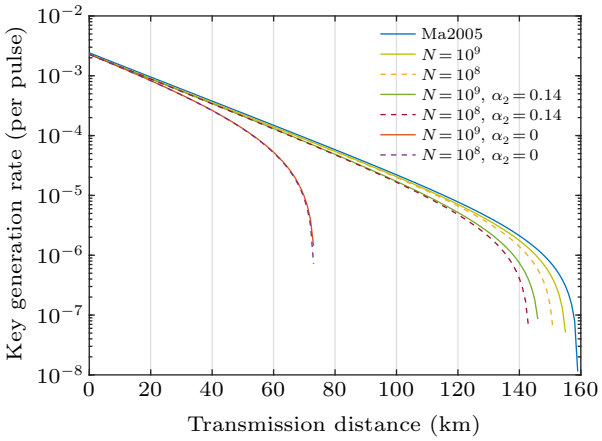


Fig. 3. The effect of statistical fluctuations caused by finite-key effect on the practical QKD protocol with the indistinguishable probability $p = 0.98$. The solid line indicates that $N = 10^9$, while the dotted line indicates that $N = 10^8$.

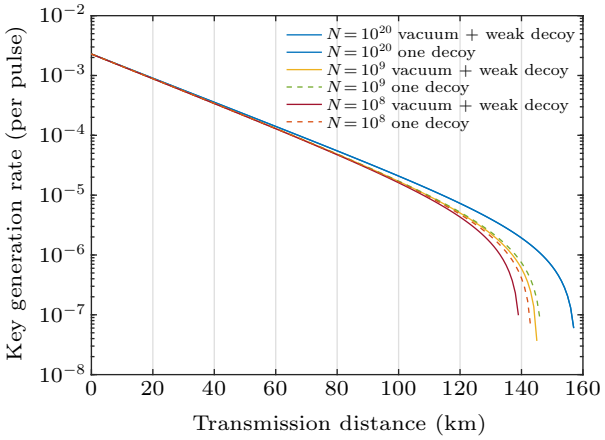


Fig. 4. Effect of statistical fluctuations on different decoy schemes with the indistinguishable probability $p = 0.98$.

We also simulate the influence of distinguishability on the key rate as follows, as shown in Fig. 5, the distinguishability will lead to a sharp decline in the secure key rate especially when we consider the Eve's control of attenuation. The distinguishable information will be exploited by Eve, and she wills the control channel attenuation to affect the estimation of gain and quantum bit error rate. Here, we give the secure key rate under different indistinguishable probabilities and different attenuation coefficients. We can see that the longer the transmission distance, the greater the impact of distinguishability. When the indistinguishability probability is less than 0.9, the protocol can hardly provide an effective secure key. Besides, we compare the conditions of normal attenuation, low loss fiber attenuation and even no attenuation for the completely distinguishable part. Eve control the attenuation has a significant impact on the secure key rate, especially when Eve's ability to control attenuation is not limited. Because with the increase of transmission distance, if the distinguishable part

is transmitted without attenuation and the other part is attenuated by the normal channel, the proportion of the part that can actually extract the key will be compressed and the quantum bit error rate will be amplified. Therefore, if the system using internal modulation to realize decoy state protocol, it is necessary to adjust the parameters of current injection to ensure the probability distribution of signal states and decoy states in the time domain is within an acceptable range. Before the implementation of the protocol, the probability distribution curves of signal state and decoy state should be adjusted to coincide as much as possible.

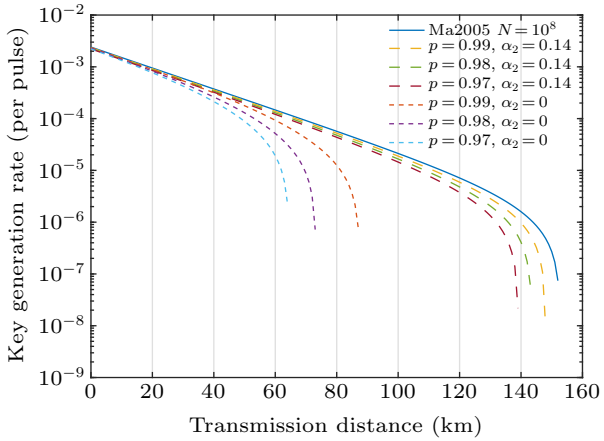


Fig. 5. Based weak-decoy-state protocol,[8] we simulate the effect of different indistinguishable probability p to key rate. The blue curve indicates the secure key rate when there is no distinguishability $p=1$. The solid lines represent the secure key rate when Eve does not change the channel attenuation, the dashed line and the dotted line represent that Eve adopts low loss fiber attenuation and even no attenuation to completely distinguishable part.

In the pratical QKD system, the imperfect devices in the states preparation process also can not be ignored. Here we introduce the weak-randomness model to characterize Eve's information acquisition of preparation. Eve has weak control over the states preparation process through implicit variables, but Eve can not control it with certainty. Therefore, we believe that Eve cannot amplify this weak randomness through channel attenuation. Here we characterize the weak control by introducing two parameters ε_0 and ε_1 for coding and basis-choice. We simulate the protocol with different weak-randomness parameters and the results are as follows.

As shown in the Fig. 6, we can infer that Eve's control of basis-choice has a greater impact than the coding on the secure key rate, for the dotted line always has a longer transmission distance than the dashed line. This conclusion can also be obtained by analyzing the estimation method of phase error (see Eq. (14)). In addition, we can see that with the increase of weak-randomness parameters, its impact on the secure key rate surge and the purple dotdash line has a sharp decline when $\varepsilon_0=\varepsilon_1=0.2$. Figure 7 shows the ratio θ of secure key rate before and after considering Eve's weak control. The deviation parameters caused by weak randomness mainly affect the phase error rate. From the figure, we can see that the ratios under different weak-randomness deviation parameters have a significant gap from the beginning, and the curves change gently in the short distance. It can be seen from Eq. (14) that the initial bit error rate is directly affected by ε_0 and ε_1, and it will increase rapidly over the long distance. Therefore, we need to estimate the weak-randomness parameters in the process of states preparation by measuring the imperfection of devices of the QKD system before carrying out protocols.

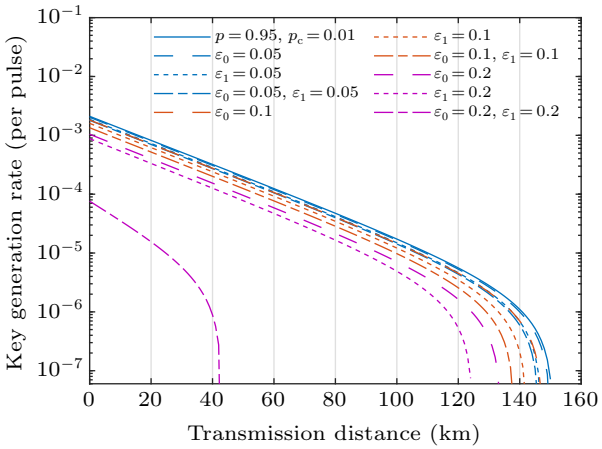


Fig. 6. The secure key rate under different parameters. The blue, orange and purple lines represent the different deviation parameters. And the dashed line, dotted line and dotdash line consider the weak-randomness parameter ε_0, ε_1, and $\varepsilon_0=\varepsilon_1$, respectively.

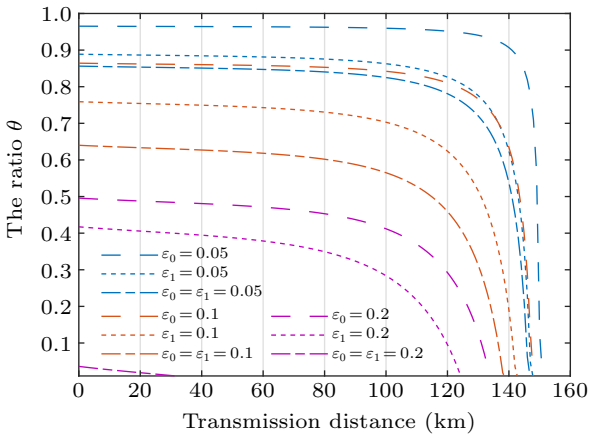


Fig. 7. The ratios of secure key rate before and after considering weak randomness. The dashed line, dotted line and dotdash line correspond to the curve in Fig. 6.

Finally, we simulate the relationship between the indistinguishability and weak randomness. As shown in the Fig. 8, both factors affect the secure key rate. When the two factors are considered together, we can see that the effect of weak randomness on the secure key rate increases with the decrease of indistinguishability probability. Because the increase of weak-randomness parameters will lead to the raise of quantum bit error rate, the reduction of indistinguishability probability will decrease the yield of single photon and enable Eve to have greater ability to use attenuation to influence the above defects. The above conclusion can be obtained by analyzing the

parameters in Eq. (18). For the parameter p_1 will increase with the rise of the indistinguishable probability p and the phase error rate is positively correlated with the weak-randomness parameters.

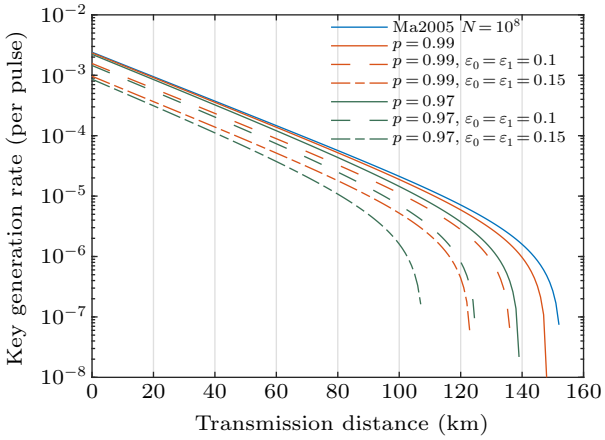


Fig. 8. Secure key rate under different parameters. The orange and green lines represent the different indistinguishable probabilities and completely distinguishable probabilities. The dashed line, dotted line and dotdash line are the secure key rates under different weak-randomness parameters.

5. Conclusion

We consider the imperfection of the source and analysis the practical security of the BB84 protocol. We propose the characterization method of indistinguishable probability of internal intensity modulation. Then, considering that Eve may have the ability to completely distinguish partial decoy states, we analyse the impact on secure key rate when Eve can control the channel attenuation to different states. For the indistinguishable states, Eve's weak control over the preparation is taken into account. Based on the weak random model, we further discuss the practical security of the sender. The simulation results show that the above factors have significant impacts on the practical security, especially when multiple factors are considered. Our work give a comprehensive analysis to the practical QKD protocol and the simulation results under different parameters can provide a reference for the security key rate. It is significant for sides of communication to analyse the imperfections of the practical devices and measure the specific parameters before implementing QKD protocol. In conclusion, we derive an analytical model to the practical QKD protocol considering the distinguishability of states and weak-randomness. It provides a theoretical reference for secure analysis of practical protocols.

Acknowledgments

Project supported by the National Key Research and Development Program of China (Grant No. 2020YFA0309702), NSAF (Grant No. U2130205), the National Natural Science Foundation of China (Grant Nos. 62101597, 61605248, and 61505261), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan (Grant Nos. 202300410534 and 202300410532), and the Anhui Initiative in Quantum Information Technologies.

References

[1] Bennett C H and Brassard G 1984 *Theor. Comput. Sci.* **560** 7
[2] Lo H K and Chau H F 1999 *Science* **283** 2050
[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[4] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 012332
[5] Brassard G, Lutkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[6] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[7] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[8] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[9] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[10] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503
[11] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 *Opt. Express* **16** 18790
[12] Liao S K, Yong H L, Liu C, *et al.* 2017 *Nat. Photonics* **11** 509
[13] Yin H L, Fu Y, Liu H, Tang Q J, Wang J, You L X, Zhang W J, Chen S J, Wang Z, Zhang Q, Chen T Y, Chen Z B and Pan J W 2017 *Phys. Rev. A* **95** 032334
[14] Huang A, Sun S H, Liu Z and Makarov V 2018 *Phys. Rev. A* **98** 012330
[15] Maan P 2022 *Phys. Rev. B* **128** 178
[16] Li H W, Xu Z M and Cai Q Y 2018 *Phys. Rev. A* **98** 062325
[17] Li H W, Yin Z Q, Wang S, Qian Y J, Chen W, Guo G C and Han Z F 2015 *Sci. Rep.* **5** 16200
[18] Li H W, Xu Z M, Yin Z Q and Cai Q Y 2020 *Phys. Rev. A* **102** 022605
[19] Sun S H, Tian Z Y, Zhao M S and Ma Y 2020 *Sci. Rep.* **10** 18145
[20] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
[21] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 *New J. Phys.* **16** 123030
[22] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
[23] Li H W, Wang S, Huang J Z, Chen W, Yin Z Q, Li F Y, Zhou Z, Liu D, Zhang Y, Guo G C, Bao W S and Han Z F 2011 *Phys. Rev. A* **84** 062308
[24] Sajeed S, Chaiwongkhot P, Bourgoin J P, Jennewein T, Lutkenhaus N and Makarov V 2015 *Phys. Rev. A* **91** 062301
[25] Qian Y J, Li H W, He D Y, Yin Z Q, Zhang C M, Chen W, Wang S and Han Z F 2015 *Chin. Phys. B* **24** 090305
[26] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[27] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Y, Yin H L and Chen Z B 2022 *PRX Quantum* **3** 020315
[28] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[29] Yin H L and Chen Z B 2019 *Sci. Rep.* **9** 14918
[30] Yin H L and Chen Z B 2019 *Sci. Rep.* **9** 17113
[31] Tamura Y, Sakuma H, Morita K, Suzuki M, Yamamoto Y, Shimada K, Honma Y, Sohma K, Fujii T and Hasegawa T 2018 *Journal of Lightwave Technology* **36** 44
[32] Liu W B, Li C L, Xie Y M, Weng C X, Gu J, Cao X Y, Lu Y S, Li B H, Yin H L and Chen Z B 2021 *PRX Quantum* **2** 040334
[33] Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2016 *Phys. Rev. A* **94** 032335
[34] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 *Phys. Rev. A* **89** 022307
[35] Azuma K 1967 *Tohoku Math. J.* **19** 357
[36] Hasegawa T, Tamura Y, Sakuma H, Kawaguchi Y, Yamamoto Y and Koyano Y 2018 *SEI Tech. Rev.* **86** 18
[37] Rusca D, Boaron A, Grunenfelder F, Martin A and Zbinden H 2018 *Appl. Phys. Lett.* **112** 171104