Chin. Phys. B Vol. 29, No. 3 (2020) 030303

Reference-frame-independent quantum key distribution with an untrusted source[*]

Jia-Ji Li(李家骥)[1,2], Yang Wang(汪洋)[1,2], Hong-Wei Li(李宏伟)[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 Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 11 October 2019; revised manuscript received 23 December 2019; accepted manuscript online 9 January 2020)

Reference frame independent quantum key distribution (RFI-QKD) allows two legitimate parties to share the common secret keys with the drift of reference frames. In order to reduce the actual requirements of RFI-QKD protocol on light source and make it more suitable for practical applications, this paper gives a specific description of RFI-QKD protocol with an untrusted source and analyzes the practical security of this protocol based on the two-way “plug and play” structure commonly used in practical systems. In addition, we also investigate the performance of RFI-QKD with an untrusted source considering statistical fluctuations based on Chernoff bound. Using simulations, we compare the secret key rate of RFI-QKD with an untrusted source to RFI-QKD with trusted source. The results show that the performance of RFI-QKD with an untrusted source is similar to that of RFI-QKD with trusted source, and the finite data size clearly effects the performance of our protocol.

Keywords: quantum key distribution, reference frame independent, finite key, untrusted source

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/ab695d

1. Introduction

With the development of science and technology, cryptography as the core of communication security has been widely concerned, and the key is the crucial point of cryptography to protect communication security. Quantum key distribution (QKD) based on the principle of quantum physics theoretically enables both legitimate parties to share the common secret keys securely. Since the BB84 protocol was proposed in 1984,[1] scholars worldwide have carried out a lot of research and experiments on QKD.[2–14] At present, with the deepening of QKD theory research, researchers gradually focus on the satellite-earth QKD,[15,16] the establishment of quantum secure communication network,[17,18] and the chip-based QKD equipment.[19,20] However, it is difficult to calibrate the reference frame in these three QKD application scenarios. To solve this problem, Laing *et al.* put forward the reference frame independent quantum key distribution (RFI-QKD) protocol in 2010.[21] Through this protocol, both legal communication parties can transmit the key securely without reference frame calibration or in the presence of deviations in the reference frame. This provides new theoretical support for the practical development of the earth-to-satellite, network and chip-based QKD. Due to the advantages of RFI-QKD protocol in practical applications, it has attracted extensive attention of researchers worldwide.[22–31]

Although RFI-QKD protocol can theoretically enable the sender Alice and receiver Bob to realize the transmission of secret key in the case of reference frame deviation, an important prerequisite for the successful implementation of this protocol is that the light source is reliable. However, the light source used in the practical QKD system inevitably has some security risks. The plug and play structure, which has been widely used in current commercial systems,[32] can automatically compensate for the phase and polarization drift in the transmission process, thus making the system more stable. However, the safety of the light source has been a concern. In the plug and play structure, the light source is set at the Bob end and the bright pulses are generated by Bob and sent to Alice. After encoded by Alice, the pulses will be sent back to Bob. Before the pulses arriving Alice’s equipment, they are completely exposed to Eve. At this time, Eve can perform arbitrary operations on the pulses. In the worst case, Eve completely replaced Bob’s pulses sent to Alice. Obviously, the security of the QKD protocol is threatened if the light source is not trusted.[33]

2. Preliminary

For the untrustworthy situation of the light source, there are two solutions: active solution[34] and passive solution.[35] The main difference is that the active method uses the optical switch to randomly select the pulse to enter the light intensity monitor or the encoder, while the passive method uses the beam splitter. Instead of the optical switch, the beam splitter splits the light pulse into two parts, one into the light intensity monitor and the other into the encoder and sent to Bob. The schematic diagram is shown in Figs. 1 and 2.

---

[*] Project supported by the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grant Nos. 61505261, 61675235, 61605248, and 11304397).

[†] Corresponding author. E-mail: bws@qiclab.cn

http://iopscience.iop.org/cpb http://cpb.iphy.ac.cn

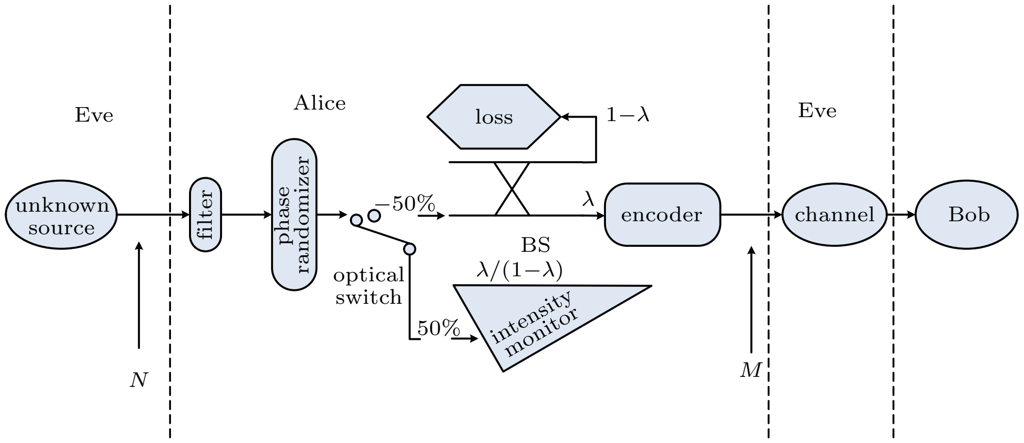

Fig. 1. Schematic diagram of the QKD scheme with an active estimate on an untrusted source.

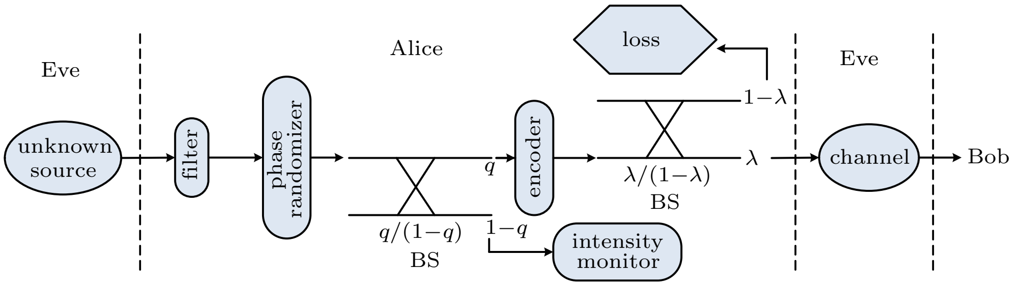

Fig. 2. Schematic diagram of the QKD scheme with a passive estimate on an untrusted source.

In the QKD system, there are many difficulties in using the active device in Fig. 1. The reasons are as follows: (1) The optical switch in Fig. 1 requires a synchronous clock for control, which is difficult to implement in a high-speed QKD system. (2) Optical switch selection requires a high-speed quantum random number generator, which is currently difficult to implement. Secondly, due to the random selection using the optical switch, only half of the pulses generated by the light source can enter the encoder and be encoded by Alice and sent to Bob, which affects the efficiency and performance of the entire system. For the above reasons, in the RFI-QKD with untrusted light source, we choose the passive approach scheme shown in Fig. 2. The detailed description of our protocol is presented in the following.

Step 1 Quantum state preparation and distribution: Bob produces a bright light pulse and sends it to Alice. To make sure that only the pulses of the desired mode can arrive the Alice end, the bright pulse first passes through a filter to remove the remaining modes of light. After the phase randomization process, it is divided into two parts by the beam splitter, one part enters the light intensity monitor to obtain the photon number information of input pulses, and the other part arrive the Alice end to get encoded. Alice randomly selected a basis from the three sets of bases $\{X,Y,Z\}$, and one of the bit information $\{0,1\}$, and the output light intensity $g \in \{\mu, v, 0\}$ is determined by setting the internal transmittance $\lambda \in \{\lambda_\mu, \lambda_v, \lambda_0\}$, and then the selected bit is encoded and loaded on the optical pulse with the selected light intensity and the base vector. After that, pulses will be sent to Bob.

Step 2 Quantum state measurement: Bob randomly selects a set of base from the three sets of bases $\{X,Y,Z\}$ to measure the received pulses.

Step 3 Sifting: Alice and Bob announce their choice of base and light intensity through the classic channel, and record the measurements under different bases and light intensity selections.

Step 4 Parameter estimation: The raw key is obtained from the untagged pulses when both Alice and Bob selecting Z basis. And the data of X basis and Y basis is used to estimate Eve's information. Alice and Bob use the decoy state method to estimate the gain and quantum bit error rate of single photon pulses of untagged pulses in different base selections.

Step 5 Post processing: Alice and Bob perform error correction to ensure the consistency of the keys of both parties, and finally obtain the security key by privacy amplification.

In this paper, pulses are divided into tagged pulses and untagged pulses depending on the number of photons contained in the input pulse. The pulse with photon number $n \in [(1-\delta)N, (1+\delta)N]$ is defined as untagged pulse and the pulse with photon number $n < (1-\delta)N$ or $n > (1+\delta)N$ is defined as tagged pulse. Here N is the average number of photons of the input light pulse and δ is a positive real number with a smaller value chosen by Alice and Bob. In this paper, we focus on the untagged pulse and only the untagged pulse is used to generate security key.

Since in the QKD system, Alice and Bob are not capable of quantum non-demolition measurement to obtain photon number information of input light pulses. Therefore, Alice and Bob cannot directly obtain the gain Q and quantum bit error rate E of the untagged pulse in the experiment. They can only measure the overall gain Q_e and the overall quantum bit error rate E_e of all received pulses. In the RFI-QKD protocol with an untrusted source, we use beam splitters and intensity monitors to obtain information about the distribution of photons in pulses from untrusted sources. Assume that the number of pulses sent by the untrusted light source to Alice is k, each pulse is divided into two parts A and B after passing through the BS, wherein the A pulse is taken as a sample into the light intensity monitor to analyze the photon number distribution information of the input pulse, and the B pulse is encoded as a coded pulse and sent to Bob. Let V_A be the number of pulses in the untagged part of the A pulse and V_B is the number of untagged part in the B pulse. According to Ref. [35], the probability that the inequality $V_\mathrm{B} \leq V_\mathrm{A} - \varepsilon k$ holds satisfies

$$P\left(V_\mathrm{B} \leq V_\mathrm{A} - \varepsilon k\right) \leq 2\exp\left(\frac{-k\varepsilon^2}{4}\right). \tag{1}$$

That is, the confidence of the inequality is

$$\tau > 1 - 2\exp\left(\frac{-k\varepsilon^2}{4}\right). \tag{2}$$

As can be seen from the above relationship, Alice can estimate the number of untagged pulses in the encoded pulse from the number of untagged pulses in the sample pulse. Let $\varDelta$ be the proportion of the tagged pulse in the sample pulse, then there are $(1-\varDelta-\varepsilon)k$ untagged pulses with a great probability in the coded pulse. Therefore, Alice and Bob can use the measured Q_e, E_e to estimate the upper and lower bounds of the untagged pulse gain and error rate

$$\begin{aligned}\bar{Q} &= \frac{Q_\mathrm{e}}{1-\varDelta-\varepsilon},\quad \underline{Q} = \max\left(0, \frac{Q_\mathrm{e}-\varDelta-\varepsilon}{1-\varDelta-\varepsilon}\right),\\ \overline{EQ} &= \frac{Q_\mathrm{e}E_\mathrm{e}}{1-\varDelta-\varepsilon},\quad \underline{EQ} = \max\left(0, \frac{Q_\mathrm{e}E_\mathrm{e}-\varDelta-\varepsilon}{1-\varDelta-\varepsilon}\right).\end{aligned} \tag{3}$$

The number of photons in the untagged pulse is m, and the conditional probability $P_n(m)$ that there are n photons transmitted to Bob after Alice encoded conforms to Bernoulli distribution,

$$P_n(m) = C_m^n (q\lambda)^n (1-q\lambda)^{m-n}, \tag{4}$$

where λ is the internal transmittance of Alice, $0 \leq \lambda \leq 1$, and Alice controls the intensity of the pulse sent to Bob by adjusting λ. Here q is the splitting ratio of the BS for monitoring the information of the input pulse photon number distribution. For untagged bits, under the condition of $(1+\delta)N\lambda < 1$, the upper and lower bounds of $P_n(m)$ are respectively

$$\overline{P_n} = \begin{cases} (1-\lambda)^{(1-\delta)N}, & n=0,\\ \begin{pmatrix}(1+\delta)N\\ n\end{pmatrix}\lambda^n(1-\lambda)^{(1+\delta)N-n}, & 1\leq n\leq(1+\delta)N,\\ 0, & n>(1+\delta)N,\end{cases} \tag{5}$$

$$\underline{P_n} = \begin{cases} (1-\lambda)^{(1+\delta)N}, & n=0,\\ \begin{pmatrix}(1-\delta)N\\ n\end{pmatrix}\lambda^n(1-\lambda)^{(1-\delta)N-n}, & 1\leq n\leq(1-\delta)N,\\ 0, & n>(1-\delta)N.\end{cases} \tag{6}$$

The constraint $(1+\delta)N\lambda < 1$ guarantees that the average number of photons of any untagged pulse output from the Alice terminal is less than 1, which is easily achievable experimentally.

In the case of the trusted source, since the attacker Eve only knows the photon number distribution information in the pulse sent from Alice, it is considered that the bit error rate and the count rate of the n photons in the decoy state are the same as those in the signal state. This is the theoretical basis for the successful application of the decoy state method in the trusted source QKD. However, this condition does not hold under the condition that the light source is not reliable. In the case that the light source is untrusted, we believe that Eve not only controls the light source but also controls the transmission channel, so Eve not only grasps the photon number distribution information in the light pulse emitted from the Alice, but also grasps the photon number distribution information of the light pulse entering the Alice end. At this time,

$$\tau > 1 - 2\exp\left(\frac{-k\varepsilon^2}{4}\right), \tag{7}$$

$$Y_{m,n}^{\mathrm{S}} = Y_{m,n}^{\mathrm{D}},\quad e_{m,n}^{\mathrm{S}} = e_{m,n}^{\mathrm{D}}, \tag{8}$$

where $Y_{m,n}$ indicates the conditional probability that m photons enter the Alice end, and n photons are emitted from Alice and trigger the Bob end detector. Here $e_{m,n}$ denotes the bit error rate when m photons enter the Alice end and n photons are emitted from Alice and trigger the Bob end detector. The superscript S indicates the signal state, at that time the internal transmittance is λ^{S}, and the superscript D indicates the decoy state, and the internal transmittance is λ^{D}.

3. Security analysis of RFI-QKD with an untrusted source

When analyzing the security of RFI-QKD protocol with an untrusted source under the condition of infinite key length, we only pay attention to the calculation methods of single-photon counting rate and single-photon bit error rate in different base selection conditions of untagged pulses. Firstly, Bob can measure the total counting rate under the signal intensity and the decoy intensity $Q_{\mathrm{e}}^{\mathrm{S}}$, $Q_{\mathrm{e}}^{\mathrm{D}}$. Bob can also get the bit error rate $Q_{\mathrm{e}}^{\mathrm{S}}E_{\mathrm{e},ij}^{\mathrm{S}}\,(ij\in\{ZZ,XX,YY,XY,YX\})$ in the signal state when Alice chooses i-basis coding and Bob chooses j-basis measuring, respectively,

$$\begin{aligned}
Q_{\mathrm{e}}^{\mathrm{S}} &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n},\\
Q_{\mathrm{e}}^{\mathrm{D}} &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{D}}(m)\,Y_{m,n}, \qquad (9)\\
Q_{\mathrm{e}}^{\mathrm{S}}E_{\mathrm{e},ZZ}^{\mathrm{S}} &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{ZZ},\\
Q_{\mathrm{e}}^{\mathrm{S}}E_{\mathrm{e},XX}^{\mathrm{S}} = Q_{\mathrm{e}}^{\mathrm{S}}E_{\mathrm{e},YY}^{\mathrm{S}} &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{XX},\\
Q_{\mathrm{e}}^{\mathrm{S}}E_{\mathrm{e},XY}^{\mathrm{S}} = Q_{\mathrm{e}}^{\mathrm{S}}E_{\mathrm{e},YX}^{\mathrm{S}} &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{XY}, \qquad (10)
\end{aligned}$$

where $P_{\mathrm{in}}(m)$ denotes the probability that the input photon numbers of Alice are m, and the superscripts S and D represent the signal state and the decoy state, respectively. It can be seen from Eqs. (9) and (10) that the gain is obtained under the signal state light intensity and decoy state light intensity in the untagged pulse, and the bit error rate of the untagged pulse is measured by Bob choosing the j-basis and encoded by Alice choosing the i-basis in the signal state

$$\begin{aligned}
Q^{\mathrm{S}} &= \sum_{m=(1-\delta)N}^{(1+\delta)N}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n},\\
Q^{\mathrm{D}} &= \sum_{m=(1-\delta)N}^{(1+\delta)N}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{D}}(m)\,Y_{m,n}, \qquad (11)\\
Q^{\mathrm{S}}E_{ZZ}^{\mathrm{S}} &= \sum_{m=(1-\delta)N}^{(1+\delta)N}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{ZZ},\\
Q^{\mathrm{S}}E_{XX}^{\mathrm{S}} = Q^{\mathrm{S}}E_{YY}^{\mathrm{S}} &= \sum_{m=(1-\delta)N}^{(1+\delta)N}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{XX},\\
Q^{\mathrm{S}}E_{XY}^{\mathrm{S}} = Q^{\mathrm{S}}E_{YX}^{\mathrm{S}} &= \sum_{m=(1-\delta)N}^{(1+\delta)N}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{XY}. \qquad (12)
\end{aligned}$$

The bit error rate under different bases when m photons enter the Alice end and n photons are emitted from Alice end and trigger the Bob end detector is given as $e_{m,n}^{ij}=\frac{e_{ij}\eta_{m,n}+d_{\mathrm{B}}/2}{Y_{m,n}}$.[36] Here e_{ij}, $\eta_{m,n}$ and d_{B} denote the erroneous detection probability under i and j bases, the detection efficiency of n-photon state and the dark count rate of Bob's detector. We have $e_{ZZ}=\frac{1-P}{P}$, $e_{XY}=e_{YX}=\frac{1}{2}$, $e_{XX}=e_{YY}=\frac{1-P\cos\beta}{2}$. P represents the probability that the signal state is correctly measured, and β represents the deviation of the angle between two reference frames.

Using the method in Ref. [22], when the inequality

$$\frac{\lambda_{\mathrm{S}}}{\lambda_{\mathrm{D}}} > \frac{(1+\delta)N-2}{(1-\delta)N-2}\left(\frac{(1+\delta)N-2}{2\delta N}\right)^{2\delta N/[(1-\delta)N-2]} \times\left(\frac{(1+\delta)N-2}{(1-\delta)N-2}\,\frac{e^{2}}{2\delta N}\right)^{1/2[(1-\delta)N-2]} \qquad (13)$$

is established, the lower bound of the gain of single photon pulses under signal state light intensity in the untagged pulses can be expressed as

$$\begin{aligned}
Q_{1}^{\mathrm{S}} > \underline{Q_{1}^{\mathrm{S}}} = \underline{P_{1}^{\mathrm{S}}}\Big\{&\underline{Q^{\mathrm{D}}P_{2}^{\mathrm{S}}} - \overline{Q^{\mathrm{S}}P_{2}^{\mathrm{D}}} + (\underline{P_{0}^{\mathrm{S}}}\overline{P_{2}^{\mathrm{D}}} - \overline{P_{0}^{\mathrm{D}}}\underline{P_{2}^{\mathrm{S}}})\overline{Q^{V}}\\
&-\frac{2\delta N(1-\lambda_{\mathrm{D}})^{2\delta N-1}\underline{P_{2}^{\mathrm{S}}}}{[(1-\delta)N+1]!}\Big\}\Big\{\overline{P_{1}^{\mathrm{D}}}\underline{P_{2}^{\mathrm{S}}}-\underline{P_{1}^{\mathrm{S}}}\overline{P_{2}^{\mathrm{D}}}\Big\}^{-1}. \qquad (14)
\end{aligned}$$

In order to calculate the single-photon error rate in signal state of the untagged pulses when Alice and Bob both select the Z basis, from Eq. (12) we can obtain the following formula:

$$\begin{aligned}
Q^{\mathrm{S}}E_{ZZ}^{\mathrm{S}} &= \sum_{m=(1-\delta)N}^{(1+\delta)N}\sum_{n=0}^{\infty} P_{\mathrm{in}}(m)\,P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{ZZ}\\
&= \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)P_{0}^{\mathrm{S}}(m)\,Y_{m,0}e_{m,0}^{ZZ}\\
&\quad+\sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)P_{1}^{\mathrm{S}}(m)\,Y_{m,1}e_{m,1}^{ZZ}\\
&\quad+\sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)\sum_{n=2}^{\infty} P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{ZZ}. \qquad (15)
\end{aligned}$$

Because

$$\sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)\sum_{n=2}^{\infty} P_{n}^{\mathrm{S}}(m)\,Y_{m,n}e_{m,n}^{ZZ} \geq 0, \qquad (16)$$

we have

$$\begin{aligned}
Q^{\mathrm{S}}E_{ZZ}^{\mathrm{S}} \geq &\sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)P_{0}^{\mathrm{S}}(m)\,Y_{m,0}e_{m,0}^{ZZ}\\
&+\sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)P_{1}^{\mathrm{S}}(m)\,Y_{m,1}e_{m,1}^{ZZ}. \qquad (17)
\end{aligned}$$

Then, when Alice and Bob both select the Z-basis, the upper bound of the single-photon error rate in signal state of the untagged pulses is

$$\begin{aligned}
e_{1,ZZ}^{\mathrm{S}} &\leq \frac{Q^{\mathrm{S}}E_{ZZ}^{\mathrm{S}}-\underline{P_{0}^{\mathrm{S}}}E^{V}Q^{V}}{Q_{1}^{\mathrm{S}}}\\
&\leq \frac{\overline{Q^{\mathrm{S}}E_{ZZ}^{\mathrm{S}}}-\underline{P_{0}^{\mathrm{S}}}\,\underline{E^{V}Q^{V}}}{\underline{Q_{1}^{\mathrm{S}}}} = \overline{e_{1,ZZ}^{\mathrm{S}}}. \qquad (18)
\end{aligned}$$

Using the same method, we can obtain $\overline{e_{1,ij}^{\mathrm{S}}}$ $(ij\in\{XX,$ $YY,\ XY,\ YX\})$, which represents the upper bound of the single-photon error rate in the signal state of the untagged pulses when Alice selects the i-basis to prepare, and Bob selects the j-basis to measure. Thus, the lower bound $\underline{C_1}$ of the parameter C and the information mastered by Eve in the case of the single photon of the untagged pulses can be calculated

$$\underline{C_{1}} = \left(1-2\overline{e_{1,XX}^{\mathrm{S}}}\right)^{2}+\left(1-2\overline{e_{1,XY}^{\mathrm{S}}}\right)^{2}$$

$$
\begin{aligned}
&+\left(1-2\overline{e_{1,YX}^{\mathrm{S}}}\right)^2+\left(1-2\overline{e_{1,YY}^{\mathrm{S}}}\right)^2,\\
I_{\mathrm{E}} \;=\;& \left(1-\overline{e_{1,ZZ}^{\mathrm{S}}}\right)^2 h\left(\frac{1+V_{\max}}{2}\right)\\
&+\overline{e_{1,ZZ}^{\mathrm{S}}}h\left(\frac{1+f\left(V_{\max}\right)}{2}\right), \qquad (19)
\end{aligned}
$$

where

$$
\begin{aligned}
V_{\max} &= \min\left[\frac{1}{1-\overline{e_{1,ZZ}^{\mathrm{S}}}}\cdot\sqrt{\frac{\underline{C_1}}{2}},1\right],\\
f\left(V_{\max}\right) &= \frac{\sqrt{\frac{\underline{C_1}}{2}-\left(1-\overline{e_{1,ZZ}^{\mathrm{S}}}\right)^2{V_{\max}}^2}}{\overline{e_{1,ZZ}^{\mathrm{S}}}}. \qquad (20)
\end{aligned}
$$

Combined with the GLLP formula, we can obtain the RFI-QKD protocol secret key rate formula under ideal conditions with the untrusted source as follows:

$$
R=-Q_{\mathrm{e}}^{\mathrm{S}} f\left(E_{\mathrm{e},ZZ}^{\mathrm{S}}\right) h\left(E_{\mathrm{e},ZZ}^{\mathrm{S}}\right)+(1-\varDelta-\varepsilon)\,\underline{Q_1^{\mathrm{S}}}\left(1-I_{\mathrm{E}}\right), \qquad (21)
$$

where $Q_{\mathrm{e}}^{\mathrm{S}}$ is the total signal state gain detected at the Bob end, and $E_{\mathrm{e},ZZ}^{\mathrm{S}}$ is the bit error rate in the signal state when Alice and Bob both select the Z-basis. Here $f(E_{\mathrm{e},ZZ}^{\mathrm{S}})$ is the error correction efficiency, and $\underline{Q_1^{\mathrm{S}}}$ is the lower bound of the signal state gain of single-photon pulses of untagged pulses; $h\left(x\right)=-x\log_2\left(x\right)-\left(1-x\right)\log_2\left(1-x\right)$ is the binary Shannon function, and I_{E} is the information of Eve. $\varDelta$ is the average probability that a sampling pulse belongs to a tagged sampling pulse in the asymptotic case, and the specific calculation method will be given in the following.

The above security analysis is based on the fact that the output key length is infinite, but an actual QKD system runtime is limited, which means that its output key length is limited. The impact of the finite length of the key on the untrusted source protocol mainly includes two aspects: Firstly, in the finite key case, the calculations of the untagged pulses are different. In the case of infinite key, when the confidence level defined by Eq. (2) approaches 1, we can think $\varepsilon\sim 0$ because of $k\sim\infty$. However, when the key length is finite, for a fixed k, if you want the confidence level to be no less than τ, we need to choose

$$
\varepsilon=\sqrt{-\frac{4\ln\left(\left(1-\tau\right)/2\right)}{k}}. \qquad (22)
$$

Secondly, in the decoy state QKD protocol, the influence of the statistical fluctuation caused by the finite key in the parameter estimation cannot be ignored. In this section, we use the Chernoff bound to characterize the statistical fluctuations in the parameter estimation of the decoy state RFI-QKD protocol with an untrusted source under finite key conditions. In the decoy state RFI-QKD protocol with an untrusted source, the gains under different light intensities and the bit error rates in different signal bases are measured by a limited number of samples, and the measured values and mathematical expectations meet the relevant conditions of the Chernoff bound. According to Chernoff bound, the measured values of gain under the light intensity of signal state $Q_{\mathrm{e}}^{\mathrm{S}}$ and the actual value $Q_{\mathrm{e}}^{\mathrm{S}*}$ are in accordance with Eq. (23) with a probability that is not less than $1-\varepsilon_3-\varepsilon_4$,

$$
\begin{aligned}
Q_{\mathrm{e}}^{\mathrm{S}}-\sqrt{\frac{2Q_{\mathrm{e}}^{\mathrm{S}}}{p_{\mathrm{S}}M}\ln\frac{1}{\left(\varepsilon_4\right)^{3/2}}} &= Q_{\mathrm{e}}^{\mathrm{S}*\mathrm{L}}\le Q_{\mathrm{e}}^{\mathrm{S}*}\le Q_{\mathrm{e}}^{\mathrm{S}*\mathrm{U}}\\
&= Q_{\mathrm{e}}^{\mathrm{S}}+\sqrt{\frac{2Q_{\mathrm{e}}^{\mathrm{S}}}{p_{\mathrm{S}}M}\ln\frac{16}{\left(\varepsilon_3\right)^4}}. \qquad (23)
\end{aligned}
$$

Here M is the number of pulses emitted by Alice; p_{S} is the probability that the signal state light intensity sent from Alice is μ; ε_3 and ε_4 are the probabilities that the actual value is out of the statistical fluctuation range of the measured value. Similarly, we can obtain the upper and lower bounds of the decoy state gain in Bob-end as follows:

$$
\begin{aligned}
Q_{\mathrm{e}}^{\mathrm{D}}-\sqrt{\frac{2Q_{\mathrm{e}}^{\mathrm{D}}}{p_{\mathrm{D}}M}\ln\frac{1}{\left(\varepsilon_4\right)^{3/2}}} &= Q_{\mathrm{e}}^{\mathrm{D}*\mathrm{L}}\le Q_{\mathrm{e}}^{\mathrm{D}*}\le Q_{\mathrm{e}}^{\mathrm{D}*\mathrm{U}}\\
&= Q_{\mathrm{e}}^{\mathrm{D}}+\sqrt{\frac{2Q_{\mathrm{e}}^{\mathrm{D}}}{p_{\mathrm{D}}M}\ln\frac{16}{\left(\varepsilon_3\right)^4}}, \qquad (24)
\end{aligned}
$$

where p_{D} is the probability that the decoy state light intensity sent from Alice is v.

Therefore, the upper and lower bounds of the gain of the signal state in the untagged pulses under finite key conditions are, respectively,

$$
\overline{Q^{\mathrm{S}*}}=\frac{Q_{\mathrm{e}}^{\mathrm{S}*\mathrm{U}}}{1-\varDelta-\varepsilon}, \qquad (25)
$$

$$
\underline{Q^{\mathrm{S}*}}=\max\left(\frac{Q_{\mathrm{e}}^{\mathrm{S}*\mathrm{L}}-\varDelta-\varepsilon}{1-\varDelta-\varepsilon},0\right). \qquad (26)
$$

Similarly, under finite key conditions, the upper and lower bounds of the decoy state gain in the untagged pulses are, respectively,

$$
\overline{Q^{\mathrm{D}*}}=\frac{Q_{\mathrm{e}}^{\mathrm{D}*\mathrm{U}}}{1-\varDelta-\varepsilon}, \qquad (27)
$$

$$
\underline{Q^{\mathrm{D}*}}=\max\left(\frac{Q_{\mathrm{e}}^{\mathrm{D}*\mathrm{L}}-\varDelta-\varepsilon}{1-\varDelta-\varepsilon},0\right). \qquad (28)
$$

Combining Eq. (14) with Eq. (25),the lower bound of the counting rate of the single photon pulses in the untagged pulses under finite key conditions, Eq. (28), can be rewritten as

$$
\begin{aligned}
Q_1^{\mathrm{S}*} > \underline{Q_1^{\mathrm{S}*}} = \underline{P_1^{\mathrm{S}}}\Bigg\{&\underline{Q^{\mathrm{D}*}P_2^{\mathrm{S}}}-\overline{Q^{\mathrm{S}*}P_2^{\mathrm{D}}}+\left(\underline{P_0^{\mathrm{S}}}\overline{P_2^{\mathrm{D}}}-\overline{P_0^{\mathrm{D}}}\underline{P_2^{\mathrm{S}}}\right)\overline{Q^{V}}\\
&-\frac{2\delta N(1-\lambda_{\mathrm{D}})^{2\delta N-1}\underline{P_2^{\mathrm{S}}}}{[(1-\delta)N+1]!}\Bigg\}\left\{\overline{P_1^{\mathrm{D}}}\underline{P_2^{\mathrm{S}}}-\underline{P_1^{\mathrm{S}}}\overline{P_2^{\mathrm{D}}}\right\}^{-1}. \qquad (29)
\end{aligned}
$$

In the signal state, when Alice selects Z-basis to prepare and Bob selects Z-basis to measure, the bit error rate measurement value $E_{\mathrm{e},ZZ}^{\mathrm{S}}$ and the actual error rate $E_{\mathrm{e},ZZ}^{\mathrm{S}*}$ match the formula (29) with a probability that is not less than $1-\varepsilon_3-\varepsilon_4$,

$$E^{\mathrm{S*U}}_{\mathrm{e},ZZ}=E^{\mathrm{S}}_{\mathrm{e},ZZ}+\sqrt{\frac{2E^{\mathrm{S}}_{\mathrm{e},ZZ}}{p_s(1-2a)^2M}\ln\frac{16}{(\varepsilon_3)^4}},$$
$$E^{\mathrm{S*L}}_{\mathrm{e},ZZ}=E^{\mathrm{S}}_{\mathrm{e},ZZ}-\sqrt{\frac{2E^{\mathrm{S}}_{\mathrm{e},ZZ}}{p_s(1-2a)^2M}\ln\frac{1}{(\varepsilon_4)^{3/2}}}. \qquad (30)$$

In the same way, we can obtain the upper and lower bounds of the bit error rate when Alice selects $i\in\{X,Y\}$ basis and Bob selects $j\in\{X,Y\}$ basis in the signal state

$$E^{\mathrm{S*U}}_{\mathrm{e},ij}=E^{\mathrm{S}}_{\mathrm{e},ij}+\sqrt{\frac{2E^{\mathrm{S}}_{\mathrm{e},ij}}{p_s(1-2a)^2M}\ln\frac{16}{(\varepsilon_3)^4}},$$
$$E^{\mathrm{S*L}}_{\mathrm{e},ij}=E^{\mathrm{S}}_{\mathrm{e},ij}-\sqrt{\frac{2E^{\mathrm{S}}_{\mathrm{e},ij}}{p_s(1-2a)^2M}\ln\frac{1}{(\varepsilon_4)^{3/2}}}, \qquad (31)$$

where subscript $j\in\{XX,YY,XY,YX\}$ indicates that Alice selects i-basis to encode and Bob selects j-basis to measure. Similar to the method of calculating the lower bound of the single photon counting rate in untagged pulses under finite key conditions, we can obtain upper and lower bounds of the bit error rate of different selections of bases in untagged signal state pulses, and then we can obtain the upper bound of the error rate of single-photon pulse of untagged signal pulses under finite key conditions when Alice selects i-basis and Bob selects j-basis to measure $\overline{e^{\mathrm{S}*}_{1,ij}}\,(ij\in\{XX,YY,XY,YX\})$. Thereby, $\underline{C^*_1}$ can be calculated, which denotes the lower bound of the parameter C in the case of single photon in untagged pulses under finite key conditions. Then, we can calculate $I_{\mathrm{E}}{}^*$, which denotes the information of Eve. Finally, the secret key rate R of RFI-QKD with an untrusted source under finite key conditions can be found using Eq. (31),

$$\begin{aligned}R\ =&\ -Q^{\mathrm{S*U}}_{\mathrm{e}}f\left(E^{\mathrm{S*U}}_{\mathrm{e},ZZ}\right)h\left(E^{\mathrm{S*U}}_{\mathrm{e},ZZ}\right)+(1-\varDelta-\varepsilon)\,\underline{Q^{\mathrm{S}*}_1}\,(1-I_{\mathrm{E}}{}^*)\\&-\frac{6}{M}\log_2\frac{21}{\varepsilon_{\mathrm{sec}}}-\frac{1}{M}\log_2\frac{2}{\varepsilon_{\mathrm{cor}}},\end{aligned} \qquad (32)$$

where

$$I^*_{\mathrm{E}}=\left(1-\overline{e^{\mathrm{S}*}_{1,ZZ}}\right)^2h\left(\frac{1+V^*_{\max}}{2}\right)+\overline{e^{\mathrm{S}*}_{1,ZZ}}h\left(\frac{1+f\left(V^*_{\max}\right)}{2}\right),$$

$\varepsilon_{\mathrm{cor}}$ is the probability that Alice and Bob have different keys, and $\varepsilon_{\mathrm{sec}}$ is the probability that Eve knows the key information, and M is the amount of the pulses sent from Alice to Bob.

Finally, the relationship between the secret key rate and the secret key transmission distance of the decoy state RFI-QKD protocol in the case of infinite key length and finite key length is demonstrated by numerical simulation. The numerical simulation of this section employs the QKD system channel model with standard fiber transmission. The experimental parameters used are listed in Table 1.

Table 1. Experimental parameters used in the numerical simulation of the RFI-QKD protocol with an untrusted source.

α	Y_0	η_{I}	σ_{I}	q	f	η_{B}
0.2 dB/km	6×10^{-7}	0.7	6×10^{5}	0.01	1.16	0.2

Among them, α and Y_0 are the transmission loss coefficient of optical fiber and the dark count of Bob detector, η_{I} and σ_{I} are the detection efficiency of light intensity monitor and the noise of light intensity monitor, q and f are the beam splitting ratio and the protocol error correction efficiency, and η_{B} is the detection efficiency of Bob's detector. In the optical fiber transmission process, the total transmission efficiency is $\eta=\eta_{\mathrm{B}}10^{-\alpha L/10}$, L is the distance between Alice and Bob in kilometers. In order to improve the performance of the protocol, the decoy state light intensity is selected to be $v=0.05$ and the value of signal state light intensity is optimized. The probability of Alice choosing to prepare signal state is set to be $P_{\mathrm{S}}=0.7$, and the probability of decoy state is set to be $P_{\mathrm{D}}=0.2$. Referring to Ref. [35], we choose $\delta=0.01$, the confidence level $\tau>1-10^{-10}$ and $\varepsilon_3=\varepsilon_4=\varepsilon_{\mathrm{sec}}=\varepsilon_{\mathrm{cor}}=10^{-10}$ in simulation. The proportion of tagged pulses in sample pulses $\varDelta$ can be obtained by the following formula:

$$\varDelta=1-\mathrm{erf}\left(\frac{N\eta_{\mathrm{I}}(1-q)+\varsigma}{\sqrt{2N+2\sigma_{\mathrm{I}}{}^2}}\right), \qquad (33)$$

where $\mathrm{erf}(x)=\frac{2}{\sqrt{\pi}}\int_0^x\mathrm{e}^{-t^2}\,\mathrm{d}t$ is error function, and $\varsigma=6\sigma_{\mathrm{I}}$ is the confidence interval for guaranteeing protocol security.

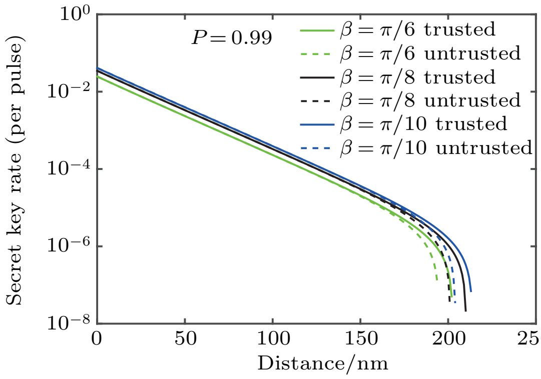

Fig. 3. Comparison of the secret key rate between RFI-QKD with a trusted source and an untrusted source.

In Fig. 3, we analyze the relationship between the secret key rate and the secure transmission distance of the decoy-state RFI-QKD protocol without considering the finite key effect. In the figure, we simulate the relationship between the secret key rate and the secure transmission distance when the angular deviation between two reference frames is $\pi/10$, $\pi/8$, $\pi/6$ and the probability that the signal state is correctly measured is 0.99 in the case of trusted source and untrusted source, respectively. The blue line is the simulation result with the trusted source, and the red line is the simulation result with the untrusted source. As can be seen from the figure, under ideal conditions, the decoy-state RFI-QKD protocol with an untrusted source can achieve the nonzero asymptotic secret key rate in a long distance of approximately 194 km when the reference frame deviation between Alice and Bob is $\pi/10$.

Considering the influence of finite key length on the secret key rate of the decoy-state RFI-QKD protocol with an untrusted source, we simulate the relationship between the secret key rate and the security transmission distance when the number of pulses Alice sends to Bob is 10^{11} and 10^{13}. In Fig. 4, the blue line represents the secret key rate of the decoy-state RFI-QKD with an untrusted source without considering the finite key effect, while the red line and the black line represent the secret key rate of the decoy-state RFI-QKD with an untrusted source when the number of pulses Alice sends to Bob is 10^{13} and 10^{11}, respectively. Figure 4 shows that the data size has a significant effect on the secret key rate of the decoy-state RFI-QKD protocol with an untrusted source. When the number of pulses that Alice sends to Bob is 10^{11} and the reference frame deviation between Alice and Bob is $\pi/10$, the decoy-state RFI-QKD protocol with an untrusted source can tolerate about a distance of 119 km.

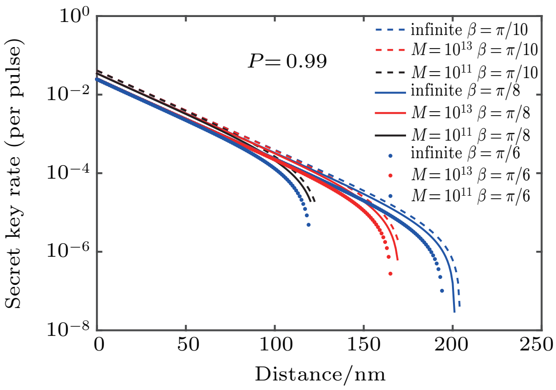

Fig. 4. Secret key rate comparison of RFI-QKD with an untrusted source under different pulse number conditions.

4. Conclusion

In summary, we have proposed and analyzed the decoy-state RFI-QKD protocol with an untrusted source based on plug-play structure. In order to compare the secret key rates with the real QKD system, our analysis and simulation consider the finite key effect using Chernoff bound. The results of the numerical simulation show that the transmission distance of the decoy-state RFI-QKD with an untrusted source is similar to the decoy-state RFI-QKD with a trusted source, and the finite data size clearly affects the performance of our protocol. The research in this paper provides an implementation scheme for the practical application of the RFI-QKD protocol, and reduces the requirement of the source for the specific implementation of the RFI-QKD protocol.

References

[1] Bennett C H and Brassard G 1984 *Proceddings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1999 Bangalore, India (IEEE, New York, 1984) p. 175

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[3] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595

[4] Guo Y, Su Y, Zhou J, Zhang L and Huang D 2019 *Chin. Phys. B* **28** 010305

[5] Tang G Z, Sun S H, Chen H, Li C Y and Liang L M 2016 *Chin. Phys. Lett.* **33** 120301

[6] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C and Han Z F 2016 *Phys. Rev. X* **9** 021046

[7] Cui C H, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053

[8] Qian Y J, He D Y, Wang S, Chen W, Yin Z Q, Guo G C and Han Z F 2019 *Optica* **6** 1178

[9] Wang S, Chen W, Yin Z Q *et al.* 2018 *Opt. Lett.* **43** 2030

[10] Wang S, Yin Z Q, Chau H F, Chen W, Wang C, Guo G C and Han Z F 2018 *Quantum Sci. Technol.* **3** 025006

[11] Yin Z Q, Wang S, Chen W, Han Y G, Wang R, Guo G C and Han Z F 2018 *Nat Commun.* **9** 457

[12] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat Photon.* **9** 832

[13] Wang S, Chen W, Yin Z Q *et al.* 2014 *Opt. Express* **22** 21739

[14] Wang S, Chen W, Guo F J, Yin Z Q, Li H W, Zhou Z, Guo G C and Han Z F 2012 *Opt. Lett.* **37** 1008-1010

[15] Rarity J G, Tapster P R, Gorman P M and Knight P 2002 *New J. Phys.* **4** 82

[16] Bonato C, Tomaello A, Deppo V D, Naletto G and Villoresi P 2009 *New J. Phys.* **11** 045017

[17] Bose S, Vedral V and Knight P L 1998 *Phys. Rev. A* **57** 822

[18] Chen K and Lo H K url = 2007 *Quantum Inf. Comput.* **7** 689

[19] Bacco D, Ding Y, Dalgaard K, Rottwitt K and Leif K O 2017 *Sci. Rep.* **7** 1

[20] Sibson P, Erven C, Godfrey M, Miki S, Yamashita T and Fujiwara M 2017 *Nat. Commun.* **8** 13984

[21] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev. A* **82** 012304

[22] Xue Q and Jiao R 2019 *Quantum Inf. Process.* **18** 313

[23] Li Y P, Chen W, Wang F X, Yin Z Q, Zhang L, Liu H and Han Z F 2019 *Opt. Lett.* **44** 4523

[24] Li X, Mao C, Zhu J, Zhang C and Wang Q 2019 *Eur. Phys. J. D* **73** 86

[25] Zhang H, Zhang C H, Zhang C M, Guo G C and Wang Q 2019 *J. Opt. Soc. Am. B* **36** 959

[26] Zhang C M, Wang W B, Li H W and Wang Q 2019 *Opt. Lett.* **44** 1226

[27] Yin Z Q, Wang S, Chen W, Li H W, Guo G C and Han Z F 2014 *Quantum Inf. Process.* **13** 1237

[28] Zhang C M, Zhu J R and Wang Q 2017 *Phys. Rev. A.* **95** 032309

[29] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502

[30] Wang C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2017 *Optica* **4** 1016

[31] Liang W Y, Wang S, Li H W, Yin Z Q, Chen W, Yao Y, Huang Z J, Guo G C and Han Z F 2015 *Sci. Rep.* **4** 3617

[32] Stucki D, Gisin N, Guinnard O, Robordy G and Zbinden H 2002 *New J. Phys.* **4** 41

[33] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320

[34] Zhao Y, Qi B and Lo H K 2008 *Phys. Rev. A* **77** 052327

[35] Zhao Y, Qi B, Lo H K and Qian L 2010 *New J. Phys.* **12** 023024

[36] Tanumoy P, Byung K P, Cho Y W *et al.* 2017 arXiv:1701.07587v1 [quant-ph]