SCIENCE CHINA
Information Sciences

• Supplementary File •

Security of few-state quantum key distribution with virtual mutual unbiased bases

Li Gong[1], Chenpeng Hao[1], Zhijiang Chen[1], Yifei Lu[1], Yang Wang[1*], Jiaji Li[1], Yanyang Zhou[1], Chun Zhou[1] & Hongwei Li[1*]

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

Appendix A The Few-State protocol

We present two few-state QKD protocols. One is the two-basis three-state QKD protocol, and the other is the three-basis four-state QKD protocol.

To start with, we introduce a two-basis three-state QKD protocol based on the BB84 protocol. We assume that Alice prepares ideal $|0\rangle, |1\rangle$ in the Z-basis, and $|+\rangle$ in the X-basis. Let $P_{0+}(P_{1+})$ denote the probability that Bob gets the measurement result $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ when Alice sends $|0\rangle(|1\rangle)$. Let $P_{++}(P_{+-})$ denote the probability that Bob's measurement result is $|+\rangle(|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$ when Alice sends $|+\rangle$. The essential steps of the two-basis three-state QKD protocol are as follows:

1. Alice selects a random classical bit string a for Z-basis's states modulation. Additionally, she selects a classical bit string b for basis selection, where the probability of 0 is $\frac{2}{3}$ and the probability of 1 is $\frac{1}{3}$. Then, according to the bit strings a and b, Alice prepares the corresponding quantum states and transmits them to Bob.

2. Bob chooses a random classical bit string c for measurement basis selection. After the measurement is completed, he obtains a bit string m.

3. Alice and Bob exchange the information about bases selection through a classic authentication channel. They save the encoding and decoding information of $b_i = c_i$, respectively. Furthermore, Bob constructs the decoded information at $b_i \neq c_i$ into a new string e.

4. Bob uses the string e to calculate probabilities P_{0+} and P_{1+}. Subsequently, he calculates the quantum bit error rate (QBER) of the X-basis using mismatch basis measurement information and sends it to Alice.

5. Alice and Bob randomly select some bits from the same basis set to evaluate the error rate. If the error rate is too high, then they abort the protocol. On the contrary, they apply error correction and privacy amplification to obtain the final secret key.

Then, we introduce a three-basis four-state QKD protocol. In this protocol, Alice prepares the ideal states $|0\rangle, |1\rangle$ in the Z-basis, the state $|+\rangle$ in the X-basis, and the state $|\tilde{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ in the Y-basis. Let $P_{0\tilde{+}}(P_{1\tilde{+}})$ denote the probability that Bob gets the measurement result $|\tilde{+}\rangle$ when Alice sends $|0\rangle(|1\rangle)$. Let $P_{\tilde{+}\tilde{+}}(P_{\tilde{+}\tilde{-}})$ denote the probability that Bob's measurement result is $|\tilde{+}\rangle(|\tilde{-}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))$ when Alice sends $|\tilde{+}\rangle$. The detailed steps of the three-basis four-state QKD protocol are as follows.

1. Alice selects a randomly classical bit string a for Z-basis's states modulation. Additionally, she selects a ternary string b for basis selection, where the probability of 0 is $\frac{1}{2}$, the probability of 1 is $\frac{1}{4}$, and the probability of 2 is $\frac{1}{4}$. Then, according to the bit strings a and b, Alice prepares the corresponding quantum states and transmits them to Bob.

2. Bob chooses a random ternary string c for measurement basis selection. After the measurement is completed, he obtains a bit string m.

3. Alice and Bob exchange the information about bases selection through a classic authentication channel. They save the encoded and decoded information of $b_i = c_i$, respectively. Furthermore, Bob constructs the decoded information at $b_i \neq c_i$ into a new string e.

* Corresponding author (email: wy@qiclab.cn, lihow@ustc.edu.cn)

4. Bob uses the string e to calculate probabilities $P_{0+}, P_{1+}, P_{0\tilde{+}}$ and $P_{1\tilde{+}}$. Subsequently, he calculates the QBER fo the X-basis and Y-basis using mismatch basis measurement information and sends it to Alice.

5. Alice and Bob randomly select and exchange some quantum states from the same basis set to estimate the error rate. If the error rate is too high, then they abort the protocol. On the contrary, Alice and Bob perform error correction and privacy amplification to obtain the final secret key.

By analyzing the detailed processes of the two few-state QKD protocols, we can identify two differences from the original protocol. The first difference is in the quantum state preparation stage. Alice must prepare four quantum states for the BB84 QKD protocol and six quantum states for the six-state QKD protocol. However, in the two-basis three-state QKD protocol, she only needs to prepare three quantum states. In the three-basis four-state QKD protocol, Alice only needs to prepare four quantum states. The second difference is in the basis comparison stage. The mismatched bits are discarded in the BB84 and six-state QKD protocols. However, in these few-state QKD protocols, the mismatched bits will be used to evaluate the QBER of the monitoring basis.

In these few-state protocols, the probability distribution used for the bit string b is a design choice and does not compromise the protocols' security. A biased basis scheme can also be adopted to enhance the efficiency of these few-state protocols. Besides, if Eve obtains the quantum states $|-\rangle$ or $|\tilde{-}\rangle$, she can only know that Alice has prepared quantum states in the Z-basis, but cannot determine the specific quantum states in the Z-basis. Therefore, if Eve launches an attack on these protocols, it will trigger an abnormally high QBER. This will enable Alice and Bob to detect Eve's malicious activity.

Appendix B Density matrix equivalence with VMUB Method

In the original BB84 QKD protocol, Alice randomly prepares the following quantum states,

$$\begin{aligned} \rho_0 &= |0\rangle\langle 0|, \qquad \rho_1 = |1\rangle\langle 1|, \\ \rho_+ &= |+\rangle\langle +|, \quad \rho_- = |-\rangle\langle -|, \end{aligned} \tag{B1}$$

where ρ_0 and ρ_1 are randomly prepared in the Z-basis. ρ_+ and ρ_- are randomly prepared in the X-basis. In addition, the corresponding quantum states have the following properties

$$\begin{aligned} \rho_Z &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|, \\ \rho_X &= \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|, \end{aligned} \tag{B2}$$

where we can simply get $\rho_Z = \rho_X$. In addition, Bob can randomly use the following measurement operators

$$\begin{aligned} M_Z &= \{M_0 = |0\rangle\langle 0|, \qquad M_1 = |1\rangle\langle 1|\}, \\ M_X &= \{M_+ = |+\rangle\langle +|, \quad M_- = |-\rangle\langle -|\}. \end{aligned} \tag{B3}$$

Since Alice randomly prepares quantum states in the Z-basis and X-basis, we can conclude that the density matrices in these two preparation bases are identical, $\rho_Z = \rho_X$. Because the density matrices in the Z-basis and X-basis are equal, Eve cannot distinguish the quantum states ρ_X and ρ_Z. Since Eve cannot distinguish ρ_X and ρ_Z, she can only apply the same attack strategy to the quantum states ρ_X and ρ_Z. Based on the previous analysis results, the quantum states received by Bob still have the same density matrices in the Z-basis and X-basis.

$$\tilde{\rho}_Z = \tilde{\rho}_X. \tag{B4}$$

where $\tilde{\rho}_i, i \in \{Z, X\}$ denote the received density matrix on Bob's side for the two bases.

After Bob performs the measurement, he may get the different measurement outcomes. When he gets the measurement outcomes $|+\rangle$, the corresponding probabilities can be given by

$$\begin{aligned} P_{0+} + P_{1+} &= tr(\tilde{\rho}_Z M_+), \\ P_{++} + P_{-+} &= tr(\tilde{\rho}_X M_+), \end{aligned} \tag{B5}$$

According to Eqs. (B4) and (B5), we can derive the main formula

$$P_{0+} + P_{1+} = P_{++} + P_{-+}. \tag{B6}$$

Appendix C Security Analysis and Simulation of Three-Basis Four-State QKD protocol

Since the state preparation and measurement-based scheme can be analyzed using the entanglement-based protocol [1], we can assume that Alice prepares a maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and the second quantum state will be transmitted to Bob. According to the Ref. [2], we briefly introduce security analysis of the preparation and measurement protocol. Let both H_A and H_B be denoted as two-dimensional Hilbert spaces, $\sigma_{ABE} \in P(H_A \otimes H_B \otimes H_E)$ denotes a

density operator, where $P(H)$ is the set of non-negative operators on H. Alice and Bob obtain the classical measurement outcomes, when they apply projective measurements on H_A and H_B. Alice and Bob will share the quantum state σ_{AB}, where $\sigma_{AB} = tr_E(\sigma_{ABE})$. We can use the $\mathcal{D}$ operation

$$\mathcal{D}(\sigma_{AB}) := \frac{1}{4} \sum_{\tau \in \{I, \sigma_x, \sigma_y, \sigma_z\}} \tau^{\otimes 2} \sigma_{AB} \tau^{\otimes 2}, \tag{C1}$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, σ_x, σ_y and σ_z are the Pauli operators $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Because the D-operation commutes with the measurement operation on $H_A \otimes H_B$, it is easy to verify that the QBER is unchanged. According to Lemma 13 in Ref. [3], we can prove that Eve's information has not been reduced by applying the D-operation. Thus, this is a general analysis method to analyze the information security of different QKD protocols [4, 5].

Through a straightforward calculation, the operator $\mathcal{D}(\sigma_{AB})$ can be expressed as follows:

$$\mathcal{D}(\sigma_{AB}) = \sum_{i=0}^{3} \lambda_i |\Phi_i\rangle \langle\Phi_i|, \ with \ \sum_{i=0}^{3} \lambda_i = 1, \tag{C2}$$

where

$$\begin{aligned} |\Phi_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}, \\ |\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB}, \\ |\Phi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB}, \\ |\Phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AB}. \end{aligned} \tag{C3}$$

Let $\tilde{\sigma}_{ABE}$ be an arbitrary purification of $\mathcal{D}(\sigma_{AB})$ with an auxiliary system H_E. The operator $\tilde{\sigma}_{XYE}$ is obtained from $\tilde{\sigma}_{ABE}$ by measurements, where X, Y are Alice and Bob's measurement outcomes, respectively. E denotes Eve's ancillary system. It has been proved that the entropy $S(X|E)$ evaluated for σ_{ABE} is lower-bounded by the entropy evaluated for $\tilde{\sigma}_{ABE}$, where $S(X|E) = S(X, E) - S(E)$ and $S(\rho) = -tr(\rho log \rho)$. We can utilize $\tilde{\sigma}_{ABE}$ to estimate the quantum channel parameters λ_i, and the lower bound of $S(X|E)$ can be efficiently estimated correspondingly. Based on the operation $\mathcal{D}(\sigma_{AB})$, the Z-basis error rate e_Z and X-basis error rate e_X can be given by

$$\begin{aligned} e_Z &= \lambda_2 + \lambda_3, \\ e_X &= \lambda_1 + \lambda_3, \\ e_Y &= \lambda_1 + \lambda_2. \end{aligned} \tag{C4}$$

This analysis result demonstrates that e_Z, e_X and e_Y can be estimated from the quantum channel parameters λ_i. Since Eve can control the practical quantum channel, she can optimize λ_i to reduce the secret key rate. Furthermore, $\mathcal{D}$ commutes with the projective measurements on H_A and H_B, so the entropy $H(X|Y)$ can be estimated from the corresponding entropy for $\tilde{\sigma}_{XY}$. Thus we can derive the lower bound of the final secret key rate

$$R \geqslant min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} [S(X|E) - H(X|Y)], \tag{C5}$$

where $H(x) = -x log_2 x - (1-x) log_2 (1-x)$.

According to the mutual information formula $I(X:E) = S(X) - S(X|E)$, we can evaluate the mutual information between Alice and Eve that Eve obtains via eavesdropping.

$$\begin{aligned} I(X:E) &= S(X) - S(X|E), \\ &= 1 - S(X|E), \\ &= (\lambda_0 + \lambda_1) H(\frac{\lambda_0}{\lambda_0 + \lambda_1}) + (\lambda_2 + \lambda_3) H(\frac{\lambda_2}{\lambda_2 + \lambda_3}) \end{aligned} \tag{C6}$$

Based on the above analysis and simple calculation, we can obtain the secret key formula for the three-basis four-state QKD protocol

$$R \geqslant \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} \left[1 - (\lambda_0 + \lambda_1) H\left(\frac{\lambda_0}{\lambda_0 + \lambda_1}\right) - (\lambda_2 + \lambda_3) H\left(\frac{\lambda_2}{\lambda_2 + \lambda_3}\right) - H(\lambda_0 + \lambda_1) \right]. \tag{C7}$$

To analyze the worst-case key rate, we use the parameter κ to quantify the QBER in three bases,

$$\begin{aligned} e_{01} &\leqslant \kappa, \\ e_{10} &\leqslant \kappa, \\ e_{+-} &\leqslant \kappa, \\ e_{\bar{+}\bar{-}} &\leqslant \kappa, \end{aligned} \tag{C8}$$

where $e_{\tilde{+}\tilde{-}}$ is defined as the $|\tilde{+}\rangle$'s QBER. κ denotes the maximum value of these QBERs. Note that $e_{\tilde{+}\tilde{-}}$ can be directly obtained in this protocol.

For the Y-basis, we can derive $P_{0\tilde{+}}, P_{1\tilde{-}}$ via a similar derivation,

$$\begin{aligned} P_{0\tilde{+}} &= \frac{1}{2} + \epsilon_2(\epsilon_2 \in [-\frac{1}{2}, \frac{1}{2}]), \\ P_{1\tilde{+}} &= \frac{1}{2} + \epsilon_3(\epsilon_3 \in [-\frac{1}{2}, \frac{1}{2}]), \end{aligned} \tag{C9}$$

where ϵ_2 and ϵ_3 respectively denote slight offset value when Bob selects the Y basis to measure the Z-basis quantum state $(|0\rangle, |1\rangle)$ sent by Alice.

Similarly, in order to simplify the analysis, we use δ_2 to represent the total offset values of the Y bases. The equations are given by

$$\delta_2 = |P_{0\tilde{+}} + P_{1\tilde{+}} - 1|. \tag{C10}$$

We can represent the QBER $e_{\tilde{-}\tilde{+}}$ of the unprepared state $|\tilde{-}\rangle$ as follows

$$e_{\tilde{-}\tilde{+}} \leqslant \kappa + \delta_2. \tag{C11}$$

Thus, the QBER in the Y-basis e_Y can be expressed respectively as

$$e_Y = \frac{1}{2}(e_{\tilde{+}\tilde{-}} + e_{\tilde{-}\tilde{+}}) \leqslant \kappa + \frac{\delta_2}{2}. \tag{C12}$$

Based on the security proof framework of the original BB84 QKD protocol [2], $\lambda_i, i \in \{0, 1, 2, 3\}$ can be expressed as follows

$$\begin{aligned} \lambda_0 &= 1 - e_Z - e_X + \lambda_3, \\ \lambda_1 &= e_X - \lambda_3, \\ \lambda_2 &= e_Z - \lambda_3, \\ \lambda_1 + \lambda_2 &= e_Y. \end{aligned} \tag{C13}$$

Based on the above analysis, we can get the secret key formula of the three-basis four-state QKD protocol.

Then, we simulate the secret key rates of the three-basis four-state QKD protocol. Note that we assume that the offsets of the X-basis and Y-basis are equal to δ_2. The simulation results are shown in Fig. C1.

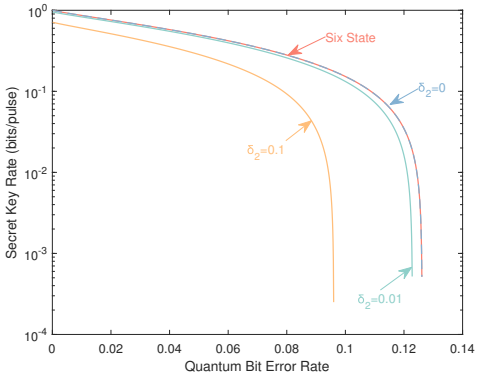

Figure C1 The secret key rate of the three-basis four-state QKD protocol varies with different offset parameters δ_2. For comparative analysis, the original six-state QKD protocol's secret key rate is plotted as a red solid line. The orange solid line represents the three-basis four-state QKD protocol with $\delta_2 = 0.1$, showing a maximum error tolerance of 0.096. The cyan solid line corresponds to $\delta_2 = 0.01$, achieving a maximum error tolerance of 0.122. The blue dashed line ($\delta_2 = 0$) exhibits the same maximum error tolerance (0.126) as that of the original six-state QKD protocol.

From these results, we conclude that the secret key rate gradually increases as δ_2 decreases. When $\delta_2 = 0$, the secret key rate of this scheme is equal to that of the original six-state protocol.

Appendix D Analysis of the decoy-state QKD with finite key length

In this section, we introduce the decoy-state protocol [6–8] under the finite-key length condition. According to the work of M.Tomamichel *et al.* [9], they utilized the entropic uncertainty relation to derive a bound on the smooth min-entropy of the raw key conditioned on Eve's information. This approach enabled a rigorous composable security proof for the BB84 protocol, following the composable security framework in [10]. Consequently, the expression for the ϵ-secret key can be obtained through this methodology as follows:

$$l \geqslant s^L_{Z,0} + s^L_{Z,1} - [1 - H(\phi_Z)] - Leak_{EC} - log_2\frac{2}{\epsilon_{cor}} - 6log_2\frac{21}{\epsilon_{sec}}, \tag{D1}$$

where $s^L_{Z,0}, s^L_{Z,1}$ denote the lower bounds of the number of vacuum events $s_{Z,0}$ and single-photon events $s_{Z,1}$ in the Z basis, respectively. $H(x) := -xlog_2(x) - (1-x)log_2(1-x)$ is the binary entropy. ϕ_Z represents the upper bound of the phase error rate in the Z basis. $Leak_{EC} = n_Z f_{EC} h(e_Z)$ represents the number of bits consumed in the error correction step, where f_{EC} is the efficiency of error correction. n_Z, e_Z represent the post-processing block size and the bit error rate in the Z basis, respectively. ϵ_{cor} and ϵ_{sec} denote the security parameters of correctness and secrecy, respectively.

We analyze the three-intensity decoy-state QKD protocol using Z-basis coding to generate secret key, which employs one signal state μ_1, two decoy states μ_2, μ_3. The protocol employs a biased basis selection strategy, where the Z and X bases are chosen with probability p_Z and $p_X = 1 - p_Z$, respectively. The intensities satisfy $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geqslant 0$. The selection probabilities for the intensities are P_{μ_1}, P_{μ_2} and $P_{\mu_3} = 1 - P_{\mu_1} - P_{\mu_2}$, respectively.

Let $s_{Z,n}$ represent the number of detection events observed by receiver given that sender sent n-photons states in the Z basis. Thus, we can derive that

$$n_Z = \sum_{n=0}^{\infty} s_{Z,n}, \tag{D2}$$

where n_Z represents the total number of detection counts given that sender sent states in the Z basis.

In the asymptotic regime, for the intensities $k \in \{\mu_1, \mu_2, \mu_3\}$, the expected value of $n_{Z,k}$ is expressed as

$$n_{Z,k} = \sum_{n=0}^{\infty} P_{k|n} s_{Z,n}, \forall k \in \{\mu_1, \mu_2, \mu_3\}, \tag{D3}$$

where $P_{k|n}$ is the conditional probability of selecting intensity k intensity given sender sends an n-photon state. Based on Bayes' rule, we can get the equation as follows:

$$P_{k|n} = \frac{P_k}{\chi_n} P_{n|k} = \frac{P_k}{\chi_n} \frac{e^{-k} k^n}{n!}, \forall k \in \{\mu_1, \mu_2, \mu_3\}, \tag{D4}$$

where $\chi_n := \sum_{k \in \{\mu_1, \mu_2 \mu_3\}} P_k \frac{e^{-k} k^n}{n!}$ is the average probability that Alice sends a n-photon state.

According to Wang *et al.* [11] research, the Chernoff bound [12] provides a tighter constraint than the Hoeffding's inequality [13]. Therefore, we utilize the Chernoff bound to characterize the statistical fluctuations. We derive that $n_{Z,k}$ and $m_{X,k}$ satisfy inequality as follows:

$$\begin{aligned} |\tilde{n}_{Z,k} - n_{Z,k}| &\leqslant \delta(n_{Z,k}, \epsilon_1), \\ |\tilde{m}_{X,k} - m_{X,k}| &\leqslant \delta(m_{X,k}, \epsilon_2), \end{aligned} \tag{D5}$$

where,$\tilde{n}_{Z,k}$ is the expected value of detected counts. ,$\tilde{m}_{X,k}$ represents the expected number of errors in the X-basis. $\epsilon_i, i \in \{1,2\}$ denote the probability of satisfying these inequalities, respectively. $\delta = \delta(x,y) \in (-\Delta, \tilde{\Delta})$ with $\Delta = \sqrt{2xln(16y^{-4})}$ and $\tilde{\Delta} = \sqrt{2xln(y^{-3/2})}$.

Based on the findings in Ref. [14], we are able to determine the lower bound of the number of vacuum events in the Z basis

$$s_{Z,0} \geqslant s^L_{Z,0} = \frac{\chi_0}{\mu_2 - \mu_3} \left(\frac{\mu_2 e^{\mu_3} n^-_{Z,\mu_3}}{P_{\mu_3}} - \frac{\mu_3 e^{\mu_2} n^+_{Z,\mu_2}}{P_{\mu_2}} \right) \tag{D6}$$

where $s_{Z,0}$ denotes $n^{\pm}_{Z,k}$ is the upper and lower bounds of the detected counts, where Alice and Bob choose the Z-basis for intensity k.

The lower bound of the number of single-photon events in the Z basis is

$$s_{Z,1} \geqslant s^L_{Z,1} = \frac{\mu \chi_1}{(\mu_2 - \mu_3)(\mu_1 - \mu_2 - \mu_3)} \left[\frac{e^{\mu_3} n^+_{Z,\mu_2}}{P_{\mu_2}} - \frac{e^{\mu_3} n^-_{Z,\mu_3}}{P_{\mu_3}} - \frac{\mu_2^2 - \mu_3^2}{\mu_2^2} \left(\frac{e^{\mu_1} n^+_{Z,\mu_1}}{P_{\mu_1}} - \frac{s^-_{Z,0}}{\chi_0} \right) \right] \tag{D7}$$

We can also calculate the low bound of the number of vacuum events $s^L_{X,0}$, and the lower bound of the number of single-photon events $s^L_{X,1}$ in the X-basis by using (D6), (D7).

Moreover, the upper bound of the number of bit errors $c^U_{X,1}$ associated with the single-photon events in the X-basis is given by

$$c_{X,1} \leqslant c^U_{X,1} = \frac{\chi_1}{\mu_2 - \mu_3} \left(\frac{e^{\mu_2} m^+_{X,\mu_2}}{P_{\mu_2}} - \frac{e^{\mu_3} m^-_{X,\mu_3}}{P_{\mu_3}} \right), \tag{D8}$$

where $c_{X,1}$ is the number of bit errors for single-photon events in the X-basis. $m^{\pm}_{X,k}$ are the upper bound and lower bound on the number of bit errors with different intensity k in the X-basis, respectively.

By extending a random-sampling without replacement problem [15], the formula for the phase error rate of the single-photon events in the Z-basis is given by

$$\phi_Z \leqslant \phi^U_Z = \frac{c^U_{X,1}}{s^L_{X,1}} + \gamma(\epsilon_{sec}, \frac{c^U_{X,1}}{s^L_{X,1}}, s^L_{X,1}, s^L_{Z,1}) \tag{D9}$$

where ϕ_Z denotes the phase error rate for single-photon Z-basis events.

$$\gamma(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cdln2} \log_2 \left(\frac{c+d}{cd(1-b)b} \frac{21^2}{a^2} \right)}. \tag{D10}$$

Appendix E Simulation parameters

The simulation of the decoy-state few-state QKD protocol with finite key length utilizes practical experimental parameters [16]. The scheme utilizes two bases: the optimal probability for selecting the Z-basis is 0.8 and the probability for the X-basis is 0.2. Additionally, it employs three types of quantum states: a signal state μ, one weak decoy state ν_1 and one vacuum state ν_2, following the scheme in [17]. To demonstrate the key rate advantage of this scheme, we optimize the average photon number of photons in the signal state and weak decoy state, as well as the transmission probabilities of the three light intensities. The error correction efficiency is $f_{EC} = 1.16$, and the dark count probability is $P_d = 6 \times 10^{-7}$. The optical misalignment error rate is $e_d = 0.5\%$. Bob's detector efficiency is $\eta_B = 0.1\%$, and the single-photon avalanche detector (SPAD) exhibits an after-pulse probability of $P_{ap} = 4 \times 10^{-2}$.

The simulation parameters are as listed in Table E1.

Table E1 Simulation parameter values

α	η_B	P_d	P_{ap}	e_d	f_{EC}
0.2	0.1	6×10^{-7}	4×10^{-2}	0.5%	1.16

We conduct a theoretical analysis based on the same fiber channel model from Ref. [14].

For different intensities k, the yield of the expected detection rate is as follows

$$Q_k = (1 + P_{ap})(1 - (1 - 2P_d)e^{-\eta k}), \tag{E1}$$

where, η denotes total transmittance for a single photon ($\eta = \eta_c \eta_B$). η_c (channel loss) equals $10^{-\alpha L/10}$, with L denoting the transmission distance. Meanwhile, for different intensities k, we can express the probability of a bit error as follows

$$E_k = P_d + e_d(1 - e^{-k\eta_c}) + \frac{P_{ap} Q_k}{2(1 + P_{ap})}. \tag{E2}$$

We set the security parameters as $\epsilon_{sec} = 1 \times 10^{-10}, \epsilon_{cor} = 1 \times 10^{-15}$, with all other failure probabilities in the parameter estimation process set to 1×10^{-10}.

References

1 Shor P W, Preskill J. Simple proof of security of the bb84 quantum key distribution protocol. Physical Review Letters, 2000, 85: 441
2 Renner R. Security of quantum key distribution. International Journal of Quantum Information, 2008, 6: 1–127
3 Tomamichel M, Colbeck R, Renner R. Duality between smooth min-and max-entropies. IEEE Transactions on Information Theory, 2010, 56: 4674–4681
4 Kraus B, Gisin N, Renner R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. Physical Review Letters, 2005, 95: 080501
5 Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. Physical Review A, 2005, 72: 012332
6 Hwang W Y. Quantum key distribution with high loss: toward global secure communication. Physical Review Letters, 2003, 91: 057901
7 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. Physical Review Letters, 2005, 94: 230504
8 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Physical Review Letters, 2005, 94: 230503
9 Tomamichel M, Renner R. Uncertainty relation for smooth entropies. Physical Review Letters, 2011, 106: 110506
10 Müller-Quade J, Renner R. Composability in quantum cryptography. New Journal of Physics, 2009, 11: 085006
11 Wang Y, Bao W S, Zhou C, et al. Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources. Physical Review A, 2016, 94: 032335
12 Chernoff H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. The Annals of Mathematical Statistics, 1952: 493–507
13 Hoeffding W. Probability inequalities for sums of bounded random variables. The collected works of Wassily Hoeffding, 1994: 409–426
14 Lim C C W, Curty M, Walenta N, et al. Concise security bounds for practical decoy-state quantum key distribution. Physical Review A, 2014, 89: 022307
15 Fung C H F, Ma X, Chau H. Practical issues in quantum-key-distribution postprocessing. Physical Review A, 2010, 81: 012318
16 Lucamarini M, Patel K, Dynes J, et al. Efficient decoy-state quantum key distribution with quantified security. Optics Express, 2013, 21: 24550–24565
17 Ma X, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution. Physical Review A, 2005, 72: 012326