SCIENCE CHINA
Information Sciences

• LETTER •

August 2026, Vol. 69, Iss. 8, 189501:1–189501:2
https://doi.org/10.1007/s11432-025-4612-2

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

Li GONG, Chenpeng HAO, Zhijiang CHEN, Yifei LU, Yang WANG*, Jiaji LI, Yanyang ZHOU, Chun ZHOU & Hongwei LI*

Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou 450001, China

Received 11 June 2025/Revised 2 August 2025/Accepted 18 September 2025/Published online 29 April 2026

Citation Gong L, Hao C P, Chen Z J, et al. Security of few-state quantum key distribution with virtual mutual unbiased bases. Sci China Inf Sci, 2026, 69(8): 189501, https://doi.org/10.1007/s11432-025-4612-2

Quantum key distribution (QKD) enables two remote entities, typically designated as Alice and Bob, to securely establish a shared secret key, even in the presence of a potential eavesdropper Eve [1]. In practical QKD systems, reducing system costs and improving system robustness have become important research directions, especially in satellite QKD systems [2]. Few-state QKD protocols can simplify system design and have been proven using different methods [3]. However, the security analysis of existing few-state QKD protocols is complex or limited by additional constraints, which reduces their flexibility to adapt to diverse practical scenarios. Therefore, it is interesting to propose a simple and universal few-state analysis method for few-state QKD protocols. In this study, we analyze few-state QKD protocols using the virtual mutually unbiased bases (VMUB) method [4], which estimates the error rate of the unprepared monitoring state by using mismatched data. We present two few-state QKD protocols based on our method in Appendix A. Based on our analysis method, these few-state QKD protocols can achieve the same secret key rate as the original QKD protocols if the measurement outcomes of the mismatched bases are random.

The main idea of our study is that we use the VMUB method to build a virtual QKD protocol. For the few-state QKD protocol, we assume that Alice only prepares three types of quantum states $|0\rangle$, $|1\rangle$ and $|+\rangle$ in the preparation stage, and that Bob performs two types of measurements: Z-basis measurement M_Z and X-basis measurement M_X. We define P_{ij} as the probability of Bob obtaining the measurement outcome $|j\rangle$ ($j \in \{0,1,+,-\}$) when Alice sends $|i\rangle$ ($i \in \{0,1,+\}$). Alice and Bob can use the mismatched measurement results to calculate probabilities P_{0+} and P_{1+}. The quantum bit error rate (QBER) of the unprepared state $|-\rangle$ can be characterized based on our analysis method.

In the virtual QKD protocol, Alice prepares quantum states in the X-basis, which can be characterized by ρ_X ($\rho_+ = |+\rangle\langle+|, \rho_- = I - |+\rangle\langle+|$), and Bob's measurement operators in the X-basis can be characterized by M_X ($M_+ = |+\rangle\langle+|, M_- = |-\rangle\langle-|$). Based on the VMUB method [4], we can derive the following equation:

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

Note that the derivation process of the above formula is shown in Appendix B. The QBER (e_{-+}) of the virtual state $|-\rangle$ can be estimated by P_{0+}, P_{1+} and P_{+-}. Based on (1), we can construct a virtual QKD protocol that is equivalent to the few-state QKD protocol. Then, we can use the security proof framework of the original BB84 QKD protocol [5] to analyze the few-state QKD protocol.

For our proposed two-basis three-state QKD protocol, we use the parameter κ to quantify the upper bounds of the QBERs in the two bases,

$$e_{01} \leqslant \kappa,\ e_{10} \leqslant \kappa,\ e_{+-} \leqslant \kappa, \tag{2}$$

where e_{01}, e_{10} and e_{+-} represent QBER values when Alice prepares the quantum states $|0\rangle, |1\rangle$ and $|+\rangle$, respectively. Note that e_{01}, e_{10} and e_{+-} can be directly obtained in the experiment implementation of the few-state QKD.

When Bob chooses a mismatched basis with Alice's, Bob should obtain random measurement outcomes in the ideal case. However, there may be some minor offsets in the practical scenario. Therefore, the probabilities of Bob choosing X-basis to measure Z-basis quantum states are as follows:

$$\begin{aligned} P_{0+} &= \frac{1}{2} + \epsilon_0 \left(\epsilon_0 \in \left[-\frac{1}{2}, \frac{1}{2}\right]\right), \\ P_{1+} &= \frac{1}{2} + \epsilon_1 \left(\epsilon_1 \in \left[-\frac{1}{2}, \frac{1}{2}\right]\right), \end{aligned} \tag{3}$$

where ϵ_0 and ϵ_1 denote slight offset values when Bob selects the X-basis to measure the Z-basis quantum states $|0\rangle$ and $|1\rangle$, respectively.

We use δ_1 to represent the total offset value of the X-basis, which is given by

$$\delta_1 := |P_{0+} + P_{1+} - 1|. \tag{4}$$

By substituting (3) and (4) into (1), we can calculate the QBER e_{-+} of the unprepared monitoring state $|-\rangle$ as follows:

$$e_{-+} \leqslant \kappa + \delta_1. \tag{5}$$

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

Thus, the QBERs in the Z-basis and X-basis (e_Z, e_X) can be expressed respectively as

$$\begin{aligned} e_Z &= \frac{1}{2}(e_{01} + e_{10}) \leqslant \kappa, \\ e_X &= \frac{1}{2}(e_{+-} + e_{-+}) \leqslant \kappa + \frac{\delta_1}{2}. \end{aligned} \tag{6}$$

Based on the security proof framework of the original BB84 QKD protocol [5], the quantum channel parameters λ_i $(i \in \{0,1,2,3\})$ can be expressed as follows:

$$\begin{aligned} \lambda_0 &= 1 - e_Z - e_X + \lambda_3, \\ \lambda_1 &= e_X - \lambda_3, \\ \lambda_2 &= e_Z - \lambda_3. \end{aligned} \tag{7}$$

Finally, the secret key rate formula for the two-basis three-state QKD protocol is derived as follows:

$$R \geqslant 1 - H\left(\kappa + \frac{\delta_1}{2}\right) - H(\kappa). \tag{8}$$

The simulation results show that the two-basis three-state QKD protocol can achieve the same secret key rate as that of the BB84 QKD protocol in the case of $\delta_1 = 0$. Similarly, the security analysis and simulation results of the three-basis four-state QKD protocol are provided in Appendix C.

Next, we analyze the secret key rate of the two-basis three-state QKD protocol with the decoy-state method and finite key length. The parameter estimation of the decoy-state QKD protocol with finite key length is shown in Appendix D. We assume that Alice and Bob use the Z-basis for secure key extraction, and use the X-basis to estimate Eve's information. Based on our method, we need to re-estimate the bit error rates of the X-basis with few-state protocols.

From the X-basis measurement results, we can directly calculate the single-photon QBER when Alice prepares the quantum state $|+\rangle$. By using our method, we can derive the QBER in the single-photon events in the X-basis $c^U_{X,1}$, which is given as follows:

$$c^U_{X,1} = \kappa + \frac{\delta_1}{2}. \tag{9}$$

Therefore, the phase error rate of the single-photon events in the Z-basis ϕ_Z is given by

$$\phi_Z = \left(\kappa + \frac{\delta_1}{2}\right) + \gamma\left(\epsilon_{sec}, \left(\kappa + \frac{\delta_1}{2}\right), s^L_{X,1}, s^L_{Z,1}\right), \tag{10}$$

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

The secret key length l of the decoy-state few-state QKD protocol can be calculated as follows:

$$\begin{aligned} l \geqslant & s^L_{Z,0} + s^L_{Z,1} - [1 - H(\phi_Z)] - \mathrm{Leak}_{EC} \\ & - \log_2\frac{2}{\epsilon_{cor}} - 6\log_2\frac{21}{\epsilon_{sec}}, \end{aligned} \tag{11}$$

where the lower bounds of the number of vacuum events and single-photon events $s^L_{Z,0}$, $s^L_{Z,1}$ can be directly calculated in the Z-basis. $\mathrm{Leak}_{EC} = n_Z f_{EC} h(e_Z)$ 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 for correctness and secrecy, respectively.

The secret key rate is $R = l/N$, where N is the total number of quantum signals transmitted by Alice. For the two-basis three-state QKD protocol with finite key length, the simulation results of the secret key rate under different values of δ_1 are shown in Figure 1, where the simulation parameters are shown in Appendix E.

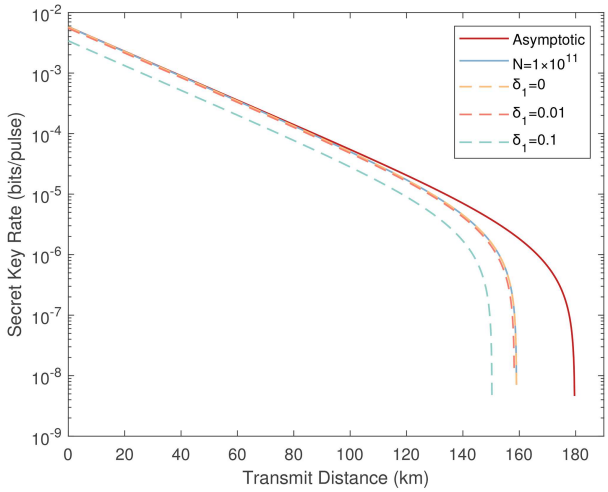

Figure 1 (Color online) The secret key rate of the two-basis three-state QKD protocol with finite key length under different parameters δ_1. For comparison, we plot the secret key rate of the asymptotic decoy-state QKD protocol, represented by the red solid line. The blue solid line represents the secret key rate of the finite-key decoy-state QKD protocol with $N = 1 \times 10^{11}$. The dashed line shows the secret key rates for different offset values (from left to right, the offset values are $0.1, 0.01$, and 0, respectively).

From the simulation results, we can find that the transmission distance gradually increases as δ_1 decreases. When δ_1 is small enough, the transmission distance can be similar to that of the original QKD protocol.

In this work, we propose a simple and general method for analyzing few-state QKD protocols based on the VMUB method. In the case of $\delta_1 = 0$, our analysis results indicate that the few-state QKD protocol can achieve the same secret key rate as the original QKD protocol. On the one hand, our method only needs to utilize the mismatched basis information to analyze the secret key rate, and thus does not impose additional requirements on QKD devices. On the other hand, our method can reduce the consumption of random numbers and simplify the design of physical devices. In addition, our method can also be applied to improve the robustness and performance of different QKD systems. It would be valuable to extend our method to various QKD systems in the future.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. U2130205) and Natural Science Foundation of Henan (Grant No. 242300421219).

Supporting information Appendixes A–E. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices. Rev Mod Phys, 2020, 92: 025002
2 Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution. Nature, 2017, 549: 43–47
3 Xie Z, Tian Z, Fan X, et al. Four-state reference-frame-independent quantum key distribution over 200 km. Phys Rev Appl, 2024, 22: 064037
4 Li H W, Hao C P, Chen Z J, et al. Security of quantum key distribution with virtual mutually unbiased bases. Sci China-Phys Mech Astron, 2024, 67: 270313
5 Renner R. Security of quantum key distribution. Int J Quantum Inform, 2008, 06: 1–127