Supplemental Document

Optics Letters

Reference-frame-independent measurement-device-independent quantum key distribution with mismatched-basis statistics: supplement

ZHENHUA LI,[1] HONGWEI LIU,[2] JIPENG WANG,[1] SHUNYU YANG,[1] TIANQI DOU,[1] WENXIU QU,[1] FEN ZHOU,[1] YUQING HUANG,[1] ZHONGQI SUN,[1] YANXIN HAN,[1] GUOXING MIAO,[3,4] AND HAIQIANG MA[1,3,*]

[1]*School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*China Information Technology Security Evaluation Center, Beijing 100085, China*
[3]*Institute for Quantum Computing, Department of Chemistry, Department of Physics and Astronomy, and Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[4]*e-mail: guo-xing.miao@uwaterloo.ca*
[*]*Corresponding author: hqma@bupt.edu.cn*

Supplement DOI: https://doi.org/10.6084/m9.figshare.13089611

Parent Article DOI: https://doi.org/10.1364/OL.403481

Reference-frame-independent measurement-device-independent quantum key distribution with mismatched-basis statistics: Supplementary material

This document provides supplementary information to "Reference-frame-independent measurement-device-independent quantum key distribution with mismatched-basis statistics". For completeness, we first review the step of the Reference-frame-independent measurement-device-independent quantum key distribution protocol with discarded mismatched-basisstatistics and uncharacterized qubit source. Subsequently, we provide the derivation procedure of crucial equations.

1. THE URFI-MDI-QKD PROTOCOL STEPS

The RFI-MDI-QKD protocol with discarded mismatched-basis statistics and uncharacterized qubit source (URFI-MDI-QKD) is set up as follows. The use of time-bin coding (Z basis) and phase coding (X basis and Y basis) was assumed. The X basis and Y basis can be characterized according to the Z basis, meaning the encoding state is in the two-dimensional Hilbert space. For convenience, we assume that $|0\rangle = |Z_0\rangle$, $|1\rangle = |Z_1\rangle$, $|2\rangle = |X_0\rangle$, $|3\rangle = |X_1\rangle$, $|4\rangle = |Y_0\rangle$ and $|5\rangle = |Y_1\rangle$. The communication parties Alice and Bob can send the pure quantum state $\rho_{A,a}$ and $\rho_{B,b}$ to the measurement terminal of an untrusted third party (Considering the worst case, it is assumed to be Eve.) via the quantum channels, where $a(b) \in [0,1,2,3,4,5]$. The quantum states sent by the Alice and Bob can be changed due to the imperfection of the experimental equipment or though Eve's eavesdropping activity. Therefore, Alice and Bob may not be able to characterize the quantum states they sent in detail. The defect of the experimental equipment and Eve's activity are defined as ρ_{Eve}. Therefore, Eve performs Bell state measurements (BSM) on the received quantum states $\rho_{A,a} \otimes \rho_{B,b} \otimes \rho_{Eve}$ and announces the measurement results to Alice and Bob. It is worth noting that Eve can only distinguish the results of one of the BSM and declare it successful, while the other cases will be considered as failed measurements. The entanglement distillation protocol (EDP) [1, 2] method is widely used for the security proofs of QKD. Here, we use the EDP to describe the protocol process in detail.

1. State preparation. Alice and Bob prepare the N pairs of entangled states,

$$\begin{aligned} |\phi^+\rangle_{AA'} =& \sqrt{\frac{1}{6}}(|0\rangle_A |\varphi_0\rangle_{A'} + |1\rangle_A |\varphi_1\rangle_{A'} + |2\rangle_A |\varphi_2\rangle_{A'} \\ &+ |3\rangle_A |\varphi_3\rangle_{A'} + |4\rangle_A |\varphi_4\rangle_{A'} + |5\rangle_A |\varphi_5\rangle_{A'}), \\ |\phi^+\rangle_{BB'} =& \sqrt{\frac{1}{6}}(|0\rangle_B |\varphi_0\rangle_{B'} + |1\rangle_B |\varphi_1\rangle_{B'} + |2\rangle_B |\varphi_2\rangle_{B'} \\ &+ |3\rangle_B |\varphi_3\rangle_{B'} + |4\rangle_B |\varphi_4\rangle_{B'} + |5\rangle_B |\varphi_5\rangle_{B'}), \end{aligned} \tag{S1}$$

respectively. Here, $|a\rangle_A$ and $|b\rangle_B$ $(a(b) \in [0,1,2,3,4,5])$ denote both Alice's and Bob's selected basis and raw key bit, respectively, while $|\varphi_a\rangle_{A'}$ and $|\varphi_b\rangle_{B'}$ are Alice's and Bob's uncharacterized encoding qubits to be sent to Eve. Alice and Bob know that $|\varphi_a\rangle_{A'}$ and $|\varphi_b\rangle_{B'}$ are two-dimensional states but do not know the details, since they do not trust the accuracies of their encoding systems. Eq. (S1) shows that the probability of sending each quantum state is the same.

2. Measurement. Alice and Bob send $|\varphi_a\rangle_{A'}$ and $|\varphi_b\rangle_{B'}$ to Eve who performs BSM and declares the measurement results. Here, it should be noted that Eve may be dishonest and may declare the contradictory results. There are two possible outcomes: BSM failure or a successful measurement result in the Bell states: $|\phi^+\rangle_{A'B'} = \frac{1}{\sqrt{2}}(|0\rangle_{A'}|0\rangle_{B'} + |1\rangle_{A'}|1\rangle_{B'})$. Regardless of the honesty of Eve, she must declare the results after each measurement.

3. Bit and basis sifting. After receiving Eve's measurement results through the classic channels, Alice and Bob perform bit sifting, which involves discarding the failed measurement results

and retaining the successful measurement results. They can then project systems A and B in Eq. (S1) onto $|0\rangle|0\rangle+|1\rangle|1\rangle$, $|2\rangle|2\rangle+|3\rangle|3\rangle$ or $|4\rangle|4\rangle+|5\rangle|5\rangle$, which correspond with the Z basis, X basis, and Y basis, respectively. Next, Alice and Bob can perform basis sifting. When their systems collapse into the same or a different basis, they can obtain the counting rate $p(a,b)$.

4. Entangled distillation. Alice and Bob can perform the entanglement distillation operation and obtain the maximum entangled Bell state $\left|\phi^{+\theta}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B+e^{i\theta}|1\rangle_A|1\rangle_B\right)$, where secret key bits can be extracted.

2. THE DERIVATION PROCEDURE OF CRUCIAL EQUATIONS

According to the protocol mentioned above and the previous research [3, 4], the encoding state is in the two-dimensional Hilbert space. Thus we can know that

$$\begin{aligned}
|\varphi_0\rangle_{A'} &= k_{02}|\varphi_2\rangle_{A'}+k_{03}e^{i\beta_0}|\varphi_3\rangle_{A'}\\
|\varphi_1\rangle_{A'} &= k_{12}|\varphi_2\rangle_{A'}+k_{13}e^{i\beta_1}|\varphi_3\rangle_{A'}\\
|\varphi_0\rangle_{B'} &= k'_{02}|\varphi_2\rangle_{B'}+k'_{03}e^{i\beta'_0}|\varphi_3\rangle_{B'}\\
|\varphi_1\rangle_{B'} &= k'_{12}|\varphi_2\rangle_{B'}+k'_{13}e^{i\beta'_1}|\varphi_3\rangle_{B'}
\end{aligned} \tag{S2}$$

where k and k' are non-negative real number and β denotes real number.

The most general collective attack by Eve can be represented by a unitary transformation as follows:

$$U_{Eve}|\varphi_a\rangle_{A'}|\varphi_b\rangle_{B'}|e\rangle_{Ea}|0\rangle_M=\sqrt{p(0|a,b)}|\Gamma_{ab0}\rangle_E|0\rangle_M+\sqrt{p(1|a,b)}|\Gamma_{ab1}\rangle_E|1\rangle_M \tag{S3}$$

where $p(0|a,b)$ and $p(1|a,b)$ are the counting rate when the measurement fails and succeeds respectively, $|e\rangle_{Ea}$ is Eve's arbitrary ancilla, $|0\rangle_M$ is the message which will be sent to Alice and Bob, $|\Gamma_{ab0}\rangle_E$ and $|\Gamma_{ab1}\rangle_E$ are all normalized Eve's arbitrary quantum states for Eve's ancilla and photons A', B'. $|\Gamma\rangle_E$ can be expanded by a set of normalized orthogonal basis $|n\rangle_E$ (i.e. $|\Gamma\rangle_E=\sum_n\gamma_n|n\rangle_E$, where the complex number $\gamma_n={}_E\langle n\mid\Gamma\rangle_E$ and $\sum_n|\gamma_n|^2=1$). And we assume $p(a,b)=p(1|a,b)$. Thus, in the case that both Alice and Bob send X basis, the density matrix of the system is:

$$\rho=\frac{\sum_n P\left\{\begin{array}{l}\sqrt{p(2,2)}\gamma_{221n}|2\rangle_A|2\rangle_B+\sqrt{p(3,3)}\gamma_{331n}|3\rangle_A|3\rangle_B\\ +\sqrt{p(2,3)}\gamma_{231n}|2\rangle_A|3\rangle_B+\sqrt{p(3,2)}\gamma_{221n}|3\rangle_A|2\rangle_B\end{array}\right\}}{p(2,2)+p(3,3)+p(2,3)+p(3,2)}, \tag{S4}$$

where $P\{x\}=|x\rangle\langle x|$. Considering the target Bell state (X base) of the entanglement distillation operation is: $\left|\phi^{+\alpha}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(|2\rangle_A|2\rangle_B+e^{i(\alpha_A+\alpha_B)}|3\rangle_A|3\rangle_B\right)$. The bit error rate E_{XX}^{bit} and phase error rate E_{XX}^{phase} can be expressed as follows:

$$\begin{aligned}
E_{XX}^{bit} &= {}_A\langle 2|{}_B\langle 3|\rho|3\rangle_B|2\rangle_A+{}_A\langle 3|{}_B\langle 2|\rho|2\rangle_B|3\rangle_A\\
&= \frac{p(2,3)+p(3,2)}{p(2,2)+p(3,3)+p(2,3)+p(3,2)},
\end{aligned} \tag{S5}$$

$$\begin{aligned}
E_{\mathrm{XX}}^{phase} &= {}_{AB}\left\langle\phi^{-\alpha}\right|\rho\left|\phi^{-\alpha}\right\rangle_{AB}+{}_{AB}\left\langle\psi^{-\alpha}\right|\rho\left|\psi^{-\alpha}\right\rangle_{AB}\\
&= \frac{\left\{\begin{array}{l}\Sigma_n\left|\sqrt{p(2,2)}\gamma_{221n}-e^{-i(\alpha_A+\alpha_B)}\sqrt{p(3,3)}\gamma_{331n}\right|^2\\ +\Sigma_n\left|\sqrt{p(2,3)}\gamma_{231n}-e^{-i(\alpha_A-\alpha_B)}\sqrt{p(3,2)}\gamma_{321n}\right|^2\end{array}\right\}}{2\left(p(2,2)+p(3,3)+p(2,3)+p(3,2)\right)}\\
&\leq \frac{\Sigma_n\left|\sqrt{p(2,2)}\gamma_{221n}-e^{-i(\alpha_A+\alpha_B)}\sqrt{p(3,3)}\gamma_{331n}\right|^2}{2\left(p(2,2)+p(3,3)+p(2,3)+p(3,2)\right)}+E_{XX}^{bit},
\end{aligned} \tag{S6}$$

where $\left|\phi^{-\alpha}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(\left|2\right\rangle\left|2\right\rangle-e^{-i(\alpha_A+\alpha_B)}\left|3\right\rangle\left|3\right\rangle\right)$ and $\left|\varphi^{-\alpha}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\left(\left|2\right\rangle\left|3\right\rangle-e^{-i(\alpha_A-\alpha_B)}\left|3\right\rangle\left|2\right\rangle\right)$. According to Eq. (S2, S3) , we can obtain:

$$\left(\begin{array}{l}k_{a2}k_{b2}^{'}\sqrt{p\left(2,2\right)}|\Gamma_{221}\rangle_E+k_{a2}k_{b3}^{'}e^{i\beta_b^{'}}\sqrt{p\left(2,3\right)}|\Gamma_{231}\rangle_E\\+k_{a3}k_{b2}^{'}e^{i\beta_a}\sqrt{p\left(3,2\right)}|\Gamma_{321}\rangle_E+k_{a3}k_{b3}^{'}e^{i\left(\beta_a+\beta_b^{'}\right)}\sqrt{p\left(3,3\right)}|\Gamma_{231}\rangle_E\end{array}\right)=\sqrt{p\left(a,b\right)}|\Gamma_{ab1}\rangle_E. \quad \text{(S7)}$$

Considering that $|\Gamma\rangle_E$ can be expanded by a set of normalized orthogonal basis $|n\rangle_E$, we can get the following constraints:

$$\begin{aligned}&\Sigma_n\left|k_{12}k_{02}^{'}\sqrt{p\left(2,2\right)}\gamma_{221n}+k_{13}k_{03}^{'}e^{i\left(\beta_1+\beta_0^{'}\right)}\sqrt{p\left(3,3\right)}\gamma_{331n}\right|^2\\&\leq\left(\sqrt{p\left(1,0\right)}+\sqrt{p\left(2,3\right)}k_{12}k_{03}^{'}+\sqrt{p\left(3,2\right)}k_{13}k_{02}^{'}\right)^2,\end{aligned} \quad \text{(S8)}$$

when $a=1$ and $b=0$. Relying on triangle inequality and Cauchy-Schwarz inequality, we have

$$\begin{aligned}&\Sigma_n\left|k_{12}k_{02}^{'}\sqrt{p\left(2,2\right)}\gamma_{221n}+k_{13}k_{03}^{'}e^{i\left(\beta_1+\beta_0^{'}\right)}\sqrt{p\left(3,3\right)}\gamma_{331n}\right|^2\\&\geq\Sigma_n\left(k_{12}k_{02}^{'}\left|\sqrt{p\left(2,2\right)}\gamma_{221n}+\sqrt{p\left(3,3\right)}e^{i\left(\beta_1+\beta_0^{'}\right)}\gamma_{331n}\right|-\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p\left(3,3\right)}\left|\gamma_{331n}\right|\right)^2\\&=k_{12}^2k_{02}^{'2}\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}+\sqrt{p\left(3,3\right)}e^{i\left(\beta_1+\beta_0^{'}\right)}\gamma_{331n}\right|^2+\left(k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right)^2p\left(3,3\right)\\&-2k_{12}k_{02}^{'}\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p\left(3,3\right)}\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}+\sqrt{p\left(3,3\right)}e^{i\left(\beta_1+\beta_0^{'}\right)}\gamma_{331n}\right|\left|\gamma_{331n}\right|\\&\geq k_{12}^2k_{02}^{'2}\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}+\sqrt{p\left(3,3\right)}e^{i\left(\beta_1+\beta_0^{'}\right)}\gamma_{331n}\right|^2+\left(k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right)^2p\left(3,3\right)\\&-2k_{12}k_{02}^{'}\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p\left(3,3\right)}\sqrt{\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}+\sqrt{p\left(3,3\right)}e^{i\left(\beta_1+\beta_0^{'}\right)}\gamma_{331n}\right|^2\Sigma_n\left|\gamma_{331n}\right|^2}\\&=\left(k_{12}k_{02}^{'}\sqrt{\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}+\sqrt{p\left(3,3\right)}e^{i\left(\beta_1+\beta_0^{'}\right)}\gamma_{331n}\right|^2}-\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p\left(3,3\right)}\right)^2\end{aligned} \quad \text{(S9)}$$

Combining with Eq. (S8) and Eq. (S9) we can obtain

$$\begin{aligned}&\frac{\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}-e^{-i\left(\beta_1+\beta_0^{'}\right)}\sqrt{p\left(3,3\right)}\gamma_{331n}\right|^2}{2\left(p\left(2,2\right)+p\left(3,3\right)+p\left(2,3\right)+p\left(3,2\right)\right)}\\&\leq\begin{cases}\frac{\left(\sqrt{p(1,0)}+\sqrt{p(2,3)}k_{12}k_{03}^{'}+\sqrt{p(3,2)}k_{13}k_{02}^{'}+\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p(3,3)}\right)^2}{2(p(2,2)+p(3,3)+p(2,3)+p(3,2))k_{12}^2k_{02}^{'2}}, & \text{if}\quad k_{12}^2k_{02}^{'2}\neq0\\1-E_{XX}^{bit}. & \text{if}\quad k_{12}^2k_{02}^{'2}=0\end{cases}\end{aligned} \quad \text{(S10)}$$

Similarly, we can obtain

$$\begin{aligned}&\frac{\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}-e^{-i\left(\beta_1+\beta_0^{'}\right)}\sqrt{p\left(3,3\right)}\gamma_{331n}\right|^2}{2\left(p\left(2,2\right)+p\left(3,3\right)+p\left(2,3\right)+p\left(3,2\right)\right)}\\&\leq\begin{cases}\frac{\left(\sqrt{p(1,0)}+\sqrt{p(2,3)}k_{12}k_{03}^{'}+\sqrt{p(3,2)}k_{13}k_{02}^{'}+\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p(2,2)}\right)^2}{2(p(2,2)+p(3,3)+p(2,3)+p(3,2))k_{13}^2k_{03}^{'2}}, & \text{if}\quad k_{13}^2k_{03}^{'2}\neq0\\1-E_{XX}^{bit}, & \text{if}\quad k_{13}^2k_{03}^{'2}=0\end{cases}\end{aligned} \quad \text{(S11)}$$

when $a=0$ and $b=1$.
According to Eq. (S10, S11), there is

$$\frac{\Sigma_n\left|\sqrt{p\left(2,2\right)}\gamma_{221n}-e^{-i\left(\beta_1+\beta_0^{'}\right)}\sqrt{p\left(3,3\right)}\gamma_{331n}\right|^2}{2\left(p\left(2,2\right)+p\left(3,3\right)+p\left(2,3\right)+p\left(3,2\right)\right)}\leq\max_{k,k^{'}}f\left(k,k^{'}\right), \quad \text{(S12)}$$

where

$$f(k,k^{'})=\begin{cases}\min\{A,B\}, & \text{if} \quad k_{12}^{2}k_{02}^{'2}\neq 0 \quad \text{and} \quad k_{13}^{2}k_{03}^{'2}\neq 0\\ A, & \text{if} \quad k_{12}^{2}k_{02}^{'2}\neq 0 \quad \text{and} \quad k_{13}^{2}k_{03}^{'2}=0\\ B, & \text{if} \quad k_{12}^{2}k_{02}^{'2}=0 \quad \text{and} \quad k_{13}^{2}k_{03}^{'2}\neq 0\\ 1-E_{XX}^{Bit}, & \text{if} \quad k_{12}^{2}k_{02}^{'2}=0 \quad \text{and} \quad k_{13}^{2}k_{03}^{'2}=0\end{cases} \tag{S13}$$

$$A=\frac{\left(\sqrt{p\left(1,0\right)}+\sqrt{p\left(2,3\right)}k_{12}k_{03}^{'}+\sqrt{p\left(3,2\right)}k_{13}k_{02}^{'}+\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p\left(3,3\right)}\right)^{2}}{2\left(p\left(2,2\right)+p\left(3,3\right)+p\left(2,3\right)+p\left(3,2\right)\right)k_{12}^{2}k_{02}^{'2}}, \tag{S14}$$

and

$$B=\frac{\left(\sqrt{p\left(1,0\right)}+\sqrt{p\left(2,3\right)}k_{12}k_{03}^{'}+\sqrt{p\left(3,2\right)}k_{13}k_{02}^{'}+\left|k_{12}k_{02}^{'}-k_{13}k_{03}^{'}\right|\sqrt{p\left(2,2\right)}\right)^{2}}{2\left(p\left(2,2\right)+p\left(3,3\right)+p\left(2,3\right)+p\left(3,2\right)\right)k_{13}^{2}k_{03}^{'2}}. \tag{S15}$$

Next, we calculate the constraint condition of the variable k and $k^{'}$. It can be deduced from Eq. (S3) that

$$\left|\langle 1|_{M}U_{Eve}|\varphi_{a}\rangle_{A^{'}}|\varphi_{b}\rangle_{B^{'}}|e\rangle_{Ea}|0\rangle_{M}\right|^{2}=p\left(a,b\right). \tag{S16}$$

Thus, we can obtain

$$\begin{aligned}
&k_{12}^{2}p\left(2,2\right)+k_{13}^{2}p\left(3,2\right)+2k_{12}k_{13}\sqrt{p\left(2,2\right)}\sqrt{p\left(3,2\right)}\mathrm{Re}\left(e^{i\beta_{1}}{}_{E}\left\langle\Gamma_{221}\right|\left.\Gamma_{321}\right\rangle_{E}\right)=p\left(1,2\right),\\
&k_{12}^{2}p\left(2,3\right)+k_{13}^{2}p\left(3,3\right)+2k_{12}k_{13}\sqrt{p\left(2,3\right)}\sqrt{p\left(3,3\right)}\mathrm{Re}\left(e^{i\beta_{1}}{}_{E}\left\langle\Gamma_{231}\right|\left.\Gamma_{331}\right\rangle_{E}\right)=p\left(1,3\right),\\
&k_{02}^{'2}p\left(2,2\right)+k_{03}^{'2}p\left(2,3\right)+2k_{02}^{'}k_{03}^{'}\sqrt{p\left(2,2\right)}\sqrt{p\left(2,3\right)}\mathrm{Re}\left(e^{i\beta_{0}^{'}}{}_{E}\left\langle\Gamma_{221}\right|\left.\Gamma_{231}\right\rangle_{E}\right)=p\left(2,0\right),\\
&k_{02}^{'2}p\left(3,2\right)+k_{03}^{'2}p\left(3,3\right)+2k_{02}^{'}k_{03}^{'}\sqrt{p\left(3,2\right)}\sqrt{p\left(3,3\right)}\mathrm{Re}\left(e^{i\beta_{0}^{'}}{}_{E}\left\langle\Gamma_{321}\right|\left.\Gamma_{331}\right\rangle_{E}\right)=p\left(3,0\right).
\end{aligned} \tag{S17}$$

where $\mathrm{Re}\left(x\right)$ returns the real part of a complex number x. By numerical computation, we can obtain the boundary conditions of k and k' as:

$$\begin{aligned}
&\left|p\left(1,2\right)-k_{12}^{2}p\left(2,2\right)-k_{13}^{2}p\left(3,2\right)\right|\leq 2k_{12}k_{13}\sqrt{p\left(2,2\right)}\sqrt{p\left(3,2\right)},\\
&\left|p\left(1,3\right)-k_{12}^{2}p\left(2,3\right)+k_{13}^{2}p\left(3,3\right)\right|\leq 2k_{12}k_{13}\sqrt{p\left(2,3\right)}\sqrt{p\left(3,3\right)},\\
&\left|p\left(2,0\right)-k_{02}^{'2}p\left(2,2\right)-k_{03}^{'2}p\left(2,3\right)\right|\leq 2k_{02}^{'}k_{03}^{'}\sqrt{p\left(2,2\right)}\sqrt{p\left(2,3\right)},\\
&\left|p\left(3,0\right)-k_{02}^{'2}p\left(3,2\right)-k_{03}^{'2}p\left(3,3\right)\right|\leq 2k_{02}^{'}k_{03}^{'}\sqrt{p\left(3,2\right)}\sqrt{p\left(3,3\right)}.
\end{aligned} \tag{S18}$$

Finally, the phase error rate of the XY basis, the YX basis and the YY basis can be obtained in the same way.

REFERENCES

1. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).
2. P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441 (2000).
3. Z.-Q. Yin, C.-H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Measurement-device-independent quantum key distribution with uncharacterized qubit sources," Phys. Rev. A **88**, 062322 (2013).
4. Z.-Q. Yin, C.-H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources," Phys. Rev. A **90**, 052319 (2014).