

Improved decoy-state quantum key distribution with uncharacterized heralded single-photon sources

Le-Chen Xu(徐乐辰), Chun-Hui Zhang(张春辉), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)

Citation: Chin. Phys. B, 2024, 33 (**2**): 020313. DOI: 10.1088/1674-1056/ad062a
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Improved statistical fluctuation analysis for two decoy-states phase-matching quantum key distribution

Jiang-Ping Zhou(周江平), Yuan-Yuan Zhou(周媛媛), Xue-Jun Zhou(周学军), and Xuan Bao(暴轩)
Chin. Phys. B, 2023, 32 (**8**): 080306. DOI: 10.1088/1674-1056/acbdea

Improved statistical fluctuation analysis for two decoy-states phase-matching quantum key distribution

Jiang-Ping Zhou(周江平), Yuan-Yuan Zhou(周媛媛), Xue-Jun Zhou(周学军), and Xuan Bao(暴轩)
Chin. Phys. B, 2023, 32 (**8**): 080306. DOI: 10.1088/1674-1056/acbdea

Phase-matching quantum key distribution with imperfect sources

Xiao-Xu Zhang(张晓旭), Yi-Fei Lu(陆宜飞), Yang Wang(汪洋), Mu-Sheng Jiang(江木生), Hong-Wei Li(李宏伟), Chun Zhou(周淳), Yu Zhou(周雨), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2023, 32 (**5**): 050308. DOI: 10.1088/1674-1056/ac9b03

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

Yu Zhou(周雨), Hong-Wei Li(李宏伟), Chun Zhou(周淳), Yang Wang(汪洋), Yi-Fei Lu(陆宜飞),Mu-Sheng Jiang(江木生), Xiao-Xu Zhang(张晓旭), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2023, 32 (**5**): 050305. DOI: 10.1088/1674-1056/ac8730

Security of the traditional quantum key distribution protocols with finite-key lengths

Bao Feng(冯宝), Hai-Dong Huang(黄海东), Yu-Xiang Bian(卞宇翔), Wei Jia(贾玮), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)
Chin. Phys. B, 2023, 32 (**3**): 030307. DOI: 10.1088/1674-1056/ac9b33

Improved decoy-state quantum key distribution with uncharacterized heralded single-photon sources

Le-Chen Xu(徐乐辰)[1,2,3], Chun-Hui Zhang(张春辉)[1,2,3], Xing-Yu Zhou(周星宇)[1,2,3], and Qin Wang(王琴)[1,2,3,†]

[1] *Institute of Quantum Information and Technology, Nanjing* 210003, *China*
[2] *Broadband Wireless Communication and Sensor Network Technology, Key Laboratory of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[3] *Telecommunication and Networks National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 12 September 2023; revised manuscript received 13 October 2023; accepted manuscript online 24 October 2023)

Encoding system plays a significant role in quantum key distribution (QKD). However, the security and performance of QKD systems can be compromised by encoding misalignment due to the inevitable defects in realistic devices. To alleviate the influence of misalignments, a method exploiting statistics from mismatched basis is proposed to enable uncharacterized sources to generate secure keys in QKD. In this work, we propose a scheme on four-intensity decoy-state quantum key distribution with uncharacterized heralded single-photon sources. It only requires the source states are prepared in a two-dimensional Hilbert space, and can thus reduce the complexity of practical realizations. Moreover, we carry out corresponding numerical simulations and demonstrate that our present four-intensity decoy-state scheme can achieve a much higher key rate compared than a three-intensity decoy-state method, and meantime it can obtain a longer transmission distance compared than the one using weak coherent sources.

Keywords: quantum key distribution, heralded single-photon source, decoy-state method

PACS: 03.67.Dd, 03.67.Hk, 42.65.Lm **DOI:** 10.1088/1674-1056/ad062a

1. Introduction

Quantum key distribution (QKD),[1,2] based on the fundamental laws of physics,[3,4] allows two distant parties, Alice and Bob, to share secret keys in the presence of a malicious eavesdropper, Eve. Since the first QKD protocol (BB84) was proposed in 1984,[1] a great number of QKD experiments have been reported.[5–12] In most previous QKD protocols and corresponding security proofs,[13–19] people often assume the prepared states are perfect. However, preparation flaws inevitably exist in real-life situations due to the imperfect devices, resulting in reduced security of practical QKD systems.

To alleviate the influence of state preparations flaws, Tamaki *et al.*[20] presented a loss-tolerant protocol, but it requires full characterization of the preparation states and causes increased system complexity. Fortunately, Yin *et al.*[21] proposed a QKD protocol without characterizing misalignment errors and the only assumption is that the quantum states are prepared in a two-dimensional Hilbert space. With which the secret keys can be extracted out using uncharacterized sources by exploiting the mismatched-basis statistics which are normally discarded, and related experiments have been successfully demonstrated.[22–24]

Based on those previous works,[21–23] here we present a four-intensity decoy-state proposal on quantum key distribution using uncharacterized heralded single-photon sources (HSPS). First, the four-intensity scheme with biased basis can help to improve the key rate compared with the standard three-intensity method.[22,23] Second, by employing the intrinsic advantages of HSPS with a higher single-photon probability and a lower dark count rate compared with weak coherent sources (WCS),[25,26] one can obtain not only a much longer secure transmission distance, but also a higher key rate, compared with previous similar works.[22,23]

2. Protocol description

In our four-intensity BB84 protocol, Alice randomly modulates each pulse into one of the four different intensities, i.e., the signal state μ, the decoy states ν and ω, and the vacuum state o. However, different from the standard three-intensity method, Alice only prepares the signal pulses in basis $Z_{\rm A}$ and randomly prepares the decoy pulses in basis $Z_{\rm A}$ or basis $X_{\rm A}$. Considering typical encoding misalignments, Alice randomly prepares quantum states $|\varphi_0\rangle = |0\rangle, |\varphi_1\rangle = \sin a\,|0\rangle + \cos a\,|1\rangle, |\varphi_2\rangle = \cos(\pi/4+b)\,|0\rangle + \sin(\pi/4+b)\,|1\rangle, |\varphi_3\rangle = \sin(\pi/4+c)\,|0\rangle - \cos(\pi/4+c)\,|1\rangle$, in which the degrees of angles a, b, and c are the encoding misalignments. We define that basis $Z_{\rm A}$ consists of $|\varphi_0\rangle$ and $|\varphi_1\rangle$, while basis $X_{\rm A}$ consists of $|\varphi_2\rangle$ and $|\varphi_3\rangle$. Besides, we make the assumption that Bob performs projective measurement on the received states to ensure protocol security.[21] Let Bob's measurement for basis $Z_{\rm B}$ be a projection onto $\{|\bar{\varphi}_0\rangle, |\bar{\varphi}_1\rangle\}$, and for basis $X_{\rm B}$ be $\{|\bar{\varphi}_2\rangle, |\bar{\varphi}_3\rangle\}$, where $\langle\bar{\varphi}_0|\bar{\varphi}_1\rangle = \langle\bar{\varphi}_2|\bar{\varphi}_3\rangle = 0$ and $|\bar{\varphi}_0\rangle\langle\bar{\varphi}_0| + |\bar{\varphi}_1\rangle\langle\bar{\varphi}_1| = |\bar{\varphi}_2\rangle\langle\bar{\varphi}_2| + |\bar{\varphi}_3\rangle\langle\bar{\varphi}_3| = I$. After basis sifting, the number of detected pulses can be obtained,

†Corresponding author. E-mail: qinw@njupt.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

of which matched-basis events are kept as sifted keys and mismatched-basis events are used to estimate the information leaked to Eve.

By sacrificing some bits from matched-basis events and revealing all bits from mismatched-basis events, we can deduce conditional probability distribution $P_\lambda(y|x)$, where $\lambda \in \{\mu,\nu,\omega,o\}, x \in \{|\varphi_0\rangle,|\varphi_1\rangle,|\varphi_2\rangle,|\varphi_3\rangle\}$ and $y \in \{|\bar{\varphi}_0\rangle,|\bar{\varphi}_1\rangle,|\bar{\varphi}_2\rangle,|\bar{\varphi}_3\rangle\}$. For simplicity, we assign value 0 to $|\varphi_0\rangle$ and $|\bar{\varphi}_0\rangle$, value 1 to $|\varphi_1\rangle$ and $|\bar{\varphi}_1\rangle$, value 2 to $|\varphi_2\rangle$ and $|\bar{\varphi}_2\rangle$, and value 3 to $|\varphi_3\rangle$ and $|\bar{\varphi}_3\rangle$. $P_\lambda(y|x)$ can be expressed as follows:

$$P_\lambda(y|x)=\sum_{i=0}^{\infty}P_i(\lambda)\sum_{j=0}^{i}C_i^j\eta_t^i(1-\eta_t)^{i-j}\left(|\langle x|y\rangle|^2\right)^j F(j), \tag{1}$$

$\eta_t=\eta 10^{-\alpha l/10}$ represents the total transmission and detection efficiency, where η represents the detection efficiency of the single-photon detector, α denotes the loss coefficient of standard optical fibers and L denotes the fiber length. $F(j)$ represents the probability of the valid detection events (those only one detector clicks) on j-photon states, such as

$$F(j)=\begin{cases}(1-d), & \text{if } j>0,\\ d(1-d), & \text{if } j=0,\end{cases} \tag{2}$$

where d represents the dark count rate of the single-photon detector and $P_i(\lambda)$ is the photon number distribution of the light sources. Here, we take HSPS as the uncharacterized source. Through a parametric down-conversion process, a two-mode state, including the idler mode and the signal mode,[27] is generated in HSPS. The idler modes are detected by Alice's local single-photon detector working as heralding signals and the signal modes will be encoded and sent out to Bob. The photon number distribution of HSPS can be expressed as[26]

$$P_i(\lambda)=\left[1-(1-d_{\rm A})(1-\eta_{\rm A})^i\right]\frac{\lambda^i}{i!}\mathrm{e}^{-\lambda}, \tag{3}$$

where $d_{\rm A}$ and $\eta_{\rm A}$ each denote the dark count rate and the detection efficiency of Alice's local detector, respectively.

With Eqs. (1)–(3), we can obtain the expression of each observable $M_\lambda(y|x)$, namely the number of valid detections at Bob's side after sifting. Considering statistical fluctuation, we use method in Refs. [28,29] to account for the finite-size key effects, which provides a tighter bound for the deviation between ideal expectations and actual observations. Then, the underlying expectation value of $M_\lambda(y|x)$ for a given failure probability ε is

(i) if $M_\lambda(y|x)=0$

$$\begin{aligned}M_\lambda(y|x)^{\rm L}&=0,\\ M_\lambda(y|x)^{\rm U}&=-\ln\left(\frac{\varepsilon}{2}\right),\end{aligned} \tag{4}$$

(ii) if $M_\lambda(y|x)>0$

$$\begin{aligned}M_\lambda(y|x)^{\rm L}&=\frac{M_\lambda(y|x)}{1+\delta^{\rm L}},\\ M_\lambda(y|x)^{\rm U}&=\frac{M_\lambda(y|x)}{1-\delta^{\rm U}},\end{aligned} \tag{5}$$

where $\delta^{\rm L}$ and $\delta^{\rm U}$ can be obtained by solving the following equations:[28]

$$\begin{aligned}\left[\frac{\mathrm{e}^{\delta^{\rm L}}}{(1+\delta^{\rm L})^{1+\delta^{\rm L}}}\right]^{M_\lambda(y|x)/(1+\delta^{\rm L})}&=\frac{1}{2}\varepsilon,\\ \left[\frac{\mathrm{e}^{-\delta^{\rm U}}}{(1-\delta^{\rm L})^{1-\delta^{\rm L}}}\right]^{M_\lambda(y|x)/(1-\delta^{\rm U})}&=\frac{1}{2}\varepsilon.\end{aligned} \tag{6}$$

If $M_\lambda(y|x)\geq -6\ln(\varepsilon/2)$

$$\delta^{\rm L}=\delta^{\rm U}=\frac{-3\ln(\varepsilon/2)+\sqrt{-8M_\lambda(y|x)\ln(\varepsilon/2)+\ln(\varepsilon/2)^2}}{2\left(M_\lambda(y|x)+\ln(\varepsilon/2)\right)}. \tag{7}$$

With Eqs. (4)–(7), the expectation value of $P_\lambda(y|x)$ can be bounded as

$$\begin{aligned}P_\lambda(y|x)^{\rm L}&=\frac{M_\lambda(y|x)^{\rm L}}{N_\lambda(y|x)},\\ P_\lambda(y|x)^{\rm U}&=\frac{M_\lambda(y|x)^{\rm U}}{N_\lambda(y|x)},\end{aligned} \tag{8}$$

where $N_\lambda(y|x)$ represents the total conditional detection events. Then, by using decoy-state method,[5,25] we can bound the conditional probabilities of single-photon events $p(y|x)$ for both matched-basis and mismatched-basis as

$$\begin{aligned}p(y|x)^{\rm L}&=\frac{\nu}{\nu\omega-\omega^2}\left(P_\omega(y|x)^{\rm L}\mathrm{e}^{\omega}+P_\nu(y|x)^{\rm U}\mathrm{e}^{\nu}\frac{\omega^2}{\nu^2}-\frac{\nu^2-\omega^2}{\nu^2}P_o(y|x)^{\rm U}\right),\\ p(y|x)^{\rm U}&=\min\left\{\frac{P_\omega(y|x)^{\rm U}\mathrm{e}^{\omega}-P_o(y|x)^{\rm L}}{\omega},\frac{P_\nu(y|x)^{\rm U}\mathrm{e}^{\nu}-P_o(y|x)^{\rm L}}{\nu}\right\}.\end{aligned} \tag{9}$$

Thus, the detections on single-photon pulses with intensity λ in basis Z can be expressed as

$$M_{1,\lambda}^Z=\frac{p(0|0)^{\rm L}+p(1|0)^{\rm L}+p(0|1)^{\rm L}+p(1|1)^{\rm L}}{2}N_\lambda^Z, \tag{10}$$

and the lower bound of the $M_{1,\lambda}^Z$ satisfies the following expressions:

$$M_{1,\lambda}^{Z,{\rm L}}=(1-\delta)M_{1,\lambda}^Z, \tag{11}$$

where

$$\delta=\frac{-\ln(\varepsilon/2)+\sqrt{[\ln(\varepsilon/2)]^2-8\ln(\varepsilon/2)M^Z_{1,\lambda}}}{2M^Z_{1,\lambda}},$$

N^Z_λ represents the conditional detection events with intensity λ prepared in basis Z by Alice. The single-photon bit error rate in basis Z is given by

$$e^Z_{\rm b}=\frac{p(1|0)+p(0|1)}{p(0|0)+p(1|0)+p(0|1)+p(1|1)}, \tag{12}$$

and the single-photon phase error rate is bounded by

$$e^Z_{\rm p}=e^Z_{\rm b}+\varepsilon. \tag{13}$$

The deviation ε is defined as[21]

$$\varepsilon\triangleq \max f\left(C_{30},C_{31},C'_{20},C'_{21}\right). \tag{14}$$

The function $f(C_{30},C_{31},C'_{20},C'_{21})$ is given by[21]

$$\begin{cases}\min\left\{\dfrac{\left(\sqrt{p(2|3)}+\sqrt{p(1|0)}C_{30}C'_{21}+\sqrt{p(0|1)}C_{31}C'_{20}+\sqrt{p(1|1)}\left|C_{30}C'_{20}-C_{31}C'_{21}\right|^2\right)^2}{2\left(p(0|0)+p(1|0)+p(0|1)+p(1|1)\right)C^2_{30}C'_{20}},\right.\\ \left.\dfrac{\left(\sqrt{p(2|3)}+\sqrt{p(1|0)}C_{30}C'_{21}+\sqrt{p(0|1)}C_{31}C'_{20}+\sqrt{p(0|0)}\left|C_{30}C'_{20}-C_{31}C'_{21}\right|^2\right)^2}{2\left(p(0|0)+p(1|0)+p(0|1)+p(1|1)\right)C^2_{31}C_{21}\prime 2}\right\}, & \text{if } C_{30}C'_{20}\neq 0 \text{ and } C_{31}C'_{21}\neq 0,\\ \dfrac{\left(\sqrt{p(2|3)}+\sqrt{p(1|0)}C_{30}C'_{21}+\sqrt{p(0|1)}C_{31}C'_{20}+\sqrt{p(1|1)}\left|C_{30}C'_{20}-C_{31}C'_{21}\right|^2\right)^2}{2\left(p(0|0)+p(1|0)+p(0|1)+p(1|1)\right)C^2_{30}C'^2_{20}}, & \text{if } C_{30}C'_{20}\neq 0 \text{ and } C_{31}C'_{21}=0,\\ \dfrac{\left(\sqrt{p(2|3)}+\sqrt{p(1|0)}C_{30}C'_{21}+\sqrt{p(0|1)}C_{31}C'_{20}+\sqrt{p(0|0)}\left|C_{30}C'_{20}-C_{31}C'_{21}\right|^2\right)^2}{2\left(p(0|0)+p(1|0)+p(0|1)+p(1|1)\right)C^2_{31}C'^2_{21}}, & \text{if } C_{30}C'_{20}=0 \text{ and } C_{31}C'_{21}\neq 0,\\ 1-e^Z_{\rm b}, & \text{if } C_{30}C'_{20}=0 \text{ and } C_{31}C'_{21}=0,\end{cases}$$

where C_{30}, C_{31}, C'_{20}, and C'_{21} are non-negative real numbers. And constraints for searching the maximum value of function $f(C_{30},C_{31},C'_{20},C'_{21})$ are

$$\begin{aligned}2\sqrt{p(0|0)p(0|1)C_{30}C_{31}}&\geq\left|p(0|3)-p(0|0)C^2_{30}-p(0|1)C^2_{31}\right|,\\ 2\sqrt{p(1|0)p(1|1)C_{30}C_{31}}&\geq\left|p(0|3)-p(0|0)C^2_{30}-p(0|1)C^2_{31}\right|,\\ 2\sqrt{p(0|0)p(1|0)C'_{20}C'_{21}}&\geq\left|p(0|3)-p(0|0)C'_{20}-p(0|1)C'_{21}\right|,\\ 2\sqrt{p(0|1)p(1|1)C'_{20}C'_{21}}&\geq\left|p(0|3)-p(0|0)C'_{20}-p(0|1)C'_{21}\right|.\end{aligned} \tag{15}$$

We note that $p(y|x)$ in the above equations is constrained by lower bound $p(y|x)^{\rm L}$ and upper bound $p(y|x)^{\rm U}$.

Finally, the secret key rate in basis Z is given by[23]

$$R=-f_{\rm EC}M^Z_\mu H\left(E^Z_\mu\right)+M^{Z,{\rm L}}_{1,\mu}\left[1-H\left(e^Z_{\rm p}\right)\right], \tag{16}$$

where $H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ is the binary entropy function; $f_{\rm EC}$ denotes the inefficiency of error correction; M^Z_μ represents the valid detections of signal-state in basis Z and E^Z_μ represents the quantum-bit error rate in basis Z. We note that the variables C_{30}, C_{31}, C'_{20}, and C'_{21} are restricted by the mismatched-statistics. Thus, we can obtain the phase error rate by numerical optimization.

3. Numerical simulation and discussion

In this section, we carry out corresponding numerical simulations for our present scheme. In order to show the performance of our scheme, we first compare it with the three-intensity method in Ref. [23]. To explain the main factors that make our scheme performs better, we do comparison of the phase error rate and comparison of the numbers of valid single-photon detection events used to generate final key bits. Indispensably, we also show that our scheme can generate secret key against encoding misalignments. Moreover, we also do comparisons between using HSPS and WCS. The full parameter optimization is carried out to obtain better performance, including optimizing the intensities of the signal state, two decoy states, and the probability to prepare quantum states with different intensities. In practical implementation of QKD, people often use the non-degenerated parametric down-conversion to produce photon pairs, with one photon at the wavelength convenient for detection acting as heralding signal, and the other falls into the telecommunication windows for optimal propagation along the fiber or in open air acting as heralded signal. For example, in Ref. [10], the idler mode and signal mode are each centered at 633 nm and 1545 nm, respectively, and each is detected with a silicon-avalanche pho-

todiode detector (SAPD) and InGaAs single-photon detector. Therefore, in our simulations, we have set reasonable values for the system parameters as shown in Table 1. Simulation results are shown in Figs. 1–5.

Table 1. List of practical parameters for simulations. η ($\eta_{\rm A}$) represents the detection efficiency of the single-photon detector at Bob (Alice)'s side; d ($d_{\rm A}$) represents the dark count rate of the single-photon detector at Bob (Alice)'s side; $e_{\rm d}$ is the misalignment-error probability; α denotes the loss coefficient of standard optical fibers; $f_{\rm EC}$ represents the inefficiency of error correction; ε represents the failure probability and N represents the total number of pulses sent out by Alice.

α	$e_{\rm d}$	d	η	$f_{\rm EC}$	ε	N	$d_{\rm A}$	$\eta_{\rm A}$
0.2 dB/km	1.0%	3.0×10^{-6}	0.145	1.16	1.0×10^{-9}	1.0×10^{13}	3.0×10^{-6}	0.9

In Fig. 1, we do comparisons on the key rate between using different light sources (HSPS and WCS) and using different decoy-state methods when $a=b=c=0°$, i.e., the three-intensity method[23] and the present four-intensity method. When comparing with using different light sources, it shows that HSPS experiences an enhancement of 17 km in the transmission distance, approximately 14% improvement due to the much lower vacuum component in HSPS. On the other hand, when comparing schemes with different decoy-state methods, although there is no obvious improvement in transmission distance, the four-intensity scheme significantly increases the key rate. As a result, the combination of HSPS and the four-intensity scheme can improve both the secure key rate and the transmission distance.

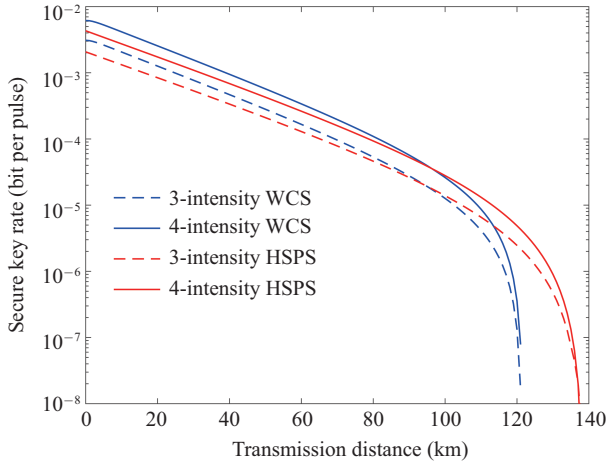


Fig. 1. Secure key rate *versus* transmission distance for different decoy-state schemes: The red solid (dash) lines represent four (three)-intensity method with HSPS for $a=b=c=0°$. The blue solid (dash) lines represent four (three)-intensity method with WCS for $a=b=c=0°$.

We compare the phase error rate and the single-photon detection event between using different light sources when $a=b=c=0°$ in Figs. 2 and 3 respectively. As we can see from Fig. 2 that, our present work using HSPS gives a much lower phase error rate comparing those using WCS because of the negligible vacuum components. Besides, for the ones using WCS, the curves of the single-photon detection event decline rapidly after 120 km, while for those using HSPS, the cut-off points reach up to 140 km.

In Fig. 4, based on four-intensity decoy-state method with HSPS (WCS), we plot out variations of the key rate with transmission distance under different values of encoding misalignments. The transmission distance decreases 4 km (5 km) when $a=b=c=3°$ and 18 km (23 km) when $a=b=c=6°$ as using HSPS (WCS). Overall, our protocol exhibits excellent tolerance to the existence of misalignment errors. It is worth noting that there is no need to characterize encoding errors in practical applications for our scheme, and consequently above-mentioned misalignments are just used to test the robust.

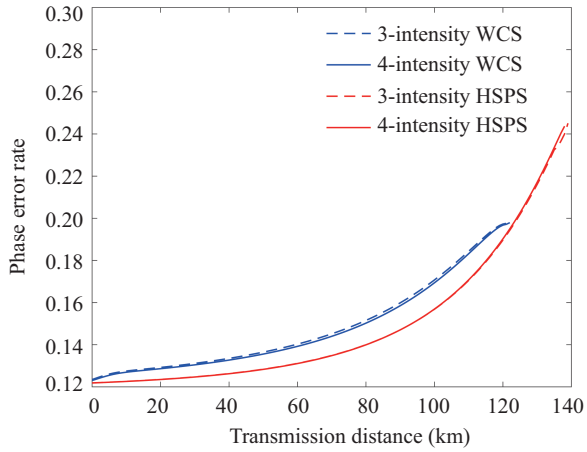


Fig. 2. Phase error rate *versus* transmission distance for different decoy-state schemes. The red solid (dash) lines represent four (three)-intensity method with HSPS for $a=b=c=0°$. The blue solid (dash) lines represent four (three)-intensity method with WCS for $a=b=c=0°$.

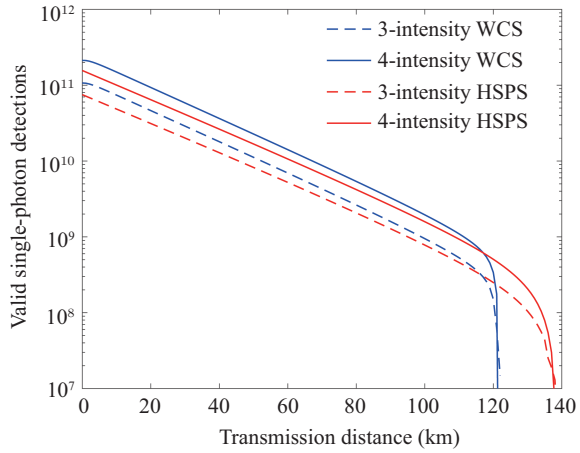


Fig. 3. Valid single-photon detections *versus* transmission distance for different decoy-state schemes. The red solid (dash) lines represent four (three)-intensity method with HSPS for $a=b=c=0°$. The blue solid (dash) lines represent four (three)-intensity method with WCS for $a=b=c=0°$.

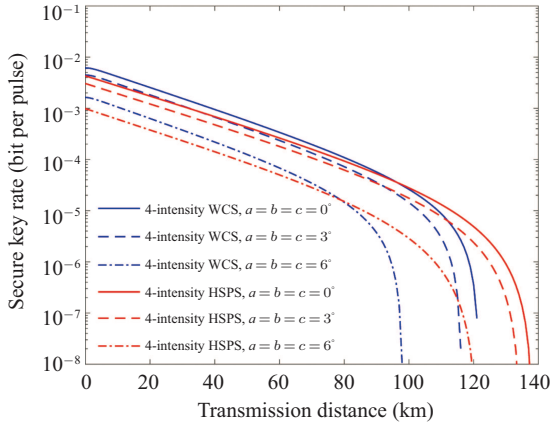


Fig. 4. Secure key rate *versus* transmission distance for different schemes with different source preparation errors. The red lines represent four-intensity method with HSPS for $a=b=c=0^\circ$, 3°, 6°. The blue lines represent four-intensity method with WCS for $a=b=c=0^\circ$, 3°, 6°.

Finally, we do investigation on the detection efficiency of the local detectors at Alice's side ($\eta_{\rm A}$), by fixing the encoding misalignments as $a=b=c=3^\circ$, see Fig. 5. We can see from Fig. 5 that the higher the detection efficiency, the higher the key rate and the transmission distance. With the state-of-the-art superconducting nanowire single-photon detector ($\eta_{\rm A}=0.9$),[30] our scheme only presents a slightly lower key rate than the one using WCS at short transmission distance (<90 km); while shows more than 20-km longer transmission distance.

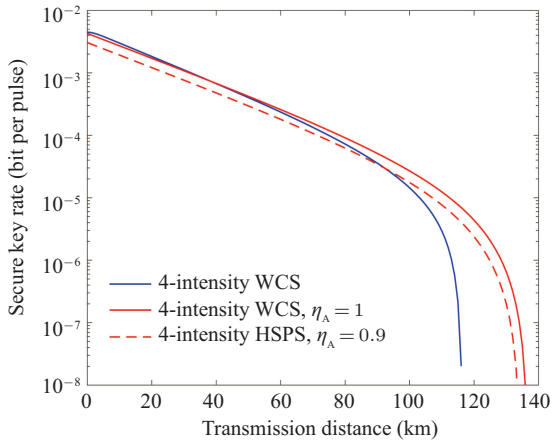


Fig. 5. Secure key rate *versus* transmission distance by using different light sources: The blue lines represent four-intensity method with WCS. The red lines represent four-intensity method with HSPS for $\eta_{\rm A}=0.9$ and 1.

4. Conclusion

In conclusion, we have presented an improved decoy-state QKD protocol with uncharacterized HSPS and investigated its performance. By exploiting the mismatched-basis statistics and preparing quantum states in a two-dimensional Hilbert space, our scheme reduces the requirements for preparation errors and lowers the system complexity compared with normal BB84 QKD protocol. Moreover, our simulation results show that the secure key rate and transmission distance have been significantly improved by using our present scheme comparing with former similar protocols. Therefore, our present work seems to be a very promising choice for practical implementations of QKD systems.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 12074194, 12104240, and 62101285), the Industrial Prospect and Key Core Technology Projects of Jiangsu Provincial Key Research and Development Program (Grant No. BE2022071), and the Natural Science Foundation of Jiangsu Province, China (Grant Nos. BK20192001 and BK20210582).

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 1984, New York, pp. 175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Lo H K and Chau H F 1999 *Science* **283** 2050
[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[5] Wang Q, Chen W, Xavier G, Swillo M, Zhang T, Sauge S, Tengner M, Han Z F, Guo G C and Karlsson A 2008 *Phys. Rev. Lett.* **100** 090501
[6] Liu Y, Chen T Y, Wang J, Cai W Q, Wan X, Chen L K, Wang J H, Liu S B, Liang H, Yang L, Peng C Z, Chen K, Chen Z B and Pan J W 2010 *Opt. Express* **18** 8587
[7] Stucki D, Legre M, Buntschu F, *et al.* 2011 *New J. Phys.* **13** 123001
[8] Wang S, Chen W, Yin Z Q, *et al.* 2014 *Opt. Express* **22** 21739
[9] 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
[10] Zhang C H, Wang D, Zhou X Y, Wang S, Zhang L B, Yin Z Q, Chen W, Han Z F, Guo G C and Wang Q 2018 *Opt. Express* **26** 25921
[11] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[12] 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 2019 *Phys. Rev. X* **9** 021046
[13] Gottesman D, Lo H K, Lutkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[14] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[15] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[16] Qi B, Fung C H F, Lo H K and Ma X 2007 *Quantum Inf. Comput.* **7** 73
[17] Fung C H F, Qi B, Tamaki K and Lo H K 2007 *Phys. Rev. A* **75** 032314
[18] Laing A, Scarani V, Rarity J G and O'Brien, J L 2010 *Phys. Rev. A* **82** 012304
[19] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[20] Tamaki K, Curty M, Kato G, Lo H K and Azuma K 2014 *Phys. Rev. A* **90** 052314
[21] Yin Z Q, Fung C H F, Ma X, Zhang C M, Li H W, Chen W, Wang S, Guo G C and Han Z F 2014 *Phys. Rev. A* **90** 052319
[22] Wang C, Wang S, Yin Z Q, Chen W, Li H W, Zhang C M, Ding Y Y, Guo G C and Han Z F 2016 *Opt. Lett.* **41** 5596
[23] Zhu J R, Wu W Z, Ji L and Wang Q 2019 *Opt. Lett.* **44** 5703
[24] Zhou X Y, Ding H J, Zhang C H, Li J, Zhang C M and Wang Q 2020 *Opt. Lett.* **45** 4176
[25] Wang Q, Wang X B and Guo G C 2007 *Phys. Rev. A* **75** 012312
[26] Wang Q and Wang X B 2013 *Phys. Rev. A* **88** 052332
[27] Zhou X Y, Zhang C H, Zhang C M and Wang Q 2017 *Phys. Rev. A* **96** 052337
[28] Zhang Z, Zhao Q, Razavi M and Ma X 2017 *Phys. Rev. A* **95** 012333
[29] Mao C C, Zhou X Y, Zhu J R, Zhang C H, Zhang C M and Wang Q 2018 *Opt. Express* **26** 13289
[30] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Wang R C, Wu J, Chen T Y, You L, Wang X B, Zhang Q and Pan J W 2023 *Phys. Rev. Lett.* **130** 210801