IOP Publishing New J. Phys. 26 (2024) 093011 https://doi.org/10.1088/1367-2630/ad7493

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
13 May 2024

REVISED
14 August 2024

ACCEPTED FOR PUBLICATION
28 August 2024

PUBLISHED
9 September 2024

PAPER

Mode pairing quantum key distribution with light source monitoring

Zhenhua Li[1,*], Tianqi Dou[1], Yuheng Xie[1], Weiwen Kong[1], Na Chen[1], Qi Zhao[1], Wenpeng Gao[1], Peizhe Han[1], Yuanchen Hao[1], Haiqiang Ma[2,*], Yang Liu[1] and Jianjun Tang[1,*]

[1] China Telecom Research Institute, Beijing 102209, People's Republic of China
[2] School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China
[*] Authors to whom any correspondence should be addressed.

E-mail: lizh84@chinatelecom.cn, hqma@bupt.edu.cn and tangjj6@chinatelecom.cn

Keywords: quantum key distribution, quantum cryptography, mode pairing protocol, light source monitoring, untrusted source

Abstract

Mode pairing quantum key distribution (MP-QKD) overcomes the repeaterless bound without requiring phase locking and phase tracking. However, MP-QKD still assumes that the light source is trusted, which can present challenges in practical deployments and potentially introduce security vulnerabilities. In this paper, we propose a light source monitoring (LSM) scheme that guarantees the security of MP-QKD with the untrusted light sources. The simulation results demonstrate that, when considering untrusted light sources, the performance of MP-QKD with the LSM scheme remains nearly identical to that of ideal MP-QKD, even in the presence of the source fluctuations. Furthermore, we simplify some of the complex integration calculations involved in simulating the observed quantities of MP-QKD, which reduces the running time of the parameter optimization procedure.

1. Introduction

Quantum key distribution (QKD), grounded in the fundamental principles of quantum mechanics [1, 2], ensures the security of message transmission. Since the proposal of the BB84 protocol [3], QKD has achieved significant advancements in experiment [4, 5]. However, considering the imperfections inherent in real-world devices, the security of practical QKD implementations is a compromise between various factors. Therefore, numerous protocols have been proposed to bridge the gap between theoretical advancements and experimental implementations.

In response to the limitations of non-ideal single-photon sources [6], researchers have proposed a decoy state method [7–11], which has now become a basic configuration in QKD systems. This method proves the security of weak coherence sources and enables nearly ideal single-photon source communication. In terms of measurements, the measurement-device-independent QKD (MDI-QKD) protocol [12–14] effectively eliminates all vulnerabilities associated with single photon detectors (SPDs) in the practical system by introducing an untrusted intermediate node for performing the interference measurement. Twin-field QKD (TF-QKD) [15–19] exploits the single photon interference properties to surpasses the fundamental limit of the repeaterless bound. TF-QKD has achieved significant breakthroughs [20–24] in point-to-point long-distance experiment by elevating the relationship between secure key rate and distance from linear to square root level.

The implementation of complex laser frequency and phase locking techniques in TF-QKD increases the experimental challenges and requires significant cost investment. Compared to TF-QKD, the recently proposed mode pairing QKD (MP-QKD, also called asynchronous MDI-QKD) [25, 26] overcomes the aforementioned limitations and offers a relatively simplified approach. Furthermore, in contrast to MDI-QKD, it leverages detection events more effectively for key generation, thereby enhancing the secure key rate. MP-QKD has been successfully demonstrated over distances of 404 km [27] and 508 km [28] in

laboratory settings, with the latter exceeding the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) repeaterless bound [29]. MP-QKD has been employed on existing inter-city fiber links [30], with field tests conducted over distances from tens to approximately a hundred kilometers. However, similar to MDI-QKD and TF-QKD, while MP-QKD diminishes the detector requirements in a QKD system, it is still assumed that the source is trusted, implying that the photon number distribution (PND) of the source must be known. This assumption may be challenged by imperfections in experimental equipment and potential eavesdropping attacks [31–36]. The light source structure in MP-QKD resembles that of the BB84 protocol, which can also encounter the issue of an untrusted light source, leading to an unknown PND. Hence, in the case of untrusted light sources, it is essential to utilize light source monitoring (LSM) [37, 38] to recalibrate the PND of the light source.

In this paper, we discuss the MP-QKD protocol where the PND is unknown. We propose the MP-QKD with LSM scheme, which aims to estimate the probabilities associated with optical pulse signals containing the zero-photon, one-photon, and two-photon. Through the integration of the decoy state method, our proposed scheme effectively addresses the issue of untrusted light sources, thereby enhancing the security of the MP-QKD protocol. Remarkably, despite this improvement, the performance of our scheme remains comparable to that of the original protocol with trusted light sources. Moreover, our proposed scheme exhibits robustness against the source fluctuations, outperforming the original MP-QKD protocol. Furthermore, by simplifying the complex integration calculations involved in simulating the observed quantities of MP-QKD, we achieve a reduction in the running time of the parameter optimization procedure.

The structure of the paper is as follows. Section 2 provides an review of the MP-QKD protocol. In section 3, we conduct a comprehensive analysis of the performance of the LSM scheme in combination with the decoy state method and the source fluctuations. Section 4 involves a comparative simulation of the secure key rates between the LSM scheme and the original protocol under various scenarios. The conclusions are drawn in section 5. In the appendix, we present detailed simulation models, and the statistical fluctuation analysis.

2. MP-QKD

Considering the three-intensity decoy state method, the specific steps of MP-QKD [25, 27, 39] can be summarized as follows.

1. State preparation
In the mth round of communication, Alice prepares the coherent state pulse $\left|e^{i\theta_a^m}\sqrt{k_a^m}\right\rangle$ with the probability $p_{k_a^m}$, where k_a^m is randomly chosen from $\{\mu,\nu,\omega\}$, representing the signal, decoy, and vacuum states, respectively. In the ideal scenario, ω is typically set to 0. And a phase θ_a^m uniformly chosen from $\{0,\frac{2\pi}{\Delta},\frac{4\pi}{\Delta},\ldots,\frac{2\pi(\Delta-1)}{\Delta}\}$, where Δ is the number of phase slices. In parallel, Bob follows a similar procedure to prepare the coherent state pulse $\left|e^{i\theta_b^m}\sqrt{k_b^m}\right\rangle$ with the probability $p_{k_b^m}$.

2. Measurement
Alice and Bob send pulse $\left|e^{i\theta_a^m}\sqrt{k_a^m}\right\rangle$ and pulse $\left|e^{i\theta_b^m}\sqrt{k_b^m}\right\rangle$, respectively, to Charlie, an untrusted third party, for the single-photon interference measurement. Subsequently, Charlie publicly declares the measurement results of detectors L and R.

3. Mode pairing
After repeating steps 1 and 2 for a total of N rounds, only the data where there is a single click from both detectors L and R is retained, while results where L and R do not click or both click are discarded. For all retained clicks, Alice and Bob pair clicks with their immediate next neighbor within a maximal pairing interval $l_{\max}$ to form a successful pairing. To avoid the influence of the detector dead time and after-pulse effect, it is also important to set a minimum pairing interval $l_{\min}$.

4. Basis sifting
For each pairing, Alice (Bob) records an effective event pair $F_{a(b)}^{m,n}=\{k_{a(b)}^m,k_{a(b)}^n,\theta_{a(b)}^m,\theta_{a(b)}^n\}$, where $n\,(m+l_{\min}\leqslant n\leqslant m+l_{\max})$ is another effective detection click. Define the intensity group of the mth and nth rounds as $(k_a,k_b)=\left(k_a^m+k_a^n,k_b^m+k_b^n\right)$. Alice (Bob) labels the basis of each $F_{a(b)}^{m,n}$ as Z-basis if $k_{a(b)}=\mu$ or ν, as X-basis if $k_{a(b)}=2\mu$ or 2ν, as 0-basis if $k_{a(b)}=0$. Event pair obtained in other scenarios are discarded. For convenience, define the pair of $F_a^{m,n}$ and $F_b^{m,n}$ as $F^{m,n}$. For each $F^{m,n}$ pair, Alice and Bob record it as Z-pair, X-pair, or 0-pair when both $F_a^{m,n}$ and $F_b^{m,n}$ are labeled as Z-basis, X-basis, or 0-basis, respectively. They record $F^{m,n}$ as Z-pair (X-pair) when one of $F_a^{m,n}$ and $F_b^{m,n}$ is labeled as 0-basis and the other is labeled as Z-basis (X-basis), and as 0-pair when both $F_a^{m,n}$ and $F_b^{m,n}$ are labeled as 0-basis.

5. Key mapping

For each $F^{m,n}$ of Z-pair, Alice (Bob) extracts a bit 0 when $k_a^m \neq k_a^n = 0$ ($k_b^n \neq k_b^m = 0$), and extracts a bit 1 when $k_a^n \neq k_a^m = 0$ ($k_b^m \neq k_b^n = 0$).

When $k_a^n = k_a^m = 0$ ($k_b^n = k_b^m = 0$), which represents 0-pair, Alice (Bob) randomly obtains a bit 0 or 1 with a probability of 50%.

For each $F^{m,n}$ of X-pair, Alice's (Bob's) key is extracted from the relative phase $\theta_{a(b)}^m - \theta_{a(b)}^n = \phi_{a(b)} + \pi\kappa_{a(b)}$, where the raw key bit is given by $\kappa_{a(b)} = [(\theta_{a(b)}^m - \theta_{a(b)}^n)/\pi] \bmod 2$ and and the alignment angle is $\delta_{a(b)} = \left(\theta_{a(b)}^m - \theta_{a(b)}^n\right) \bmod \pi$. As an extra step on the X-pair, if Charlie announces a measurement of (L,R) or (R,L), Bob flips the bit κ_b. After the alignment angle δ_a and δ_b are announced, if $|\delta_a - \delta_b| \leqslant \Delta$, κ_b remains unchanged, whereas if $|\delta_a - \delta_b| \geqslant \pi - \Delta$, Bob flips the bit κ_b. $F^{m,n}$ where $|\delta_a - \delta_b|$ does not satisfy the above conditions are discarded. In particular, when $(k_a, k_b) = (2k_a, 0)$ or $(0, 2k_b)$, $F^{m,n}$ of X-pair is preserved regardless of the value of $|\delta_a - \delta_b|$.

6. Parameter estimation

The portion of the Z-pair that corresponds to $(k_a, k_b) = (\mu, \mu)$ is utilized for generating key bits. The number of pairs used to distill final key bits $M_{(\mu,\mu)}$, and the bit error rate $E_{(\mu,\mu)}$ can be directly obtained from the experiment. The single-photon component of the Z-pair M_{11}^Z, and the corresponding phase error rate $e_{11}^{Z,\mathrm{ph}}$ can be estimated by the decoy-state method.

7. Key distillation

Alice and Bob perform error correction and privacy amplification to distill the final key bits. According to the entropic uncertainty relation for smooth entropies [40–42], the key length of MP-QKD with finite key analysis can be expressed as [11, 39, 43]:

$$\ell \geqslant M_{11}^Z \left[1 - h\left(e_{11}^{Z,\mathrm{ph}}\right)\right] - fM_{(\mu,\mu)} h\left(E_{(\mu,\mu)}\right) - \log_2 \frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2 \frac{1}{\sqrt{2}\hat{\varepsilon}\varepsilon_{\mathrm{PA}}}, \tag{1}$$

where M_{11}^Z can be expressed by the yield of Z basis single-photon pulse pairs y_{11}^Z, i.e. $M_{11}^Z = N_{(\mu,\mu)}^Z \mu^2 \mathrm{e}^{-2\mu} y_{11}^Z$, and $N_{(\mu,\mu)}^Z$ represents the number of Z-pair containing $(k_a, k_b) = (\mu, \mu)$. f denotes the error correction efficiency, $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. $\varepsilon_{\mathrm{cor}}$, $\hat{\varepsilon}$, $\varepsilon_{\mathrm{PA}}$ are security coefficients regarding the correctness and secrecy (detail in appendix D).

3. The LSM scheme with MP-QKD

3.1. The LSM scheme

As depicted in figure 1(a), the LSM scheme facilitates the monitoring of untrusted light sources, distinguishing it from the original MP-QKD protocol. Charlie is positioned between Alice and Bob, and the setup of both Alice and Bob is symmetrical. After the modulation process, the untrusted optical pulse is divided into two components by a beam splitter (BS). One component is directed towards the LSM scheme for source monitoring, while the other is transmitted to Charlie for the interference measurement. A LSM scheme comprises a variable optical attenuator (VOA) and a SPD as shown in figure 1(b). By passively monitoring the click of the SPD, the probability bounds for zero-photon, single-photon, and two-photon in an untrusted light pulse can be estimated. Compared to passive optical devices, active optical devices such as VOA introduce larger fluctuations. To mitigate this impact, the setup depicted in figure 1(c) can be employed as a substitute to eliminate such fluctuations.

3.2. The decoy state method with untrusted light sources

In the original MP-QKD protocol, the light fields in the signal, decoy, and vacuum states of Alice and Bob can be expressed as respectively:

$$\begin{aligned}
\rho_a^{\mathrm{signal}} &= \sum_n^{\infty} a_n^{\mu} |n\rangle\langle n|, \rho_b^{\mathrm{signal}} = \sum_n^{\infty} b_n^{\mu} |n\rangle\langle n|, \\
\rho_a^{\mathrm{decoy}} &= \sum_n^{\infty} a_n^{\nu} |n\rangle\langle n|, \rho_b^{\mathrm{decoy}} = \sum_n^{\infty} b_n^{\nu} |n\rangle\langle n|, \\
\rho_a^{\mathrm{vacuum}} &= \sum_n^{\infty} a_n^{\omega} |n\rangle\langle n|, \rho_b^{\mathrm{vacuum}} = \sum_n^{\infty} b_n^{\omega} |n\rangle\langle n|,
\end{aligned} \tag{2}$$

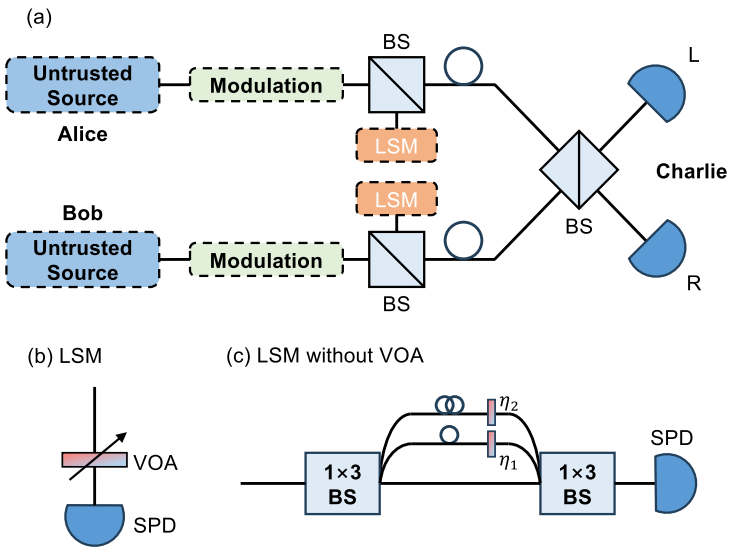

Figure 1. The structure for the MP-QKD with LSM scheme. BS: beam splitter; LSM: the light source monitoring scheme; L, R: the single photon detector of Charlie; VOA: variable optical attenuator; SPD: the single photon detector of LSM. (a) After modulation, the untrusted source is split into two components by the BS. One part is directed towards Charlie for the interference measurement, while the other part is routed to the LSM scheme. (b) the LSM scheme consists of a VOA and an SPD. (c) Passive component solutions for LSM.

where $a_n^{k_a}$ and $b_n^{k_b}$ are the coefficients of Fock state $|n\rangle$. In the ideal scenario, $a_n^{k_a}$ and $b_n^{k_b}$ are individually manipulated by Alice and Bob, respectively, and generally follow the Poisson distribution. However, in practical scenarios, untrusted light sources may disrupt the assumptions made in the ideal scenario. In the presence of untrusted light sources, after coincidence pairing, the boundaries [44–46] for y_{11}^Z are determined as follows:

$$y_{11}^Z \geqslant \frac{\frac{a_1^{\mu,L} b_2^{\mu,L} \tilde{n}^Z_{(\nu,\nu)}}{1+\sigma_C^Z} - \frac{a_1^{\nu,U} b_2^{\nu,U} \tilde{n}^Z_{(\mu,\mu)}}{1-\sigma_A^Z-\sigma_B^Z}}{a_1^{\nu,U} a_1^{\mu,L} \left(b_1^{\nu,U} b_2^{\mu,L} - b_2^{\nu,U} b_1^{\mu,L}\right)}, \tag{3}$$

where $a_n^{k_a,U(L)}$ and $b_n^{k_b,U(L)}$ represent the PND after coincidence pairing, the superscripts U, L refer to the upper and the lower bound. Through a random-sampling theory (without replacement) [47–50], the single-photon phase error rate $e_{11}^{Z,\mathrm{ph}}$ can be estimated by the single-photon bit error rate of X-pair $e_{11}^{X,\mathrm{bit}}$,

$$e_{11}^{Z,\mathrm{ph}} \leqslant e_{11}^{X,\mathrm{bit}} + \Gamma\left(\xi_{ee}, e_{11}^{X,\mathrm{bit}}, M_{11}^X, M_{11}^Z\right), \tag{4}$$

where

$$\Gamma(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cd} \ln\left(\frac{c+d}{2\pi cd(1-b)ba^2}\right)}, \tag{5}$$

ξ_{ee} is the failure probability of the random-sampling (without replacement), and M_{11}^X is the effective detection number of the single-photon states of X-pair. The definitions of the remaining parameters are provided in the appendices A and C. In the subsequent analysis, we calculate the bounds of $a_n^{k_a}$ and $b_n^{k_b}$ utilizing the LSM scheme.

3.3. Parameters estimation with LSM scheme

As depicted in figure 1, for each untrusted optical pulse, the attenuation $\eta_p \in \{\eta_0, \eta_1, \eta_2\}\,(\eta_0 \geqslant \eta_1 \geqslant \eta_2)$ can be randomly selected to monitor the click of the SPD. The probability $P_{\eta_p}^{k_a}$ of non-click by the Alice's SPD [37, 38] can be expressed as:

$$P_{\eta_p}^{k_a} = \left(1 - p_d^{\mathrm{LSM}}\right) \sum_{n=0}^{\infty} \left(1-\eta_p\right)^n a_n^{k_a}, \tag{6}$$

where p_d^{LSM} is the dark count rate of the local SPD in the LSM scheme. By combining equation (6) with three different attenuation coefficients $\{\eta_0, \eta_1, \eta_2\}$, a system of three equations can be derived. By solving this

system of three equations, the bounds of $a_n^{k_a}$ can be determined as follows:

$$\begin{aligned}
a_0^{k_a,U} &= a_0^{k_a,L} = \frac{P_{\eta_0}^{k_a}}{1-p_d^{\mathrm{LSM}}},\\
a_1^{k_a,L} &= \frac{(1-\eta_2)^2 P_{\eta_1}^{k_a} - (1-\eta_1)^2 P_{\eta_2}^{k_a}}{\left(1-p_d^{\mathrm{LSM}}\right)(1-\eta_1)(1-\eta_2)(\eta_1-\eta_2)} - \left(\frac{1}{1-\eta_1}+\frac{1}{1-\eta_2}\right) a_0^{k_a,U}\\
a_1^{k_a,U} &= \frac{(1-\eta_2)(1-\eta_1)}{\left[1-\eta_2-(1-\eta_1)(2-\eta_2)\right]}\left\{\frac{P_{\eta_1}^{k_a}}{(1-\eta_1)^2\left(1-p_d^{\mathrm{LSM}}\right)} - \frac{P_{\eta_2}^{k_a}}{\left(1-p_d^{\mathrm{LSM}}\right)(1-\eta_2)^2\eta_2}\right.\\
&\quad \left. + \frac{1-\eta_2}{\eta_2} + \frac{\left[1-(1-\eta_2)^3\right]}{(1-\eta_2)^2\eta_2} a_0^{k_a,U} - \frac{a_0^{k_a,L}}{(1-\eta_1)^2}\right\},\\
a_2^{k_a,L} &= \frac{P_{\eta_2}^{k_a}}{\left(1-p_d^{\mathrm{LSM}}\right)(1-\eta_2)^2\eta_2} - \frac{2-\eta_2}{1-\eta_2} a_1^{k_a,U} - \frac{1-\eta_2}{\eta_2} - \frac{\left[1-(1-\eta_2)^3\right]}{(1-\eta_2)^2\eta_2} a_0^{k_a,U}\\
a_2^{k_a,U} &= \frac{P_{\eta_2}^{k_a}}{\left(1-p_d^{\mathrm{LSM}}\right)(1-\eta_2)^2} - \frac{a_0^{k_a,L}}{(1-\eta_2)^2} - \frac{a_1^{k_a,L}}{1-\eta_2}
\end{aligned} \tag{7}$$

where $\eta_1(2-\eta_2) > 1$. Bob can obtain $b_n^{k_b}$ using a similar approach. As depicted in equation (3), there are different intensities [51] in each of the Z-pair and X-pair after coincidence pairing. In the Z-pair, the intensities are μ, ν, and ω, while in the X-pair, the intensities are 2μ, 2ν, and 2ω. Regarding the Z-pair, the findings presented in equation (7) can be directly applied. However, in the X-pair, the intensity 2ν is derived by pairing the two intensities ν in the i and j time bins, without actually preparing the optical pulse with intensity 2ν in the experimental setup. Consequently, we consider $a_n^{2\nu}$ and $b_n^{2\nu}$ to possess the same boundary percentage as a_n^{ν} and b_n^{ν}, that is $\frac{a_n^{2\nu,L(U)}}{a_n^{2\nu}} = \frac{a_n^{\nu,L(U)}}{a_n^{\nu}}$ and $\frac{b_n^{2\nu,L(U)}}{b_n^{2\nu}} = \frac{b_n^{\nu,L(U)}}{b_n^{\nu}}$.

3.4. Source fluctuations

In practical QKD experimental deployments, the PND of the light source is generally unstable, which means that there are source fluctuations [44, 52]. The impact of the source fluctuations can also be alleviated through the utilization of the LSM scheme depicted in figure 1. For simplicity, we assume that the optical pulse prepared by Alice is considered as the coherent state with the source fluctuations, which has an average photon number k_a with Gaussian distribution [47, 53–55]:

$$G_{k_a} = \frac{1}{\sqrt{2\pi}\,\sigma_{k_a}} \exp\left[-\frac{\left(k_a-k_a^0\right)^2}{2\sigma_{k_a}^2}\right], \tag{8}$$

where k_a^0 and σ_{k_a} are the mean value and the standard deviation of k_a. The probability that the local SPD in the LSM scheme does not click becomes:

$$\begin{aligned}
P_{\eta_p}^{k_a,\mathrm{GD}} &= \int P_{\eta_p}^{k_a} G_{k_a} dk_a\\
&= \left(1-p_d^{\mathrm{LSM}}\right) \exp\left[-\eta_p k_a^0 + \frac{\left(\eta_p \sigma_{k_a}\right)^2}{2}\right].
\end{aligned} \tag{9}$$

Similarly, $P_{\eta_p}^{k_b,\mathrm{GD}}$ can be obtained using the same methodology. By utilizing equations (7) and (9), the PND can be derived considering the source fluctuations.

4. Numerical simulation

In this section, we numerically simulate the secure key rates for both the original MP-QKD protocol and the MP-QKD with LSM scheme in the finite key analysis. The parameters used for the numerical simulations are presented in table 1. In the simulation, we perform optimization [56] to determine the appropriate intensities and their corresponding sending probabilities for each distance. We assume that Alice and Bob have equal distances to Charlie, and that they both have identical equipment deployment. We simulate observed values through the methods outlined in the appendix A, which simplifies the complex calculations involved in MP-QKD and reduces the running time of the program. Additionally, in the LSM scheme, we assign the attenuation coefficients as follows: $\eta_0 = 1$, $\eta_1 = 0.95$, and $\eta_2 = 0.9$.

Table 1. Values of parameters used in simulation.

Variable	Parameter	Value
p_d	dark count rate of Charlie's SPD	10^{-8}
η_d	detection efficiency of Charlie's SPD	72%
α	fiber loss coefficient	0.18 dB km^{-1}
Δ	number of phase slices	16
$\varepsilon_{\rm cor}, \hat{\varepsilon}, \varepsilon_{\rm PA}$[a]	correction and security coefficients	3.28×10^{-23}
ξ_{ee}, ϵ	failure probability	10^{-10}
f	error correction efficiency	1.1
e_d^X	misalignment-error of the X-pair	0.05
e_d^Z	misalignment-error of the Z-pair	10^{-6}
$p_d^{\rm LSM}$	dark count rate of local SPD	10^{-6}
$l_{\rm max}$	maximal pairing interval	2000
$l_{\rm min}$	minimum pairing interval	63

[a] Data from [39].

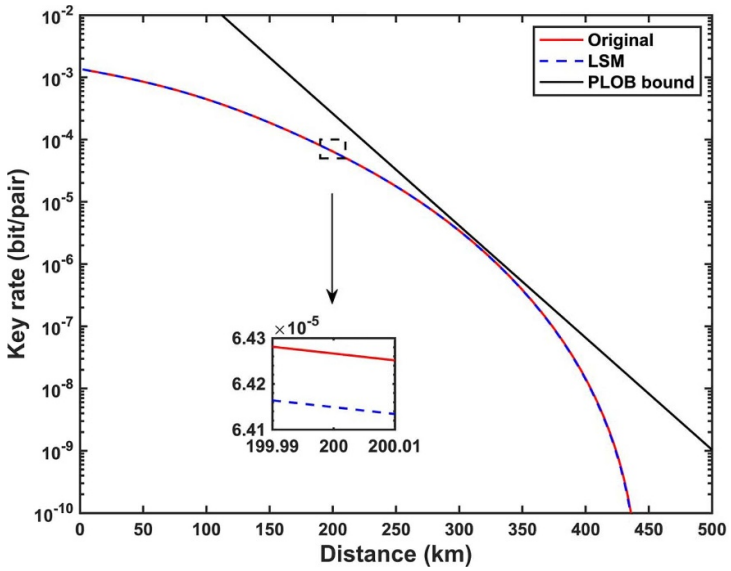

Figure 2. Secure key rate versus the transmission distance under original protocol (the red solid line) and LSM (the blue dash line). The secure key rate performance at a transmission distance of 200 km is magnified in the depicted graph. The total pulse numbers is fixed to $N = 10^{13}$.

As depicted in figure 2, we simulate the secure key rate of the original MP-QKD and the MP-QKD with the LSM scheme with an ideal source at different transmission distances. The results demonstrate that both protocols achieve comparable maximum transmission distances. Notably, we observed that while the secure key rate of the original MP-QKD protocol is slightly higher than that of our proposed the MP-QKD with the LSM scheme , the secure key rate curves exhibit significant overlap. For example, at a distance of 200 km, the ratio of secure key rate between the MP-QKD with the LSM scheme and original MP-QKD is about 99.82%. This proves that our scheme can achieve an excellent secure key rate characteristics close to the original MP-QKD. Furthermore, it signifies that the deployment of the LSM scheme has negligible impact on the system's secure key rate. Instead, it facilitates the monitoring of the PND of the source, thereby enhancing the overall security of the system.

Figure 3 presents the performance comparison of different protocols under source fluctuations. To ensure a fair comparison, we employed the relative standard deviation $\sigma = \frac{\sigma_{k_a}}{k_a} = \frac{\sigma_{k_b}}{k_b}$ as a metric to assess and compare the performance of different protocols. We observed that when the value of σ is set to 0.05 or 0.1, the secure key rate of MP-QKD with the LSM scheme remains relatively stable, whereas the original MP-QKD protocol exhibits a substantial decrease in performance. When $\sigma = 0.05$, the maximum transmission distance of the original protocol decreases to 384 km, and notably, when $\sigma = 0.1$, the maximum transmission distance further decreases to 312 km. At a distance of 200 km, the secure key rate of original MP-QKD decreases by 81.50% and 456.98% for $\sigma = 0.05$ and $\sigma = 0.1$, respectively, while the secure key rate of MP-QKD with the LSM scheme remains relatively stable. For a more intuitive illustration, figure 4

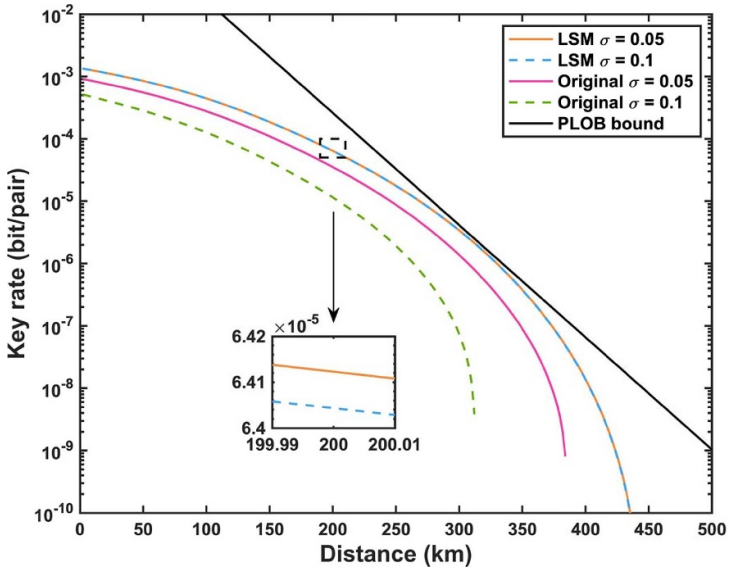

Figure 3. Compared with the original MP-QKD protocol, the secure key rate of the LSM scheme with fluctuating light source. σ: the relative standard deviation. As σ increases, the secure key rate for the LSM scheme remains relatively constant, whereas for the original protocol, the secure key rate experiences a substantial decrease. The total pulse numbers is fixed to $N = 10^{13}$.

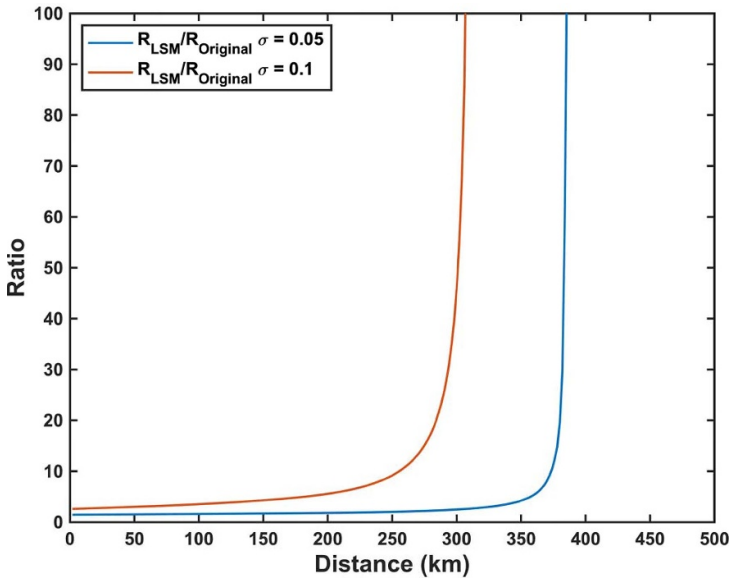

Figure 4. The ratio of the MP-QKD with the LSM scheme to the original MP-QKD protocol secure key rate. The ratios exhibit an upward trend as both the σ value and transmission distance increase. The trend highlights the enhanced advantages of the MP-QKD with the LSM scheme in long-distance transmission. The total pulse numbers is fixed to $N = 10^{13}$.

presents the ratio of the secure key rates between these two protocols. The superiority of MP-QKD with the LSM scheme becomes more pronounced as increasing transmission distances.

Figure 5 depicts the simulation results of the LSM scheme and the original MP-QKD protocol for varying data sizes. Under the conditions of $\sigma = 0.1$ and $N = 10^{14}$, it can be observed that the utilization of the LSM scheme enables a reach of 475 km, whereas the original scenario achieves only 370 km. The simulation curves shows that larger data sizes would yield higher key rates. We also observed that, with an increase in data sizes, the secure key rate slightly surpasses the PLOB bound. This is attributed to our conservative choice of the maximum pairing length, $l_{\max}$, as 2000 based on [27]. In practice, $l_{\max}$ can be estimated by multiplying the laser coherence time by the system repetition rate. Therefore, selecting better lasers or increasing the system repetition rate can enhance the secure key rate, making it easier to surpass the PLOB bound.

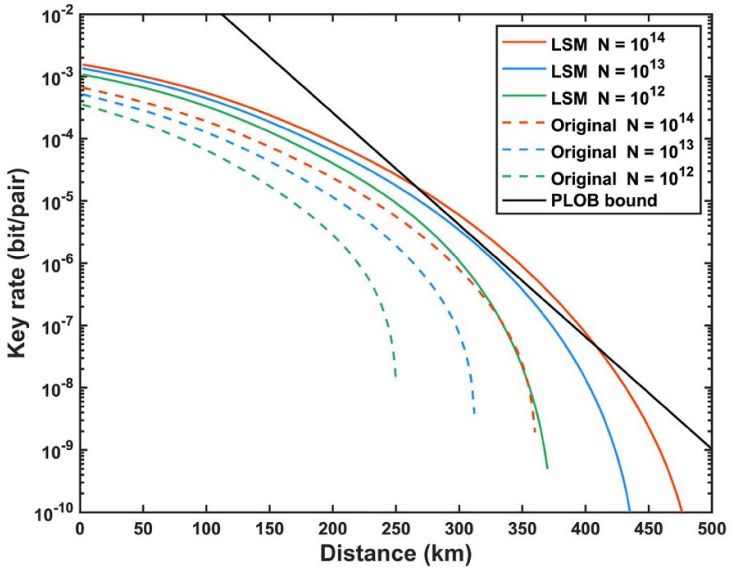

Figure 5. Secure key rate as a function of transmission distance for the LSM scheme (the solid line) and the original case (the dotted line). The red line, blue line, and green line are for total pulse numbers $N = 10^{14}$, 10^{13},10^{12}, respectively. The relative standard deviation is fixed to $\sigma = 0.1$.

5. Conclusion

In this paper, we employ the LSM scheme to address the issue of untrusted sources in the MP-QKD protocol. By leveraging the LSM scheme, we can achieve a more accurate estimation of the PND associated with untrusted sources. Consequently, this leads to a tighter secure key rate of MP-QKD. The simulation results demonstrate that MP-QKD with LSM scheme achieves comparable performance to the original MP-QKD protocol, while also exhibiting robustness against the source fluctuations. In addition, we present a simplification of the intricate integration calculations required for simulating the observed quantities in MP-QKD. This simplification leads to a notable reduction in the running time of the parameter optimization procedure.

Data availability statement

The data generated and/or analysed during the current study are not publicly available for legal/ethical reasons but are available from the corresponding author on reasonable request. The data that support the findings of this study are available upon reasonable request from the authors.

Acknowledgments

We would like to express our deepest gratitude to Hao-tao Zhu and Wen-xin Pan for their invaluable discussions and assistance throughout this research.

Funding

This work was supported by the Innovation Program for Quantum Science and Technology (2021ZD0301300); the state Key Laboratory of Information Photonics and Optical Communications No. IPOC2024ZT10.

Conflict of interest

The authors declare that they have no competing interests.

Appendix A. Simulation method of observed values

As depicted in figure 1, the detection probabilities of the detectors L and R are given by

$$\begin{aligned} D_{k_a^m k_b^m}^{L,\theta^m} &= 1 - y\mathrm{e}^{-x\cos\theta^m}, \\ D_{k_a^m k_b^m}^{R,\theta^m} &= 1 - y\mathrm{e}^{x\cos\theta^m}, \end{aligned} \tag{A1}$$

where $y = (1-p_d)\,\mathrm{e}^{-k^m/4}$, $x = \frac{\sqrt{\eta_a k_a^m \eta_b k_b^m}}{2}$, $k^m = \eta_a k_a^m + \eta_b k_b^m$, and $\theta^m = \theta_a^m - \theta_b^m$. In the absence of the LSM scheme and the BS, which represents the original MP-QKD protocol, the aforementioned values can be expressed as $y = (1-p_d)\,\mathrm{e}^{-k^m/2}$ and $x = \sqrt{\eta_a k_a^m \eta_b k_b^m}$. $\eta_a\,(\eta_b)$ is the transmission coefficient from Alice (Bob) to Charlie.

In the mth round, the response probability of only L or R detectors is given by

$$\begin{aligned} q_{k_a^m k_b^m}^{L,\theta^m} &= D_{k_a k_b}^{L,\theta^m}\left(1 - D_{k_a^m k_b^m}^{R,\theta^m}\right) = y\left(\mathrm{e}^{x\cos\theta^m} - y\right), \\ q_{k_a^m k_b^m}^{R,\theta^m} &= D_{k_a^m k_b^m}^{R,\theta^m}\left(1 - D_{k_a^m k_b^m}^{L,\theta^m}\right) = y\left(\mathrm{e}^{-x\cos\theta^m} - y\right). \end{aligned} \tag{A2}$$

Based on the results of the L and R detectors, denoted as $\left\{C_m^L, C_m^R\right\} \in \mathbb{Z}_2$ respectively, the click is retained only when the condition $C_m^L \oplus C_m^R = C_m = 1$ is satisfied.

The overall gain $q_{k_a^m k_b^m}$ can be given by

$$\begin{aligned} q_{k_a^m k_b^m} &= \Pr\left(C_m = 1 | k_a^m k_b^m\right) = \int_0^{2\pi} q_{k_a^m k_b^m}^{\theta^m} \mathrm{d}\theta^m \\ &= 2y\left[I_0(x) - y\right], \end{aligned} \tag{A3}$$

where $q_{k_a^m k_b^m}^{\theta^m} = q_{k_a^m k_b^m}^{L,\theta^m} + q_{k_a^m k_b^m}^{R,\theta^m}$ and $I_0(x)$ represents the zero-order modified Bessel function of the first kind. The average response probability p of each round is

$$\begin{aligned} p &= \Pr(C_m = 1) \sum_{k_a k_b} p_{k_a^m} p_{k_b^m} \Pr\left(C_m = 1 | k_a^m k_b^m\right) \\ &= \sum_{k_a k_b} p_{k_a^m} p_{k_b^m} q_{k_a^m k_b^m}. \end{aligned} \tag{A4}$$

Considering the influence of the detector dead time and after-pulse effect, the expected pairing number per pulse [27] is given by

$$r_p = \left[\frac{1}{p(1-p)^{l_{\min}-1} - (1-p)^{l_{\max}}} + \frac{1}{p}\right]^{-1}, \tag{A5}$$

where $l_{\min}$ and $l_{\max}$ is the minimum pairing interval and the maximal pairing interval, respectively.

Given the characteristics of conditional probability, the number of the effective detection [39] for the Z-pair or 0-pair can be calculated as follows:

$$\begin{aligned} n_k^Z &= N r_p \sum_{(k_a,k_b)=k} \Pr\left(k_a^m k_a^n k_b^m k_b^n | C_m = C_n = 1\right) \\ &= N r_p \sum_{(k_a,k_b)=k} \left(\frac{\Pr\left(k_a^m k_b^m\right)\Pr\left(C_m = 1 | k_a^m k_b^m\right)}{\Pr(C_m = 1)} \times \frac{\Pr\left(k_a^n k_b^n\right)\Pr\left(C_n = 1 | k_a^n k_b^n\right)}{\Pr(C_n = 1)}\right) \\ &= \frac{N r_p}{p^2} \sum_{(k_a,k_b)=k} p_{k_a^m} p_{k_a^n} p_{k_b^m} p_{k_b^n} q_{k_a^m k_b^m} q_{k_a^n k_b^n}, \end{aligned} \tag{A6}$$

where $k \in \{(\mu,\mu),(\mu,\nu),(\mu,0),(\nu,\mu),(0,\mu),(\nu,\nu),(\nu,0),(0,\nu),(0,0)\}$. The number of the error effective detections for $k \in \{(\mu,0),(0,\mu),(\nu,0),(0,\nu),(0,0)\}$ is

$$t_{k,0}^Z = \frac{n_k^Z}{2}, \tag{A7}$$

whereas for $k \in \{(\mu,\mu),(\mu,\nu),(\nu,\mu),(\nu,\nu)\}$, the number of the error effective detections is

$$\begin{aligned} t_{k,0}^{Z} &= Nr_p \sum_{(k_a,k_b)=k} \Pr\left(k_a^m = k_b^m = 0 | C_m = C_n = 1\right) + Nr_p \sum_{(k_a,k_b)=k} \Pr\left(k_a^n = k_b^n = 0 | C_m = C_n = 1\right) \\ &= \frac{Nr_p}{p^2} \sum_{(k_a,k_b)=k,k_a^m=k_a^m=0} p_{k_a^m} p_{k_b^m} p_{k_a^n} p_{k_b^n} q_{k_a^m k_b^m} q_{k_a^n k_b^n} + \frac{Nr_p}{p^2} \sum_{(k_a,k_b)=k,k_a^n=k_a^n=0} p_{k_a^m} p_{k_b^m} p_{k_a^n} p_{k_b^n} q_{k_a^m k_b^m} q_{k_a^n k_b^n}. \end{aligned} \tag{A8}$$

Considering the misalignment-error of the Z-pair, the number of the error effective detections is adjusted to

$$t_k^Z = \left(1 - e_d^Z\right) t_{k,0}^Z + e_d^Z \left(n_k^Z - t_{k,0}^Z\right), \tag{A9}$$

where e_d^Z is the misalignment-error of the Z-pair.

Before performing key mapping, similar to equation (A6), the number of the effective detections for the X-pair can be expressed as

$$n_{k,\mathrm{all}}^X = \frac{Nr_p}{p^2} \sum_{(k_a,k_b)=k} p_{k_a^m} p_{k_a^n} p_{k_b^m} p_{k_b^n} q_{k_a^m k_b^m} q_{k_a^n k_b^n}, \tag{A10}$$

where $k \in \{(2\mu,2\mu),(2\mu,2\nu),(2\nu,2\mu),(2\nu,2\nu),(2\mu,0),(0,2\mu),(2\nu,0),(0,2\nu)\}$.

After the announcement of the alignment angle δ_a and δ_b, Alice and Bob retain the data pair where $|\delta_a - \delta_b| \leqslant \Delta$ or $|\delta_a - \delta_b| \geqslant \pi - \Delta$. The number of the reversed effective detection can be written as

$$\begin{aligned} n_k^X &= n_{k,\mathrm{all}}^X \frac{\int_0^{2\pi}\int_{-\Delta}^{+\Delta} q_{k_a^m k_b^m}^{\theta^m} q_{k_a^m k_b^m}^{\theta^m+\delta} \mathrm{d}\delta\mathrm{d}\theta^m}{\int_0^{2\pi}\int_0^{2\pi} q_{k_a^m k_b^m}^{\theta^m} q_{k_a^m k_b^m}^{\theta^m+\delta} \mathrm{d}\delta\mathrm{d}\theta^m} + n_{k,\mathrm{all}}^X \frac{\int_0^{2\pi}\int_{\pi-\Delta}^{\pi+\Delta} q_{k_a^m k_b^m}^{\theta^m} q_{k_a^m k_b^m}^{\theta^m+\delta} \mathrm{d}\delta\mathrm{d}\theta^m}{\int_0^{2\pi}\int_0^{2\pi} q_{k_a^m k_b^m}^{\theta^m} q_{k_a^m k_b^m}^{\theta^m+\delta} \mathrm{d}\delta\mathrm{d}\theta^m} \\ &= \frac{Nr_p}{p^2} \frac{2\Delta}{\pi} p_{k_a^m} p_{k_a^n} p_{k_b^m} p_{k_b^n} \left(4y^4 - 8y^3 I_0(x) + y^2 \int_0^{2\pi}\int_{-\Delta}^{+\Delta} \frac{\left(\mathrm{e}^{x\cos\theta^m} + \mathrm{e}^{-x\cos\theta^m}\right)\left(\mathrm{e}^{x\cos(\theta^m+\delta)} + \mathrm{e}^{-x\cos(\theta^m+\delta)}\right)}{2\pi \times 2\Delta} \mathrm{d}\delta\mathrm{d}\theta^m\right) \\ &\approx \frac{Nr_p}{p^2} \frac{2\Delta}{\pi} p_{k_a^m} p_{k_a^n} p_{k_b^m} p_{k_b^n} \left(4y^4 - 8y^3 I_0(x) + 2y^2 \left(I_0\left(x\sqrt{2-2\cos\Delta}\right) + I_0\left(x\sqrt{2+2\cos\Delta}\right)\right)\right), \end{aligned} \tag{A11}$$

where $\delta = \delta_a - \delta_b$, $k \in \{(2\mu,2\mu),(2\mu,2\nu),(2\nu,2\mu),(2\nu,2\nu)\}$. The number of the corresponding error effective detections is

$$\begin{aligned} t_{k,0}^X &= n_{k,\mathrm{all}}^X \frac{\int_0^{2\pi}\int_{-\Delta}^{+\Delta} \left(q_{k_a^m k_b^m}^{L,\theta^m} q_{k_a^m k_b^m}^{R,\theta^m+\delta} + q_{k_a^m k_b^m}^{R,\theta^m} q_{k_a^m k_b^m}^{L,\theta^m+\delta}\right) \mathrm{d}\delta\mathrm{d}\theta^m}{\int_0^{2\pi}\int_0^{2\pi} q_{k_a^m k_b^m}^{\theta^m} q_{k_a^m k_b^m}^{\theta^m+\delta} \mathrm{d}\delta\mathrm{d}\theta^m} + n_{k,\mathrm{all}}^X \frac{\int_0^{2\pi}\int_{\pi-\Delta}^{\pi+\Delta} \left(q_{k_a^m k_b^m}^{L,\theta^m} q_{k_a^m k_b^m}^{R,\theta^m+\delta} + q_{k_a^m k_b^m}^{R,\theta^m} q_{k_a^m k_b^m}^{L,\theta^m+\delta}\right) \mathrm{d}\delta\mathrm{d}\theta^m}{\int_0^{2\pi}\int_0^{2\pi} q_{k_a^m k_b^m}^{\theta^m} q_{k_a^m k_b^m}^{\theta^m+\delta} \mathrm{d}\delta\mathrm{d}\theta^m} \\ &= \frac{Nr_p}{p^2} \frac{2\Delta}{\pi} p_{k_a^m} p_{k_a^n} p_{k_b^m} p_{k_b^n} \left(2y^4 - 4y^3 I_0(x) + y^2 \int_0^{2\pi}\int_{-\Delta}^{+\Delta} \frac{\mathrm{e}^{x(\cos\theta^m - \cos(\theta^m+\delta))} + \mathrm{e}^{-x(\cos\theta^m - \cos(\theta^m+\delta))}}{2\pi \times 2\Delta} \mathrm{d}\delta\mathrm{d}\theta^m\right) \\ &\approx \frac{Nr_p}{p^2} \frac{2\Delta}{\pi} p_{k_a^m} p_{k_a^n} p_{k_b^m} p_{k_b^n} \left(2y^4 - 4y^3 I_0(x) + 2y^2 I_0\left(x\sqrt{2-2\cos\Delta}\right)\right). \end{aligned} \tag{A12}$$

Due to the complexity of the integral calculations in equations (A11) and (A12), we have provided approximate results to reduce the computational burden. This approximation significantly reduces the computational complexity and offers a substantial time advantage, particularly when optimizing the intensity and probability of the decoy states.

Furthermore, the data where $k \in \{(2\mu,0),(0,2\mu),(2\nu,0),(0,2\nu)\}$ is also preserved. The number of the effective detections for this situation is

$$\begin{aligned} n_k^X &= n_{k,\mathrm{all}}^X, \\ t_k^X &= \frac{n_k^X}{2}. \end{aligned} \tag{A13}$$

Considering the misalignment-error of the X-pair, the number of the error effective detections is adjusted to

$$t_k^X = \left(1 - e_d^X\right) t_{k,0}^X + e_d^X \left(n_k^X - t_{k,0}^X\right), \tag{A14}$$

where e_d^X is the misalignment-error of the X-pair.

Appendix B. The simplification process of equations (A11) and (A12)

For convenience, we define the integral in equation (A12) as

$$G=\int_{0}^{2\pi}\int_{-\Delta}^{+\Delta}\frac{e^{x(\cos\theta^{m}-\cos(\theta^{m}+\delta))}+e^{-x(\cos\theta^{m}-\cos(\theta^{m}+\delta))}}{2\pi\times 2\Delta}\mathrm{d}\delta\mathrm{d}\theta^{m}. \tag{B1}$$

The integration variable δ spans from $-\Delta$ to Δ, encompassing all conceivable values within this interval. When Δ is very small, typically set to $\frac{\pi}{16}$ [27, 28, 30], G can be approximated as

$$G\approx\int_{0}^{2\pi}\frac{e^{x(\cos\theta^{m}-\cos(\theta^{m}+\Delta))}+e^{-x(\cos\theta^{m}-\cos(\theta^{m}+\Delta))}}{2\pi}\mathrm{d}\theta^{m}. \tag{B2}$$

Concerning the term $\cos\theta^{m}-\cos(\theta^{m}+\Delta)$ in the numerator of equation (B2), we can simplify it as follows

$$\begin{aligned}\cos\theta^{m}-\cos(\theta^{m}+\Delta)&=\cos\theta^{m}-(\cos\theta^{m}\cos\Delta-\sin\theta^{m}\sin\Delta)\\&=(1-\cos\Delta)\cos\theta^{m}+\sin\Delta\sin\theta^{m}\\&=\sqrt{(1-\cos\Delta)^{2}+\sin^{2}\Delta}\left(\frac{1-\cos\Delta}{\sqrt{(1-\cos\Delta)^{2}+\sin^{2}\Delta}}\cos\theta^{m}+\frac{\sin\Delta}{\sqrt{(1-\cos\Delta)^{2}+\sin^{2}\Delta}}\sin\theta^{m}\right)\\&=\sqrt{2-2\cos\Delta}\sin(\theta^{m}+\gamma),\end{aligned} \tag{B3}$$

where

$$\begin{aligned}\sin\gamma&=\frac{1-\cos\Delta}{\sqrt{(1-\cos\Delta)^{2}+\sin^{2}\Delta}},\\\cos\gamma&=\frac{\sin\Delta}{\sqrt{(1-\cos\Delta)^{2}+\sin^{2}\Delta}}.\end{aligned} \tag{B4}$$

Therefore, G can be reformulated as

$$G\approx\frac{1}{2\pi}\int_{0}^{2\pi}\left(e^{x\sqrt{2-2\cos\Delta}\sin(\theta^{m}+\gamma)}+e^{-x\sqrt{2-2\cos\Delta}\sin(\theta^{m}+\gamma)}\right)\mathrm{d}\theta^{m}=2I_{0}\left(x\sqrt{2-2\cos\Delta}\right). \tag{B5}$$

Similarly, we can obtain

$$\int_{0}^{2\pi}\int_{-\Delta}^{+\Delta}\frac{\left(e^{x\cos\theta^{m}}+e^{-x\cos\theta^{m}}\right)\left(e^{x\cos(\theta^{m}+\delta)}+e^{-x\cos(\theta^{m}+\delta)}\right)}{2\pi\times 2\Delta}\mathrm{d}\delta\mathrm{d}\theta^{m}\approx 2\left(I_{0}\left(x\sqrt{2-2\cos\Delta}\right)+I_{0}\left(x\sqrt{2+2\cos\Delta}\right)\right). \tag{B6}$$

Our approximate estimates for the laborious integrals in equations (A11) and (A12) are tight. For comparison, we define the ratio

$$\begin{aligned}W_{n}&=\frac{\int_{0}^{2\pi}\int_{-\Delta}^{+\Delta}\frac{\left(e^{x\cos\theta^{m}}+e^{-x\cos\theta^{m}}\right)\left(e^{x\cos\theta^{m}}+e^{-x\cos\theta^{m}}\right)}{2\pi\times 2\Delta}\mathrm{d}\delta\mathrm{d}\theta^{m}}{2\left(I_{0}\left(x\sqrt{2-2\cos\Delta}\right)+I_{0}\left(x\sqrt{2+2\cos\Delta}\right)\right)},\\W_{t}&=\frac{\int_{0}^{2\pi}\int_{-\Delta}^{+\Delta}\frac{e^{x(\cos\theta^{m}-\cos(\theta^{m}+\delta))}+e^{-x(\cos\theta^{m}-\cos(\theta^{m}+\delta))}}{2\pi\times 2\Delta}\mathrm{d}\delta\mathrm{d}\theta^{m}}{2I_{0}\left(x\sqrt{2-2\cos\Delta}\right)}.\end{aligned} \tag{B7}$$

Figure 6 illustrates the variation of W_n and W_t with respect to distance, with the photon intensities fixed at $k_a^m=0.2$ and $k_b^m=0.2$. It can be observed that at longer distances, the ratios W_n and W_t converge to approximately 1, which means that our approximation closely resembles the ideal scenario. Even at shorter distances, the maximum fluctuations of W_n and W_t occur at 0 kilometers, with the maximum fluctuation ratios not exceeding 1% and 0.2%, respectively. This phenomenon occurs because as the distance increases, the variable x decreases. Consequently, equations (B1) and (B2) become less sensitive to changes in δ or Δ when x is small. The integration calculations consume significant time during the parameter optimization procedure. However, our proposed approximate calculation allows for quick results without compromising accuracy.

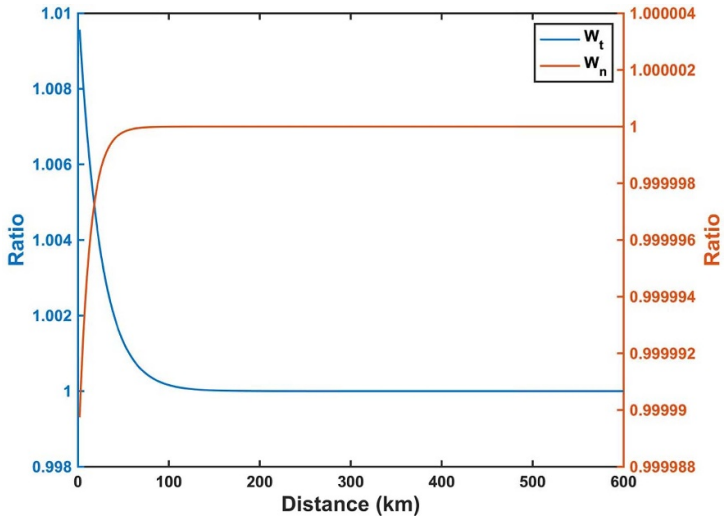

Figure 6. The variations of W_n and W_t with respect to distance, where $k_a^m = 0.2$, $k_b^m = 0.2$, $\Delta = 16$. As the distance increases, the values of W_n and W_t converge to 1.

Appendix C. Parameters in equation (3)

The parameters in y_{11}^Z are defined as

$$\begin{aligned}
\tilde{n}^Z_{(\nu,\nu)} &= \frac{n^Z_{(\nu,\nu)}}{N_{(\nu,\nu)}} - \frac{a_0^{\nu,U} n^Z_{(\omega,\nu)}}{a_0^{\omega,L} N_{(\omega,\nu)}} - \frac{b_0^{\nu,U} n^Z_{(\nu,\omega)}}{b_0^{\omega,L} N_{(\nu,\omega)}} + \frac{a_0^{\nu,L} b_0^{\nu,L} n^Z_{(\omega,\omega)}}{a_0^{\omega,U} b_0^{\omega,U} N_{(\omega,\omega)}}, \\
\tilde{n}^Z_{(\mu,\mu)} &= \frac{n^Z_{(\mu,\mu)}}{N_{(\mu,\mu)}} - \frac{a_0^{\mu,L} n^Z_{(\omega,\mu)}}{a_0^{\omega,U} N_{(\omega,\mu)}} - \frac{b_0^{\mu,L} n^Z_{(\mu,\omega)}}{b_0^{\omega,U} N_{(\mu,\omega)}} + \frac{a_0^{\mu,U} b_0^{\mu,U} n^Z_{(\omega,\omega)}}{a_0^{\omega,L} b_0^{\omega,L} N_{(\omega,\omega)}}, \\
\sigma_A^Z &= \frac{a_0^{\mu,U} a_1^{\omega,U}}{a_0^{\omega,L} a_1^{\mu,L}}, \sigma_B^Z = \frac{b_0^{\mu,U} b_1^{\omega,U}}{b_0^{\omega,L} b_1^{\mu,L}}, \sigma_C^Z = \frac{a_0^{\nu,U} a_1^{\omega,U} b_0^{\nu,U} b_1^{\omega,U}}{a_0^{\omega,L} a_1^{\nu,L} b_0^{\omega,L} b_1^{\nu,L}},
\end{aligned} \tag{C1}$$

where $N_k = \frac{N}{2} \sum_k p_{k_a}^m p_{k_b}^m p_{k_a}^n p_{k_b}^n$.

The single-photon bit error rate of X-pair $e_{11}^{X,\mathrm{bit}}$ can be expressed as

$$\begin{aligned}
e_{11}^{X,\mathrm{bit}} &\leqslant \frac{a_1^{2\nu,U} b_1^{2\nu,U} \tilde{t}^X_{(2\nu,2\nu)}}{\left(a_1^{2\nu,L} b_1^{2\nu,L}\right)^2 (1 - \sigma_A^X - \sigma_B^X) y_{11}^Z}, \\
\tilde{t}_{(2\mu,2\mu)} &= \frac{t_{(2\nu,2\nu)}}{N_{(2\nu,2\nu)}} - \frac{a_0^{2\nu,L} t_{(2\omega,2\nu)}}{a_0^{2\omega,U} N_{(2\omega,2\nu)}} - \frac{b_0^{2\nu,L} t_{(2\nu,2\omega)}}{b_0^{2\omega,U} N_{(2\nu,2\omega)}} + \frac{a_0^{2\nu,U} b_0^{2\nu,U} t_{(2\omega,2\omega)}}{a_0^{2\omega,L} b_0^{2\omega,L} N_{(2\omega,2\omega)}}, \\
\sigma_A^X &= \frac{a_0^{2\mu,U} a_1^{2\omega,U}}{a_0^{2\omega,L} a_1^{2\mu,L}}, \sigma_B^X = \frac{b_0^{2\mu,U} b_1^{2\omega,U}}{b_0^{2\omega,L} b_1^{2\mu,L}},
\end{aligned} \tag{C2}$$

where $N_{(2\nu,2\nu)} = \frac{N\Delta}{\pi} p_\nu^m p_\nu^m p_\nu^n p_\nu^n$, the other N_k is $N_k = \frac{N}{2} \sum_k p_{k_a}^m p_{k_b}^m p_{k_a}^n p_{k_b}^n$.

Appendix D. The details of key distillation

Key distillation primarily comprises error correction (including key reconciliation and error verification) and privacy amplification. The primary tool utilized for analyzing the effect of finite key sizes is the universally composable framework [57]. After the error correction step, the MP-QKD protocol either outcomes a pair of key bit strings $\boldsymbol{S}$ and $\boldsymbol{S}'$ for Alice and Bob, or a symbol $\perp$ to indicate the abort of the protocol. Ideally, the correctness condition is met if $\boldsymbol{S} = \boldsymbol{S}'$. However, in finite key analysis, this guarantee is unattainable. In practice, this implies that we need to allow for some minuscule errors. we say that a protocol is $\varepsilon_{\mathrm{cor}}$-correct if $\Pr\left(\boldsymbol{S} = \boldsymbol{S}'\right) \leqslant \varepsilon_{\mathrm{cor}}$, that is the probability that Alice's and Bob's key bit strings are not identical does not exceed $\varepsilon_{\mathrm{cor}}$.

We define the set $\mathcal{Z}$, which denotes situations where Alice and Bob choose the same basis Z and Charlie achieves a successful measurement. Alice and Bob utilize the random bits from $\mathcal{Z}$ to generate the raw key bit strings $\boldsymbol{Z}$ and $\boldsymbol{Z}'$, respectively. Alice sends up to $\lambda_{\mathrm{EC}} = fM_{(\mu,\mu)}h\left(E_{(\mu,\mu)}\right)$ bits to Bob for key reconciliation, through which Bob derives an estimate $\hat{\boldsymbol{Z}}$ of $\boldsymbol{Z}$ with a key reconciliation protocol. Nevertheless, numerous key reconciliation protocols, such as Cascade [58, 59], Winnow [60], and low-density parity-check[58], fail to ensure absolute conformity between the reconciled keys of Alice and Bob. Therefore, error verification [48], typically accomplished by comparing the hash values of the reconciled keys, stands as an essential step in QKD. Alice computes a hash of $\boldsymbol{Z}$ of length $\log_2\frac{2}{\varepsilon_{\mathrm{cor}}}$ with a random universal$_2$ hash function [42], which she sends to Bob together with the hash. They compare the random hash values of their corrected keys hash($\boldsymbol{Z}$) and hash($\hat{\boldsymbol{Z}}$) with failure probability $\varepsilon_{\mathrm{hash}}$, which means that identical probability of key bit strings $\boldsymbol{S}$ and $\boldsymbol{S}'$ is more than $1-\varepsilon_{\mathrm{hash}}$. It is still considered correct, where $\boldsymbol{S}=\boldsymbol{S}'=\perp$, in spite of the protocol is aborted. Consequently, the correctness of the protocol is $\varepsilon_{\mathrm{cor}}=\varepsilon_{\mathrm{hash}}$.

To ensure the security of final secure keys, Alice and Bob employ the privacy amplification based on the Quantum Leftover Hash Lemma [40–42], which offers a clear operational interpretation of smooth min-entropy. According to a random universal$_2$ hash function, Alice and Bob can extract a $\varepsilon_{\mathrm{sec}}$-secret string of length ℓ from the raw key $\boldsymbol{Z}$ [42],

$$\varepsilon_{\mathrm{sec}} = 2\varepsilon + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon}(\boldsymbol{Z}|\boldsymbol{E}')}}, \tag{D1}$$

where $\boldsymbol{E}'$ represents all information Eve obtained from $\boldsymbol{Z}$ during the protocol. The smooth min-entropy, $H_{\min}^{\varepsilon}(\boldsymbol{Z}|\boldsymbol{E}')$ quantifies the maximum probability that Eve can accurately guess $\boldsymbol{Z}$ given $\boldsymbol{E}'$. Based on a chain-rule inequality for smooth entropies [61], we have

$$H_{\min}^{\varepsilon}(\boldsymbol{Z}|\boldsymbol{E}') \geqslant H_{\min}^{\varepsilon}(\boldsymbol{Z}|\boldsymbol{E}) - \lambda_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}}, \tag{D2}$$

where $\boldsymbol{E}$ is the information of before error correction, $\lambda_{\mathrm{EC}}+\log_2\frac{2}{\varepsilon_{\mathrm{cor}}}$ is the maximum amount of information about $\boldsymbol{Z}$ revealed to Eve during the error correction step. Furthermore, we can decompose $\boldsymbol{Z}$ as $\boldsymbol{Z}_{11}\boldsymbol{Z}_{\mathrm{rest}}$, where $\boldsymbol{Z}_{11}$ is the bits in which both Alice and Bob have each sent a single photon, $\boldsymbol{Z}_{\mathrm{rest}}$ is the rest of bits. In accordance with a chain rules for smooth entropies, we have

$$H_{\min}^{\varepsilon}(\boldsymbol{Z}|\boldsymbol{E}) \geqslant H_{\min}^{\bar{\varepsilon}}(\boldsymbol{Z}_{11}|\boldsymbol{Z}_{\mathrm{rest}}\boldsymbol{E}) + H_{\min}^{\varepsilon'}(\boldsymbol{Z}_{\mathrm{rest}}|\boldsymbol{E}) - 2\log_2\frac{\sqrt{2}}{\hat{\varepsilon}}, \tag{D3}$$

where $\varepsilon = 2\bar{\varepsilon}+\varepsilon'+\hat{\varepsilon}$ and $H_{\min}^{\varepsilon'}(\boldsymbol{Z}_{\mathrm{rest}}|\boldsymbol{E}) \geqslant 0$.

Here, we denote the Z basis as $|10\rangle, |01\rangle$, and X basis as $\frac{1}{\sqrt{2}}\left(|10\rangle + \mathrm{e}^{\mathrm{i}\varphi}|01\rangle\right), \frac{1}{\sqrt{2}}\left(|10\rangle - \mathrm{e}^{\mathrm{i}\varphi}|01\rangle\right)$, where φ can be an arbitrary value. Obviously, the single-photon component prepared in the Z basis and X basis are mutually unbiased. We employ the bit string $\boldsymbol{X}_{11}$ ($\boldsymbol{X}'_{11}$) to indicate the outcomes Alice (Bob) would have obtained if they have measured in the X basis rather than the Z basis. According to the uncertainty relation of smooth min- and max-entropy, we have

$$H_{\min}^{\bar{\varepsilon}}(\boldsymbol{Z}_{11}|\boldsymbol{Z}_{\mathrm{rest}}\boldsymbol{E}) \geqslant M_{11}^{Z} - H_{\max}^{\bar{\varepsilon}}(\boldsymbol{X}_{11}|\boldsymbol{X}'_{11}), \tag{D4}$$

where M_{11}^{Z} is the lower bound of the length of $\boldsymbol{Z}_{11}$. And we denote $e_{11} = (\boldsymbol{X}_{11}\oplus\boldsymbol{X}'_{11})/M_{11}^{Z}$, which is the mismatching rate of $\boldsymbol{X}_{11}$ and $\boldsymbol{X}'_{11}$ and cannot be direct observed in the experiment. Through random-sampling theory (without replacement) [47–50], we can obtain the estimated value of e_{11} as $e_{11}^{Z,\mathrm{ph}}$. If the the probability that $e_{11} \geqslant e_{11}^{Z,\mathrm{ph}}$ is no larger than $\bar{\varepsilon}^2$, we have

$$H_{\max}^{\bar{\varepsilon}}(\boldsymbol{X}_1|\boldsymbol{X}'_1) \leqslant M_{11}^{Z} h\left(e_{11}^{Z,\mathrm{ph}}\right). \tag{D5}$$

We can set $\varepsilon'=0$ without compromising security and $\varepsilon_{\mathrm{sec}} = 2\hat{\varepsilon}+4\bar{\varepsilon}+\varepsilon_{\mathrm{PA}}$. And $\bar{\varepsilon}=\sqrt{\varepsilon_1+\varepsilon_e}$, where ε_1 and ε_e are the failure probability for estimating the terms of M_{11}^{Z} and $e_{11}^{Z,\mathrm{ph}}$. $\varepsilon_{\mathrm{PA}}$ is the failure probability of privacy amplification. Finally, we have

$$\ell \geqslant M_{11}^{Z}\left[1-h\left(e_{11}^{Z,\mathrm{ph}}\right)\right] - fM_{(\mu,\mu)}h\left(E_{(\mu,\mu)}\right) - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{1}{\sqrt{2}\hat{\varepsilon}\varepsilon_{\mathrm{PA}}}. \tag{D6}$$

The protocol is ε-secure, where $\varepsilon = \varepsilon_{\mathrm{sec}}+\varepsilon_{\mathrm{cor}}$.

Appendix E. Statistical fluctuation analysis

The Chernoff–Hoeffding method provides a means to estimate the expected value based on the observed values [62]. Given an observed quantity χ, the upper and lower bounds of the expected value can be expressed as

$$\begin{aligned} E^L(\chi) &= \frac{\chi}{1+\vartheta^L}, \\ E^U(\chi) &= \frac{\chi}{1-\vartheta^L}, \end{aligned} \tag{E1}$$

where

$$\begin{aligned} \left[\frac{\mathrm{e}^{\vartheta^L}}{(1+\vartheta^L)^{1+\vartheta^L}}\right]^{\frac{\chi}{(1+\vartheta^L)}} &= \frac{1}{2}\epsilon, \\ \left[\frac{\mathrm{e}^{-\vartheta^U}}{(1-\vartheta^U)^{1-\vartheta^U}}\right]^{\frac{\chi}{(1-\vartheta^L)}} &= \frac{1}{2}\epsilon. \end{aligned} \tag{E2}$$

where ε is the failure probability.

ORCID iD

Haiqiang Ma https://orcid.org/0000-0002-1558-8877

References

[1] Lo H-K and Chau H F 1999 *Science* **283** 2050
[2] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* p 175
[4] Liao S-K *et al* 2017 *Nature* **549** 43
[5] Liao S-K *et al* 2018 *Phys. Rev. Lett.* **120** 030501
[6] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[7] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[8] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[9] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[10] Hayashi M 2007 *New J. Phys.* **9** 284
[11] Hayashi M 2007 *Phys. Rev.* A **76** 012329
[12] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[13] Ma X and Razavi M 2012 *Phys. Rev.* A **86** 062319
[14] Yu Z-W, Zhou Y-H and Wang X-B 2013 *Phys. Rev.* A **88** 062339
[15] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[16] Ma X, Zeng P and Zhou H 2018 *Phys. Rev.* X **8** 031043
[17] Lin J and Lütkenhaus N 2018 *Phys. Rev.* A **98** 042332
[18] Wang X-B, Yu Z-W and Hu X-L 2018 *Phys. Rev.* A **98** 062323
[19] Cui C, Yin Z-Q, Wang R, Chen W, Wang S, Guo G-C and Han Z-F 2019 *Phys. Rev. Appl.* **11** 034053
[20] Minder M, Pittaluga M, Roberts G L, Lucamarini M, Dynes J F, Yuan Z and Shields A J 2019 *Nat. Photon.* **13** 334
[21] Liu Y *et al* 2019 *Phys. Rev. Lett.* **123** 100505
[22] Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Woodward R I, Li M-J, Yuan Z and Shields A J 2021 *Nat. Photon.* **15** 530
[23] Chen J-P *et al* 2021 *Nat. Photon.* **15** 570
[24] Liu Y *et al* 2023 *Phys. Rev. Lett.* **130** 210801
[25] Zeng P, Zhou H, Wu W and Ma X 2022 *Nat. Commun.* **13** 3903
[26] Xie Y-M, Lu Y-S, Weng C-X, Cao X-Y, Jia Z-Y, Bao Y, Wang Y, Fu Y, Yin H-L and Chen Z-B 2022 *PRX Quantum* **3** 020315
[27] Zhu H-T *et al* 2023 *Phys. Rev. Lett.* **130** 030801
[28] Zhou L, Lin J, Xie Y-M, Lu Y-S, Jing Y, Yin H-L and Yuan Z 2023 *Phys. Rev. Lett.* **130** 250801
[29] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 1
[30] Zhu H-T *et al* 2024 *Optica* **11** 883
[31] Wang X-B 2007 *Phys. Rev.* A **75** 052301
[32] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320
[33] Zhao Y, Qi B and Lo H-K 2008 *Phys. Rev.* A **77** 052327
[34] Peng X, Jiang H, Xu B, Ma X and Guo H 2008 *Opt. Lett.* **33** 2077
[35] Peng X, Xu B and Guo H 2010 *Phys. Rev.* A **81** 042320
[36] Xu B, Peng X and Guo H 2010 *Phys. Rev.* A **82** 042301
[37] Wang G, Li Z, Qiao Y, Chen Z, Peng X and Guo H 2018 *IEEE J. Quantum Electron.* **54** 1–10
[38] Qiao Y, Wang G, Li Z, Xu B and Guo H 2019 *Phys. Rev.* A **99** 052302
[39] Wang Z-H, Wang R, Yin Z-Q, Wang S, Lu F-Y, Chen W, He D-Y, Guo G-C and Han Z-F 2023 *Commun. Phys.* **6** 265
[40] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506
[41] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[42] Renner R 2008 *Int. J. Quantum Inf.* **6** 1

[43] Hayashi M and Tsurumaru T 2012 *New J. Phys.* **14** 093014
[44] Jiang C, Yu Z-W and Wang X-B 2016 *Phys. Rev.* A **94** 062323
[45] Jiang C, Yu Z-W and Wang X-B 2017 *Phys. Rev.* A **95** 032325
[46] Jiang C, Yu Z-W and Wang X-B 2018 *Phys. Rev.* A **97** 042331
[47] Hayashi M and Nakayama R 2014 *New J. Phys.* **16** 063009
[48] Fung C-H F, Ma X and Chau H 2010 *Phys. Rev.* A **81** 012318
[49] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 *Phys. Rev.* A **89** 022307
[50] Chau H 2018 *Phys. Rev.* A **97** 040301
[51] Xie Y-M, Bai J-L, Lu Y-S, Weng C-X, Yin H-L and Chen Z-B 2023 *Phys. Rev. Appl.* **19** 054070
[52] Wang G, Chen Z, Xu B, Li Z, Peng X and Guo H 2016 *APS Division of Atomic, Molecular and Optical Physics Meeting Abstracts* vol 2016 pp K1–095 (available at: http://meetings.aps.org/link/BAPS.2016.DAMOP.K1.95)
[53] Nakata K, Tomita A, Fujiwara M, Yoshino K-i, Tajima A, Okamoto A and Ogawa K 2017 *Opt. Express* **25** 622
[54] Yoshino K-i, Fujiwara M, Nakata K, Sumiya T, Sasaki T, Takeoka M, Sasaki M, Tajima A, Koashi M and Tomita A 2018 *npj Quantum Inf.* **4** 8
[55] Mizutani A, Curty M, Lim C C W, Imoto N and Tamaki K 2015 *New J. Phys.* **17** 093011
[56] Xu F, Xu H and Lo H-K 2014 *Phys. Rev.* A **89** 052333
[57] Müller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006
[58] Watanabe Y, Matsumoto W and Imai H 2004 *Proc. Int. Symp. on Information Theory and its Applications*, (*ISITA2004, Parma, Italy*) pp 1265–9
[59] Pedersen T B and Toyran M 2015 *Quantum Inf. Comput.* **15** 419
[60] Buttler W T, Lamoreaux S K, Torgerson J R, Nickel G, Donahue C and Peterson C G 2003 *Phys. Rev.* A **67** 052303
[61] Vitanov A, Dupuis F, Tomamichel M and Renner R 2013 *IEEE Trans. Inf. Theory* **59** 2603
[62] Zhang Z, Zhao Q, Razavi M and Ma X 2017 *Phys. Rev.* A **95** 012333