Improved security bounds against the Trojan-Horse attack in decoy-state quantum key distribution

Zijian Li[1], Bingbing Zheng[1], Chengxian Zhang[1],

Zhenrong Zhang[2], Hong-Bo Xie[3], Kejin Wei[1,*]

[1]*Guangxi Key Laboratory for Relativistic Astrophysics,*

School of Physical Science and Technology,

Guangxi University, Nanning 530004, China

[2]*Guangxi Key Laboratory of Multimedia Communications and Network Technology,*

School of Computer, Electronics and Information,

Guangxi University, Nanning 530004, China

[3]*Ji Hua Laboratory, Foshan City, Guangdong Province 528200, China*

[*]Corresponding author: kjwei@gxu.edu.cn

(Dated: December 27, 2023)

Abstract

In a quantum Trojan-horse attack (THA), eavesdroppers learn encoded information by injecting bright light into encoded or decoded devices of quantum key distribution (QKD) systems. These attacks severely compromise the security of non-isolated systems. Thus, analytical security bound was derived in previous studies. However, these studies achieved poor performance unless the devices were strongly isolated. Here, we present a numerical method for achieving improved security bound for a decoy-state QKD system under THAs. The developed method takes advantage of the well-established numerical framework and significantly outperforms previous analytical bounds regarding the achievable final key and secure transmitted distance. The results provide a new tool for investigating the efficient security bounds of THA in practical decoy-state QKD systems. This study constitutes an important step toward securing QKD with real-life components.

I. INTRODUCTION

Quantum key distribution (QKD) [1] is a powerful tool for secure communication in the quantum information era. Currently, QKD has been experimentally proven to be applicable to several scenarios, such as optical fiber [2–12] and free-space [13–16] channels. Several small-scale networks [17–19] have been tested in the field, and a satellite-to-ground large-scale QKD network has been reported [20]. Recently, the recorded repeaterless distance of QKD has reached 830 km [21].

Nevertheless, some significant challenges remain in the broad application of QKD technology [22, 23]. In particular, bridging the gap between realistic devices and idealized models used in security proofs is crucial [23, 24]. In particular, the eavesdropper (Eve) has exploited such deviations, such as source flaws [25, 26] and detector-efficiency mismatch [27–30], to perform several subtle quantum hacking attacks [29, 31, 32].

The Trojan-horse attack (THA) is a well-known hacking strategy in the QKD community [33, 34]. In this attack, Eve illuminates bright light at encoders in legitimate users (namely, Alice and Bob) and subsequently measures the back-reflection to probe information regarding how the photon string has been encoded. In this way, Eve can break the critical assumption that no unwanted information about the settings in Alice and Bob's devices is leaked to Eve [35, 36] in most QKD security proofs without disturbing the encoded quantum states. Such assumptions are rigorously required even in device-independent QKD [37–39]. THA has been proven feasible for most practical components in QKD systems [40, 41], even in small-scale chip-based devices [42]. The earliest versions of commercial QKD systems were reported to be of considerable risk to THA [43].

Two major countermeasures exist for restoring QKD security during THA. The first one is the so-call "patches," where Alice can use watch-dog devices to monitor unwanted injected light or use additional isolators to bound the intensity of the injected light. However, such countermeasures are *ad hoc* and can be potentially compromised by unanticipated attacks. For example, the authors [44] reported that the isolation component against a Trojan-horse attack could be decreased using a high-power laser.

The second countermeasure is considering the effect of side channels due to a Trojan-horse attack in the security proof. This countermeasure was first performed by Lucamarini et al. [45] using a refinement of the well-known GLLP approach [36]. In the remainder

of the paper, we refer to this countermeasure the "refined GLLP" approach for simplification. After that, in [46], the asymptotic security bound for decoy-state BB84 QKD under information leakage from a legitimate user's intensity and phase device was investigated. Subsequently, the method was extended to a finite-key regime [47, 48] and applied to decoy-state measurement-device-independent (MDI) [49] and sending-or-not-sending twinfield QKD [50]. Unfortunately, the achieved secret key rate of the refined GLLP is poor unless good isolation of the transmitting unit is obtained.

In this paper, we present a numerical method that improves the security bounds for decoy-state QKD protocols under THAs. Specifically, we considered two important protocols: decoy-state BB84 [51, 52] and decoy-state MDI-QKD [53, 54]. The decoy-state BB84 is the most mature method and is widely applied in practice. In contrast, the decoy-state MDI-QKD can remove all detector-side-channel attacks; this method has attracted considerable interest. The proposed method comprises two main components. First, we use the numerical framework recently reported in [55]. This allowed us to analyze the BB84 and MDI-QKD protocols using a finite number of decoy states. Second, we exploit the concept of a source-replacement scheme [56], which allows us to incorporate the potential information leakage due to THAs into the numerical framework. Therefore, the proposed method takes full advantage of the numerical framework for calculating key rates for practical QKD systems, which outperformed the analytical method in previous studies [57–60]. Benefitting from the tight bound provided by the numerical framework, the proposed method significantly improves the achievable distance and distilled secret key rate for decoy-state BB84 and MDI-QKD protocols under THAs compared with the refined GLLP approach.

The remainder of this paper is organized as follows. In Sec. II, the methodology used in this study is introduced. Subsequently, we use the proposed numerical method to analyze the decoy-state BB84 and MDI protocols in Sec. III. In Sec. IV, we describe the simulation performed to compare the proposed method with the refined GLLP approach. Finally, we conclude this study in Sec. V.

II. METHOD

Here, we introduce the methodology to bound a secure key rate for decoy-state BB84 and MDI-QKD under THAs. We briefly review the numerical framework presented in [55] and

explain how to use a source-replacement scheme to incorporate potential information leakage due to THAs into the numerical framework. Furthermore, we give an intuitive explanation that our numerical method outperforms the refined GLLP method.

A. Numerical framework for decoy-state QKD

We first provide a brief description of the numerical framework for decoy-state QKD, first introduced in [61] and then developed the case of a finite number of decoy states proposed by Wang et al. [55]. The details of this process can be found in [55]. A simple step-by-step descirption of the decoy-state QKD protocol based on entanglement scheme in the numerical framework is as follows:

1. **State preparation and measurement:** Alice and Bob each receive phase randomized weak coherent states in four BB84 states $\{H, V, D, A\}$ with a mean photon number μ as signal states or mean photon number v as decoy states from a source. Than Alice (Bob) randomly select POVMs $P^A = \{P_i^A\}$ $(P^B = \{P_j^B\})$ and to measure the received quantum states.

2. **Testing:** Alice and Bob select a portion of their preparation and measurement data to publish, which includes state preparation, basis selection, and measurement results for signal state events and decoy state events. This data is then used to decide whether the protocol should proceed.

3. **Announcement, sifting and postselection:** In each round, Bob announces the basis selection, and Alice makes her choice based on Bob's announcement. She then discards the data that is inconsistent with Bob's basis selection and informs Bob of the discarded results. This process can be represented using the Kraus operator $\{K_i\}$.

4. **key mapping:** Alice maps the data retained through the above steps to the raw key. This can be expressed using the key mapping operator $\{Z_j\}$.

5. **Error correction and privacy amplification:** Alice and Bob perform standard error correction, and then they proceed to use the privacy amplification protocol to obtain the shared key.

In a well-established numerical framework [57], the secure key rate calculation for the above decoy QKD was treated as an optimization problem, which can be written as follows:

$$R = \min_{\rho_{AB} \in S} f(\rho_{AB}) - p_{\text{pass}} \times \text{leak}_{\text{obs}}^{\text{EC}}. \tag{1}$$

where ρ_{AB} denotes a state shared by two remote parties, Alice and Bob; $\text{leak}_{\text{obs}}^{\text{EC}}$ is the bits consumed during error correction; p_{pass} is the probability of a signal being detected and passing the basis sifting. Moreover, $f(\rho_{AB})$ is a function related to the privacy amplification, defined as follows:

$$f(\rho_{AB}) = D(\mathcal{G}(\rho_{AB}) \| \mathcal{Z}(\mathcal{G}(\rho_{AB}))). \tag{2}$$

Here, $D(\sigma \| \tau) = \text{Tr}(\sigma \log \sigma) - \text{Tr}(\sigma \log \tau)$ is the relative quantum entropy. $\mathcal{G}(\rho_{AB})$ and $\mathcal{Z}(\mathcal{G}(\rho_{AB}))$ are determined by Kraus operators K_i (representing the measurements, public announcements and postselection process) and key map operators Z_j (representing the key map), respectively. They satisfy the following expression:

$$\begin{aligned} \mathcal{G}(\rho_{AB}) &= \sum_i K_i \rho_{AB} K_i^\dagger, \\ \mathcal{Z}(\mathcal{G}(\rho_{AB})) &= \sum_j Z_j \mathcal{G}(\rho_{AB}) Z_j. \end{aligned} \tag{3}$$

The density operator ρ_{AB} is generally unknown. However, it can be bound by a set of states S obtained from the experimental data, satisfying the following equation:

$$S = \{\rho_{AB} \in \mathbf{H}_+ \mid \text{Tr}(\Gamma_k \rho_{AB}) = \gamma_k, \forall k\}, \tag{4}$$

where $\mathbf{H}_+$ is the set of positive semidefinite operators, Γ_k is the general positive operator-valued measures (POVM) elements representing the measurements performed by Alice and Bob, and γ_k are the expectation values of the measurements.

In particular, the study presented in [55] has two fundamental merits to incorporate decoy-state analysis into the above numerical framework.

First, when a phase-randomized weak coherent pulse is used in the QKD system, the photon number statistics of the pulses follow a Poisson probability distribution: $p_{\mu_i}(n) = \frac{\mu_i^n}{n!} e^{-\mu_i}$, with μ_i being the mean intensity. In this setup, the secure key rate is generated only from single photons, which can be rewritten as

$$R \geq p_1 \min_{\rho_{AB}^{(1)} \in S_1} f\left(\rho_{AB}^{(1)}\right) - p_{\text{pass}} \times \text{leak}_{\text{obs}}^{\text{EC}}, \tag{5}$$

where p_1 corresponds to the Poissonian distribution for sending a single photon number state, $\rho_{AB}^{(1)}$ is the shared state conditional to a single photon being sent, and S_1 is the domain-bounded possible values of $\rho_{AB}^{(1)}$.

Second, the decoy-state analysis can be used as a "wrapper" to generate loosened bounds for S_1, which has the following form:

$$S_1 = \left\{ \rho_{AB}^{(1)} \in \mathbf{H}_+ \mid \gamma_{1,k}^L \leq \mathrm{Tr}\left(\Gamma_k \rho_{AB}^{(1)} \right) \leq \gamma_{1,k}^U, \forall k \right\}, \tag{6}$$

where $\gamma_{1,k}^L (\gamma_{1,k}^U)$ is the lower (upper) bound of the single-photon statistics obtained from the decoy-state analysis.

Finally, the key rate for the decoy-state QKD can be calculated by running the optimization routine, based on Eq. (5), under the constraints given in Eq. (13).

B. Trojan-horse analysis

In the security proof of the QKD protocol, an essential assumption is that the devices in Alice and Bob do not leak unwanted information to Eve. A simple strategy to break this assumption is the so-called Trojan-horse attack. The attack is specifically described as follows: Eve sends a bright pulse containing Trojan-horse photons to the coding devices of legitimate users. Some Trojan-horse photons are encoded with the same quantum states prepared by legitimate users and reflected back to Eve. By analyzing the reflected Trojan-horse photons, Eve can compromise the security of the QKD system.

In the security proof of the QKD protocol, an essential assumption is that the devices in Alice and Bob do not leak unwanted information to Eve. A simple strategy to break this assumption is the so-called Trojan-horse attack. The attack is specifically described as follows. Eve sends a bright pulse containing Trojan-horse photons to the coding devices of legitimate users. Some Trojan-horse photons are encoded with the same quantum states prepared by legitimate users and reflected back to Eve. By analyzing the reflected Trojan-horse photons, Eve can compromise the security of the QKD system.

To simplify our analysis, we considered only a specific THA targeting the phase modulator in the transmitter. In this case, Eve uses a laser emitting weak coherent pulses in a coherent state $\left| \sqrt{\mu_{\mathrm{in}}} \right\rangle$ given the average photon number μ_{in}. A fraction of the pulses is encoded by carrying phase modulation information ϕ_A. These pulses are then reflected back to Eve as

$\left| e^{i\phi_A} \sqrt{\mu_{\text{out}}} \right\rangle$, where $\mu_{\text{out}} = \gamma \mu_{\text{in}}$ is the average photon number with $\gamma \ll 1$, the optical isolation of the transmitter. We can see that the light pulse retrieved by Eve is correlated to phase ϕ_A, which compromises the security of the system.

Considering a decoy-state QKD protocol, Alice sends a state $|\phi_{A_i}\rangle$ with a probability p_i, where $i = 0...N$ and N is the total number of sending quantum states. Owing to the existence of THA, the output quantum state can be written as follows:

$$|\psi_i\rangle = |\phi_{A_i}\rangle_S \otimes \left| e^{i\phi_{A_i}} \sqrt{\mu_{\text{out}}} \right\rangle_E, \tag{7}$$

where ϕ_{A_i} is the specific encoded phase in the $i-$pulse; the subscript "S" and "E" denote the signal state prepared by Alice and the Trojan-horse state obtained by Eve, respectively. Here, we assume that the THA does not affect the decoy-state analysis. Hence, the state can be straightforward in the single-photon form following the analysis described in [45, 55].

To incorporate the Trojan-horse analysis into the decoy-state numerical framework, we use a source-replacement method. The method has been used to recast prepare-and-measure protocols as entanglement-based protocols [62]. The encoder can recast the state in Eq. (7) as the entanglement state using the source-replacement scheme as follows:

$$|\Phi\rangle_{AA'E} = \sum_i \sqrt{p_i} |i\rangle_A |\psi_i\rangle_{A'E}, \tag{8}$$

where A is a registration system for storing the information $|i\rangle_A$ regarding which state Alice has prepared. Subsequently, Alice keeps system A and sends system A' to Bob through a quantum channel ξ, so that the final joint state is as follows:

$$\rho_{AB} = (\mathbb{I}_A \otimes \xi) \, \text{Tr}_E \left(|\Phi\rangle_{AA'E} \langle \Phi| \right), \tag{9}$$

where $\mathbb{I}_A$ denotes the identity channel on A. By applying the numerical optimization method described in Sec. II A to state ρ_{AB} in Eq. (9), we can calculate the final key rate by considering THAs. Furthermore, we must add additional constraints to account for the particular form of ρ_{AB}.

For the measurement, we have the following constraints:

$$\text{tr} \left(\left(\text{P}_j^A \otimes \text{P}_i^B \right) \rho_{AB} \right) = p_{ji}. \tag{10}$$

In addition to measurement constraints, in order to optimize the key rate in the presence of THA, the assumption in [57] is used: Alice has well characterized her source. In other

words, Alice strictly knows the following states

$$\rho_A = \mathrm{Tr}_B \left(\rho_{AB} \right) = \mathrm{Tr}_{A'E} \left(|\Phi\rangle_{AA'E} \langle\Phi| \right). \tag{11}$$

Therefore, we need to add constraints of the form

$$\mathrm{Tr} \left(\left(\Theta_j \otimes \mathbb{I}_B \right) \rho_{AB} \right) = \theta_j, \tag{12}$$

into the constraints Alice and Bob have on their states, where $\{\Theta_j\}$ is a set of the tomographic observables on system A.

We can see that the constraint of Eq. (10) is the measured value of the single photon component. In the case of WCP source, we cannot know it. However, we can use the decoy state analysis technology to obtain its estimated value, so we will have the following constraints:

$$\gamma_{1,k}^L \leq \mathrm{tr} \left(\left(\mathrm{P}_j^A \otimes \mathrm{P}_i^B \right) \rho_{AB} \right) \leq \gamma_{1,k}^U, \tag{13}$$

where $\gamma_{1,k}^L$ and $\gamma_{1,k}^U$ are the lower and upper bounds of POVM measurement $\mathrm{P}_j^A \otimes \mathrm{P}_i^B$ respectively. For the above constraints, we need corresponding statistical data. In practice, we can get these statistics from experiments. In the simulation, we can obtain the original statistical information of these WCP sources through the channel model. See the appendix B for the specific channel model.

C. Improved security bound under THA attack

In this section, we will explain in detail why our numerical method enables improving the key rate under THA attacks.

For clarity, let's briefly review the refined GLLP's method. In refined-GLLP approach presented in [45], the final key rate in presence of THA can be expressed as

$$R = 1 - h_2(e_X') - h_2(e_Z). \tag{14}$$

Here, e_Z is the quantum bit error rate of the signal states in the Z basis, e_X' is phase error rate of a single photon under THA, $h_2(x)$ is the binary Shannon information function. Finally, based on the analysis in [45], e_X' is given by "Bloch Sphere bound" [63], which can

be expressed the following equation:

$$\begin{aligned}
e'_X =&\, e_X + 4\Delta' \left(1 - \Delta'\right)\left(1 - 2e_X\right) \\
&+ 4\left(1 - 2\Delta'\right)\sqrt{\Delta'\left(1 - \Delta'\right)e_X\left(1 - e_X\right)}, \\
\Delta' =&\, \frac{\Delta}{Y}, \\
\Delta =&\, \frac{1}{2}\left[1 - \exp\left(-\mu_{\text{out}}\right)\cos\left(\mu_{\text{out}}\right)\right],
\end{aligned} \tag{15}$$

where e_X is the quantum bit error rate in the X basis, and Y is defined as $Y := \min\left[Y_Z^1, Y_X^1\right]$ with Y_Z^1 (Y_X^1) as the single-photon yields on the Z (X) basis.

From the above description, we can see that the refined GLLP's method essentially bounds the Eve's information by using several inequalities, which have looseness bound, resulting a poor performance of the final key rate. In contrast, the numerical method presented in Ref. [58] provides a tight bound by using two-step optimization. This advantages are feasible even in presence of THA. For a first shot, we take an ideal case (single photon case, no loss, no dark counting) as an example. The results are shown in the Fig. 1. It can seen that the numerical method outperfoms the refined GLLP's method with different leaked intensity μ_{out}. We remark that these results also are proved in Ref. [58] but it did not consider decoy-state analysis.

III.   EXAMPLES

This section provides examples of the proposed numerical approach applied to specific protocols, including decoy-state BB84 and MDI under THAs.

A.   Decoy-state BB84 QKD

Here, we consider the phase-encoding BB84 scheme. Typical units for generating the four BB84 quantum states can be found in the asymmetrical, fiber-based, phase-modulated QKD setup in Ref. [5]. In this setup, we can write the Z-basis states corresponding the phase $\phi_A = \{0, \pi\}$ as $|z_\pm\rangle := \frac{1}{\sqrt{2}}\left(|1\rangle_L|0\rangle_M \pm |0\rangle_L|1\rangle_M\right)$. Moreover, the X-basis states corresponding the phase $\phi_A = \{\pi/2, 3\pi/2\}$ can be written as $|x_\pm\rangle := \frac{1}{\sqrt{2}}\left(|1\rangle_L|0\rangle_M \pm i|0\rangle_L|1\rangle_M\right)$ for X basis, where $(|n\rangle_L)$ and $|n\rangle_M)$ denote the $n-$photon passing the long and short arm of interferometer, respectively. In the presence of THAs, the output quantum state from Alice

FIG. 1. Simulation result of key rate vs error rate for single photon BB84 protocol under Trojan attack. The key rate is plotted for different values of μ_{out}. e_d represents the intrinsic misalignment.

can be rewritten as follows:

$$
\begin{aligned}
|\psi_{z+}\rangle &= |z_+\rangle_S \otimes |+\sqrt{\mu_{\text{out}}}\rangle_E \,, \\
|\psi_{z-}\rangle &= |z_-\rangle_S \otimes |-\sqrt{\mu_{\text{out}}}\rangle_E \,, \\
|\psi_{x+}\rangle &= |x_+\rangle_S \otimes |+i\sqrt{\mu_{\text{out}}}\rangle_E \,, \\
|\psi_{x-}\rangle &= |x_-\rangle_S \otimes |-i\sqrt{\mu_{\text{out}}}\rangle_E \,.
\end{aligned}
\tag{16}
$$

By following the method described in Sec. II B, Alice can be regarded as preparing the

following states:

$$|\Phi\rangle_{AA'E} = \sqrt{p_{z+}}|0\rangle_A |\psi_{z+}\rangle_{A'E} + \sqrt{p_{z-}}|1\rangle_A |\psi_{z-}\rangle_{A'E} +$$
$$\sqrt{p_{x+}}|2\rangle_A |\psi_{x+}\rangle_{A'E} + \sqrt{p_{x-}}|3\rangle_A |\psi_{x-}\rangle_{A'E}, \tag{17}$$

where Alice, with a probability p_α, is the probability of sending state $\alpha \in \{z+, z-, x+, x-\}$ from Alice. In the communication stage, Alice first sends part of the state $|\Phi\rangle_{AA'}$ to Bob (i.e., system A') using the quantum channel ξ; thus, we obtain the following joint state:

$$\rho_{AB} = (\mathbb{I}_A \otimes \xi) \operatorname{Tr}_E (|\Phi\rangle_{AA'E}(\Phi\,|) . \tag{18}$$

The measurement considered the following constraints (see Appendix A for detailed description of measurement operators):

$$\operatorname{Tr}\left(\left(P_j^A \otimes P_i^B\right) \rho_{AB}\right) = p_{ji}.$$
$$\operatorname{Tr}\left(\left(\Theta_j \otimes \mathbb{I}_B\right) \rho_{AB}\right) = \theta_j. \tag{19}$$

where Θ_j is the tomographic operator of system A.

In this study, we compare our method to the refined-GLLP approach presented in [45], where the final key rate is

$$R = p_Z^2 p_1 Y_1 \left[1 - h_2\left(e_X'\right)\right] - p_Z^2 Q_\mu f h_2\left(E_\mu\right) . \tag{20}$$

Here, Q_μ is the gain of the signal states, E_μ is the quantum bit error rate of the signal states, p_1 is the probability of sending a single photon, Y_1 and e_X' are the yield and error rate of a single photon under THA, estimated following the decoy-state analysis. Moreover, f is the error correction efficiency. Finally, based on the analysis in [45], e_X' is given by the following equation:

$$e_X' = e_X + 4\Delta'\left(1 - \Delta'\right)\left(1 - 2e_X\right)$$
$$+ 4\left(1 - 2\Delta'\right)\sqrt{\Delta'\left(1 - \Delta'\right) e_X\left(1 - e_X\right)},$$
$$\Delta' = \frac{\Delta}{Y}, \tag{21}$$
$$\Delta = \frac{1}{2}\left[1 - \exp\left(-\mu_{\text{out}}\right)\cos\left(\mu_{\text{out}}\right)\right],$$

where e_X is the quantum bit error rate in the X basis, and Y is defined as $Y := \min\left[Y_Z^1, Y_X^1\right]$ with Y_Z^1 (Y_X^1) as the single-photon yields on the Z (X) basis.

B. Decoy-state MDI QKD

In the phase-encoding MDI protocol, Alice and Bob both prepare four BB84 states using similar setups of the BB84 QKD system; an example is shown in [64]. Therefore, the output states sent from Alice and Bob have the same form as in Eq. (16).

Similarly, using the source-replacement scheme, Alice prepares the entangled states as follows:

$$
\begin{aligned}
|\Phi\rangle_{AA'E_A} = &\sqrt{p_{z+}}|0\rangle_A |\psi_{z+}\rangle_{A'E_A} + \sqrt{p_{z-}}|1\rangle_A |\psi_{z-}\rangle_{A'E_A} + \\
&\sqrt{p_{x+}}|2\rangle_A |\psi_{x+}\rangle_{A'E_A} + \sqrt{p_{x-}}|3\rangle_A |\psi_{x-}\rangle_{A'E_A} .
\end{aligned}
\tag{22}
$$

Moreover, Bob prepares the entangled states as follows:

$$
\begin{aligned}
|\Phi\rangle_{BB'E_B} = &\sqrt{p_{z+}}|0\rangle_A |\psi_{z+}\rangle_{A'E_B} + \sqrt{p_{z-}}|1\rangle_A |\psi_{z-}\rangle_{A'E_B} + \\
&\sqrt{p_{x+}}|2\rangle_A |\psi_{x+}\rangle_{A'E_B} + \sqrt{p_{x-}}|3\rangle_A |\psi_{x-}\rangle_{A'E_B} .
\end{aligned}
\tag{23}
$$

Here, $E_A(E_B)$ denotes the system obtained by Eve in the channel between Alice (Bob) and Charlie. At the communication stage, Alice and Bob first send part of the state $|\Phi\rangle_{AA'}$ and $|\Phi\rangle_{BB'}$ to Charlie (i.e., states in system A' and system B') through the quantum channel ξ to obtain the final joint state

$$
\begin{aligned}
\rho_{ABC} = &(\mathbb{I}_A \otimes \xi) \operatorname{Tr}_{E_A} (|\Phi\rangle_{AA'E_A}\langle\Phi|) \otimes \\
&(\mathbb{I}_B \otimes \xi) \operatorname{Tr}_{E_B} (|\Phi\rangle_{BB'E_B}\langle\Phi|) .
\end{aligned}
\tag{24}
$$

The measurement considered the following constraints (See Appendix A for detailed description of measurement operators):

$$
\operatorname{tr} \left(\left(\mathrm{P}_j^A \otimes \mathrm{P}_i^B \otimes \mathrm{P}_k^C \right) \rho_{ABC} \right) = \mathrm{p}_{jik} ,
\tag{25}
$$

In this scenario, because system A and B has well characterized source, we have the following expression:

$$
\begin{aligned}
\rho_{AB} = \operatorname{Tr}_C (\rho_{ABC}) = &\operatorname{Tr}_{A'E_A} (|\Phi\rangle_{AA'E_A}\langle\Phi|) \otimes \\
&\operatorname{Tr}_{B'E_B} (|\Phi\rangle_{BB'E_B}\langle\Phi|) .
\end{aligned}
\tag{26}
$$

Therefore, the following constraints must be added:

$$
\operatorname{Tr} \left(\left(\Theta_j^A \otimes \Theta_i^B \otimes \mathbb{I}_C \right) \rho_{ABC} \right) = \theta_{ji},
\tag{27}
$$

12

where Θ_j^A and Θ_K^B are the tomographic operators in space A and space B, respectively.

Similarly, we compared the proposed approach with the refined GLLP for MDI-QKD presented in [42]. The key rate is as follows:

$$R = p_Z^2 p_{11} Y_{11}^Z \left[1 - h_2 \left(e_{11}^{X'} \right) \right] - p_Z^2 Q_{\mu\mu}^Z f h_2 \left(E_{\mu\mu}^Z \right), \tag{28}$$

where $Q_{\mu\mu}^Z$ is the signal state gain, $E_{\mu\mu}^Z$ is the signal state quantum bit error rate, p_{11} is the probability that Alice and Bob simultaneously send a single photon, f is the error correction efficiency, and Y_{11}^Z is the single-photon yield in the Z basis, directly estimated by the decoy-state analysis). Moreover, e_{11}^X is the single-photon error rate in the X basis and satisfies the following equation:

$$\begin{aligned} e_{11}^{X'} =& e_{11,\text{bit}}^X + 4\Delta' \left(1 - \Delta' \right) \left(1 - 2e_{11}^{X,\text{bit}} \right) \\ & + 4 \left(1 - 2\Delta' \right) \sqrt{\Delta' \left(1 - \Delta' \right) e_{11,\text{bit}}^X \left(1 - e_{11,\text{bit}}^X \right)}, \end{aligned} \tag{29}$$

where $e_{11,\text{bit}}^X$ is the single-photon error rate estimated using the decoy-state analysis. Moreover, e_{11}^X is the quantum bit error rate when THA does not exist, and Δ' satisfies

$$\Delta' = \frac{\Delta}{Y_{11}^Z}, \tag{30}$$

where

$$\Delta = \frac{1}{2} \left[1 - \exp \left[-(\mu_{out}^{Alice} + \mu_{out}^{Bob}) \right] \cos \left[\frac{1}{2} (\mu_{out}^{Alice} + \mu_{out}^{Bob}) \right]^2 \right], \tag{31}$$

where μ_{out}^{Alice} and μ_{out}^{Bob} represent the intensities reflected from Alice and Bob, respectively.

IV. SIMULATION

In this section, we first present a simulation performed to compare the proposed method with the refined GLLP approach in [45]. The parameters used in our simulation were extracted from previous related work. The parameters are summarized in Tab. I. The specific channel models for simulating the raw statistics obtained from WCP sources for BB84 and MDI-QKD are shown in Appendix B.

In Fig. 2, we plot the key rate of the decoy-state BB84 protocol using our method and compare it with the result obtained using the GLLP approach for different reflected Trojan-horse intensity μ_{out} values. The parameters used were the same as those used in a previous study analyzing decoy-state BB84 using a refined GLLP approach. The specific values are

TABLE I. Parameters for the experiments and numerical simulations. η_d is the detection efficiency, e_d denotes the optical misalignment, Y_0 is the dark count rate, and f is the error correction efficiency.

Parameter	Reference	Protocol	e_d	Y_0	η_d	f
Case 1	Ref. [45]	BB84	0.01	1×10^{-5}	0.125	1.2
Case 2	Ref. [42]	MDI	0.02	8×10^{-8}	0.495	1.16

listed for Case 1 in Tab. I. As shown in Fig. 2, the proposed numerical method provides a higher key rate and longer transmission distance than the refined GLLP approach. In particular, the advantage of our method is evident at a large value of $\mu_{\text{out}} = 10^{-3}$. At this large value, the refined GLLP approach can only reach a secure distance of 55 km, which is only 78.6% of that obtained using the proposed numerical approach.

In Fig. 3, we depict the key rate for MDI-QKD using the proposed method. The parameters used were extracted from Refs. [42] and are listed as Case 2 in Tab. I. Fig. 3 shows a behavior similar to that of decoy-state BB84. In other words, our numerical method outperforms the refined GLLP approach, providing a higher key rate and allowing a longer secure distance. In particular, when $\mu_{\text{out}} = 10^{-3}$, the proposed numerical method can provide a communication distance of 40 km. In contrast, the transmitted distance is 28 km using the refined GLLP approach. It should be noted that when $\mu_{\text{out}} = 0$, long distance, the existence of constraint noise makes the optimization very difficult and leads to incomplete optimization, so the key rate is lower than that of GLLP approach. However, this is not caused by numerical method, but only due to technical problems.

V. CONCLUSION

In summary, we developed a numerical method for calculating the security bounds for decoy-state QKD protocols under THAs. Benefitting from the tight security bound provided by the numerical framework, the proposed method improved the achieved secure key rate and prolonged the maximum communication distance for the decoy-state BB84 QKD and MDI-QKD protocols under THAs. In future research, the numerical method could be extended to more general Trojan-horse attacks, as described in [46], or jointly incorporating more imperfections into the numerical framework, as in the GLLP-based analysis in [65].

FIG. 2. Simulation results for decoy-state BB84 under THA. μ_{out} is the average number of photons reflected by THA. The black, blue, and red solid (dotted) lines are the key rate of using (our numerical method) the refined GLLP approach for various values of the parameters μ_{out}. For each point, we optimized the intensity of signal states and set the intensity of decoy state $\nu_1 = 0.02$ and the intensity of vacuum state $\nu_2 = 0.001$.

.

Furthermore, this study only considered the asymptotic case. Thus, its combination with a finite-key analysis [59, 60] could be the subject of future work.

FIG. 3. Simulation results for decoy-state MDI under THA. μ_{out} is the average number of photons reflected by THA. The black, blue, and red solid (dotted) lines are the key rate of using (our numerical method) the refined GLLP approach for various values of the parameters μ_{out}. For each point, we optimized the intensity of signal states and set the intensity of decoy state $\nu_1 = 0.02$ and the intensity of vacuum state $\nu_2 = 0.001$.

VI.   ACKNOWLEDGMENTS

VII.   DATA AVAILABILITY

Data will be made available on reasonable request

---

[1] C. H. Bennett, G. Brassard, *et al.*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (New York, 1984).

[2] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).

[3] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, Phys. Rev. A **96**, 022317 (2017).

[4] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).

[5] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, J. Lightwave. Technol. **36**, 3427 (2018).

[6] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Phys. Rev. Lett. **121**, 190502 (2018).

[7] D. Ma, X. Liu, C. Huang, H. Chen, H. Lin, and K. Wei, Opt. Lett. **46**, 2152 (2021).

[8] C. Huang, Y. Chen, L. Jin, M. Geng, J. Wang, Z. Zhang, and K. Wei, Phys. Rev. A **105**, 012421 (2022).

[9] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, Nat. Photon. **17**, 1 (2023).

[10] F. Grunenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hanggi, N. Bosshard, F. Bussieres, and H. Zbinden, Nat.

Photon. **17**, 422 (2023).

[11] Y. Du, X. Zhu, X. Hua, Z. Zhao, X. Hu, Y. Qian, X. Xiao, and K. Wei, Chip **2**, 100039 (2023).

[12] K. Wei, X. Hu, Y. Du, X. Hua, Z. Zhao, Y. Chen, C. Huang, and X. Xiao, Photon. Res. **11**, 1364 (2023).

[13] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, Nature **549**, 43 (2017).

[14] H. Chen, J. Wang, B. Tang, Z. Li, B. Liu, and S. Sun, Opt. Lett. **45**, 3022 (2020).

[15] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, Npj Quantum Inf. **7**, 93 (2021).

[16] A. Al-Juboori, H. Z. J. Zeng, M. A. P. Nguyen, X. Ai, A. Laucht, A. Solntsev, M. Toth, R. Malaney, and I. Aharonovich, Adv. Quantum Technol. **6**, 2300038 (2023).

[17] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, and A. Tanaka, Opt. Express **19**, 10387 (2011).

[18] J. F. Dynes, A. Wonfor, W. W. S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J. P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, Npj Quantum Inf. **5**, 101 (2019).

[19] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, Opt. Express **22**, 21739 (2014).

[20] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, Nature **589**, 214 (2021).

[21] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nature Photon. (2022), 10.1038/s41566-021-00928-2.

[22] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Npj Quantum Inf. **2**, 16025 (2016).

[23] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).

[24] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photon. **8**, 595 (2014).

[25] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, Phys. Rev. A **92**, 032305 (2015).

[26] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Sci. Adv. **6**, eaaz4487 (2020).

[27] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74** (2006), 10.1103/PhysRevA.74.022313.

[28] B. Qi, F. C.-h. Fred, H.-K. Lo, and X. Ma, Quant. Inf. Comput. **7**, 73 (2007).

[29] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. L Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).

[30] K. Wei, W. Zhang, Y.-L. Tang, L. You, and F. Xu, Phys. Rev. A **100**, 022325 (2019).

[31] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photon. **4**, 686 (2010).

[32] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[33] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Optic. **48**, 2023 (2001).

[34] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73** (2006), 10.1103/PhysRevA.73.022320.

[35] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[36] D. Gottesman, H.-K. Lo, N. L Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004).

[37] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98** (2007), 10.1103/PhysRevLett.98.230501.

[38] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y. Z. Tan, R. Wolf, V. Scarani, and C. C. W. Lim, Nat. Commum. **12**, 2880 (2021).

[39] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **128**, 110506 (2022).

[40] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, IEEE. J. Sel. Top. Quant **21**, 168 (2015).

[41] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Sci. Rep. **7**, 8403 (2017).

[42] H. Tan, W. Li, L. Zhang, K. Wei, and F. Xu, Phys. Rev. Appl. **15**, 064038 (2021).

[43] J. Nitin, A. Elena, K. Imran, M. Vadim, M. Christoph, and L. Gerd, New J. Phys. **16**, 123030 (2014).

[44] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, arXiv preprint arXiv:2201.06114 (2022).

[45] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015).

[46] K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).

[47] W. Wang, K. Tamaki, and M. Curty, New J. Phys. **20**, 083027 (2018).

[48] A. Navarrete and M. Curty, arXiv preprint arXiv:2202.06630 (2022).

[49] W. Wang, K. Tamaki, and M. Curty, Sci. Rep. **11**, 1678 (2021).

[50] Y.-F. Lu, Y. Wang, M.-S. Jiang, X.-X. Zhang, F. Liu, H.-W. Li, C. Zhou, S.-B. Tang, J.-Y. Wang, and W.-S. Bao, Entropy **23**, 1103 (2021).

[51] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94** (2005), 10.1103/PhysRevLett.94.230504.

[52] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[53] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[54] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[55] W. Wang and N. Lütkenhaus, Phys. Rev. Research **4**, 043097 (2022).

[56] A. Ferenczi and N. Lütkenhaus, Phys. Rev. A **85**, 052310 (2012).

[57] P. J. Coles, E. M. Metodiev, and N. L Lütkenhaus, Nat. Commun. **7**, 11712 (2016).

[58] A. Winick, N. L Lütkenhaus, and P. J. Coles, Quantum **2**, 77 (2018).

[59] I. George, J. Lin, and N. L Lütkenhaus, Physical Review Research **3**, 013274 (2021).

[60] D. Bunandar, L. C. G. Govia, H. Krovi, and D. Englund, Npj Quantum Inf. **6**, 104 (2020).

[61] N. K. H. Li and N. Lütkenhaus, Phys. Rev. Research **2**, 043172 (2020).

[62] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[63] H.-K. Lo and J. Preskill, Quant. Info. Comp. **7**, 431 (2006).

[64] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, T.-Y. Chen, F. Xu, and J.-W. Pan, Phys. Rev. Lett. **122**, 160501 (2019).

[65] S. Sun and F. Xu, New J. Phys. **23**, 023011 (2021).

Appendix A: measurement operator, Kraus operator, key mapping

In this section, we will describe the specific forms of operators required in BB84 and MDI protocols. Our protocol description model is similar to Ref. [55].

1. BB84

The measurement operator is:

P_i^A	$|0\rangle\langle0|$	$|1\rangle\langle1|$	$|2\rangle\langle2|$	$|3\rangle\langle3|$
P_i^B	$|Z_+\rangle\langle Z_+|\oplus 0$	$|Z_-\rangle\langle Z_-|\oplus 0$	$|X_+\rangle\langle X_+|\oplus 0$	$|X_-\rangle\langle X_-|\oplus 0$ $1-\sum_{i=1}^{4}P_i^B$

The tomographic scanning operator is:

$$|i\rangle\langle j|_A \otimes \mathbb{I}_{\dim\,B}. \tag{A1}$$

The Kraus operator is:

$$
K_Z = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & & \\ & 0 & \\ & & 0 \\ & & & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & & \\ & 1 & \\ & & 0 \\ & & & 0 \end{pmatrix} \right]
$$

$$
\sqrt{p_Z} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix},
$$

$$
K_X = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & & \\ & 0 & \\ & & 1 \\ & & & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & & \\ & 0 & \\ & & 0 \\ & & & 1 \end{pmatrix} \right]
$$

$$
\sqrt{p_X} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{A2}
$$

While the key maps are:

$$
Z_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{I}_{\dim_A \times \dim_B \times 2},
$$

$$
Z_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \mathbb{I}_{\dim_A \times \dim_B \times 2}. \tag{A3}
$$

2. MDI

The measurement operator is

P_i^A	$|0\rangle\langle 0|$	$|1\rangle\langle 1|$	$|2\rangle\langle 2|$	$|3\rangle\langle 3|$
P_i^B	$|0\rangle\langle 0|$	$|1\rangle\langle 1|$	$|2\rangle\langle 2|$	$|3\rangle\langle 3|$
P_i^C	$|\Phi^+\rangle_{ab}\langle\Phi^+|_{ab}$	$|\Phi^+\rangle_{ab}\langle\Phi^+|_{ab}$	$1-\sum_{i=1}^{2}P_i^C$	

The tomographic scanning operator is

$$|i\rangle\langle j|_A \otimes |k\rangle\langle l|_B \otimes \mathbb{I}_{\dim\,C}. \tag{A4}$$

The Kraus operator is

$$
K_Z = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \right]
$$

$$
\otimes \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix},
$$

$$
K_X = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 0 & \\ & & & 1 \end{pmatrix} \right]
$$

$$
\otimes \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}.
\tag{A5}
$$

while the key maps are

$$
Z_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{I}_{\dim_A \times \dim_B \times \dim_C \times 2},
$$

$$
Z_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \mathbb{I}_{\dim_A \times \dim_B \times \dim_C \times 2}.
\tag{A6}
$$

Appendix B: Channel model

In this section, we will provide a description of the channel model used in our simulation. The channels utilized in our simulation include loss, misalignment, and dark count rate channels, which are similar to [55].

1. BB84

In the WCP source, the output is a coherent state with amplitude of μ. After passing through the misaligned channel, the amplitude reaching each detector can be summarized as

		Bob's detectors (passive detection)			
		Z_+	Z_-	X_+	X_-
	Z_+	$\sqrt{p_Z}\cos\theta$	$\sqrt{p_Z}\sin\theta$	$\sqrt{p_X}\cos\alpha$	$\sqrt{p_X}\sin\alpha$
Alice	Z_-	$-\sqrt{p_Z}\sin\theta$	$\sqrt{p_Z}\cos\theta$	$\sqrt{p_X}\sin\alpha$	$-\sqrt{p_X}\cos\alpha$
sends	X_+	$\sqrt{p_Z}\sin\alpha$	$\sqrt{p_Z}\cos\alpha$	$\sqrt{p_X}\cos\theta$	$-\sqrt{p_X}\sin\theta$
	X_-	$\sqrt{p_Z}\cos\alpha$	$-\sqrt{p_Z}\sin\alpha$	$\sqrt{p_X}\sin\theta$	$\sqrt{p_X}\cos\theta$

$$(\text{B1})$$

Here, $\alpha = \frac{\pi}{4} - \theta$, θ is the misalignment. Considering the channel loss, the loss factor $\sqrt{\mu\eta}$ should be multiplied before the above amplitudes. By considering the dark count, we can get the click probability of each detector:

$$p_{j|i}^{\text{click}} = 1 - (1 - p_d) \times e^{-\left|\alpha_{j|i}\right|^2}, \tag{B2}$$

where $\alpha_{j|i}$ is the amplitude reaching the detector, p_d is the detector dark count rate $i,j \in \{H, V, +, -\}$. The probabilities of individual detector clicks are known, for a given i, there could be a total of 4 detectors that will register a click, leading to 16 possible detection patterns. The probability of each detection pattern $b_1b_2b_3b_4$ is represented by

$$p_{b_1b_2b_3b_4|i} = \Pi_{j=1,2,3,4}\left\{ \overline{b_j} + p_{j|i}^{\text{click}} (-1)^{\overline{b_j}} \right\}, \tag{B3}$$

where b_k represents the response of the k detectors, $b_k = 0, 1$. $\overline{b_k}$ is the bit flip of $\overline{b_k}$.

For a given signal intensities μ ($\mu \in \{u, v, w\}$), iterate through all the i and all of the detection mode to obtain 4×16 data, and then write it into a matrix $P_{raw,\mu}$ with 4×16 data.

Suppose that double click events on the same basis are randomly assigned to a measurement value, while double click events on different basis are discarded. The following deletion model is defined:

$$M_H = [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0.5, 0, 0, 0]$$

$$M_V = [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0.5, 0, 0, 0]$$

$$M_+ = [0, 0, 1, 0.5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$ (B4)

$$M_- = [0, 1, 0, 0.5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$

$$M_\varnothing = [1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1]$$

$$M = \left[M_H^T, M_V^T, M_+^T, M_-^T, M_\varnothing^T \right].$$

Then the simulated statistical data can be given by

$$P_\mu = P_{\text{raw},\mu} \times M. \tag{B5}$$

2. MDI

In the case of MDI, the WCP source of Alice and Bob transmits a weak coherent state with amplitude of μ. After passing through the misaligned channel, the signals of Alice and Bob are mismatched θ_A, θ_B. Because H and V are different modes, we can simply think of $\sqrt{\mu_A} \cos \theta_A$ in H mode (similar to Alice and Bob), $\sqrt{\mu_A} \sin \theta_A$ in mode V(Alice and Bob are similar), then the amplitude reaching each detector is expressed as follows:

$$\alpha_{3H}^\phi = \sqrt{\mu_A \eta_A} \cos \theta_A / 2 + i \sqrt{\mu_B \eta_B} \cos \theta_B / 2 e^{i\phi}$$

$$\alpha_{4H}^\phi = i \sqrt{\mu_A \eta_A} \cos \theta_A / 2 + \sqrt{\mu_B \eta_B} \cos \theta_B / 2 e^{i\phi}$$ (B6)

$$\alpha_{3V}^\phi = \sqrt{\mu_A \eta_A} \sin \theta_A / 2 + i \sqrt{\mu_B \eta_B} \sin \theta_B / 2 e^{i\phi}$$

$$\alpha_{4V}^\phi = i \sqrt{\mu_A \eta_A} \sin \theta_A / 2 + \sqrt{\mu_B \eta_B} \sin \theta_B / 2 e^{i\phi}.$$

Then the click probability of each detector can be given by

$$p_{k|ij}^{\text{click},\phi} = 1 - (1 - p_d) \times e^{-\left|\alpha_{k|ij}^\phi\right|^2}, \tag{B7}$$

where $\alpha_{k|ij}^\phi$ is the amplitude reaching the detector, $i, j \in \{H, V, +, -\}$, $k \in \{3H, 3V, 4H, 4V\}$.

For fixed i, j, a total of 4 detectors may respond, which results in a total of 16 possible detection modes. The response probability of each detection mode $b_1 b_2 b_3 b_4$ is given by

$$p_{b_1 b_2 b_3 b_4 | ij} = \prod_{k=1,2,3,4} \left\{ \overline{b_k} + p_{k|ij}^{\text{click}} (-1)^{\overline{b_k}} \right\}, \tag{B8}$$

where b_k represents the response of the k detectors, $b_k = 0, 1$. $\overline{b_k}$ is the bit flip of $\overline{b_k}$.

For a given signal intensities $\mu_A \mu_B$ ($\mu_A, \mu_B \in \{u, v, w\}$), Traverse all i, j and detection modes, there are $4 \times 4 \times 16$ data in total. Write the data as $P_{raw, \mu_A \mu_B}$ and define the following deletion model

$$M_{\Psi^-} = [0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0]$$

$$M_{\Psi^+} = [0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0]$$

$$M_\varnothing = 1_{1 \times 16} - M_{\Psi^+} - M_{\Psi^-} \tag{B9}$$

$$M = \left[M_{\Psi^-}^T, M_{\Psi^+}^T, M_\varnothing^T \right].$$

Then the simulated statistical data can be given by

$$P_{\mu_A \mu_B} = P_{\text{raw}, \, \mu_A \mu_B} \times M. \tag{B10}$$