Journal of Physics Communications

PAPER

Reference frame independent twin field quantum key distribution with source flaws

Comfort Sekga and Mhlambululi Mafu

Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16 Palapye, Botswana

E-mail: duxeesekga@gmail.com

Keywords: Twin field quantum key distribution, Loss tolerant quantum key distribution, Reference frame independent quantum key distribution

OPEN ACCESS

RECEIVED
24 December 2020

REVISED
29 March 2021

ACCEPTED FOR PUBLICATION
1 April 2021

PUBLISHED
14 April 2021

Abstract

The trade-off between distance and secret key generation rate remains one of the major challenges in the practical implementation of quantum key distribution (QKD). As a solution, a twin field QKD protocol was proposed by Lucamarini *et al* (2018) to address this challenge. In this protocol, the achievable secret key rate scales with the square root of channel transmittance and can surpass the secret key capacity for repeaterless QKD. However, the protocol exploits phase to encode information which presents the problem of active stabilization of interferometers. We propose a reference frame independent twin field quantum key distribution (RFITF QKD), which does not require the reference frames' alignment. Thus, this reduces the complexity of practical QKD systems in achieving active stabilization of phase. Moreover, we employ the loss-tolerant method proposed by Tamaki *et al* (2014) which allows us to prove the security of the protocol by considering imperfections in the state preparation. Our simulation results show that our proposed protocol can extract a secure key over a transmission distance of $l = 505$ km, $l = 516$ km and $l = 530$ km for deviation of 8.42°, 7.28° and 5.15°, respectively from the desired phase encoding angle. These results demonstrate that despite the state preparation flaws, the key rates achieved are still comparable to the perfect encoding scenario. When our proposed protocol is implemented with an imperfect source, it achieves a transmission distance beyond the secret key capacity bound for repeaterless QKD.

1. Introduction

Quantum key distribution (QKD) allows two trusted parties, Alice and Bob, to securely share an information-theoretic secure key guaranteed by quantum physics laws in the presence of an adversary [1]. Since the primitive BB84 QKD protocol [2] great strides have been made both in theory [3–10] and experiments [11–15] to develop quantum technologies for real-life applications. Moreover, some countries have ventured into widening the reach of QKD by developing global quantum networks [16, 17]. Despite these advances, several theoretical and experimental challenges remain unresolved [18]. For instance, in practice, QKD protocols rely on trusted devices scenario, an assumption that enables them to attain effective rates, but this also opens the possibility of dangerous side-channel attacks [19]. Other challenges include obtaining reasonable key rates over large distances, high costs associated with deploying QKD technologies, and combining QKD with information-theoretic cryptographic protocols or algorithms, for instance, AES encryption [18, 20, 21]. Thus, these challenges make QKD technologies not a viable immediate alternative to conventional cryptography.

To address the problem of detector side-channel attacks, device-independent (DI) QKD protocol was proposed, and its security is based on the violation of Bell inequalities [22]. Unfortunately, the DI-QKD requires loophole-free Bell experiments, which makes it not feasible with current technology. A more practical solution is measurement device-independent (MDI) QKD, which is inherently immune to all side-channel attacks targeting the measurement device and removes all detection-related security loopholes [23]. In the MDI-QKD, two parties Alice and Bob, are linked by an untrusted relay, resulting in a significant increase in the transmission

distance compared with the conventional QKD schemes. Despite MDI-QKD overcoming the distance limit and device imperfections, the secret key rates achieved with the protocol are relatively low. Precisely, most QKD schemes produce secret key rates which scale linearly with channel transmittance and are unable to surpass the secret-key capacity (SKC) bound of an optical quantum channel with losses [24]. Recently, a novel QKD that relies on phase randomized twin fields of optical pulses to encode information was developed and can surpass the secret key capacity bound for repeaterless QKD schemes [25]. Similar to MDI-QKD, the possibility of side-channel attacks are removed in this protocol as an untrusted relay connects the communicating parties. The protocol is based on the single-photon interference of optical fields generated with almost identical electromagnetic phases. This single-photon interference at the untrusted relay leads to an improved secret key rate which scales with the square root of channel transmittance. Since the original TF-QKD scheme lacked rigorous security proof, variant TF protocols aimed at proving TF-QKD security have been proposed [26–28]. Moreover, the experimental demonstrations of TF-QKD have already been successfully implemented [29–31].

In most QKD systems mentioned above, a shared reference frame is required between Alice and Bob. For instance, there is a need to align polarization states in polarization encoding or active stabilization of interferometers in phase encoding protocols. Although it is feasible to share a reference frame between Alice and Bob, it comes at a cost as additional systems required for phase calibration may lead to more information leakage and thus reduce practical systems' performance [32, 33]. Fortunately, a reference-frame-independent (RFI) QKD protocol was proposed to address these challenges [34]. Since its inception, outstanding results have been achieved theoretically [35–40] and experimentally [41–43], thus demonstrating its capability to achieve a higher secure key rate under a varying reference frame.

Ideally, the encoding of light pulses is carried out perfectly without any state preparation flaw (SPF). However, this assumption falls short experimentally due to inherent deficiencies of phase modulators. The problem with SPFs can be addressed by using the Gottesman-Lo-Lutkenhaus-Preskill (GLLP) security analysis [44], but the main drawback is that the approach leads to a low achievable secret key rate and is not robust against channel loss. Tamaki *et al* (2014) recently proposed a loss-tolerant protocol which is robust against channel losses due to SPFs and capable of attaining key rates comparable to a protocol that assumes perfect encoding [45]. The protocol is resource-efficient as it employs only three states out of the possible four states for BB84 protocol and considers modulation errors due to an imperfect phase modulator. It is conjectured that the protocol can be generalized to the six-state protocol where only four states are required instead of the usual six states.

Therefore, in this work, we investigate the practicality of TF-QKD by employing the loss tolerant protocol to derive the security bounds under the imperfect state preparation. We also study the protocol under reference frame independence condition, eliminating the need for active stabilization of phase. The protocol is implemented with three mutually unbiased bases (X; Y; Z) which are used to encode information. The X and Y bases are used to monitor the eavesdropper's (Eve) knowledge on the key and are allowed to vary slowly in the quantum channel. The Z basis states are naturally well-aligned, and this basis is generally used to generate the final key. Furthermore, we demonstrate that the TF-QKD can be implemented without the alignment of a reference frame and imperfect state preparation but still achieve secret key rates and transmission distances comparable to the original TF-QKD. This paper is arranged according to the following. In section 1, we provide an introduction where we make a brief review of QKD security developments and the motivation of our work. In section 2, we describe the operation of the proposed RFI-TF QKD protocol. This is followed by section 3, where we show details of the security proof for the loss tolerant RFI-TF QKD protocol. In section 4, we discuss our simulation results, and finally, in section 5 we provide concluding remarks about our work. We provide the security proof of our protocol in appendix C, and some technical details relevant to the key rate calculation are presented in the appendixes.

2. Operation of RFI-TF QKD protocol

We propose a loss tolerant based RFI-TF QKD protocol that uses four signal states from three mutually unbiased bases defined by the Pauli operators, X, Y and Z. This protocol is conjectured to achieve error rates that are similar to the QKD protocol that employs all six states from three bases $\{Z, X, Y\}$ [45]. The four states are denoted as $|\phi_{0Z}\rangle = |0_Z\rangle, |\phi_{1Z}\rangle = |1_Z\rangle, |\phi_{0X}\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle)$ and $|\phi_{0Y}\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + i|1_Z\rangle)$ where $|0\rangle, |1\rangle$ represent vacuum and one photon states, respectively. We begin by describing the protocol implemented with the idealized photon source and then discussing the practical protocol that employs the weak coherent laser source.

Protocol 1 The entanglement-based description of the protocol is as follows:

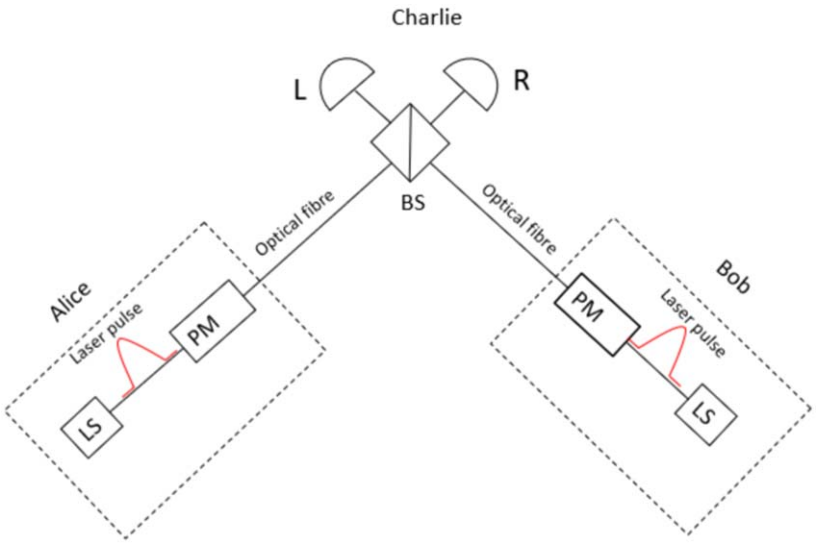

Figure 1. The setup of the proposed RFI TF-QKD. Alice and Bob use their laser sources (LS) to prepare coherent states $|\sqrt{\mu_{a(b)}}\,e^{i\chi}\rangle$ with random phase χ in the Z basis and states $|\sqrt{\mu_{a(b)}}\,e^{i(0+\chi)}\rangle$ and $|\sqrt{\mu_{a(b)}}\,e^{i(\frac{\pi}{2}+\chi)}\rangle$ for X and Y basis, respectively. The phase is encoded using phase modulators (PM). Alice and Bob send the prepared optical signals through an insecure channel to the untrusted Charlie, who is supposed to perform a single-photon interference in a symmetric beamsplitter (BS) followed by threshold detection in either L or R detector. In the X and Y bases, the random phase χ is selected from discrete M phase slices $\Delta_j = \left(\frac{2\pi j}{M}, \frac{2\pi(j+1)}{M}\right)$ over the semi-interval $[0, 2\pi)$ with $j = \{0,\ldots,M-1\}$. During classical post-processing, the random phases are announced, and states are postselected according to the satisfaction of condition; $|j_A - j_B| \bmod M = 0$ or $|j_A - j_B| \bmod M = \frac{M}{2}$ where $j_{A(B)} = \left(\frac{\Delta_j M}{2\pi}\right) \bmod M$.

1. Alice (Bob) starts by preparing the entangled state $|\Psi\rangle_{Aa(Bb)} = (\sqrt{1-\gamma}\;|0\rangle_{A(B)}|0\rangle_{a(b)} + \sqrt{\gamma}\;|1\rangle_{A(B)}|1\rangle_{a(b)})$ with $\gamma \in (0, 1)$. System $A(B)$ represents the qubits that remain in Alice and Bob's possession.
2. Alice (Bob) sends signal states a (b) through the insecure quantum channel to the untrusted third party, Charlie.
3. Upon receipt of the pulses, Charlie executes the single-photon Bell state measurement with a symmetric beamsplitter followed by threshold detection in two detectors.
4. Charlie announces the successful events of single-photon Bell state measurement. The two detectors labeled L and R in figure 1 are associated with destructive and constructive interference, respectively. A coincidence detection with a click in L *and* no click in R indicates a projection into Bell state $|\Phi^+\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + |1\rangle_a|0\rangle_b)$ while a click in R and no click in L corresponds to projection onto Bell state $|\Phi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$.
5. Following the results' announcement, Alice and Bob measure their qubits in the Z basis with probability p_z and choose the complementary bases with probability $1 - p_z$. Moreover, they post select on the events of the compatible basis to obtain a raw key.
6. Lastly, to ensure that their bit strings match, Bob always flip his qubit for all successful Bell state measurement results in the Z basis and only flip his bit for Bell state measurement result $|\Phi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$ in the complementary bases. In the RFI protocol, the key is obtained from the Z basis where the reference frames linking Alice (Bob) and Charlie are assumed to be well aligned, while in the other measurement bases (X, Y) the frames are allowed to slowly vary by an arbitrary angle β. The allowed deviations in the bases are given by $X_B = \cos\beta X_A + \sin\beta Y_A$ and $Y_B = \cos\beta Y_A - \sin\beta X_A$.

The above protocol can be converted to an equivalent prepare and measure protocol where Alice and Bob measure their qubits $A(B)$ before sending the signal states $a(b)$ to Charlie. In principle, this implies that Alice and Bob directly prepare the signal states $a(b)$, i.e., their qubits measurements herald the formation of signal states. This measurement operation does not change operations results in other steps; thus, the protocol can be alternatively described as follows.

1. Alice (Bob) prepares the signal states $a(b)$ in the state $|\phi_{0Z}\rangle = |0_Z\rangle, |\phi_{1Z}\rangle = |1_Z\rangle$ with probabilities $1-\gamma$ and γ in the Z basis for logic bits 0 and 1, respectively. The states in complementary bases

$|\phi_{0X}\rangle = \sqrt{1-\gamma}|0_Z\rangle + \sqrt{\gamma}|1_Z\rangle$ and $|\phi_{0Y}\rangle = \sqrt{1-\gamma}|0_Z\rangle + i\sqrt{\gamma}|1_Z\rangle$ are prepared with equal probabilities and encoded as logic bit 0.

2. They send the signal states a (b) through the quantum channel to untrusted Charlie, who executes the single-photon Bell state measurement with a symmetric beam splitter followed by two threshold detection.
3. Charlie announces the successful events of single-photon Bell state measurement to Alice and Bob, who then post select on the events they prepared their states on the Z basis to obtain a raw key.
4. Lastly, to ensure that their bit strings match, Bob always flip his qubit for all successful Bell state measurement results in the Z basis and only flip his bit for Bell state measurement result $|\Phi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$ in the complementary bases. The measurement results in the complementary bases are used to estimate the adversary's knowledge about the key.

Protocol 2 Since realizing a superposition between a vacuum and a single photon is challenging (for the realization of states in complementary bases in protocol 1), we now describe the practical protocol implemented with weak coherent sources (see figure 1). It exploits interference of a vacuum state and a coherent state in a symmetric beam splitter to generate a secret key. Also, twin optical fields with identical random phases are used in the complementary bases to estimate Eve's information. The protocol runs as follows:

1. In the Z basis, Alice (Bob) randomly prepares weak coherent states $|\sqrt{\mu_{a(b)}}e^{i\chi}\rangle$ with intensities 0 (vacuum) and μ with probabilities $1-\gamma$ and γ, respectively. The bit values 0 and 1 encodes for intensity 0 and μ, respectively. If the parties (Alice and Bob) choose complementary bases, they prepare the states $|\sqrt{\mu_{a(b)}}e^{i(\theta_{A(B)}+\chi)}\rangle$ with phase values $\theta_{A(B)} = 0$ and $\theta_{A(B)} = \pi/2$ for X and Y basis, respectively with both states coding for bit value 0. In these two bases, the optical pulses are prepared with intensity $\mu_{a(b)} \in \{u/2, v/2, 0\}$ (where u, v and 0 represent signal, decoy and vacuum pulses). Furthermore, in this protocol the random phase χ is picked from discrete M phase slices $\Delta_j = \left(\frac{2\pi j}{M}, \frac{2\pi(j+1)}{M}\right)$ over the semi-interval $[0, 2\pi)$ with $j = \{0, \ldots, M-1\}$.
2. The optical pulses are sent through an insecure channel to Charlie, who allows them to interfere in the symmetric beam splitter. This is followed by threshold detection, and after that, Charlie announces the successful detection events. The successful results correspond to a click in the L detector and no click in the R detector or vice versa.
3. Following announcement of results, Alice and Bob perform sifting by post selecting on the successfully detected states which were prepared using the same basis. Precisely, in the Z basis, these events correspond to cases where Alice chose intensity μ while Bob selected intensity 0 and vice versa. For complementary bases, they consider the states prepared with the same intensity and in which they picked the random phase slices according to the phase post-selection matching method, i.e., $|j_A - j_B| \bmod M = 0$ or $|j_A - j_B| \bmod M = \frac{M}{2}$ where $j_{A(B)} = \left(\frac{\Delta_j M}{2\pi}\right) \bmod M$. Note that during sifting, Alice and Bob only announce the random phase χ for the states prepared in the complementary bases, while random phases for Z basis states are not disclosed. The key is generated from measurements in the Z basis. The results in X and Y bases are used to monitor eavesdropping. It should be noted that these bases are allowed to vary by an arbitrary angle β. The allowed deviations in the bases are given by $X_B = \cos\beta X_A + \sin\beta Y_A$ and $Y_B = \cos\beta Y_A - \sin\beta X_A$.

3. Security analysis of the protocol

Following the sequential transmission and measurement of optical pulses, Alice and Bob are now in possession of partially correlated bit strings. They proceed with the parameter estimation step to deduce the bit error rate in the key basis. The quantum bit error rate is given by

$$E_{ZZ} = \frac{1 - \langle Z_A Z_B\rangle}{2} \tag{1}$$

where Z_A and Z_B represent that Alice and Bob send the two states prepared in the Z basis, respectively. To compute Eve's knowledge on the key, we consider a depolarising channel where $E_{ZZ} \leqslant 15.9\%$ [34]. The bound is given by

$$I_E = (1 - E_{ZZ})h\left(\frac{1 + u_{\max}}{2}\right) - E_{ZZ}h\left(\frac{1 + v(u_{\max})}{2}\right), \tag{2}$$

where

$$u_{\max} = \min\left[\frac{1}{1 - E_{ZZ}}\sqrt{C/2}, 1\right],$$
$$v(u_{\max}) = \sqrt{[C/2 - (1 - E_{ZZ})^2 u_{\max}^2]}\Big/E_{ZZ}. \tag{3}$$

The quantity C is obtained from the measurement results in the complementary bases and is given by

$$C = \langle X_A X_B\rangle^2 + \langle X_A Y_B\rangle^2 + \langle Y_A X_B\rangle^2 + \langle Y_A Y_B\rangle^2. \tag{4}$$

This expression can be rewritten in terms of the error rate as

$$C = (1 - 2E_{XX})^2 + (1 - 2E_{XY})^2 + (1 - 2E_{YX})^2 + (1 - 2E_{YY})^2. \tag{5}$$

To compute C, we employ a loss tolerant technique where Alice and Bob prepare their optical pulses using four states $|\phi_{0Z}\rangle, |\phi_{1Z}\rangle, |\phi_{0X}\rangle$ and $|\phi_{0Y}\rangle$. Due to imperfections in the phase modulation, the actual states that Alice (Bob) prepares can be described by

$$|\phi_{j\beta}\rangle_{A(B)} = |\sqrt{\mu}\, e^{i\chi}\rangle_r |\sqrt{\mu}\, e^{i(\chi + \theta_{A(B)} + \delta\theta_{A(B)}/\pi)}\rangle_s \tag{6}$$

where $r(s)$ denotes reference (signal) states, μ corresponds to the intensity of pulses and δ represents the deviation from desired encoding angle θ in the actual states. Here $\beta \in \{X, Y, Z\}$ and $j \in \{0, 1\}$. Note that a coherent state of intensity μ and global phase χ is a linear superposition of photon number states $\{|n\rangle\}$ of $|\sqrt{\mu}\, e^{i\chi}\rangle = \sum_{n=0}^{\infty} e^{-\mu/2}\frac{(\sqrt{\mu}\, e^{i\chi})^n}{\sqrt{n!}}|n\rangle$. Therefore, the single-photon part of the coherent states in equation (6) prepared by Alice and Bob can be expressed as

$$|\phi_{j\beta}\rangle_{A(B)} = \frac{1}{\sqrt{2}}(|1\rangle_r|0\rangle_s + e^{i(\theta_{A(B)} + \delta\theta_{A(B)}/\pi)}|0\rangle_r|1\rangle_s) \tag{7}$$

where 0 and 1 represent the photon number. From above representation we define $|1\rangle_r|0\rangle_s = |0_Z\rangle$, $|0\rangle_r|1\rangle_s = |1_Z\rangle, |0_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle), |1_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle - |1_Z\rangle), |0_Y\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + i|1_Z\rangle)$ and $|1_Y\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle - i|1_Z\rangle)$. Therefore, equation (7) can be equivalently rewritten as

$$e^{i\left(\frac{(\theta_{A(B)} + \delta\theta_{A(B)}/\pi)}{2}\right)}\left[\cos\left(\frac{\theta_{A(B)}}{2} + \frac{\delta}{2}\right)|0_X\rangle + i\sin\left(\frac{\theta_{A(B)}}{2} + \frac{\delta}{2}\right)|1_X\rangle\right]. \tag{8}$$

Similar expression as above can be obtained for the eigenstates $|0_Y\rangle, |1_Y\rangle$. If the overall phase factor in equation (8) is ignored, we obtain the following expressions for the four states

$$\begin{aligned}
|\phi_{0Z}\rangle &= |0_Z\rangle \\
|\phi_{1Z}\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle) \\
|\phi_{0X}\rangle &= \cos\left(\frac{0}{2} + \frac{\delta_1}{2}\right)|0_X\rangle + i\sin\left(\frac{0}{2} + \frac{\delta_1}{2}\right)|1_X\rangle \\
&= \cos\left(\frac{\delta_1}{2}\right)|0_X\rangle + i\sin\left(\frac{\delta_1}{2}\right)|1_X\rangle \\
|\phi_{0Y}\rangle &= \cos\left(\frac{\pi}{2} + \frac{\delta_2}{2}\right)|0_Y\rangle + i\sin\left(\frac{\pi}{2} + \frac{\delta_2}{2}\right)|1_Y\rangle,
\end{aligned}$$

where $\theta_{A(B)} = 0, \pi/2$ for X and Y, respectively. These signal states can be written in terms of an identity and Pauli matrices and their density matrices representation are

$$\rho_{0Z} = |\phi_{0Z}\rangle\langle\phi_{0Z}| = (\mathbb{1} + \sigma_z)/2, \tag{9}$$

$$\begin{aligned}
\rho_{1Z} &= |\phi_{1Z}\rangle\langle\phi_{1Z}| = \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} \\
&= \frac{1}{2}\mathbb{1} - \frac{1}{2}\sigma_x,
\end{aligned} \tag{10}$$

$$\rho_{0X} = |\phi_{0X}\rangle\langle\phi_{0X}| = \frac{1}{2}\begin{bmatrix} \cos^2\left(\frac{\delta_1}{2}\right) + \sin^2\left(\frac{\delta_1}{2}\right) & \cos^2\left(\frac{\delta_1}{2}\right) + i\sin(\delta_1) - \sin^2\left(\frac{\delta_1}{2}\right) \\ \cos^2\left(\frac{\delta_1}{2}\right) - i\sin(\delta_1) - \sin^2\left(\frac{\delta_1}{2}\right) & \cos^2\left(\frac{\delta_1}{2}\right) + \sin^2\left(\frac{\delta_1}{2}\right) \end{bmatrix}$$
$$= \frac{1}{2}\mathbb{1} + \frac{1}{2}\cos(\delta_1)\sigma_x, \tag{11}$$

$$\rho_{0Y} = |\phi_{0Y}\rangle\langle\phi_{0Y}| = \begin{bmatrix} \frac{1}{2}\cos^2\Theta + \frac{1}{2}\sin^2\Theta & -\frac{i}{2}\cos^2\Theta + \frac{i}{2}\sin^2\Theta \\ & +\sin\Theta\cos\Theta \\ \frac{i}{2}\cos^2\Theta - \frac{i}{2}\sin^2\Theta & \frac{1}{2}\cos^2\Theta + \frac{1}{2}\sin^2\Theta \\ +\sin\Theta\cos\Theta & \end{bmatrix}$$
$$= \frac{1}{2}\mathbb{1} + \frac{1}{2}\sin(2\Theta)\sigma_x, \tag{12}$$

where $\Theta = \frac{\pi}{2} + \frac{\delta_2}{2}$. From this representation of signal states, one can obtain the joint probability, $Y_{\Phi^\pm;j_\alpha k_\beta}$ that Alice (Bob) prepares any of the state $|\phi_{j\alpha}\rangle$ ($|\phi_{k\beta}\rangle$) and Charlie declares $|\Phi^\pm\rangle$ by exploiting transmission rate of the Pauli operators and subsequently estimate error rates E_{XX}, E_{XY}, E_{YX} and E_{YY} used for calculating C. Here, we show how to estimate the phase error rate E_{XX}; other parameters can be obtained similarly. The parameter E_{XX} is computed by considering a virtual protocol where Alice and Bob prepare entangled state $|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{A(B)}|\phi_{0Z}\rangle_C + |1\rangle_{A(B)}|\phi_{1Z}\rangle_C)$, (here C denotes the system sent to Charlie) and measure their subsystems in the X basis when Charlie announces the measurement result $|\Phi^+\rangle$. The error rate is expressed as

$$E_{XX} = \frac{Y^{Z,\mathrm{vir}}_{\Phi^+;0_X1_X} + Y^{Z,\mathrm{vir}}_{\Phi^+;1_X0_X}}{Y^{Z,\mathrm{vir}}_{\Phi^+;0_X1_X} + Y^{Z,\mathrm{vir}}_{\Phi^+;1_X0_X} + Y^{Z,\mathrm{vir}}_{\Phi^+;0_X0_X} + Y^{Z,\mathrm{vir}}_{\Phi^+;1_X1_X}} \tag{13}$$

where $Y^{Z,\mathrm{vir}}_{\Phi^+;j_Xk_X}$ denotes the joint probability that Alice and Bob measured $|j_X\rangle$ and $|k_X\rangle$, respectively and Charlie declares the result $|\Phi^+\rangle$. In this hypothetical protocol, the state of pulses received by Charlie can be expressed as

$$\hat{\sigma}^{\mathrm{vir}}_{C;j_Xk_X} = \mathrm{Tr}_{AB}[\hat{P}(|j_X\rangle_A) \otimes \hat{P}(|k_X\rangle_B) \otimes \mathbb{1}_C\hat{P}(|\Psi_Z\rangle_{AC} \otimes |\Psi_Z\rangle_{BC})]. \tag{14}$$

Here $\hat{P}(|x\rangle) = |x\rangle\langle x|$ corresponds to a projection operator for a particular pure state $|x\rangle$. The normalized state can be defined as $\hat{\tilde{\sigma}}^{\mathrm{vir}}_{C;j_Xk_X} = \hat{\sigma}^{\mathrm{vir}}_{C;j_Xk_X} \big/ \mathrm{Tr}(\hat{\sigma}^{\mathrm{vir}}_{C;j_Xk_X})$. The joint probability that Alice (Bob) measures $|j_X\rangle$ ($|k_X\rangle$) and Charlie declares $|\Phi^+\rangle$ is given by

$$Y^{Z,\mathrm{vir}}_{\Phi^+;j_Xk_X} = p(j_X)p(k_X)\mathrm{Tr}(\hat{D}_{\Phi^+}\hat{\tilde{\sigma}}^{\mathrm{vir}}_{C;j_Xk_X}) \tag{15}$$

where $\hat{D}_{\Phi^+}$ is the operator that contains Eve's operation and Charlie's single photon Bell state measurement and $p(j_X)$, $p(k_X)$ represent the probabilities for Alice and Bob to choose X basis, respectively. Since the virtual state $\hat{\sigma}^{\mathrm{vir}}_{C;j_Xk_X}$ can also be expressed in terms of identity and Pauli operators as

$$\hat{\sigma}^{\mathrm{vir}}_{C;j_Xk_X} = \frac{1}{2}\left(\mathbb{1} + \sum_{s=x,y,z}\mathbf{n}_s^{j_X}\hat{\sigma}_s\right) \otimes \frac{1}{2}\left(\mathbb{1} + \sum_{t=x,y,z}\mathbf{n}_t^{j_X}\hat{\sigma}_t\right), \tag{16}$$

it follows that equation (15) can be rewritten as

$$Y^{Z,\mathrm{vir}}_{\Phi^+;j_Xk_X} = p(j_X)p(k_X)\sum_{s,t=X,Y,Z}\mathbf{n}_s\mathbf{n}_t q_{\Phi^+|s,t}. \tag{17}$$

Therefore, to obtain $Y^{Z,\mathrm{vir}}_{\Phi^+;j_Xk_X}$, it suffices to calculate the transmission rate of Pauli operators defined by

$$q_{\Phi^+|s,t} = \mathrm{Tr}(\hat{D}_{\Phi^+}\sigma_s \otimes \sigma_t)\big/4 \tag{18}$$

with $s, t \in \{1, X, Y, Z\}$. The parameters $\mathbf{n}_s$ and $\mathbf{n}_t$ denote the coefficients of Pauli matrices. Note that the transmission rate of operators can also be determined from the yield of signal states used in the actual protocol. To evaluate the yield of these states we employ the entanglement description where Alice (Bob) prepares state $|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle_{A(B)}|\phi_{0Z}\rangle_C + |1_Z\rangle_{A(B)}|\phi_{1Z}\rangle_C)$ in the Z basis and likewise the preparation of optical pulses in the complementary bases can be described as a process where Alice (Bob) generates $|\Phi_X\rangle = |0_X\rangle_{A(B)}|\phi_{0X}\rangle_C$ or $|\Phi_Y\rangle = |0_Y\rangle_{A(B)}|\phi_{0Y}\rangle_C$. By using the same method previously described for the yield of virtual states, we obtain the expression for the yield of actual states as

$$Y_{\Phi^+;j_\alpha k_\beta} = p(j_\alpha)p(k_\beta)\mathrm{Tr}(\hat{D}_{\Phi^+}\rho_{j\alpha} \otimes \rho_{k\beta}) = p(j_\alpha)p(k_\beta)\sum_{s,t=X,Y,Z} \mathbf{n}_s\mathbf{n}_t q_{\Phi^+|s,t} \tag{19}$$

with $p(j_\alpha)$ and $p(k_\beta)$ denoting probabilities for Alice and Bob to measure their subsystems as state $j\alpha$ and $k\beta$, respectively. The states $\rho_{j\alpha}$ and $\rho_{k\beta}$ correspond to the four states defined in equations (8) to (12). We demonstrate in appendix A that explicit computation of (17) can lead to the realization of the transmission rate of identity and Pauli operators $q_{\Phi^+|s,t}$. Furthermore, in appendix B we determine the transmission rate of operators from the yield of actual states as defined in equation (19). By combining the results of equations (A.13) and (B.21) we can deduce the yield of virtual states and subsequently obtain the error rate E_{XX} using equation (13).

Indeed, with this formalism of estimating error rate E_{XX}, we have shown that it is possible to obtain the yield of states which have not been sent during the actual protocol such as $Y^{Z,\mathrm{vir}}_{\Phi^+;1_X 1_X}$. We have shown how to represent this yield in terms of transmission rate of identity and Pauli operators in equation (A.4). Furthermore, we demonstrated how obtain the transmission rate of Pauli operators from the yield of states used in the actual protocol in appendix B, hence enabling us to substitute the obtained results into equation (A.4), and subsequently obtaining $Y^{Z,\mathrm{vir}}_{\Phi^+;1_X 1_X}$. The same argument can be used to obtain the yield of states such as $Y^{Z,\mathrm{vir}}_{\Phi^+;1_X 1_Y}$, $Y^{Z,\mathrm{vir}}_{\Phi^+;1_Y 1_X}$ and $Y^{Z,\mathrm{vir}}_{\Phi^+;1_Y 1_Y}$ which are used to obtain error rates E_{XY}, E_{YX} and E_{YY}, respectively. Remarkably, the error rates obtained are exactly the same as the ones achieved for protocol employing two orthonormal states from the X and Y bases. Therefore, additional states, $|\phi_{1X}\rangle$ and $|\phi_{1Y}\rangle$ that are used in the six state protocol seems to be redundant.

4. Estimation of key generation rate

In our protocol, note that Alice and Bob never reveal their random phase for coherent states prepared in the key (Z) basis. Therefore, the phase randomized coherent states $|\sqrt{\mu}\,e^{i\chi}\rangle$ prepared by Alice and Bob can be described as

$$\int_0^{2\pi} |\sqrt{\mu}\,e^{i\chi}\rangle\langle\sqrt{\mu}\,e^{i\chi}|\,d\chi = \sum_0^\infty \frac{e^{-\mu}\mu^n}{n!}|n\rangle\langle n|, \tag{20}$$

which is a classical mixture of photon number states. This means that the photon number channel model [46] holds and tagging method [44] proposed by Gottesman *et al* (2004) can be employed in our protocol. Therefore, the key generation rate for RFI TF-QKD is given by

$$R = q[-f_{EC}Q^Z_\mu H(E^Z_\mu) + Q^Z_1(1 - I_E)]. \tag{21}$$

where q is the sifting factor and in an asymmetric encoding $q \sim 1$ for an infinitely large number of signals. The terms Q^Z_μ and E^Z_μ correspond to the gain and quantum bit error rate (QBER) in the Z basis. According to the decoy-state theory, the overall gain is given by [47]

$$Q^Z_\mu = \sum_{n=0}^\infty Y_n \frac{\mu^n}{n!}\mathrm{e}^{-\mu}, \tag{22}$$

and the corresponding quantum bit error rate is given by

$$E^Z_\mu Q^Z_\mu = \frac{1}{2}\mathrm{e}^{\mu}Y_0 + e^Z_1\mu\mathrm{e}^{-\mu}Y_1 + \sum_{n\geqslant 2} e^Z_1\frac{\mu\mathrm{e}^{-\mu}}{n!}Y_n. \tag{23}$$

The gain for single photon components in the Z basis is expressed as

$$Q^Z_1 = \mu e^{-\mu}(Y^1_{\Phi^\pm;0Z0Z} + Y^1_{\Phi^\pm;0Z1Z} + Y^1_{\Phi^\pm;1Z0Z} + Y^1_{\Phi^\pm;1Z1Z}). \tag{24}$$

The parameter I_E is estimated from the lower bound of C and upper bound on the error rate, $E^{1,U}_{ZZ}$ from single-photon contributions as shown in equation (2). The parameter $E^{1,U}_{ZZ}$ is estimated from the yield of single photons as follows

$$E^{1,U}_{ZZ} = \frac{E^Z_\mu Q^Z_\mu - e_0 Y_0 \mathrm{e}^{-\mu}}{\mathrm{e}^{-\mu}(Y^{1,L}_{\Phi^\pm;0Z0Z} + Y^{1,L}_{\Phi^\pm;0Z1Z} + Y^{1,L}_{\Phi^\pm;1Z0Z} + Y^{1,L}_{\Phi^\pm;1Z1Z})}, \tag{25}$$

where

$$Y^{1,L}_{\Phi^\pm;j\alpha s\beta} = \frac{\mu}{\mu\nu - \nu^2}\left[Q_{\nu;j\alpha k\beta}\mathrm{e}^{\nu} - Q_{\mu;j\alpha k\beta}\frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2}Q_0\right]. \tag{26}$$

The values $Q_{\nu;j\alpha k\beta}$, $Q_{\mu;j\alpha k\beta}$ are gains obtained on conditional probabilities that Alice and Bob measure the states $j\alpha$, $k\beta$ while Q_0 is the background gain. Finally, the parameter C is computed from the error rates in complementary bases as follows

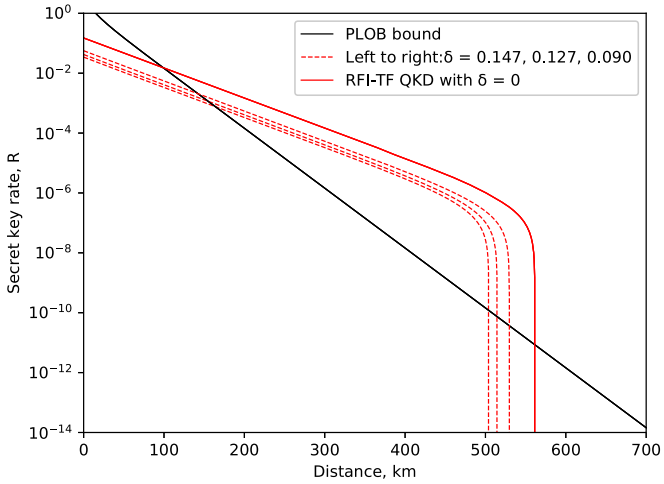

Figure 2. Secret key rate (in logarithmic scale) for RFI-TF protocol with source flaws (dashed lines) as a function of transmission distance measured in km, for experimental parameters: dark counts rate, $p_d = 5 \times 10^{-7}$, the loss coefficient of the channel, $\alpha = 0.2$ km/dB, the detection efficiency, $\eta = 14.5\%$. From left to right the plots represent the encoding flaws $\delta = 0.147$, $\delta = 0.127$ and $\delta = 0.090$. The solid line corresponds to the RFI-TF protocol with perfect encoding, and the solid black line represents the PLOB bound [24].

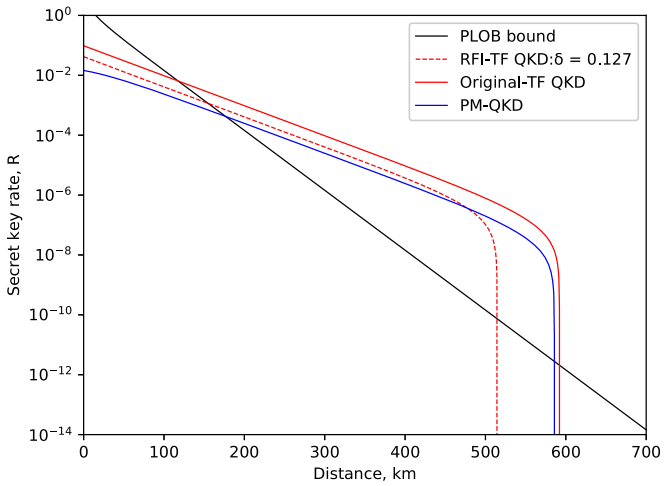

Figure 3. Secret key rate (in logarithmic scale) for RFI-TF protocol with $\delta = 0.127$ (dashed line) as a function of transmission distance measured in km, for experimental parameters: dark counts rate, $p_d = 5 \times 10^{-7}$, loss coefficient of the channel, $\alpha = 0.2$ km/dB, the detection efficiency, $\eta = 14.5\%$. For comparison purposes, we plot the curve for Phase matching (PM) QKD [52] denoted by the blue solid line. The solid red line corresponds to the original TF protocol [25] and the black solid line represents the PLOB bound [24].

$$C = (1 - 2E_{XX})^2 + (1 - 2E_{XY})^2 + (1 - 2E_{YX})^2 + (1 - 2E_{YY})^2. \tag{27}$$

These error rates are computed using yields obtained from the virtual protocol, which are evaluated as shown in the previous section.

4.1. Simulation of the key rate

We demonstrate the performance of the proposed protocol based on fibre implementation. The simulation formulas for parameters Q_μ^Z and E_μ^Z are given in Appendix D. We set intensity parameters for Alice and Bob at $u_{a,b} = 0.6$ and $v_{a,b} = 0.053$. We also assume Charlie uses detectors with efficiency $\eta_{\text{det}} = 14.5\%$ and the dark count rate is assumed to be $p_d = 5 \times 10^{-7}$ which is in line with the current technologies [48–50]. The channel loss coefficient is $\alpha = 0.2\text{dBkm}^{-1}$ and its transmittance is $\eta_{\text{ch}} = 10^{-\frac{0.1\alpha L}{2}}$, with L denoting the fibre length. We consider error correction efficiency, $f_{\text{EC}} = 1.16$.

Our simulation results are depicted in figures 2 and 3. In figure 2 the plots were obtained with $\delta = 0.090$, $\delta = 0.127$ and $\delta = 0.147$, which correspond to deviation of 5.15°, 7.28° and 8.42° from the desired phase angle, respectively. For comparison we plotted the curve for $\delta = 0$ which corresponds to perfect encoding scenario. The

characterization of parameter δ is based on its relation to the extinction ratio according to the definition; $|\tan(\delta/2)|^2 = \eta_{ex}$ [51]. The non-zero extinction ratio is mainly due to imperfections in phase modulators and is of order 10^{-3} in typical experiments. For this value of extinction ratio, we obtain $\delta \approx 0.063$, but in our simulation, we chose pessimistic values for estimation of encoding imperfection to demonstrate the capability of beating repeaterless bound with currently available devices. The results demonstrate that despite an increase in encoding flaws, the key rates achieved are still comparable to the perfect encoding scenario. It is also evident that our protocol implemented with an imperfect source still achieves transmission distances that are beyond the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound for repeaterless QKD [24]. We obtain the maximum transmission distance of 505 km, 516 km and 530 km for preparation flaws $\delta = 0.147$, $\delta = 0.127$ and $\delta = 0.090$, respectively. For the purpose of comparison, the curves for original TF QKD [25], Phase matching (PM) QKD [52] and RFI-TF QKD are plotted in figure 3. The results show that the original TF QKD attains maximum transmission distance of 592 km and RFI-TF QKD can reach a maximum secure distance of 516 km. At a distance of 0 km, the key rate for original TF QKD and RFI-TF QKD are 9.10×10^{-2} and 4.90×10^{-2}, respectively. The gap between the two curves is so small and almost remains constant when the distance increases. This demonstrates that the performance of RFI-TF QKD is still comparable to the original TF-QKD. It is also evident that PM QKD outperforms our proposed protocol in terms of maximum transmission distance realized. However, at shorter distances, our protocol achieves slightly better key rates compared to the PM QKD. Moreover, the merit of the RFI-TF QKD protocol is that it eliminates the need for alignment of reference frames and active phase stabilization.

Furthermore, we compare our results with some TF QKD schemes available in the literature. More recently, Tamaki *et al* (2018) proposed a modified version of the original TF QKD, which employs testing mode for monitoring an eavesdropper and the coding mode for key generation [53]. The phase error rate is estimated in their protocol by considering the bias between two bases (coding and testing modes). On the contrary, our protocol exploits the mismatched basis data to determine error rates in complementary bases (X, Y) in order to estimate Eve's information. Also, our protocol employs the GLLP tagging key rate method [44] since Alice and Bob never reveal the phase information in the key basis, and hence their coherent states are regarded as a mixture of photon number states in the Fock space. In contrast, the GLLP tagging model does not hold in protocol by Tamaki *et al* (2018) since Alice and Bob announces the phase information in the coding mode. Remarkably, our simulation results agree very well with their results. The observed superiority in their results compared to ours may be attributed to a different choice of experimental parameters and the fact that we consider the source flaws in our analysis.

Moreover, we compare our protocol's performance with a TF variant scheme proposed by Lin *et al* (2018) [54]. The first noticeable difference between this work and ours is in key generation mode. In their protocol, Lin *et al* (2018) consider phase matching coherent states for key generation purposes, while in our protocol, we exploit vacuum and phase randomized coherent states to extract secure keys. As already stated, our approach enables us to use the traditional BB84 tagging key generation formula since the phase randomized coherent states are regarded as a mixture of photon number states. However, the method is not applicable for scheme in [54]. Moreover, the scheme in [54] employs non phase randomized coherent test states to perform a variation of tomography on the quantum channel to deduce the information leaked to Eve. In our approach, we use the yields of rejected data to estimate the error rates in the X and Y bases which are used to deduce Eve's information. In terms of maximum attainable distances, we observe that our protocol outperforms the scheme proposed in [54]. We obtain a maximum distance of approximately 500 km while a distance of 400 km was achieved for the previous scheme.

5. Conclusion

We proved the security of the RFI-TF QKD protocol with state preparation flaws. Our results demonstrate that our protocol can overcome the repeaterless PLOB bound. In addition, our protocol is capable of extracting a secure key over a transmission distance of $l = 505$ km, $l = 516$ km and $l = 530$ km for encoding flaws $\delta = 0.090$, $\delta = 0.127$ and $\delta = 0.147$, which corresponds to deviation of $5.15°$, $7.28°$ and $8.42°$ from the desired phase angle, respectively. The results show that despite the state preparation flaws, the key rates achieved are still comparable to those of perfect encoding scenario. Although our protocol cannot achieve a transmission distance beyond the original TF-QKD protocol, its greatest advantage is that it can be implemented without the alignment of reference frames, eliminating the need for active stabilization of interferometers.

Acknowledgments

This work is based on research supported by funding from Botswana International University of Science and Technology Research Initiation Grants (Grant number: R00015 and S00100).

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Appendix A. Determination of yield for virtual states

This section provides an explicit derivation of the yield for virtual states, which are used to deduce error rates for bounding Eve's information. We demonstrate how to concisely represent the joint probabilities of these states in terms of transmission rate of identity and Pauli operators. The yields for virtual states as defined by equation (15) in the main text are given by

$$\begin{aligned} Y^{Z,\mathrm{vir}}_{\Phi^+;0_X0_X} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\hat{\tilde{\sigma}}^{\mathrm{vir}}_{C;0_X0_X}) \\ &= \frac{1}{32}\Bigg[\left(\frac{3}{16}+\frac{1}{4\sqrt{2}}\right)q_{\Phi^+|\mathbb{1},\mathbb{1}} + \left(\frac{1}{8}+\frac{1}{8\sqrt{2}}\right)q_{\Phi^+|\mathbb{1},Z} + \frac{1}{16}\left(\frac{7}{2}+\frac{5}{\sqrt{2}}\right)q_{\Phi^+|\mathbb{1},X} \\ &\quad + \left(\frac{1}{8}+\frac{1}{8\sqrt{2}}\right)q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{8}q_{\Phi^+|Z,Z} + \frac{1}{16}\left(\frac{3}{2+\sqrt{2}}\right)q_{\Phi^+|Z,X} + \frac{1}{16}\left(\frac{7}{2}+\frac{5}{\sqrt{2}}\right)q_{\Phi^+|X,\mathbb{1}} \\ &\quad + \frac{1}{16}\left(\frac{3}{2+\sqrt{2}}\right)q_{\Phi^+|X,Z} + \frac{1}{16}\left(\frac{6}{\sqrt{2}}+\frac{17}{4}\right)q_{\Phi^+|X,X}\Bigg], \end{aligned} \tag{A.1}$$

$$\begin{aligned} Y^{Z,\mathrm{vir}}_{\Phi^+;0_X1_X} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\hat{\tilde{\sigma}}^{\mathrm{vir}}_{C;0_X1_X}) \\ &= \frac{1}{32}\Bigg[\frac{1}{8\sqrt{2}}q_{\Phi^+|\mathbb{1},\mathbb{1}} - \frac{1}{16}q_{\Phi^+|\mathbb{1},Z} - \frac{1}{16}q_{\Phi^+|\mathbb{1},X} + \frac{1}{16}\left(\frac{4}{\sqrt{2}-2}\right)q_{\Phi^+|Z,\mathbb{1}} \\ &\quad + \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right)q_{\Phi^+|Z,Z} + \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right)q_{\Phi^+|Z,X} + \frac{1}{16}\left(\frac{1}{\sqrt{2}}+1\right)q_{\Phi^+|X,\mathbb{1}} \\ &\quad - \frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right)q_{\Phi^+|X,Z} - \frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right)q_{\Phi^+|X,X}\Bigg], \end{aligned} \tag{A.2}$$

$$\begin{aligned} Y^{Z,\mathrm{vir}}_{\Phi^+;1_X0_X} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\hat{\tilde{\sigma}}^{\mathrm{vir}}_{C;1_X0_X}) \\ &= \frac{1}{32}\Bigg[\frac{1}{8\sqrt{2}}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{16}\left(\frac{4}{\sqrt{2}}-2\right)q_{\Phi^+|\mathbb{1},Z} + \frac{1}{16}\left(\frac{1}{\sqrt{2}}+1\right)q_{\Phi^+|\mathbb{1},X} - \frac{1}{16}q_{\Phi^+|Z,\mathbb{1}} \\ &\quad + \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right)q_{\Phi^+|Z,Z} - \frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right)q_{\Phi^+|Z,X} - \frac{1}{16}q_{\Phi^+|X,\mathbb{1}} \\ &\quad + \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right)q_{\Phi^+|X,Z} - \frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right)q_{\Phi^+|X,X}\Bigg], \end{aligned} \tag{A.3}$$

$$\begin{aligned} Y^{Z,\mathrm{vir}}_{\Phi^+;1_X1_X} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\hat{\tilde{\sigma}}^{\mathrm{vir}}_{C;1_X1_X}) \\ &= \frac{1}{32}\Bigg[\frac{1}{16}\left(6-\frac{8}{\sqrt{2}}\right)q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right)q_{\Phi^+|\mathbb{1},Z} + \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right)q_{\Phi^+|\mathbb{1},X} \\ &\quad + \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right)q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right)q_{\Phi^+|Z,Z} + \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right)q_{\Phi^+|Z,X} \\ &\quad + \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right)q_{\Phi^+|X,Z} + \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right)q_{\Phi^+|X,X}\Bigg]. \end{aligned} \tag{A.4}$$

Let the coefficients of transmission rates be given by a row vector $V_{\Phi^+;jXkX}$ and transmission rate of identity and Pauli operators be denoted by a column vector $\mathbf{q}$ such that

$$Y^{Z,\mathrm{vir}}_{\Phi^+;j_X k_X} = V_{\Phi^+;jXkX}\mathbf{q}, \tag{A.5}$$

where

$$\mathbf{q} = [q_{\Phi^+|\mathbb{1},\mathbb{1}}, q_{\Phi^+|\mathbb{1},X}, q_{\Phi^+|\mathbb{1},Y}, q_{\Phi^+|\mathbb{1},Z}, q_{\Phi^+|X,\mathbb{1}}, q_{\Phi^+|X,X}, q_{\Phi^+|X,Y}, q_{\Phi^+|X,Z}, q_{\Phi^+|Y,\mathbb{1}}, q_{\Phi^+|Y,X}, q_{\Phi^+|Y,Y}, q_{\Phi^+|Y,Z}, q_{\Phi^+|Z,\mathbb{1}}, q_{\Phi^+|Z,X}, q_{\Phi^+|Z,Y}, q_{\Phi^+|Z,Z}]^T. \tag{A.6}$$

Then, the vectors $\mathbf{V}_{\Phi^+;jXkX}$ for different yields become

$$\mathbf{V}_{\Phi^+;0X0X} = \left[\left(\frac{3}{16}+\frac{1}{4\sqrt{2}}\right), \frac{1}{16}\left(\frac{7}{2}+\frac{5}{\sqrt{2}}\right), 0, \left(\frac{1}{8}+\frac{1}{8\sqrt{2}}\right), \frac{1}{16}\left(\frac{7}{2}+\frac{5}{\sqrt{2}}\right), \frac{1}{16}\left(\frac{6}{\sqrt{2}}+\frac{17}{4}\right), 0, \frac{1}{16}\left(\frac{3}{2+\sqrt{2}}\right), 0, 0, 0, 0, \left(\frac{1}{8}+\frac{1}{8\sqrt{2}}\right), \frac{1}{16}\left(\frac{3}{2+\sqrt{2}}\right), 0, \frac{1}{8}\right] \tag{A.7}$$

$$V_{\Phi^+;0X1X} = \left[\frac{1}{8\sqrt{2}}, -\frac{1}{16}, 0, -\frac{1}{16}, \frac{1}{16}\left(\frac{1}{\sqrt{2}}+1\right), -\frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right), 0, -\frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right), 0, 0, 0, 0, \frac{1}{16}\left(\frac{4}{\sqrt{2}-2}\right), \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right), 0, \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right)\right] \tag{A.8}$$

$$V_{\Phi^+;1X0X} = \left[\frac{1}{8\sqrt{2}}, \frac{1}{16}\left(\frac{1}{\sqrt{2}}+1\right), 0, \frac{1}{16}\left(\frac{4}{\sqrt{2}}-2\right), -\frac{1}{16}, -\frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right), 0, \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right), 0, 0, 0, 0, -\frac{1}{16}, -\frac{1}{16}\left(\frac{1}{\sqrt{2}}+\frac{1}{2}\right), 0, \frac{1}{16}\left(\frac{2}{\sqrt{2}}-2\right)\right] \tag{A.9}$$

$$V_{\Phi^+;1X1X} = \left[\frac{1}{16}\left(6-\frac{8}{\sqrt{2}}\right), \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right), 0, \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right), \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right), \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right), 0, \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right), 0, 0, 0, 0, \frac{1}{16}\left(4-\frac{6}{\sqrt{2}}\right), \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right), 0, \frac{1}{16}\left(3-\frac{4}{\sqrt{2}}\right)\right] \tag{A.10}$$

Furthermore, if we denote yields as a vector

$$\mathbf{Y}^{Z,\mathrm{vir}}_{\mathbf{\Phi}^+;jXkX} = [Y^{Z,\mathrm{vir}}_{\Phi^+;0_X 0_X}, Y^{Z,\mathrm{vir}}_{\Phi^+;0_X 1_X}, Y^{Z,\mathrm{vir}}_{\Phi^+;1_X 0_X}, Y^{Z,\mathrm{vir}}_{\Phi^+;1_X 1_X}]^T \tag{A.11}$$

and $\mathbf{V}$ as a matrix

$$\mathbf{V} = [V_{\Phi^+;0X0X}, V_{\Phi^+;0X1X}, V_{\Phi^+;1X0X}, V_{\Phi^+;1X1X}], \tag{A.12}$$

the joint probabilities can succinctly be written as

$$\mathbf{Y}^{Z,\mathrm{vir}}_{\mathbf{\Phi}^+,jXkX} = \mathbf{V}\mathbf{q}. \tag{A.13}$$

Appendix B. Determination of yield of states used in the actual protocol

We compute the joint probabilities for sending the four states used in the actual protocol and show that by using the transmission rate for these states, one can obtain the yield of virtual states described above and subsequently estimate the error rate E_{XX}. From the actual experiment, we have the following constraints,

$$\begin{aligned} Y_{\Phi^+;0_Z 0_Z} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Z 0_Z}) \\ &= (q_{\Phi^+|\mathbb{1},\mathbb{1}} + q_{\Phi^+|\mathbb{1},Z} + q_{\Phi^+|Z,\mathbb{1}} + q_{\Phi^+|Z,Z})/32, \end{aligned} \tag{B.1}$$

where

$$\begin{aligned} \sigma^Z_{C;0_Z 0_Z} &= \mathrm{Tr}[\hat{P}(|0_Z\rangle) \otimes \hat{P}(|0_Z\rangle) \otimes \mathbb{1}_C \hat{P}(|\Psi_Z\rangle_{AC} \otimes |\Psi_Z\rangle_{BC})] \\ &= \frac{1}{4}|\phi_{0Z}\rangle\langle\phi_{0Z}| \otimes |\phi_{0Z}\rangle\langle\phi_{0Z}|, \end{aligned} \tag{B.2}$$

$$\begin{aligned} Y_{\Phi^+;0_Z 1_Z} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Z 1_Z}) \\ &= \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{4}q_{\Phi^+|Z,X}\right), \end{aligned} \tag{B.3}$$

$$\begin{aligned} Y_{\Phi^+;1_Z 0_Z} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;1_Z 0_Z}) \\ &= \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}q_{\Phi^+|\mathbb{1},Z} + \frac{1}{4}q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}q_{\Phi^+|X,Z}\right), \end{aligned} \tag{B.4}$$

$$\begin{aligned} Y_{\Phi^+;1_Z 1_Z} &= \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;1_Z 1_Z}) \\ &= \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}q_{\Phi^+|X,X}\right), \end{aligned} \tag{B.5}$$

$$Y_{\Phi^+;0_X0_Z} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_X0_Z}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}q_{\Phi^+|\mathbb{1},Z} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|X,Z}\right), \tag{B.6}$$

$$Y_{\Phi^+;0_X1_Z} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_X1_Z}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} - \frac{1}{4}q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|X,X}\right), \tag{B.7}$$

$$Y_{\Phi^+;0_X0_X} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_X0_X}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}\cos^2(\delta_1)q_{\Phi^+|X,X}\right), \tag{B.8}$$

$$Y_{\Phi^+;0_X0_Y} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_X0_Y}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}\cos(\delta_1)\sin(2\Theta)q_{\Phi^+|X,X}\right), \tag{B.9}$$

$$Y_{\Phi^+;0_Y0_Y} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Y0_Y}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}\sin^2(2\Theta)q_{\Phi^+|X,X}\right), \tag{B.10}$$

$$Y_{\Phi^+;0_Y0_Z} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Y0_Z}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}q_{\Phi^+|\mathbb{1},Z} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|X,Z}\right),$$

$$Y_{\Phi^+;0_Y1_Z} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Y1_Z}) = \frac{1}{8}\left(\frac{1}{2\sqrt{2}}q_{\Phi^+|\mathbb{1},\mathbb{1}} - \frac{1}{2\sqrt{2}}q_{\Phi^+|\mathbb{1},X} + \frac{1}{2\sqrt{2}}\sin(2\Theta)q_{\Phi^+|X,\mathbb{1}} - \frac{1}{2\sqrt{2}}\sin(2\Theta)q_{\Phi^+|X,X}\right), \tag{B.11}$$

$$Y_{\Phi^+;0_Y0_X} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Y0_X}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|X,\mathbb{1}} + \frac{1}{4}\cos(\delta_1)\sin(2\Theta)q_{\Phi^+|X,X}\right), \tag{B.12}$$

$$Y_{\Phi^+;0_Z0_X} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Z0_X}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|Z,X}\right), \tag{B.13}$$

$$Y_{\Phi^+;0_Z0_Y} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;0_Z0_Y}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|\mathbb{1},X} + \frac{1}{4}q_{\Phi^+|Z,\mathbb{1}} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|Z,X}\right), \tag{B.14}$$

$$Y_{\Phi^+;1_Z0_X} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;1_Z0_X}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\cos(\delta_1)q_{\Phi^+|\mathbb{1},X} - \frac{1}{4}q_{\Phi^+|X,\mathbb{1}} - \frac{1}{4}\cos(\delta_1)q_{\Phi^+|X,X}\right), \tag{B.15}$$

$$Y_{\Phi^+;1_Z0_Y} = \frac{1}{8}\mathrm{Tr}(\hat{D}_{\Phi^+}\sigma^Z_{C;1_Z0_Y}) = \frac{1}{8}\left(\frac{1}{4}q_{\Phi^+|\mathbb{1},\mathbb{1}} + \frac{1}{4}\sin(2\Theta)q_{\Phi^+|\mathbb{1},X} - \frac{1}{4}q_{\Phi^+|X,\mathbb{1}} - \frac{1}{4}\sin(2\Theta)q_{\Phi^+|X,X}\right). \tag{B.16}$$

Similar to the virtual protocol, the joint probabilities can be concisely written in terms of vector $\mathbf{q}$ and row vector $V_{\Phi^+,j\alpha k\beta}$ corresponding to the coefficients of transmission rate of Pauli operators as follows

$$Y_{\Phi^+;j\alpha k\beta} = V_{\Phi^+;j\alpha s\beta}\,\mathbf{q}. \tag{B.17}$$

Hence, the vector $\mathbf{Y}_{\Phi^+;j\alpha k\beta}$ can be represented as

$$\begin{aligned}\mathbf{Y}_{\Phi^+;j\alpha k\beta} = [&Y_{\Phi^+;0_Z0_Z},\ Y_{\Phi^+;0_Z1_Z},\ Y_{\Phi^+;1_Z0_Z},\ Y_{\Phi^+;1_Z1_Z},\ Y_{\Phi^+;0_X0_Z},\ Y_{\Phi^+;0_X1_Z},\ Y_{\Phi^+;0_X0_X},\\ &Y_{\Phi^+;0_X0_Y},\ Y_{\Phi^+;0_Y0_Y},\ Y_{\Phi^+;0_Y0_Z},\ Y_{\Phi^+;0_Y1_Z},\ Y_{\Phi^+;0_Y0_X},\ Y_{\Phi^+;0_Z0_X},\ Y_{\Phi^+;0_Z0_Y},\ Y_{\Phi^+;1_Z0_X},\\ &Y_{\Phi^+;1_Z0_Y}]^T\end{aligned} \tag{B.18}$$

and matrix $\mathbf{V}$ obtained from vectors $V_{\Phi^+,j\alpha k\beta}$ is expressed as

$$\begin{aligned}\mathbf{V} = [&V_{\Phi^+;0Z0Z},\ V_{\Phi^+;0Z1Z},\ V_{\Phi^+;1Z0Z},\ V_{\Phi^+;1Z1Z},\ V_{\Phi^+;0X0Z},\ V_{\Phi^+;0X1Z},\ V_{\Phi^+;0X0X},\\ &V_{\Phi^+;0X0Y},\ V_{\Phi^+;0Y0Y},\ V_{\Phi^+;0Y0Z},\ V_{\Phi^+;0Y1Z},\ V_{\Phi^+;0Y0X},\ V_{\Phi^+;0Z0X},\ V_{\Phi^+;0Z0Y},\\ &V_{\Phi^+;1Z0X},\ V_{\Phi^+;1Z0Y}]^T.\end{aligned} \tag{B.19}$$

Finally, we obtain an expression for the joint probabilities,

$$\mathbf{Y}_{\Phi^+;j\alpha k\beta} = \mathbf{V}\mathbf{q}. \tag{B.20}$$

The above result can be rewritten in terms of the transmission rate vector, $\mathbf{q}$ as follows

$$\mathbf{q} = \mathbf{V}^{-1}\mathbf{Y}_{\Phi^+;j\alpha k\beta}. \tag{B.21}$$

Combining the above equation with equation (A.13) we can obtain the yield for virtual states from transmission rate of actual states and thus deduce the error rate E_{XX}.

Appendix C. Security proof against coherent attacks

In this section, we provide security proof using a virtual protocol. The protocol generates measurement statistics that are the same as ones obtained in the actual protocol. Moreover, classical communication between Alice and Bob is precisely the same for both actual and virtual protocols. Therefore, our security claim stems from the fact that two protocols are indistinguishable from Eve's viewpoint. The security proof of our protocol is based on complementarity principle proposed by Koashi in [55, 56]. This technique exploits a virtual protocol that uses an observable which is conjugate of the key generation basis. More precisely, in the actual protocol Alice and Bob generate a key from measurements performed in Z basis, whereas, in the virtual protocol, two parties prepare their signals in an eigenstate of the X basis. In doing so, the two parties can accurately estimate the phase error rate, which is the bit error rate that Alice and Bob would have observed if they would have measured their Z basis state in the X basis. We have shown in the main text how to use the complementarity formalism to estimate this phase error rate. Here, we provide a more detailed description of the virtual protocol used for security proof and consider coherent attacks by Eve through the use of Azuma's inequality [57]. Most importantly, we consider a general case where Alice and Bob prepare mixed states, which can be attributed to the inherent deficiencies in their sources of photons. Note that in the main text, we considered only the pure states for simplicity of our analysis. The mixed states can be represented as

$$\hat{\rho}_{jZ} = P^0_{jZ}|\phi^0_{jZ}\rangle\langle\phi^0_{jZ}| + P^1_{jZ}|\phi^1_{jZ}\rangle\langle\phi^1_{jZ}|, \qquad j \in \{0,\ 1\} \tag{C.1}$$

$$\hat{\rho}_{0X} = P^0_{0X}|\phi^0_{0X}\rangle\langle\phi^0_{0X}| + P^1_{0X}|\phi^1_{0X}\rangle\langle\phi^1_{0X}|, \tag{C.2}$$

$$\hat{\rho}_{0Y} = P^0_{0Y}|\phi^0_{0Y}\rangle\langle\phi^0_{0Y}| + P^1_{0Y}|\phi^1_{0Y}\rangle\langle\phi^1_{0Y}|, \tag{C.3}$$

where P^0_{jZ}, P^1_{jZ}, P^0_{0X}, P^1_{0X}, P^0_{0Y} and P^1_{0Y} are the probabilities that satisfy $P^0_{jZ} + P^1_{jZ} = 1$, $P^0_{0X} + P^1_{0X} = 1$ and $P^0_{0Y} + P^1_{0Y} = 1$. These probabilities are given by

$$P^i_{j\beta} = \frac{1}{2}(1 - (-1)^i\sqrt{(\mathbf{n}^{j\beta}_x)^2 + (\mathbf{n}^{j\beta}_z)^2}). \tag{C.4}$$

The states $\{|\phi^0_{jZ}\rangle,\ |\phi^1_{jZ}\rangle\}$,$\{|\phi^0_{0X}\rangle,\ |\phi^1_{0X}\rangle\}$ and $\{|\phi^0_{0Y}\rangle,\ |\phi^1_{0Y}\rangle\}$ form orthonormal bases. Also, the explicit form of these eigenstates is given by

$$|\phi^i_{j\beta}\rangle = \begin{cases}\dfrac{1}{N}\left(\dfrac{\mathbf{n}^{j\beta}_z - (-1)^i\sqrt{(\mathbf{n}^{j\beta}_x)^2 + (\mathbf{n}^{j\beta}_z)^2}}{\mathbf{n}^{j\beta}_x}|0_Z\rangle + |1_Z\rangle\right) & (\mathbf{n}^{j\beta}_x \neq 0)\\ |i_Z\rangle & (\mathbf{n}^{j\beta}_x = 0\ \wedge\ \mathbf{n}^{j\beta}_z < 0)\\ |i \oplus 1_Z\rangle & (\mathbf{n}^{j\beta}_x = 0\ \wedge\ \mathbf{n}^{j\beta}_z > 0)\end{cases} \tag{C.5}$$

for $i, j \in \{0, 1\}$, $\beta \in \{X, Y, Z\}$ and N denoting the normalization factor while $\mathbf{n}^{j\beta}_x$ and $\mathbf{n}^{j\beta}_z$ represent the coefficients of Pauli operators σ_x and σ_z, respectively. In our security proof, we consider purifications of these mixed states, and that is realized by introducing Alice and Bob's ancilla systems. Thus, we get the following expressions

$$|\tilde{\psi}_{jZ}\rangle_{A_1C} = \sqrt{P^0_{jZ}}\ |0_Z\rangle_{A_1}|\phi^0_{jZ}\rangle_C + \sqrt{P^1_{jZ}}\ |1_Z\rangle_{A_1}|\phi^1_{jZ}\rangle_C \tag{C.6}$$

$$|\tilde{\psi}_{0X}\rangle_{A_1C} = \sqrt{P^0_{0X}}\ |0_X\rangle_{A_1}|\phi^0_{0X}\rangle_C + \sqrt{P^1_{0X}}\ |1_X\rangle_{A_1}|\phi^1_{0X}\rangle_C, \tag{C.7}$$

$$|\tilde{\psi}_{0Y}\rangle_{A_1C} = \sqrt{P^0_{0Y}}\ |0_Y\rangle_{A_1}|\phi^0_{0Y}\rangle_C + \sqrt{P^1_{0Y}}\ |1_Y\rangle_{A_1}|\phi^1_{0Y}\rangle_C, \tag{C.8}$$

where the index A_1 represents Alice's ancilla system that purifies the state and C corresponds to the system that is sent to Charlie. Similarly, for Bob the purifications are given by

$$|\tilde{\psi}_{jZ}\rangle_{B_1C} = \sqrt{P^0_{jZ}}\ |0_Z\rangle_{B_1}|\phi^0_{jZ}\rangle_C + \sqrt{P^1_{jZ}}\ |1_Z\rangle_{B_1}|\phi^1_{jZ}\rangle_C, \tag{C.9}$$

$$|\tilde{\psi}_{0X}\rangle_{B_1C} = \sqrt{P^0_{0X}}\ |0_X\rangle_{B_1}|\phi^0_{0X}\rangle_C + \sqrt{P^1_{0X}}\ |1_X\rangle_{B_1}|\phi^1_{0X}\rangle_C, \tag{C.10}$$

$$|\tilde{\psi}_{0Y}\rangle_{B_1C} = \sqrt{P^0_{0Y}}\ |0_Y\rangle_{B_1}|\phi^0_{0Y}\rangle_C + \sqrt{P^1_{0Y}}\ |1_Y\rangle_{B_1}|\phi^1_{0Y}\rangle_C. \tag{C.11}$$

Now, to proceed with our analysis, we define the entangled states initially prepared by Alice and Bob by incorporating the purified states. For, Alice these states are expressed as

$$|\Psi_Z\rangle_{A_1A_2C} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_{A_2}|\tilde{\psi}_{0Z}\rangle_{A_1C} + |1_Z\rangle_{A_2}|\tilde{\psi}_{1Z}\rangle_{A_1C}\right), \tag{C.12}$$

$$|\Psi_X\rangle_{A_1A_2C} = |0_X\rangle_{A_2}|\tilde{\psi}_{0X}\rangle_{A_1C}, \tag{C.13}$$

$$|\Psi_Y\rangle_{A_1A_2C} = |0_Y\rangle_{A_2}|\tilde{\psi}_{0Y}\rangle_{A_1C}. \tag{C.14}$$

Likewise, Bob prepares the states

$$|\Psi_Z\rangle_{B_1B_2C} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_{B_2}|\tilde{\psi}_{0Z}\rangle_{B_1C} + |1_Z\rangle_{B_2}|\tilde{\psi}_{1Z}\rangle_{B_1C}\right), \tag{C.15}$$

$$|\Psi_X\rangle_{B_1B_2C} = |0_X\rangle_{B_2}|\tilde{\psi}_{0X}\rangle_{B_1C}, \tag{C.16}$$

$$|\Psi_Y\rangle_{B_1B_2C} = |0_Y\rangle_{B_2}|\tilde{\psi}_{0Y}\rangle_{B_1C}, \tag{C.17}$$

where A_2 and B_2 in the equations above represent the systems used by Alice and Bob to generate key bits. Recall that in the virtual protocol, as explained in the main text, Alice and Bob prepare the states in equations (C.12) and (C.15) and measure their subsystems A_2 and B_2 in the X basis rather than Z basis. Therefore, to simplify our analysis we rewrite the state (C.12) in the X basis form as

$$|\Psi_Z\rangle_{A_1A_2C} = \sqrt{\frac{1 + \langle\tilde{\psi}_{0Z}|\tilde{\psi}_{1Z}\rangle_{A_1C}}{2}}\ |0_X\rangle_{A_2}|\tilde{\psi}^{\text{vir}}_{0X}\rangle_{A_1C} + \sqrt{\frac{1 - \langle\tilde{\psi}_{0Z}|\tilde{\psi}_{1Z}\rangle_{A_1C}}{2}}\ |1_X\rangle_{A_2}|\tilde{\psi}^{\text{vir}}_{1X}\rangle_{A_1C}, \tag{C.18}$$

with the normalized virtual states given by

$$|\tilde{\psi}^{\text{vir}}_{jX}\rangle_{A_1C} = \frac{|\tilde{\psi}_{0Z}\rangle_{A_1C} + (-1)^j|\tilde{\psi}_{1Z}\rangle_{A_1C}}{\sqrt{2[1 + (-1)^j\langle\tilde{\psi}_{0Z}|\tilde{\psi}_{1Z}\rangle_{A_1C}]}}. \tag{C.19}$$

The same results are obtained for states prepared by Bob. In what follows, we present a virtual protocol that employs two virtual states, $|\tilde{\psi}^{\text{vir}}_{jX}\rangle_{A_1(B_1)C}$ and four actual states, $|\tilde{\psi}_{jZ}\rangle_{A_1(B_1)C}$, $|\tilde{\psi}_{0X}\rangle_{A_1(B_1)C}$, $|\tilde{\psi}_{0Y}\rangle_{A_1(B_1)C}$ that are sent by Alice (Bob) to Charlie. The preparation, selection, and measurement process of these states can be defined in a more compact form as

$$|\varphi\rangle_{sh_AA_1C} = \sum_{c_A=1}^{6}\sqrt{P(c_A)}\ |c_A\rangle_{sh_A}|\phi^c\rangle_{A_1C} \tag{C.20}$$

and

$$|\varphi\rangle_{sh_BB_1C} = \sum_{c_B=1}^{6}\sqrt{P(c_B)}\ |c_B\rangle_{sh_B}|\phi^c\rangle_{B_1C}, \tag{C.21}$$

for Alice and Bob, respectively. Here the shield systems sh_A and sh_B remains with Alice and Bob. The states $|\phi^c\rangle_{A_1(B_1)C}$ prepared by Alice (Bob) correspond to

$$|\phi^1\rangle_{A_1(B_1)C} = |\tilde{\psi}^{\text{vir}}_{0X}\rangle_{A_1(B_1)C} \tag{C.22}$$

$$|\phi^2\rangle_{A_1(B_1)C} = |\tilde{\psi}^{\text{vir}}_{1X}\rangle_{A_1(B_1)C} \tag{C.23}$$

$$|\phi^3\rangle_{A_1(B_1)C} = |\tilde{\psi}_{0Z}\rangle_{A_1(B_1)C} \tag{C.24}$$

$$|\phi^4\rangle_{A_1(B_1)C} = |\tilde{\psi}_{1Z}\rangle_{A_1(B_1)C} \tag{C.25}$$

$$|\phi^5\rangle_{A_1(B_1)C} = |\tilde{\psi}_{0X}\rangle_{A_1(B_1)C} \tag{C.26}$$

$$|\phi^6\rangle_{A_1(B_1)C} = |\tilde{\psi}_{0Y}\rangle_{A_1(B_1)C}, \tag{C.27}$$

with probabilities given by

$$P(1) = P_Z(1 + \langle\tilde{\psi}_{0Z}|\tilde{\psi}_{1Z}\rangle_{A_1(B_1)C}) \tag{C.28}$$

$$P(1) = P_Z(1 - \langle\tilde{\psi}_{0Z}|\tilde{\psi}_{1Z}\rangle_{A_1(B_1)C}) \tag{C.29}$$

$$P(3) = P(4) = P_Z \tag{C.30}$$

$$P(5) = P_X \tag{C.31}$$

$$P(6) = P_Y. \tag{C.32}$$

We now present comprehensive steps of a virtual protocol as follows.

Virtual protocol

Before starting the protocol, Alice and Bob set a fixed number of rounds (say N trials) needed to complete key generation.

1. *Preparation*. Alice and Bob prepare the states $|\varphi\rangle_{sh_A A_1 C}$ and $|\varphi\rangle_{sh_B B_1 C}$ defined in equations (C.20) and (C.21), respectively, and send the systems C to Charlie through a quantum channel. They delay their measurements until the announcement by Charlie.
2. *Detection announcement*. Charlie performs single-photon interference followed by threshold detection in two detectors and announces successful detection results.
3. *Measurement and classical communication*. Steps 1-2 are repeated until N trials agreed on by two parties are completed. After that, for the case where Charlie declares detection results $|\Phi^+\rangle$, Alice and Bob measure their shield systems $|c_A\rangle$,$|c_B\rangle$ and announce Z (X, Y) basis choice when the results of their measurements is $c = 1, 2, 3, 4$ ($c = 5, 6$). This is done to ensure that classical information in the actual protocol is same as virtual protocol.
4. *Estimation of the number of phase errors*. Alice and Bob use the events $c = 3, 4, 5, 6$ which correspond to actual states to estimate the number of phase errors.

The virtual protocol described above is equivalent to the actual protocol because quantum states sent by Alice and Bob in two protocols are the same and classical communication by two parties is precisely identical. To elucidate this argument, when Alice and Bob prepare the virtual states ($c = 1, 2$), they measure their subsystems in the X basis and announce the Z basis instead. The announcement is made in this manner to make the virtual protocol indistinguishable from the actual protocol in which the events ($c = 1, 2$) are used for key generation, i.e., In these events, Alice and Bob measure their systems in the Z basis and also declares the same basis. Such being the case, both protocols are equivalent from Eve's viewpoint.

Now, we present a method used to estimate observed phase errors in N measurements performed by Alice and Bob in their systems c_A and c_B. We consider coherent attacks where Eve interacts with all signals sent by the two parties and executes a joint measurement after classical communication is completed. For this kind of attack, it suffices to use Azuma's inequality [57] which consider any random variables including correlated ones provided that a Martingale and Bounded difference condition (BDC) are satisfied. Azuma's inequality is described as follows.

A sequence of random variables $X^{(0)}, X^{(1)}, \ldots$ is called Martingale if and only if $E[X^{m+1}|X^{(0)}, X^{(1)},\ldots, X^{(m)}] = X^{(m)}\ \forall\ m \geqslant 0$ with $E[\,\cdot\,]$ denoting the expectation value. In addition, $X^{(0)}, X^{(1)}, \ldots$ is considered to satisfy BDC if there exists $c^{(m)} > 0$ such that $|X^{(m+1)} - X^{(m)}| \leqslant c^{(m)}\ \forall\ m \geqslant 0$. Consider a case of N trials described by random variable $X^{(m)}$, where m corresponds to the m^{th} trial. If $X^{(m)}$ is a Martingale and fulfils the BDC with $c^{(m)} = 1$ then Azuma's inequality asserts that

$$\Pr[|X^{(N)} - X^{(0)}| > N\delta] \leqslant 2e^{-\frac{N\delta^2}{2}} \tag{C.33}$$

for any $\delta \in (0, 1)$. For m^{th} trial the random variable $X^{(m)}$ is defined as

$$X^{(m)} := \Lambda^{(m)} - \sum_{j=1}^{m} P(\xi_j = 1|\xi_0,\ldots, \xi_{j-1}), \tag{C.34}$$

where $\Lambda^{(m)}$ is a random variable that corresponds to the actual number of events ($\Lambda^{(m)} = \sum_{j=1}^{m} \xi_j$) observed in the first m trials and ξ_j is a Bernoulli random variable. Furthermore, $P(\xi_j = 1|\xi_0,\ldots, \xi_{j-1})$ is probability of having event $\xi_j = 1$ in the j^{th} run conditioned on the first $j - 1$ outcomes, $\xi_0,\ldots, \xi_{j-1}$. It can be easily shown that the random variables in equation (C.34) are Martingale and fulfils BDC Thus, by applying Azuma's inequality we obtain

$$P[|\Lambda^{(N)} - \sum_{j=1}^{N} P(\xi_j = 1|\xi_0,\ldots,\xi_{j-1})| > N\delta] \leqslant 2e^{-\frac{N\delta^2}{2}} \tag{C.35}$$

where $X^{(0)} = 0$. This essentially implies that

$$\sum_{j=1}^{N} P(\xi_j = 1|\xi_0,\ldots,\xi_{j-1}) - N\delta \leqslant \Lambda^{(N)} \leqslant P(\xi_j = 1|\xi_0,\ldots,\xi_{j-1}) + N\delta \tag{C.36}$$

holds at least with probability $P = 1 - 2e^{-\frac{N\delta^2}{2}}$. Hence,

$$\Lambda^{(N)} = \sum_{j=1}^{N} P(\xi_j = 1|\xi_0,\ldots,\xi_{j-1}) + \delta_A \tag{C.37}$$

except with error probability $\varepsilon_A + \hat{\varepsilon}_A$ where parameter δ_A is bounded by an interval $\delta_A \in [-\Delta_A, \hat{\Delta}_A]$ with $\Delta_A = f_A(N, \varepsilon_A)$, and where $f_A(x, y) = \sqrt{2x \ln \frac{1}{y}}$.

Now, applying Azuma's inequality to our scenario, from the N trials by Alice and Bob in the virtual protocol, if we consider the j^{th} run of the protocol and once we obtain probability for measuring systems c_A and c_B for that particular run conditioned on previous measurement outcomes, then we can find actual number of events observed. Precisely, for random variables $X^l_{c_A c_B}$ with $l = 1,\ldots,N$ Azuma's inequality states that

$$X^l_{c_A c_B} = \Lambda^l_{c_A c_B} - \sum_{j=1}^{l} P_{c_A c_B}(\xi_j|\xi_0,\ldots,\xi_{j-1}), \tag{C.38}$$

where $\Lambda^l_{c_A c_B}$ is a random variable that corresponds to the actual number of events during l trials (l=1, …, N). Moreover, $P_{c_A c_B}(\xi_j|\xi_0,\ldots,\xi_{j-1})$ is the probability of Alice and Bob obtaining the values c_A and c_B in their measurements performed in the j^{th}, conditioned on the previous $j-1$ measurement outcomes, $\xi_j|\xi_0,\ldots,\xi_{j-1}$. To determine this conditional probability in the j^{th} run, we use the joint state prepared by Alice and Bob for N trials

$$\begin{aligned} |\Phi\rangle_{sh_A A_1 C_A sh_B B_1 C_B} &= |\varphi\rangle_{sh_A A_1 C_A} \otimes |\varphi\rangle_{sh_B B_1 C_B} \\ &= |\phi_{j-1}\rangle_{sh_A A_1 C_A}|\phi_j\rangle_{sh_A A_1 C_A}|\phi_{N-j}\rangle_{sh_A A_1 C_A} \\ &\quad \otimes |\phi_{j-1}\rangle_{sh_B B_1 C_B}|\phi_j\rangle_{sh_B B_1 C_B}|\phi_{N-j}\rangle_{sh_B B_1 C_B} \end{aligned} \tag{C.39}$$

where $|\phi_{j-1}\rangle_{sh_{A(B)}\, A(B)_1 C_{A(B)}}$, $|\phi_j\rangle_{sh_{A(B)}\, A(B)_1 C_{A(B)}}$ and $|\phi_{N-j}\rangle_{sh_{A(B)}\, A(B)_1 C_{A(B)}}$ represent states prepared by Alice (Bob) in the first $j-1$ runs, j^{th} run and the remaining $N-j$ runs, respectively. Let define the evolution of the joint state after Eve's action by

$$\mathcal{U}_{\mathbf{C}E}\, |\Phi\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}}|0\rangle_E = \sum_t \hat{C}_{t,\mathbf{C}}\, |\Phi\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}}|t\rangle_E, \tag{C.40}$$

where $\mathcal{U}_{\mathbf{C}E}$ is Eve's unitary transformation on $\mathbf{C}E$ and $\hat{C}_{t,\mathbf{C}}$ corresponds to the Kraus operator which acts on system $\mathbf{C}$ according to Eve's measurement results on her ancilla. Note that here we denote Charlie's system with index $\mathbf{C}$ which essentially corresponds to a joint system constituted by subsystems C_A and C_B received from Alice and Bob, respectively. Now, taking into consideration measurement outcomes prior to the j^{th} run, we define the joint measurement operator for the $j-1$ systems as

$$\hat{\mathcal{O}}_{j-1, sh_A sh_B \mathbf{C}} = \otimes_{i=1}^{j-1} \hat{M}_{sh_A^i sh_B^i \mathbf{C}_i} \tag{C.41}$$

where $\hat{M}_{sh_A^i sh_B^i \mathbf{C}_i}$ represents the Kraus operator associated with i^{th} measurement outcome of Alice and Bob 's systems sh_A, sh_B and Charlie's system $\mathbf{C}$. From this joint measurement operation on $j-1$ systems, we define the measurement outcomes of $j-1$ runs as O_{j-1}. After Eve's interaction, the joint state of the j^{th} run conditioned on the measurement results of the first $j-1$ runs can be expressed as

$$\hat{\rho}^{sh_A sh_B \mathbf{C}}_{j|O_{j-1}} = \frac{\sigma^{sh_A sh_B \mathbf{C}}_{j|O_{j-1}}}{\mathrm{Tr}\,(\sigma^{sh_A sh_B \mathbf{C}}_{j|O_{j-1}})} \tag{C.42}$$

where the state $\sigma^{sh_A sh_B \mathbf{C}}_{j|O_{j-1}}$ is defined as

$$\sigma^{sh_A sh_B \mathbf{C}}_{j|O_{j-1}} = \sum_t \mathrm{Tr}_{\bar{j}}(\hat{P}[\hat{\mathcal{O}}_{j-1, sh_A sh_B \mathbf{C}} \hat{C}_{t,\mathbf{C}}\, |\Phi\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}}]). \tag{C.43}$$

Here Tr is the trace over all systems sh_A, sh_B, A_1, B_1 and $\mathbf{C}$ for all events except for the j^{th} run. This precisely means taking trace with basis $\{|\vec{x}_{j-1}\rangle, |\vec{x}_{N-j}\rangle\}$ where $|\vec{x}_{j-1}\rangle$ and $|\vec{x}_{N-j}\rangle$ correspond to systems in the first $j-1$ runs and remaining $N-j$ runs, respectively. Then equation (C.43) can be equivalently rewritten as

$$\sigma^{sh_A sh_B \mathbf{C}}_{j|O_{j-1}} = \sum_t \sum_{\vec{x}_{j-1}, \vec{x}_{N-j}} \mathrm{Tr}^j_{A_1 B_1}(\hat{P}[\hat{A}^{(\vec{x}_{j-1}, \vec{x}_{N-j})}_{t,\mathbf{C}|O_{j-1}}\, |\phi_j\rangle_{sh_A A_1 sh_B B_1 \mathbf{C}}]) \tag{C.44}$$

where $\mathrm{Tr}^{j}_{A_1B_1}$ denotes trace over A_1 and B_1 in the j^{th} run and $\hat{A}^{(\vec{x}_{j-1},\vec{x}_{N-j})}_{t,\mathbf{C}|O_{j-1}}$ is the Kraus operator acting on the j^{th} system conditioned on the previous measurement outcomes O_{j-1}, and it is given by

$$\hat{A}^{(\vec{x}_{j-1},\vec{x}_{N-j})}_{t,\mathbf{C}|O_{j-1}} = \langle\vec{x}_{N-j}|\langle\vec{x}_{j-1}|\ \hat{\mathcal{O}}_{j-1,sh_Ash_B\mathbf{C}}\hat{C}_{t,\mathbf{C}}\,|\phi_{j-1}\rangle_{sh_AA_1sh_BB_1\mathbf{C}}|\phi_{N-j}\rangle_{sh_AA_1sh_BB_1\mathbf{C}}. \tag{C.45}$$

By substituting equations (C.20) and (C.21) into equation (C.44) we obtain

$$\sigma^{sh_Ash_B\mathbf{C}}_{j|O_{j-1}} = \sum_{c_A,c_B,c_A^*c_B^*}\sqrt{P(c_A)P(c_B)P(c_A^*)P(c_B^*)}\sum_t\sum_{\vec{x}_{j-1},\vec{x}_{N-j}}\mathrm{Tr}^{j}_{A_1B_1}(\hat{P}[\hat{A}^{(\vec{x}_{j-1},\vec{x}_{N-j})}_{t,\mathbf{C}|O_{j-1}}\ |c_A\rangle_{sh_A} \otimes |c_B\rangle_{sh_B}(|\phi^{(c)}\rangle_{A_1}\otimes|\phi^{(c)}\rangle_{B_1})_{\mathbf{C}}]). \tag{C.46}$$

Now the probability that Alice and Bob obtains outcomes c_A and c_B, and Charlie announces detection result $|\Phi^+\rangle$ after measuring his system $\mathbf{C}$ conditioned on the first $j-1$ measurement outcomes is given by

$$\begin{aligned} Y_{\Phi^+c_Ac_B|O_{j-1}} &= \frac{P(c_A)P(c_B)}{\mathrm{Tr}\,(\sigma^{sh_Ash_B\mathbf{C}}_{j|O_{j-1}})}\sum_t\sum_{\vec{x}_{j-1},\vec{x}_{N-j}}\mathrm{Tr}(\hat{P}[\hat{A}^{(\vec{x}_{j-1},\vec{x}_{N-j})}_{t,\mathbf{C}|O_{j-1}}\mathrm{Tr}_{A_1B_1}(|\phi^{(c)}\rangle_{A_1}\otimes|\phi^{(c)}\rangle_{B_1})_{\mathbf{C}}\hat{M}_{\Phi^+}]) \\ &= \frac{P(c_A)P(c_B)}{\mathrm{Tr}\,(\sigma^{sh_Ash_B\mathbf{C}}_{j|O_{j-1}})}\mathrm{Tr}(\hat{D}_{\Phi^+|O_{j-1}}\hat{P}[\mathrm{Tr}_{A_1B_1}(|\phi^{(c)}\rangle_{A_1}\otimes|\phi^{(c)}\rangle_{B_1})_{\mathbf{C}}]) \end{aligned} \tag{C.47}$$

where $\hat{D}_{\Phi^+|O_{j-1}} = \hat{A}^{(\vec{x}_{j-1},\vec{x}_{N-j})}_{t,\mathbf{C}|O_{j-1}}\hat{M}_{\Phi^+}\hat{A}^{(\vec{x}_{j-1},\vec{x}_{N-j})\,\dagger}_{t,\mathbf{C}|O_{j-1}}$ and $\hat{M}_{\Phi^+}$ represent Charlie's measurement operation.

Note that for $c_{A(B)} = 3, 4, 5, 6$ the probability $Y_{\Phi^+c_Ac_B|O_{j-1}}$ corresponds to the actual yields $Y_{\phi^+j\alpha s_\beta}$ ($\alpha, \beta \in \{X, Y, Z\}, s, j \in \{0, 1\}$) described in the main text. From experimental results we know the actual events $\Lambda_{c_Ac_B}$ (for different combinations $c_A(c_B) \in \{3, 4, 5, 6\}$),thus, using equation (C.37) of Azuma's inequality we can calculate the conditional probabilities that corresponds to the yields $Y_{\phi^+j\alpha s_\beta}$. We have shown in the main text and A that we can determine transmission rate of operators from the actual yields and in turn determine the yields of virtual states $Y^{Z\,\mathrm{vir}}_{\Phi^+jXs_X}$ from those transmission rates. These virtual yields corresponds to the conditional probabilities $Y_{\Phi^+c_Ac_B|O_{j-1}}$ for $c_A(c_B) = 1, 2$. Again, we employ Azuma's inequality to determine the actual number of events $\Lambda_{c_Ac_B}$ where $c_A(c_B) = 1, 2$, which represent the number of phase errors.

Appendix D. Channel model

Here, we introduce a channel model to simulate the quantities observed in an actual experiment. We consider a symmetric lossy channel that links Alice and Bob through Charlie with transmittance η. We assume that dark count rate, p_d is measured from the transmission of optical pulses.

D.1. Estimation of gain and error rate from Z basis

In the Z basis, states sent by Alice and Bob are in four possible combinations; $|0\rangle_A \otimes |0\rangle_B$, $|\sqrt{\mu}\,e^{i\chi_a}\rangle_A \otimes |0\rangle_B$, $|0\rangle_A \otimes |\sqrt{\mu}\,e^{i\chi_b}\rangle_B$ and $|\sqrt{\mu}\,e^{i\chi_a}\rangle_A \otimes |\sqrt{\mu}\,e^{i\chi_b}\rangle_B$ where $|0\rangle$ represents the vacuum state (when intesity 0 is selected). After going through the beam-splitter, the resultant states are

$$\begin{aligned} &|0\rangle_A|0\rangle_B \rightarrow BS\,|0\rangle_L|0\rangle_R \\ &|0\rangle_A|\sqrt{\mu}\,e^{i\chi_b}\rangle_B \rightarrow BS\left|\,e^{i\chi_b}\sqrt{\frac{\mu\eta}{2}}\right\rangle_L\left|-e^{i\chi_b}\sqrt{\frac{\mu\eta}{2}}\right\rangle_R \\ &|\sqrt{\mu}\,e^{i\chi_a}\rangle_A|0\rangle_B \rightarrow BS\left|\,e^{i\chi_a}\sqrt{\frac{\mu\eta}{2}}\right\rangle_L\left|\,e^{i\chi_a}\sqrt{\frac{\mu\eta}{2}}\right\rangle_R \\ &|\sqrt{\mu}\,e^{i\chi_a}\rangle_A|\sqrt{\mu}\,e^{i\chi_b}\rangle_B \rightarrow BS\left|\,e^{i\chi_a}\sqrt{\frac{\mu\eta}{2}}+e^{i\chi_b}\sqrt{\frac{\mu\eta}{2}}\right\rangle_L\left|\,e^{i\chi_a}\sqrt{\frac{\mu\eta}{2}}-e^{i\chi_b}\sqrt{\frac{\mu\eta}{2}}\right\rangle_R. \end{aligned} \tag{D.1}$$

The detection probabilities are given by

$$\begin{aligned} p_0 &= 1-\eta \\ p_L &= \eta\cos^2\left(\frac{\chi}{2}\right) \\ p_R &= \eta\sin^2\left(\frac{\chi}{2}\right), \end{aligned} \tag{D.2}$$

where p_0, p_L and p_R denote the probabilities for no click, click in L-detector and click in R-detector, respectively. Taking into consideration the effects caused by dark counts p_d, we have that

$$P_0 = (1-p_d)^2(1-\eta)^2, \tag{D.3}$$

$$P_L = (1-p_d)^2 \exp\left(-\mu\eta\cos^2\left(\frac{\chi}{2}\right)\right) + p_d(1-p_d)\left[(1-\eta)\exp\left(-\mu\eta\cos^2\left(\frac{\chi}{2}\right)\right)\right]$$
$$= p_d(1-p_d)(1-\eta) + (1-p_d)\exp\left(-\mu\eta\cos^2\left(\frac{\chi}{2}\right)\right), \tag{D.4}$$

$$P_R = (1-p_d)^2 \exp\left(-\mu\eta\sin^2\left(\frac{\chi}{2}\right)\right) + p_d(1-p_d)\left[(1-\eta)\exp\left(-\mu\eta\sin^2\left(\frac{\chi}{2}\right)\right)\right]$$
$$= p_d(1-p_d)(1-\eta) + (1-p_d)\exp\left(-\mu\eta\sin^2\left(\frac{\chi}{2}\right)\right), \tag{D.5}$$

$$\begin{aligned} P_{LR} &= 1 - P_0 - P_L - P_R \\ &= (1-p_d)^2\left[1 + (1-\eta) - \left[(1-\eta) + \exp\left(-\mu\eta\cos^2\left(\frac{\chi}{2}\right)\right)\right] - \left[(1-\eta) + \exp\left(-\mu\eta\sin^2\left(\frac{\chi}{2}\right)\right)\right]\right] \\ &\quad + p_d(1-p_d)\left[\exp\left(-\mu\eta\cos^2\left(\frac{\chi}{2}\right)\right) + \exp\left(-\mu\eta\sin^2\left(\frac{\chi}{2}\right)\right)\right] + p_d^2 \\ &= (1-p_d)^2[1 + (1-\eta)e^{-\mu\eta}] + p_d(1-p_d)e^{-\mu\eta} + p_d^2 \end{aligned} \tag{D.6}$$

where P_0, P_{LR}, P_L and P_R correspond to the probabilities that n-photon coherent states from Alice and Bob results in no click in both detectors, click in both detectors, click in L-detector only and click in R-detector only, respectively. The gain Q_μ^Z is therefore estimated from detection probabilities as

$$\begin{aligned} Q_\mu^Z &= P_0 + P_L + P_R + P_{LR} \\ &= (1-p_d)^2(1-\eta)^2 + p_d(1-p_d)(1-\eta) + (1-p_d)\exp\left(-\mu\eta\cos^2\left(\frac{\chi}{2}\right)\right) \\ &\quad + p_d(1-p_d)(1-\eta) + (1-p_d)\exp\left(-\mu\eta\sin^2\left(\frac{\chi}{2}\right)\right) \\ &\quad + (1-p_d)^2[1 + (1-\eta)e^{-\mu\eta}] + p_d(1-p_d)e^{-\mu\eta} + p_d^2 \\ &\approx (1-p_d)^2(1-\eta)e^{-\mu\eta} + 1 + (1-\eta) - 2(1-p_d)^2(1-\eta)e^{-\mu\eta} \\ &\approx (1-p_d)^2(1-\eta)e^{-\mu\eta} + 1 - (1-2p_d)(1-\eta)e^{-\mu\eta} \end{aligned} \tag{D.7}$$

The quantum bit error rate E_μ^Z is estimated as

$$\begin{aligned} E_\mu^Z &= \frac{P_0^n + P_{LR}}{P_0 + P_L + P_R + P_{LR}} \\ &= \frac{1}{Q_\mu}(1-p_d)^2(1-\eta)^2 + (1-p_d)^2[1 + (1-\eta)e^{-\mu\eta}] + p_d(1-p_d)e^{-\mu\eta} + p_d^2 \end{aligned} \tag{D.8}$$

D.2. Estimation of gain in the *X* and *Y* bases

For the states prepared in the complementary bases, we adopt the channel model developed in [52] to estimate gain used for simulation. For simplicity, we study the case where Alice and Bob select the same state and same phase slices according to the phase postselection method ($j_a = j_b$). The states sent by Alice and Bob are $|\sqrt{\mu_a}e^{i\chi_a}\rangle$ and $|\sqrt{\mu_b}e^{i\chi_b}\rangle$, respectively where $\mu_a = \mu_b = \mu/2$. Due to channel losses and detection inefficiencies, the states transform into $|\sqrt{\eta\mu_a}e^{i\chi_a}\rangle$ and $|\sqrt{\eta\mu_a}e^{i\chi_b}\rangle$. After going through the beam splitter, the resultant states are

$$|\alpha_L\rangle = \left|\frac{\sqrt{\eta\mu}}{2}(e^{i\chi_a} + e^{i\chi_b})\right\rangle = \left|\frac{\sqrt{\eta\mu}}{2}e^{i\chi_a}(1 + e^{i\chi_\omega})\right\rangle, \tag{D.9}$$

$$|\alpha_R\rangle = \left|\frac{\sqrt{\eta\mu}}{2}(e^{i\chi_a} - e^{i\chi_b})\right\rangle = \left|\frac{\sqrt{\eta\mu}}{2}e^{i\chi_a}(1 - e^{i\chi_\omega})\right\rangle, \tag{D.10}$$

where χ_ω is the fixed phase difference between the global phases χ_a and χ_b. The detection probabilities are

$$P_\mu(\bar{L}) = (1-p_d)\exp(-|\alpha_L|^2)$$
$$= (1-p_d)\exp\left(-\eta\mu\cos^2\left(\frac{\chi_\omega}{2}\right)\right), \tag{D.11}$$

$$P_\mu(L) = 1 - P_\mu(\bar{L}), \tag{D.12}$$

$$P_\mu(\bar{R}) = (1 - p_d)\exp(-|\alpha_R|^2)$$
$$= (1 - p_d)\exp\left(-\eta\mu \sin^2\left(\frac{\chi_\omega}{2}\right)\right), \quad \text{(D.13)}$$
$$P_\mu(R) = 1 - P_\mu(\bar{R}), \quad \text{(D.14)}$$

where $P_\mu(L)$ and $P_\mu(\bar{L})$ are the probabilities of L click and no click events, respectively, and $P_\mu(R)$ and $P_\mu(\bar{R})$ are defined similarly for R-detector. The total gain is approximated as

$$\begin{aligned} Q_\mu &= P(L)P(\bar{R}) + P(\bar{L})P(R) \\ &= (1 - p_d)\exp\left(-\eta\mu \sin^2\left(\frac{\chi_\omega}{2}\right)\right)\left[1 - (1 - p_d)\exp\left(-\eta\mu \cos^2\left(\frac{\chi_\omega}{2}\right)\right)\right] \\ &\quad + (1 - p_d)\exp\left(-\eta\mu \cos^2\left(\frac{\chi_\omega}{2}\right)\right)\left[1 - (1 - p_d)\exp\left(-\eta\mu \sin^2\left(\frac{\chi_\omega}{2}\right)\right)\right] \\ &\approx (1 - p_d)[1 - (1 - p_d)\exp(-\eta\mu_b)] + p_d(1 - p_d)\exp(-\eta\mu_b) \\ &= (1 - p_d)[1 - (1 - 2p_d)e^{-\eta\mu}] \\ &\approx 1 - e^{-\eta\mu} + 2p_d e^{-\eta\mu}. \end{aligned} \quad \text{(D.15)}$$

ORCID iDs

Comfort Sekga https://orcid.org/0000-0003-4651-9388
Mhlambululi Mafu https://orcid.org/0000-0001-9304-7374

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–50
[2] Bennett C, Brassard G *et al* 1984 Quantum cryptography: public key distribution and coin tossing *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* **175** (Bangalore, India)
[3] Ekert A 1991 *Phys. Rev. Lett.* **67** 661–3
[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121–4
[5] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–21
[6] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[7] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[8] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[9] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 20504
[10] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[11] Stucki D, Walenta N, Vannel F, Thew R, Gisin N, Zbinden H, Gray S, Towery C and Ten S 2009 *New J. Phys.* **11** 075003
[12] Boaron A *et al* 2018 *Phys. Rev. Lett.* **121** 190502
[13] Liao S K *et al* 2017 *Nature* **549** 43
[14] Tang Y L *et al* 2016 *Phys. Rev.* X **6** 011024
[15] Yin J *et al* 2017 *Science* **356** 1140–4
[16] Liao S K *et al* 2018 *Phys. Rev. Lett.* **120** 030501
[17] Peev M *et al* 2009 *New J. Phys.* **11** 075001
[18] Diamanti E, Lo H K, Qi B and Yuan Z 2016 *Npj Quantum Information* **2** 1–12
[19] Pirandola S *et al* 2019 arXiv:1906.01645
[20] Lo H K, Curty M and Tamaki K 2014 *Nat. Photonics* **8** 595
[21] Alléaume R *et al* 2014 *Theor. Comput. Sci.* **560** 62–81
[22] Hänggi E 2010 arXiv:1012.3878
[23] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[24] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 1–15
[25] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[26] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev.* A **98** 062323
[27] Yu Z W, Hu X L, Jiang C, Xu H and Wang X B 2019 *Sci. Rep.* **9** 1–8
[28] Curty M, Azuma K and Lo H K 2019 *Npj Quantum Information* **5** 1–6
[29] Minder M, Pittaluga M, Roberts G, Lucamarini M, Dynes J, Yuan Z and Shields A 2019 *Nat. Photonics* **13** 334–8
[30] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C and Han Z F 2019 *Phys. Rev.* X **9** 021046
[31] Liu Y *et al* 2019 *Phys. Rev. Lett.* **123** 100505
[32] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
[33] Liu J Y, Ding H J, Zhang C M, Xie S P and Wang Q 2019 *Phys. Rev.* A **12** 014059
[34] Laing A, Scarani V, Rarity J and O'Brien J 2010 *Phys. Rev.* A **82** 012304
[35] Wang C, Sun S H, Ma X C, Tang G Z and Liang L M 2015 *Phys. Rev.* A **92** 042319
[36] Zhang C M, Zhu J R and Wang Q 2017 *J. Lightwave Technol.* **35** 4574–8
[37] Yin H L and Fu Y 2019 *Sci. Rep.* **9** 1–13
[38] Liu H, Wang J, Ma H and Sun S 2019 *Phys. Rev.* A **12** 034039
[39] Li Q, Zhu C, Ma S, Wei K and Pei C 2018 *Int. J. Theor. Phys.* **57** 2192–202
[40] Liu K, Li J, Zhu J R, Zhang C M and Wang Q 2017 *Chin. Phys.* B **26** 120302
[41] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502

[42] Liang W Y, Wang S, Li H W, Yin Z Q, Chen W, Yao Y, Huang J Z, Guo G C and Han Z F 2014 *Sci. Rep.* **4** 3617
[43] Wang J, Liu H, Ma H and Sun S 2019 *Phys. Rev.* A **99** 032309
[44] Gottesman D, Lo H K, Lutkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings (IEEE)* 136
[45] Tamaki K, Curty M, Kato G, Lo H K and Azuma K 2014 *Phys. Rev.* A **90** 052314
[46] Ma X 2008 arXiv:0808.1385
[47] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[48] Miki S, Yamashita T, Fujiwara M, Sasaki M and Wang Z 2010 *Opt. Lett.* **35** 2133–5
[49] Nambu Y *et al* 2011 *Opt. Express* **19** 20531–41
[50] Sasaki M *et al* 2011 *Opt. Express* **19** 10387–409
[51] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev.* A **85** 042307
[52] Ma X, Zeng P and Zhou H 2018 *Phys. Rev.* X **8** 031043
[53] Tamaki K, Lo H K, Wang W and Lucamarini M 2018 arXiv: 1805.05511
[54] Lin J and Lütkenhaus N 2018 *Phys. Rev.* A **98** 042332
[55] Koashi M 2007 arXiv:0704.3661
[56] Koashi M 2009 *New J. Phys.* **11** 045018
[57] Azuma K 1967 *Tohoku Mathematical Journal, Second Series* **19** 357–67