

Three-party reference frame independentquantum key distribution protocol

Comfort Sekga and Mhlambululi Mafu

Citation: Chin. Phys. B, 2021, 30 (**12**): 120301. DOI: 10.1088/1674-1056/abff1f
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Three-party reference frame independentquantum key distribution protocol

Comfort Sekga and Mhlambululi Mafu
Chin. Phys. B, 2021, 30 (**12**): 120301. DOI: 10.1088/1674-1056/abff1f

Reference-frame-independent quantum key distribution of wavelength division multiplexing with multiple quantum channels

Zhongqi Sun(孙钟齐), Yanxin Han(韩雁鑫), Tianqi Dou(窦天琦), Jipeng Wang(王吉鹏), Zhenhua Li(李振华), Fen Zhou(周芬), Yuqing Huang(黄雨晴), and Haiqiang Ma(马海强)
Chin. Phys. B, 2021, 30 (**11**): 110303. DOI: 10.1088/1674-1056/abf350

Realization of simultaneous balanced multi-outputs for multi-protocols QKD decoding based onsilica-based planar lightwave circuit

Jin You(游金), Yue Wang(王玥), and Jun-Ming An(安俊明)
Chin. Phys. B, 2021, 30 (**8**): 080302. DOI: 10.1088/1674-1056/abe2ff

Practical decoy-state BB84 quantum key distribution with quantum memory

Xian-Ke Li(李咸柯), Xiao-Qian Song(宋小谦), Qi-Wei Guo(郭其伟), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)
Chin. Phys. B, 2021, 30 (**6**): 060305. DOI: 10.1088/1674-1056/abda31

Continuous-variable quantum key distribution based on photon addition operation

Xiao-Ting Chen(陈小婷), Lu-Ping Zhang(张露萍), Shou-Kang Chang(常守康), Huan Zhang(张欢), and Li-Yun Hu(胡利云)
Chin. Phys. B, 2021, 30 (**6**): 060304. DOI: 10.1088/1674-1056/abd931

Three-party reference frame independent quantum key distribution protocol*

Comfort Sekga and Mhlambululi Mafu†

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

(Received 21 February 2021; revised manuscript received 8 April 2021; accepted manuscript online 8 May 2021)

We present a three-party reference frame independent quantum key distribution protocol which can be implemented without any alignment of reference frames between the sender and the receiver. The protocol exploits entangled states to establish a secret key among three communicating parties. We derive the asymptotic key rate for the proposed protocol against collective attacks and perform a finite-size key security analysis against general attacks in the presence of statistical fluctuations. We investigate the impact of reference frame misalignment on the stability of our protocol, and we obtain a transmission distance of 180 km, 200 km, and 230 km for rotation of reference frames $\beta = \pi/6$, $\beta = \pi/8$ and $\beta = 0$, respectively. Remarkably, our results demonstrate that our proposed protocol is not heavily affected by an increase in misalignment of reference frames as the achievable transmission distances are still comparable to the case where there is no misalignment in reference frames (when $\beta = 0$). We also simulate the performance of our protocol for a fixed number of signals. Our results demonstrate that the protocol can achieve an effective key generation rate over a transmission distance of about 120 km with realistic 10^7 finite data signals and approximately achieve 195 km with 10^9 signals. Moreover, our proposed protocol is robust against noise in the quantum channel and achieves a threshold error rate of 22.7%.

Keywords: three-party reference frame independent, quantum key distribution, finite-size key security

PACS: 03.67.Dd **DOI:** 10.1088/1674-1056/abff1f

1. Introduction

Quantum key distribution (QKD) provides the information-theoretically secure communication by exploiting the laws of quantum mechanics to detect an eavesdropper.[1] Since the inception of the primitive BB84 protocol,[2] much effort has been directed towards achieving large-scale practical implementation of QKD in the past decades. Impressively, QKD has made various advances both in theory and experiment, and commercial QKD systems have become available on the market.[3,4] Moreover, practical implementations have also been reported in various countries, for example, during the 2010 World Cup in South Africa,[5] installations in fiber networks at metropolitan areas[6–9] as well as in satellite QKD communications.[10–13] These examples demonstrate that QKD will be vital in securing the next generation of digital communications. Despite these achievements, in practice, several challenges need to be addressed to bridge the gap between theoretical assumptions in security proofs, and actual implementations.[14] To address some of these challenges, a novel protocol capable of overcoming the rate-distance limit of QKD without quantum repeaters was proposed, which is a promising milestone in extending the range of secure quantum communications.[15] Moreover, high dimensional encoding via exploitation of orbital angular momentum has been explored to increase the key generation rates.[16–18] One of the challenges in the practical implementation of QKD is the requirement for an aligned reference frame between the communicating parties.[19] For instance, alignment of polarisation states for polarising encoding and interferometric stability for phase coding. These requirements have proven difficult to be satisfied owing to unstable fiber communication links and imperfections in the measuring devices leading to unknown and varying reference frames and subsequent detrimental effects on the received states.[20] Effort to tackle potential reference frame misalignment by encoding qubits with larger systems requires the creation and manipulation of many photon entangled states that are very difficult to generate and very sensitive to losses.[21–23] Fortunately, the reference frame independent (RFI) protocol was proposed by Laing *et al.*[19] to address this problem of alignment. Since inception of the RFI protocol, outstanding results have been achieved both theoretically[24–30] and experimentally,[20,31–33] thus demonstrating its capability to achieve higher secure key rate under a varying reference frame.

In this work, we widen the reach of QKD by considering the RFI protocol employing the two-qubit entangled photons to establish a secret key between three communicating parties. We demonstrate that the number of communicating parties can be further extended and still achieve a secret key rate and transmission distance comparable to the traditional two-party QKD. We also demonstrate the feasibility of multipartite QKD and its potential for achieving global-scale quantum networks. It has also been shown that multipartite QKD schemes

*Project supported by the Botswana International University of Science and Technology Research Initiation (Grant Nos. R00015 and S00100).

†Corresponding author. E-mail: mafum@biust.ac.bw

© 2021 Chinese Physical Society and IOP Publishing Ltd

are robust in some noise regimes,[34] thus rendering them secure compared to generating a multipartite secret key via many independent bipartite protocols. Moreover, we provide a composable finite-key analysis for the proposed three-party protocol implemented with decoy states based on entropic uncertainty relations. The entropic uncertainty relations is a direct and robust method for quantifying the amount of information held by communicating parties and the eavesdropper. This method also provides tight bounds on the secret key rates obtained from finite resources and avoids estimates compared to pre-existing approaches such as post-selection technique[35] and de Finetti theorem[36] which provide pessimistic finite key rate estimates.

Moreover, our security analysis considers implementation with decoy states, making our proposed protocol robust against photon number splitting (PNS) attacks.[37] This allows us to demonstrate unconditional security against general attacks under practical conditions where a source produces multiple photons. To account for statistical fluctuations in the finite regime, we employ the tail inequality for random sampling without replacement, and multiplicative Chernoff bound proposed in Ref. [38], which provides the tightest bounds on expected and observed values. A large-deviation Chernoff bound[39] is another pre-existing method used for statistical analysis, which is equally rigorous as multiplicative Chernoff bound but fails to produce tight bounds on observed values in the high-loss regime leading to a rapid decrease in the achieved secret key rate. The Gaussian analysis method[40] is also comparable to multiplicative Chernoff bound. However, it is not rigorous as it is only limited to independent and identically distributed random variables. The tail inequality for random sampling without replacement provides the tightest bounds on observed error rates and avoids inequality scaling compared to pre-existing methods used in Refs. [39,41]. This article is organized as follows. In Section 2, we describe the operation of our proposed protocol, and in Section 3, we derive the asymptotic key rate formula against collective attacks. In Section 4, the finite-size key analysis with decoy states is presented, and in Section 5, we discuss the simulation results. Lastly, concluding remarks are provided in Section 6.

2. Operation of the proposed protocol

Alice starts by preparing two-photon entangled state using a spontaneous parametric down-conversion (SPDC) source. She then applies polarization modulation in these entangled photons using the same basis chosen from three Pauli encoding bases X, Y, and Z. The two photons are sent to communicating parties, Bob and Charlie, via insecure quantum channels. Upon receipt of photons, they (Bob and Charlie) measure them using any of the three randomly selected measuring bases, $\{X,Y,Z\}$ to guess the Alice preparation basis. In this protocol, Alice, Bob, and Charlie share a common aligned measurement basis $Z_A = Z_B$ and $Z_A = Z_C$ while other measurements bases X and Y are allowed to slowly vary by an arbitrary angle β (see Fig. 1). Due to the drift in reference frames, the measurement bases complementary to the Z basis is given by

$$X_B = \cos\beta X_A + \sin\beta Y_A, \quad X_C = \cos\beta X_A + \sin\beta Y_A,$$
$$Y_B = \cos\beta Y_A - \sin\beta X_A, \quad Y_C = \cos\beta Y_A - \sin\beta X_A.$$

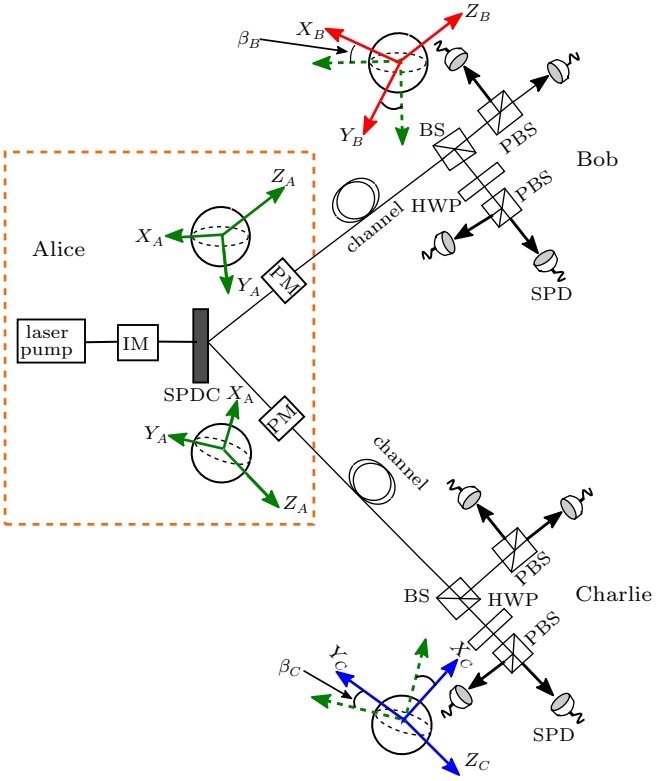


Fig. 1. The schematic diagram of the three-party RFI-QKD protocol. Alice starts by preparing an two-photon entangled state using a spontaneous parametric down-conversion (SPDC) source. Next, the two photons are modulated into polarized states belonging to three bases $\{X,Y,Z\}$ using polarization modulator (PM) and sent to Bob and Charlie through an insecure channel. The photons prepared in the X and Y basis experience misalignment by degree β_B and β_C for Bob and Charlie, respectively. The acronyms IM, BS, PBS, HWP, and SPD, stand for intensity modulator, beam splitter, polarizing beam splitter, a half-wave plate, and single-photon detector, respectively.

We consider the asymmetric basis choice in which the Z basis is chosen with probability $p_z > 1/2$ and the complementary bases, $\{X,Y\}$ with probability $p_c = 1 - p_z$.[42] The three parties uniformly choose a random bit $r_i \in \{0,1\}$ to encode information for their chosen basis. The first steps of the protocol are repeated until they have exchanged enough qubits for the sifting process. Alice, Bob, and Charlie announce their basis choices over an authenticated classical channel and proceed with parameter estimation. The raw key is extracted from the cases where Alice prepared her states in the Z basis while Bob and Charlie measured their received qubits in the Z direction. Therefore, the quantum bit error rate is given by

$$E_{ZZZ} = \frac{1 - \langle Z_A Z_B Z_C \rangle}{2}, \tag{1}$$

where Z_A represents that Alice sends the two states prepared in the Z basis while Z_B and Z_C denote that Bob and Charlie measure received states in the Z direction, respectively. The measurement results in the complementary bases are used to estimate the information that has leaked to Eve. The information is bounded by the statistical quantity C defined as

$$C=\langle X_AX_BX_C\rangle^2+\langle X_AY_BX_C\rangle^2+\langle X_AX_BY_C\rangle^2+\langle Y_AX_BX_C\rangle^2 + \langle Y_AY_BX_C\rangle^2+\langle Y_AX_BY_C\rangle^2+\langle Y_AY_BY_C\rangle^2+\langle X_AY_BY_C\rangle^2, \quad (2)$$

where $\langle \Gamma_A\Gamma_B\Gamma_C\rangle$ (with $\Gamma\in\{X,Y\}$) corresponds to the expectation that Alice prepares two states in the basis Γ_A while Bob and Charlie measure received states in basis Γ_B and Γ_C, respectively. Furthermore, it can be shown that C is independent of the value β when substituting the relations X_B, Y_B and X_C, Y_C in Eq. (2). However, to get an accurate estimate of C, the angle β is assumed to vary slowly in time short enough to allow for the exchange of key.

3. Security analysis

To compute the error bound, we consider the collective attacks, where Eve applies the same attack to each system of Bob and Charlie. The security analysis is sketched along the lines in Refs. [19,43]. We consider an entanglement based protocol in which Alice, Bob and Charlie initially share an entangled state $|\phi^+\rangle_{A_bA_cBC}=\frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)$ with the first two particles A_b and A_c belonging to Alice and the last two particles, B and C are in possession of Bob and Charlie, respectively. Alice measures her qubits in the same direction using three Pauli basis $\{X,Y,Z\}$ while Bob and Charlie also measure their particles using the same mutually unbiased bases. This protocol is equivalent to the prepare and measure protocol described in Section 2. Note that in this entanglement-based description, Alice performs measurement on two particles (which we refer to as b and c) to encode her bit of information which is equivalent to preparing two states sent to Bob and Charlie in prepare and measure protocol. For collective attacks, the density matrix describing the state shared by Alice, Bob, and Charlie is the diagonal in the GHZ state basis known to Eve and written as

$$\begin{aligned}\rho_{A_bA_cBC}=&\mu_1|\phi^+\rangle\langle\phi^+|+\mu_2|\phi^-\rangle\langle\phi^-|+\mu_3|\psi^+\rangle\langle\psi^+|\\&+\mu_4|\psi^-\rangle\langle\psi^-|+\mu_5|\Phi^+\rangle\langle\Phi^+|+\mu_6|\Phi^-\rangle\langle\Phi^-|\\&+\mu_7|\Psi^+\rangle\langle\Psi^+|+\mu_8|\Psi^-\rangle\langle\Psi^-|+\mu_9|\varphi^+\rangle\langle\varphi^+|\\&+\mu_{10}|\varphi^-\rangle\langle\varphi^-|+\mu_{11}|\Phi^+\rangle\langle\Phi^+|+\mu_{12}|\Phi^-\rangle\langle\Phi^-|\\&+\mu_{13}|\Psi^+\rangle\langle\Psi^+|+\mu_{14}|\Psi^-\rangle\langle\Psi^-|\\&+\mu_{15}|\chi^+\rangle\langle\chi^+|+\mu_{16}|\chi^-\rangle\langle\chi^-|, \quad (3)\end{aligned}$$

where $|\phi^\pm\rangle=\frac{1}{\sqrt{2}}(|0000\rangle\pm|1111\rangle)$, $|\psi^\pm\rangle=\frac{1}{\sqrt{2}}(|0001\rangle\pm|1110\rangle)$, $|\Phi^\pm\rangle=\frac{1}{\sqrt{2}}(|0011\rangle\pm|1100\rangle)$, $|\Psi^\pm\rangle=\frac{1}{\sqrt{2}}(|0100\rangle\pm|1011\rangle)$, $|\varphi^\pm\rangle=\frac{1}{\sqrt{2}}(|1000\rangle\pm|0111\rangle)$, $|\Phi^\pm\rangle=\frac{1}{\sqrt{2}}(|0101\rangle\pm|1010\rangle)$, $|\Psi^\pm\rangle=\frac{1}{\sqrt{2}}(|1001\rangle\pm|0110\rangle)$ and $|\Psi^\pm\rangle=\frac{1}{\sqrt{2}}(|0010\rangle\pm|1101\rangle)$. The eigenvalues in Eq. (3) are complex numbers that satisfy the normalization condition

$$\sum_i^{16}|\mu_i|^2=1. \quad (4)$$

Based on the fact that C is invariant under the following transformations $X_{A_{b(c)}}\to-X_{A_{b(c)}}$, $X_B\to-X_B$, $X_C\to-X_C$, $Y_{A_{b(c)}}\to-Y_{A_{b(c)}}$, $Y_B\to-Y_B$, $Y_C\to-Y_C$, we can equivalently represent these transformations with the quantum operation $\rho\to(Z_{A_b}\otimes Z_{A_c}\otimes Z_B\otimes Z_C)\rho(Z_{A_b}\otimes Z_{A_c}\otimes Z_B\otimes Z_C)$. Thus, it follows that the state $\rho_{A_bA_bBC}$ can be written as a mixture

$$\tilde{\rho}=\frac{1}{2}(\rho+Z_{A_b}Z_{A_c}Z_BZ_C\rho Z_{A_b}Z_{A_c}Z_BZ_C). \quad (5)$$

This can be explicitly written as

$$\begin{aligned}&\rho_{A_bA_cBC}\\&=\mu_1|\phi^+\rangle\langle\phi^+|+\mu_2|\phi^-\rangle\langle\phi^-|+\Big(\frac{a}{2}|\phi^-\rangle\langle\phi^+|+\text{H.c}\Big)\\&\quad+\mu_3|\psi^+\rangle\langle\psi^+|+\mu_4|\psi^-\rangle\langle\psi^-|+\Big(\frac{b}{2}|\psi^-\rangle\langle\psi^+|+\text{H.c}\Big)\\&\quad+\mu_5|\Phi^+\rangle\langle\Phi^+|+\mu_6|\Phi^-\rangle\langle\Phi^-|+\Big(\frac{c}{2}|\Phi^-\rangle\langle\Phi^+|+\text{H.c}\Big)\\&\quad+\mu_7|\Psi^+\rangle\langle\Psi^+|+\mu_8|\Psi^-\rangle\langle\Psi^-|+\Big(\frac{d}{2}|\Psi^-\rangle\langle\Psi^+|+\text{H.c}\Big)\\&\quad+\mu_9|\varphi^+\rangle\langle\varphi^+|+\mu_{10}|\varphi^-\rangle\langle\varphi^-|+\Big(\frac{e}{2}|\varphi^-\rangle\langle\varphi^+|+\text{H.c}\Big)\\&\quad+\mu_{11}|\Phi^+\rangle\langle\Phi^+|+\mu_{12}|\Phi^-\rangle\langle\Phi^-|+\Big(\frac{f}{2}|\Phi^-\rangle\langle\Phi^+|+\text{H.c}\Big)\\&\quad+\mu_{13}|\Psi^+\rangle\langle\Psi^+|+\mu_{14}|\Psi^-\rangle\langle\Psi^-|+\Big(\frac{g}{2}|\Psi^-\rangle\langle\Psi^+|+\text{H.c}\Big)\\&\quad+\mu_{15}|\chi^+\rangle\langle\chi^+|+\mu_{16}|\chi^-\rangle\langle\chi^-|+\Big(\frac{h}{2}|\chi^-\rangle\langle\chi^+|+\text{H.c}\Big), \quad (6)\end{aligned}$$

where H.c denotes the complex conjugate of each matrix in the bracket. For ease of notation, let us denote this state as $\tilde{\rho}(a,b,\ldots,h)$. By computing $C=\sum_{\alpha_{Ab}\alpha_{Ac}\beta_B\delta_C}[\text{Tr}(\alpha_{Ab}\otimes\alpha_{Ac}\otimes\beta_B\otimes\delta_C\rho_{A_bA_cBC})]^2$ with $\alpha,\beta,\delta\in\{X,Y\}$, it yields

$$\begin{aligned}C=&4[(\mu_1-\mu_2)^2+4(\mu_3-\mu_4)^2+4(\mu_5-\mu_6)^2+(\mu_7-\mu_8)^2\\&+(\mu_9-\mu_{10})^2+4(\mu_{11}-\mu_{12})^2+4(\mu_{13}-\mu_{14})^2\\&+(\mu_{15}-\mu_{16})^2+\text{Im}(a)^2+\text{Im}(b)^2+\text{Im}(c)^2+\text{Im}(d)^2\\&+\text{Im}(e)^2+\text{Im}(f)^2+\text{Im}(g)^2+\text{Im}(h)^2]. \quad (7)\end{aligned}$$

This result is also attained for its conjugate $\rho(-a^*,-b^*,\ldots,-h^*)$. By using the same logic as before, it is not restrictive to analyze the mixture of $\acute{\rho}=\frac{1}{2}[\tilde{\rho}(a,b,\ldots,h)+\tilde{\rho}(-a^*,-b^*,\ldots,-h^*)]=\bar{\rho}(\text{iA},\text{iB},\ldots,\text{iH})$ to obtain the value of C. Here $\text{A}=\text{Im}(a)$, $\text{B}=\text{Im}(b)$, $\text{H}=\text{Im}(h)$ and other imaginary values have the same meaning. The state $\acute{\rho}$ can be expressed as

$$\acute{\rho}=\sum_{k=1}^{16}\lambda_k|\Phi_k\rangle\langle\Phi_k|, \quad (8)$$

where $|\Phi_{1,2}\rangle=\frac{1}{\sqrt{2}}(e^{i\theta_1}|0000\rangle\pm e^{-i\theta_1}|1111\rangle$, $|\Phi_{3,4}\rangle=\frac{1}{\sqrt{2}}(e^{i\theta_2}|0001\rangle\pm e^{-i\theta_2}|1110\rangle$, $|\Phi_{5,6}\rangle=\frac{1}{\sqrt{2}}(e^{i\theta_3}|0011\rangle\pm$

$e^{-i\theta_3}|1100\rangle$, $|\Phi_{7,8}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_4}|0100\rangle \pm e^{-i\theta_4}|1011\rangle$, $|\varphi_{9,10}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_5}|1000\rangle \pm e^{-i\theta_5}|0111\rangle$, $|\Phi_{11,12}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_6}|0101\rangle \pm e^{-i\theta_6}|1010\rangle$, $|\Psi_{13,14}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_7}|1001\rangle \pm e^{-i\theta_7}|0110\rangle$ and $|\chi_{15,16}\rangle = \frac{1}{\sqrt{2}}(e^{i\theta_8}|0010\rangle \pm e^{-i\theta_8}|1101\rangle$. The parameters are related as follows. Define $\acute{A} = \sqrt{(\mu_1-\mu_2)^2+A^2}$, then $\lambda_{1,2} = \frac{1}{2}(\mu_1+\mu_2 \pm \acute{A})$ and $\cos^2\theta_1 = \frac{1}{2}+(\mu_1-\mu_2)/\acute{A}$. Similarly, if $\acute{B} = \sqrt{4(\mu_3-\mu_4)^2+B^2}$, then we have $\lambda_{3,4} = \frac{1}{2}(\mu_3+\mu_4 \pm \acute{B})$ and $\cos^2\theta_2 = \frac{1}{2}+(\mu_3-\mu_4)/\acute{B}$. The expressions for other eigenvalues and imaginary parts are calculated in similar manner. This implies that the parameter C can now be expressed as

$$\begin{aligned} C = 4\big[&(\lambda_1-\lambda_2)^2+4(\lambda_3-\lambda_4)^2+4(\lambda_5-\lambda_6)^2+(\lambda_7-\lambda_8)^2 \\ &+(\lambda_9-\lambda_{10})^2+4(\lambda_{11}-\lambda_{12})^2+4(\lambda_{13}-\lambda_{14})^2 \\ &+(\lambda_{15}-\lambda_{16})^2\big]. \end{aligned} \tag{9}$$

In what follows we now use parameter C to estimate Eve's information and determine the lower bound on the error rate, E_{ZZZ}. The asymptotic secret key rate under collective attacks is given by[19]

$$r = 1-h(E_{ZZZ})-I_E(E_{ZZZ},C). \tag{10}$$

To estimate Eve's information, I_E, the eigenvalues λ_i have to satisfy the condition: $\sum\lambda_i = 1$ and yield the measured values E_{ZZZ} and C. Since the key is obtained from the measurements in computational basis, this implies $\lambda_1+\lambda_2 = 1-E_{ZZZ}$ and $\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7+\lambda_8+\lambda_9+\lambda_9+\lambda_{10}+\lambda_{11}+\lambda_{12}+\lambda_{13}+\lambda_{14}+\lambda_{15}+\lambda_{16} = E_{ZZZ}$.

The following parametrization is chosen to satisft the above conditions:

$$\begin{aligned} &\lambda_1 = (1-E_{ZZZ})\left(\frac{1+u}{2}\right),\ \lambda_2 = (1-E_{ZZZ})\left(\frac{1-u}{2}\right), \\ &\lambda_3 = \frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}\right),\ \lambda_4 = \frac{1}{7}E_{ZZZ}\left(\frac{1-v}{2}\right), \\ &\lambda_5 = \frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}\right),\ \lambda_6 = \frac{1}{7}E_{ZZZ}\left(\frac{1-v}{2}\right), \\ &\lambda_7 = \frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}\right),\ \lambda_8 = \frac{1}{7}E_{ZZZ}\left(\frac{1-v}{2}\right), \\ &\lambda_9 = \frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}\right),\ \lambda_{10} = \frac{1}{7}E_{ZZZ}\left(\frac{1-v}{2}\right), \\ &\lambda_{11} = \frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}\right),\ \lambda_{12} = \frac{1}{7}E_{ZZZ}\left(\frac{1-v}{2}\right), \\ &\lambda_{13} = \frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}\right),\ \lambda_{14} = \frac{1}{7}E_{ZZZ}\left(\frac{1-v}{2}\right), \\ &\lambda_{15} = \frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}\right),\ \lambda_{16} = \frac{1}{7}E_{ZZZ}\left(\frac{1-v}{2}\right), \end{aligned}$$

where $u,v \in [0,1]$.

The parameter C is calculated to be

$$\begin{aligned} C = 4\Bigg(&\left[(1-E_{ZZZ})\left(\frac{1+u}{2}-\frac{1-u}{2}\right)\right]^2 \\ &+19\left[\frac{1}{7}E_{ZZZ}\left(\frac{1+v}{2}-\frac{1-v}{2}\right)\right]^2\Bigg) \\ = 4&\left[(1-E_{ZZZ})^2u^2+\frac{19}{49}E_{ZZZ}^2v^2\right]. \end{aligned} \tag{11}$$

Eve's information, I_E, is given by the Holevo bound, $I_E = S(\rho_E)-\frac{1}{2}S(\rho_{E|0})-\frac{1}{2}(\rho_{E|1})$. Eve holds a purification of the state shared by Alice, Bob and Charlie, therefore this implies $S(\rho_E) = S(\rho_{A_bA_cBC}) = H(\underline{\lambda})$. To compute $S(\rho_{E|i})$, $i \in [0,1]$, we trace out Bob and Charlie from the state $|\Psi\rangle_{A_bA_cBCE}$ and project Alice on $|+z\rangle$ for $i=0$ and on $|-z\rangle$ for $i=1$. Since both $S(\rho_{E|0})$ and $S(\rho_{E|1})$ occur with equal probability, we obtain $S(\rho_{E|0}) = S(\rho_{E|1}) = h(E_{ZZZ})$. The explicit computation of $H(\underline{\lambda})$ from the eigenvalues λ_i (with $i \in \{0,\ldots,16\}$) is given by

$$\begin{aligned} H(\lambda) &= -\sum_i \lambda_i\log\lambda_i \\ &= -\Big[(1-E_{ZZZ})\Big(\frac{1+u}{2}\Big)\log(1-E_{ZZZ})\Big(\frac{1+u}{2}\Big) \\ &\quad +(1-E_{ZZZ})\Big(\frac{1-u}{2}\Big)\log(1-E_{ZZZ})\Big(\frac{1-u}{2}\Big)\Big] \\ &\quad -7\Big[\frac{E_{ZZZ}}{7}\Big(\frac{1+v}{2}\Big)\log\frac{E_{ZZZ}}{3}\Big(\frac{1+v}{2}\Big) \\ &\quad +\frac{E_{ZZZ}}{7}\Big(\frac{1-v}{2}\Big)\log\frac{E_{ZZZ}}{7}\Big(\frac{1-v}{2}\Big)\Big] \\ &= -(1-E_{ZZZ})\Big[\Big(\frac{1+u}{2}\Big)\log\Big(\frac{1+u}{2}\Big)+\Big(\frac{1-u}{2}\Big)\log\Big(\frac{1-u}{2}\Big)\Big] \\ &\quad -E_{ZZZ}\Big[\Big(\frac{1+v}{2}\Big)\log\Big(\frac{1+v}{2}\Big)+\Big(\frac{1-v}{2}\Big)\log\Big(\frac{1-v}{2}\Big)\Big] \\ &\quad -(1-E_{ZZZ})\Big[\Big(\frac{1+u}{2}\Big)\log(1-E_{ZZZ}) \\ &\quad +\Big(\frac{1-u}{2}\Big)\log(1-E_{ZZZ})\Big] \\ &\quad -E_{ZZZ}\Big[\Big(\frac{1+v}{2}\Big)\log\frac{E_{ZZZ}}{3}+\Big(\frac{1-v}{2}\Big)\log\frac{E_{ZZZ}}{3}\Big] \\ &= h(E_{ZZZ})+(1-E_{ZZZ})h\Big(\frac{1+u}{2}\Big) \\ &\quad +E_{ZZZ}h\Big(\frac{1+v}{2}\Big)+E_{ZZZ}\log 7, \end{aligned} \tag{12}$$

where $h(x) = -x\log(x)-(1-x)\log(1-x)$ is the Shannon entropy function. This yields the following results for Eve's information bound:

$$\begin{aligned} I_E(E,u,v) &= S(\rho_E)-\frac{1}{2}S(\rho_{E|0})-\frac{1}{2}(\rho_{E|1}) \\ &= h(E_{ZZZ})+(1-E_{ZZZ})h\left(\frac{1+u}{2}\right) \\ &\quad +E_{ZZZ}h\left(\frac{1+v}{2}\right)+E_{ZZZ}\log 7-h(E_{ZZZ}) \\ &= (1-E_{ZZZ})h\left(\frac{1+u}{2}\right)+E_{ZZZ}h\left(\frac{1+v}{2}\right) \\ &\quad +E_{ZZZ}\log 7. \end{aligned} \tag{13}$$

Now to compute $I_E(E_{ZZZ},C) = \max_C I_E(E_{ZZZ},u,v)$, we consider the fact that $C = 4[(1-E_{ZZZ})^2u^2+\frac{19}{49}E_{ZZZ}^2v^2]$ and maximizes it over the parameters E_{ZZZ}, u and v. For

$E_{ZZZ}=0$ it can be shown that $I_{\rm E}(E_{ZZZ},C)=h[(1+\sqrt{C/4})/2]$, which gives $I_{\rm E}(E_{ZZZ},C)=0$ for maximally entangled states with $C=4$. For $E_{ZZZ}>0$, we have $v(u)=\sqrt{\frac{49}{19}[(C/4)-(1-E_{ZZZ})^2u^2]}/E_{ZZZ}$, and the condition $v\in[0,1]$ implies that $u\in[u_{\min},u_{\max}]$, where $u_{\min}=\max\left[\frac{\sqrt{(C/4-\frac{19}{49}E_{ZZZ}^2)}}{1-E_{ZZZ}},0\right]$, $u_{\max}=\min\left[\frac{\sqrt{C/4}}{1-E_{ZZZ}},1\right]$. When $E_{ZZZ}\leq 15.9\%$, which is a reasonable value for the practical implementation, we find that $\mathrm{d}I_{\rm E}(E_{ZZZ},u,v(u))/\mathrm{d}u>0$ between $u_{\min}$ and $u_{\max}$. This implies that Eve's information can be bounded by

$$I_{\rm E}(E_{ZZZ},C)=I_{\rm E}(E_{ZZZ},u_{\max},v(u_{\max})). \tag{14}$$

Now, to estimate the parameter C, we consider a case where the state $|\phi^+\rangle_{A_bA_cBC}=\frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)$ initially shared by Alice, Bob and Charlie goes through a depolarising channel and gives rise to the Werner state, $\rho_{A_bA_bBC}=p|\phi^+\rangle\langle\phi^+|+(1-p)I/16$. Here I denotes the identity matrix and p is the probability for state to remain unchanged while $(1-p)$ represents the probability for state to transform into a mixed state. For this four qubit Werner state, the measurement statistics by Alice, Bob and Charlie satisfy $E_{ZZZ}=(1-p)/2$ and $C=4p^2=4(1-2E_{ZZZ})^2$. Thus, we have

$$I_{\rm E}(E_{ZZZ})=(1-E_{ZZZ})h\left(\frac{1-3E_{ZZZ}/2}{1-E_{ZZZ}}\right)+E_{ZZZ}+E_{ZZZ}\log 7. \tag{15}$$

The corresponding secret key rate is therefore derived to be

$$r=1-h(E_{ZZZ})-(1-E_{ZZZ})h\left(\frac{1-3E_{ZZZ}/2}{1-E_{ZZZ}}\right)-E_{ZZZ}-E_{ZZZ}\log 7. \tag{16}$$

The lower bound on the error rate E_{ZZZ} can be obtained for the worst case value of the key generation rate r and hence is given by the solution to the equation

$$1-h(E_{ZZZ})-(1-E_{ZZZ})h\left(\frac{1-3E_{ZZZ}/2}{1-E_{ZZZ}}\right)-E_{ZZZ}-E_{ZZZ}\log 7=0. \tag{17}$$

4. Implementation with decoy states

We extend our security analysis to accommodate imperfections in the state preparation devices. In practice, the secret key is generated by using a spontaneous parametric down-conversion (SPDC) source, which occasionally emits more than one photon. The signals produced by this source contains photons whose probability distribution is given by

$$p(k|\gamma)=\frac{(k+1)(\frac{\gamma}{2})^k}{(1+\frac{\gamma}{2})^{k+2}}, \tag{18}$$

where k is the number of photons and γ is the average intensity of the laser source.[44] Therefore, to combat PNS attack Alice randomly prepares the photons using three different intensities (μ,ν,ω), where μ is the intensity for signal states, ν for decoy states, and ω for vacuum states.[40] The three intensities are usually selected with the probabilities $P_\mu>P_\nu>P_\omega$ where P_μ,P_ν and P_ω correspond to the probabilities for signal, decoy and vacuum states, respectively. The photons are sent to Bob and Charlie, who measures the received pulses in three bases $\{Z,X,Y\}$. The signal states obtained with intensity μ are used for generating the final key, while decoy states acquired from the intensity ν are for bounding Eve's knowledge to the key. In the proposed protocol, Alice measures all the signal pulses, (μ) in the Z basis, and weak decoy pulses, ν in all bases $\{X,Y,Z\}$. The key generation rate is given by

$$r=q\left[Q_0+Q_{ZZZ}^{\mu,1}(1-I_{\rm E}^{\rm U})-\mathrm{leak}_{\rm EC}\right], \tag{19}$$

where q is the raw sift factor. The parameter $\mathrm{leak}_{\rm EC}=f_{\rm EC}Q_{ZZZ}^{\mu}H(E_{ZZZ}^{\mu})$ corresponds to the fraction of bits that have leaked to Eve during the error correction procedure and $f_{\rm EC}\geq 1$ is the error correction efficiency. Q_{ZZZ}^{μ} is the gain of signals prepared using Z basis and intensity μ, and measured by Bob and Charlie in the Z basis. The parameter E_{ZZZ}^{μ} is the quantum bit error rate (QBER) for signals sent using intensity μ and measured in the Z basis. Here $H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ represents the Shannon binary entropy. The term $Q_{ZZZ}^{\mu,1}$ is the gain of single-photon components, Q_0 is the background gain, and $I_{\rm E}^{\rm U}$ is the upper bound on Eve's knowledge of the key. These parameters are estimated by using the decoy theory as follows. Firstly, we highlight that these parameters are generally derived under two-party communication scenarios, but here we extend our analysis to accommodate the third party. In our analysis, we assume that the detection probabilities of photons are independently determined by the channel transmittance, $t=10^{-0.02l}$ where l is the channel length, and detection efficiencies, η_B and η_C of Bob and Charlie's detection systems, respectively. The overall background gain is calculated as

$$\begin{aligned}Q_0&=Q_{0,B}Q_{0,C}\\&=Y_0\left(1+\frac{\mu}{2}\right)^{-2}Y_0\left(1+\frac{\mu}{2}\right)^{-2}=Y_0^2\left(1+\frac{\mu}{2}\right)^{-4},\end{aligned} \tag{20}$$

where $Q_{0,B}$ and $Q_{0,C}$ are the background gains for Bob and Charlie, respectively, and Y_0 is the background count rate. Following the method used in Ref. [45], the gain of signal or decoy states of intensity γ prepared by Alice in basis Γ_A and measured by Bob and Charlie in basis Γ_B and Γ_C, respectively, can be expressed as

$$\begin{aligned}Q_{\Gamma_A\Gamma_B\Gamma_C}^{\gamma}=\frac{1}{2}\Big[&P_{\Gamma_A^0\Gamma_B^0\Gamma_C^0}^{\gamma}+P_{\Gamma_A^0\Gamma_B^1\Gamma_C^1}^{\gamma}+P_{\Gamma_A^1\Gamma_B^0\Gamma_C^0}^{\gamma}+P_{\Gamma_A^1\Gamma_B^1\Gamma_C^1}^{\gamma}\\&+P_{\Gamma_A^0\Gamma_B^0\Gamma_C^1}^{\gamma}+P_{\Gamma_A^0\Gamma_B^1\Gamma_C^0}^{\gamma}+P_{\Gamma_A^1\Gamma_B^0\Gamma_C^1}^{\gamma}+P_{\Gamma_A^1\Gamma_B^1\Gamma_C^0}^{\gamma}\Big],\end{aligned} \tag{21}$$

with $\gamma\in\{\mu,\nu\}$, $\Gamma_A,\Gamma_{\rm B},\Gamma_C\in\{X,Y,Z\}$. The orthonormal states $\Gamma_{A(B)(C)}^0$ and $\Gamma_{A(B)(C)}^1$ belong to the basis $\Gamma_{A(B)(C)}$. The parameter $P_{\Gamma_A^0\Gamma_B^0\Gamma_C^0}^{\gamma}$ corresponds to the probability of Bob and Charlie measuring Γ_B^0 and Γ_C^0 , respectively, conditional on Alice preparing the two states Γ_A^0 with intensity γ. The other

conditional probabilities can be described in a similar manner. The factor $1/2$ in Eq. (21) represents the probability of Alice preparing the qubits in state Γ_A^0 or Γ_A^1. Equation (21) is a generalized expression for different gains, so we evaluate $Q^{\gamma}_{X_AX_BX_C}$ as an example to demonstrate how to explicitly obtain these gains. Firstly, we define $P^{\gamma}_{X_A^0X_B^0X_C^0}$ as follows:

$$\begin{aligned}P^{\gamma}_{X_A^0X_B^0X_C^0} &= \sum_{k=0}^{\infty} p(k|\gamma)\sum_{j=0}^{k} C_j^k(\eta_B t)^j(1-\eta_B t)^{k-j}(\langle X_A^0\rangle X_B^0)^2\chi(k)\\ &\quad\times\sum_{k=0}^{\infty} p(k|\gamma)\sum_{j=0}^{k} C_j^k(\eta_C t)^j(1-\eta_C t)^{k-j}(\langle X_A^0\rangle X_C^0)^2\chi(k)\\ &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1+\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1+\cos\beta}{2}}+Y_0-1\right),\end{aligned} \tag{22}$$

where

$$\chi(k)=\begin{cases}1-Y_0, & \text{if } k>0,\\ Y_0(1-Y_0), & \text{if } k=0\end{cases}$$

denotes the probability of valid detection events conditional on k-photon states. The other conditional probabilities are analogously obtained as

$$\begin{aligned}P^{\gamma}_{X_A^0X_B^1X_C^1} &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1-\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1-\cos\beta}{2}}+Y_0-1\right),\end{aligned} \tag{23}$$

$$\begin{aligned}P^{\gamma}_{X_A^1X_B^0X_C^0} &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1-\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1+\cos\beta}{2}}+Y_0-1\right),\end{aligned} \tag{24}$$

$$\begin{aligned}P^{\gamma}_{X_A^1X_B^1X_C^1} &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1+\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1-\cos\beta}{2}}+Y_0-1\right),\end{aligned} \tag{25}$$

$$\begin{aligned}P^{\gamma}_{X_A^0X_B^0X_C^1} &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1+\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1-\cos\beta}{2}}+Y_0-1\right),\end{aligned} \tag{26}$$

$$\begin{aligned}P^{\gamma}_{X_A^0X_B^1X_C^0} &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1+\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1+\cos\beta}{2}}+Y_0-1\right),\end{aligned} \tag{27}$$

$$\begin{aligned}P^{\gamma}_{X_A^1X_B^0X_C^1} &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1-\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1+\cos\beta}{2}}+Y_0-1\right),\end{aligned} \tag{28}$$

$$\begin{aligned}P^{\gamma}_{X_A^1X_B^0X_C^0} &= \mathrm{e}^{-2\gamma\eta_B t\eta_C t}(1-Y_0)^2\left(\mathrm{e}^{\gamma\eta_B t\frac{1+\cos\beta}{2}}+Y_0-1\right)\\ &\quad\times\left(\mathrm{e}^{\gamma\eta_C t\frac{1-\cos\beta}{2}}+Y_0-1\right).\end{aligned} \tag{29}$$

Here, we assume that the degree of misalignment β is the same for Bob and Charlie's channels. The overall gain, $Q^{\gamma}_{X_AX_BX_C}$ is obtained by combining the results of Eqs. (22)–(29). The overall quantum bit error rate is described as follows:

$$E^{\gamma}_{\Gamma_A\Gamma_B\Gamma_C}=\frac{P^{\gamma}_{\Gamma_A^0\Gamma_B^1\Gamma_C^1}+P^{\gamma}_{\Gamma_A^1\Gamma_B^0\Gamma_C^0}+P^{\gamma}_{\Gamma_A^0\Gamma_B^0\Gamma_C^1}+P^{\gamma}_{\Gamma_A^0\Gamma_B^1\Gamma_C^0}+P^{\gamma}_{\Gamma_A^1\Gamma_B^0\Gamma_C^1}+P^{\gamma}_{\Gamma_A^1\Gamma_B^1\Gamma_C^0}}{Q^{\gamma}_{\Gamma_A\Gamma_B\Gamma_C}}. \tag{30}$$

The gain for single photon components is expressed as

$$\begin{aligned}Q^{\mu,1}_{ZZZ} &= Q^{\mu,1}_{Z_AZ_B}Q^{\mu,1}_{Z_AZ_C}\\ &= [1-(1-Y_{0B})(1-\eta_B t)]\\ &\quad\times[1-(1-Y_{0C})(1-\eta_C t)]\frac{\mu}{(1+\frac{\mu}{2})^3}.\end{aligned} \tag{31}$$

The upper bound $I_{\mathrm{E}}^{\mathrm{U}}$, dependent on the parameters C and E_{ZZZ}, is obtained from the lower bound C_1^{L} and upper bound for the error rate in the Z basis, $e^{1,\mathrm{U}}_{ZZZ}$ for single photon components. The latter parameter is expressed as

$$e^{1,\mathrm{U}}_{ZZZ}=\frac{E_{\mu,ZZZ}Q_{\mu}-e_0Y_0p(\mu|0)}{Y_{1,\mathrm{L}}p(\mu|1)}, \tag{32}$$

where

$$Y_{1,\mathrm{L}}=\frac{p(\mu|2)[Q^{\nu}_{\Gamma_A\Gamma_B\Gamma_C}-p(\nu|0)Y_0]-p(\nu|2)[Q^{\mu}_{\Gamma_A\Gamma_B\Gamma_C}-p(\mu|0)Y_0]}{p(\mu|2)p(\nu|1)-p(\mu|1)p(\nu|2)}. \tag{33}$$

In the above equation, $p(\gamma|k)$ is the probability that signals generated with intensity $\gamma\in\{\mu,\nu\}$ contain k photons. The lower bound of C for single-photon states can be obtained in terms of error rates from measurements in the complementary bases as

$$\begin{aligned}C_1^{\mathrm{L}} &= (1-2e^{1,\mathrm{U}}_{XXX})^2+(1-2e^{1,\mathrm{U}}_{XXY})^2+(1-2e^{1,\mathrm{U}}_{XYY})^2\\ &\quad+(1-2e^{1,\mathrm{U}}_{YXX})^2+(1-2e^{1,\mathrm{U}}_{YYX})^2+(1-2e^{1,\mathrm{U}}_{XYX})^2\\ &\quad+(1-2e^{1,\mathrm{U}}_{YXY})^2+(1-2e^{1,\mathrm{U}}_{YYY})^2.\end{aligned} \tag{34}$$

The upper bound on error rates $e_{\alpha\beta\delta}$ with α, β and $\delta\in\{X,Y\}$ obtained from the signals produced using the decoy intensity are given by

$$\begin{aligned}E^{\nu}_{\Gamma_A\Gamma_B\Gamma_C}Q^{\nu}_{\Gamma_A\Gamma_B\Gamma_C} &= \frac{1}{2}\left(1+\frac{\nu}{2}\right)^{-2}Y_0+e^1_{\alpha\beta\delta}\frac{\nu}{(1+\frac{\nu}{2})^3}Y_1\\ &\quad+\sum_{k\geq 2}e^k_{\alpha\beta\delta}\frac{(1+k)(\frac{\nu}{2})^k}{(1+\frac{\nu}{2})^{k+2}}Y_k;\\ e^{1,\mathrm{U}}_{\alpha\beta\delta} &\leq \frac{E^{\nu}_{\Gamma_A\Gamma_B\Gamma_C}Q^{\nu}_{\Gamma_A\Gamma_B\Gamma_C}-e_0Y_0(1+\frac{\nu}{2})^{-2}}{Y_{1,\mathrm{L}}\frac{\nu}{(1+\frac{\nu}{2})^3}}.\end{aligned} \tag{35}$$

Finally, the upper bound of I_{E} based on $e^{1,\mathrm{U}}_{ZZZ}$ and C_1^{L} is determined using the following equations:

$$\begin{aligned}I_{\mathrm{E}}^{\mathrm{U}} &= (1-e^{1,\mathrm{U}}_{ZZZ})h\left(\frac{1+u_{\max}}{2}\right)-e^{1,\mathrm{U}}_{ZZZ}h\left(\frac{1+v(u_{\max})}{2}\right)\\ &\quad+e^{1,\mathrm{U}}_{ZZZ}\log_2 7,\end{aligned} \tag{36}$$

where

$$u_{\max}=\min\left[\frac{1}{1-e^{1,\mathrm{U}}_{ZZZ}}\sqrt{C_1^{\mathrm{L}}/4},1\right],$$

$$v(u_{\max}) = \sqrt{\frac{49}{19}\left[C_1^{\mathrm{L}}/4 - (1-e_{ZZZ}^{1,\mathrm{U}})^2 u_{\max}^2\right]} \Big/ e_{ZZZ}^{1,\mathrm{U}}. \quad (37)$$

4.1. Finite security analysis

We provide a security proof under a realistic scenario where the communicating parties exchange a finite number of signals N and subsequently account for statistical fluctuations due to finite-size effects. Our security analysis is sketched along the lines presented in[38,39,46–48] based on universally composable framework. Firstly, we point that the three-party RFI protocol generates a triplet of key bit strings $\mathsf{S_A}$, $\mathsf{S_B}$ and $\mathsf{S_C}$ for Alice, Bob, and Charlie, respectively. The key bit strings are of the length ℓ and subject to satisfying the correctness and secrecy criteria for the protocol to be deemed secure. Under the composability criteria, a QKD protocol is regarded correct, if $\mathsf{S_A} = \mathsf{S_B} = \mathsf{S_C}$, for any given attacking strategy by an eavesdropper. Therefore, an $\varepsilon_{\mathrm{cor}}$-correct protocol is invariant from the correct one by a small error probability, $\varepsilon_{\mathrm{cor}}$, i.e., $\Pr[\mathsf{S_A} \neq \mathsf{S_B} \neq \mathsf{S_C}] \leq \varepsilon_{\mathrm{cor}}$. Furthermore, the secrecy conditions are defined as follows: Let ρ_{E} be the state of a quantum system containing the information acquired by an eavesdropper during the execution of a QKD protocol. The correlation of Alice's key bit string $\mathsf{S_A}$ with Eve's quantum state ρ_E can be described by classical-quantum state, $\rho_{\mathsf{S_A}E}$. There is no correlation between Eve's system and Alice's key bit string in an ideal case, i.e., $\rho_U \otimes \rho_E$ where ρ_U is a completely mixed state on the keyspace. The classical-quantum state, $\rho_{\mathsf{S_A}E}$ is said to be Δ-secret if

$$\min_{\rho_E} \frac{1}{2}||\rho_{\mathsf{S_A}E} - \rho_U \otimes \rho_E||_1 \leq \Delta. \quad (38)$$

In particular, a $\varepsilon_{\mathrm{sec}}$-protocol is one protocol which generates the Δ-secure keys with $(1-p_{\mathrm{abort}})\Delta \leq \varepsilon_{\mathrm{sec}}$, with p_{abort} representing the probability that it aborts. Therefore, the key rate of $\varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{cor}}$-three-party rfi protocol is given by

$$\frac{\ell}{N_{\mathrm{total}}} = q\left[Q_0 + Q_{ZZZ}^{\mu,1}(1-I_{\mathrm{E}}^{\mathrm{U}}) - \mathrm{leak}_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{11}{\varepsilon_{\mathrm{sec}}}\right], \quad (39)$$

with $q = \frac{N_\mu p_z^3}{N_{\mathrm{total}}}$, N_μ is the number of exchanged signals of intensity μ, while p_z is the probability of selecting Z basis for preparation and measurement of states, and N_{total} is total number of exchanged signals. In the finite key distillation case, the parameter estimation is not perfect due to fluctuations in the observed error rates and detection rates. From the values directly observed in the experiment, $n_\mu = Q^\mu N_\mu$ and $E^\mu n_\mu$, which corresponds to the number of detected signal states and erroneous detections (using signal intensity μ), respectively, we can use variant multiplicative Chernoff bound presented in lemma 3 of Ref. [38] to estimate their lower and upper bounds from expected values. To demonstrate that, we rewrite n_μ as

$$n_{k,\mu} = \sum_{l=1}^{n_k} \chi_{k,l}^{\mu}, \quad (40)$$

where

$$\chi_{k,l}^{\mu} = \begin{cases} 1 & \text{with probability } p(k|\mu), \\ 0 & \text{with probability } (1-p(k|\mu)), \end{cases} \quad l = 1,\ldots,n_k \quad (41)$$

are independent Bernoulli random variables. In particular, $\chi_{k,l}^{\mu} = 1$ means that k-photon signal state has resulted in the lth detection event, while $\chi_{k,l}^{\mu} = 0$ means either vacuum or decoy state has been used. The term $p(k|\mu)$ is the conditional probability that a source set at signal intensity μ produces a k-photon state. It then follows that for a set of Bernoulli random variables, $\chi_{k,1}^{\mu}, \chi_{k,2}^{\mu}, \ldots, \chi_{k,n_k}^{\mu}$, the expected value of $n_{k,\mu}$ is $\bar{n}_{k,\mu} = E[n_{k,\mu}] = \sum_{l=1}^{n_k} p(k|\mu)$. Let an observed outcome, $n_{k,\mu}$ be denoted by x for a given trial. Then, for any $\varepsilon_3 > 0$ we have

$$\begin{aligned} \bar{n}_{k,\mu} &\geq \max\{0, x - \Delta(x,\varepsilon_3)\}, \\ \bar{n}_{k,\mu}^{\mathrm{L}} &:= \max\{0, x - \Delta(x,\varepsilon_3)\}, \end{aligned} \quad (42)$$

which holds with failure probability ε_3, where $\bar{n}_{k,\mu}^{\mathrm{L}}$ is the lower bound and $\Delta(x,\varepsilon_3)$ is the positive root of the equation $\Delta(x,\varepsilon_3) - [x+\Delta(x,\varepsilon_3)]\ln[1+\Delta(x,\varepsilon_3)/x] - \ln x = 0$. Also, for any $\varepsilon_3 > 0$, we have

$$\begin{aligned} \bar{n}_{k,\mu} &\leq x + \Delta(x,\varepsilon_3), \\ \bar{n}_{k,\mu}^{\mathrm{U}} &:= x + \Delta(x,\varepsilon_3), \end{aligned} \quad (43)$$

which holds with failure probability ε_3, where $\bar{n}_{k,\mu}^{\mathrm{U}}$ is the upper bound of $\bar{n}_{k,\mu}$ and $\Delta(x,\varepsilon_3)$ is the positive root of equation $\Delta(x,\varepsilon_3) + x\ln(x/[x+\Delta(x,\varepsilon_3)]) + \ln\varepsilon_3 = 0$. The same argument can be applied to determine the lower and upper bounds of $n_\nu = Q_\nu N_\nu$ and $n_\omega = Q_\omega N_\omega$ for decoy states and vacuum states, respectively. Next, the lower and upper bounds of n_μ, n_ν and n_ω are used to calculate the lower and upper bounds of gains, Q_μ, Q_ν and Q_ω which are in turn used to calculate $Y_{1,\mathrm{L}}$ by using Eq. (33). Finally, the parameter $Y_{1,\mathrm{L}}$ is used to evaluate lower bound on the expected number of detected single photon components, $n_{1,\mu} = Y_{1,\mathrm{L}} N_\mu p(1|\mu)$. We use multiplicative Chernoff bound (lemma 2) of Ref. [38] to deduce lower bound of parameter $n_{1,\mu}$ as follows. The single photon events are defined by independent Bernoulli random variables as $n_{1,\mu} = \sum_{l=1}^{n_1} \chi_{1,l}$ and the expected value of $n_{1,\mu}$ is denoted as $\bar{n}_{1,\mu} = E[n_{1,\mu}] = \sum_{l=1}^{n_1} p(1|\mu)$. According to results of lemma 2, if $g(\bar{n}_{1,\mu},\delta) = [e^\delta/(1+\delta)^{1+\delta}]^{\bar{n}_{1,\mu}}$, for any $\delta > 0$, the upper tail is defined as

$$\Pr[n_{1,\mu} \geq (1+\delta)\bar{n}_{1,\mu}] < g(\bar{n}_{1,\mu},\delta) = \varepsilon_2, \quad (44)$$

where δ is the positive root of the equation $\bar{n}_{1,\mu}[\delta - (1+\delta)\ln(1+\delta)] - \ln\varepsilon_2 = 0$. For any $0 < \hat{\delta} \leq 1$, we have the lower tail given by

$$\Pr[n_{1,\mu} \leq (1-\hat{\delta})\bar{n}_{1,\mu}] < g(\bar{n}_{1,\mu},-\hat{\delta}) = \hat{\varepsilon_2}, \quad (45)$$

where $\hat{\delta}$ is the positive root of equation $\bar{n}_{1,\mu}[\hat{\delta}+(1-\hat{\delta})\ln(1-\hat{\delta})]+\ln\hat{\varepsilon}_2=0$. The observed lower bound of $n_{1,\mu}$ is given by the upper tail of lemma 2 with failure probability ε_2. The tail inequality for random sampling without replacement is exploited to provide an upper bound for the observed error rates from the expected error rates. The method is described in lemma 1 of Ref. [38] as follows.

Lemma 1[38] For a given $n+m$ string of binary bits $\mathcal{X}_{n+m}\{x_1,x_2,\ldots,x_{n+m}\}$, let $\mathcal{X}_m$ denotes a random sample (without replacement) of size m bit strings and $\mathcal{X}_n$ represents a random sample of the remaining n bit string. Then, for λ_m and λ_n, the probabilities of observing bit 1 value in string $\mathcal{X}_m$ and $\mathcal{X}_n$, respectively, it holds that for any $\epsilon>0$

$$\Pr[\lambda_n\le\lambda_m+\mu(n,m,\lambda_m,\epsilon)]>1-\epsilon,$$

where $\mu(n,m,\lambda_m,\epsilon)$ is the positive root of the following equation:

$$\ln C_m^{m\lambda_m}+\ln C_n^{n\lambda_m+n\mu}-\ln C_{n+m}^{(n+m)\lambda_m+n\mu}-\ln\epsilon=0.$$

Here $C=i!/[j!(1-j)!]$ is the binomial coefficient.

We can use Lemma 1 to estimate the upper bound on observed error rates in the Z basis, e_{ZZZ} by considering a thought experiment picture where an $n+m$ string of bits correspond to compatible measurements made by Alice, Bob and Charlie in the Z basis. If the observed average error rate obtained from m random bit strings is $\bar{e}_{ZZZ}=\sum_{i=1}^{m}r_{Z,A}\oplus r_{Z,B}\oplus r_{Z,C}$ ($r_{Z,A}$, $r_{Z,B}$ and $r_{Z,C}$ are Alice, Bob and Charlie's bits) then by using the upper tail inequality, the remaining n bits give bounds for error rate in the Z basis under the condition that

$$e_{ZZZ}\le\bar{e}_{ZZZ}+\xi(n,m,\bar{e}_{ZZZ},\varepsilon_1),\tag{46}$$

with probability $1-\varepsilon_1$. The other upper bound for error rates in the complementary bases $e_{\alpha\beta\delta}$ with $\alpha,\beta,\delta\in\{X,Y\}$ can be obtained analogously by applying Lemma 1.

5. Simulation results

In this section, we simulate performance of the proposed protocol on a fiber-based QKD system model. We use the following experimental parameters: the loss coefficient of the fiber is 0.2 dB/km, Bob and Charlie's detection efficiencies, $\eta=14.5\%$, and dark count rate of single-photon detector, $P_{\rm d}=1.7\times10^{-6}$. The security parameters of secrecy and correctness are fixed at $\varepsilon_{\rm cor}=10^{-15}$ and $\varepsilon_{\rm sec}=10^{-10}$. We assume that error correction efficiency, $f_{\rm EC}=1.22$ and the expected photon number for signal states is set at $\mu=0.6$. The optimal probability, p_z for key basis is set at 0.95 according to Ref. [49].

Figure 2 shows the secret key rate, ℓ/N, as a function of signal size N for the two-party and three-party RFI protocols. The key rates are obtained at different values for the intrinsic error rate, $Q=(0.02\%,0.03\%,0.05\%)$ due to the misalignment and instability of the optical system. We observe that our proposed protocol can achieve a positive key rate with a minimum of 10^3 signals. It can also be observed that higher key rates are achieved for the three-party protocol as compared to the two-party counterparts for the same number of signals exchanged. Our simulation result demonstrates that the three-party RFI QKD is a feasible scheme in the finite-key regime.

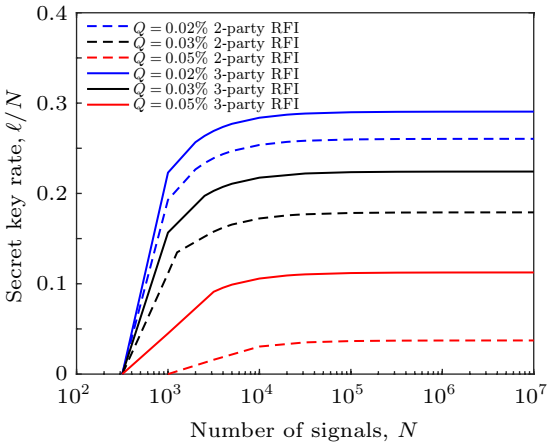


Fig. 2. Plot of secret key fraction versus number of signals N for the proposed three-party RFI protocol (solid lines) for security parameters: $\varepsilon_{\rm cor}=10^{-15}$, $\varepsilon_{\rm sec}=10^{-10}$, and the misalignment error rates $Q=(0.02\%,0.03\%,0.05\%)$. For comparison, we also plot the two-party RFI protocol (dashed lines) for the same error rates.

In Fig. 3(a), we simulate the secret key rate for three-party RFI protocol as a function of transmission distance for fixed misalignment degree $\beta=0,\pi/6,\pi/8$. For comparison, we also simulate the key rate for the two-party RFI protocol (dashed line) for the same parameters. We observe that despite the increase in misalignment of reference frames, the achievable transmission distance is still comparable to when there is no misalignment in reference frames (when $\beta=0$). Also, our results indicate that the two-party RFI protocol outperforms our proposed three-party RFI protocol in terms of maximum attainable transmission distance for different misalignment degrees of β. These results may be attributed to the fact that the three-party RFI protocol considers misalignment in two channels linking Alice to Bob and Charlie. On the contrary, the two-party RFI protocol employs one channel linking Alice and Bob hence a slight increase in signal gain and superiority in performance. Nevertheless, our proposed three-party RFI protocol is more efficient for secure communication involving multiple parties as a secret key for each party is produced from a single run of the protocol rather than performing multiple bipartite QKD protocols to establish a secret key for each communication party.

In Fig. 3(b) we demonstrate the performance of three-party RFI protocol for a fixed number of signals, $N=10^7$, 10^8

and 10^9. For comparison, we provide the plots for the two-party RFI protocol for the same number of signals. Our results demonstrate that with a minimum data size of $N = 10^7$, it is possible to achieve a secure key rate at a reasonable transmission distance of approximately 120 km for the three-party protocol. We also observe the slight superiority of two-party RFI protocol over three-party RFI protocol in terms of achievable secret key rate and transmission distance. Thus, this demonstrates that our proposed protocol fares well against the two-party protocol, which proves its feasibility.

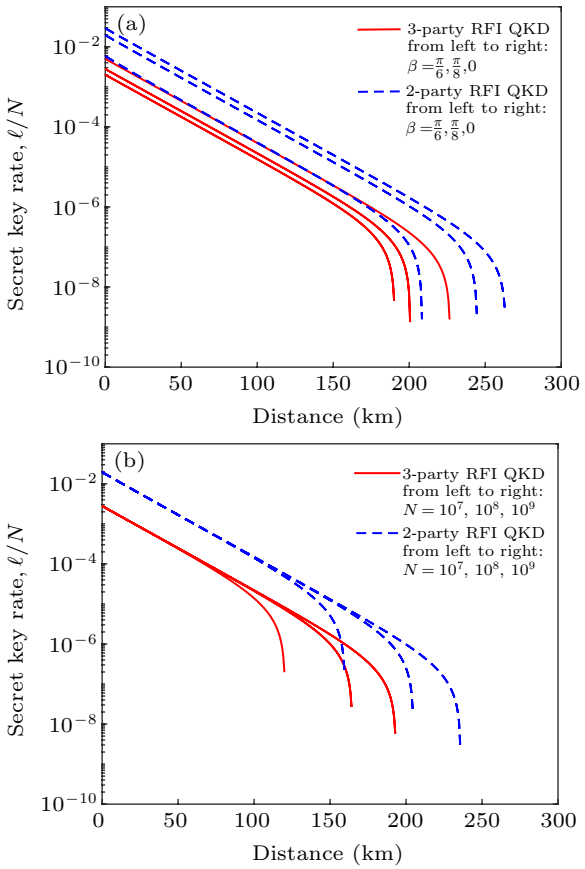


Fig. 3. (a) Expected secret key rate (in logarithmic scale) for the proposed three-party RFI protocol (solid red line) as a function of transmission distance measured in km, for the fixed misalignment degree β. From left to right, the curves represent $\beta = \pi/6$, $\beta = \pi/8$ and $\beta = 0$. The number of signals are fixed at 10^9. (b) Expected secret key rate (in logarithmic scale) for the proposed three party RFI protocol (solid red line) as a function of transmission distance measured in km, for the fixed number of signals, $N = 10^7$, $N = 10^8$ and $N = 10^9$. The relative rotation of reference frames is set at $\beta = \pi/8$ and security parameters are $\varepsilon_{\text{cor}} = 10^{-15}$, $\varepsilon_{\text{sec}} = 10^{-10}$, experimental parameters: dark counts rate, $P_{\text{d}} = 1.7 \times 10^{-6}$, the loss coefficient of the channel is 0.2 km/dB, the detection efficiency is $\eta = 14.5\%$. For comparison purposes we show the plots of two-party RFI protocol, represented by blue dashed lines in both figures.

In Fig. 4, we plot the key rate against the quantum bit error rate in the asymptotic regime to deduce the lower bound on the tolerable error rate. We obtain $E_{ZZZ} \approx 0.2265$ for the proposed protocol, which indicates that a secure key is achievable at higher error rates compared to the two-party RFI protocol[19] with an error bound of 12.62% and the well-known error bound for BB84 protocol of 11.0%.[50]

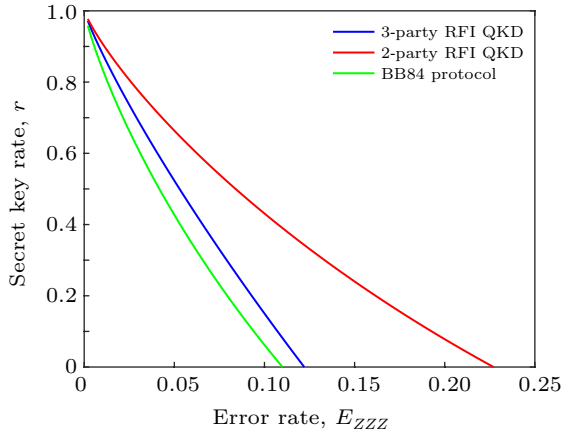


Fig. 4. Plots of secret key rate vs quantum bit error rate, E_{ZZZ} for the BB84 protocol,[50] two-party rfi protocol[19] and the proposed three-party rfi protocol.

6. Conclusion

We presented a three-party RFI QKD protocol that can be implemented without any alignment between the sender and the receiver. The protocol exploits entangled states to establish a secret key between three communicating parties. We derived the asymptotic key rate for the proposed protocol against collective attacks and performed finite-size key security of the three-party RFI QKD protocol. Furthermore, we simulated the secret key rate for three-party RFI protocol as a function of transmission distance for different misalignment degrees ($\beta = \pi/6, \pi/8$) to investigate the impact on statistical quantity C and stability of the protocol. The simulation results demonstrate that our proposed protocol is not heavily affected by an increase in misalignment of reference frames as the achievable transmission distances are still comparable to the case where there is no misalignment in reference frames (when $\beta = 0$).

Furthermore, we investigated the performance of our proposed three-party RFI protocol for a fixed number of signals. The simulation results demonstrate that the protocol can achieve a significant secret key rate at reasonable transmission distances of about 120 km with 10^7 signals. However, a further distance of 195 km can be achieved with about 10^9 finite signals. The proposed protocol presents a suitable alternative for practical QKD implementations. This was demonstrated by reasonable secret key rates obtained with rigorous and tight statistical fluctuation analysis methods for finite-size key effects. Furthermore, our protocol is more efficient than the two-party RFI protocol in terms of resource consumption, as few data signals are required to produce reasonable secret key rates, as evidenced by the finite key analysis results. Moreover, we have also shown that our protocol is robust against noise in the quantum channel based on the realized error rate threshold of 22.7%, which is an improvement to the existing two-party BB84 protocols.

Appendix A: Secrecy

We provide details for the derivation of key length and security bounds presented in this work. We use the entropic uncertainty relations to establish bounds on the smooth-min entropy of the raw key conditioned on Eve's information. Let system $\acute{E}$ be information that Eve gains on Z_A, Z_B and Z_C, i.e., the raw key for Alice, Bob, and Charlie up to the error correction step. If Alice, Bob, and Charlie apply a privacy amplification scheme based on two universal hashing[51] to extract shorter key strings of length ℓ from Z measurement statistics, the protocol is Δ-secret if

$$\Delta \leq 2\varepsilon + \frac{1}{2}\sqrt{2^{\ell - \mathrm{H}^{\varepsilon}_{\min}(Z_A|\acute{E})}}, \tag{A1}$$

where $\mathrm{H}^{\varepsilon}_{\min}(Z_A|\acute{E})$ is the smooth-min entropy.[48,52] It measures the maximum probability that an eavesdropper with access to $\acute{E}$ can guess correctly Alice's bit string, Z_A by using the optimal attacking strategy. Let $v = \frac{1}{2}\sqrt{2^{\ell - \mathrm{H}^{\varepsilon}_{\min}(Z_A|\acute{E})}}$ then,

$$\ell = \mathrm{H}^{\epsilon}_{\min}(Z_A|\acute{E}) - 2\log_2\left(\frac{1}{2v}\right). \tag{A2}$$

By applying chain rule inequality for smooth entropies, and using the fact that the amount of information leaked to an eavesdropper during error correction step is $\mathrm{leak}_{\mathrm{EC}} + \log_2\left(\frac{2}{\varepsilon_{\mathrm{cor}}}\right)$ we have

$$\mathrm{H}^{\epsilon}_{\min}(Z_A|\acute{E}) \geq \mathrm{H}^{\epsilon}_{\min}(Z_A|E) - \mathrm{leak}_{\mathrm{EC}} + \log_2\left(\frac{2}{\varepsilon_{\mathrm{cor}}}\right), \tag{A3}$$

where E is the remaining information available to Eve. Since we are considering the implementation with decoy states, it is important to note that Z_A can be decomposed into $Z^v_A Z^s_A Z^m_A$ which corresponds to bit strings due to vacuum, single photon and multi-photon events. By applying the generalized chained rule according to Ref. [39] we have

$$\begin{aligned}\mathrm{H}^{\epsilon}_{\min}(Z_A|E) \geq\ & \mathrm{H}^{\delta_1}_{\min}(Z^s_A|Z^v_A Z^m_A E) + \mathrm{H}^{\delta_3+2\delta_4+\delta_5}_{\min}(Z^v_A Z^m_A|E) \\ & - 2\log_2\left(\frac{1}{\delta_2}\right) - 1,\end{aligned} \tag{A4}$$

where $\epsilon = 2\delta_1 + \delta_2 + (\delta_3 + \delta_4 + \delta_5)$ for all $\delta_i > 0$. Further, we can apply chain rule on the second term on the r.h.s to obtain

$$\begin{aligned}\mathrm{H}^{\delta_3+2\delta_4+\delta_5}_{\min}(Z^v_A Z^m_A|E) &\geq \mathrm{H}^{\delta_4}_{\min}(Z^m_A|Z^v_A E) + \mathrm{H}^{\delta_5}_{\min}(Z^v_A|E) \\ &\quad - 2\log_2\left(\frac{1}{\delta_3}\right) - 1 \\ &\geq N_\mu p_z^3 Q_0 - 2\log_2\left(\frac{1}{\delta_3}\right) - 1,\end{aligned} \tag{A5}$$

where N_μ is the number of signals sent with intensity μ, p_z is the probability of selecting the Z basis and Q_0 is the gain vacuum events. The second inequality results from these two conditions; $\mathrm{H}^{\delta_4}_{\min}(Z^m_A|Z^v_A E) \geq 0$ and $\mathrm{H}^{\delta_5}_{\min}(Z^v_A|E) = \mathrm{H}_{\min}(Z^v) = \log_2 2^{N_\mu p_z^3 Q_0} = N_\mu p_z^3 Q_0$. The former stems from the fact that all multi-photon events are considered to be insecure due to PNS attack. The latter is due to the fact that vacuum contributions do not carry any information on bit encodings.

We now provide the bound for smooth min entropy $\mathrm{H}^{\delta_1}_{\min}(Z^s_A|Z^v_A Z^m_A E)$ with restriction to single photon events based on the uncertainty relations for smooth entropies.[52] We consider a gedankenexperiment in which all measurements are done in the Y and X bases by the communicating parties; Alice, Bob and Charlie. They have to extract n raw keys from single photon events using compatible measurements,i.e. $X_A \otimes X_B \otimes X_C$ and $Y_A \otimes Y_B \otimes Y_C$. The bound obtained from the max-entropy between Alice, Bob and Charlie is given by

$$\begin{aligned}\mathrm{H}^{\delta_1}_{\min}(Z^s_A|Z^v_A Z^m_A E) &\geq n - \mathrm{H}^{\varepsilon}_{\max}(C_A|\acute{C}) \\ &= n\left[1 - I^{\mathrm{U}}_{\mathrm{E}}(C,e)\right].\end{aligned} \tag{A6}$$

Here, $n = N_\mu p_z^3 Q^{1,\mu}_{ZZZ}$ is the size of a sifted raw key from single-photon events, C_A is Alice's key bit string obtained from complementary bases, (X,Y) and similarly $\acute{C}$ is key bit string for either Bob or Charlie. The term $I^{\mathrm{U}}_{\mathrm{E}}(C,e)$ is determined in terms of C and e. The statistical quantity C is obtained from average values of incompatible measurement results from the hypothetical experiment, and lastly e is the bit error rate of bit strings C_A and $\acute{C}$ which is equivalent to the error rate e_{ZZZ} in the real QKD protocol as described in the main text.

Finally, we compose the error terms due to finite sample sizes and estimation of observed values from expected values as described in the main text. From the main text, we found out that there is error probability, ε_1 due to estimation of observed error rate, e_{ZZZ} by using Lemma 1 of Ref. [38]. The observed error rates in the complementary bases $e_{\alpha\beta\delta}$ with $\alpha,\beta,\delta \in \{X,Y\}$ are obtained analogously applying Lemma 1 with failure probability, ε_1. The error rates from the incompatible measurements in the complementary bases are eight all together which brings the sum of error probabilities to $8\varepsilon_1$. We also estimated the observed number of detected single photon components using lemma 2 of Ref. [38] with failure probability, ε_2. Lemma 3 was used to estimate the expected values, n_μ, n_ν and n_ω with failure probability, ε_3 for each. Therefore combining all the error terms for min-entropies and estimation of observed values, the secrecy is given by

$$\varepsilon_{\mathrm{sec}} = 2\varepsilon + 2(\delta_1 + \delta_2 + \delta_3) + \nu + 9\varepsilon_1 + \varepsilon_2 + 3\varepsilon_3. \tag{A7}$$

In this case, $\delta_4, \delta_5 = 0$ and we set every error term to a common value ε and $\varepsilon_{\mathrm{sec}} = 22\varepsilon$. The final key length ℓ is obtained by substituting the results of Eq. (A3) up to Eq. (A6) and secrecy condition from Eq. (A7) into Eq. (A2). The formula is expressed as

$$\ell = N_\mu p_z^3\left[Q_0 + Q^{1,\mu}_{ZZZ}(1 - I^{\mathrm{U}}_{\mathrm{E}}) - \mathrm{leak}_{\mathrm{EC}} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{11}{\varepsilon_{\mathrm{sec}}}\right]. \tag{A8}$$

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Bennett C and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol. 175 (Bangalore, India)
[3] Pirandola S, Andersen U L, Banchi L, *et al.* 2020 *Adv. Opt. Photonics* **12** 1012
[4] Mao Y, Zeng P and Chen T Y 2020 *Adv. Quantum Technol.* **4** 2000084
[5] Mirza A and Petruccione F 2010 *J. Opt. Soc. Am. B* **27** A185
[6] Peev M, Pacher C, Alléaume R, Barreiro C, *et al.* 2009 *New J. Phys.* **11** 075001
[7] Sasaki M, Fujiwara M, Ishizuka H, *et al.* 2011 *Opt. Express* **19** 10387
[8] Wang S, Chen W, Yin Z Q, *et al.* 2014 *Opt. Express* **22** 21739
[9] Courtland R 2016 *IEEE Spectrum.* **53** 11
[10] Bedington R, Arrazola J M and Ling A 2017 *npj Quantum Inf.* **3** 30
[11] Liao S K, Cai W Q, Liu W Y, *et al.* 2017 *Nature* **549** 43
[12] Yin J, Cao Y, Li Y H, *et al.* 2017 *Science* **356** 1140
[13] Liao S K, Cai W Q, Handsteiner J, *et al.* 2018 *Phys. Rev. Lett.* **120** 030501
[14] Scarani V and Kurtsiefer C 2014 *Theor. Comput. Sci.* **560** 27
[15] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[16] Sit A, Bouchard F, Fickler R, *et al.* 2017 *Optica* **4** 1006
[17] Mirhosseini M, Magaña-Loaiza O S, O'Sullivan M N, Rodenburg B, Malik M, Lavery M P J, Padgett M J, Gauthier D J and Boyd R W 2015 *New J. Phys.* **17** 033033
[18] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 *Phys. Rev. A* **88** 032305
[19] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev. A* **82** 012304
[20] Wabnig J, Bitauld D, Li H, Laing A, O'Brien J and Niskanen A 2013 *New J. Phys.* **15** 073001
[21] Zhang P, Aungskunsiri K, Martín-López E, *et al.* 2014 *Phys. Rev. Lett.* **112** 130501
[22] D'ambrosio V, Nagali E, Walborn S P, Aolita L, Slussarenko S, Marrucci L and Sciarrino F 2012 *Nat. Commun.* **3** 961
[23] Fang X, Wang C, Han Y G, Yin Z Q, Chen W and Han Z F 2016 *Commun. Theor. Phys.* **66** 496
[24] Wang C, Sun S H, Ma X C, Tang G Z and Liang L M 2015 *Phys. Rev. A* **92** 042319
[25] Zhang C M, Zhu J R and Wang Q 2017 *J. Lightwave Technol.* **35** 4574
[26] Yin H L and Fu Y 2019 *Sci. Rep.* **9** 3045
[27] Liu H, Wang J, Ma H and Sun S 2019 *Phys. Rev. Appl* **12** 034039
[28] Li Q, Zhu C, Ma S, Wei K and Pei C 22018 *Int. J. Theor. Phys.* **57** 2192
[29] Liu K, Li J, Zhu J R, Zhang C M and Wang Q 2017 *Chin. Phys. B* **26** 120302
[30] Sekga C and Mafu M 2021 *J. Phys. Commun.* **5** 045008
[31] 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
[32] 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
[33] Wang J, Liu H, Ma H and Sun S 2019 *Phys. Rev. A* **99** 032309
[34] Ribeiro J, Murta G and Wehner S 2018 *Phys. Rev. A* **97** 022307
[35] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504
[36] Renner R 2007 *Nat. Phys.* **3** 645
[37] Lütkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44
[38] Yin H L and Chen Z B 2019 *Sci. Rep.* **9** 17113
[39] Curty M, Xu F, Cui W, Lim C C W, Tamaki K and Lo H K 2014 *Nat. Commun.* **5** 1
[40] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[41] Fung C H F, Ma X and Chau H 2010 *Phys. Rev. A* **81** 012318
[42] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133
[43] Pironio S, Acin A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021
[44] Ma X, Fung C H F and Lo H K 2007 *Phys. Rev. A* **76** 012307
[45] Zhang C M, Zhu J R and Wang Q 2018 *J. Phys. Commun.* **2** 055029
[46] Mafu M, Garapo K and Petruccione F 2013 *Phys. Rev. A* **88** 062306
[47] Mafu M, Garapo K and Petruccione F 2014 *Phys. Rev. A* **90** 032308
[48] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[49] Wei Z, Wang W, Zhang Z, Gao M, Ma Z and Ma X 2013 *Sci. Rep.* **3** 2453
[50] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[51] Renner R 2008 *Int. J. Quantum Inf* **6** 1
[52] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506