Three-party reference frame independent quantum key distribution with an imperfect source

Comfort Sekga[1]* and Mhlambululi Mafu[1]

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

E-mail: *comfort.sekga@gmail.com

Abstract. We propose a reference frame independent quantum key distribution (RFI-QKD), allowing three legitimate parties to share a common secret key without alignment of reference frames in their quantum channels. We relax perfect state preparation assumption by employing loss tolerant technique, making the proposed protocol suitable for practical applications. The results show that the proposed RFI-QKD with an imperfect source is comparable to the RFI-QKD with a perfect source. Moreover, we investigate the impact of reference frame misalignment on the stability of our protocol when the reference frames drift by various misalignment angles. Moreover, we demonstrate that our protocol is not heavily affected by an increase in misalignment of reference frames and it finds immediate applications in quantum networks.

1. Introduction

Quantum key distribution (QKD) provides 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], considerable theoretical and experimental efforts have been accomplished to improve the security and implementation of QKD. However, several challenges remain for QKD to become fully adopted in securing communication. One of the challenges is a requirement for an aligned reference frame between the communicating parties [3]. However, Laing et al. (2010) proposed the reference frame independent (RFI) protocol to address this problem of alignment [4]. Typically, various QKD security proofs assume perfect state preparation. But, in practical implementations, this is impossible due to inherent deficiencies of photon sources. Thus, Tamaki et al. (2014) recently proposed a loss-tolerant protocol that is robust against channel losses due to state preparation flaws and capable of attaining key rates comparable to a protocol that assumes perfect encoding [5]. Considering that this protocol is resource-efficient, we employ the loss tolerant technique in our security proof, which makes the proposed protocol suitable for practical applications.

Against this background, we harness the loss tolerant protocol and derive the security bounds under the imperfect state preparation for the three-party RFI protocol. Also, 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 organise this work according to the following. First, section 2 describes the operation of the proposed protocol, and in section 3, we derive its security bounds. Then, in section 4, we discuss the simulation results and finally, in section 5, we conclude.

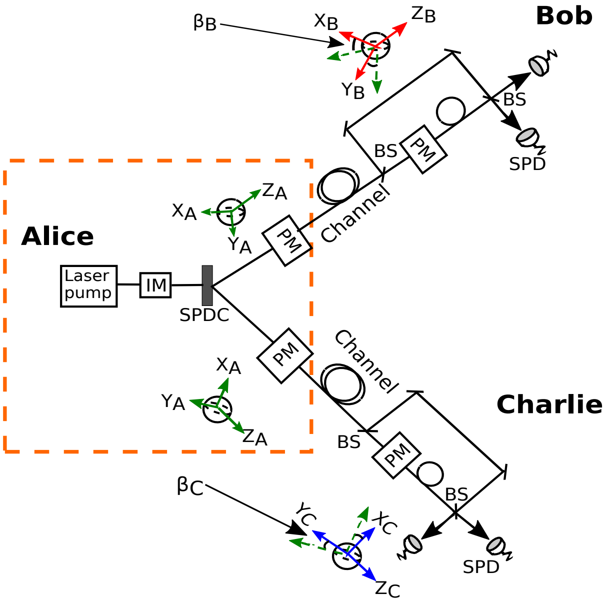


Figure 1: The schematic diagram of the three-party RFI-QKD protocol. Alice starts by preparing two-photon entangled state using an SPDC source. The acronyms IM, BS and SPD, stand for intensity modulator, beam splitter and single-photon detector, respectively.

Spontaneous Parametric Down Conversion

2. Operation of the proposed protocol

Alice starts by preparing a two-photon entangled state using a spontaneous parametric down-conversion source (SPDC). She applies phase modulation in these entangled photons using the same basis chosen from three Pauli encoding bases, X, Y, and Z. The two photons are delivered to Bob and Charlie via insecure quantum channels. Upon receipt of photons, they measure them using any of the three randomly selected measuring bases, $\{X, Y, Z\}$ to guess the

Upper case

Alice preparation basis. Bob and Charlie's measurements are defined by the positive-operator valued measures (POVMs) $\{\hat{M}_{0\beta}, \hat{M}_{1\beta}, \hat{M}_f\}$, where $\hat{M}_{0,\beta}$ $(\hat{M}_{1\beta})$ with $\beta \in \{X, Y, Z\}$ corresponds to obtaining the bit value 0 (1) when Bob and Charlie chooses the basis β and $\hat{M}_f$ represents an inconclusive event and is assumed the same for all bases. In this protocol, Alice, Bob, and Charlie share a common aligned measurement basis $Z_A = Z_B$, $Z_A = Z_C$ while other measurements bases X and Y are allowed to vary by an arbitrary angle β slowly (See Figure 1). Due to drift in reference frames, the measurement bases complementary to the Z basis are given by $X_B = \cos\beta X_A + \sin\beta Y_A$, $X_C = \cos\beta X_A + \sin\beta Y_A$, and $Y_B = \cos\beta Y_A - \sin\beta X_A$, $Y_C = \cos\beta Y_A - \sin\beta X_A$.

We consider the asymmetric basis choice in which the Z basis is chosen with probability $p_z > \frac{1}{2}$ and the complementary bases, $\{X, Y\}$ with probability $p_c = 1 - p_z$ [6]. 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. All the parties announce their basis choices over an authenticated classical channel and proceed with parameter estimation. The raw key is extracted from cases where Alice prepared her states in the Z basis while Bob and Charlie measured their received qubits in the Z direction.

3. Security Analysis

After the sequential transmission and measurement of optical pulses, Alice, Bob, and Charlie possess 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 $E_{ZZZ} = \frac{1 - \langle Z_A Z_B Z_C \rangle}{2}$, 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's measure received states in the Z direction,

Rephrase

respectively. The measurement results in the complementary bases are used to estimate the information that has leaked to Eve. To compute Eve's knowledge on the key, we consider a depolarising channel $E_{ZZ} \leq 15.9\%$ [4]. The bound is given by [7]

$$I_E = (1 - E_{ZZZ})h\left(\frac{1 + u_{\max}}{2}\right) - E_{ZZZ}h\left(\frac{1 + v(u_{\max})}{2}\right) + E_{ZZZ}\log_2 7, \tag{1}$$

where $u_{\max} = \min\left[\frac{1}{1-E_{ZZZ}}\sqrt{C/4}, 1\right]$ and $v(u_{\max}) = \sqrt{\frac{49}{19}\left[C/4 - (1 - E_{ZZZ})^2 u_{\max}^2\right]/E_{ZZZ}}$. The statistical quantity C defined as

$$\begin{aligned} C = {} & \langle X_A X_B X_C \rangle^2 + \langle X_A Y_B X_C \rangle^2 + \langle X_A X_B Y_C \rangle^2 + \langle Y_A X_B X_C \rangle^2 + \langle Y_A Y_B X_C \rangle^2 + \langle Y_A X_B Y_C \rangle^2 \\ & + \langle Y_A Y_B Y_C \rangle^2 + \langle X_A Y_B Y_C \rangle^2, \end{aligned} \tag{2}$$

~~where~~ C is independent of β, $\langle \mathit{\Gamma}_A \mathit{\Gamma}_B \mathit{\Gamma}_C \rangle$ (with $\mathit{\Gamma} \in \{X, Y\}$), corresponds to the expectation that Alice prepares two states in the basis $\mathit{\Gamma}_A$ while Bob and Charlie measure received states in basis $\mathit{\Gamma}_B$ and $\mathit{\Gamma}_C$, respectively. To estimate C, the angle β is assumed to vary slowly in time short enough to allow for the exchange of keys. The expression in 2 can be rewritten as

$$\begin{aligned} C = {} & (1 - 2E_{XXX})^2 + (1 - 2E_{XXY})^2 + (1 - 2E_{XYY})^2 + (1 - 2E_{YXX})^2 + (1 - 2E_{YYX})^2 \\ & + (1 - 2E_{XYX})^2 + (1 - 2E_{YXY})^2 + (1 - 2E_{YYY})^2. \end{aligned} \tag{3}$$

To compute C, we employ a loss tolerant technique which takes into consideration the imperfections in the phase modulation of photons [5]. The actual states that Alice prepares is $|\phi_{0Z}\rangle = |0_Z\rangle$, $|\phi_{1Z}\rangle = \sin\frac{\delta_1}{2}|0_Z\rangle + \cos\frac{\delta_1}{2}|1_Z\rangle$, $|\phi_{0X}\rangle = \cos\left(\frac{\pi}{4} + \frac{\delta_2}{4}\right)|0_Z\rangle + \sin\left(\frac{\pi}{4} + \frac{\delta_2}{4}\right)|1_Z\rangle$, and $|\phi_{0Y}\rangle = \cos\left(\frac{\pi}{4} + \frac{\delta_3}{4}\right)|0_Z\rangle + i\sin\left(\frac{\pi}{4} + \frac{\delta_3}{4}\right)|1_Z\rangle$. These signal states can be written in terms of an identity and Pauli matrices and their density matrix representation is as $\rho_{j\alpha} = |\phi_{j\alpha}\rangle\langle\phi_{j\alpha}| = \frac{1}{2}(\mathbb{1} + \mathbf{n}_X^{j\alpha}\sigma_x + \mathbf{n}_Y^{j\alpha}\sigma_y + \mathbf{n}_Z^{j\alpha}\sigma_z)$, with $\mathbf{n}_\alpha^{j\alpha}$ denoting the coefficients of the Bloch vector of $\rho_{j\alpha}$ where $\alpha \in \{X, Y, Z\}$ and $j \in \{0, 1\}$. From this representation of signal states, one can obtain the joint probability, $Y^\omega j_\alpha; k_\beta m_\beta$ $(\omega \in \{X, Y, Z\})$ that Alice prepares any of the state $|\phi_{j\alpha}\rangle$ while Bob and Charlie measures it in the basis β and obtains a bit value s and t, by exploiting transmission rate of the Pauli operators and subsequently estimate error rates in 3 used for calculating C. Here, we show how to estimate the phase error rate E_{XXX}; other parameters can be obtained similarly. The parameter E_{XXX} is computed by considering a virtual protocol where Alice prepares entangled state $|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|\phi_{0Z}\rangle_{B(C)} + |1\rangle_{A(B)}|\phi_{1Z}\rangle_{B(C)})$, (here B and C denote the systems sent to Bob and Charlie), and then Alice, Bob and Charlie measure their subsystems in the X basis. The error rate is expressed as

Refer to the equation using (3) or Equation 3

Is this refer to the Base ?

$$\begin{aligned} E_{XXX} = {} & \left(Y^{Z,\mathrm{vir}}_{0_X;0_X1_X} + Y^{Z,\mathrm{vir}}_{0_X;1_X1_X} + Y^{Z,\mathrm{vir}}_{1_X;0_X1_X} + Y^{Z,\mathrm{vir}}_{1_X;0_X0_X} + Y^{Z,\mathrm{vir}}_{1_X;1_X0_X} + Y^{Z,\mathrm{vir}}_{0_X;1_X0_X}\right) \\ & \div \left(Y^{Z,\mathrm{vir}}_{0_X;0_X1_X} + Y^{Z,\mathrm{vir}}_{0_X;1_X1_X} + Y^{Z,\mathrm{vir}}_{1_X;0_X1_X} + Y^{Z,\mathrm{vir}}_{1_X;0_X0_X} + Y^{Z,\mathrm{vir}}_{1_X;1_X0_X} + Y^{Z,\mathrm{vir}}_{0_X;1_X0_X} \right. \\ & \left. + Y^{Z,\mathrm{vir}}_{0_X;0_X0_X} + Y^{Z,\mathrm{vir}}_{1_X;1_X1_X}\right) \end{aligned} \tag{4}$$

where $Y^{Z,\mathrm{vir}}_{j_X;k_Xm_X}$ denotes the joint probability that Alice, Bob and Charlie measured $|j_X\rangle$, $|k_X\rangle$ and $|m_X\rangle$, respectively. In this hypothetical protocol, the state of pulses received by Bob (Charlie) can be expressed as $\hat{\sigma}^{\mathrm{vir}}_{B(C);j_X} = \mathrm{Tr}_A[\hat{P}(|j_X\rangle_A)\otimes\mathbb{1}_{B(C)}\hat{P}(|\Psi_Z\rangle_{AB(C)})]$. 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 $\hat{\hat{\sigma}}^{\mathrm{vir}}_{B(C);j_X} = \hat{\sigma}^{\mathrm{vir}}_{B(C);j_X}/\mathrm{Tr}(\hat{\sigma}^{\mathrm{vir}}_{B(C);j_X})$. The joint probability that Alice, Bob and Charlie measures $|j_X\rangle$, $|k_X\rangle$ and $|m_X\rangle$, respectively is given by

$$Y^{Z,\mathrm{vir}}_{j_X;k_Xm_X} = p(j_X)\mathrm{Tr}(\hat{D}_{k_X}\hat{\hat{\sigma}}^{\mathrm{vir}}_{B;j_X})\mathrm{Tr}(\hat{D}_{m_X}\hat{\hat{\sigma}}^{\mathrm{vir}}_{C;j_X}) \tag{5}$$

where $\hat{D}_{k_X(m_X)}$ is the operator that contains Eve's operation and Bob (Charlie)'s POVM measurement and $p(j_X)$ represent the probability that Alice chooses X basis. Since the virtual state $\hat{\sigma}^{\text{vir}}_{B(C);j_X}$ can also be expressed in terms of identity and Pauli operators as $\hat{\sigma}^{\text{vir}}_{B(C);j_X} = \frac{1}{2}\left(\mathbb{1} + \sum_{s(t)=x,y,z} \mathbf{n}^{j_X}_{s(t)} \hat{\sigma}_{s(t)}\right)$. It follows that Equation 5 can be rewritten as $Y^{Z,\text{vir}}_{j_X;k_X m_X} = p(j_X) \sum_{s=X,Y,Z} \mathbf{n}_s q_{k_X|s} \sum_{t=X,Y,Z} \mathbf{n}_t q_{m_X|t}$. Therefore, to obtain $Y^{Z,\text{vir}}_{j_X;k_X m_X}$, it suffices to calculate the transmission rate of Pauli operators defined by $q_{k(m)_X|s(t)} = \text{Tr}(\hat{D}_{k(m)_X} \sigma_{s(t)})/2$ with $s, t \in \{\mathbb{1}, X, Y, Z\}$. The parameters $\mathbf{n}_s$ and $\mathbf{n_t}$ denote the coefficients of Pauli matrices. To evaluate the yield of these states we employ the entanglement description where Alice prepares state $|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle_A |\phi_{0Z}\rangle_{B(C)} + |1_Z\rangle_A |\phi_{1Z}\rangle_{B(C)})$ in the Z basis and likewise the preparation of optical pulses in the complementary bases can be described as a process where Alice generates $|\Phi_X\rangle = |0_X\rangle_A |\phi_{0X}\rangle_{B(C)}$ or $|\Phi_Y\rangle = |0_Y\rangle_A |\phi_{0Y}\rangle_{B(C)}$. By using the same method previously described for the yield of virtual states, we obtain the expression for the yield of actual states as

$$Y^{\omega}_{j_\alpha;k_\beta m_\beta} = p(j_\alpha)\text{Tr}(\hat{D}_{k_\beta} \rho_{j\alpha})\text{Tr}(\hat{D}_{m_\beta} \rho_{j\alpha}) = p(j_\alpha) \sum_{s=X,Y,Z} \mathbf{n}_s q_{k_\beta|s} \sum_{t=X,Y,Z} \mathbf{n}_t q_{m_\beta|t} \tag{6}$$

with $p(j_\alpha)$ denoting probability that Alice measures her subsystems as state j_α. The state $\rho_{j\alpha}$ corresponds to one of the four states defined in Equation 3. The yields of actual states in 6 can be compactly written as

$$\begin{aligned}[Y^Z_{0_Z;k_\beta m_\beta}, Y^Z_{1_Z;k_\beta m_\beta}, Y^X_{0_X;k_\beta m_\beta}, Y^Y_{0_Y;k_\beta m_\beta}]^T =& \frac{1}{64}\mathbf{A}[q_{k_X|\mathbb{1}}, q_{k_X|x}, q_{k_X|y}, q_{k_X|z}]^T \\ & \mathbf{A}[q_{m_X|\mathbb{1}}, q_{m_X|x}, q_{m_X|y}, q_{m_X|z}]^T\end{aligned} \tag{7}$$

where $\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & \sin(2\delta_1) & 0 & -\cos(2\delta_1) \\ 1 & \cos(2\Theta_2) & 0 & \sin(2\Theta_2) \\ 1 & \sin(2\Theta_3) & 0 & 0 \end{bmatrix}$. Here, $\Theta_2 = \frac{\pi}{4} + \frac{\delta_2}{2}$ and $\Theta_3 = \frac{3\pi}{4} + \frac{\delta_3}{2}$. The same logic can be applied to determine the yield of virtual states in terms of transmission rate as follows

$$[Y^{Z,\text{vir}}_{0_X;k_X m_X}, Y^{Z,\text{vir}}_{1_X;k_X m_X}]^T = \frac{1}{48}\mathbf{B}[q_{k_X|\mathbb{1}}, q_{k_X|x}, q_{k_X|y}, q_{k_X|z}]^T \mathbf{C}[q_{k_X|\mathbb{1}}, q_{k_X|x}, q_{k_X|y}, q_{k_X|z}]^T \tag{8}$$

where

Seems that this part need to be clarified. Please see the comment at the end of the manuscript (Comment 1)

$$\mathbf{B} = \mathbf{C} = \begin{bmatrix} (1 + \sin\delta_1) & \sin\delta_1(1 + \sin\delta_1) & \cos\delta_1(1 + \sin\delta_1) & 0 \\ (1 - \sin\delta_1) & -\sin\delta_1(1 - \sin\delta_1) & -\cos\delta_1(1 - \sin\delta_1) & 0 \end{bmatrix}. \tag{9}$$

By combining the results of Equations 7 and 8 we can deduce the yield of virtual states and subsequently obtain the expression for error rate E_{XXX}.

4. Estimation of key rate

The key generation rate for our proposed RFI QKD protocol is given by

$$r = Q^{\mu,1}_{ZZZ}(1 - I^U_E) - f_{EC} Q^{\mu}_{ZZZ} h(E^{\mu}_{ZZZ}). \tag{10}$$

To estimate the above parameters, we consider the channel model proposed in [7], where the yield of actual states is expressed as

$$\begin{aligned} Y^{\omega}_{j_\alpha;k_\beta m_\beta} =& \sum_{n=0}^{\infty} p(n|\gamma) \sum_{i=0}^{n} C^n_i (\eta_B t)^i (1 - \eta_B t)^{n-i} (\langle \phi_{k\beta} | \phi_{j\alpha} \rangle)^2 \chi(n) \sum_{n=0}^{\infty} p(n|\gamma) \sum_{i=0}^{n} C^n_i (\eta_C t)^i \\ & \times (1 - \eta_C t)^{n-i} (\langle \phi_{m\beta} | \phi_{j\alpha} \rangle)^2 \chi(n), \end{aligned} \tag{11}$$

where $\chi(n) = \begin{cases} 1 - Y_0 & \text{if } n > 0 \\ Y_0(1 - Y_0) & \text{if } n = 0 \end{cases}$ and $C_i^n = n!/[i!(1-i)!]$ is the binomial coefficient. The term $p(n|\gamma) = (n+1)(\frac{\gamma}{2})^n/(1+\frac{\gamma}{2})^{n+2}$ denotes probability that the source emits n-photon pulse when modulated with intensity γ. The parameter $\eta_{B(C)}$ represents efficiency of Bob (Charlie)'s detection system and t denotes the total transmittance of the quantum channel. Y_0 corresponds to the background count rate. According to the decoy-state theory, the overall gain is [8]

$$\begin{aligned} Q^{\omega,\gamma}_{j_\alpha;k_\beta m_\beta} = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!}\mathrm{e}^{-\mu} = \frac{1}{2}\Big\{ & \big[1 + (1-e_d)[e^{(-\eta_B t + a\eta_B t)\gamma} - e^{-a\eta B\gamma t} - (1-e_d)e^{\eta_B\gamma t}]\big] \\ & \times \big[1 + (1-e_d)[e^{(-\eta_C t + b\eta_C t)\gamma} - e^{-b\eta_C\gamma t} - (1-e_d)e^{\eta_C\gamma t}]\big]\Big\}, \end{aligned} \tag{12}$$

where $a = (\langle\phi_{k\beta}|\phi_{j\alpha}\rangle)^2$, $b = (\langle\phi_{m\beta}|\phi_{j\alpha}\rangle)^2$ and e_d corresponds to the erroneous detection. Additionally, the overall gain in the Z basis is expressed as

$$\begin{aligned} Q^{\mu}_{ZZZ} =& (Q^{Z,\mu}_{0Z;0Z0Z} + Q^{Z,\mu}_{0Z;0Z1Z} + Q^{Z,\mu}_{0Z;1Z0Z} + Q^{Z,\mu}_{0Z;1Z1Z} + Q^{Z,\mu}_{1Z;0Z0Z} + Q^{Z,\mu}_{1Z;0Z1Z} + Q^{Z,\mu}_{1Z;1Z0Z} \\ & + Q^{Z,\mu}_{1Z;1Z1Z}) \end{aligned} \tag{13}$$

and the corresponding quantum bit error rate is $E^{\mu}_{ZZZ} = (+Q^{Z,\mu}_{0Z;0Z1Z} + Q^{Z,\mu}_{0Z;1Z0Z} + Q^{Z,\mu}_{0Z;1Z1Z} + Q^{Z,\mu}_{1Z;0Z0Z} + Q^{Z,\mu}_{1Z;0Z1Z} + Q^{Z,\mu}_{1Z;1Z0Z})/Q_{ZZZ}$. The gain for single photon components in the Z basis is expressed as $Q^{\mu,1}_{ZZZ} = \mu e^{-\mu}(Y^{Z,1}_{0Z;0Z0Z} + Y^{Z,1}_{0Z;0Z1Z} + Y^{Z,1}_{0Z;1Z0Z} + Y^{Z,1}_{0Z;1Z1Z} + Y^{Z,1}_{1Z;0Z0Z} + Y^{Z,1}_{1Z;0Z1Z} + Y^{Z,1}_{1Z;1Z0Z} + Y^{Z,1}_{1Z;1Z1Z})$. The parameter I^U_E is estimated from value of C and upper bound on the error rate, $E^{1,U}_{ZZZ}$ from single-photon contributions as shown in Equation 1. The parameter $E^{1,U}_{ZZZ}$ is estimated from the yield of single photons as follows

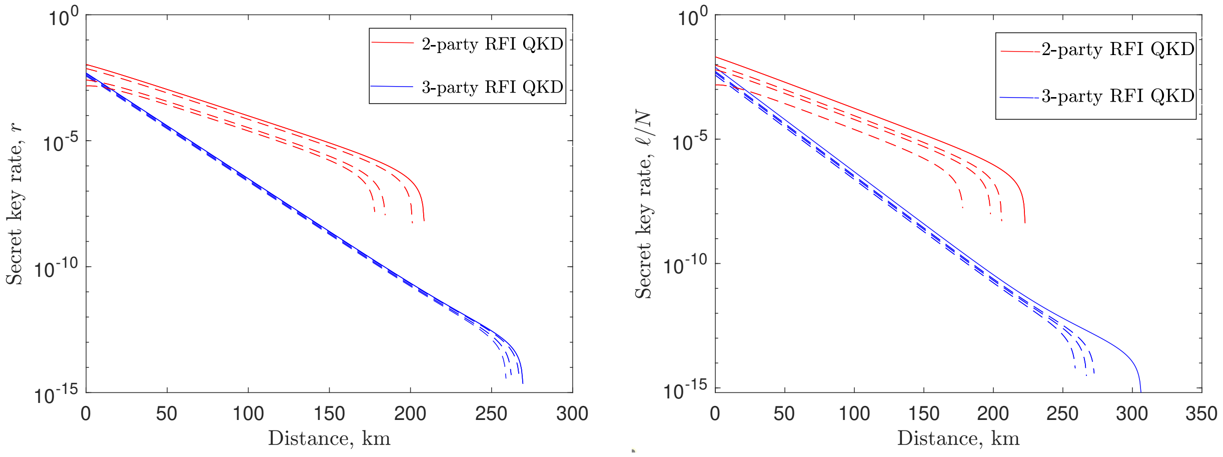
$$\begin{aligned} E^{1,U}_{ZZZ} = \Big(E^{\mu}_{ZZZ}Q^{\mu}_{ZZZ} - e_0 Y_0 \mathrm{e}^{-\mu}\Big) \div \Big(\mathrm{e}^{-\mu}\big(& Y^{1,L}_{0Z;0Z0Z} + Y^{1,L}_{0Z;0Z1Z} + Y^{1,L}_{0Z;1Z0Z} + Y^{1,L}_{0Z;1Z1Z} \\ & + Y^{1,L}_{1Z;0Z0Z} + Y^{1,L}_{1Z;0Z1Z} + Y^{1,L}_{1Z;1Z0Z} + Y^{1,L}_{1Z;1Z1Z}\big)\Big), \end{aligned} \tag{14}$$

where $Y^{1,L}_{j_\alpha;k_\beta m_\beta} = \frac{\mu}{\mu\nu - \nu^2}\Big[Q^{\nu}_{j_\alpha;k_\beta m_\beta}\mathrm{e}^{\nu} - Q^{\mu}_{j_\alpha;k_\beta m_\beta}\frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2}Q_0\Big]$. 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.

5. Simulation results

We simulate the performance of the proposed protocol on a fiber-based QKD system model. The plots in Figure 2a were obtained with $\delta = 0.35$, $\delta = 0.20$ and $\delta = 0.10$, which correspond to deviation of 20.05°, 11.46° and 5.73° from the desired phase angle, respectively. For comparison, we plotted the curve for $\delta = 0$, which corresponds to a perfect encoding scenario. The characterization of parameter δ is based on its relation to the extinction ratio according to the definition; $|\tan(\delta/2)|^2 = \eta_{ex}$ [10]. 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 to estimate encoding imperfection to demonstrate the robustness of our proposed protocol against source flaws. The results demonstrate that the key rates achieved are comparable to the perfect encoding scenario despite increased encoding flaws. In Figure 2b, we simulate the secret key rate for three-party RFI protocol as a function of transmission distance for fixed misalignment degree $\beta = 0, \pi/5, \pi/6$ and $\pi/7$. Despite the increase in misalignment of reference frames, the achievable key rates are comparable to when there is no misalignment in reference frames (when $\beta = 0$). Also, we simulate the key rate for the two-party RFI protocol (red lines) for the same parameters in Figure 2a and Figure 2b. It is evident from both figures that the two-party RFI protocol outperforms our proposed three-party RFI protocol in terms of achievable secret key rate for

Just a simple suggestion. (The Author can omit the suggestion)
I suggest to change the way on how the parameter Beta changes. For example can be done by an arrow or any other form to avoid to say "*From the left to the right*".



(a)

(b)

Figure 2: Comparison of our protocol with the two-party RFI protocol, (red lines). (a) Expected secret key rate (in logarithmic scale) for the proposed protocol (blue lines) as a function of distance measured in km, for the fixed encoding source flaws δ. From left to right, the curves represent $\delta = 0.35$, $\delta = 0.20$, $\delta = 0.10$ and $\delta = 0$ (blue solid line). The relative rotation of reference frames is set at $\beta = \pi/5$. (b) Expected secret key rate for the proposed protocol (blue lines) as a function of distance measured in km, for the fixed misalignment degree β. From left to right, the curves represent $\beta = \pi/5$, $\beta = \pi/6$, $\beta = \pi/7$ and $\beta = 0$ (blue solid line). The encoding source flaws are fixed at $\delta = 0.10$, dark counts rate, $P_d = 1.7 \times 10^{-6}$, loss channel coefficient=0.2 km/dB, detection efficiency $\eta = 14.5\%$, error correction efficiency, $f_{EC} = 1.22$ and expected photon number for signal states, $\mu = 0.6$, and optimal probability, $p_z = 0.95$ [9].

different encoding source flaws and misalignment degrees of β. Nevertheless, our proposed 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 party.

Rephrase

6. Conclusion

We presented a three-party RFI QKD protocol to be implemented without alignment between the parties. We investigated the performance of our proposed protocol for encoding flaws and despite the state preparation flaws, the key rates achieved are comparable to those of perfect encoding scenarios. Furthermore, we simulated the secret key rate for the proposed 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. We demonstrated that our protocol is affected only moderately by an increase in misalignment of reference frames.

Rephrase

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74**(1) 145–195
[2] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7–11
[3] Wabnig J, Bitauld D, Li H, Laing A, O'Brien J and Niskanen A 2013 *New J. Phys.* **15** 073001
[4] Laing A, Scarani V, Rarity J and O'Brien J 2010 *Physical Review A* **82** 012304
[5] Tamaki K, Curty M, Kato G, Lo H K and Azuma K 2014 *Physical Review A* **90** 052314
[6] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133–165
[7] Sekga C and Mafu M 2021 *Chinese Physics B*
[8] Lo H K, Ma X and Chen K 2005 *Physical Review Letters* **94** 230504
[9] Wei Z, Wang W, Zhang Z, Gao M, Ma Z and Ma X 2013 *Sci. Rep.* **3** 2453
[10] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Physical Review A* **85** 042307

Personally I have the problem to accept the manuscript as it is. The reason is due to the Equation (9)
For my understanding B and C are two matrices (2x4) multiplied by a transposed row vector (1,4). The multiplication Gives a matrix (4x1) and multiplied by a matrix (4x1).
If the error is not present, the author may need to be more clear on the highlighted part, or need to re-evaluate the simulation.