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 aligning reference frames in their quantum channels. Furthermore, we relax the perfect state preparation assumption by employing a 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. Also, 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, 2]. Since the inception of the primitive BB84 protocol [3], 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 in the practical implementation of QKD is a requirement for an aligned reference frame between the communicating parties [4, 5, 6]. 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 [7]. 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 [8]. Furthermore, considering that this protocol is resource-efficient, we employ the loss tolerant technique in our security proof, making 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.

2. Operation of the proposed protocol

State preparation

In each run i, Alice prepares a two-photon entangled state using a Spontaneous Parametric Down Conversion source (SPDC). She then randomly selects the basis $a_i \in \{X, Y, Z\}$ with

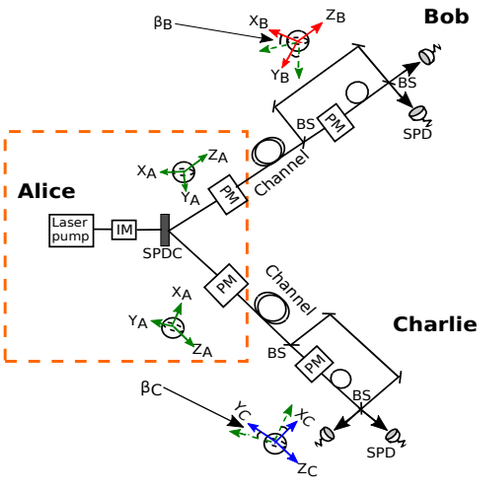

Figure 1: The schematic diagram of the three-party RFI-QKD protocol. Alice starts by preparing a two-photon entangled state using an SPDC source. The acronyms IM, BS and SPD stand for intensity modulators, beam splitter, and single-photon detectors.

probabilities p_z and $p_c = 1 - p_z$, respectively. Here, Z basis is chosen with probability $p_z > \frac{1}{2}$ and the complementary bases, $\{X, Y\}$ with probability $p_c = 1-p_z$. She applies phase modulation $\theta_A \in \{0, \frac{\pi}{2}\}$, $\theta_A \in \{\frac{\pi}{4}, \frac{3\pi}{4}\}$ and $\theta_A \in \{\pi, \frac{3\pi}{2}\}$ when she selects the Z, X and Y basis, respectively. Here the phase values $\theta_A \in \{0, \frac{\pi}{4}, \pi\}$ and $\theta_A \in \{\frac{\pi}{2}, \frac{3\pi}{4}, \frac{3\pi}{2}\}$ are assigned bit values $r_i = 0$ and $r_i = 1$, respectively. Note that for each run i, Alice performs the same phase shift to both entangled photons, i.e., both photons are prepared in the same state, therefore she keeps one bit value r_i corresponding to that state. The two photons are delivered to Bob and Charlie via insecure quantum channels.

Measurement

Upon receipt of photons, Bob and Charlie measure them using the basis $b_i \in \{X, Y, Z\}$ and $c_i \in \{X, Y, Z\}$, respectively, with probabilities p_z and p_c. They choose uniform random bits $r_i' \in \{0, 1, \emptyset\}$ and $r_i'' \in \{0, 1\,\emptyset\}$ to store their outcomes. Here the symbol $\emptyset$ corresponds to inconclusive result 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 $Y_B = \cos\beta Y_A - \sin\beta X_A$, $Y_C = \cos\beta Y_A - \sin\beta X_A$.

Sifting

Alice, Bob and Charlie publish their basis choices over an authenticated classical channel. We define the set $\mathcal{Z} := \{i : a_i = b_i = c_i, r_i' \neq \emptyset, r_i'' \neq \emptyset\}$. The first steps are repeated as long as $|\mathcal{Z}| < n$. Here n corresponds to the required number of bit strings to form a raw key. 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 prepared two states in the Z basis while Z_B and Z_C denote that Bob and Charlie's 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. To compute Eve's knowledge on the key, we consider a depolarising channel

where $E_{ZZ} \leq 15.9\%$ [4]. The bound is given by [6]

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

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

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

C is independent of β, $\langle \Gamma_A \Gamma_B \Gamma_C\rangle$ (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. 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 Equation 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 [8]. The actual states that Alice prepares are $|\phi_{0Z}\rangle = |0_Z\rangle$, $|\phi_{1Z}\rangle = \sin\frac{\delta_1}{2}|0_Z\rangle + \cos\frac{\delta_1}{2}|1_Z\rangle$, $|\phi_{0X}\rangle = \cos\left(\frac{\pi}{4} + \frac{\delta_2}{4}\right)|0_Z\rangle + \sin\left(\frac{\pi}{4} + \frac{\delta_2}{4}\right)|1_Z\rangle$, 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 given by $\rho_{j\alpha} = |\phi_{j\alpha}\rangle\langle\phi_{j\alpha}| = \frac{1}{2}(\mathbb{1} + \mathbf{n}_X^{j\alpha}\sigma_x + \mathbf{n}_Y^{j\alpha}\sigma_y + \mathbf{n}_Z^{j\alpha}\sigma_z)$. Here $\mathbf{n}_\alpha^{j\alpha}$ denotes the coefficient 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 states $|\phi_{j\alpha}\rangle$ while Bob and Charlie measure them in the basis β and obtain bit values s and t. This can be realized through exploitation of transmission rate of the Pauli operators. Subsequently the joint probability, $Y^\omega j_\alpha; k_\beta m_\beta$ can be used to estimate error rates in Equation 3 in order to obtain the value of 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 $|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|\phi_{0Z}\rangle_{B(C)} + |1\rangle_{A(B)}|\phi_{1Z}\rangle_{B(C)})$, ($B$ and C denote the subsystems sent to Bob and Charlie), and then Alice, Bob and Charlie measure their subsystems in the X basis. The error rate is expressed as

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

where $Y_{j_X;k_Xm_X}^{Z,\text{vir}}$ 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 $\hat{\sigma}_{B(C);j_X}^{\text{vir}} = \text{Tr}_A[\hat{P}(|j_X\rangle_A)\otimes\mathbb{1}_{B(C)}\hat{P}(|\Psi_Z\rangle_{AB(C)})]$. 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 $\hat{\tilde{\sigma}}_{B(C);j_X}^{\text{vir}} = \hat{\sigma}_{B(C);j_X}^{\text{vir}}/\text{Tr}(\hat{\sigma}_{B(C);j_X}^{\text{vir}})$. The joint probability that Alice, Bob and Charlie measure $|j_X\rangle$, $|k_X\rangle$ and $|m_X\rangle$, respectively is given by

$$\begin{aligned} Y_{j_X;k_Xm_X}^{Z,\text{vir}} &= p(j_X)\text{Tr}(\hat{D}_{k_X}\hat{\tilde{\sigma}}_{B;j_X}^{\text{vir}})\text{Tr}(\hat{D}_{m_X}\hat{\tilde{\sigma}}_{C;j_X}^{\text{vir}}) \\ &= p(j_X)Y_{j_X;k_X}^{Z,\text{vir}}Y_{j_X;m_X}^{Z,\text{vir}} \end{aligned} \tag{5}$$

where $\hat{D}_{k_X(m_X)}$ is the operator that contains Eve's operation and Bob (Charlie)'s POVM measurement, $p(j_X)$ represents the probability that Alice chooses X basis and $Y^{Z,\text{vir}}_{j_X;k_X(m_X)}$ denotes yields of the states sent to Bob (Charlie). Since the virtual state $\hat{\sigma}^{\text{vir}}_{B(C);j_X}$ can also be expressed in terms of identity and Pauli operators as $\hat{\sigma}^{\text{vir}}_{B(C);j_X} = \frac{1}{2}\Big(\mathbb{1} + \sum_{s(t)=x,y,z} \mathbf{n}^{j_X}_{s(t)}\hat{\sigma}_{s(t)}\Big)$, 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 parameter $\mathbf{n}_{s(t)}$ denotes the coefficient 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

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

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 parameters $Y^{\omega}_{j_\alpha;k_\beta}$ and $Y^{\omega}_{j_\alpha;m_\beta}$ correspond to the yields of states sent to Bob and Charlie, respectively. We consider the cases where Bob (Charlie) measured the states sent by Alice in the X basis to determine the transmission rate of Pauli operators as follows

$$[Y^{Z}_{0_Z;k_X(m_X)}, Y^{Z}_{1_Z;k_X(m_X)}, Y^{X}_{0_X;k_X(m_X)}, Y^{Y}_{0_Y;k_X(m_X)}]^T = \frac{1}{64}\mathbf{A}[q_{k_X(m_X)|\mathbb{1}}, q_{k_X(m_X)|x}, q_{k_X(m_X)|y}, q_{k_X(m_X)|z}]^T \tag{7}$$

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

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

where

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

By combining the results of Equations 7 and 8 we can deduce the yield of virtual states sent to Bob and Charlie. The results can then be used to obtain the virtual yield in Equation 5 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 [6], 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 [9]

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

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

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

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

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

where $Y_{j_\alpha;k_\beta m_\beta}^{1,L} = \frac{\mu}{\mu\nu - \nu^2}\Big[Q_{j_\alpha;k_\beta m_\beta}^{\nu} \mathrm{e}^{\nu} - Q_{j_\alpha;k_\beta m_\beta}^{\mu} \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Q_0\Big]$. The values $Q_{j_\alpha;k_\beta m_\beta}^{\mu}$, $Q_{j_\alpha;k_\beta m_\beta}^{\nu}$ are gains obtained on conditional probabilities that Alice prepares the state j_α, while Bob and Charlie measure the states k_α, m_β, and 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; $|\tan(\delta/2)|^2 = \eta_{ex}$ [11]. The non-zero extinction ratio is mainly due to imperfections in phase modulators and is of order 10^{-3} in typical experiments. 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 different encoding source flaws and misalignment degrees of β. Nevertheless, our proposed protocol is more resourceful for secure communication tasks involving multiple parties since a secret key for each party is generated

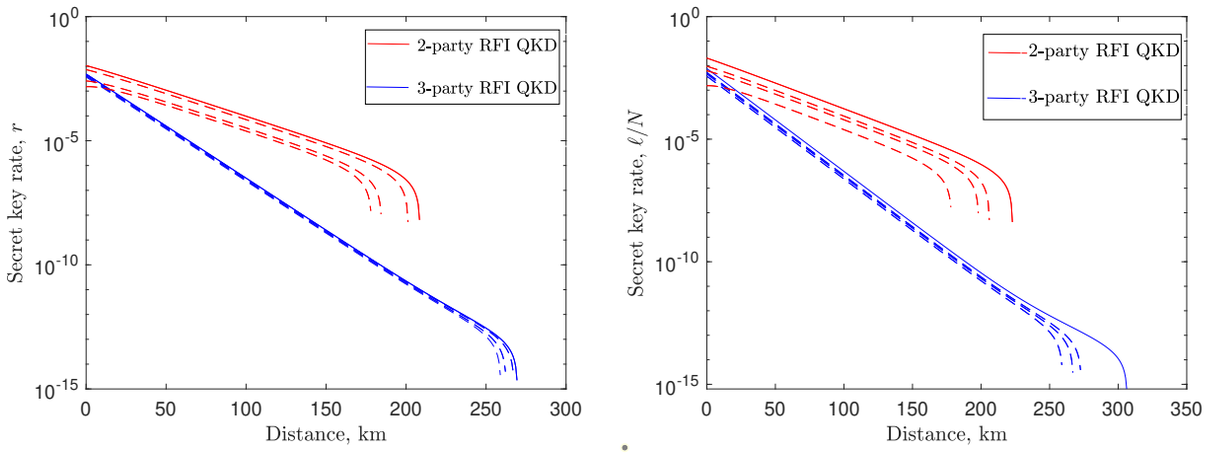

Figure 2: Comparison of our protocol with the two-party RFI protocol, (red lines). (a) Expected secret key rate (in logarithmic scale) for the proposed protocol (blue lines) as a function of distance measured in km, for the fixed encoding source flaws δ. From left to right, the curves represent $\delta = 0.35$, $\delta = 0.20$, $\delta = 0.10$ 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, $p_z = 0.95$ [10].

from a single execution of the protocol. On the contrary, if the two-party QKD protocol is employed in a multiparty communication scenario, multiple protocols need to be performed to establish a secret key for each party.

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 performed a simulation for the variation of the secret key rate concerning transmission distance for different misalignment degrees ($\beta = \pi/6, \pi/8$) to investigate the impact of the shift in the reference frames 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.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74**(1) 145–195
[2] Mafu M 2013 *Security in quantum key distribution protocols* Ph.D. thesis
[3] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7–11
[4] Laing A, Scarani V, Rarity J and O'Brien J 2010 *Physical Review A* **82** 012304
[5] Sekga C and Mafu M 2021 *Journal of Physics Communications* **5** 045008
[6] Sekga C and Mafu M 2021 *Chinese Physics B* **30** 120301
[7] Mafu M, Sekga C and Senekane M 2021 *Scientific African* e01008
[8] Tamaki K, Curty M, Kato G, Lo H K and Azuma K 2014 *Physical Review A* **90** 052314
[9] Lo H K, Ma X and Chen K 2005 *Physical Review Letters* **94** 230504
[10] Wei Z, Wang W, Zhang Z, Gao M, Ma Z and Ma X 2013 *Sci. Rep.* **3** 2453
[11] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Physical Review A* **85** 042307