# Security Analysis for the Rio Quantum Network

**Mario C. Ribeiro**$^1$**, Raul O. Vallejos**$^1$**, Guilherme Temporão** $^2$**,**
**Antônio Z. Khoury**$^3$**, Fernando de Melo** $^1$

$^1$ Centro Brasileiro de Pesquisas Físicas (CBPF)
Rio de Janeiro – RJ – Brazil

$^2$Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)
Rio de Janeiro – RJ – Brazil

$^3$Universidade Federal Fluminense (UFF)
Niterói – RJ – Brazil

mcurvo@cbpf.br, vallejos@cbpf.br, temporao@puc-rio.br, azkhoury@id.uff.br

***Abstract.*** *The Rio Quantum Network (RQN) is a multi-user quantum communication network connecting several research institutions across the city of Rio de Janeiro. Capitalizing on its ring topology, the network implements a Sagnac-based variant of Twin-Field Quantum Key Distribution (TF-QKD)—a protocol that falls under the broader class of Measurement-Device Independent QKD (MDI-QKD). This design eliminates the need to trust the measurement devices, enhancing security against potential vulnerabilities. In the RQN, instead of each user operating a quantum light source in their lab, they perform phase and amplitude modulations on signals distributed by a central node. In this contribution, we employ the security framework of TF-QKD to estimate the secret key rate, ensuring rigorous performance evaluation under realistic conditions.*

## 1. Introduction

The Rio Quantum Network (RQN) consists of the deployment of a metropolitan quantum communication network between PUC-Rio, CBPF, UFRJ, IME and UFF. While the communication among PUC-Rio, CBPF, UFRJ and IME is through optical fibers, it also comprises free-space optical links between CBPF and UFF, and also between CBPF and IME. As its first step, the network will be used to implement a quantum key distribution (QKD) protocol among its users. Given the intrinsic challenges of a metropolitan implementation, the chosen protocol was the so-called Twin-Field QKD [Lucamarini et al. 2018, Curty et al. 2019], as it has been shown to be reliable even in high loss scenarios.

Following the works of [Zhong et al. 2022], the use of a Sagnac Interferometer based TF-QKD protocol seemed best suited for the RQN. First and foremost, Sagnac interferometers have inherent phase stability, meaning that any two users sharing the same laser source remain phase-locked. Second, a Sagnac based TF-QKD protocol has high tolerance for channel asymmetry due to the signal having a common traveling path. Finally, as opposed to most QKD protocols, the users do not need to have their own light sources and detectors, significantly reducing the costs and facilitating the possible addition of any new users to the network.

## 2. Ideal Scenario and BB84 Equivalence

An untrusted central node, Charlie, is located outside the loop and is in possession of a light source and photon detectors. He is responsible for preparing and sending a signal through the network, as well as performing measurements upon the signal's return. In order to encode bits to be exchanged through the network, Alice and Bob will apply phase shifts to the signal. Such phases will then affect the interference pattern and Charlie's measurement's results, as shown in Figure 1. When assuming single-photon emissions, the step-by-step protocol is described as follows.

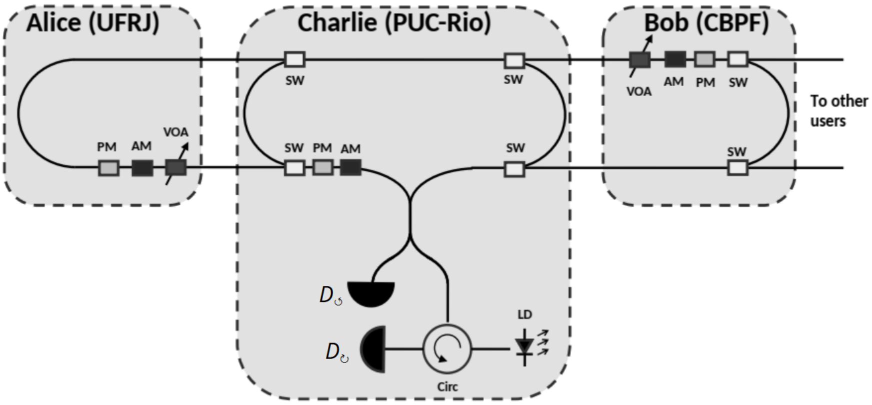

**Figure 1. Two-parties QKD in Rio Quantum Network using a Sagnac-based topology: experimental setup. Charlie prepares an optical signal and sends it to the network. A 50:50 BS acts on the signal creating a uniform superposition between the clockwise and anti-clockwise modes. Alice and Bob independently apply a phase shift on the anti-clockwise mode randomly sampling the phase value from four possible settings. The signal then goes back to Charlie's lab, where it interferes back at the BS, and it is followed by two detectors $D_{\circlearrowright}$ and $D_{\circlearrowleft}$. The relay announces detection results $k_{\circlearrowright}$ and $k_{\circlearrowleft}$. The parties keep the rounds in which they choose the same basis and $k_{\circlearrowright} \oplus k_{\circlearrowleft} = 1$, all the other rounds are discarded. The network has optical switches that can be used to allow other users to communicate.**

*Ideal Protocol.* $(i)$: In each round, the central node, Charlie, prepares a state $|\psi\rangle = \frac{1}{\sqrt{2}}(|\circlearrowright\rangle + |\circlearrowleft\rangle)$ by sending photon through a 50:50 Beam Splitter. Alice and Bob will act on the counter-clockwise mode of the signal by independently and randomly choosing between two different phases within two different sets and applying it to the signal. Each set corresponds to a choice of basis, and each phase is associated with a bit value. See table 1 for details.

**Table 1. Bit encoding: Possible phase values and their respective sets.**

| bit | Z set | Y set |
|---|---|---|
| 0 | 0 | $\pi/2$ |
| 1 | $\pi$ | $3\pi/2$ |

$(ii)$: The signal returns to Charlie's lab and goes back through the BS followed by threshold detectors labeled $D_{\circlearrowright}$ and $D_{\circlearrowleft}$. Just before detection, the state reads:

$$|\psi\rangle_C = \frac{1}{2}[(1 + e^{i(\phi_A+\phi_B)})\,|\circlearrowright\rangle + (1 - e^{i(\phi_A+\phi_B)})\,|\circlearrowleft\rangle]. \tag{1}$$

Charlie performs a measurement and records the outcomes $k_{\circlearrowright}$ and $k_{\circlearrowleft}$ where $k_{\circlearrowright(\circlearrowleft)} = 0$ corresponds to a no-click event and $k_{\circlearrowright(\circlearrowleft)} = 1$ corresponds to a click event. This step is repeated until they complete a predetermined $M$ number of rounds. Since there was a bit value associated with each possible phase applied by Alice and Bob, they each hold now a bit string of length $M$.

$(iii)$: Alice and Bob publicly announce which set they chose in each round, and discard the bits for rounds in which they chose different sets. The relay publicly announces the outcome of his measurements for each round. After this step, Alice and Bob should each have a bit string of length $\approx M/2$.

$(iv)$: Alice and Bob publicly share a random subset of their bit strings, $S \subset M$, and compare them bit-by-bit. They used this data to evaluate the quantum bit error rates (QBERs) for each choice of set, $E_Z$ and $E_Y$.

$(v)$: Alice and Bob can then proceed with the usual post-processing of the remaining strings: they perform error correction and privacy amplification protocols of their choice.

We can see from Eq.(1) that the probability of Charlie obtaining a particular outcome depends on the phase applied by the parties. If they apply phases from different sets, each detector in Charlie's lab will have a 50% chance of clicking, and this is why those rounds are not used for key generation. In case they choose phases from the same set, the sum of the phases will determine which detector is going to click. The only information available to an eavesdropper (Eve) is thus the sum of phases applied on the signal, even if she is in control of the measurement devices. However, since Alice knows which phase she applied in each round, as well as the detection result (i.e. the sum of phases), she automatically knows which phase Bob applied and vice-versa (as long as they chose the same set). Thus, they communicate to each other their bit value in each successful round.

In order to establish the protocol security, and to estimate its key rate, we introduce the so-called "virtual" scenario, where Alice and Bob each hold a "virtual" qubit in their labs. By doing so, we are able to trace an equivalence to the well-known entanglement-based BB84 protocol, and, in the asymptotic scenario, employ the Devetak-Winter key rate expression [Devetak and Winter 2005] for our protocol. Say Alice and Bob each have a virtual qubit in their labs that they can perform measurements on. Instead of randomly selecting a phase and applying it to the signal, they will instead correlate their qubit with the signal by performing a conditional unitary operation on the joint state $|\psi\rangle_{CAB} = \frac{1}{\sqrt{2}}(|\circlearrowright\rangle+|\circlearrowleft\rangle)_C \otimes \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_A \otimes \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_B$. Here, $|0\rangle_{A(B)}$ and $|1\rangle_{A(B)}$ denote Alice's (Bob's) qubit state in the $Z$ basis. The unitary is $U_A = (\mathbb{I}_C \otimes |0\rangle\langle 0|_A + Z_C \otimes |1\rangle\langle 1|_A) \otimes \mathbb{I}_B$ for Alice and $U_B = \mathbb{I}_A \otimes (\mathbb{I}_C \otimes |0\rangle\langle 0|_B + Z_C \otimes |1\rangle\langle 1|_B)$ for Bob, where $Z$ is the usual Pauli matrix and $\mathbb{I}$ is the identity operator. Note that, after the application of the unitary operations, performing measurements on the qubit on the $Z$ or $Y$ basis introduces the corresponding phase onto the signal. As the measurement on the qubits commutes with the interferometer propagation, such measurements can be postponed. In this scenario, after the final BS, the state before measurement reads:

$$|\psi\rangle_{final} = \Big(\frac{|00\rangle_{AB} + |11\rangle_{AB}}{2}\Big)\,|\circlearrowright\rangle_C + \Big(\frac{|01\rangle_{AB} + |10\rangle_{AB}}{2}\Big)\,|\circlearrowleft\rangle_C\,. \tag{2}$$

From the above expression it is then clear that independently of the relays measurement outcome, Alice and Bob will share a maximally entangled state. As such, they will be able to implement a entanglement-based BB84 protocol. This establishes the formal correspondence between the ideal protocol being implemented in the RQN, and the entanglement-based BB84. Now, we can consider the secret key rate for the BB84 protocol [Renner 2008] as the secret key rate to be used in the RQN protocol:

$$r_{ideal} = p_{\text{click}}(1 - h(E_Z) - h(E_Y)), \tag{3}$$

where $E_Z$ and $E_Y$ are the QBERs in the Z and Y basis respectively and $p_{\text{click}}$ is the probability of a successful detection event, which in the ideal scenario is simply given by the transmittance of the network, $\eta$. In the RQN case, the QBERs are:

$$E_Z = p_{ZZ}[b_a \neq b_b \oplus k_{\circlearrowleft} | k_{\circlearrowright} \oplus k_{\circlearrowleft} = 1], \tag{4}$$

$$E_Y = p_{YY}[b_a \neq b_b \oplus k_{\circlearrowleft} | k_{\circlearrowright} \oplus k_{\circlearrowleft} = 1]. \tag{5}$$

Note that only the rounds where $k_{\circlearrowright} \oplus k_{\circlearrowleft} = 1$ (only one detector clicked) are considered for the protocol, since any other case can only happen due to multiple photons being sent or dark counts. When using single photon sources, the protocol's security analysis ends here. One can observe the measurement results and easily estimate the QBERs on step $(iii)$, and therefore calculate the secret key rate for the protocol.

## 3. Practical Protocol: The Rio Quantum Network implementation

In practice, high-rate reliable single photon sources are not available. To overcome this, in our implementation, Charlie uses an attenuated LASER source, whose state is fairly described by a coherent state $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$, with mean photon number $|\alpha|^2 \ll 1$. By doing so, Charlie inputs into the network weak coherent pulses (WCP), with Alice and Bob performing phase shifts in a similar manner as the single-photon case. To avoid attacks that rely on multi-photon signals, we employ the standard decoy states strategy [Lo et al. 2005]. Here, when they choose the $Z$-set, the protocol remains the same, however, when the $Y$-set is chosen, Alice (Bob) will independently introduce a random phase $\Phi_{A(B)}$ with $0 \leq \Phi_{A(B)} \leq 2\pi$ and modulate the amplitude with intensities $\mu_i$ ($\nu_j$) drawn from a set $\{\mu_i\}$ ($\{\nu_j\}$). Only the $Z$-set rounds are used for key generation, while the $Y$-set rounds are used for parameter estimation. Additionally, in step $(iv)$ of the protocol, Alice and Bob also publicly disclose their amplitude settings for each round.

### 3.1. Secret Key Rate

The secret key rate for the ideal protocol, Eq.(3), is now changed to:

$$r_{RQN} \geq r_{RQN}^{1,0} + r_{RQN}^{0,1} \tag{6}$$

where $r_{RQN}^{k_{\circlearrowright},k_{\circlearrowleft}}$ is the key rate resulting of a detection event $k_{\circlearrowright}$, $k_{\circlearrowleft}$ with $k_{\circlearrowright} \oplus k_{\circlearrowleft} = 1$ and is defined as:

$$r_{RQN}^{k_{\circlearrowright},k_{\circlearrowleft}} = p_{ZZ}(k_{\circlearrowright}, k_{\circlearrowleft})[1 - h(E_Z^{k_{\circlearrowright},k_{\circlearrowleft}}) - h(\bar{e}_Y^{k_{\circlearrowright},k_{\circlearrowleft}})], \tag{7}$$

where $p_{ZZ}(k_{\circlearrowright}, k_{\circlearrowleft})$ is the probability of Alice and Bob choosing the $Z$-set for a given detection event. Since the $Z$-set rounds are unchanged, the QBER $E_Z^{k_{\circlearrowright},k_{\circlearrowleft}}$ is given by (4). The error rate $\bar{e}_Y^{k_{\circlearrowright},k_{\circlearrowleft}}$, however, is a bound on the phase-error rate based on the photon yields $Y_{n,m}^{k_{\circlearrowright},k_{\circlearrowleft}}$ that arise in decoy state protocols [Curty et al. 2019]:

$$e_Y^{k_{\circlearrowright},k_{\circlearrowleft}} \leq \frac{1}{2p_{ZZ}(k_{\circlearrowright}, k_{\circlearrowleft})}\Big[\sum_{(n,m)\in\mathbb{S}} C_n C_m^{k_{\circlearrowright}} \sqrt{\bar{Y}_{n,m}^{k_{\circlearrowright},k_{\circlearrowleft}}} + \sum_{(n,m)\notin\mathbb{S}} C_n C_m^{k_{\circlearrowright}}\Big]^2. \tag{8}$$

with $C_n = e^{\frac{-|\alpha|^2}{2}}(\frac{\alpha}{\sqrt{2}})^n/\sqrt{n!}$ and $C_m^{k_{\circlearrowright}} = e^{\frac{-|\alpha|^2}{2}}((-1)^{k_{\circlearrowright}}\alpha/\sqrt{2})^m/\sqrt{m!}$. In summary, we upper bound the yields $Y_{nm}^{k_{\circlearrowright},k_{\circlearrowleft}}$ for $(n,m) \in \mathbb{S}$ where $\mathbb{S}$ is a subset of $\{(n,m)|n,m \in \mathbb{N}_0\}$ which depends on the number of decoy settings used. In practice, the observed quantities are the gains (probability of having a detection given the intensity of the signal), and are used to estimate the yields (probability of having a detection event given the photon number), which cannot be observed. Thus, the yields are constrained by the following set of equations:

$$p_{YY}(k_{\circlearrowright}, k_{\circlearrowleft}|\mu_i\nu_j) = \sum_{n,m=0}^{\infty} e^{-\mu_i-\nu_j}\frac{\mu_i^n\nu_j^m}{n!m!}Y_{n,m}^{k_{\circlearrowright},k_{\circlearrowleft}}. \tag{9}$$

### 3.2. Key Rate Estimation

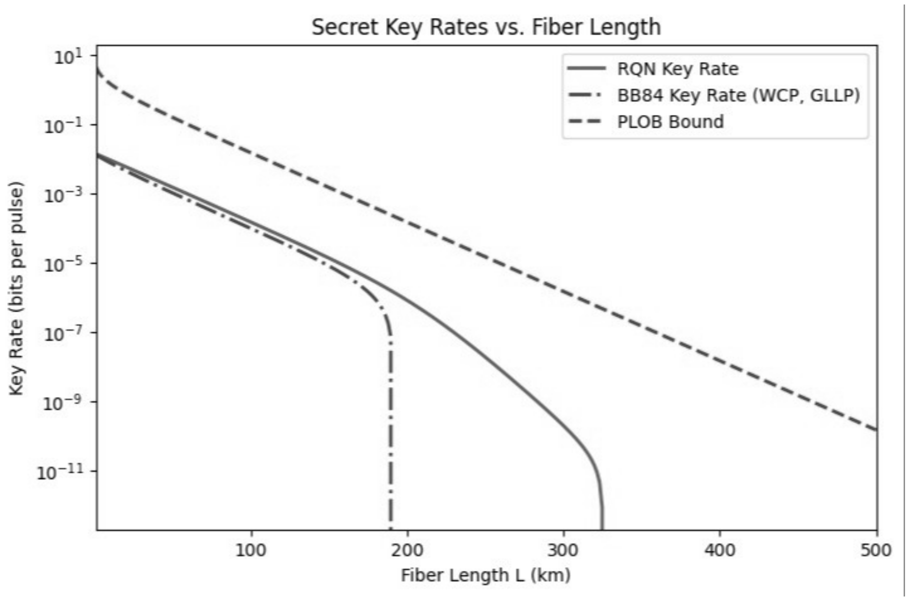

**Figure 2. Theoretical estimation of the secret key rate per pulse in logarithmic scale for the Rio Quantum Network as a function of the fiber length in kilometers. The solid line represents the secret key rate for the RQN protocol. We compare it to the PLOB-bound [Pirandola et al. 2017], and to the GLLP secret key rate for a BB84 protocol using WCPs [Gottesman et al. 2004].**

For our rough estimation, we model the errors in the $Z$ basis as:

$$E_Z^{(1,0)} = E_Z^{(0,1)} = \frac{p_{\text{error}}}{p_{\text{click}}} = \frac{e_d\eta(1-e^{-\mu_s}) + \frac{Y_{00}}{2}}{Y_{00} + \eta(1-e^{-\mu_s})}, \tag{10}$$

where $Y_{00} \approx 10^{-6}$ represents the $n = m = 0$ photon yield associated with detector dark counts, $e_d \approx 0.01$ is the intrinsic misalignment error attributed to the devices and $\mu_s = |\alpha|^2 \approx 0.02$ is the signal intensity. As for the phase-error rate $e_Y^{k_\circlearrowright,k_\circlearrowright}$ in the decoy state scenario, we consider the yields for up to 2 photons emitted by the source. We follow poissonian distributions to estimate the yields for single-photon: $Y_{01} = Y_{10} = \mu_d e^{-\mu_d}\eta$ and two photon: $Y_{11} = Y_{02} = Y_{20} = \frac{\mu_d^2}{2!}e^{-\mu_d}\eta$ scenarios. Here, $\mu_d \approx 0.1$ is the decoy intensity. When Alice and Bob choose the $Z$-set with 90% probability, we have that $p_{ZZ} = 0.81$ and $p_{ZZ}(1,0) = p_{ZZ}(0,1) = p_{ZZ}/2 * p_{\text{click}}$ and $p_{\text{click}} = Y_{00} + \eta(1 - e^{-\mu_s})$ is the probability of a successful detection event. This model calculates the secret key rate (6) based on the network's overall loss, quantified by the fiber length $L$. The transmittance $\eta$ is given by $\eta = 10^{-0,2L/10}$ representing the signal attenuation over the fiber (see Figure 2). For a transmittance value of $\eta = 0.5$, we estimate:

$$r_{\text{RQN}} \approx 0.0072 \tag{11}$$

per round. When using a pulse emission rate in the MHz order, the protocol is able to produce around $\sim$ 7200 secret key bits/second in this simplified model, which shows a promising ideal scenario. In Figure (2), we compare it to the GLLP secret key rate for the BB84, and remark that the protocol being implemented in the RQN shows an improvement over high-loss regimes.

The deployment of TF-QKD marks a promising first step in implementing the Rio Quantum Network. The security analysis presented here demonstrates that the Sagnac-based TF-QKD protocol is advantageous in the high-loss regime typical of metropolitan networks, and it estimates the possibility of establishing thousands of secret bits per second.

## References

Curty, M., Azuma, K., and Lo, H.-K. (2019). Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Information*, 5(1):64.

Devetak, I. and Winter, A. (2005). Distillation of secret key and entanglement from quantum states. *Proc. Math. Phys. Eng. Sci.*, 461(2053):207–235.

Gottesman, D., Lo, H.-K., Lutkenhaus, N., and Preskill, J. (2004). Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, pages 136–.

Lo, H.-K., Ma, X., and Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters*, 94(23).

Lucamarini, M., Yuan, Z. L., Dynes, J. F., and Shields, A. J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403.

Pirandola, S., Laurenza, R., Ottaviani, C., and Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043.

Renner, R. (2008). Security of quantum key distribution. *International Journal of Quantum Information*, 06(01):1–127.

Zhong, X., Wang, W., Mandil, R., Lo, H.-K., and Qian, L. (2022). Simple multiuser twin-field quantum key distribution network. *Phys. Rev. Appl.*, 17:014025.