The Rio Quantum Network: a reconfigurable hybrid multi-user metropolitan quantum key distribution network

Guilherme P. Temporão[1], **Fernando R. V. Bandeira de Melo**[2], **Antonio Z. Khoury**[3]

[1]Departamento de Eng. Elétrica, Pontifícia Universidade Católica do Rio de Janeiro
Rio de Janeiro, RJ – Brazil

[2]Centro Brasileiro de Pesquisas Físicas
Rio de Janeiro, RJ – Brazil

[3]Departamento de Física, Universidade Federal Fluminense
Niterói, RJ – Brazil

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

Abstract. *This paper describes the current status of the Rio Quantum Network project, a metropolitan quantum communication network under construction connecting four research institutions in the state of Rio de Janeiro through optical fibers from Rede Rio de Computadores / FAPERJ and a 7-km free space link. The Twin-Field Measurement Device Independent Quantum Key Distribution (TF-MDI-QKD) protocol is being implemented to enable secure communication between any two network nodes independently, without the need for trusted nodes. The main challenges of the practical implementation of the network will be presented and discussed.*

1. Introduction

A quantum network (QN) is a communication structure responsible for connecting different entities (nodes) that have some quantum information processing power. In other words, a QN's main objective is to allow transmission, distribution and sharing of quantum states among multiple users geographically distant from each other. The existence of QNs is essential for all the sub-areas of quantum information. For Quantum Computing, they allow remote access to quantum computers, whether in a standard ”server/client” configuration or in more sophisticated applications such as blind quantum computing [Fitzsimons 2017] and distributed quantum computing [Meter and Devitt 2016]. In the case of Quantum Communications, a QN not only enables the implementation of distributed encryption protocols (Leader Election, Byzantine Agreement) but also allows Quantum Key Distribution (QKD) [Gisin et al. 2002] protocols to be carried out between any two nodes on the network that do not have a direct physical connection, without the need for ”trusted nodes”. For Quantum Metrology, there are numerous applications ranging from the implementation of interferometric telescopes [Gottesman et al. 2012], clock synchronization [Ilo-Okeke et al. 2018] and fundamental tests of Quantum Physics, such as the demonstration of violation of Bell Inequality free of *loopholes* [Hensen et al. 2015].

The *Rio Quantum Network* project is a first step on the national stage towards the construction of a metropolitan quantum network and its future connection to the Quantum Internet [Kimble 2008, Simon 2017]. This network, initially, will connect four institutions in the state of Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro

(PUC-Rio), Centro Brasileiro de Pesquisas Físicas (CBPF), Universidade Federal do Rio de Janeiro (UFRJ) and Universidade Federal Fluminense (UFF); a fifth institution, Instituto Militar de Engenharia (IME), is also about to integrate the network. We employ optical fibers installed and made available by Rede-Rio de Computadores/FAPERJ to build a metropolitan quantum network involving three institutions: PUC-Rio, CBPF and UFRJ. Furthermore, a connection to UFF will be provided via a CBPF/UFF free space link over the Guanabara Bay. Initially, we will develop and put into operation a system using the MDI-QKD (*Measurement Device Independent Quantum Key Distribution*) [Lo et al. 2012] protocol, in which Alice and Bob will be able to establish a random and secret key through a Charlie intermediate station. The network is reconfigurable, in the sense that any of the four institutions may play the roles of Alice or Bob; only Charlie is fixed at PUC-Rio. The configuration can be seen on Figure 1.

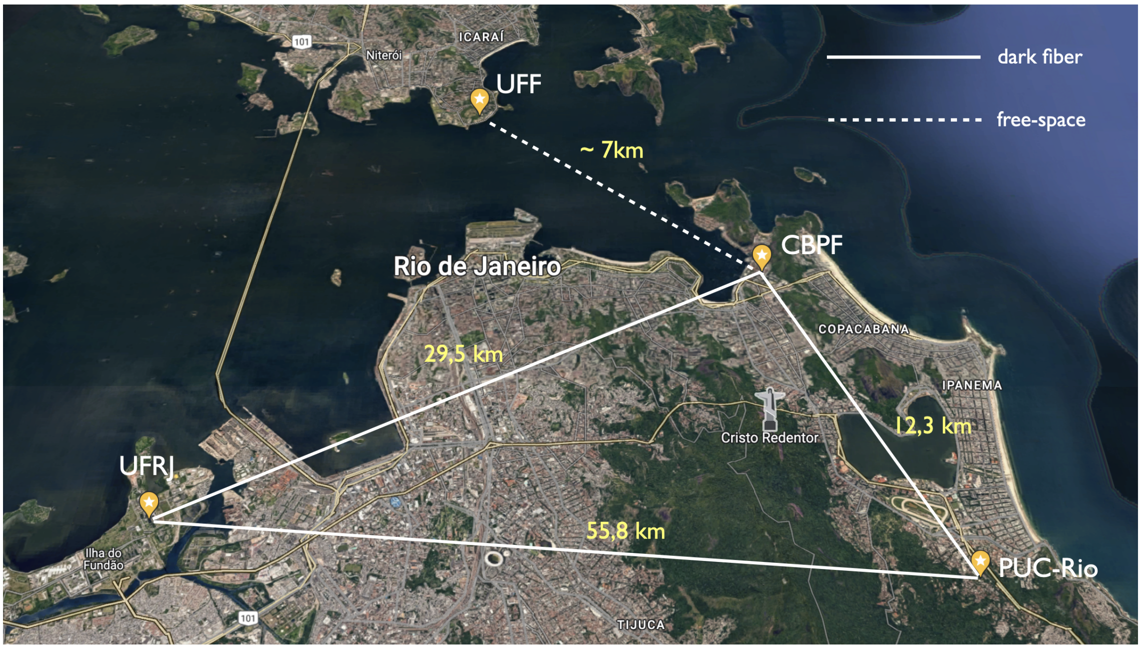

Figura 1. The Rio Quantum Network layout. Picture by Google Maps.

In the following sections we describe the first phase of the project, which comprises the engineering choices for the network topology, the issue of integration of a free-space link into the Sagnac loop and the experimental challenges that have been encountered.

2. Network Structure

2.1. The folded fiber-optical Sagnac configuration

The structure of the Rio Quantum Network is based on a Sagnac-loop implementation of the Twin-Field MDI QKD protocol [Zhong et al. 2022]. In this implementation, Charlie concentrates almost all of the hardware: he concentrates the optical source and the single-photon detectors, whereas Alice and Bob only need phase modulators and amplitude modulators for adding the decoy states modification. The advantage of using a Sagnac loop is that phase fluctuations are automatically compensated and therefore there is no need to deploy a phase control system. On the other hand, any optical-fiber Sagnac interferometer is susceptible to polarization fluctuations, which means that a polarization control scheme must be implemented.

Figure 1 shows a schematic triangle in the network, which can be immediately thought of as a Sagnac loop. However, this choice would not be optimal for a series of reasons, including the optical fiber link availability in the UFRJ-CBPF link and the impossibility of reconfiguring the loop. Given the availability of two optical fibers per link, the configuration of choice was a *folded* Sagnac loop, as shown in Figure 2. Note that there is no direct connection between Alice and Bob, i.e., the 29,5km link between UFRJ and CBPF is not used.

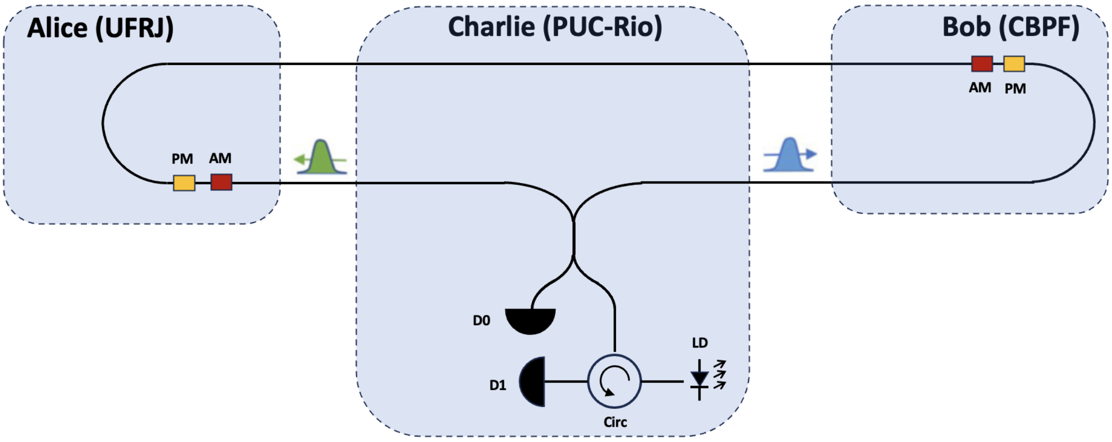

Figura 2. The folded Sagnac configuration for a specific example where Alice is at UFRJ and Bob at CBPF. See text for details.

In this configuration, Charlie uses a Laser Diode (LD) to produce weak coherent pulses. Each pulse is divided at the beamsplitter, one in the clockwise direction (green pulse) and other in the counterclockwise direction (blue pulse). This is a two-level system, therefore comprising a qubit. The idea is that Alice and Bob apply a relative phase between these two modes, by correctly timing the activation of the phase modulators (PM) - the amplitude modulators (AM) are employed only for implementation of the decoy stats modification. The general expression for the qubit in this configuration is given by:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + ie^{i(\phi_A-\phi_B)}\,|1\rangle\right] \tag{1}$$

where $\{|0\rangle\,,|1\rangle\}$ are the clockwise / counterclockwise modes, which comprise an orthonormal basis. By adjusting the phases $\phi_{A,B} \in \{0, \pi/2, \pi, 3\pi/2\}$, Alice and Bob can produce the four BB84-like states that form two mutually unbiased bases - namely, the states $|+\rangle\,, |-\rangle\,, |+i\rangle\,, |-i\rangle$ which lie in the equator of Bloch sphere. Table 1 indicates the different probabilities of detection in single-photon detectors D0 and D1 for each added phase difference between Alice and Bob.

One may argue that this configuration doubles the distance travelled by the photons if compared to the regular MDI-QKD scheme. However, one must take into account that the Twin-Field variety has the advantage of the losses scaling with the square root of

Tabela 1. Probabilities of detection for different phase differences

$\phi_A - \phi_B$	Prob(D0)	Prob(D1)
0	0	1
$\pi/2$	0.5	0.5
π	1	0
$3\pi/2$	0.5	0.5

the transmission coefficient [Yin and Fu 2019], such that the raw key rates in each scenario - regular MDI-QKD (R_{MDI}) and Twin-Field MDI-QKD (R_{TF}) are given by:

$$\begin{aligned} R_{MDI} &\sim e^{-\alpha L_A} e^{-\alpha L_B} (\eta)^2 \\ R_{TF} &\sim \left(e^{-2\alpha L_A} e^{-2\alpha L_B}\right)^{\frac{1}{2}} \eta \end{aligned} \tag{2}$$

where η is the quantum efficiency of the single-photon detectors, L_A and L_B are the (one-way) fiber lengths between Alice-Charlie and Bob-Charlie, respectively, and α is the optical fiber attenuation coefficient in dB/km. The Twin-Field variety has a higher key rate because it only needs one single-photon detector, whereas the regular MDI-QKD needs coincidence counts between two detectors in a Bell State Measurement.

2.2. Adding the free-space link CBPF-UFF

Now we turn to the question of how a free-space link can be included in the previously shown Sagnac loop, which is entirely comprised of optical fiber links. One possible solution that employs a single telescope is shown below in Figure 3, which shows a fraction of the Sagnac loop in the CBPF-UFF connection. The idea is employing polarization controllers (PC) such that a clockwise pulse is mapped into a horizontal polarization state, whereas a counterclockwise pulse always exits the PC in a vertical polarization state. On the other end, an optical fiber loop (required for the asymmetry needed to activate the PM only for clockwise pulses) is ended at a Faraday Mirror (FM), which converts vertical polarization into horizontal and vice-versa. Note that this ensures that an incoming pulse - which entered the polarizing beamsplitter (PBS) in a vertical polarization state from the upper mode, will leave it in a horizontal polarization state in the lower mode, and vice-versa, keeping the clockwise/counterclockwise direction unchanged. Of course, two pairs of telescopes could also be employed, consequently increasing the implementation cost.

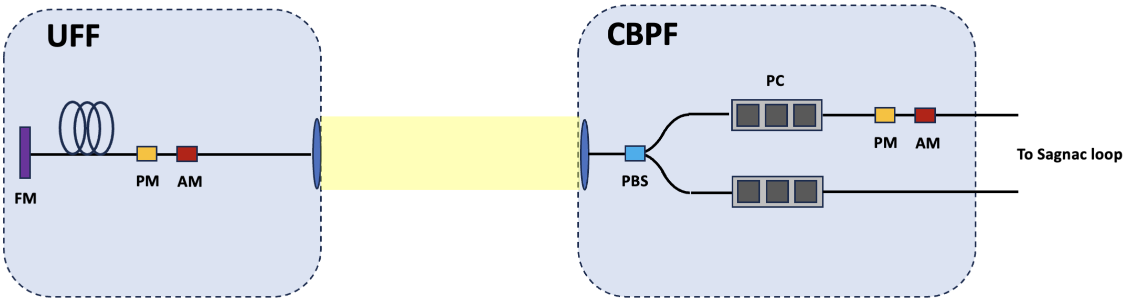

Figura 3. Including a free-space link in an optical fiber Sagnac loop with a single telescope. See text for details.

3. Experimental Challenges

The construction of the Rio Quantum Network is already under way, and the PUC-CBPF link is currently active with many ongoing experiments. This section briefly describes some of the experimental challenges that are expected.

3.1. Network Synchronization

The first issue that concerns any MDI-QKD implementation is synchronization between Alice, Bob and Charlie. Charlie's pulses must be modulated by Alice and Bob's PMs at a very precise time that cannot rely on individual clocks because of electronic jitter and wander. The Rio Quantum Network employs a master clock sent by Charlie, which consists of a secondary pulsed laser, in phase with the pulses sent in the quantum channel. This synchronization laser has a different central wavelength from the quantum channel, lying in a separate DWDM (dense wavelength division multiplexing) channel. This solution requires the deployment of a DWDM in each user of the network; part of the synchronization pulse is split from the weak coherent pulses and detected in order to drive the AM and PM at the correct time.

Another issue that is related to synchronization is the very nature of the Sagnac architecture, which limits the maximum number of pulses that can exist in the fiber at the same time. This problem can be solved by sending ”bursts”of pulses with a dead time between bursts. Solutions that minimize this deadtime are currently being developed.

3.2. Polarization stabilization and control

All interferometers depend on polarization stabilization for maximum interferometric visibilities; this is problematic in optical fibers, due to fiber birefringence which leads to random polarization rotations [Xavier et al. 2008]. Moreover, the AMs and PMs present in all users exhibit polarization dependent losses (PDL), which can also be mitigated by appropriately controlling the polarization state.

Luckily, as the polarization degree of freedom does not carry quantum information in the Twin Field-MDI-QKD protocol, we don't need a full polarization control method; it suffices to control one polarization axis on Poincaré Sphere, which can be done with commercial polarization trackers. It should be clear, however, that the quantum channel cannot be employed for performing the control; one must use a classical channel instead, such as the synchronization channel cited above.

3.3. Losses

Losses are the main limitation to the net key generation rate in any QKD implementation. There are a few ways to circumvent losses that are being exploited in the Rio Quantum Network, of which we can highlight two. The first one is observing that Charlie does not need to send pulses at a single-photon level, because they do not carry any information. In fact, it is at the entrance of Alice and Bob's offices that the pulses must be attenuated. We are employing variable optical attenuators that can be configured such that they are activated only when needed. The second way concerns the use of optical switches that are capable of changing the network size; depending on the location of Alice and Bob - for example, Alice at PUC-Rio and Bob at CBPF - there is no need to have photons travelling to and from UFRJ. Some ”bypass”optical switches can be placed in order to create a reconfigurable network setup that minimizes losses.

4. Conclusions

The Rio Quantum Network is currently under development, with many experiments taking place. We have shown how a reconfigurable network topology can be used to decrease losses and increase the key generation rate, and how synchronization and stabilization issues are being approached. We hope to have the first key exchange between UFRJ and CBPF by the end of 2024. The free-space link between UFF and CBPF is currently being implemented independently from the remainder of the network and employs structured light, and a connection CBPF-IME is under way.

Referências

Fitzsimons, J. F. (2017). Private quantum computation: an introduction to blind quantum computing and related protocols. In *npj Quantum Inf*, volume 3, page 23. Nature Publishing Group.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. In *Rev. Mod. Phys.*, volume 74, pages 145–195. American Physical Society.

Gottesman, D., Jennewein, T., and Croke, S. (2012). Longer-baseline telescopes using quantum repeaters. In *Phys. Rev. Lett.*, volume 109, page 070503. American Physical Society.

Hensen, B., Bernien, H., Dréau, A. E., Reiserer, A., Kalb, N., Blok, M. S., Ruitenberg, J., Vermeulen, R. F. L., Schouten, R. N., Abellán, C., Amaya, W., Pruneri, V., Mitchell, M. W., Markham, M., Twitchen, D. J., Elkouss, D., Wehner, S., Taminiau, T. H., and Hanson, R. (2015). Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. In *Nature*, volume 526, pages 682–686. Nature Publishing Group.

Ilo-Okeke, E. O., Tessler, L., Dowling, J. P., and Byrnes, T. (2018). emote quantum clock synchronization without synchronized clocks. In *npj Quantum Information*, volume 4, page 40. Nature Publishing Group.

Kimble, H. J. (2008). The quantum internet. In *Nature*, volume 453, pages 1023–1030. Nature Publishing Group.

Lo, H.-K., Curty, M., and Qi, B. (2012). Measurement-device-independent quantum key distribution. In *Phys. Rev. Lett.*, volume 108, page 130503. American Physical Society.

Meter, R. V. and Devitt, S. J. (2016). The path to scalable distributed quantum computing. In *Computer*, volume 49, pages 31–42.

Simon, C. (2017). Towards a global quantum network. In *Nature Photonics*, volume 11, pages 678–680. Nature Publishing Group.

Xavier, G. B., de Faria, G. V., ao, G. P. T., and von der Weid, J. P. (2008). Full polarization control for fiber optical quantum communication systems using polarization encoding. *Opt. Express*, 16(3):1867–1873.

Yin, H.-L. and Fu, Y. (2019). Measurement-device-independent twin-field quantum key distribution. volume 9, page 3045. Nature Publishing Group.

Zhong, X., Wang, W., Mandil, R., Lo, H.-K., and Qian, L. (2022). Simple multiuser twin-field quantum key distribution network. volume 17, page 014025. American Physical Society.