QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Funded by
the European Union

Quantum-Safe Internet (QSI)

Scientific Deliverable 2:

Communication Networks Projects State of Play

Deliverable D.2.1 – WP 2.

Index:

I. INTRODUCTION

The Work Package 2 on quantum-safe communication networks studies the quantum-safe cryptography protocols which are used in communications networks, and must enable any two network users, at any distance, to communicate securely. This, in the first generation of quantum networks, is expected to be achieved by means of trusted nodes, including satellite links. Such a trust requirement could later be removed by using quantum repeater technologies.

These are the doctoral candidates participating in Work Package 2 and the institutions to which they belong:

Doctoral Candidate 6,	Sergio Juárez,	Toshiba.	(United Kingdom)
Doctoral Candidate 7,	*Pending*,	University of Geneva.	(Switzerland)
Doctoral Candidate 8,	Matías Bolaños,	University of Padova.	(Italy)
Doctoral Candidate 9,	Javier Rey,	University of Leeds.	(United Kingdom)
Doctoral Candidate 10,	Loïc Millet,	IDQuantique.	(Switzerland)
Doctoral Candidate 11,	Vaisakh Mannalath,	University of Vigo.	(Spain)

Next we provide a brief overview of the main objective of their projects. For a detailed description of the projects, see section II:

Doctoral Candidate 6, will take on the challenges of developing an autonomous twin-field quantum key distribution (QKD) prototype which is able to operate continuously on a deployed fibre-based network. The final goal is to further simplify the integration and enhance the rate-versus-distance performance of QKD in optical networks.

Doctoral Candidate 7, (pending) will design novel QKD network architectures for existing telecom networks.

Doctoral Candidate 8, will aim at improving the rate and versatility of satellite-based QKD as well as those of hybrid wireless-fibre QKD networks. The goal is to further extend the transmission distance of quantum communication schemes to a global scale.

Doctoral Candidate 9, will work on advanced quantum repeater protocols compatible with packet-switched networking.

Doctoral Candidate 10, will determine optimal solutions for service providers and various use cases, and embed next-generation QKD setups in a global security ecosystem composed of quantum and post-quantum protocols.

Doctoral Candidate 11, will study the security and performance of quantum cryptographic schemes implemented over quantum networks with multiple users.

II. DETAILED DESCRIPTION OF THE PROJECTS

Project of Doctoral Candidate 6, Sergio Juárez, Toshiba.
"TWIN-FIELD QUANTUM KEY DISTRIBUTION ON INSTALLED FIBRE NETWORKS".

OBJECTIVES

Autonomous prototype system for Twin-Field Quantum Key Distribution.

EXPECTED RESULTS

Operation of TF-QKD on installed networks.

DESCRIPTION

Twin-Field QKD is a novel protocol to greatly increase the rate-vs-distance performance of QKD. Most interestingly the bit rate of TF-QKD has better resilience to channel loss than conventional QKD. In fact, it can allow key rates above the secret key capacity of a point-to-point quantum channel. Recently we demonstrated intermittent operation of TF-QKD over 600km fiber spools in the lab. In this project we plan to greatly extend this work to realize an autonomous prototype that can operate continuously on installed fiber. In TF-QKD, the two parties (Alice and Bob) send encoded laser pulses to a central measurement station Charlie. The main challenge in TF-QKD is to ensure phase stability between the pulses from Alice and Bob, even after propagation in fibers which are 100's of km in length. We will achieve this using the interference of stabilization pulses sent from Alice and Bob, as a feedback signal to fix the relative phase difference between the fibers. We target building a prototype system and deploying it in a field trial by the end of the project.

METHODOLOGY

We first establish a continuously running prototype under lab conditions; we then implement field trials for first >1h operation, and then >24h operation.

RISKS

If continuous operation is not possible over long distances, we reduce the link distance, or use shorter time periods.

Project of Doctoral Candidate 7, *Pending*, University of Geneva.
"QKD IN MODERN TELECOMMUNICATIONS NETWORKS".

OBJECTIVES

Study telecom network designs and the co-existence of quantum and classical signals in optical networks. Develop QKD systems to simplify the integration and standard their performance in optical networks. Study trusted repeater implementations with standard security.

EXPECTED RESULTS

New designs of QKD devices and networks that allow for a seamless integration in existing telecom networks.

Funded by the European Union

DESCRIPTION

Point to point QKD over dark fiber has become a mature technology for years. One of the remaining challenges is to produce QKD network equipment that can easily be integrated with modern communications networks. A key figure is the total cost of ownership, which is currently too high also due to expensive installations and maintenance as well as the need for dark fibers. To avoid the latter, we need co-existence of classical and quantum channels, as well as a quantum network multiplexing many channels between many different transmitters and receivers. Co-existence and standardization are studied in the current Open QKD project. In this experimental project, the Doctoral Candidate will study the telecom networks and benefit from the Open QKD experience, in particular, with the use-cases in Geneva over the fiber network of the Services Industries de Genève (SIG). The results of these studies will feed back into the design of quantum and classical signal integration. The Doctoral Candidate will work out how QKD can optimally deal with rerouting, amplifiers and switches, which are present in the established infrastructure. Another aspect is the optimal architecture of a QKD network, integrating eventual trusted nodes. All this is done considering the latest notions in network architectures such as software-defined networking and recent requirements coming from the smart grid Internet of Things and 5G applications. The latter require cheap and compact devices, in line with on-going efforts at UNIGE of implementing QKD with photonic integrated circuits. During the project, the Doctoral Candidate will test the performance of latest QKD devices at UNIGE in different configurations, in the lab and in the telecom environment, and implement necessary changes.

METHODOLOGY

It is based on extensive exchanges with the telecom specialists from SIG and the QKD manufacturer IDQ (both in Geneva) to learn about their practical constraints in order to find solutions that allow for seamless integration of QKD in a telecom environment.

RISKS

Implementing QKD on live fibers, in the presence of amplifiers and switches, requires coordination with different stakeholders; if this causes delay the scope of the.

Project of Doctoral Candidate 8, Matias Bolaños, University of Padua. “INTERMODAL QUANTUM COMMUNICATIONS IN FREE-SPACE AND FIBRE”.

OBJECTIVES

Experimental study and modelling of intermodal quantum communications, aiming at bridging free-space and fibre links.

EXPECTED RESULTS

Efficient free-space to fibre quantum interfaces, qubit preparation, measurement, synchronization, and QBER mitigation. The channel multiplexing and the matching of QKD with fibre network standards for high speed communications will be implemented.

DESCRIPTION

The envisaged framework for global-scale quantum communications networks will comprise various nodes interconnected via optical fibres or free-space channels, depending on the link distance. The free-space segment of such a network should guarantee certain key requirements, such as daytime operation and the compatibility with the complementary telecom-based fibre infrastructure. In addition, space-to-ground links will require light and compact quantum devices to be placed in orbit. For these reasons, investigating solutions satisfying all the above requirements is necessary. This requires to conceive and develop ways to leverage the benefit of both fibre and free- space channels. The intermodal exchange plays a crucial role in QKD between different continental networks, to provide redundancy on the network and to advance the paradigm of untrusted nodes. Recent progress in daylight QKD by UNIPD has extended the application domain and the overlap with the usage of fibre links. In addition, the modelling of key rate in a network of mixed link types will be developed for assessing the capacity of mutual connection with different users even considering the peculiarities of the free-space links. The study of the free-space to fibre integration will be the next necessary ingredient. The expertise and experience of secondment partners are used to increase the chance of success.

METHODOLOGY

Initial prototypes will be designed for optical table demonstration, with investigations under real conditions to follow; facilities in Matera and Asiago Observatories will be used appropriately.

RISKS

The satellite link is already quite lossy; it is possible that the additional loss because of the interface makes the overall QKD link insecure. We consider using adaptive optics and different types of fiber if needed.

Project of Doctoral Candidate 9, Javier Rey, University of Leeds.
“TRUST-FREE PACKET-SWITCHED QUANTUM COMMUNICATIONS NETWORKS”.

OBJECTIVES

Designing quantum communications networks, at different layers, compatible with current packet-switched networks.

EXPECTED RESULTS

New quantum repeater protocols compatible with packet-switched networking; Performance analysis, e.g., entanglement generation rates and secret key rates in QKD applications, over such repeaters; New network and transport layer protocols.

DESCRIPTION

A functional quantum Internet is the holy grail of quantum communications technologies. While there are plenty of proposals for building scalable quantum repeaters, most of which work on a circuit-switched basis. That is, we need to secure resources over different segments of an end-to-end link before being able to generate an entangled state between two remote users. This means that all required resources for that link has to be allocated to those two users for the entirety of the protocol, and other network users cannot use those resources. The only exception to this is the so-called third generation quantum repeaters, which, similar to their classical counterpart, transfer quantum states hop-by-hop by using excessive amount of quantum error correction to combat loss and noise. These repeaters, however, face several technological challenges, including the need to have intermittent nodes in close proximity on the order of a few kms. This can effectively make them incompatible with existing infrastructure for the Internet, which crucially works on the basis of packet switching. This project aims at designing feasible, in near to mid-term, quantum repeaters in an aligned way with the concept of packet switching. That is, we generate entangled states between two far end nodes by starting from one end and extending the entanglement, node by node, in a similar fashion that a packet finds its way in the Internet. Similar to classical networks one could then optimize the path based on availability of resources, e.g., entangled states, or reliability of the links. This requires revisiting network layer protocols for this application. End-to-end reliable quantum data transfer can then be managed in such networks by updating the relevant transport layer protocols.

METHODOLOGY

We explore the use of simple quantum error correction codes for distillation purposes. It has recently been shown that even a simple 3-qubit repetition code could offer advantage in QKD applications [Phys. Rev. Appl. 15, 044027 (2021)]. We benchmark the performance of our proposed repeater setups by calculating the corresponding secret key generation rate when you run trust-free QKD protocols.

RISKS

Simulating large quantum systems is time consuming; efficient numerical techniques will be developed if analytical.

Project of Doctoral Candidate 10, Loïc Millet, IDQuantique.
"ARCHITECTURE AND HARDWARE FOR A HIGH-PERFORMANCE QUANTUM-SAFE INTERNET".

OBJECTIVES

Develop a future-proof and practical architecture and hardware components for a QS Internet that optimally address the needs for security, functionality, and usability.

EXPECTED RESULTS

Integration of the state-of-the-art building blocks in commercial QKD systems and demonstration of their value in QKD networks.

DESCRIPTION

The value of transferred data is constantly increasing as the unwanted disclosure or loss of integrity can even have an impact on human lives. At the same time, the technology to threaten current communication security (with the quantum computer as prominent example) is constantly improving. New cybersecurity solutions are therefore in order. While QKD systems have become commercially available and they can be deployed in various network infrastructures, there is a constant need to improve their performance in a practical and industry-compatible manner in terms of QKD metrics (key rate, link loss, entropy source performance), security (quantum hacking countermeasures, physical and theoretical security) and sensitivity to adjacent multiplexed classical channels. In parallel, the combination of these components and their operational parameters influence the performance of the QKD system and how it matches with the physical constraints of the network in which they will be installed. Adaptability of the system to the network's physical condition, and vice-versa, is an aspect of high practical value.

The DR will work on the development of some of the key sub-systems of a modular commercial platform based on the BB84 protocol to improve their performance. The focus of this work will range from hardware components like single-photon detector and QRNGs to processing modules like error correction and privacy amplification algorithms. The DR will also study the influence of each sub-system on the overall system performance to evaluate to evaluate the adaptability the highest impact for different deployment use cases.

METHODOLOGY

The development of sub-systems will be aligned with the interfaces of IDQ's QKD platform. Their impact on performance and their added value will be evaluated and quantified. Secondments will enhance the development possibilities and will allow addressing the overall architecture and security aspects.

RISKS

Implementing new sub-system inside a commercial QKD product requires tight integration in a production environment; if this causes delay the scope of the project will be adjusted appropriately (e.g. limit the scope to a working PoC which is only partially integrated in to the commercial system).

Project 11 of Doctoral Candidate 11, Vaisakh Mannalath, University of Vigo. "QUANTUM CRYPTOGRAPHIC SCHEMES FOR QUANTUM NETWORKS".

OBJECTIVES

Designing efficient multi-user quantum cryptographic schemes for entanglement-based quantum networks.

EXPECTED RESULTS

Proposals for quantum cryptographic schemes with multiple users over quantum networks. Performance and security analysis of such schemes in a practical setting.

DESCRIPTION

Most quantum cryptographic schemes assume a two-user setting in a point-to-point network configuration, which do not fully exploit the richness of complex quantum networks. Moreover, to extend the achievable distance between end users, they typically rely on the use of trusted nodes. A principal goal of this project is to design efficient quantum cryptographic schemes such as e.g. those achieving conference key agreement or distributed quantum computing for various entanglement-based quantum network topologies with multiple users and untrusted nodes, and evaluate their security in a practical setting. Moreover, we shall investigate their performance and robustness against typical device imperfections of the users' apparatuses, as well as those of the untrusted networks nodes.

METHODOLOGY

The Doctoral Candidate will study conference key agreement and beyond QKD multi-user cryptographic schemes suitable for entanglement-based quantum networks. Efficient techniques to establish different kinds of entanglement between the end users will be explored. The security and robustness of the designed schemes against side-channels will be investigating by adapting known QKD methods to this scenario.

RISKS

If obtaining analytical results turn out to be too complex to achieve, or they provide loose security bounds, numerical methods will be used. If a quantum cryptographic scheme does not provide advantages over classical solutions, or over a combination of multiple two-users setups, alternative schemes will be considered.

III. PROGRESS OF EACH DOCTORAL CANDIDATE AND HER/HIS PROJECT

Project of Doctoral Candidate 6, Sergio Juárez, Toshiba.

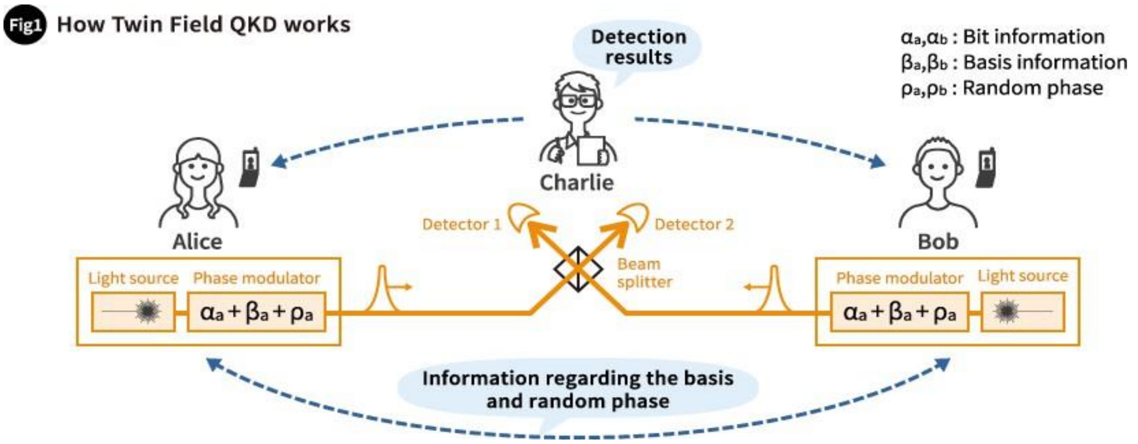
CONTRACT STARTING DATE: 04/09/2023.

SUPERVISORS: Shields (TOSHEU), Pittaluga (TOSHEU), Woodward (TOSHEU), Razavi (ULEEDS), Curty (UVIGO), Calonico (INRIM).

PROGRESS and RESULTS:

The first five months of my PhD have been devoted to acquiring a deep understanding of the fundamental principles of quantum cryptography. This initial period has been essential for equipping me with the knowledge and skills necessary to engage effectively with the complexities of the Twin Field Quantum Key Distribution (TF-QKD) protocol and its associated technologies.

The advancement of Quantum Key Distribution (QKD) marks a significant milestone in the field of secure communication, with Twin Field Quantum Key Distribution (TF-QKD) emerging recently as an important development for long-distance quantum communication. My PhD project is centered on enhancing the TF-QKD protocol to align it with the existing optical fibre network infrastructure, allowing it to become a crucial tool towards the potential realization of a quantum internet. Beyond refining TF-QKD, in this project I will also explore alternative quantum communication protocols and study fundamental experimental techniques with the broader goal in mind of contributing to the foundational technology necessary for a quantum internet.



Https://www.global.toshiba/ww/company/digitalsolution/articles/tsoul/tech/t0204.html

My research methodology encompasses both theoretical and practical approaches, including experimental validations and adaptation techniques for TF-QKD, alongside a thorough review of existing and emerging quantum internet technologies.

Familiarization with Quantum Cryptography Basics BB84 Protocol

My research began with an exploration of the BB84 protocol, an influential protocol in quantum cryptography developed by Charles Bennett and Gilles Brassard in 1984. This protocol is fundamental in secure quantum key distribution, utilizing quantum mechanics principles. My study involved a detailed examination of the BB84 protocol, with a focus on its use of quantum bits (qubits) for key generation and the security features inherent in quantum mechanics. This provided me the necessary foundation for understanding advanced QKD systems, including TF-QKD.

Polarization and Phase Encoding Techniques

The BB84 protocol and other QKD protocols can be experimentally implemented using different degrees of freedom of the photons for the encoding of information, such as phase or polarization. I delved into both polarization and phase encoding techniques, examining their applications and implications. While both techniques are applicable and offer insights in the BB84 protocol, I focused most of my time to understand the intricacies of phase encoding, since it plays a fundamental role in the context of TF-QKD.

MDI-QKD Insights into TF-QKD.

Another key component that I need to fully understand before tackling TF-QDK head on is Measurement-Device-Independent Quantum Key Distribution (MDI-QKD). Which has the advantage of the elimination of the detector vulnerabilities, and this advantage translates directly into TF-QKD. This has also allowed me to familiarize myself with concepts of the field of quantum hacking, and the security proofs of the protocols.

Key Sifting Process

Additionally, I also employed some time to understand the key sifting process, a procedure used in QKD to distil a shared secret key from the raw key material produced in the experimental quantum communication. This process involves classical communication between the parties to reconcile and discard bits that are not identically received, thereby ensuring the security and integrity of the resultant key. Mastery of this process is essential for understanding the security assurances of QKD systems and their resilience to eavesdropping attempts.

This initial phase of my PhD has been instrumental in building a strong theoretical and practical understanding of quantum communication principles. The knowledge gained during these five months forms the bedrock upon which my future research on TF-QKD and the development of quantum internet protocols will be built. As I progress from this initial phase to the practical implementation of an operational TF-QKD system, this groundwork ensures that I will do so seamlessly and that I am well-prepared to contribute meaningfully to the field of quantum cryptography.

Project of Doctoral Candidate 7, Pending, University of Geneva.

CONTRACT STARTING DATE: PENDING.

SUPERVISORS: Thew (UNIGE), Gudet (SIG), Layat (IDQUANTIQUESA), Curty (UVIGO), Villoresi (UNIPD)

A doctoral candidate started in November 2023 but did not fit and the vacancy is still pending.

Project of Doctoral Candidate 8, Matías Bolaños, University of Padova.

CONTRACT STARTING DATE: 01/11/2022.

SUPERVISORS: Villoresi (UNIPD), Vallone (UNIPD), Razavi (ULEEDS), Diamanti (SU), Finocchiaro (EUTELSAT)

PROGRESS and RESULTS:

My first task was the development of a Time-To-Digital converter for Quantum Key Distribution (QKD) applications. My current design is implemented on two development boards: The Zed board, with 20 PS resolution and 30 PS jitter, and a ZCU104 with 4 PS resolution and 8.5 PS jitter. This system will be capable of replacing the current TDCs in the laboratory, with the added capability of real-time post-processing of the time tags thanks to the parallel nature of an FPGA chip. We also worked on the calibration of such devices and its temperature dependence, and are currently working on a publication on this topic.

Later, I collaborated on the design of a QKD source scheme capable of implementing the three-state one-decoy BB84 protocol within the near-infrared (NIR) optical band, which consists of a pulsed laser source operating at a repetition rate of $R = 50$ MHz, coupled with two iPOGNAC-based modulation stages (see Fig. 1 below). This scheme was implemented with two gain-switched PM fiber-coupled distributed feedback lasers at different wavelengths to test its robustness: The Eagle yard EYP-DFB-0795 and the Gooch & Housego AA1406-192000-100-PM250-FCA-NA, which emit light pulses at wavelengths of 795 nm and 1550 nm respectively.

For the first stage, the iPOGNAC-based intensity modulator requires a fixed polarization state as input; hence, a PM fiber-based polarizer was introduced to ensure that the input state was fixed as $|D\rangle$. Subsequently, the iPOGNAC settings were modified to achieve a signal-to-decoy ratio of $\nu/\mu \approx 0.30$, considered optimal for the efficient three-state and one-decoy protocol for a wide range of total losses (30 dB to 60 dB) relevant to satellite-based QKD. For the second iPOGNAC stage, which is assigned to manipulate the polarization of the qubit, the iPOGNAC settings were modified to introduce a phase shift $\pm\pi/2$. In this way, from an input state $|D\rangle$, the iPOGNAC is capable of producing circular left ($|L\rangle$) and circular right ($|R\rangle$) states. With this scheme, we define the key generation basis Z $= \{|0\rangle, |1\rangle\}$, where $|0\rangle := |L\rangle$ and $|1\rangle := |R\rangle$, alongside the control basis X $= \{|+\rangle, |-\rangle\}$, where $|+\rangle := |D\rangle$ and $|-\rangle := |A\rangle$.

Funded by
the European Union

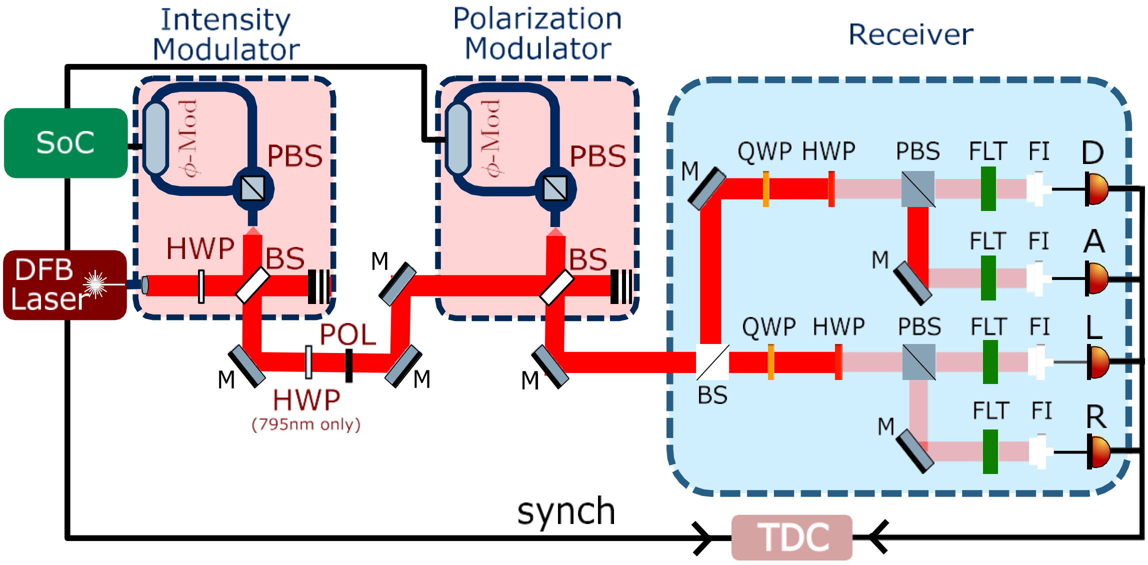
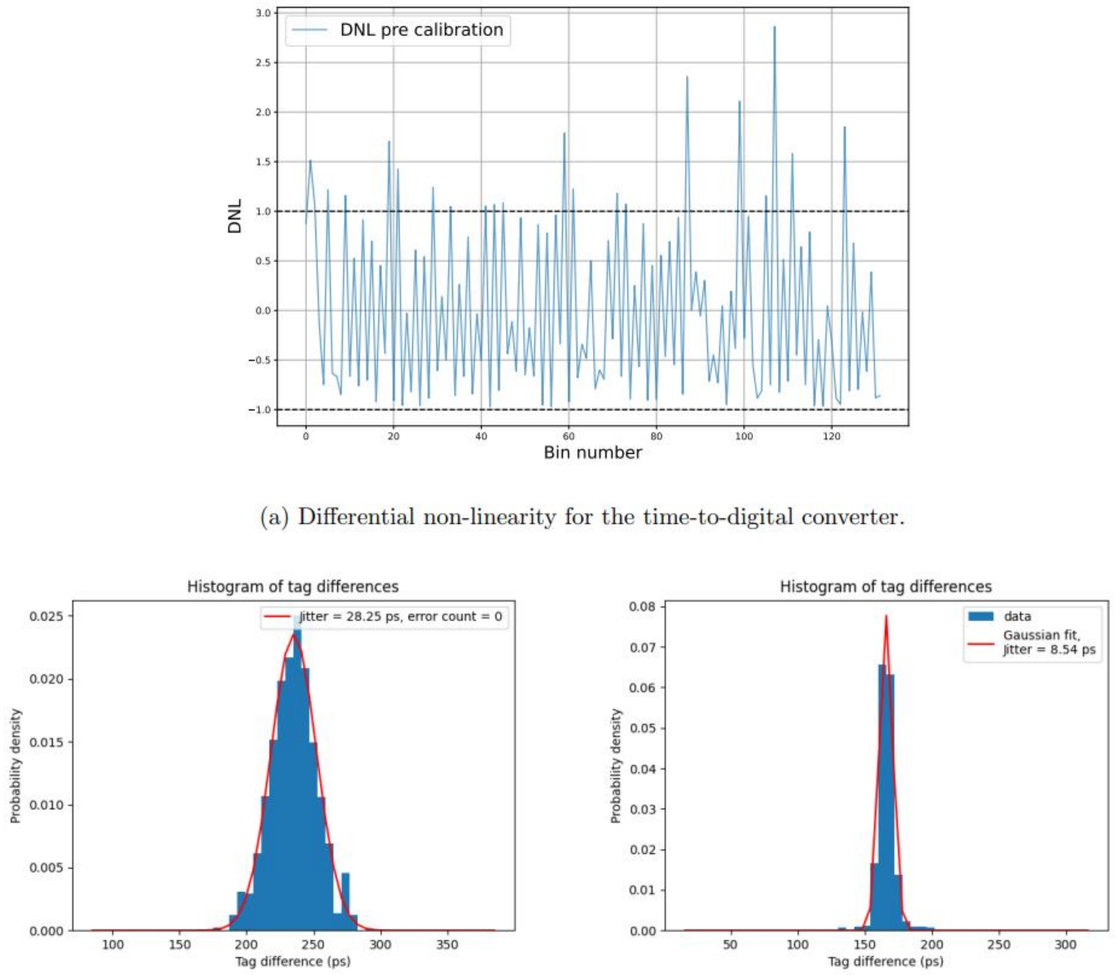


Figure 1: From the left we have a system-on-a-chip (SoC) and a laser that is connected to the source realized with two iPOGNACs (highlighted in red). iPOGNACs are composed of a half wave plate (HWP), a beam splitter (BS), a polarization beam splitter (PBS), and a phase modulator (ϕ-Mod). The first iPOGNAC projects its polarization into a polarizer (POL) through a sequence of mirrors (M). The source is then connected in free-space to the receiver (highlighted in blue), which splits the incoming qubits into two bases with a BS and projects them with a cascade of quarter-wave plate (QWP), HWP, and PBS. The signal is finally injected into fiber injectors (FI) after passing through a filtering stage (FLT) and reaches the detectors (D).

The orchestration of the electronic signals that trigger the laser pulser and the modulator control signals is governed by a system-on-a-chip (SoC) incorporating a field-programmable gate array (FPGA) and a CPU. For the 795 nm source, this system was hosted on a Zed board by Avnet, and the control signals were amplified using the TB-509-84+ and TB-410-84+ from Mini Circuits. For the 1550 nm source, the Zed board was replaced with an Ultra scale ZCU102+ by Xilinx, and the amplifiers replaced by the DR-VE-10-MO, DR-DG-20-MO and DR-PL-20-MO, all by iXblue. The ZCU104 is equipped with a number of transceiver channels capable of sending information at 16 Gbps, which will allow for future improvements in the repetition rate of the system. On that same note, the amplifiers are capable of reaching higher output voltage, and have a higher bandwidth, thus allowing the future increase in repetition rate. Some experimental results are shown in Fig. 2 and 3.

Lastly, I'm working on the development of a polarization-time bin hyper entangled source and receiver, together with a novel way to measure Bell inequalities for time-bin states. We expect that both of these works will lead to publications in high impact journals.



(a) Differential non-linearity for the time-to-digital converter.

(b) Jitter of ∼ 28 ps obtained for the time-to-digital converter using a Zedboard development board.

(c) Jitter of ∼ 8.5 ps obtained for the time-to-digital converter using a ZCU104 development board.

Figure 2: Results obtained for the FPGA-based time-to-digital converter.

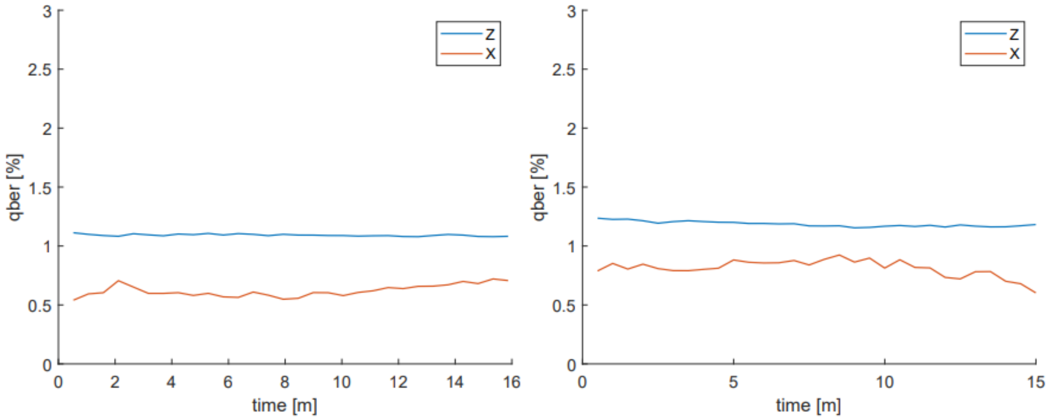


Figure 3: QBERs of the quantum source at 795 nm (on the left) and 1550 nm (on the right).

Publications:

- Berra F., Agnesi C., Karakosta-Amarantidou I., Avesani M., Bolaños M., De Toni A., Stanco A., Picciariello F., Vedovato F., Laurenti N., Villoresi P., Vallone G., “High speed source for satellite quantum key distribution”. IAC2023, Baku, Azerbaijan, 1-7 October 2023.
- F. Berra, M. Bolaños, C. Agnesi, M. Avesani, A. Stanco, G. Vallone, P. Villoresi, “Quantum Key Distribution at 1 GHz and time-tagging system development”, 108a Reunión Anual de la Asociación de Física Argentina, 19th to the 22nd of September, 2023.

Project of Doctoral Candidate 9, Javier Rey, University of Leeds.

CONTRACT STARTING DATE: 01/05/2023.

SUPERVISORS: Razavi (ULEEDS), Indjin (ULEEDS), Munro (NTT), Walter (RUB), Shabani (Cisco).

PROGRESS and RESULTS:

Here we give a brief overview to the scientific progress of the project “Trust-free packet-switched quantum communications networks”, up to the end of 2023. Moreover, below we describe how such progress relates to work package 2 (WP2).

Background:

The existence of the future quantum Internet, a global network of interconnected quantum de- vices, requires long-distance quantum communication to be possible among its users. Almostall current quantum communication schemes require photonic transfer, where the probabilityof receiving a photon decreases quadratically with distance for a free-space link (e.g. satellital communication) and exponentially for transmission over optical fiber. To allow for reliable communication, long links must be split into smaller segments connecting intermediary nodes. Early experimental implementations of quantum networks use trusted nodes as their intermediary devices [1, 2]. This approach introduces several security risks, as the users must not only believe that the trusted nodes will not have malicious intent, but also that they are safe from malicious third-parties. Whilst some proposals mitigate this vulnerability by using disjoint paths with limited information [3], the trusted node solution is in general not scalable. Instead, trust-free quantum communication requires the implementation of devices called quantum repeaters.

There exist several types of quantum repeater schemes. Nevertheless, in our project we are interested in those technologies that can be implemented in the near to mid-term future. There- fore, we will skip over the so-called third generation of quantum repeaters [4], including one-way

and all-photonic [6] repeaters, as these schemes require a large amount of physical resources and have very high technological demands that cannot be fulfilled by current or near-future technology. Thus, we will mainly focus on the first and second generation of quantum repeaters, which are generally based on the idea of entanglement distribution. That is, entanglement is generated probabilistically between neigh boring pairs of devices and then the generated elementary links are connected, typically using entanglement swapping [7], to obtain end-to-end entanglement.

Many protocols for entanglement distribution over quantum networks have been proposed over the last years, and most of those protocols apply a connection-oriented approach. That is, a connection is first established between the users, allocating the resources of the nodes in the pathbefore starting entanglement distribution. These resources are then locked away from the rest of the user in the network until the distribution has finished. This approach is similar to thatof circuit switching in classical communications, which we know was later superseded by packet switching. Since it is expected that the future quantum Internet will be integrated with current infrastructure, we are interested in finding new repeater protocols that not only allow for better resource utilization, but also are more in line with the packet-switched paradigm underlying to the Internet protocols.

Packet switching in quantum networks

While the differences between circuit switching and packet switching are quite clear in classical networks, several of their core features are harder to apply in the case of quantum communications. For example, the idea behind circuit switching is that, after a connection has been established and the resources have been allocated, the users can communicate as if connected by a simple wire. This means that the throughput and latency are constant, and no control information needs to be sent with the data. However, because the repeater schemes that we are focusing on rely on probabilistic operations, it is not possible to guarantee constant performance parameters, and due to the stateful nature of entanglement, some control information (e.g. qubits where stored, estimated fidelity...) is always needed, albeit it is exchanged through the underlying classical network and not through the quantum channel itself. In the case of packet switching, even some conceptual differences appear, like the definition of the packet asa data unit, i.e. a carrier of information. Strictly speaking, the entanglement being distributed does not carry any information, and is instead only a resource that the end-to-end applicationwill use to exchange or process information (e.g. through quantum teleportation). Furthermore, each packet is supposed to contain common control information, but as we explained earlier, eachentanglement pair requires its own control data to be maintained. Therefore, it may be more correct to think of every distribution request as its own packet, where the control information is sent through classical channels.

As a first step towards applying the ideas from packet switching to quantum networks, it is clear that core concepts about switching techniques must be revisited. To this effect, we review the literature and come up with a classification for switching strategies in entanglement-based networks, shown in fig. 4a. This classification focuses mainly in the existence, or not, of a connection establishment phase prior to the start of the distribution. Moreover, those schemes that do include this phase, which we refer to as connection-oriented, can be of unbounded or boundedcircuit. In an unbounded circuit, similarly to classical circuit switching, the resources in thepath are allocated from the start of the distribution until its end, while in bounded circuits, the actions to be delivered by each node are negotiated before distribution starts. An example of thisconcept of bounded circuit can be seen in [8], where a failure in connecting two entangled pairs

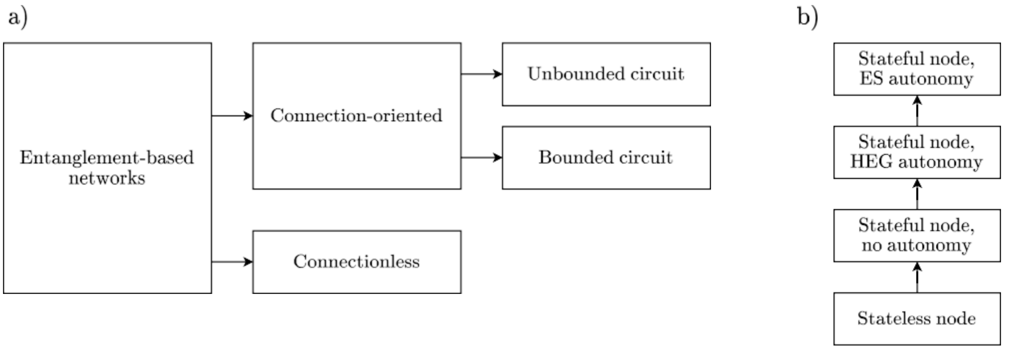

a)
Entanglement-based networks
Connection-oriented
Unbounded circuit
Bounded circuit
Connectionless
b)
Stateful node, ES autonomy
Stateful node, HEG autonomy
Stateful node, no autonomy
Stateless node

Figure 4: Summary of the work in reviewing the types of quantum networks. a) Switching techniques in networks based in entanglement distribution. b) Node classification based on autonomous capabilities.

leads to the distribution up to that point being scrapped and, in turn, a renegotiation of the connection. As opposed to connection-oriented communication, connectionless communication does not need a previous coordination between the nodes in the path, but instead relies on each node doing its best to service each request when it can. This approach is similar to datagram- based packet switching in classical networks, which is indeed the technology upon which the Internet is implemented. A key difference is that, instead of store-and-forward, the main mechanism here is store-and-swap, meaning distribution is neither directional nor necessarily orderly. Unfortunately, the storage of quantum states is a complex issue and has to deal with quantum decoherence, which is part of the reason why these types of networks are not favored with respect to connection-oriented ones, where the expected quantum storage time is much more manageable.

Another result of the literature review included in this task is the identification of the levelsof functionality that a node can have in a quantum network. These levels are shown in fig. 4b, and range from a completely clueless node with no memory management module (which we call stateless node), to nodes capable of generating link-level entanglement on their own (heralded entanglement generation autonomy) and even connecting these link-level entangled pairs (entanglement swapping autonomy).

Design of a connectionless protocol

Given the results of the task described in the previous section, we focus then on verifying the advantage of connectionless repeater schemes in terms of resource utilization. While some articles have come out in the last few months [9, 10] concerning this topic, the state-of-the-art is still ina very preliminary phase. Following the insight from out literature review, we attempt to take advantage of the increased resource optimization characteristic of packet-switched approaches, while also keeping in mind that entanglement distribution is not necessarily orderly, and in facta strictly sequential distribution (like that in [9, 10]) can lead to high latencies and, ultimately,to quantum decoherence.

Thus, we design our connectionless protocol, currently under testing and revision, with the main idea of allowing nodes in the projected path to start accumulating resources in advance. That is, while state-of-the-art protocols only communicate a request to a node when it is already entangled with the source of the request, our scheme can give previous notice so that the nodes can use already available resources if no other request takes priority. The intuition is that oncea node performs entanglement swapping, it has already fulfilled its function for the distribution, so it makes sense that we would allow this for low-traffic states of the network where the node may have a lot of free resources.

To verify the performance of our designed protocol, we will run simulations on the software SimQN [11], and compare the results with those recorded in the literature for other connectionlessprotocols, as well as for connection-oriented schemes. As we said, we expect our protocol to be superior in low-traffic environments, as long as we assume that the elementary entangled links can be connected through deterministic entanglement swapping. Otherwise, the connection- oriented approach should prove more performant in large networks, as it allows for nesting of the probabilistic connections, resulting in less retries on average.

Future work

In the following months, we aim to:

- Complete the analysis of the designed protocol through simulations.
- Incorporate better error models for the entanglement connection step in the simulation. In particular, we would like to model the connection from the perspective of an encoded repeater [12, 13].
- Compile the results and conclusions to publish a conference paper before the end of year 1 of the PhD.
- Exploit the new insights to study the possibility of a new low-level repeater protocol that is more suited for connectionless communication.

References:

[1] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The security on quantum key distribution network in Vienna” New Journal of Physics, vol. 11, p. 075001,jul 2009.

[2] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, ŽeljkoSamec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, “A trusted node free eight user metropolitan quantum communication network”, Science Advances, vol. 6, no. 36, p. eaba0959, 2020.

[3] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, “Security of trusted repeater quantum key distribution networks”, J. Comput. Secur., vol. 18, p. 61–87,jan 2010.

[4] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, “Inside quantum repeaters”, IEEEJournal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 78–90, 2015.

[5] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, “Quantum communication without the necessity of quantum memories”, Nature Photonics, vol. 6, pp. 777–781, Nov 2012.

[6] K. Azuma, K. Tamaki, and H.-K. Lo, “All-photonic quantum repeaters”, Nature Communications, vol. 6, p. 6787, Apr 2015.

[7] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: The role of imperfect local operations in quantum communication”, Phys. Rev. Lett., vol. 81, pp. 5932–5935, Dec 1998.

[8] W. Kozlowski, A. Dahlberg, and S. Wehner, “Designing a quantum network protocol”,in *Proceedings of the 16th International Conference on Emerging Networking Experimentsand Technologies*, CoNEXT ’20, (New York, NY, USA), p. 1–16, Association for Computing Machinery, 2020.

[9] H. Choi, M. G. Davis, lvaro G. Iñesta, and D. R. Englund, “Scalable quantum networks: Congestion-free hierarchical entanglement routing with error correction”, 2023.

[10] Z. Xiao, J. Li, K. Xue, Z. Li, N. Yu, Q. Sun, and J. Lu, “A connectionless entanglement distribution protocol design in quantum networks”, *IEEE Network*, pp. 1–1, 2023.

[11] L. Chen, K. Xue, J. Li, N. Yu, R. Li, Q. Sun, and J. Lu, “Simqn: a network-layer simulatorfor the quantum network investigation”, *IEEE Network*, pp. 1–8, 2023.

[12] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, “Quantum repeater with encoding”, *Phys. Rev. A*, vol. 79, p. 032325, Mar 2009.

[13] Y. Jing, D. Alsina, and M. Razavi, “Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective post selection tool”, *Phys. Rev. Appl.*, vol. 14, p. 064037, Dec 2020.

Project of Doctoral Candidate 10, Loïc Millet, IDquantique.

CONTRACT STARTING DATE: 01/01/2024.

SUPERVISORS: Boso (IDQ), Bussières (IDQ), Zbinden (UG), Curty UV), Diamenti (SU)

PROGRESS AND RESULTS:

There is no scientific progress yet of this doctoral candidate as he has started his project on January 2024.

Project of Doctoral Candidate 11, Vaisakh Mannalath, University of Vigo.

CONTRACT STARTING DATE: 17/03/2023.

SUPERVISORS: Curty (UVIGO), Razavi (ULEEDS), Azuma (NTT), Tamaki (UT), Majenz (DTU).

PROGRESS AND RESULTS:

Enhancing Satellite QKD: Channel Modeling and Key Rate Calculation

In a first task, we explore the cutting-edge domain of satellite quantum key distribution (QKD), focusing specifically on the utilization of geostationary satellites for long-distance secure communication. The primary objective is to develop a refined channel model for satellite-based QKD, addressing key challenges such as noise and losses within the communication channel. Through extensive literature review and analysis, we identify diffraction losses as the principal contributor to channel loss, followed by other atmospheric effects. The study concentrates on downlink configurations to mitigate turbulence-related losses prevalent in uplink scenarios. A significant aspect of this research involves examining noise impacts, particularly those resulting from the reflection or albedo of the sky, which is pertinent for ground-based receivers.

Additionally, we strive to enhance the key rate generation in QKD protocols, using the decoy state BB84 as the foundational model. By integrating tighter bounds on statistical fluctuations and employing linear programming methods, we achieve a more precise estimation of the secret key rate. This includes the adoption of tighter concentration inequalities, building upon previous research to obtain higher secret key rates. The synergy of an accurate channel model and robust key rate estimation is pivotal in understanding the relationship between the secret key rate and various operational parameters, such as the availability andoptimization of onboard random numbers essential for protocol execution. This research contributes to the advancement of satellite quantum communication, presenting novel methodologies and findings that have significant implications for the futureof secure, long-distance communication.

Background

Quantum Key Distribution (QKD) has emerged as a groundbreaking technology in the realm of secure communication, leveraging the principles of quantum mechanics to enable the exchange of cryptographic keys with provable security [1]. The BB84 protocol, a cornerstone in QKD, allows two parties to communicate securely, even in the presence of a potential eavesdropper [2]. However, the terrestrial implementation of QKD faces significant challenges, primarily due to the physical limitations of fiber-optic cables which restrict the communication range [3].

Satellite-based QKD

The advent of satellite-based QKD offers a solution to this limitation, enabling long-distance secure communication [4]. Geostationary satellites, positioned approximately 35,786 kilometers above the Earth’s equator, present a viable platform for global-scale QKD. These satellites, due to their fixed position relative to the Earth, offer a stable link for continuous communication, making them ideal for establishing a global quantum communication network. This advanced framework for global quantum communication is further complemented by the pioneering satellite-based QKD experiments conducted by the group led by Jian-Wei Pan [5], which have been instrumental in demonstrating the practical feasibility and robustness of such systems.

Problem Statement

Despite its potential, satellite-based QKD is not without challenges. One of the main issues is the accurate modeling of the communication channel. Various factors, such as atmospheric conditions, satellite altitude, and experimental parameters, contribute to signal loss and noise, which can significantly impact the efficiency and security of the QKD protocol [6]. Additionally, the generation of secure keys at a viable rate remains a challenge, especially considering the large losses and noises in the satellite channel and the limitations of onboard resources such as random number generators.

Objectives

This research aims to address these challenges through two primary objectives:

<u>Developing an Accurate Channel Model</u>: By conducting an extensive literature survey and analyzing the satellite channel's characteristics, this study aims to develop a comprehensive model that accurately represents the noise and loss factors in geostationary satellite-based QKD.

<u>Enhancing Key Rate Generation</u>*:* Focusing on the decoy state BB84 protocol,the study seeks to improve the key rate generation by implementing tighter bounds onstatistical fluctuations and employing linear programming methods for a more precise secret key rate estimation.

APPROACH

Development of the Channel Model

- **Literature Survey and Analysis**: Conducted a comprehensive review of literature from the past decade focusing on satellite communication channel models. This involved comparing various models and methodologies, analyzing research based on consensus in the field, and evaluating the complexity and effectiveness of each model.
- **Modeling Atmospheric Effects**: Investigated techniques for modelling atmospheric losses, crucial in geostationary satellite communication. The study included an analysis of models suitable for downlink configurations in geostationary satellites andevaluated the relative impact of various atmospheric effects.
- **Noise Analysis**: Focused on analysing and modelling background noise in the protocol, with special emphasis on the impact of sky reflection on communication channels.

Enhancing Key Rate Generation

- **Literature Survey and Analysis**: Engaged in a detailed study of prior research to pinpoint optimal concentration inequalities suitable for bounding statistical fluctuations in satellite QKD. Special focus was directed towards scenarios with small block lengths, which are particularly relevant in the context of satellite QKD.
- **Linear Programming Methods**: Utilized linear programming techniques for the calculation of the secret key rate. This approach offered distinct advantages over traditional analytical methods, providing more precise and efficient key rate estimations.
- **Adapting Tighter Concentration Inequalities**: Focused on adapting and refining

tighter concentration inequalities from existing research to enhance key rates. Key steps in the derivation of these inequalities were scrutinized and improved upon to optimize their applicability in satellite QKD scenarios.

RESULTS AND DISCUSSION

Channel Model Development

- **Findings on Channel Characteristics**: In the context of geostationary QKD using downlink, it was found that turbulence effects are negligible, with diffraction losses emerging as the most significant factor. Additional effects such as atmospheric absorption, cloud cover, and atmospheric refraction were also identified and incorporatedinto the channel model. Noise analysis was conducted, taking into account the timing of key generation and employing noise mitigation techniques.
- **Comparison with Existing Models**: Improvements were made to the modeling of effects such as atmospheric absorption and refraction to enhance physical real- ism. This led to a channel model that is more accurate and reflective of real-world conditions compared to existing models.
- **Implications for Satellite QKD**: The refined channel model enables a more accurate prediction of the feasibility of satellite QKD. This includes considerations of the zenith angle of the satellite, the location of the ground receiver, and temporal factors such as the time of day and year.

Key Rate Generation Enhancement

- **Impact of Tighter Concentration Inequalities**: The modification of concentration inequalities led to an increase in key rates, particularly noticeable in scenarioswith higher channel loss and when dealing with smaller block sizes. This adjustment proves crucial in enhancing the efficiency of satellite QKD under challenging conditions.
- **Impact of Linear Programs**: The integration of linear programming, in tandem with the modified concentration inequalities, resulted in tighter and more accurate key rate estimates compared to traditional analytical methods. This highlights the effectiveness of linear programming in refining the key rate calculations.
- **Optimization of Variables**: Analysis of the onboard random number generation rate was conducted by varying the number and biases of the decoy intensities. Optimal values for these variables were found to be dependent on specific loss and noise regimes. The results indicate that practical satellite QKD experiments could benefit from minimal modifications to existing protocols, improving key rates effectively.

Summary of Contributions:

Developed an improved channel model for geostationary satellite-based QKD, considering factors like atmospheric losses and noise effects.

Enhanced key rate estimates through the integration of tighter concentrationinequalities and linear programming methods.

Conducted a comparative analysis with traditional methods, demonstrating noticeable improvements in various loss and noise conditions.

Optimized variable selection, specifically in terms of onboard random number

Funded by
the European Union

generation rates and decoy intensities, tailored to specific loss and noise regimes for practical satellite QKD applications.

Discussion of Limitations:

- The study's channel model might require further refinement to include additional atmospheric conditions or to account for dynamic satellite movement, in the case of low earth orbit satellites.
- Further experimental validation in real-world satellite QKD scenarios would strengthen the applicability of the findings.
- While the optimization of intensities and their probabilities demonstrated effectiveness, it requires ongoing refinement, based on the channel conditions. The feasibility of such precise adjustments in practical scenarios, given the current state of technology, remains a subject for further exploration.

CONCLUSION

The research has successfully developed an advanced channel model for geostationary satellite-based Quantum Key Distribution (QKD), providing a more accurate representation of diffraction losses and atmospheric effects. This achievement marks a significant step in enhancing the reliability and accuracy of satellite QKD systems. Additionally, the study introduced tighter statistical bounds and linear programming methods for key rate generation, substantially improving upon traditional analytical methods. These enhancements were particularly effective when applied to the decoy state BB84 protocol, resulting in a more secure and efficient system overall. Another notable advancement is the optimization of onboard random number generation, which optimizes the use of decoys and maximizes key rates, addressing one of the critical challenges in satellite QKD implementation.

We are currently writing a paper with this results.

REFERENCES

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Reviews of Modern Physics, vol. 81, p. 1301–1350, Sep 2009.Ç

[2] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol,"Physical Review Letters, vol. 85, p. 441–444, Jul 2000.

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realisticdevices," Reviews of Modern Physics, vol. 92, May 2020.

[4] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," npj QuantumInformation, vol. 3, Aug 2017.

[5] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen,

[6] S. Han, Y. Qing, K. Liang, F. Zhou, X. Yuan, M. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, and W. Liu, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature, vol. 589, p. 214–219, Jan 2021.

[7] H.-f. Chou, V. N. Ha, H. Al-Hraishawi, L. M. Garces-Socarras, J. L. Gonzalez-Rios, J. C. Merlano-Duncan, and S. Chatzinotas, "Satellite-based quantum network: Security and challenges over atmospheric channel," 2023.

PUBLICATIONS:

- Mannalath, "Multiparty Entanglement Routing in Quantum Networks", Quantum Technologies for Young Researchers Workshop held at Instituto de Química Física Blas Cabrera (IQF-CSIC) in Madrid from 4-7th July, 2023.