74th International Astronautical Congress (IAC), Baku, Azerbaijan 1-7 October 2023.

IAC-23,B2,3,4,x77635

High-speed source for satellite quantum key distribution

Federico Berra[a], Costantino Agnesi[a], Ilektra Karakosta-Amarantidou[a], Marco Avesani[a], Matías Bolaños[a], Alberto De Toni[a], Andrea Stanco[a], Francesco Picciariello[a], Francesco Vedovato[a, b], Nicola Laurenti[a], Paolo Villoresi[a, b], Giuseppe Vallone[a, b, c]

[a] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*
[b] *Padua Quantum Technologies Research Center, Universita degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*
[c] *Dipartimento di Fisica e Astronomia, Universita degli Studi di Padova, via Marzolo 8, IT-35131 Padova, Italy*

Abstract

Quantum key distribution (QKD) is a technique used to establish a secure communication channel between two parties, known as Alice and Bob. The security of QKD is based on the principles of quantum mechanics, which allow for the creation of a shared secret key that cannot be intercepted by an eavesdropper, known as Eve. The shared secret key can then be used to encrypt and decrypt messages sent between Alice and Bob. QKD is a promising technology for secure communication because it offers unconditional security, which means that the laws of physics guarantee the security of communication. This contrasts classical encryption methods, which rely on the computational difficulty of specific mathematical problems and can be theoretically broken with enough computing power. QKD is performed with an exchange of qubits that are typically encoded into single photon-level pulses that limit the maximum distance of communication in the terrestrial network. Satellite links could offer a solution to enable communication over long distances by taking advantage of the low attenuation of the free-space channel and satellite mobility. The aim of the QUANGO project is the design of a low-earth orbit constellation of 12U-CubeSats with combined capabilities for communication secured by QKD and 5G connection for the Internet of Things, as well as to develop payloads, subsystems, and ground stations for such a network and to determine the viability of its implementation. Within the project QUANGO, we report on the development of a high-speed breadboard-level QKD source realized up to TRL 4 to be evolved into a 3U engineering model, and an optical ground station with a 40 mm German mount telescope able to collect the optical signal with a pointing, acquisition and tracking system and analyze it through single-mode fiber injection. The source was developed in two different wavelengths compatible with the TELECOM standard: at 800 nm to reduce the divergence and at 1550 nm to enable daylight communication. Both sources were realized with an iPOGNAC-based modular scheme that simplified their development, testing, and qualification, especially for space missions. All the components used for their realization were space-COTS to reduce space qualification costs.

Keywords: QKD, Optical, Quantum, Communication, CubeSat.

1. Introduction

The significance of ensuring that information is shared in our society in a reliable and secure way cannot be overstated. In this context, two cutting-edge technologies have emerged, namely 5G [1] and Quantum Key Distribution (QKD) [2]. QKD makes it possible for two parties to exchange cryptographic keys while maintaining an unconditional degree of security. These technologies are now being explored for application in contemporary communication networks due to their strategic relevance. Furthermore, to attain comprehensive network coverage, the integration of satellites becomes essential. In January 2021, as part of the Horizon 2020 Research and Innovation initiative of the European Union, the QUANGO project [3], short for "QUANtum and 5G cOmmunication", has embarked on a goal to conceptualize and prototype crucial components for satellite communication for these two technologies.

In this project, the spacecraft is designed to accommodate a pair of interrelated payloads: a software-defined radio payload, meticulously optimized for seamless 5G Internet of Things (IoT) operations, and a QKD/Optical payload. A critical mission of the QKD/Optical payload is to forge a direct optical quantum communication channel between the satellite and a designated ground station. Meanwhile, the 5G IoT payload takes charge of orchestrating data exchange comprising the QKD post-processing phase, while also taking on the pivotal role of establishing the required radio connection. In addition to its crucial role in QKD services, the 5G IoT payload also

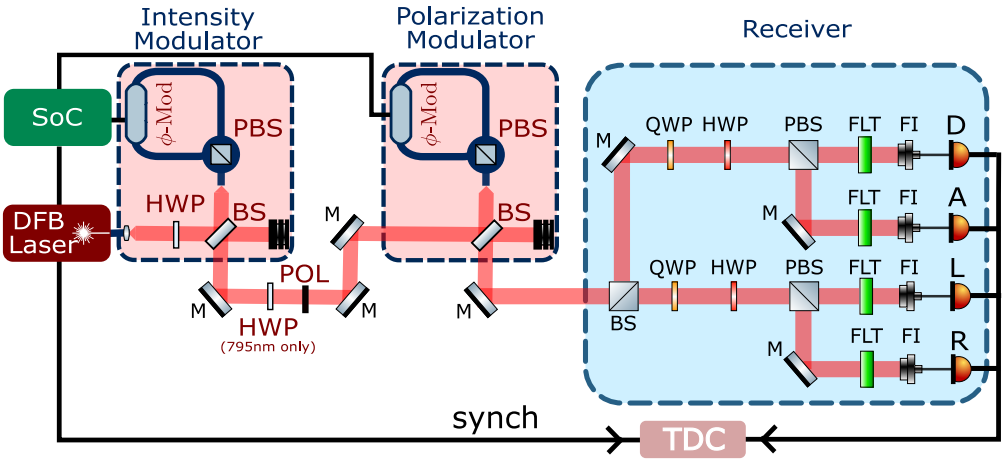

Fig. 1. From the left we have a system-on-a-chip (SoC) and a laser that is connected to the source realized with two iPOGNACs (highlighted in red). iPOGNACs are composed of a half waveplate (HWP), a beam splitter (BS), a polarization beam splitter (PBS), and a phase modulator (ϕ-Mod). The first iPOGNAC 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-waveplate (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).

serves as a bridge connecting energy-efficient and cost-effective ground-based IoT devices to satellite-based IoT connectivity services with its communication secured by QKD.

The implementation of a quantum payload presents a complex endeavor fraught with various difficult challenges. The challenge of mitigating losses constitutes a prominent issue within the domain of QKD, exerting a pronounced influence on both the efficacy and security of the protocol. In the context of QKD, information is encoded within the quantum states of individual photons. These photons, as they traverse the communication channel connecting the sender and receiver, are susceptible to attenuation or loss, resulting in the nonreceipt of a fraction of photons by the intended recipient. Losses present an impediment in the realm of QKD when juxtaposed with classical communication. This is primarily due to two overarching considerations. Firstly, the inability to bolster the signal's intensity arises from the inherent design of quantum communication, which necessitates operation at the single-photon level. Secondly, a pivotal tenet of quantum communication security, the no-cloning theorem, precludes the replication or regeneration of the quantum signal. The advent of a high-frequency Gigahertz (GHz) source emerges as a partial panacea to alleviate these losses. While some proportion of photons might be lost, the heightened emission rate of photons within the GHz regime compensates for this detriment. Consequently, an adequate number of photons ultimately traverse the communication channel and reach the receiver. This fortitude in the face of channel losses serves to maintain a commensurately reasonable key generation rate, thereby preserving the overarching efficacy of the QKD protocol.

In this paper, we explain the design of the sources for the project operating at two distinct wavelengths, namely 795 nm and 1550 nm. These sources were tested through the development of two corresponding receivers (state analyzers). The initial emphasis was on the development of the 795-nm variant, as detailed in the literature [4, 5], laying the foundation for subsequent advancements in this project to reach the GHz regime. Then, our efforts shifted towards the refinement of individual components, with a particular focus on the 1550 nm version. This pursuit was motivated by the objective of optimizing the source's performance parameters, thereby facilitating operation within the GHz frequency range.

2. Setup

2.1 Sources

We realized a QKD source scheme capable of implementing the three-state one-decoy BB84 protocol [6] 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 (Fig. 1). This scheme was implemented with two gain-switched PM fiber-coupled distributed feedback lasers at different wavelengths to test its robustness: the Eagleyard 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 [7] 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 [8]. 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 $\mathcal{Z} = \{|0\rangle, |1\rangle\}$, where $|0\rangle := |L\rangle$ and $|1\rangle := |R\rangle$, alongside the control basis $\mathcal{X} = \{|+\rangle, |-\rangle\}$, where $|+\rangle := |D\rangle$ and $|-\rangle := |A\rangle$.

To ensure the appropriate pulse intensities of signal ($\mu \approx 0.6$) and decoy ($\nu \approx 0.2$), a variable optical attenuator was used. Following this, the light was directed to the quantum receiver using a free-space channel.

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 [9]. For the 795 nm source, this system was hosted on a Zedboard by Avnet, and the control signals were amplified using the TB-509-84+ and TB-410-84+ from MiniCircuits. For the 1550 nm source, the Zedboard was replaced with an Ultrascale ZCU104+ 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 bandwith, thus allowing the future increase in repetition rate.

2.2 State analyzer

To measure the incoming states, we developed a quantum receiver capable of measuring the states of both the key generation and control basis (Fig. 1). The incoming polarization-encoded light pulses are first sent through a 30/70 beamsplitter, where each pulse is randomly sent to one of two branches. Each of the branches works as a projective measurement on one of the two bases (key generation and control). To perform the said projective measurement, a half-waveplate and a quarter-waveplate were introduced to rotate the incoming states ($|A\rangle$ and $|D\rangle$ for the control basis and $|L\rangle$ and $|R\rangle$ for the key generation basis) into the rectilinear basis, thus mapping $|D\rangle$ ($|L\rangle$) $\rightarrow |H\rangle$ and $|A\rangle$ ($|R\rangle$) $\rightarrow |V\rangle$. After rotation, the states are sent through a polarization beamsplitter, which transmits all $|V\rangle$ states and reflects all $|H\rangle$ states. The output states of each branch's PBS are then sent through a filtering stage, to be detected by a single photon detector.

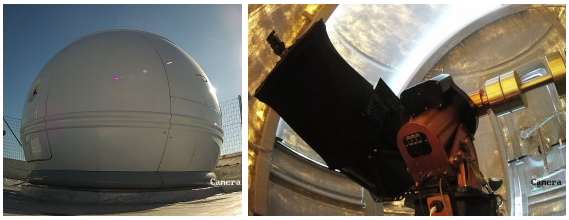

Fig. 2. Pictures of the GaliQEye observatory in Padova.

2.3 Optical Ground Station

QUANGO uses the GaliQEye observatory of the Department of Information Engineering of the University of Padova as the optical ground station (OGS) to collect and measure qubits coming from the CubeSat. The OGS is equipped with a Ritchey-Chrétien F/8 telescope with a primary mirror of 40 cm (model: PRO-RC400 by Officina Stellare, 42% linear obstruction due to the secondary mirror), a German equatorial mount (GEM, model: Paramount MEII by Software Bisque) with subarcsecond resolution, absolute on-axis encoders, and the capability of tracking low-earth orbit satellites and a dome of 3 m of diameter (model: ScopeDome 3M by ScopeDome). The observatory control software is *TheSkyX professional* by Software Bisque, on top of which we have developed in-house routines to improve the tracking capabilities. The telescope has been equipped with a 600 mm $\times$ 600 mm mechanical breadboard mounted on the back of the primary focus. Two pictures of the GaliQEye observatory are presented in Fig. 2.

We developed a pointing, acquisition, and tracking (PAT) system composed of two further subsystems, the PAT-Coarse and the PAT-Fine units. The PAT-Coarse is in charge of the raw pointing of the telescope and it is based on the optical feedback provided by a coarse camera (7 mrad of field-of-view) to the GEM to correct for the pointing uncertainty due to the two-line elements of the orbiting terminals. The PAT-Fine unit is in charge of the injection of the QKD signal at 1550 nm into a single-mode fiber [10] and exploits a two-stage Adaptive Optics (AO) system that uses a fast steering mirror (FSM) in a closed loop with a position-sensitive detector and a deformable mirror in a closed loop with a Shack–Hartmann wavefront sensor. The optical feedback to the AO system is provided by the beacon at 850 nm coming from the CubeSat. The single-mode fiber that contains the QKD signal is then connected to the state analyzer. The PAT-Coarse unit and the FSM stage have been tested during the night by exploiting the Sunlight reflected by orbiting terminals, such as the International Space Station, attest-

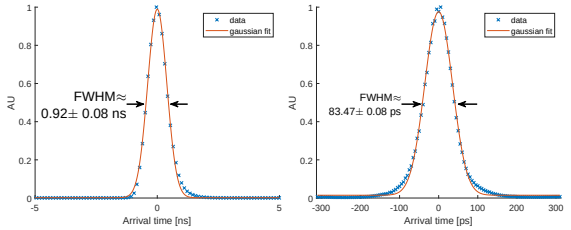

Fig. 3. Optical pulses peak generated by the quantum source at 795 nm (on the left) and 1550 nm (on the right).

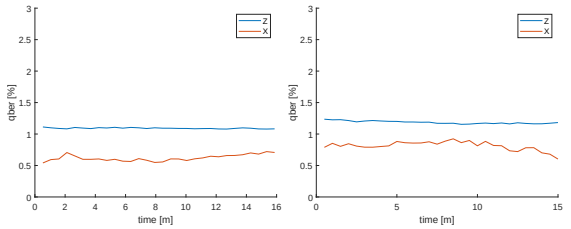

Fig. 4. QBERs of the quantum source at 795 nm (on the left) and 1550 nm (on the right).

ing to a residual pointing error of the order of 10 μrad. The AO system has been tested under laboratory conditions by exploiting a turbulence simulator based on the usage of a rotating phase plate (by Lexitek).

3. Results

To increase the performance of QKD systems and target high (1 GHz) repetition rates, the fidelity of shared quantum states becomes crucial. Analyzing the pulse shape allows researchers to identify distortions and performances of the entire chain from the transmitter to the receiver, which could compromise the data fidelity and trigger higher error rates. By ensuring a well-defined narrow pulse shape, QKD systems can maintain low error rates, which are essential for secure high-speed communication. Although they share the same design, the two sources have completely different implementations, particularly from the bandwidth perspective. To show the difference between two bandwidths, the normalized histogram of detection was calculated while sending a 50 MHz train of pulses from the source. The result is depicted in Fig.3. Being the first developed, the 795-nm source reaches a FWHM of 0.92 ± 0.08 ns limited by the bandwidth of the FPGA and the laser, and the $\approx$ 100 ps jitter of the SPADs. The second, which completely replaces the electronic chain with a higher band one, improves the performance to a FWHM of 83.47 ± 0.08 ps, where the residual error is mainly due to the jitter of the SNSPDs of ≈ 35 ps.

To evaluate the discrepancy between the expected and the actual states of qubits, we measured the Quantum Bit Error Rate (QBER). High QBER values indicate the presence of errors, either due to noise or interference, which can compromise the security and accuracy of quantum communication protocols. The QBERs for the two sources were evaluated using a sequence of 1024 symbols transmitted at a frequency of 50 MHz. The probability distribution for the transmission of states was 70% for base Z and 30% for base X, while a decoy ratio of approximately 3 was chosen. To replicate the standard duration of a low-earth orbit satellite pass, a 15-minute experiment duration was selected [11]. For both sources, we obtain an average QBER of $Q^Z_{795} = 1.09 \pm 0.01\%$, $Q^X_{795} = 0.62 \pm 0.05\%$, $Q^Z_{1550} = 1.19 \pm 0.02\%$, and $Q^X_{1550} = 0.81 \pm 0.07\%$ as shown in Fig.4.

4. Conclusions

The performance of the two sources of quantum key distribution examined in this study has been highly promising. With a remarkably low QBER of approximately 1%, these sources demonstrate their robustness and reliability in secure communication applications.

Furthermore, the pulse width observed in the 1550 nm source has great potential for achieving high bandwidth performance. This characteristic opens up exciting possibilities for achieving modulation at gigahertz (GHz) frequencies, which is a significant leap forward in the field of QKD. Such a high-speed modulation capability could pave the way for more efficient and faster quantum communication systems, enhancing the practicality and versatility of QKD technology.

5. Aknowledgment

This work was supported by the European Union's Horizon 2020 research and innovation programme, project QUANGO (grant agreement No 101004341) and by MIUR (Italian Minister for Education) under the initiative "Departments of Excellence" (Law 232/2016).
I. K. A. acknowledges funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 956071 AppQInfo - Applications And Hardware For Photonic Quantum Information Processing.

6. References

[1] Joern Krause Patrick Merias. *Study on Narrow-Band Internet of Things (NB-IoT) / enhanced Machine Type Communication (eMTC) support for non-terrestrial networks (NTN)*. Tech. rep. 3GPP A Global Initiative, June 2021.

[2] S. Pirandola et al. "Advances in quantum cryptography". In: *Adv. Opt. Photonics* 12.4 (Dec. 2020), pp. 1012–1236. ISSN: 1943-8206. DOI: 10.1364/AOP.361502.

[3] Pino. *Quango*. [Online; accessed 13. Sep. 2023]. Mar. 2023. URL: https://quango.dei.unipd.it.

[4] Federico Berra et al. “Modular source for near-infrared quantum communication”. In: *EPJ Quantum Technol.* 10.1 (July 2023), pp. 1–12. ISSN: 2196-0763. DOI: 10.1140/epjqt/s40507-023-00185-y.

[5] Federico Berra et al. “Synchronization of quantum communication over an optical classical communication channel”. In: *arXiv* (June 2023). DOI: 10.48550/arXiv.2306.17603. eprint: 2306.17603.

[6] Fadri Grünenfelder et al. “Simple and high-speed polarization-based QKD”. In: *Appl. Phys. Lett.* 112.5 (Jan. 2018), p. 051108. ISSN: 0003-6951. DOI: 10.1063/1.5016931. URL: http://aip.scitation.org/doi/10.1063/1.5016931.

[7] Marco Avesani et al. “Stable, low-error, and calibration-free polarization encoder for free-space quantum communication”. In: *Opt. Lett.* 45.17 (Sept. 2020), pp. 4706–4709. DOI: 10.1364/OL.396412. URL: http://ol.osa.org/abstract.cfm?URI=ol-45-17-4706.

[8] Davide Rusca et al. “Finite-key analysis for the 1-decoy state QKD protocol”. In: *Appl. Phys. Lett.* 112.17 (Apr. 2018), p. 171104. ISSN: 00036951. DOI: 10.1063/1.5023340. URL: https://doi.org/10.1063/1.5023340.

[9] Andrea Stanco et al. “Versatile and Concurrent FPGA-Based Architecture for Practical Quantum Communication Systems”. In: *IEEE Trans. Quantum Eng.* 3 (2022), p. 6000108. DOI: 10.1109/TQE.2022.3143997.

[10] Alessia Scriminich et al. “Optimal design and performance evaluation of free-space Quantum Key Distribution systems”. In: *Quantum Science and Technology* 7.4 (2022), p. 045029.

[11] Sheng-Kai Liao et al. “Satellite-to-ground quantum key distribution”. In: *Nature* 549.7670 (Aug. 2017), pp. 43–47. ISSN: 0028-0836. DOI: 10.1038/nature23655. URL: http://www.nature.com/doifinder/10.1038/nature23655.