# QUANGO: a CubeSat platform for quantum key distribution and 5G IoT connectivity service

Federico Berra[1], Andrea Stanco[1], Costantino Agnesi[1], Marco Avesani[1], Francesco Vedovato[1], Nicola Laurenti[1], Roberto Corvaja[1], Stefano Tomasin[1], Ignacio López Grande[2], Valerio Pruneri[2,9], Marco Guadalupi[3], Josep Ferrer[3], Ramon Ferrús[3], Alessandro Francesconi[4], Francesco Sansone[4], Edoardo Birello[4], Giulia Tollero[4], André Xuereb[5], Noel Farrugia[5], Johann A. Briffa[6], Alessandro Balossino[7], Danilo Sarica[7], Eleni Diamanti[8], Matteo Schiavon[8], Paolo Villoresi[1], Giuseppe Vallone[1]

[1]*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*
[2]*ICFO, Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels, Barcelona, Spain*
[3]*Sateliot, Carrer Berlin 61, 08029, Barcelona, Spain*
[4]*Stellar Project, Viale dell'Industria 60, 35129, Padova, Italy*
[5]*Department of Physics, University of Malta, Malta*
[6]*Department of Communications and Computer Engineering, University of Malta, Malta*
[7]*Argotec Srl, Via Cervino 52, 10155, Torino, Italy*
[8]*Sorbonne Université, 4 place Jussieu, 75005, Paris, France*
[9]*ICREA-Institucio Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain*

*Abstract*—**This paper provides an overview of the QUANGO project funded by the European Union. It presents the preliminary design considerations of the mission, the platform, and the payloads that have been developed. QUANGO envisages the design of the key elements of a satellite mission aiming at delivering both satellite 5G IoT and Quantum Key Distribution (QKD). These are implemented by using a constellation of CubeSats operating in low earth orbit. After detailing the phases required for a satellite-to-ground QKD, the paper focuses on the QKD post-processing through the 5G IoT channel and its impact on satellite operations.**

*Index Terms*—**3GPP, 5G, CubeSat, IoT, Post-Processing, QUANGO, Quantum Key Distribution, Satellite**

## I. Introduction

The secure and reliable exchange of information plays a crucial role in our society. In this regard, 5G and Quantum Key Distribution (QKD) [1], which allows two parties to share cryptographic keys with unconditional security [2], are strategic technologies seeing widespread adoption in modern communication networks. Furthermore, to achieve global network coverage the use of satellites is mandatory. All this considered, the QUANGO - cubesat for QUANtum and 5G cOmmunication - project aims at designing and prototyping the key elements of a satellite mission that targets the delivery of both satellite 5G IoT and QKD services, by exploiting a constellation of CubeSats that operate in low earth orbit. The project started in January 2021 under the Europe (EU) Horizon 2020 Research and Innovation program, can pave the way for novel satellite resource-sharing and optimization by integrating quantum-based secure communication with 5G communication.

The envisioned spacecraft will carry two interconnected payloads: a QKD/Optical payload and a software-defined radio 5G IoT payload. The QKD/Optical payload implements a direct-to-Earth optical quantum link between the satellite and a ground station, while the 5G IoT payload provides the radio link required to handle the data exchange for QKD post-processing. In addition to QKD services, the 5G IoT payload is also used for the delivery of satellite IoT connectivity services to low-power and low-cost IoT devices on the ground, by using the Release 17 NB-IoT NTN protocol [3] being standardized by 3GPP in the context of 5G systems.

The integration of these two payloads is expected to reduce the cost of both QKD and satellite 5G IoT services by sharing the satellite infrastructure. Moreover, it will allow for parallel development and improvement of these two technologies. The integration of the two systems allows for easier cross-modules development for a better and more integrated ecosystem.

The project is being developed by a consortium of European universities, research centers and small medium enterprises (SME) with a strong heritage and expertise in quantum cryptography, optical communication, micro-satellites development, and 5G networks. After a brief overview of the QUANGO project with a description of preliminary design considerations of the mission, the platform, and the payloads, this contribution will focus on a detailed presentation of the phases needed to realize a QKD protocol between a satellite and a ground station. The paper will also analyze and discuss the impact of the QKD implementation on the standard satellite operation schedule.

## II. Satellite Design

The considered spacecraft platform is a 12U CubeSat, which hosts two payloads: a 5G IoT payload, and a secure communication system based on quantum state transmitter to realize a prepare-and-measure QKD protocol with a ground station [4], [5]. Fig. 1 shows the unit allocations for each subsystem: pointing-acquisition and tracking, QKD source, 5G IoT, and platform (electrical power, altitude and orbital control, on-board computer, thermal control, wiring).

The QKD subsystem is able to implement an efficient version of the BB84 protocol [6] encoded by exploiting the polarization degree of freedom targeting 1 GHz repetition rate.

The pointing subsystem is able to produce an optical beam with a half-divergence angle lower than 30 $\mu$rad. 5G will operate in the frequency band around 2GHz with less than 10W of transmitted power.

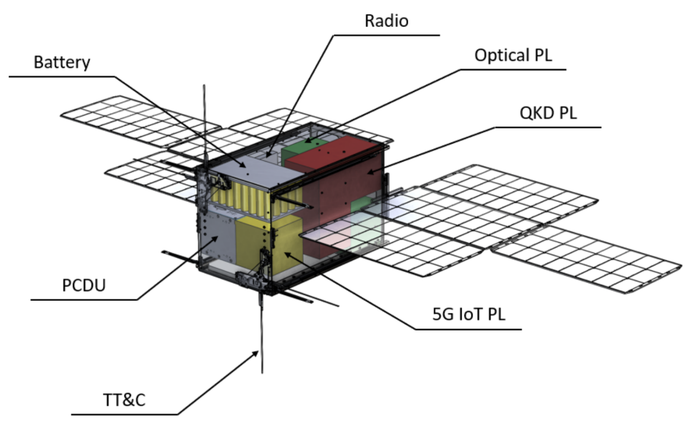

Fig. 1. The qualitative picture shows the unit allocations for each subsystem in the QUANGO satellite, which are: QKD payload (3U), optical payload (3U), 5G IoT payload (1U), and platform (5U). One unit (1U) of volume corresponds to a cube with a standard size of $10cm \times 10cm \times 10cm$. Some of the elements of the platform that are visible in the rendering are: Power Conditioning and Distribution Unit (PCDU), Telemetry, Tracking, and Command (TT&C), battery, solar panels, and chassis.

The function of the 5G IoT payload is two-fold: on the one hand, this payload is used to offer narrow-band IoT non-terrestrial network (NB-IoT NTN) connectivity services; on the other hand, this payload supports the operation of the QKD subsystem by providing the radio link needed for the realization of the QKD protocol. Fig. 2 provides an illustration of the two types of services being delivered by the proposed CubeSat design: 5G IoT connectivity and QKD.

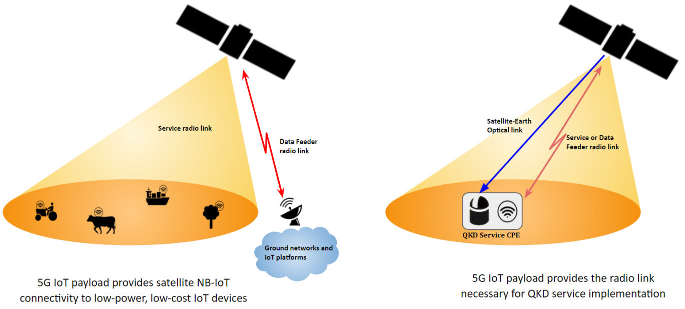
Service radio link
Data Feeder radio link
Ground networks and IoT platforms
5G IoT payload provides satellite NB-IoT connectivity to low-power, low-cost IoT devices
Satellite-Earth Optical link
Service or Data Feeder radio link
QKD Service CPE
5G IoT payload provides the radio link necessary for QKD service implementation

Fig. 2. Services provided with QUANGO CubeSat: NB-IoT connectivity and QKD.

## III. QKD PHASES

As shown in Fig. 3, in order to share a secret key between the satellite (Alice) and a ground station (Bob) several phases should be implemented. The timeline (from top to bottom) is divided into phases marked with a double dashed line: Idle, Qubit request, Qubit exchange, Sifting, Parameter estimation, Error correction, Privacy amplifications, and Key manager storage. These phases are designed to provide a full modularity thanks to a temporally disconnected scheme. Therefore, they can be carried out during different satellite passages while a single phase must be processed within the same passage. Each phase is structured with *states* (blue rectangles) and *communications* (arrows). The phases are described in the following.

*Idle*. In this phase, both Alice and Bob are in Idle state. They perform no operations and consequently they minimize their energy consumption.

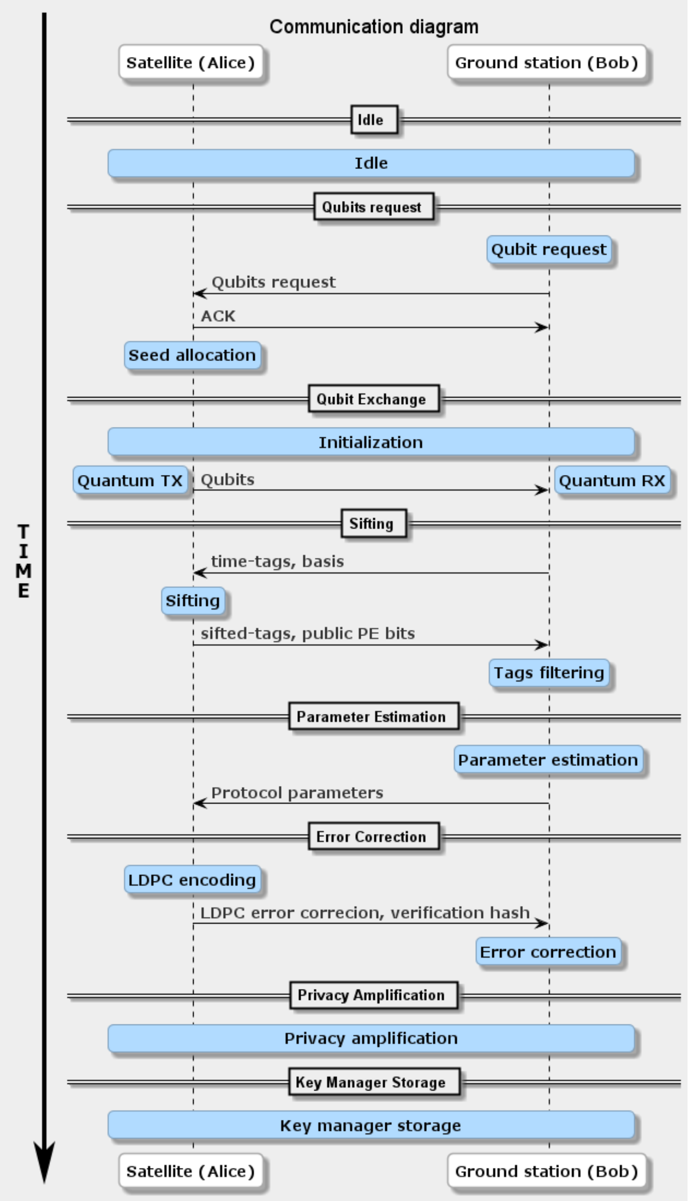

Fig. 3. Sequence time diagram of QKD phases of the communication between the satellite and the ground-station. The only phase involving the quantum optical transmission is the “Qubit Exchange” phase where the comprising the two states quantum transmission (TX) and reception (RX), all others use radio frequency (RF) classical communication.

*Qubit request.* The QKD communication occurs after the ground station request for a qubit exchange. This exchange can have various modalities: sending public qubits, sending a fixed state at maximum power, or sending a true random sequence to generate a key. If the satellite is available for the qubit exchange in the requested passage (see next phase), then Alice responds with a (logical) acknowledgment to Bob’s request.

*Qubit exchange.* Before the actual communication, Alice and Bob will have to initialize their instrumentation and make a preliminary optical alignment. After that, Alice can proceed to send the qubits to Bob. Then she will save the sequence of sent qubits. The sequence qubits must be stored up the key management storage phase. Notice that the post-processing phases can be performed after merging the data of several satellite passages.

From this step on, all the phases are organized in order to minimize the exchange of messages between Alice and Bob and, therefore, the communication delay.

*Sifting*. Bob will communicate to Alice the time-tags of the received qubits, also including the information on his bases choice. By doing this, Alice will be able to perform the sifting and to send the list of sifted-tags to Bob. A part of them will be made public for the next parameter estimation phase. Once Bob receives this message, he will filter his tags. The length of the sifted-tags string is order of magnitude smaller than the length of the sequence generated by Alice. The reason for this is that all the qubits lost in the transmission are discarded, as the propagation losses range from 20 dB to 60 dB based on several parameters: satellite position, atmospheric conditions, transmitter aperture, and ground receiver aperture. The full calculation for the estimation of the parameters can be obtained through proper channel models such as the ones presented in [7]–[10].

*Parameter estimation*. Now that Bob has all the data, he can estimate all the parameters needed to evaluate the key rate, starting from the quantum bit error rate (QBER). Here, Bob can decide to abort the communication or to communicate the necessary parameters to Alice to perform the subsequent error correction.

*Error correction*. In this phase, the error correction will be provided by a low-density parity-check (LDPC) algorithm. As a matter of fact, LDPC can provide a higher efficiency with respect to CASCADE [11] or WINNOW [12], approaching the channel Shannon limit. Moreover, being a Forward Error Correcting code, it does not require an iterative communication between the two parties, which is expensive in this scenario [13]. To maximize the performances it will be necessary to choose an adequate matrix $H$ for each communication. This will optimize the trade-off between sharing a low number of parity bits, to minimize the information revealed, and sharing enough bits to complete the corrections. To achieve this, rate-adaptive methods can be employed [13]. At this point, Alice will send Bob the syndrome along with a hash for error verification. Then, Bob will have to perform reconciliation. Direct reconciliation has been chosen since the LDPC decoder, which is computationally and power demanding, is more conveniently implemented at the ground side. In the same phase, Field Programmable Gate Array (FPGA) will append some seeds to the message that will be used to select the privacy amplification matrix.

*Privacy amplification*. Privacy amplification is the process of distilling secret keys from partially compromised data. Based on the measured parameters, the length of the secure key can be evaluated. The secure key is obtained by applying a suitable almost universal-two hashing function, such as a Toeplitz matrix to the keys obtained after error correction [14], [15].

*Key manager storage*. In this last phase, both partners will save the key in their key manager.

## IV. Choices impacting the concept of operations

In the QUANGO project, the protocol chosen for the implementation of QKD is an efficient version of the BB84, which is encoded by exploiting the polarization degree of freedom [6]. In this protocol, the qubit sequence is generated by modulating 3 (or 4) different polarizations and 2 (or 3) levels of intensity. The number of polarizations and levels of intensity depends on the chosen physical source implementation. In the most general case, two bits are needed to determine the polarization and two bits to determine the intensity. The repetition rate of the QKD source is set at 1 GHz: this implies an input stream of at least 4 Gbps random bits. For example, for 15 min of communication the bit sequence should be:

$$l_{bits} = R \cdot (b_{pol} + b_{int}) \cdot t_{com} = 3.6[Tb]$$

where the rate is $R = 1[Gbps]$, the bit for the polarizations and the intensity are $b_{pol} = b_{int} = 2$, and the communication duration is $t_{com} = 15[min]$.

A Quantum Random Number Generator (QRNG) must be used for the generation of such random and private bits. The required generation rate have been demonstrated with continuous-variable QRNG [16].

It is worth noting that the qubit exchange must be synchronized: the synchronization can happen in real-time or in post-processing. The synchronization is necessary to correctly correlate the transmitted and received signals and to filter temporally the signal from the noise.

Two system's trade-offs have impacts on CONcept of OPerationS (CONOPS):

1) The choice between a true 4 Gbps QRNG and a Pseudo-Random Number Generator (PRNG) with a QRNG seed;
2) The choice between a real-time post-processing and delayed post-processing.

The impact of the above choices is analyzed below.

**1A. True 4 Gbps QRNG**: It is necessary to develop a real-time QRNG with a generation rate greater than 4 Gbps by exploiting an FPGA technology [17]. Alternatively, it is possible to place in parallel many QRNGs with lower rates. Using several QRNGs can cause an increase in weight and power consumption, and it also requires a proper management procedure on the FPGA to handle the multiple streams.

**1B. 4 Gbps PRNG seeded by QRNG**: In this case, the Gbps random sequence is obtained by a PRNG with a seed generated by a QRNG with a lower rate. This is the simplest solution in terms of implementation. Note that in this case, it is possible to store the seed (small sequence) or the PRNG data (large sequence). In the case of real-time sifting, it could be convenient to store the PRNG data, and this has no impact on the data rate required on the radio link. With delayed post-processing, it is convenient to memorize only the seed. In this second case, additional computing power during sifting is required (i.e. recalculate the PRNG output starting from the seed). With PRNG the security is slightly lower, while Cryptographically Secure PseudoRandom Number Generator (CSPRNG) may increase security.

**2A. Real-time post-processing**: This requires real-time qubit synchronization between satellite and ground station. For example, this synchronization could be done using a qubit-based clock recovery approach (such as the Qubit4Sync method [18]) or by modulating a beacon laser sent from the Satellite to the ground station (like in the Micius demonstration [19]). Real-time synchronization can include a small latency (of the order of tens of seconds) between the qubit transmission and the post-processing. In this case, the two phases “Qubit exchange” and “Sifting” will be overlapped. The estimated data rate for real-time sifting (uplink communication) is about 50 times the qubit detection rate [20].

Due to the whole system losses ranging from 20 dB to 60 dB, according to the specific implementation, the qubit detection rate ranges from few kHz up to few MHz. The estimated data rate for error correction and privacy amplification is at least 10 times lower than the sifting one, and it is typically in the downlink. In this case, the satellite does not need to store all the random streams, but only the data accumulated in the latency between qubit transmission and sifting. For example, with 4 Gbps true random stream and 10 s of latency, the memory on the satellite should be at least 4 Gbit/s × 10 s = 40 Gbit.

**2B. Delayed post-processing**: In this case, the post-processing is performed after the end of the satellite passage over a ground station (say A). It is worth noting that a generic public authenticated communication is needed for the post-processing. No specific security requirements are needed on the generic public authentication communication. The two end-points of the "generic public authenticated communication" are the QKD payload on the satellite and the QKD ground receiver. Therefore, the post-processing could be performed by exploiting a direct communication between the satellite and a different ground station (say B) that forwards the information to the original ground station A via a public authenticated communication channel. Here, the qubit synchronization is realized in post-processing by exchanging the time of arrival of the qubits. The advantages of this solution are the following:

- no need for any real-time synchronization,
- no need for radio and optical communication at the same time,
- a lower classical data-rate compared to the real-time post-processing of the case 2A.

Disadvantages: It is required to memorize the full random stream or all the used seeds in a given passage.

## V. Conclusions

After the first year and half of the project, QUANGO completed the design of the 12U satellite and the payloads, including the optical payload, the quantum payload, and the 5G IoT payload. The development of the payloads has started and preliminary tests have already been performed to check the behavior of the physical elements from their theoretical counterparts extracted from the design. The study of the mission using 5G and QKD technologies together in a CubeSat constellation leads us to define the phases required to realize satellite-based QKD protocols. It also allows us to analyze possible mission alternatives and how they impact on the operations of the satellite.

## Acknowledgment

This work was supported by the European Union's Horizon 2020 research and innovation programme, project QUANGO (grant agreement No 101004341).

## References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. P1, pp. 7–11, Dec 2014. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2014.05.025

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.81.1301

[3] J. K. Patrick Merias, "Study on narrow-band internet of things (nb-iot) / enhanced machine type communication (emtc) support for non-terrestrial networks (ntn)," 3GPP A Global Initiative, Tech. Rep., Jun 2021.

[4] C. Agnesi, F. Vedovato, M. Schiavon, D. Dequal, L. Calderaro, M. Tomasin, D. G. Marangon, A. Stanco, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, "Exploring the boundaries of quantum mechanics: advances in satellite quantum communications," *Philos. Trans. Royal Soc. A*, vol. 376, no. 2123, p. 20170461, May 2018. [Online]. Available: https://doi.org/10.1098/rsta.2017.0461

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, no. 4, p. 1012, Dec 2020. [Online]. Available: https://www.osapublishing.org/aop/abstract.cfm?doi=10.1364/AOP.361502

[6] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," *Appl. Phys. Lett.*, vol. 112, no. 5, p. 051108, Jan 2018. [Online]. Available: http://aip.scitation.org/doi/10.1063/1.5016931

[7] A. Scriminich, G. Foletto, F. Picciariello, A. Stanco, G. Vallone, P. Villoresi, and F. Vedovato, "Optimal design and performance evaluation of free-space quantum key distribution systems," *accepted for publication in Quantum Science and Technology; pre-print at arXiv:2109.13886*, 2021. [Online]. Available: https://arxiv.org/abs/2109.13886

[8] S. Pirandola, "Satellite quantum communications: Fundamental bounds and practical security," *Phys. Rev. Research*, vol. 3, p. 023130, May 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevResearch.3.023130

[9] C. Harney and S. Pirandola, "Analytical methods for high-rate global quantum networks," *PRX Quantum*, vol. 3, p. 010349, Mar 2022. [Online]. Available: https://link.aps.org/doi/10.1103/PRXQuantum.3.010349

[10] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, "Finite key effects in satellite quantum key distribution," *npj Quantum Information*, vol. 8, no. 1, p. 18, Feb 2022. [Online]. Available: https://doi.org/10.1038/s41534-022-00525-3

[11] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," 1993.

[12] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, no. 5, p. 052303, May 2003.

[13] D. Elkouss, J. Martinez-mateo, and V. Martin, "Information reconciliation for quantum key distribution," *Quantum Info. Comput.*, vol. 11, no. 3, p. 226–238, mar 2011.

[14] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5524–5535, aug 2011. [Online]. Available: https://doi.org/10.1109%2Ftit.2011.2158473

[15] C.-H. F. Fung, X. Ma, and H. F. Chau, "Practical issues in quantum-key-distribution postprocessing," *Phys. Rev. A*, vol. 81, p. 012318, Jan 2010. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.81.012318

[16] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 gbps," *Nature Communications*, vol. 9, no. 1, dec 2018. [Online]. Available: https://doi.org/10.1038%2Fs41467-018-07585-0

[17] A. Stanco, F. B. L. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, and P. Villoresi, "Versatile and concurrent fpga-based architecture for practical quantum communication systems," *IEEE Transactions on Quantum Engineering*, vol. 3, no. 6000108, pp. 1–8, 2022.

[18] L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, and G. Vallone, "Fast and simple qubit-based synchronization for quantum key distribution," *Phys. Rev. Applied*, vol. 13, p. 054041, May 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.13.054041

[19] S.-K. Liao and et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Aug 2017. [Online]. Available: http://www.nature.com/doifinder/10.1038/nature23655

[20] N. Walenta, a. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New Journal of Physics*, vol. 16, no. 1, p. 013047, jan 2014.