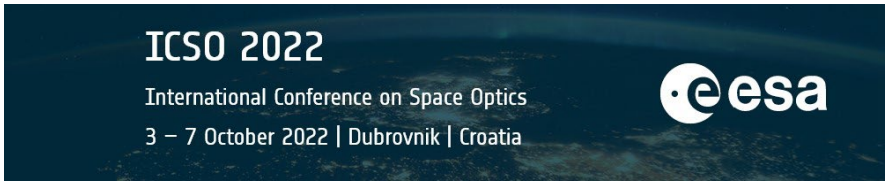
# International Conference on Space Optics—ICSO 2022

Dubrovnik, Croatia

3–7 October 2022

*Edited by Kyriaki Minoglou, Nikos Karafolas, and Bruno Cugny,*




# *Space infrastructures for Quantum-Safe Secure Communications: Technologies, Roadmap and Initiatives from an industrial standpoint*


International Conference on Space Optics — ICSO 2022, edited by Kyriaki Minoglou, Nikos Karafolas, Bruno Cugny, Proc. of SPIE Vol. 12777, 1277733 · © 2023 ESA and CNES · 0277-786X · doi: 10.1117/12.2690327

# Space infrastructures for Quantum-Safe Secure Communications: Technologies, Roadmap and Initiatives from an industrial standpoint

G. Riccardi*[a], M. Ottavi†[a], A. Geraldi[a], L. Bruno[a], N. Scaiella, P. Conforto[a], A. Pisano[a]
[a]Thales Alenia Space – Italia, Via Saccomuro, 24, 00131 Rome, Italy
*gabriele.riccardi@thalesaleniaspace.com
†martina.ottavi@thalesaleniaspace.com

## ABSTRACT

Quantum Key Distribution (QKD) is currently the only known technique that is able to guarantee information-theoretic secure communications. While many countries have already started developing use-cases based mostly on terrestrial links, the high losses that afflict fiber-based channels make them unsuitable for very-long-distance communications. Taking the quantum networks to a national and global scale thus requires the use of satellite-based quantum communications, as the attenuation experienced by photons in space communications is order of magnitudes lower than the one that characterizes terrestrial networks. Thales Alenia Space in Italy (TAS-I) is positioning itself as a key actor in the development of the technology needed to perform space quantum communications. In this work, we present an overview of the initiatives that are currently being carried out by TAS-I, and define a roadmap whose steps are planned to take the current laboratory experimentation towards the development of a fully operational QKD constellation meant to provide secret keys on a global scale. We also describe a possible implementation of an Italian demonstrator mission based on a LEO satellite that acts as a trusted node to distribute shared keys among a certain number of ground stations; we study the effects of some major system choices and assess the overall achievable performance in terms of Secret Key Volume (SKV).

**Keywords:** QKD, Quantum Communications, Optical Communications, Space Communications

## 1. INTRODUCTION

The continuous increase in the amount of digital communications, vulnerable to hacking and data breaches, calls for the rise of a secure worldwide quantum network. The safety guaranteed by most of today's public-key cryptographic schemes relies in fact on the computational complexity of solving specific problems (such as the factorization of extremely large numbers), and will be exposed to the advent of quantum computers.

Quantum communications, on the other hand, rely on the fundamental principles of quantum physics, and allow the transmission and storage of information in an intrinsically secure way. They can thus ensure a transition towards next-generation telecommunication systems whose security is not endangered by future quantum computers.

The most mature quantum-based technique is Quantum Key Distribution (QKD), which relies on the exchange of qubits (usually in the form of optical signals) between two distant parties to allow the generation of a secure common key, that can then be used to encrypt their communication using a classical symmetric cryptographic algorithm.

The topic of QKD has been deeply studied by the academic quantum information community from both theoretical and experimental sides. In the former case, efforts have been steered not only into finding new protocols [1, 2, 3] but also into looking for smart and efficient solutions to known quantum attacks [4, 5]. In the latter case, many different technologies have been demonstrated to be suitable for QKD purposes, as for instance polarization-encoded pulsed laser or high performance quantum dots [6,7,8,9,10].

Nevertheless, despite the high number of terrestrial experimental demonstrations, only a low number of them has been brought to the commercial step and an even lower number has been tested for space missions. A pioneering work in this perspective is represented by the QUESS mission [11, 12], consisting of a satellite containing a quantum source which has been able to survive the launch and operate in the harsh spatial environment.

On the governmental side, several countries have already started developing use-cases based mostly on fiber-optic links, but the high losses that afflict these kinds of channel make them unfeasible for very-long-distance communications. Taking the quantum networks to a national and global scale thus requires the use of satellite-based quantum communications, as

the attenuation experienced by photons in space communications is orders of magnitude lower than the one that characterizes terrestrial networks.

In this paper, we present the Thales Alenia Space in Italy (TAS-I) roadmap for Quantum Communications and describe the main activities that are being carried out, including the realization of a quantum optics laboratory and the development of a software tool to accurately model the free-space channel and analyze end-to-end satellite-based QKD missions.

These steps are both crucial in the definition of an Italian demonstrator mission and in the expansion to a fully operational QKD constellation.

## 2. THALES ALENIA SPACE ITALIA ACTIVITIES AND ROADMAP

Current QKD Systems place themselves in a rapidly growing market, where many entities are concurring to develop fully integrated and secure QKD infrastructures.

Above all industrial players, the European Commission has launched an initiative called Union Secure Connectivity: a European space-based Connectivity System set to provide secure communication services to the EU and its Member States as well as broadband connectivity for European citizens, commercial enterprises and public institutions. It is also meant to provide global coverage for rural and 'not-spot' areas, complementing Copernicus and Galileo.

In the frame of such study, another European Commission initiative named "EuroQCI" has been launched to build a secure quantum communication infrastructure that will span the whole EU, including its overseas territories.

The 27 EU Member States who signed the EuroQCI agreement are working with the European Commission and the European Space Agency (ESA) to design, develop and deploy the EuroQCI with the target of having it fully operational by 2027.

In coordination with the European Commission, ESA has launched the SAGA (Secure And cryptoGrAphic) mission, with the objective of designing and developing the EuroQCI space segment.

The two joint initiatives, SAGA and EuroQCI, will be able to provide cryptographic keys to protect communication systems of European institutions and critical infrastructures.

The ESA SAGA mission has concluded the phase A stage in July, where TAS-I has led one of the three consortia involved, and a prototype SAGA demonstrator is envisaged to be developed soon.

In the frame of these EC-led initiatives, several nations are starting to design their own national secured networks with the purpose of integrating them in the wider European scenario.

Thales Alenia Space in Italy, as large system integrator with a wide experience in telecommunication and security field, has intensively worked in the past years to build a Quantum Communications industrial competence centre in order to keep up with the most recent technology advancement and be in the position of a leading player in the development and deployment of a European constellation for secure communications.

With this purpose, a roadmap embracing Quantum technology, products and space and ground systems has been built aiming at supporting the potential deployment of a fully operational system capable of delivering QKD services to Italian European customers.

The identified building blocks constituting the roadmap towards a QKD operational system are the following:

- Building a quantum optics laboratory able to interface with a fiber-based terrestrial infrastructure. The lab is also being used to perform free-space quantum communication experiments, useful to gain insights into the propagation effects induced by the atmospheric channel on quantum signals.
- Developing a comprehensive software tool that, starting from orbital propagation and an accurate model of the free-space channel, allows to obtain a precise estimation of the achievable key rates in satellite-to-ground or ground-to-satellite quantum communications. The tool is designed to address scenarios involving satellites ranging from VLEO to GEO satellites and will allow the evaluation of the end-to-end performance of a satellite-based QKD system.

- Deploying a demonstrator mission, involving a single satellite meant to perform QKD with a limited number of optical ground stations. This mission will represent a pre-operational scenario; it will increase the TRL of the available QKD technologies and validate the selected QKD technology and protocols in space. It will also allow the acquisition of empirical data from quantum optical measurements.
- Expanding the mission to become a fully operational constellation, able to provide QKD services to a series of globally distributed optical ground stations, supporting European secure communication and also improving Europe's digital sovereignty and industrial competitiveness.

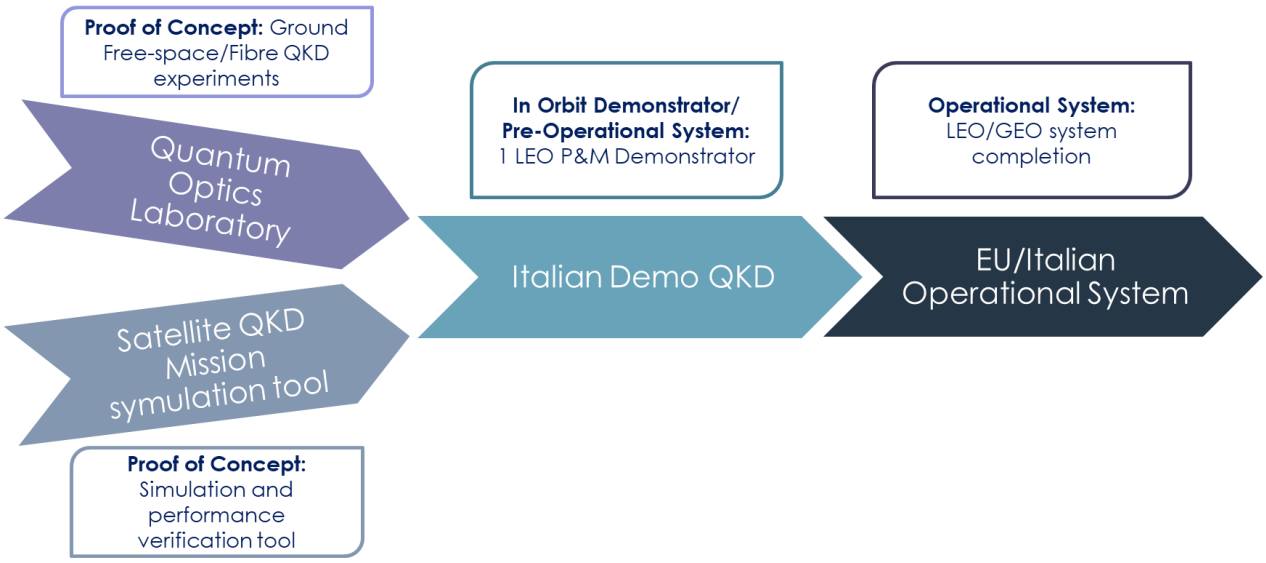



Figure 1. Thales Alenia Space Italia QKD Roadmap and Activities

In the following chapters the first three bullets are detailed as they constitute the fundamental bricks necessary to build a Quantum communications infrastructure but also stimulate the improvement of the current optical fiber terrestrial network that will need to be consolidated and expanded in order to support the deployment of a European and national system.

## 3. EXPERIMENTAL TESTBED: QUANTUM OPTICS LABORATORY

The large gap that exists between terrestrial and space QKD realizations has to be rapidly filled in order to deploy a fully operational space-based quantum communication network in the near future. To this aim, the capability to project, build and test the critical and innovative units of a cutting-edge-technology quantum payload, as well as the increase of the TRL value of such primitive units is of fundamental relevance. Such a task can be reached through an intense experimental activity envisioning a cutting-edge laboratory furnished with high-level and high-performing instrumentation.

By following this logic, TAS-I arranged a Photonic and Quantum Laboratory, which is envisioned to be at the core of several projects, not only on the quantum communication side but also on the classical one. We recently started experimental activities in both research fields with the aim of testing QKD protocols and technologies on one hand, and high-speed optical communications on the other. Within these topics, a particular attention is posed to the elements typical of a space-based mission as, for instance, efficiency and reliability of the instrumentation.

One of the main experiments that are currently being performed in our lab consists in the implementation of a free-space QKD link among two parties, A and B. The main aim of such experiment is to test the QKD protocols and technology in an environment with features analogues to the ones characterizing satellite based optical communication, as, for instance, high and time-varying losses.

The high-level scheme of the experiment is reported in Fig. 2.

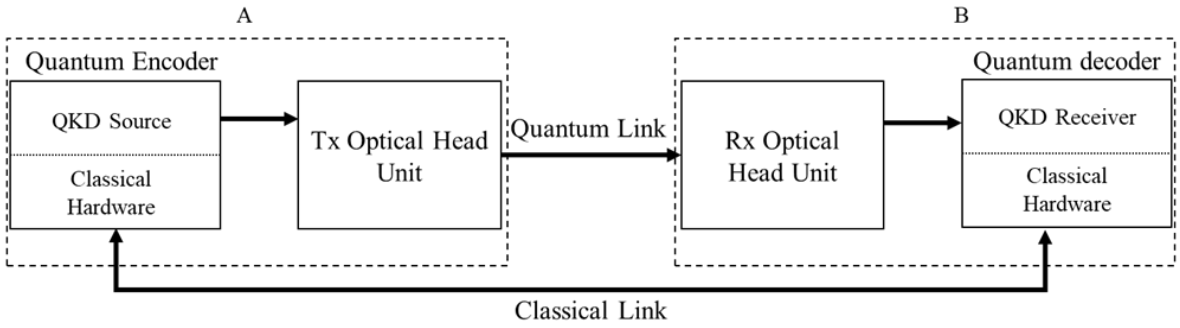



Figure 2. Block diagram of a free-space QKD experiment

The logical implementation consists of five building blocks which are typical of all the quantum optical links:

- Quantum Encoder: this comprehends the QKD source as well as the classical hardware (computer, time tagger, etc…) for synchronization and post processing purposes;
- Tx Optical Head Unit: consists of a motorized optical telescope intended to inject the quantum beam and the classical tracking one into the free space link;
- Optical link: this consists of any transmitting media between transmitter (A) and receiver (B) stations. In our case the link will be a free space one;
- Rx Optical Head Unit: consists of a receiving telescope furnished with an active tracking system able to follow the small misalignments due to atmosphere turbulence;
- Quantum Decoder: it comprehends to the QKD receiver as well as the classical hardware for synchronization and processing purposes.

The first step of the experiment corresponds to the implementation of a quantum communication link featured by a satellite losses simulator (SLS), based on a variable attenuator [13], able to reproduce the time behaviour of a the losses of a typical satellite pass. The obtained results are then used to refine the simulator output in a feedback fashion loop and validate its results. Moreover, a relevant problem that will be studied during this step corresponds to the pointing, acquisition and tracking (PAT) technique performances. Because of the very short time of a satellite pass, it is of fundamental relevance to minimize the time spent by the two nodes in this phase to maximize the time spent of the quantum communication.

The second step of the experiment consists in the implementation of a three node network, the two end users and an intermediate one, say C, which will play the role of a satellite trusted node. The node C is envisioned to complete the whole typical actions of a satellite based trusted node optically linked with the two end nodes.

The combined results of the two experiments will allow us to test 1) the capabilities of the source envisioned to be placed on board of a satellite, 2) the PAT algorithms that are considered preparatory to the ones used on board of a satellite and evaluate their performances and 3) the post-processing part of the protocol and optimize it for typical computing hardware on board of a satellite.

## 4. SATELLITE QKD MISSION SIMULATION TOOL

In the definition and design of an end-to-end System Architecture it is crucial to possess the correct tools to estimate the expected performances and correctly size the System. To this end, TAS-I is currently developing a software tool designed specifically to perform the analysis of a constellation of satellites establishing quantum links with optical ground station to provide QKD services on a regional or global area.

The software tool is meant to be used in the analyses of QKD constellations in which each satellite allows the generation of a common secure key between two ground stations, acting either as a trusted relay node (establishing, for example, two

individual satellite-to-ground quantum links to perform prepare-and-measure QKD protocols) or in an untrusted fashion, distributing pairs of entangled photons to two ground stations in simultaneous visibility of the satellite and using and entanglement-based QKD protocol.

In Fig.3, we present a block diagram showing the flow of operations performed by the software tool.

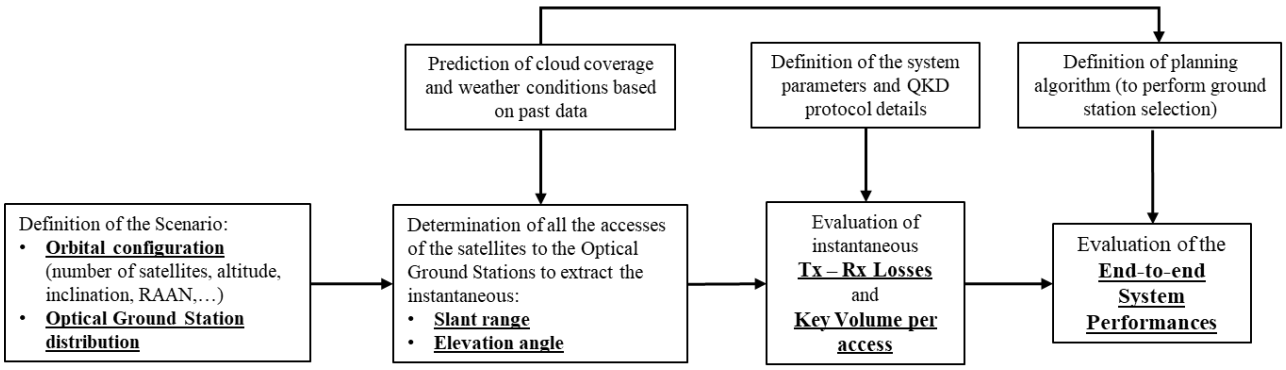



Figure 3. Functional Block diagram of the operations carried out by the simulation tool

More in detail, the software tool allows the user to:

- Define the complete scenario, including the characteristics of the optical ground stations and of the satellites building up the constellation. For each satellite, the main orbital parameters (such as orbit altitude and inclination, RAAN, true anomaly, etc.) can be selected by the user.
- Propagate the satellites to determine the accesses of the satellites with each optical ground station, accounting for the weather conditions retrieved from databases containing data collected from previous years (especially cloud coverage percentage). For each access, the slant range and the elevation angle of the satellite with respect to a certain ground station are extracted with a time definition that can be selected by the user (for example, every second).
- Evaluate the instantaneous channel losses, which, along with the knowledge of the main system parameters (such as apertures diameter, pointing performances, source and detector performances, etc.) and of the details of the employed QKD protocol allow to calculate the Secret Key Volume generated during each access.
- Define a planning algorithm, which optimizes the optical ground station selection mechanism (when more than one ground station are in the visibility of a satellite) and the QKD protocol selection (when two or more protocols can be performed). The planning algorithm shall perform the ground station selection accounting for the cloud coverage probability maps and on the individual key demand of each ground stations potentially determined by a traffic matrix.
- Evaluate the end-to-end performances of the system over a certain period, based on specific KPIs such as: overall and individual key volume, yearly access periods, weekly/monthly averages, revisit intervals (to monitor that no ground station is potentially left unserved for too many consecutive days), etc.

## 5. ITALIAN QKD DEMONSTRATION MISSION

The Italian QKD Demonstration Mission should be intended as a pre-operational System, the first actual step in the creation of an Italian domain of secure communications, and as such is meant to participate to the consolidation of the European Quantum Communication Infrastructure. In this respect, it aims to represent a huge step forward for Italian space market as it will allow to demonstrate and prove not only Italian technologies, but also an operational QKD service, capable of interfacing itself with the EuroQCI network both in space and on the ground.

Many potential users with interest in the development of a quantum-secure communication network have been identified, such as:

- Italian governmental and institutional users, (ASI – Italian Space Agency, Italian MoD, etc.);
- Research institutions and universities;
- Private organizations (NGOs and foundations, Banks, or Telecom companies).

The demonstrator mission shall be developed with the goal of validating in Space the selected QKD technology & protocol, as well as increasing the TRL of the developed products and demonstrating an End-to-End Users QKD operational connection.

**Demonstrator mission architecture and performance analysis**

In this section we present a possible implementation scenario for a demonstrator Italian QKD mission, specifically analyzing the impact of several factors on the performances that it can provide.

A LEO satellite is assumed to be operating as a trusted node to provide secret keys to a set of ground stations located on the Italian territory by means of a prepare-and-measure QKD protocol (see in the following for the details). We carry out the analyses for a set of four ground stations located in Matera (40.65°N, 16.70°E), Rome (41.91°N, 12.48°E), Padua (45.41°N, 11.88°E) and Turin (45.07°N, 7.68°E) in order to cover a large portion of the Italian territory.

For what concerns the space segment, in the definition of a demonstrator system one could choose among different kinds of orbits depending on the desired performances. In this work we assume that a LEO orbit is employed, since it is considered to be more suitable for present-day quantum communications due to the fact that it is characterized by lower propagation losses than MEO and GEO orbits. We consider a range of circular orbits with an altitude between 500 km and 700 km.

Since the demonstrator mission is meant to be optimized for Italian coverage, one could select an orbit whose inclination matches the range of latitudes in which Italy is located; this choice would maximize the amount of time that is spent by the satellite in visibility the ground stations distributed on the Italian territory. Another possible choice is to employ a Sun-synchronous orbit (SSO) which has the advantage of guaranteeing a periodical access to a certain ground station. This is particularly important in the case in which (as it is assumed in this paper) the quantum communication can be carried out only during night-time; in this case in fact, the use of an inclined orbit would lead to long time windows (several weeks in a row) during which, due to seasonal effects, the satellite does not guarantee any night-time access to a certain ground station. The SSO on the other hand, can be suited to pursue exactly this purpose, allowing at least one night-time access almost every day.

In Figure 4, the maximum time period (expressed in terms of consecutive days) during which no night-time access to a ground station (located in Matera) takes place is shown for each month when a satellite is propagated for one year; blue bars refer to the case in which an inclined orbit (i=47°) is used, while yellow bars refer to an SSO. In both cases the altitude of the orbit is set to 600 km. As evident from the figure, during certain months the inclined orbit has more than twenty consecutive days with no night-time access to the ground station, while in the SSO this figure never exceeds two days. In the inset of the figure it is also shown how, nonetheless, the inclined orbit guarantees better performances in terms of average access duration and overall yearly visibility time longer: if more than one satellite is employed in the constellation, choosing a second orbit plane with same inclination and tailored RAAN could solve the seasonal effects and maximize the coverage time of the latitudes of interest. In a demonstrator mission, on the other hand, where absolute performances are not necessarily the main driver, an SSO orbit could be favored since it guarantees a continuous operation throughout the whole year.

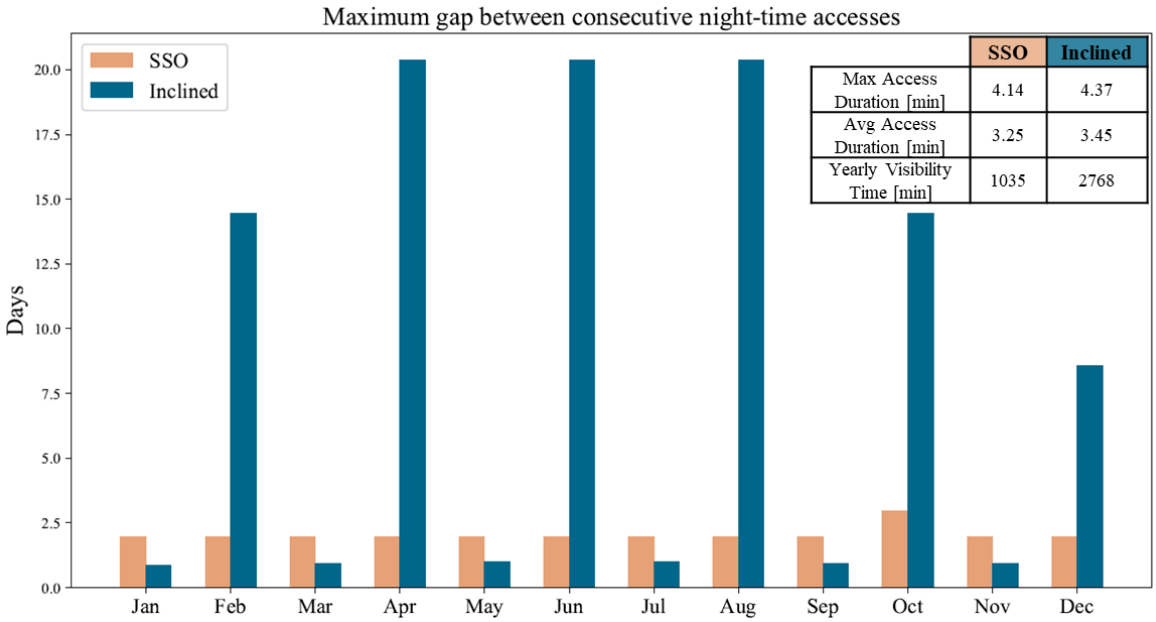



Figure 4. Maximum time period (expressed in terms of consecutive days) during which no night-time access to Matera takes place during each month for an SSO (yellow) and an orbit with i = 47° (blue).

In the evaluation of the demonstrator system performances, we first start by considering a single access to a ground station. The trajectory of the satellite with respect to the ground station causes the slant range to evolve as a function of time, which implies that the transmitter-to-receiver losses change instantaneously.

The left-hand panel of Figure 5 shows the slant range as a function of time (black, solid line) for a quasi-zenith access. Moreover, the overall link losses are shown for three different receiving apertures (a downlink communication is always assumed in this work): 40 cm, 70 cm and 100 cm. The other parameters used in the evaluation of the link budget are presented in Table 1.

Table 1. Link Budget parameters.

| Parameter | Value |
|---|---|
| Wavelength [nm] | 800 |
| Tx Telescope Diameter [m] | 0.13 |
| Rx Telescope Diameter [m] | 0.4, 0.7, 1.0 |
| Pointing accuracy rms [μrad] | 1.5 |
| Rx telescope effciency | 0.5 |

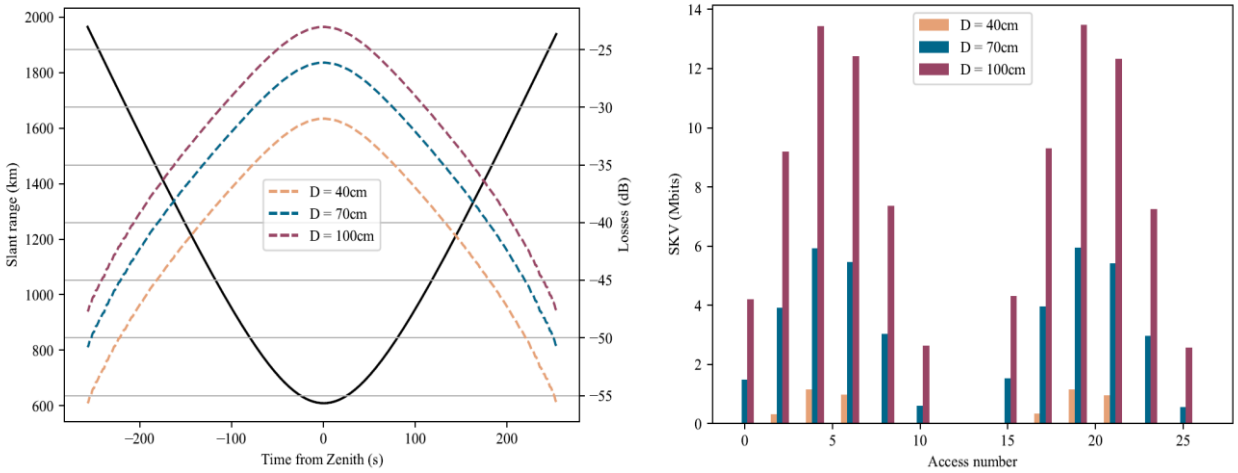



Figure 5. Effect on the receiving aperture on (left) channel losses (colored dashed lines) as a function of time for a quasi-zenith passage, and Secret Key Volume (SKV, left) extracted during a single access for different flyovers of the satellite. Finite-key effects are accounted for in the evaluation of the SKV.

The effects of the receiving apertures become even more apparent when the secret key volume (SKV) is evaluated. On the right-hand side of Figure 3 the SKV that can be extracted during a single access is presented for a series of flyovers. Notice that an SSO orbit has been assumed, which causes the periodicity of the accesses. The results are shown for the three different apertures introduced before. The differences in the SKV between two accesses are due to the fact that not every flyover approaches the zenith of the ground station, meaning that most accesses will have shorter duration and higher average losses than a zenith passage. The SKV has been evaluated assuming that a downlink decoy-state BB84 protocol is used.

The selected protocol corresponds to the efficient decoy-state BB84 one, performed in a downlink scenario. The evaluation of the SKV has been performed by applying a statistical analysis to give an estimation of lower and upper bounds of errors and number of photons in the two measurement basis, thus taking into account finite-size effects. Such analysis is based on the number of photons collected by the OGS during a single flyover passage considering the time-varying losses profile such as the ones shown in Figure 5. The computation is ultimately based on the analysis described in [14,15]. In Table 2 the details of the protocol are reported.

Table 2. Protocol parameters.

| Parameter | Value |
|---|---|
| X basis probability | 0.8 |
| Signal mean photon number | 0.6 |
| Secrecy parameter | 10^(-9) |
| Source repetition rate [MHz] | 200 |
| Dark count probability | 10^(-7) |
| Afterpulse probability | 10^(-7) |
| Detector quantum efficiency | 0.65 |

Finite key effects are accounted for in the evaluation of the SKV, and it is assumed that the key is extracted only from the photons exchanged during a single passage; because of this, during certain accesses it is not possible to extract any key when the receiving aperture is too small (as evident from the data corresponding to the 40 cm aperture in Figure 3).

The size of the optical ground station aperture should then be carefully chosen to avoid that a high number of access results in no secret key at all. A possible solution to this problem could be to extract the key from photons exchanged during several accesses; this choice, though, could result in a significantly more complex operation planning when a fully operational system is considered, and may potentially give rise to security issues.

Establishing a quantum link between a ground station and a satellite requires certain conditions. In this work we use the (fairly conservative) assumption that the minimum elevation angle to perform quantum communications is 30°. Moreover, for an optical link to be established with a ground station, it is necessary that the latter falls within the field of regard (FoR) of the satellite optical terminal. In Figure 6, we show two examples of possible FoRs: the green circle represents a hemispherical FoR, in which case the communication is only limited by the minimum elevation angle of 30°; the light blue line, on the other hand, shows a field of regard limited in the cross-track direction, that is, the direction orthogonal to the motion of the satellite. The latter case is representative of a scenario in which the design of the SoT is in general less complex and usually characterized by lower mass and volume, and as such it could be favored for small satellites applications.


Figure 6. Graphical representation two possible fields of regard: hemispherical (green) and limited in the cross-track direction (light blue).

The FoR of the satellite optical terminal inevitably impacts the performances of the system. Both scenarios (hemispherical and limited FoR) have been studied for the demonstrator system presented above. A single satellite orbiting on a circular SSO has been propagated for a year, and the results corresponding to each access to the four ground stations introduced before have been recorded. This allowed to evaluate the overall time that can be spent in a year for quantum communication purposes with each OGS; the results are presented in the left-side panel of Figure 7 for the hemispherical FoR (transparent bars) and for the limited one (solid bars); for sake of completeness, the results are shown for three different rorbit altitudes: 500 km, 600 km and 700 km. It is evident that using a limited FoR results in an overall operation time that is roughly half of that guaranteed by the hemispherical one.

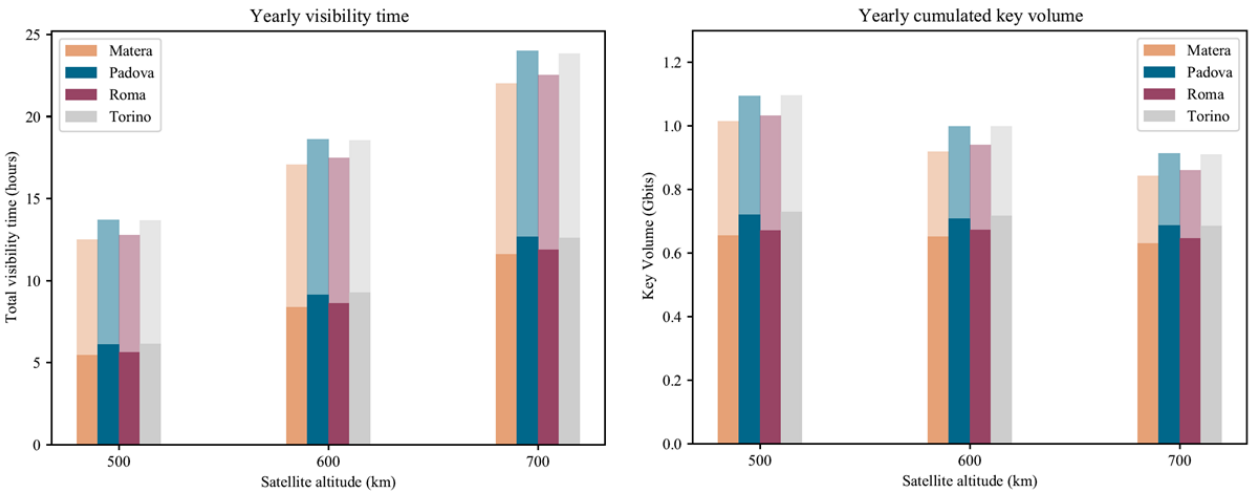



Figure 7. Yearly operation time and cumulated key volume with each optical ground station for different satellite altitudes. The higher-transparency bars show the case in which a hemispherical FoR is assumed, such that the quantum communication is only limited by the minimum elevation angle of 30°. The solid bars show the results for a limited FoR, such as the one presented by the light blue line in Figure 6.

Nonetheless, when the overall SKV is estimated, the difference between the two scenarios is less apparent. In the right-hand side of Figure 7, in fact, we show the estimated SKV that can be extracted during one year for the same scenarios as the ones presented in the left-side panel. As evident from the figure, the overall SKV that can be extracted in a year with each optical ground station when a limited-FoT terminal is employed is more than two thirds of that obtainable with a hemispherical FoR. This comes as a consequence of the fact that, even if the overall yearly duration is much lower in the limited FoR case, only the accesses that have a favorable average elevation angle are selected (due to the fact that the limited range happens in the cross direction); this implies that the instantaneous losses are lower on average, which, in turn, allows the extraction of a higher SKV per passage (as reported in Table 2).

Table 2. Effect of limited Field of Regard.

| | **Hemispherical (30° elevation)** | **Limited FoR** |
|---|---|---|
| Average access duration [s] | 193.8 | 196.9 |
| Average SKV per access [Mbits] | 2.899 | 4.263 |
| Minimum SKV per access [Mbits] | 0.061 | 0.224 |
| Maximum SKV per access [Mbits] | 6.10 | 5.93 |
| Percentage of accesses with SKV > 0 [%] | 82.65 | 87.58 |

All the considerations reported above should be accounted for in the design of a satellite-based QKD system. Notice that, at this stage, the cloud coverage has not been considered, which could clearly lead to a general worsening of the overall performances (by lowering the amount of time that can actually be spent to perform QKD operations).

## 6. CONCLUSIONS

In this work we have presented the main initiatives that are being carried out by TAS-I with the aim of developing a satellite-based secure quantum communication network. The first stepping stones in this respect are the Quantum Optics

Laboratory and the Satellite QKD Mission simulation tool, which will allow to gather the knowledge needed in the development of an Italian QKD Demonstration Mission.

The Italian QKD Demonstration program will boost the consolidation of an Italian product chain, focusing competences, research capabilities and factory capacities on a concrete and feasible initiative. It will allow measurement campaigns, to acquire a better knowledge of QKD hardware physics in space and to run a full set of QKD and Optical performances measurements to characterize the propagation environment and to prepare the technological basis for a large capacity QKD infrastructure, able to meet the Italian cybersecurity market needs in the following years.

## REFERENCES

[1] Bennett, C. H. and G. Brassard, "Quantum Cryptography: Public-Key Distribution and Coin Tossing", Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984).

[2] Ekert, A. K., "Quantum cryptography based on Bell's theorem", Physical Review Letters 67 (6), 661–663 (1991).

[3] Bennett, C. H., Brassard, G., & Mermin, N. D., "Quantum cryptography without Bell's theorem", Physical review letters 68(5), 557 (1992).

[4] Scarani, V., Acin, A., Ribordy, G., & Gisin, N., "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations", Physical review letters 92(5), 057901 (2004).

[5] Lo, H. K., Ma, X., & Chen, K., "Decoy state quantum key distribution", Physical review letters 94(23), 230504 (2005).

[6] Zhao, Y., Qi, B., Ma, X., Lo, H. K., & Qian, L., "Experimental quantum key distribution with decoy states", Physical review letters 96(7), 070502 (2006).

[7] Ling, A., Peloso, M. P., Marcikic, I., Scarani, V., Lamas-Linares, A., & Kurtsiefer, C., "Experimental quantum key distribution based on a Bell test", Physical Review A 78(2), 020301 (2008).

[8] Bacco, D., Canale, M., Laurenti, N., Vallone, G., & Villoresi, P., "Experimental quantum key distribution with finite-key security analysis for noisy channels", Nature communications 4(1), 1-8 (2013).

[9] Vallone, G., D'Ambrosio, V., Sponselli, A., Slussarenko, S., Marrucci, L., Sciarrino, F., & Villoresi, P., "Free-space quantum key distribution by rotation-invariant twisted photons", Physical review letters 113(6), 060503 (2014).

[10] Basso Basset, F., Valeri, M., Roccia, E., Muredda, V., Poderini, D., Neuwirth, J., Spagnolo, N., Rota, M. B., Carvacho, G., Sciarrino, F., & Trotta, R., "Quantum key distribution with entangled photons generated on demand by a quantum dot", Science advances 7(12), eabe6379 (2021).

[11] M. Krenn, M. Malik, T. Scheidl, R. Ursin, A. Zeilinger, "Quantum communication with photons", Optics in our Time 18, 455 (2016).

[12] J. Pan, "604 progress of the quantum experiment science satellite (QUESS) Micius project national report 2016–2018", Chin. J. Space Sci. 38(5), 604–609 (2018).

[13] Islam, T., Sidhu, J. S., Higgins, B. L., Brougham, T., Vergoossen, T., Oi, D. K. L., Jennewein, T., Ling, A., "Finite resource performance of small satellite-based quantum key distribution missions.", arXiv:2204.12509v2 (2022).

[14] Lim, C. C. W., Curty, M., Walenta, N., Xu, F., Zbinden, H., "Concise security bounds for practical decoy-state quantum key distribution." Physical Review A 89.2, 022307 (2014).

[15] Yin, H., Zhou, M., Gu, J., Xie, Y., and Lu, Y., Chen, Z., "Tight security bounds for decoy-state quantum key distribution." Scientific Reports 10.1, 1-10 (2020).