Available online at www.sciencedirect.com

ScienceDirect

Advances in Space Research 73 (2024) 5446–5463

ADVANCES IN SPACE RESEARCH (a COSPAR publication)

www.elsevier.com/locate/asr

Orbit design of satellite quantum key distribution constellations in different ground stations networks

Federico De Grossi [a,*], Stefano Alberico [b], Christian Circi [a]

[a] Sapienza University of Rome, Via Salaria 851, Rome 00138, Italy
[b] Skudo OÜ, Tartu mnt. 84a-34, Tallin 10112, Estonia

Received 30 July 2022; received in revised form 15 December 2022; accepted 27 January 2023
Available online 1 February 2023

Abstract

In the field of Cryptography, Quantum Key Distribution (QKD) is an application of Quantum Information theory that obtained a great deal of attention in recent years. It allows to establish secret keys between two or more parties, in a much safer way than that implemented by classic cryptography (based on discrete logarithms and factorization of prime numbers). The most promising way of realizing a QKD network (especially over great distances) in the near future is by a constellation of satellites. This paper considers the problem of optimizing the orbits of the satellites in order to maximize the minimum key length shared in a network of ground stations over a fixed amount of time. Different networks of stations are considered and the influence of their geographical disposition on the design and the performance index is highlighted. The networks considered are: a global constellation, a regional European constellation, and two in which there are groups of stations in two different narrow bands of latitude. The effect of Inter-satellite links is then taken into account and how, in some cases, they can improve the performances. Finally the daily performance of the considered constellations are analyzed.

Keywords: Quantum key distribution; Constellation design; Inter-satellite quantum links; Cryptography; Satellite constellation optimization

1. Introduction

One of the first practical and promising application of the theory of Quantum Information is Quantum Cryptography, in particular Quantum Key Distribution (QKD). In Cryptography, for symmetric protocols in particular, the key distribution problem consists in making sure that two parties, interested in communicating in a secure way, can share a secret common key (a sequence of bits) known only to them. It is a fundamental problem for secure communications since the key is used to encrypt and decrypt the messages, therefore the secrecy of the conversation depends on the inability of a potential eavesdropper to gain knowledge on the key. In current cryptographic systems the secrecy of the shared keys is generally based on the difficulty of solving certain mathematical problems, which are infeasible on classical computers.

QKD consists in distributing a shared secret key between two or more parties employing the principles of Quantum Mechanics and Quantum Communication, which, used properly, ensure the secrecy of the key, relying on the principles of physics instead that on the complexity of a mathematical problem. In 1984 Bennet and Brassard developed the most famous protocol for QKD, called BB84 (Bennett and Brassard (1984)), it relies on the principles of superposition and measurement of a quantum system to ensure unconditional security against possible eavesdroppers, whose presence and interference with the communication would be revealed by the two communicating parties. The BB84 protocol is implemented using the

* Corresponding author.
E-mail addresses: federico.degrossi@uniroma1.it (F. De Grossi), stefano@skudo.tech (S. Alberico), christian.circi@uniroma1.it (C. Circi).

https://doi.org/10.1016/j.asr.2023.01.056
0273-1177/

Nomenclature

List of abbreviations

BB84	Bennet-Brassard 1984
ISL	Inter-satellite link
KER	Key Exchange Rate
LEO	Low Earth Orbit
PSO	Particle Swarm Optimization
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
RAAN	Right Ascension of the Ascending Node
WCP	Weak Coherent Pulses

polarization of photons, and theoretically it requires single-photon emitters; with the current technology it is implemented by highly attenuated lasers. Other famous protocols rely on *entanglement*: a pair of entangled photons is distributed to two parties (Ekert (1991), Bennett et al. (1992)).

The research in Quantum Cryptography, and development of QKD networks saw great interest recently also because of the advances of Quantum Computers, which could render un-secure all the cryptographic protocols based on the hard problem of factorization and discrete logarithms, intractable for classical computers but solvable with a powerful enough quantum computer (Shor (1994)).

Ground based QKD suffers of distance limitations due to the exponential losses present in fiber optic, a potential solution would be to employ *quantum repeaters*, however their technology faces significant challenges and it is considered comparable to building universal quantum computers (Munro et al. (2015); Bedington et al. (2017)). Satellite-based QKD is a promising technology to provide secure keys over great distances, in fact, the faint signal needed suffers of less attenuation in free-space transmission than fiber optic. Moreover, since a satellite in orbit can pass over many distant places in a small time, a constellation could provide global coverage or over a geographical region (Bedington et al. (2017)).

A recent review of space missions employing quantum technologies, including quantum communication, can be found in (Belenchia et al. (2022)). It is worth citing the Micius satellite that in 2016 successfully established a link with the ground from LEO, proving the feasibility of QKD over a 1200 km distance (Liao et al. (2017)). Many works on satellite QKD focus on the modeling of the quantum link, analyzing and quantifying the losses, and on experimental implementation (Bonato et al. (2009); Tomaello et al. (2011a); Bourgoin et al. (2013); Liorni et al. (2019); Dequal et al. (2021); Xu et al. (2021); Vallone et al. (2015); Wang et al. (2013)); less works treat constellation design, but their number is increasing in recent years, proving the interest in the problem (Khatri et al. (2021); Vergoossen et al. (2020); Wang et al. (2021); Mazzarella et al. (2020)).

The content of this research is organized as follows: in Section 2 the general concept of satellite-based QKD is illustrated, in particular in the case of downlink transmission; furthermore, the characteristics of the link are summarized as well as the main hypotheses in its modelization. In Section 3 a performance index for comparing different constellations is introduced, together with a distinction between keys shared between a satellite and a station and those shared between two stations; the problems of designing the orbits, as well as the one of passing between the first kind of keys to the second, are cast as optimizations. In Section 4 the dynamical model and the optimization method employed are described, and the results of several cases of constellations, with different disposition of the ground stations, are reported.

The use of Inter-satellite links (ISL) (Tomaello et al. (2011b, 2019)) between the satellites is believed to provide an increase of the performances in QKD constellations, in Section 5 the ISL are implemented and their effect analyzed with the same constellations of Section 4.

In Section 6 the daily performances are considered, taking into account the need of QKD network of having new key material produced daily or in intervals of some days. The role of ISL is again highlighted. Finally, Section 7 contains the conclusions.

2. Satellite-based QKD

The most common approach to QKD via satellite currently considers the satellite as a trusted node, which establishes keys with each station in the network and carries them to the other stations; with respect to a ground trusted node, the satellite has the advantage of being more difficult to reach and to interfere with. Alternative to this approach would be the *quantum repeater*, but, as mentioned before, the required technology is still under development. Entanglement-based protocols do not require the trusted node assumption, but their performance is generally lower, and the satellite must be able to communicate with two ground stations at the same time.

There are different kinds of satellite QKD, and are distinguished by how the quantum communication is carried out: in the uplink configuration, the station is the sender of photons, and the satellite is the receiver, in the downlink configuration the satellite is the sender instead; other configurations are the retroreflector, in which downlink is sim-

ulated with the station bouncing the signal on the satellite using a retroreflecor (Vallone et al. (2015)), or the entangled source, in which the satellite sends an entangled photon-pair to a couple of stations (Boone et al. (2015)), suitable for entanglement-based protocols (Bedington et al. (2017)). Previous research points at the downlink configuration as the most promising in the near future, since it generally presents the higher signal to noise ratio, therefore it is the configuration considered in this work.

Considering a single satellite and a pair of stations, the key distribution process is illustrated in Fig. 1 and proceeds as follows: during the access time with the first station (station A), the satellite establishes a key with it by means of the BB84 protocol, let's call this key k_{SA}, then, when the satellite passes over the second station (station B), it establishes a key with it as well: k_{SB}. At this point the satellite holds both keys, while each station has only the key it shares with the satellite, however the goal is to put A and B in contact between themselves, so they must share a key k_{AB}. To accomplish this, the satellite can transmit one of its two keys to a station, for example let us suppose that it transmits k_{SA} to station B, therefore now station B has both k_{SB} and k_{SA}, and shares the latter with station A. The key k_{SA} can be sent to station B in a secure way combining the two keys with a XOR encoding ($k_{SA} \oplus k_{SB}$), supposing that the they are equal in length; the encoded key is publicly transmitted through a classical communication channel. Station B can decrypt the message and obtaining the key performing: $k_{SA} = k_{SB} \oplus (k_{SA} \oplus k_{SB})$. The XOR encryption used constitute a one-time pad if the k_{SB} is discarded after it is employed to transmit k_{SA}, and it is therefore, completely secure.

The BB84 protocol requires transmitting single-photons, but the technology of true single-photons sources is not yet mature, therefore, current implementations of BB84 employ Weak Coherent Pulses (WCP), which have mean photon number different from one, causing the possibility of multiple photons to be sent. Multiple photons could make the communication vulnerable to a *photon number splitting* type of attack, to overcome this issue it was developed the decoy-state BB84, which is used for practical applications (Hwang (2003, 2005)).

In order to compute the generated key by a passage of a satellite on a ground station, the quantum link must be characterized. In the case of downlink, the signal is sent from the satellite to ground, the losses it suffers can be enclosed in a total transmittance η_{tot}, representing how much of the signal reaches the receiver. The losses include the diffraction of the beam, that is here modeled as Gaussian, and atmospheric transmittance.

$$\eta_{tot} = \eta_{fs}\eta_{atm}\eta_{rec}\eta_{tr}\eta_{point} \tag{1}$$

$$\eta_{fs}(L) = 1 - \exp\left(-\frac{2R_{rec}^2}{w(L)^2}\right) \tag{2}$$

$$\eta_{atm}(\theta_{ze}) = \eta_{atm0}^{(1/\cos(\theta_{ze}))} \tag{3}$$

The expression of the total transmittance is reported in Eq. (1), it includes also the efficiency of the transmitter η_{tr}, of the receiver η_{rec}, and the pointing losses η_{point}. In Eq. (2) there is the expression of the free-space loss, where R_{rec} is the radius of the receiver, $w(L)$ is the width of the beam when satellite and station are separated by a distance L. Eq. (3) shows the atmospheric loss, modeled as an homogeneous layer of finite thickness (Khatri et al. (2021)), θ_{ze} is the zenith angle, η_{atm0} is the absorption at the zenith, and it depends on the signal wavelength. In the downlink scenario, the atmosphere turbulence is not the main source of loss, since it affects the beam only at the end of the propagation path, and it is usually neglected; this is not true for uplink, in which the turbulence introduces the most important losses and the link requires a more advanced model. For downlink the dominating source of loss is diffraction, therefore the performance of the link are strongly limited by the distance, so the most promising orbits are LEO orbits (Tomaello et al. (2011a)). The details and numerical values of the parameters of the link model can be found in Appendix A; while

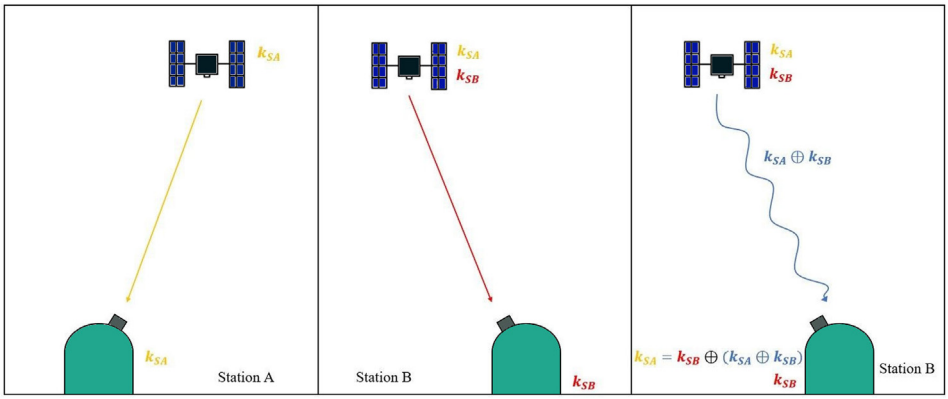

Fig. 1. The process of key distribution between two station with downlink. On the left, the satellite establishes k_{SA} with station A; in the middle, the satellite establishes k_{SB} with station B; and on the right, the satellite transmits k_{SA} to station B by XOR encryption. The straight lines represent quantum links, the undulated line represents a classical link.

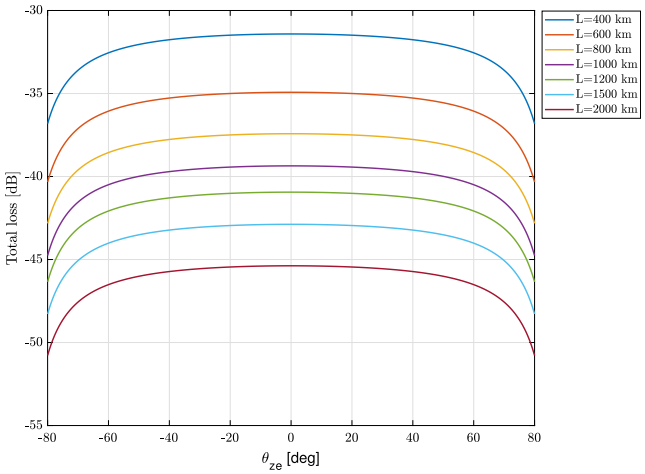

Fig. 2. Total transmittance of the quantum channel at various distances.

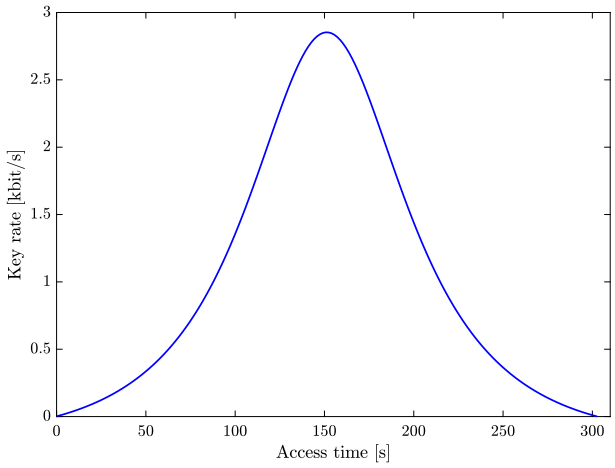

Fig. 3. Key rate during the passage of a satellite over a ground station.

a plot of the behavior of the transmittance is presented in Fig. 2, varying the zenith angle and for different distances between satellite and station.

The main source of noise, in this context, are background photons that enter the receiver together with signal photons; the noise is therefore heavily influenced by the sky brightness, which can differ from day and night of several orders of magnitude. There is research on the feasibility of QKD in sunlight (Gruneisen et al. (2015)), although the maximum performances would be achieved during the night. With the parameters of the link considered in this work the signal to noise ratio allows the transmission with non-zero key rates only during the night. It is considered that only the station must be in shadow while the satellite can be in sunlight, supposing that the reflected stray photons on the surface of the satellite can be reduced by design of the satellite or filtered out.

Local weather conditions and cloud coverage also influence the link, still, they are difficult to predict over long periods of time and can be analyzed only in a statistical way. In this sense they are dependent on the stations position, since in this work the stations network is an input of the problem, and comparisons are done only between constellations serving the same stations, the local weather is not considered, its effect would certainly be degrading for the performances but should not heavily influence the orbit design.

The rate at which the key is generated during an access between a ground station and a satellite is indicated as Key Exchange Rate (KER), it depends on the specific protocol as well as on the noise and the quantum bit error rate (QBER). This work employs the two decoy state protocol with a vacuum and weak decoy state as described by (Ma et al. (2005)), in which is also proved that it is close to optimum. The expression of the asymptotic key rate is employed, since finite key effects are difficult to predict and still being researched. The details of the mathematical expression of the KER and the numerical values employed are found in Appendix A. The repetition rate of the source on the satellite is taken as 100 MHz, as an example, the plot of the key rate during a passage is depicted in Fig. 3, where an orbit of 400 km is considered.

During each passage of a satellite on a ground station, the length of the generated key is determined in the following way: the satellite is considered in visibility if its zenith angle is less or equal than 80°, to take into account obstacles that are likely to be present close to the horizon. The station is considered in shadow (hence benefits from the lower noise level of the night) from one hour after sunset and one hour before sunrise, to avoid an unrealistic abrupt passage from daylight to night. When the above conditions are met, and if the computed key rate is higher than zero, the key length is calculated performing the integral of the key rate during the access interval (which has a shape similar to Fig. 3), the integral is numerically computed by the trapezoidal rule (the function is approximated as piece-wise linear between a set of discrete points).

3. Performance index and optimization criteria

To express the problem of designing a constellation that provides QKD to a network of stations as an optimization problem, a performance index, capable of describing the quality of the service provided, must be identified.

In this work, as it will be discussed in the following, the problem is tackled by splitting it into two consecutive problems, one for optimizing the orbits of the satellites, and the other to optimize the way keys are transferred from the satellite to each pair of stations. The second one will be described first.

For this purpose, let us consider the situation with one satellite and a number of N_g ground stations. As explained in the previous section, the satellite, passing over the stations, creates keys shared with them; let us call these keys k_{sg}, since are keys shared between the satellite and a station. So, providing that the satellite has access to all the stations, after a certain amount of time it will have in its memory the N_g keys: $(k_{sg,1}, k_{sg,2}, \ldots, k_{sg,N_g})$. But the service

required is to have the station share keys between themselves, so as showed before in the case of two stations, the k_{sg} keys must be "transformed" into keys shared by one station with another.

In this work, the optimization problem of connecting the network of stations is defined by requiring that every station shares a secret key with all the other stations, after a predetermined amount of time. Therefore, the number of station-to-station keys that must be generated is $N_g(N_g-1)/2$, these keys, that we can call k_{gg}, must come from the k_{sg} keys which are less in number (N_g). This conversion of the key material can be carried out as in the two stations case, employing XOR encoding and classically transmitting the keys, but the procedure must be extended to the case of multiple stations and the length of the k_{gg} keys must be determined from the length of the k_{sg} keys.

In the following, the symbol k referred to a key, is used also to express the length of the key in bits. Considering two stations i and j in the network, following the analogy with the two stations case, we can imagine that $k_{gg,ij}$ would be constituted by the bits (or part of the bits) of either $k_{sg,i}$ or $k_{sg,j}$, while the other key is used for the XOR encoding and transmitting. The presence of multiple stations implies that we cannot use *all* the bits of, for example, $k_{sg,i}$, because its bits would be necessary also to constitute the other keys between station i and the rest of the network, say $k_{gg,ih}$ with $h \neq j$. Therefore, now a fraction of the $k_{sg,i}$ is combined and transmitted to station j to generate $k_{gg,ij}$; this is expressed by Eq. (4), where $x_{ij} \in [0,1]$ and the min is necessary if the two satellite-station keys are different in length. A similar approach is used in Wang et al. (2021).

Similarly, every station-station key comes from an equivalent relationship, there are $N_g(N_g-1)/2$ equations showed in Eq. (5) as much as the number of keys. Assigning the numbers x_{ij} allows to calculate the length of the k_{gg} keys, but of course, being k_{sg} the "source material" from which station-station keys are taken, constraints must be considered which ensure that the length of the k_{gg} does not exceed the length of the corresponding k_{sg}. Such constraints are expressed in Eq. (6) for every satellite-station key.

$$k_{gg,ij} = x_{ij}\min(k_{sg,i}, k_{sg,j}), \text{ for } j > i \tag{4}$$

$$\begin{cases} k_{gg,12} = x_{12}\min(k_{sg,1}, k_{sg,2}) \\ k_{gg,13} = x_{13}\min(k_{sg,1}, k_{sg,3}) \\ \quad\vdots \\ k_{gg,(N_g-1)N_g} = x_{(N_g-1)N_g}\min(k_{sg,(N_g-1)}, k_{sg,N_g}) \end{cases} \tag{5}$$

$$r_{sg,i} = k_{sg,i} - \sum_{j=i+1}^{N_g} k_{gg,ij} - \sum_{j=1}^{i-1} k_{gg,ji} \geqslant 0, \text{ for } i \in \{1,\dots,N_g\} \tag{6}$$

Now, what is desirable is that every station is connected to all the others with keys as long as possible; if the stations are equally important, so that it is not required that some must have longer keys than the rest, the performance is dictated by the minimum key length among the station-station keys k_{gg}. Therefore the aim of the optimization problem that determines the design of a constellation, should be to maximize the minimum station-station key. An alternative would be to maximize the sum of all the keys, but then it could happen that some pairs of stations share short keys or none at all, while others have much longer ones. The r_{sg} value in Eq. (6) is basically a residual of the key material that remains with the satellite and is not transformed into k_{gg}; therefore, a secondary objective could be to minimize these residuals in such a way that as much as possible of the keys generated by the interaction between satellite and stations is employed.

The Eq. (5) and (6) can be already used to define an optimization problem that, given the k_{sg}, has the objective of finding the x_{ij} coefficients such that the performance index described is maximized, as expressed in Eq. (7), where $\boldsymbol{x}$ is a vector containing all the x_{ij}. The number of variables is therefore $N_g(N_g-1)/2$, and the constraints are N_g.

$$\begin{aligned} &\max_{\boldsymbol{x}} \left(\min_{i,j,j>i}(k_{gg,ij}) \right) \\ &\text{s.t. : } r_{sg,i} \geqslant 0, \text{ for } i \in \{1,\dots,N_g\} \end{aligned} \tag{7}$$

Now, consider a special case of the above problem: the satellite-station keys have all equal length $\bar{k}_{sg}$, as well as all the station-station keys, which implies that all coefficients are equal $x_{ij} = \bar{x}$. Since they are all equal, maximizing the minimum key is equivalent to maximizing $\bar{x}$, as can be deduced from Eq. (8). The constraint, instead, assumes the form of Eq. (9), so the maximum $\bar{x}$ satisfying it results to be $1/(N_g-1)$, and the length of the station-station keys is related to $\bar{k}_{sg}$ as in Eq. (10).

$$k_{gg} = \bar{x}\bar{k}_{sg} \tag{8}$$

$$\begin{cases} \bar{k}_{sg} - \sum_{j=i+1}^{N_g} \bar{x}\bar{k}_{sg} - \sum_{j=1}^{i-1} \bar{x}\bar{k}_{sg} \geqslant 0 \\ \bar{k}_{sg}\left(1 - \bar{x}(N_g-1)\right) \geqslant 0 \\ \bar{x} \leqslant \frac{1}{N_g-1} \end{cases} \tag{9}$$

$$k_{gg,opt} = \frac{\bar{k}_{sg}}{N_g-1} \tag{10}$$

Even if this relation is obtained in a specific case, from numerical results of the general optimization of the station-station keys emerges that the minimum k_{gg} is still limited by the value of Eq. (10). Clearly, in general, differently from the special case above, the coefficients and the k_{gg} keys different from the minimum one would not have the same values. From this consideration, given the problem of maximizing the minimum station-station key, it is equivalent to maximizing the minimum satellite-station key; then computing the minimum k_{gg} by Eq. (11) (note that the $k_{sg,i}$ depend on the orbit design).

$$k_{gg,min} = \frac{\min_i(k_{sg,i})}{N_g - 1} \tag{11}$$

It is still worth solving also the general optimization of the station-station keys, since the keys greater than the minimum one can be improved with a better choice of the x_{ij}, leaving less of the residual key material unused in the memory of the satellite.

Until now, only one satellite has been considered, the case with a constellation of N_s satellites, in the absence of inter-satellite links (ISL), that is to say the satellites cannot pass keys between each others, is easily derived. In fact every satellite acts independently from the others and the resulting station-station keys would simply be the sum of the ones generated from each satellite. ISLs are known to provide an improvement of the constellation performance (Vergoossen et al. (2020)) and they are treated later in this work.

In the end, this work addresses the satellite QKD problem splitting it in two optimizations: maximizing the minimum k_{sg} varying the orbit of the satellites, as expressed by the cost function in Eq. (12), which we can call problem A; and subsequently both maximizing the minimum (for every satellite) k_{gg} and minimizing the residuals varying the x_{ij}, which we can call problem B, the cost function employed (to be maximized) is given in Eq. (13). Note that J_A depends on the orbits of the satellites, while J_B depends on the k_{sg} keys; splitting the two, instead of considering a single optimization eases the calculation and does not affect the solution, since maximizing J_A has as consequence also maximizing the minimum k_{gg}.

$$J_A = \sum_h^{N_s} \min_i(k^h_{sg,i}) \tag{12}$$

$$J_B = c_k \min_{i,j,j>i}(k_{gg,ij}) - c_r \sum_{i=1}^{N_g} r_{sg,i} \tag{13}$$

It can happen that, when two or more stations are close together, they are simultaneously in visibility of a satellite; assuming that the satellite has on board only one quantum transmitter a conflict arises, and the satellite must decide with which station operate the QKD. Here the issue is addressed choosing to communicate each time with the station offering the highest mean key produced, during the conflicting interval; with this strategy the quantity of key material produced is maximized. The opposite case in which a station is in visibility with multiple satellites is not considered a conflict, since it is assumed that the stations are equipped to communicate with more satellites at the same time.

4. Orbit design

A constellation for QKD can be classified on the basis of the distribution of the ground stations considered, in fact, they can, for instance, be spread all around the Earth, without any particular concentration, or they can be gathered in a specific geographical region. With this distinction in mind, two constellations were analyzed at first: a global constellation, and a regional constellation, in which the stations are concentrated in Europe. The number of stations and satellites for both is respectively 7 and 6; while for some application may be desirable to consider a greater number of stations (and satellites), it would increase the computational burden of the optimization, without drastically changing the design considerations obtained with a smaller constellation. The list of stations is reported in Table 1, including their latitude and longitude.

With the current technology the orbits of interest for satellite QKD are LEO orbit, therefore here circular orbits with altitude $h = 400$ km are considered, since there is no advantage in increasing the height from the point of view of the length of the key generated. The six satellites can be on the same orbit or divided into two orbits, and for each orbit they are equally spaced in true anomaly, therefore the remaining free orbital parameter are i, Ω_0, the inclination and the initial Right Ascension of the Ascending Node (RAAN).

The dynamical model, employed in the optimization process, considers the gravity of the Earth approximated by a spherical harmonics expansion to the second degree, that is to say, including the perturbation given by the Earth oblateness (J_2). The results of the optimization are then validated in a more accurate model in which spherical harmonics expansion goes up to 10th degree and order. The orbital motion is propagated for one year, and the access intervals between each satellite and each station are determined, during which the key is generated based on the link

Table 1
Stations in global and regional constellations.

	Global			Regional	
Station	**Lat. [deg]**	**Lon. [deg]**	**Station**	**Lat. [deg]**	**Lon. [deg]**
Rome	41.90	12.50	Rome	41.90	12.50
Reykjavik	64.13	−22.83	Paris	48.85	2.35
Tokyo	35.65	139.83	Berlin	52.52	13.40
Sydney	−33.87	151.21	London	51.51	−0.14
Washington	38.90	−77.05	Madrid	40.42	−3.70
Buenos Aires	−34.60	−58.38	Warsaw	52.23	21.01
Lagos	6.47	3.41	Stockholm	59.33	18.07

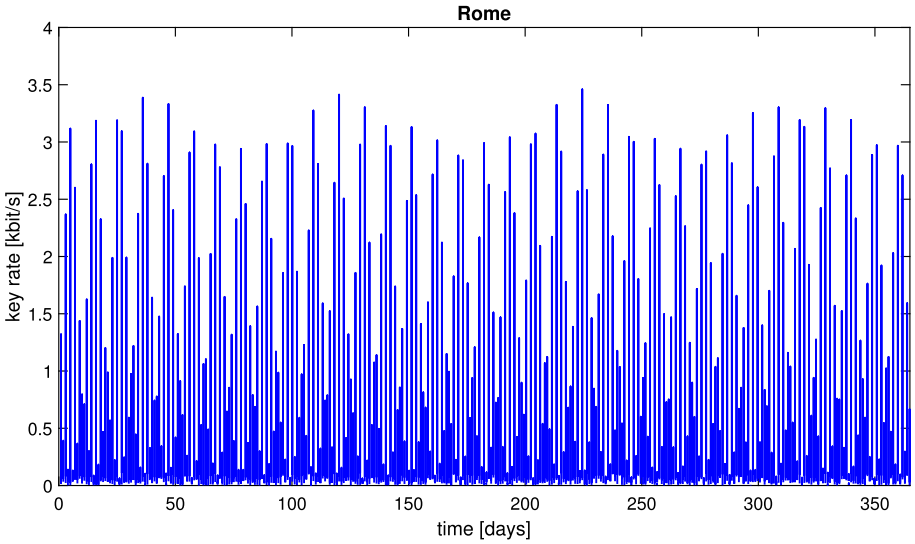

Fig. 4. Key rate between a satellite in the global constellation and Rome.

Table 2
Global and regional constellations: orbits and key generated.

	i [deg]	Ω_0 [deg]	$k_{gg,min}$ [Mb]	$k_{gg,tot}$ [Mb]
Global	96.21	−90.86	38.3	972.1
Regional	57.46	59.46	28.5	1021.6

model. In the end, the satellite-station keys $k^h_{sg,i}$ are computed for every pair of satellite h and station i, then the station-station keys are computed.

The variables of the optimization problem A are therefore the inclination and initial RAAN of every orbit, the decision of considering one or two orbits is taken instead *a priori*. The optimization is performed with Particle Swarm Optimization algorithm (PSO), and the MATLAB function *particleswarm* is used for this purpose.

For the global constellation, the optimization process returned an almost sun-synchronous orbit, very close to a noon-midnight orbit, which maximizes the nighttime passages of the satellites, and appears to be the optimal orbit when the stations are distributed around the globe in a great interval of latitude, as in this case. The two plane solution found consists in two similar sun-synchronous orbits, having a separation in RAAN and presents performances (minimum and total key length) very similar to the single plane constellation, which was preferred for being simpler. The optimal orbit of the regional constellation is instead an orbit with inclination such that it has access to the higher latitude station. Also in this case using two orbital planes instead of a single one does not bring any advantage. As an example, the plot of the key rate during the propagation period is reported in Fig. 4 for the global constellation and between a satellite and the station of Rome.

The orbital elements of the two constellations orbits are reported in Table 2, together with the obtained minimum key between all the stations and the sum of all the station-station keys. It can be seen that the global constellation has a higher minimum key, and a lower total key respect to the regional constellation, it is best to remember that the stations of the regional constellation suffer from access conflicts, which are responsible of reducing the minimum key, that would have been better than the global one otherwise. In Fig. 5 are plotted the key lengths, divided in k_{gg} keys between each pair of stations in the upper plot, and k_{sg} keys between every pair satellite and station, in the lower plot. In Table 2, the value of the minimum key is the minimum bar of the upper plot, and the total key is the sum of all the key lengths of the same plot. Analogously, in Fig. 6 there are the plots of the key lengths of the European constellation.

While, as for the above cases, given a disposition of ground stations it is possible to find the optimal orbit that maximizes the generated keys, it is interesting to ask the inverse question: what are the ground stations networks that are most favourable, allowing to produce more keys? Or what is the influence of stations disposition on the performances of the problem? Looking at the results in Table 2 there is an appreciable difference in the two networks, but not a dramatic one. The difference in absolute latitude between the stations of the global constellation is of 57.66°, and for the regional one is of 18.91°; let us instead consider the very special case of a constellation in which all the stations are at the same latitude, for instance at 50°, and sufficiently spaced in longitude to avoid generating conflicts, the performances of this constellation would be of about $k_{gg,min} = 110$ Mb, and $k_{gg,tot} = 2300$ Mb, more than twice of the respective values of the above considered global and regional constellation. A network of only equatorial stations, with the satellites on an equatorial orbit would have an even greater advantage: $k_{gg,min} = 830$ Mb, and $k_{gg,tot} = 17000$ Mb. While the cases of stations all with exactly equal latitude are unlikely to represent a realistic

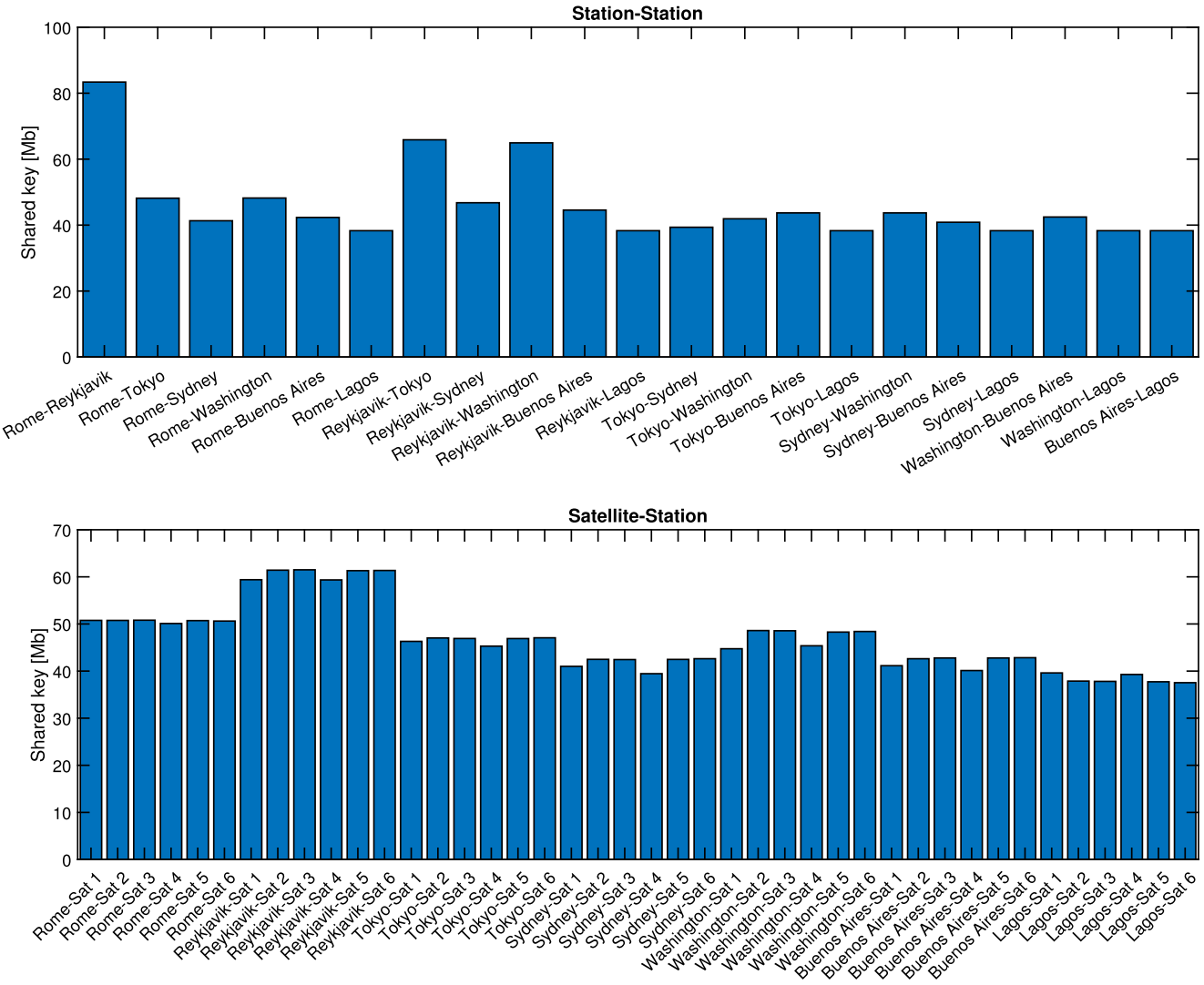

Fig. 5. Global constellation: length of the k_{gg} and k_{sg} generated.

application of a QKD constellation, the case of two groups of stations, each belonging to a narrow band of latitude values, is more interesting as it raises the question of whether is still convenient to use a single plane constellation or two planes, each one "specialized" for one group of stations.

Let us consider the networks of stations in Table 3, each has a group of three stations having latitude between 40° and 43°, and another group with almost equatorial latitude in the first case, and between 19° and 23° in the second case; for convenience let us call them network 40/0 and network 40/20. The comparison between single and two planes constellations is presented in Table 4, it can be seen that for the 40/0 case, in which the second group of stations is almost equatorial, the single plane constellation has a better minimum key, but the total key is about three times lower than the two planes constellation. Instead, in the 40/20 case, the single plane is better in both values.

The behavior of the first case can be explained looking at Fig. 7, showing the satellite-station keys and keeping in mind that, with two planes, the satellites on the inclined orbit (satellites 1,2, and 3 in Fig. 7) generate keys with all the stations, but they produce longer keys with the high latitude stations. On the other hand, the equatorial satellites (satellites 4,5, and 6) generate keys only with the equatorial stations, but such keys are much longer. Therefore, since the minimum key is limited by the minimum satellite-station key, it is determined by the shorter key between equatorial stations and inclined satellites (in Fig. 7 the ones between satellites 1,2,3 and Quito, Nairobi, and Kuala Lumpur stations); while the total key benefits both from the high length of the keys of the equatorial stations and the ones of the high latitude stations. Instead, in the case 40/20, the situation in which one group of stations gains much longer keys than the other does not happen, therefore no advantage on the total key is gained.

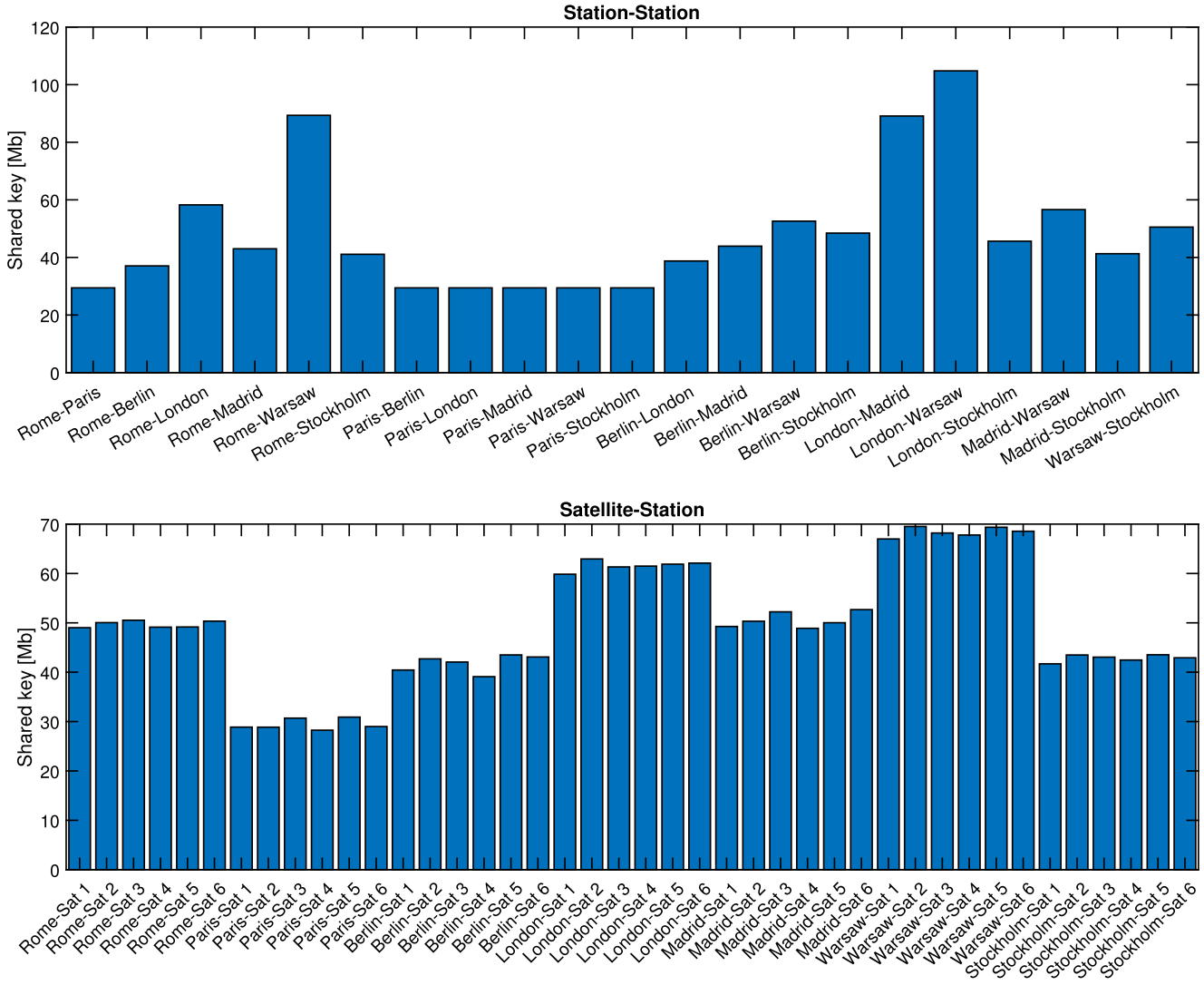

Fig. 6. Regional constellation: length of the k_{gg} and k_{sg} generated.

Table 3
Constellations with two groups of stations.

	Network 40/0			Network 40/20	
Station	**Lat. [deg]**	**Lon. [deg]**	**Station**	**Lat. [deg]**	**Lon. [deg]**
Rome	41.90	12.50	Rome	41.90	12.50
New York	40.73	−73.93	New York	40.73	−73.93
Sapporo	43.07	141.35	Sapporo	43.07	141.35
Quito	−0.18	−78.47	Mexico City	19.43	−99.13
Nairobi	−1.29	36.82	Mumbai	19.08	72.88
Kuala Lumpur	3.14	101.69	Hong Kong	22.30	114.18

Table 4
Constellations with two groups of stations: orbits and key generated.

	i [deg]	Ω_0 [deg]	$k_{gg,min}$ [Mb]	$k_{gg,tot}$ [Mb]
Single plane - 40/0	40.48	−22.60	58.40	1226.30
Two planes - 40/0	$i_1 = 43.99,\ \ i_2 = 0.17$	$\Omega_{0_1} = 127.21,\ \Omega_{0_2} = 123.01$	27.10	3731.80
Single plane - 40/20	41.33	118.31	66.10	1447.60
Two planes - 40/20	$i_1 = 43.98,\ \ i_2 = 26.86$	$\Omega_{0_1} = 192.10,\ \Omega_{0_2} = 70.49$	30.90	1341.20

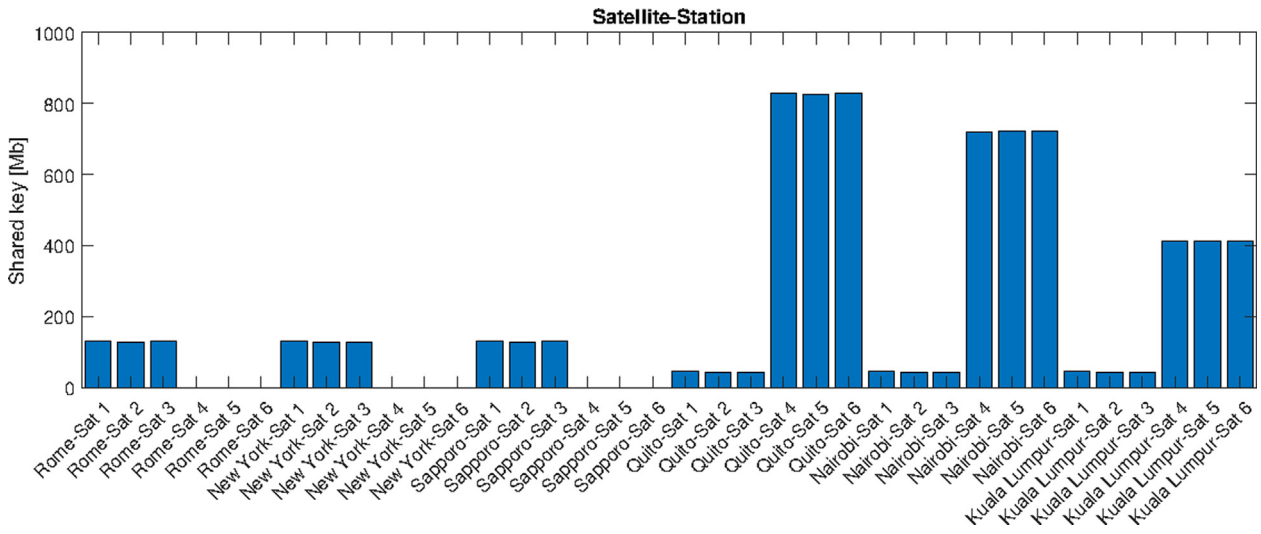

Fig. 7. Constellation with two groups of station, case 40/0: length of the k_{sg} generated.

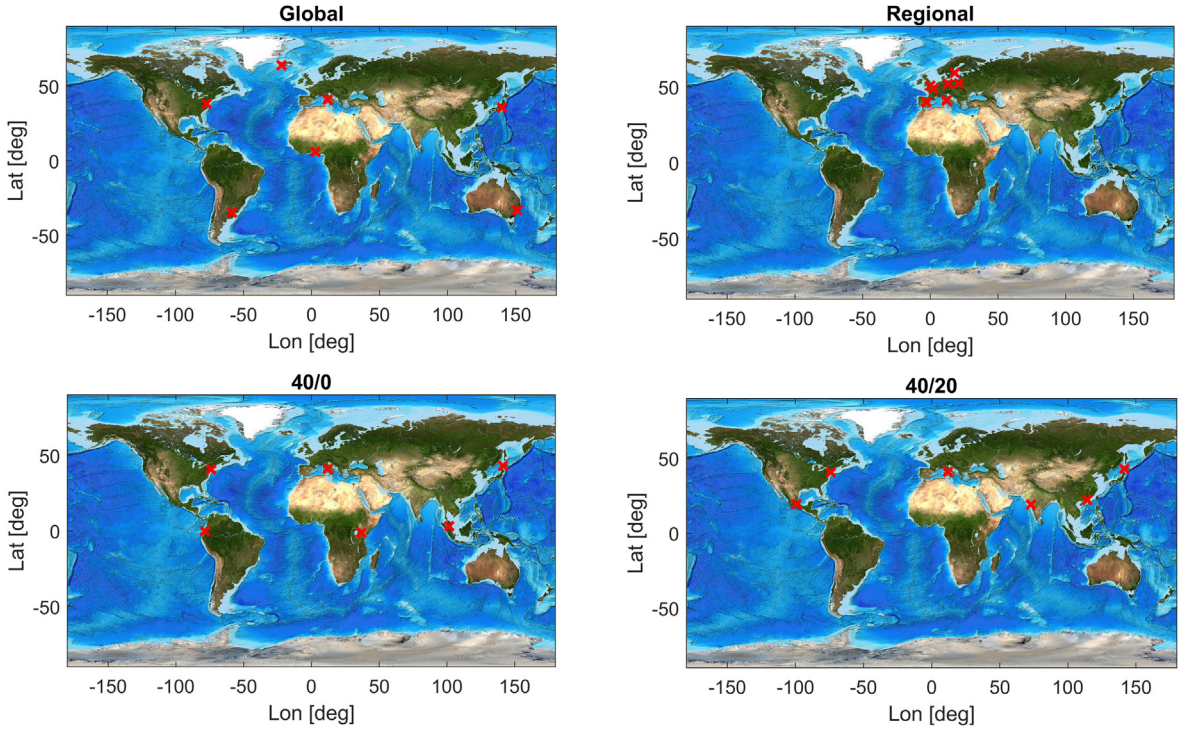

Fig. 8. Stations in the four networks considered: global, European regional, two groups of latitude 40/0 and 40/20.

Fig. 8 shows the position of the stations of all the networks considered on the world planisphere, to allow an easier visualization.

5. Constellations with Inter-satellite links

The results of Table 4, and Fig. 7 show that this kind of constellation would benefit from the ability of transmitting keys between satellites. Until now, each satellite acted on its own, independently from the others, the Inter-satellite links (ISL) can be thought as a mean of passing keys from one satellite to another. In theory, two satellites can establish a quantum link between themselves, and using it to perform QKD, thus sharing a secret key (we could call these satellite-satellite keys) that can in turn be used to securely transmit part of a satellite-station key from one to the other.

In general, the ISL can be of two kinds: intra-planar links, if the link is between two satellites on the same orbital plane, and inter-planar links, if it is between satellites on

different planes. Inter-planar links are generally believed to be more challenging, because of the high relative velocities of the satellites and the shorter visibility windows. With the key distribution process among the stations used in this work, the ISL are able to change how the satellite-station keys are divided between the satellites, while they cannot increase the total length of all the keys produced. Given the performance index considered, the minimum station-station key, ISL can improve it when the k_{sg} are not balanced between the satellites; the situation of Fig. 7 is one of these cases.

Assuming that N_s satellites exchange portions of their $k_{sg,i}$ keys, they produce a re-distributed $k_{sg\,ISL,i}$. In a formal way, the process can be described as in Eq. (14) and Eq. (15): the satellite s exchanges keys it shares with station i with the satellites having an ISL with it, which belong to the set $ISL(s)$. $y_i^{s,h} \in [-1,1]$ is a coefficient (similar to x_{ij} in Section 3) that determines the entity of the exchanged key, if it is negative, the keys is transferred from satellite s to satellite h, the other way around if it is positive. $f_{sg,i}^{s,h}(y)$ is a function that is equal to $k_{sg,i}^{s}$ if $y<0$ and to $k_{sg,i}^{h}$ if $y>0$ (sign in Eq. (15) is the sign function, equal to 1 if the argument is positive, to -1 if it is negative and to zero if it is null). The ISL key between satellite s and s' consumed by the operation for N_g ground stations is given in Eq. (16); the link must be able to sustain this quantity of bits transferred.

$$k_{sg\,ISL,i}^{s} = k_{sg,i}^{s} + \sum_{h\in ISL(s)} y_i^{s,h} f_{sg,i}^{s,h}(y_i^{s,h}) \tag{14}$$

$$f_{sg,i}^{s,h}(y_i^{s,h}) = \left[\frac{1-\mathrm{sign}(y_i^{s,h})}{2}k_{sg,i}^{s} + \frac{1+\mathrm{sign}(y_i^{s,h})}{2}k_{sg,i}^{h}\right] \tag{15}$$

$$k_{ISL,\mathrm{consumed}}^{ss'} = \sum_{i=1}^{N_g} |y_i^{ss'}|\, f_{sg,i}^{ss'} \tag{16}$$

From the equations above, an optimization problem, similar to the one of distributing the station-station keys (problem B) can be implemented. The objective would be to maximize the sum of the minimum $k_{sg,\,ISL}$ re-distributed keys, given the k_{sg} and varying the $y_i^{s,h}$ coefficients, considering also the constraint $k_{sg\,ISL,i}^{s} \geqslant 0$, i.e. a satellite cannot transfer a key longer than the one it has.

A particular solution of the ISL optimization problem is the one that equalizes all the satellite-station keys between the satellites: $k_{sg,ISL,i}^{h} = \langle k_{sg,i}\rangle_s \; \forall h \in \{1,\ldots,N_s\}$ ($\langle\ \rangle_s$ indicates the mean over all the satellites). From preliminary tests it was understood that, for what concerns the minimum key, this solution is as good as the numerical solution of the general optimization problem, with the advantage of being simpler; therefore the ISL were implemented in this way. Furthermore, it was considered that every satellite can communicate with all the others, which does not necessarily means that every satellite must have a real link with the rest, it is sufficient that: it exist a path between every pair of satellites, allowing the keys to be passed from satellite to satellite until the destination is reached, and the ISL are efficient enough to sustain all the traffic. Estimating what is the capability of the ISL is not trivial and is outside the purpose of this work, instead is kept track of the maximum ISL length needed as a measure of how good the links must be.

The equalization of k_{sg} with ISL is applied in the cases of the previous section; starting with the single plane solutions of Table 2, but in these cases the variations due to ISL are minimal (in fact, from Fig. 5 and Fig. 6) it is apparent that the satellite-station keys are already very close to be equalized). Then two planes constellations with ISL are tested for the global and regional case, the results are reported in Table 5 where it is also shown the percentage variation with respect to the single plane solution without ISL.

In the global constellation there is an increase on the minimum key and a more consistent one the total key, proving that, with ISL, the two plane solution has better performance. One of the two orbits one has access to all the stations except the higher latitude one (Reykjavik), the other has access to all the stations. The k_{gg} and k_{sg} produced are shown in Fig. 9.

For the regional constellation there is still an advantage on the minimum key, but the total key is almost unchanged, in this case as well one of the orbits have access to the highest latitude station (Stockholm) while the other does not. Fig. 10 reports the key lengths in this case.

As for the stations in Table 3, with two groups in different latitude bands, the results of the ISL application are reported in Table 6. Comparing with the two planes cases of Table 4 the 40/0 constellation with ISL maintains the length of the total key, with a great advantage over the single plane (almost three times), which is mainly due to the equatorial stations; this time also the minimum key shows a consistent improvement, gaining a 20 Mb in length. The 40/20 constellation presents a better minimum key as well, but the total key is slightly less than the correspondent single plane. The k_{sg} and k_{gg} key lengths of the two networks are reported Fig. 11 and Fig. 12.

Table 5
Global and regional constellations: orbits and key generated, with two orbital planes and ISL. In the fifth and sixth column are shown the percentages respect to the single plane without ISL case, the last column reports the required length of the links.

	i_1 [deg]	i_2 [deg]	Ω_{0_1} [deg]	Ω_{0_2} [deg]	$k_{gg,min}$ [Mb] (%)	$k_{gg,tot}$ [Mb] (%)	$k_{ISL,c}$ [Mb]
Global	38.00	114.42	40.75	51.59	44.40 (+15.7%)	1450.20 (+49.2%)	706.30
Regional	51.98	120.79	−62.14	122.54	38.00 (+33.1%)	1020.20 (−0.1%)	257.00

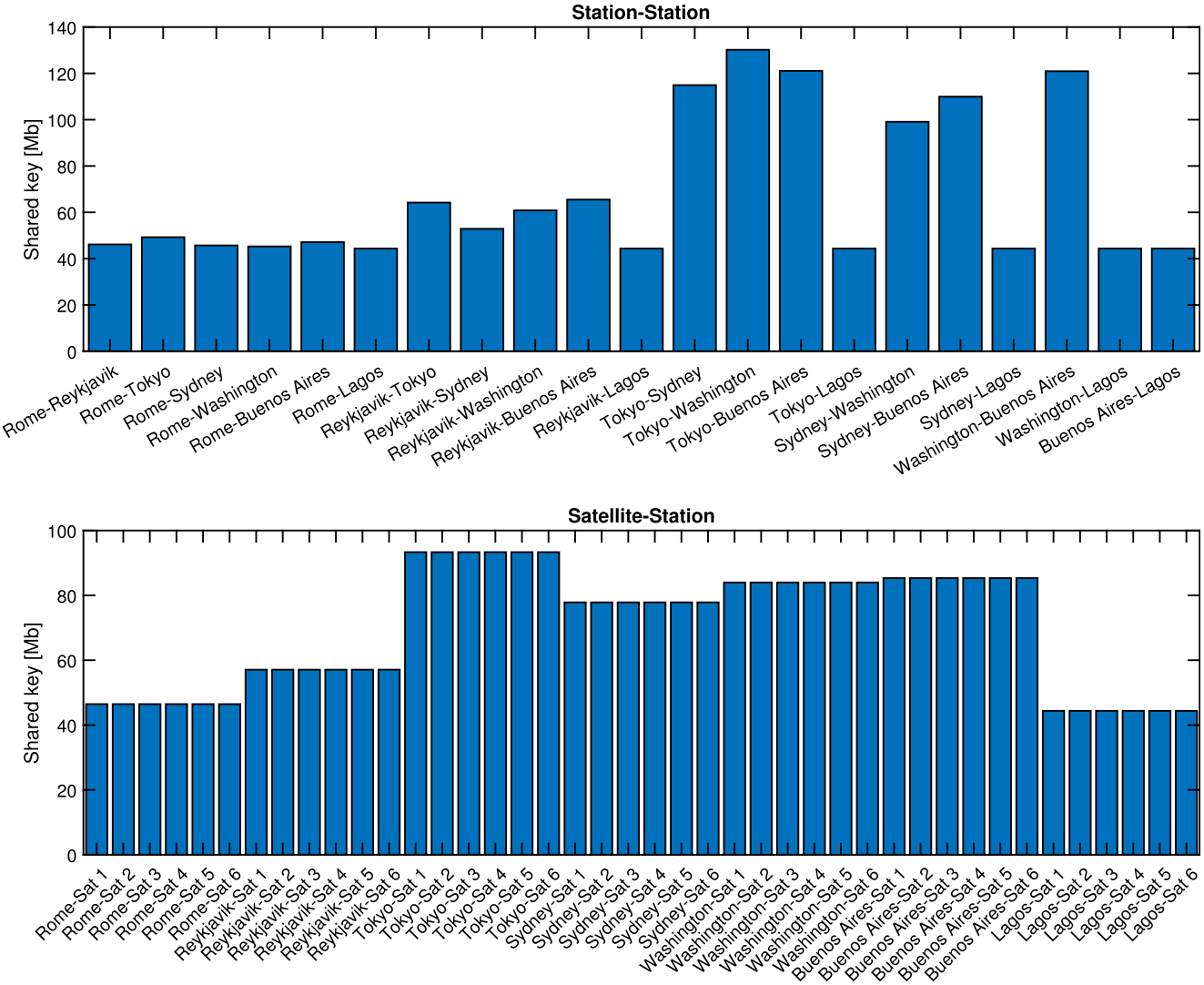

Fig. 9. Global constellation with two orbital planes and ISL, k_{gg} and k_{sg}. Notice that, for each station, the k_{sg} are equal between the satellites.

6. Daily key performance analysis

In the contest of cryptography, a shared secret key between two parties is considered less and less secure the more time passes from its generation; therefore it is interesting to analyze also the daily performance of a satellite QKD constellation. From this this point of view the constellation must be able to generate a non-zero key length value between each pair of stations every n number of days. To achieve this, at least one satellite must have access to all the stations of the network every day during the entire year; using ISL can provide a significant advantage also for this problem, since they allow to equalize the keys among the satellites.

With the notation of this work the quantity of interest is the minimum station-station daily key size $k_{day_{min,gg}}$; every day, every pair of stations share a new key with length greater or equal than this value.

Considering now the constellations studied in the previous sections, all the cases, with the exception of the sun-synchronous orbit of the single plane global constellation, present extended periods of time in which no new key is generated. As an example, in Fig. 13 it can be seen the case of the regional single plane constellation ($i = 57.46^\circ, \Omega_0 = 59.46^\circ$) key rates between one satellite and the station of Rome.

Such behavior can be fixed adding new satellites in orbital planes with a shifted Ω_0, in such a way that at least one plane is always capable of accessing the stations. Still, the constraint of only nighttime operations, naturally causes an interval of time in which the daily key decreases, in fact, every non-equatorial station will experience a period of shorter nights during the year (summer or winter depending on the hemisphere). When high (absolute) latitude stations are present, for example Reykjavik and Stockholm, the effect is more accentuated, since during summer they

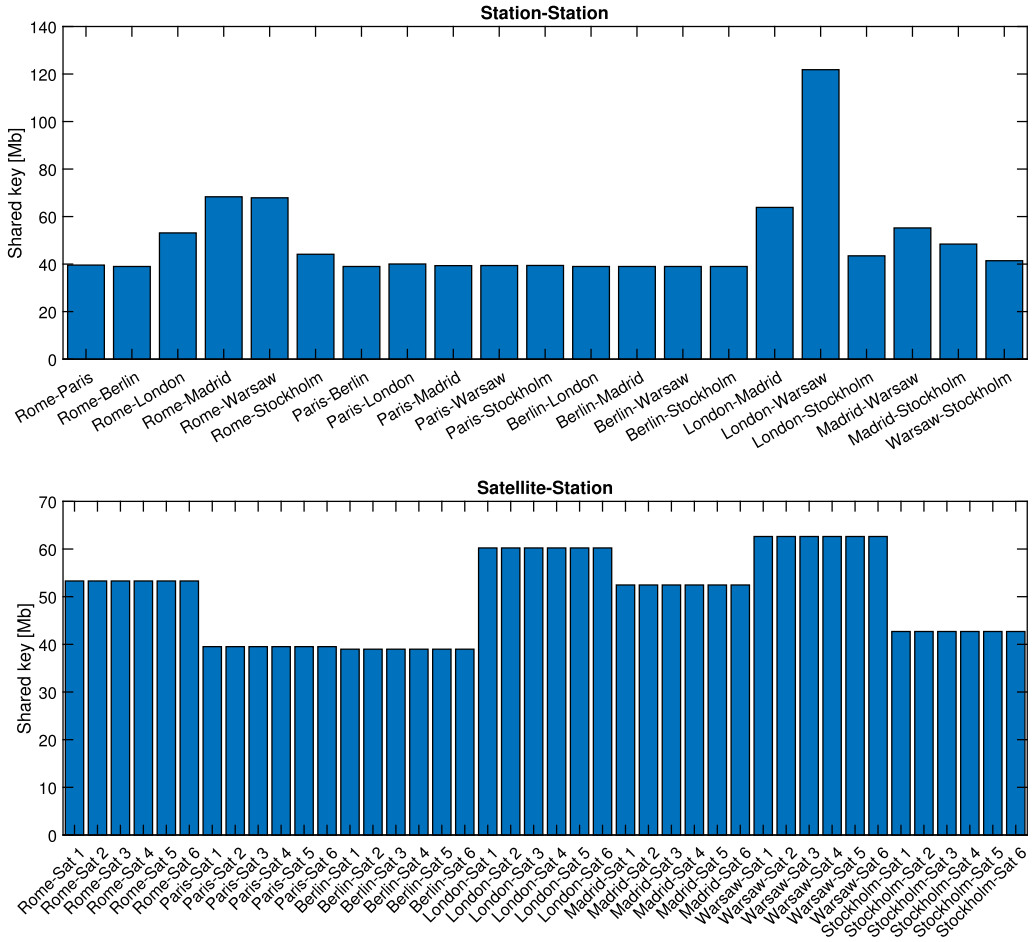

Fig. 10. Regional constellation with two orbital planes and ISL, k_{gg} and k_{sg}. Notice that, for each station, the k_{sg} are equal between the satellites.

Table 6
Constellations with two groups of stations: keys generated with two orbital planes and ISL. The stations are those of Table 3, and the orbits are the same as Table 4, the percentages are with respect to the single plane solutions.

	$k_{gg,min}$ [Mb] (%)	$k_{gg,tot}$ [Mb] (%)	$k_{ISL,c}$ [Mb]
Network 40/0	77.70 (+33.0%)	3593.50 (+193.0%)	3326.30
Network 40/20	78.30 (+18.4%)	1381.20 (−4.6%)	919.20

experience very short nights. For example the sun-synchronous orbit of the global constellation experiences a fall of the daily key from around 16 kbit to 1.5 kbit due to Reykjavik suffering the summer months. Instead, in the 40/0 and 40/20 networks this issue is less relevant.

Let us now consider the daily key performance of the previously studied configurations, every constellation is expanded adding two new orbital planes for each existing one, with the same inclination of the original ones and RAAN shifted of 120° and 240°. Therefore, for instance, the former single plane regional constellation becomes a three plane constellation with the orbital planes having the same inclination and equally spaced in right ascension; in a similar way the former two-plane regional constellation becomes a six plane constellation with two sets of three orbital planes having different inclination. The only exceptions are the sun-synchronous global constellation and the almost equatorial plane of the 40/0 constellation.

In Table 7 are reported the minimum station-station daily keys generated, averaged over one year. Since now almost all the constellations are multi-plane, the main distinction is between single inclination and double inclination configurations, in order to maintain the comparisons of the previous sections. It should be noted that these results consider the use of ISL, in fact, they are even more important for the daily key performance, since they allow to at least double the mean daily key, in both single and double inclination constellations. The values of Table 7 show an

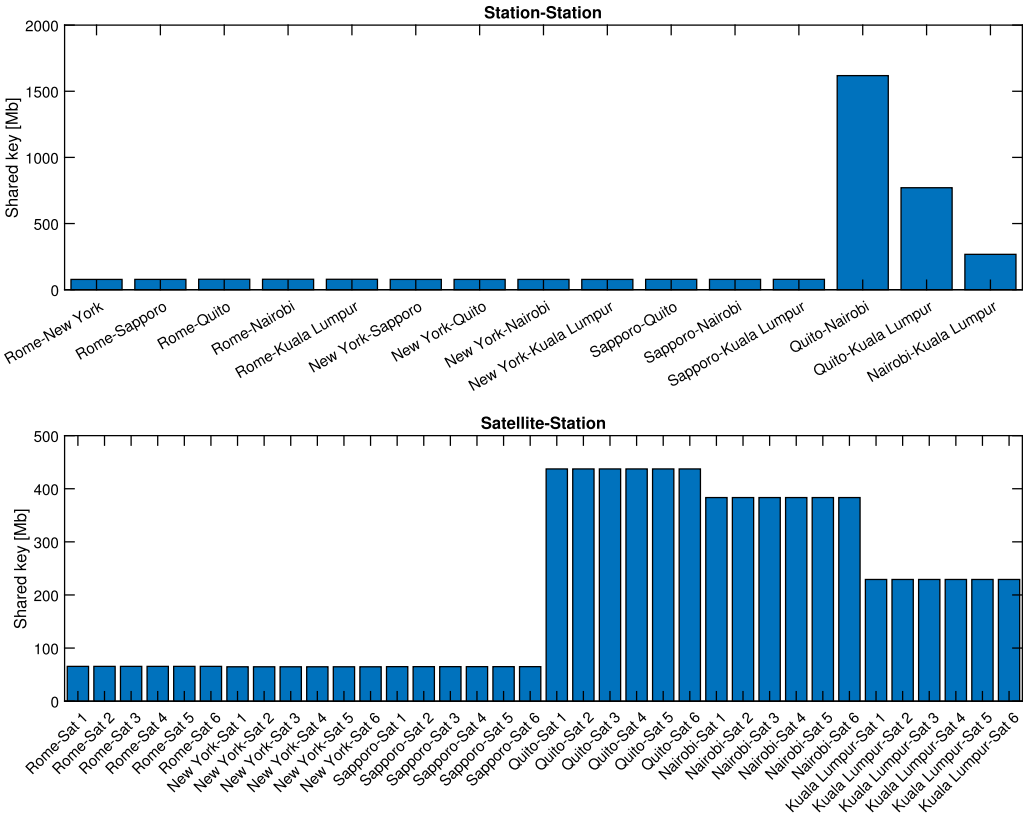

Fig. 11. k_{gg} and k_{sg} for the 40/0 constellation with two groups of stations.

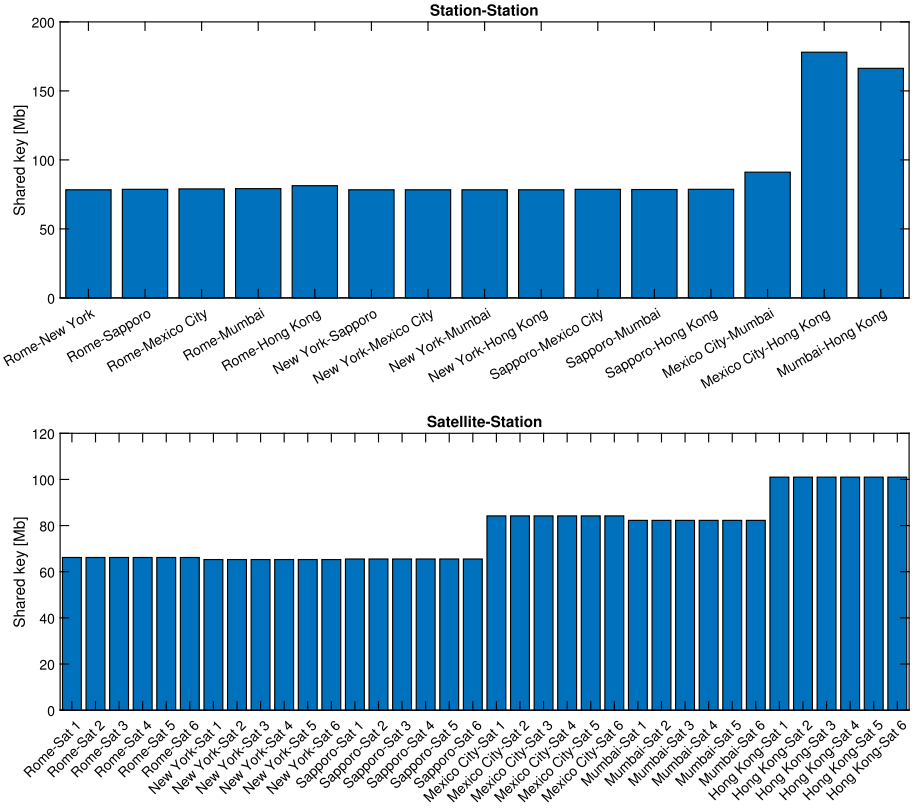

Fig. 12. k_{gg} and k_{sg} for the 40/20 constellation with two groups of stations.

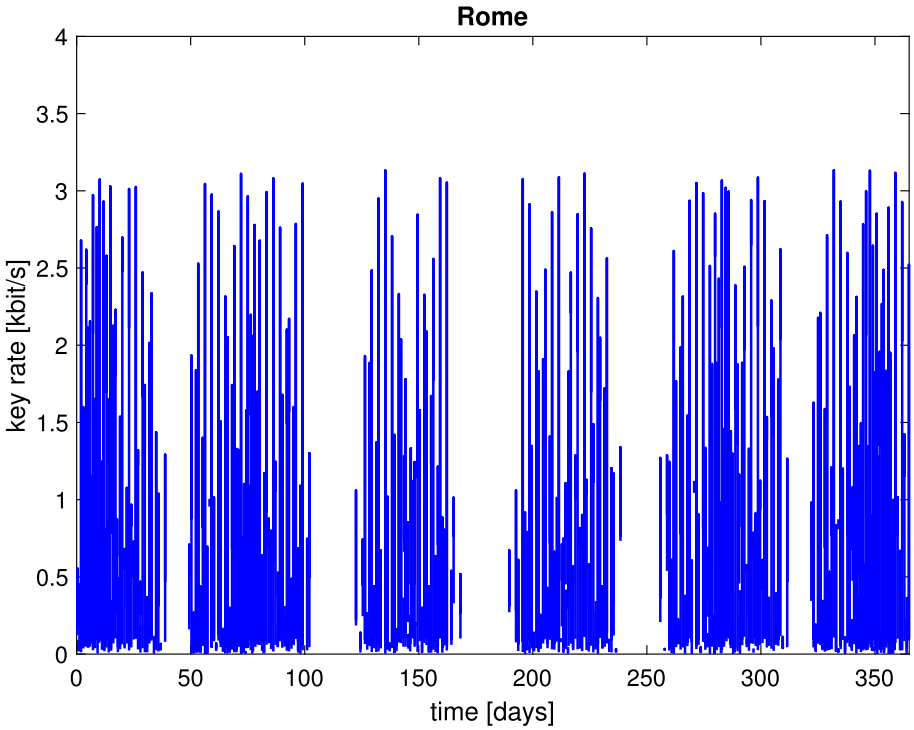

Fig. 13. Regional single plane constellation, key rates with Rome station.

Table 7
Mean of the minimum station-station daily key over one year; ISL are used. The first column refers to constellation in which all the planes have the same inclination, the second column instead considers constellations with two inclination. The values are per satellite.

	Single incl. $\langle k_{day_{gg,min}} \rangle$ [kb]	Double incl. $\langle k_{day_{gg,min}} \rangle$ [kb]
Global	10.41	12.87
Regional	9.06	12.37
Network 40/0	21.96	47.63
Network 40/20	26.11	30.75

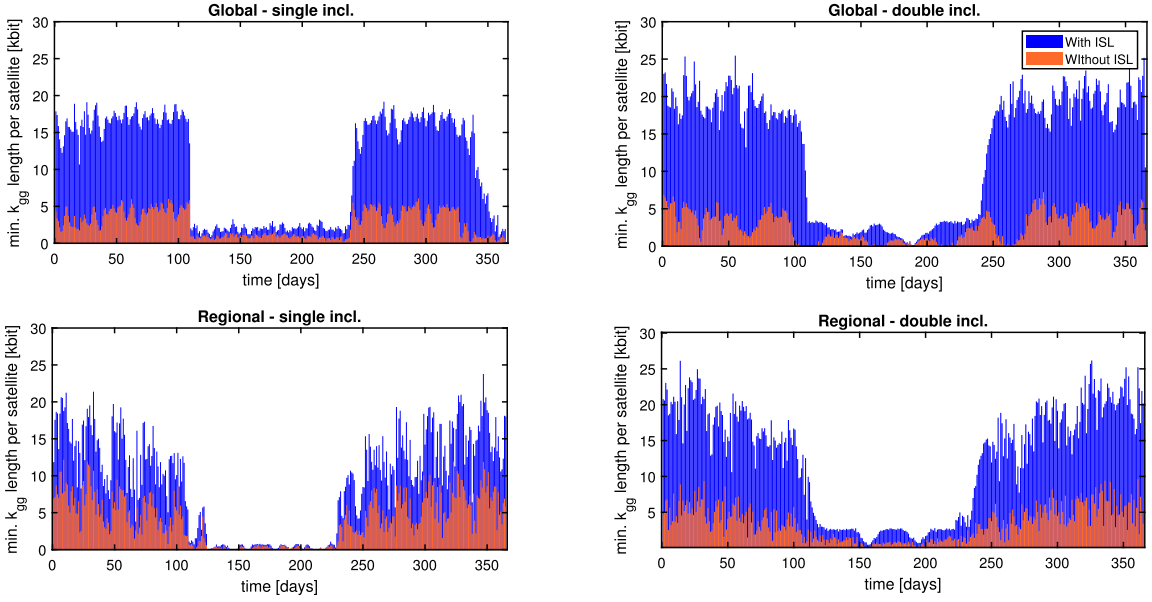

Fig. 14. Daily minimum station-station key for the global network (upper plots) and regional network (lower plots), on the left there are the single inclination constellation, on the right the double inclination ones. The blue and orange plots refer respectively to the presence or absence of ISL.

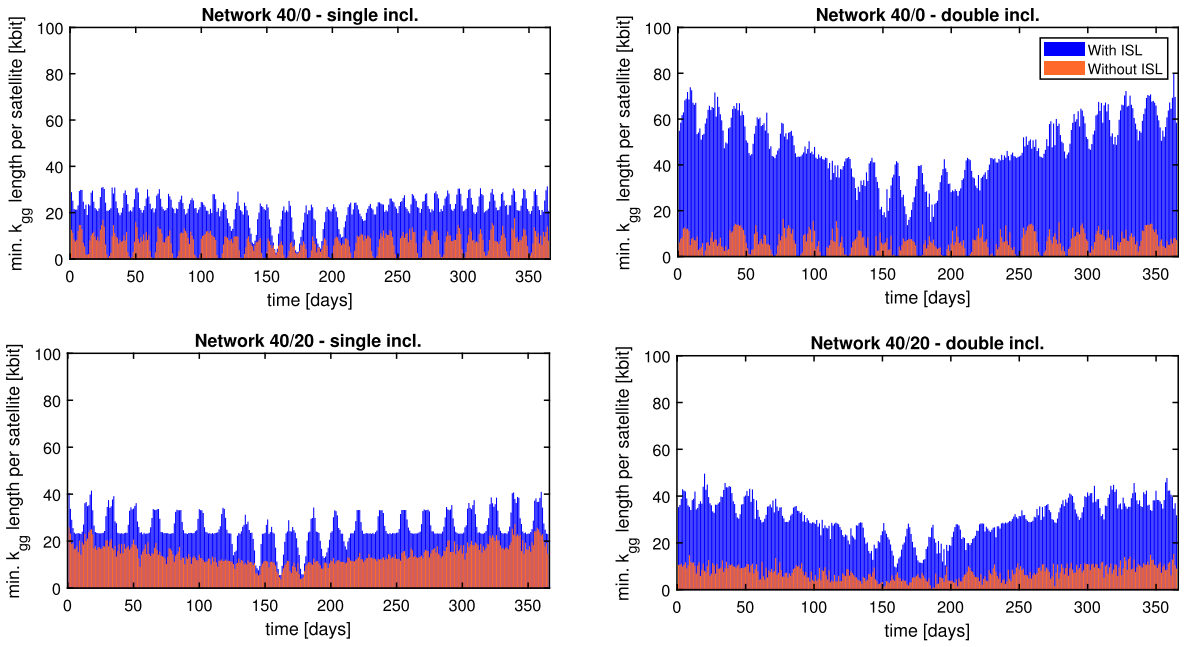

Fig. 15. Daily minimum station-station key for the 40/0 network (upper plots) and 40/20 network (lower plots), on the left there are the single inclination constellation, on the right the double inclination ones. The blue and orange plots refer respectively to the presence or absence of ISL.

improved performance of the double inclination constellation over the single ones also concerning the daily key size.

In Figs. 14 and 15 are shown the daily keys during one year for the configurations of Table 7, it is highlighted how much the ISL can change the values.

7. Conclusions

The design of the orbits for a QKD constellation was studied, with particular attention to different networks of ground stations and how their geographical disposition influences the optimal orbits of the satellites, with or without ISL. The minimum key between a pair of stations in the network was chosen as main performance index, but also the length of the total key, sum between all the stations pair, was kept in consideration. The problem of selecting the best orbit that maximizes the minimum key was cast as an optimization, as well as the problem of distributing station-station keys from satellite-station keys.

A global, a regional and two constellations with stations divided in two groups of latitude were considered; single and multi plane with different orbital inclinations constellations are compared concluding that, with ISL, the multi plane have better performances concerning the minimum key, and the total key can either remain similar to the single plane, show a slight decrease or an improvement (a big one in some cases). With multi plane constellations the ISL would include inter-planar links, which are believed to be challenging, therefore the improvements obtained are constrained to the capability of realizing such links.

In the global and the regional constellations both showed an improvement after implementing ISL and considering two orbital planes having different inclination, with an increase of 15.7% and 33.1% of the minimum key respectively; in the global case, the total key was also improved of 49.2%, while in the regional it remained almost constant.

The ground network 40/0 was the one which benefited the most from ISL and multi plane configuration, in fact, the links allow to transfer some of the keys shared with the equatorial stations to the satellites in the inclined orbit, improving the minimum key (+33.0%); at the same time the total key has a great advantage (+193.0%) due to the high key rates and frequent passages of the equatorial satellite over the equatorial stations. Not always the improvement is as good for networks with two groups of stations, as the 40/20 constellation demonstrates: in this case there is still an improvement (+18.4%) on the minimum key, but the total key is slightly decreased.

Then the performance of the daily key is addressed, the previous constellations are extended with additional orbital planes equally spaced in Ω; the comparison is now between single orbit inclination and double inclination configurations. The results show that the double inclination constellation consistently provide a better daily key size; again, the greater improvement is for the 40/0 network which passes from an average 22 kbits to 48 kbits per satellite. For this performance metrics as well, the importance of ISL is highlighted, showing how they are even more useful not only to transfer keys between orbital planes but also between the satellites in the same plane.

In conclusion, satellite constellations for QKD having multiple planes, also with different inclination, in combination with ISL, are likely to improve both the quantity of secret key material produced in a long time and the daily performance. The design choices are also heavily influenced

by the characteristic of the ground stations network and how they are distributed, their latitude being the most influential parameter. Possible future extensions of this work could include: improvements to the link model, by removing some simplifying hypotheses, a more advanced analysis of the ISL considering instantaneous inter-satellite visibility and quantum transmission, a large scale simulation, increasing the number of satellites and ground stations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Parameters of the link model and Key rate expression

This appendix gives the expression of the asymptotic key rate used to build the link model and determining the length of the generated keys. The numerical values of the parameters of the link are instead given in Table A.1.

The total transmittance, and the expressions of the free space and atmospheric transmittances are already given in the text (Eq. (1), Eq. (2) and Eq. (3)). The width of the Gaussian beam $w(L)$ at distance L appearing in the free space transmittance is expanded in Eq. (A.1), where w_0 is the minimum width of the beam, and λ is the wavelength of the signal.

$$w(L) = w_0\sqrt{1+\left(\frac{L\lambda}{\pi w_0^2}\right)^2} \tag{A.1}$$

In QKD transmission, the main source of noise comes from the background photons that enter the receiver together with the signal photons, the expression of the energy of the noise photons is given in Eq. (A.2), where H_b is the sky brightness, in this work it is considered constant during the day, the night and the twilight, considered as one hour before and after sunrise and sunset; R_{rec} is the radius of the receiver, $\Delta\lambda$ is the filter bandwidth, Δt is the detection time-window.

Table A.1
Numerical values of the employed link model parameters.

R_{rec} [cm]	25	η_{tr}	0.5
w_0 [cm]	2.5	η_{rec}	0.5
λ [nm]	800	η_{point}	0.5
$H_{b_{\text{night}}}$ [$\text{Wm}^{-2}\text{sr}^{-1}\mu\text{m}^{-1}$]	10^{-4}	η_{atm_0}	0.77
$H_{b_{\text{day}}}$ [$\text{Wm}^{-2}\text{sr}^{-1}\mu\text{m}^{-1}$]	1	μ	0.5
$H_{b_{\text{twilight}}}$ [$\text{Wm}^{-2}\text{sr}^{-1}\mu\text{m}^{-1}$]	10^{-3}	ν	0.1
Ω_{FOV} [sr]	$5.383\cdot10^{-8}$	e_0	0.5
$\Delta\lambda$ [μm]	10^{-3}	e_{det}	0.015
Δt [ns]	1	f(E_μ)	1.22
f_{dark} [Hz]	50	q	0.5
f_{source} [MHz]	100	$N_\mu/(N_\mu+N_\nu)$	0.5

$$N = H_b\Omega_{\text{FOV}}\pi R_{\text{rec}}^2\Delta\lambda\Delta t \tag{A.2}$$

The decoy-state BB84 is considered as QKD protocol, using Weak Coherent Pulses (WCP) as source and two decoy states, the mean photon number of the signal state is μ, the decoys are ν and the vacuum state. For an in depth discussion of decoy-state BB84 and the meaning of the quantities in the following equations, see (Ma et al. (2005)).

The asymptotic key rate of decoy-state BB84 is lower bounded by the expression in Eq. (A.3), the expressions of the terms appearing in the KER equation are given in Eq. (A.4) to Eq. (A.9); they depend on μ and ν, the total transmittance, e_0 the error of the background, e_{det} which characterize the alignment and stability of the optical detection system, $N_\mu/(N_\mu+N_\nu)$ is the ratio between signal photons and total number of photons, q is the basis reconciliation factor of BB84, and $f(E_\mu)$ is the efficiency of the error correction code.

$$\begin{aligned}\text{KER} \geqslant q\tfrac{N_\mu}{(N_\mu+N_\nu)}[&-Q_\mu f(E_\mu)H_2(E_\mu)\\&+Q_1^L(1-H_2(e_1^U))]\end{aligned} \tag{A.3}$$

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x) \tag{A.4}$$

$$Q_\mu = Y_0 + 1 - e^{-\eta_{tot}\mu} \tag{A.5}$$

$$E_\mu = \frac{e_0Y_0 + e_{\text{det}}(1-e^{-\eta_{tot}\mu})}{Y_0+1-e^{-\eta_{tot}\mu}} \tag{A.6}$$

$$Y_1^L = \frac{\mu}{\mu\nu-\nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu\frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2}Y_0\right) \tag{A.7}$$

$$Q_1^L = \mu e^{-\mu}Y_1^L \tag{A.8}$$

$$e_1^U = \frac{E_\nu Q_\nu e^\nu - e_0Y_0}{Y_1^L\nu} \tag{A.9}$$

$$Y_0 = \eta_{rec}\frac{N}{hc/\lambda} + 4f_{\text{dark}}\Delta t \tag{A.10}$$

Y_0 is the background rate, which includes the detector dark count and other background contributions such as the stray light, it can be related to the number of noise photons by Eq. (A.10), where h is the Planck constant, c is the speed of light, and f_{dark} is the detector dark count rate (Gruneisen et al. (2015)).

References

Bedington, R., Arrazola, J., Ling, A., 2017. Progress in satellite quantum key distribution. npj Quant. Informat. 3 (1), 1–13. https://doi.org/10.1038/s41534-017-0031-5.

Belenchia, A., Carlesso, M., Bayraktar, Ömer, et al., 2022. Quantum physics in space. Phys. Rep. 951, 1–70. https://doi.org/10.1016/j.physrep.2021.11.004. Quantum Physics in Space.

Bennett, C., Brassard, G., Mermin, N., 1992. Quantum cryptography without bell's theorem. Phys. Rev. Lett. 68 (5), 557–559. https://doi.org/10.1103/PhysRevLett.68.557.

Bennett, C.H., Brassard, G., 1984. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, New York, pp. 175–179.

Bonato, C., Tomaello, A., Deppo, V., et al., 2009. Feasibility of satellite quantum key distribution. New J. Phys. 11, 045017. https://doi.org/10.1088/1367-2630/11/4/045017.

Boone, K., Bourgoin, J.-P., Meyer-Scott, E., et al., 2015. Entanglement over global distances via quantum repeaters with satellite links. Phys. Rev. A - Atomic Mol. Opt. Phys. 91 (5), 052325. https://doi.org/10.1103/PhysRevA.91.052325.

Bourgoin, J.-P., Meyer-Scott, E., Higgins, B., et al., 2013. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. New J. Phys. 15, 023006. https://doi.org/10.1088/1367-2630/15/2/023006.

Dequal, D., Trigo Vidarte, L., Roman Rodriguez, V., et al., 2021. Feasibility of satellite-to-ground continuous-variable quantum key distribution. npj Quant. Informat. 7 (1), 1–10. https://doi.org/10.1038/s41534-020-00336-4.

Ekert, A., 1991. Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 67 (6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661.

Gruneisen, M., Flanagan, M., Sickmiller, B., et al., 2015. Modeling daytime sky access for a satellite quantum key distribution downlink. Opt. Express 23 (18), 23924–23934. https://doi.org/10.1364/OE.23.023924.

Hwang, W.-Y., 2003. Quantum key distribution with high loss: Toward global secure communication. Phys. Rev. Lett. 91 (5), 057901. https://doi.org/10.1103/PhysRevLett.91.057901.

Khatri, S., Brady, A., Desporte, R., et al., 2021. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. npj Quant. Informat. 7 (1), 1–15. https://doi.org/10.1038/s41534-020-00327-5.

Liao, S.-K., Cai, W.-Q., Liu, W.-Y., et al., 2017. Satellite-to-ground quantum key distribution. Nature 549 (7670), 43–47. https://doi.org/10.1038/nature23655.

Liorni, C., Kampermann, H., Bruß, D., 2019. Satellite-based links for quantum key distribution: Beam effects and weather dependence. New J. Phys. 21 (9), 093055. https://doi.org/10.1088/1367-2630/ab41a2.

Ma, X., Qi, B., Zhao, Y., et al., 2005. Practical decoy state for quantum key distribution. Phys. Rev. A - Atomic Mol. Opt. Phys. 72 (1), 012326. https://doi.org/10.1103/PhysRevA.72.012326.

Mazzarella, L., Lowe, C., Lowndes, D., et al., 2020. Quarc: Quantum research cubesat—a constellation for quantum communication. Cryptography 4 (1), 1–25. https://doi.org/10.3390/cryptography4010007.

Munro, W., Azuma, K., Tamaki, K., et al., 2015. Inside quantum repeaters. IEEE J. Sel. Top. Quantum Electron. 21 (3), 78–90. https://doi.org/10.1109/JSTQE.2015.2392076.

Naughton, D.P., Bedington, R., Barraclough, S., et al., 2019. Design considerations for an optical link supporting intersatellite quantum key distribution. Opt. Eng. 58 (1), 1–13. https://doi.org/10.1117/1.OE.58.1.016106.

Shor, P., 1994. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. https://doi.org/10.1109/SFCS.1994.365700.

Tomaello, A., Bonato, C., Da Deppo, V., et al., 2011a. Link budget and background noise for satellite quantum key distribution. Adv. Space Res. 47 (5), 802–810. https://doi.org/10.1016/j.asr.2010.11.009.

Tomaello, A., Dall'Arche, A., Naletto, G. et al., 2011b. Intersatellite quantum communication feasibility study. In: Proceedings of SPIE - The International Society for Optical Engineering, vol. 8163. pp. 71–78. https://doi.org/10.1117/12.893440.

Vallone, G., Bacco, D., Dequal, D., et al., 2015. Experimental satellite quantum communications. Phys. Rev. Lett. 115 (4), 040502. https://doi.org/10.1103/PhysRevLett.115.040502.

Vergoossen, T., Loarte, S., Bedington, R., et al., 2020. Modelling of satellite constellations for trusted node qkd networks. Acta Astronaut. 173, 164–171. https://doi.org/10.1016/j.actaastro.2020.02.010.

Wang, J., Chen, H., Zhu, Z., 2021. Modeling research of satellite-to-ground quantum key distribution constellations. Acta Astronaut. 180, 470–481. https://doi.org/10.1016/j.actaastro.2020.12.039.

Wang, J.-Y., Yang, B., Liao, S.-K., et al., 2013. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. Nat. Photon. 7 (5), 387–393.

Xu, S., Li, Y., Wang, Y., et al., 2021. Noiseless attenuation for continuous-variable quantum key distribution over ground-satellite uplink. Appl. Sci. 11 (23), 11289. https://doi.org/10.3390/app112311289.