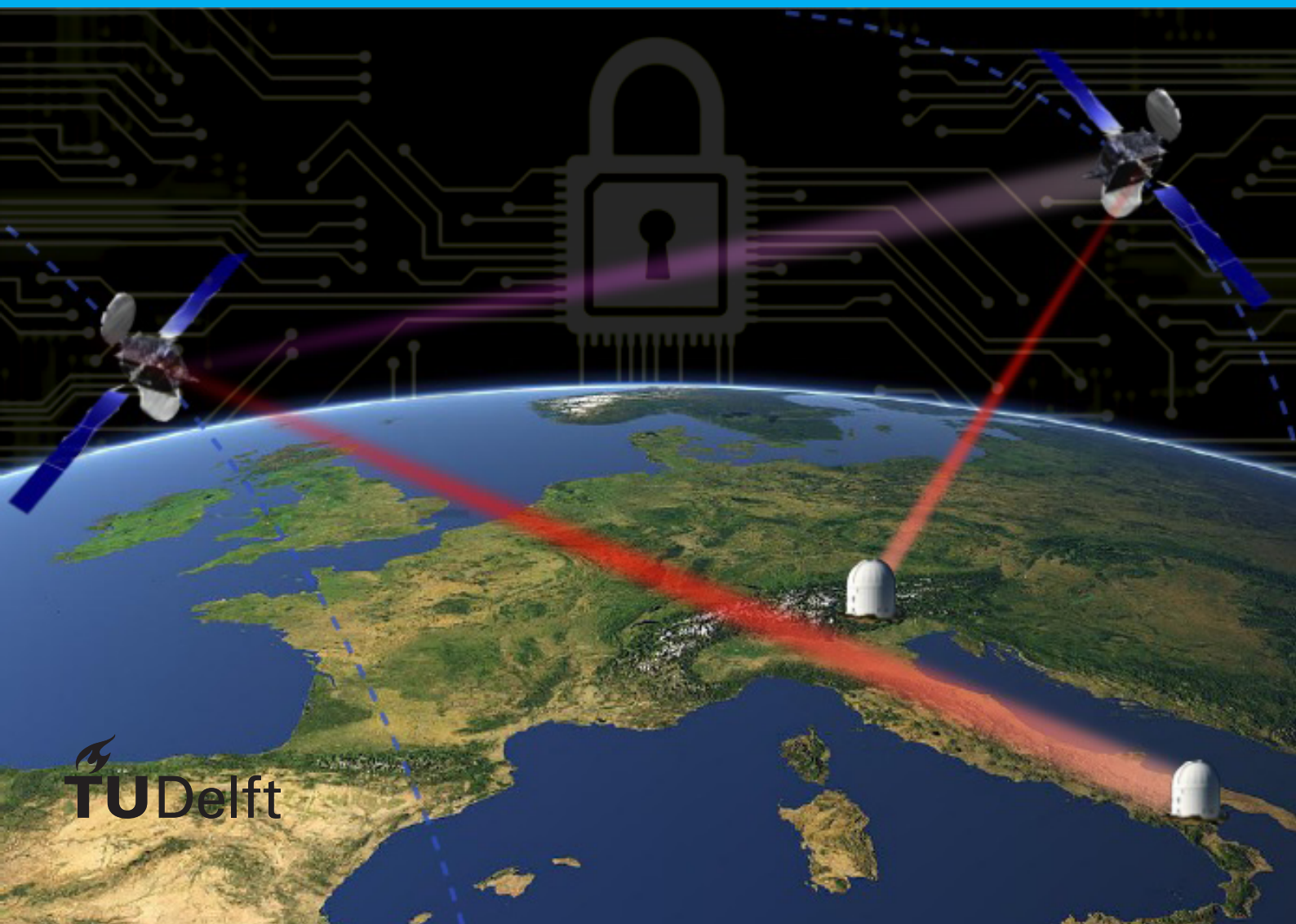
Thesis report

MSc. Aerospace Engineering

Sergio Loarte Castro

Towards a global space-based QKD network



TU Delft

Thesis report

MSc. Aerospace Engineering

by

Sergio Loarte Castro

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on Tuesday January 29, 2019 at 12:30 PM.

Student number:	4569970	
Project duration:	May 1, 2018 – January 1, 2019	
Thesis committee:	Dr. A. Cervone,	TU Delft
	Dr. ir. J.M. Kuiper,	TU Delft, supervisor
	Dr. ir. D. Dirkx,	TU Delft

This thesis is confidential and cannot be made public until January 31, 2019.

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft

Preface

This thesis is the end result of my Masters in Aerospace Engineering at TU Delft. I had the wonderful opportunity of spending six months at the Centre for Quantum Technologies at the National University of Singapore, where most of this thesis was done. This was an outstanding experience, both professionally and personally.

I could not be more grateful to Robert Bedington and Tom Vergoossen, whose daily help and guidance has been fundamental for the success of this work. In more general terms, the whole research team led by Alexander Ling has been extremely welcoming during my experience overseas, sharing their knowledge and expertise whenever it was needed – from the generation of entangled photon pairs to the tastiest Hainanese chicken rice of the island. I also want to express my gratitude to my supervisor Hans Kuiper for making this experience possible and being supportive at all times.

On a more personal level, a big gracias to all the people that have been part of this two-and-a-half-year journey, which I will never forget. Finally, a special thank you to my parents who gave me the opportunity to study what I am passionate about. I am positive it has all been worth it.

Sergio Loarte Castro
Delft, January 2019

Abstract

Quantum Key Distribution (QKD) allows a symmetric key to be distributed between two distant parties in a secure manner. The work of this thesis has been carried out at the Centre for Quantum Technologies at the National University of Singapore, the first institute in the world able to demonstrate a rugged, miniaturized source of entangled photons on a CubeSat. Ready to demonstrate QKD from space in the near future - needed to connect distant nodes due to high losses using optical fiber -, this source can fit in a small satellite. In this thesis a further step into the future is taken, conceiving trusted-node QKD satellite constellations.

A versatile model has been developed, able to simulate satellite-to-ground and inter-satellite QKD for any satellite constellation and ground station combination. Matlab scripts were integrated with the AGI STK software package to compute free-space QKD links. Valuable additions have been included with respect to simulations currently found in literature, such as a realistic cloud coverage simulation, a key management strategy and satellite behaviour designed to maximize key rate when presented with conflicting passes. The operational concept is that the satellites build up a buffer of secure key with every ground station they pass. At a later time, when two ground nodes wish to communicate securely, a symmetric key can be produced by performing an exclusive OR (XOR) on the buffered keys held within the satellites for the two ground nodes. These XOR keys are delivered classically via relay nodes in higher orbits (e.g. geostationary) to allow for secure communications with minimal latency. The XOR operation between two keys is limited by the smallest one, hindering the performance of the constellation. Inter-satellite QKD links are not required but can be used to balance the stored keys between satellites and thus maximize the options available for XOR keys. Implementation of inter-satellite QKD is included in the model, together with a proposed algorithm and high-level guidelines on its practical use and operational constraints.

The model has been successfully validated via replication of the published results obtained by the Chinese Micius satellite. To showcase the model capabilities, two scenarios are proposed, going over the design process of a trusted-node QKD constellation to distribute key to the ground nodes of each network. Trade-offs of different constellation types, key usage patterns and inter-satellite QKD are discussed in these applied cases along with the detection and proposed solutions for the issues arising from the peculiarities of a QKD constellation. Finally, an optimization process with the goal to obtain the maximum key rate possible is discussed. Despite the academic nature of this thesis, this technology presents a promising future for commercialization purposes. Optimization of future commercial QKD satellite constellations will be needed when designing these networks.

Contents

List of Figures

List of Tables

Acronyms

ADCS	—	Attitude Determination and Control System
AES	—	Advanced Encryption Standard
APD	—	Avalanche Photodiode
ASEAN	—	Association of Southeast Asian Nations
CONOPS	—	Concept of Operations
CQT	—	Centre for Quantum Technologies
CV	—	Continuous Variable
DCR	—	Dark Count Rate
DV	—	Discrete Variable
EC	—	Error Correction
EO	—	Earth Observation
FOM	—	Figure of Merit
GA	—	Genetic Algorithm
GEO	—	Geosynchronous Equatorial Orbit
GB	—	Gigabyte
GS	—	Ground Station
ISL	—	Intersatellite Link
LAN	—	Longitude of the Ascending Node
LEO	—	Low Earth Orbit
MEO	—	Medium Earth Orbit
MODIS	—	Moderate-Resolution Imaging Spectroradiometer
NIST	—	National Institute of Standards and Technology
OAT	—	One-at-a-time
OTP	—	One-time Pad
PA	—	Privacy Amplification
QBER	—	Quantum Bit Error Rate
QKD	—	Quantum Key Distribution
QUESS	—	Quantum Experiments at Space Scale
RAAN	—	Right Ascension of the Ascending Node
RF	—	Radio Frequency
RGB	—	Red, Green, Blue
RSA	—	Rivest, Shamir and Adleman
SA	—	Simulated Annealing
SPEQS	—	Small Photon-Entangling Quantum Systems
SC	—	Spacecraft
SSO	—	Sunsynchronous Orbit
STK	—	Systems Tool Kit
SWaP	—	Size Weight and Power
TRL	—	Technology Readiness Level
WCP	—	Weak Coherent Pulse
XOR	—	Exclusive-OR

Nomenclature and symbols

a	—	Orbit semimajor axis
a, b, c	—	Generic sides of triangle
A, B, C	—	Generic angles of triangle
A_f	—	Frontal area
C_D	—	Drag coefficient
d	—	Distance
D_r	—	Diameter of the receiver
e	—	Orbit eccentricity
Err_{point}	—	Satellite pointing error
f	—	Relative phase difference between satellites in adjacent planes
GS_N	—	Ground station N
h	—	Height
i	—	Orbit inclination
J_2	—	Earth's second dynamic form factor
K_N	—	Key exchanged with ground station N
m	—	Mass
mp/ns	—	Constellation with m orbital planes and n satellites per orbital plane
n	—	Orbit mean motion
R_E	—	Earth radius
Sat_i	—	Satellite i
Sky_{Br}	—	Sky brightness
ϵ	—	Elevation angle
θ	—	Generic angle
λ	—	Wavelength
λ_i	—	Longitude at location i
ν	—	Satellite true anomaly
ϕ_i	—	Latitude at location i
ω	—	Orbit argument of periapsis
Ω	—	Orbit longitude of the ascending node
$\dot{\Omega}$	—	Precession rate of the ascending node

1 Introduction

1.1. Background

Technologies based on quantum mechanics are blooming nowadays and quantum computing in particular has become a reality. Instead of having bits that can only be a one or a zero at a time, quantum computers are not limited to two states - quantum bit, or qubits, exist also in a superposition of those two states. This ability to perform several calculations at once gives future quantum computers the potential to overcome current supercomputers processing power by several orders of magnitude. While quantum computing holds great promise for most science and technology fields, it will also render useless the most widely used form of cryptography: asymmetric or public key encryption. The asymmetry in these cryptosystems - such as the RSA - relies on the mathematical complexity of reversing the so-called one-way functions; a task which can be trivially solved by a sufficiently large quantum computer. On the other hand, symmetric key cryptography is considered quantum-safe, but has the intrinsic problem of safely distributing the same key to both parties. Quantum Key Distribution (QKD) allows to distribute a symmetric key to two distant parties in a secure manner, being able to detect the presence of a possible eavesdropper [2].

In practice, QKD is performed via an optical link between Alice and Bob - names typically given in cryptography literature to sender and receiver respectively. This means that to connect two points there are two possibilities: a physical link (fibre-based) or a free-space link. In both cases, distance is severely limited by the losses [42]. Satellite-based QKD is the solution to this problem. Using a satellite to connect two points on Earth greatly reduces the free-space losses as most of the path of the optical link takes place outside the atmosphere. Furthermore, if the satellite is considered a trusted-node, keys can be delivered to any two ground stations on Earth, regardless of their location since a simultaneous optical link between the satellite and the two ground nodes is not needed.

As of today this technology is still at a demonstration level (Section 2.4) but the results are promising. It is only a matter of time for a satellite constellation to be designed and launched to provide QKD services at a global scale. In the race to do so, several research institutes are joining forces in order to bring this ambitious goal closer to reality.

1.2. Research scope

The initial project goal for this thesis was to conceive an optimal satellite constellation to provide QKD to a set of ground stations located in the Indo-ASEAN region. This project is located in the frame of a collaboration between CQT and the Indraprastha Institute of Information Technology in Delhi. Scarcity of related literature about QKD constellations has unveiled a research opportunity. The initial steps taken to approach the project goal have shown the need to develop a model that can simulate constellations of satellites performing QKD, as well as a body of knowledge stating guidelines to design a constellation with the functionality of doing QKD. The current technology readiness level (TRL) and the protocols being used will impose certain peculiarities that will need to be taken into account. This thesis aims to identify the key issues in designing a QKD constellation and assess the feasibility of these constellations together with an accurate estimation of their

performance. Furthermore, the use cases and implementation of intersatellite links in such a constellation will be researched: how can it be implemented for QKD purposes? Will it be useful?

Given the multidisciplinary character of this work and the different parties involved in a QKD network, the general research question can and should be subdivided in smaller research questions that can be classified as follows.

1.2.1. Ground segment

While not the focus of this research, the ground segment will dictate the design of the constellation as they will be the end users of the service provided by a QKD constellation.

1 What is the best distribution of ground nodes for QKD?

- 1.1 What are the main cities/points of interest for QKD?
- 1.2 How is QKD affected by cloud cover?
- 1.3 What does a ground station need to have to qualify to be a QKD receiving node?
- 1.4 What is the maximum distance that can be covered with fibre-based QKD?
- 1.5 Do ground stations have a geographical location restriction? (i.e. latitude)

1.2.2. QKD

Even though the physics of QKD are not the research focus for this thesis, a general understanding of its working principles and more importantly, a definition of its requirements have to be described. This results in a combination of fundamental physics and cryptography theory that makes this satellite constellation problem unique and adds a layer of complexity to it.

2. How does QKD constrain the constellation design?

- 2.1 What are the advantages when compared to traditional cryptography methods?
- 2.2 What disadvantages or added complexity does QKD entail?
  - 2.2.1 What are the source/receiver requirements?
  - 2.2.2 What are the distance limitations?
  - 2.2.3 Which key rates can be obtained?
  - 2.2.4 How can higher key rates be obtained?

1.2.3. Satellite constellations

This is the innovation in the QKD field. Up until now all research has focused on proving the feasibility of performing QKD in space, testing the different ways to do so (uplink, downlink, satellite working as a reflector...). A study on satellite constellations for QKD has not been published yet.

3. What will be the main characteristics of the constellation?

- 3.1 Should the constellation be homogeneous or heterogeneous?
  - 3.1.1 What are the advantages/disadvantages of having an on-board source vs a ground-based source?
  - 3.1.2 Is it useful to have satellites acting just as relay modules?
- 3.2 Which altitude (LEO/MEO/GEO) is best suited for QKD?
  - 3.2.1 What is the latency and key rate dependence on this?
  - 3.2.2 How many satellites would be needed in each case?
  - 3.2.3 Is it beneficial to have a hybrid constellation for QKD?
- 3.3 How are the satellites characterized?
  - 3.3.1 What are the satellites size, weight and power? (SWaP)
  - 3.3.2 What ballistic coefficient do the satellites have?
  - 3.3.3 Do the satellites require on-board propulsion?

3.3.4 How does the QKD payload affect the satellite?

3.3.4.1 What are the necessary Attitude and Determination Control System (ADCS) capabilities?

3.3.4.2 What is the routing scheme to perform ISL QKD?

3.3.4.3 Which model will be used to simulate QKD?

3.4 Will QKD be performed only at nighttime?

1.2.4. Optimization

The design of the constellation will be optimized. The following subquestions aim to discretize the research to be done.

4. What optimization techniques are the most appropriate for this problem?

4.1 What are the variables in this problem?

4.2 What is to be optimized? Can a cost function be defined?

4.3 How have constellations been optimized in previous literature?

4.4 Is computational cost a constraint for this problem?

2

Quantum Key Distribution

Quantum Key Distribution (QKD) is a cryptography method to establish symmetric encryption keys between two parties so that they can communicate securely. The meaning of "symmetric encryption key" will be explained in Section 2.1 and its functioning principles will be described in Section 2.2.

2.1. Cryptography

Cryptography can be defined as a tool used to encode a message in a way that it remains unintelligible for a possible eavesdropper. In a contemporary context, it is of equal or greater importance to be able to authenticate the message - i.e. verify that it has not been modified by an unauthorized transmitter - [40]. Its use has been traced back to the Egyptians around 4000 years ago [28] and since then it has only increased in complexity, playing a key role in political matters throughout history. The importance of cryptography has increased in the last decades with the invention of distant communications, especially the Internet. In parallel, the invention of computers and the continuous increase in processing power makes it possible to break this encryption. New protocols are continuously developed to patch vulnerabilities in existing cryptographic protocols. However, a method that is intrinsically secure is needed. This is where QKD comes into play.

In cryptography jargon, the sender of the message is called Alice and the receiver is called Bob. The eavesdropper that intercepts the message and tries to crack it is called Eve. From a conceptual point of view, the way Alice and Bob can encrypt their messages can be divided in symmetric or asymmetric key encryption. Symmetric key encryption means that both of them have the same key, as depicted in Figure 2.1. While simple and secure, it has the problem of securely getting the same key to Alice and Bob, which is a severe limitation when it comes to contemporary distant communications. Also, secure storage of the key has to be guaranteed. Access to the key by Eve will immediately break the encryption. However if the key was somehow securely shared, one could use One-Time Pad (OTP) encryption. OTP encrypts the message with a key as long as the message itself; if the key is randomly generated and kept secret, OTP is unbreakable. OTP requires to have a key as large as the message being sent. This is the ideal scenario, but in reality it is possible to use the secure key as a "seed" and expand it with complex algorithms, keeping security at a very high level and obtaining a much larger key. The NIST´s Advanced Encryption Standard (AES) is the one used nowadays with this purpose and it uses 128, 192 or 256-bit seed keys. This was used effectively in the QUESS mission, expanding a 128-bit seed key with a one-second refresh rate to encrypt a ~2 GB video conference that lasted 75 min [24].

To avoid the previously mentioned symmetric key encryption shortcomings, public key encryption can be used instead. It is an asymmetric encryption method, meaning Alice and Bob will have different keys. The most common algorithm to create these keys is called RSA (Rivest, Shamir and Adleman) creating a pair of keys for Alice and another pair for Bob. Each pair consists of a private key and a public key and they are mathematically linked to each other. This link relies on the so called one-way functions, more specifically, the product of large prime numbers. Alice can now encrypt the message with Bob´s public key, which can be shared openly. Thanks to the RSA algorithm, the message will only be decrypted using the private key, which Bob has to store securely. This can be seen in Figure 2.2.

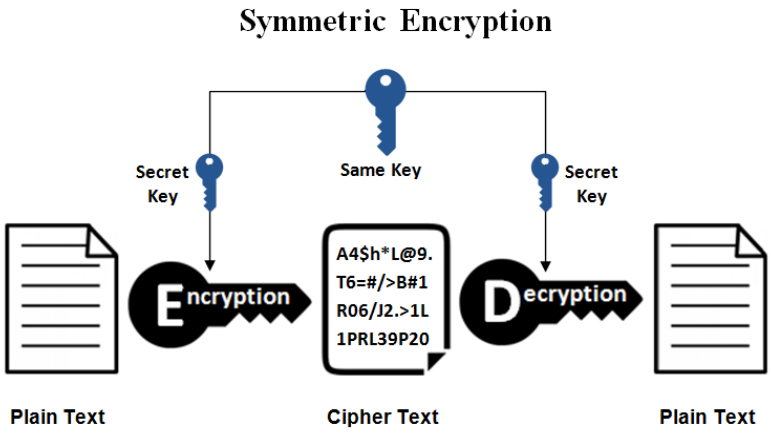


Figure 2.1: Schematic describing symmetric key encryption. Retrieved from [25]

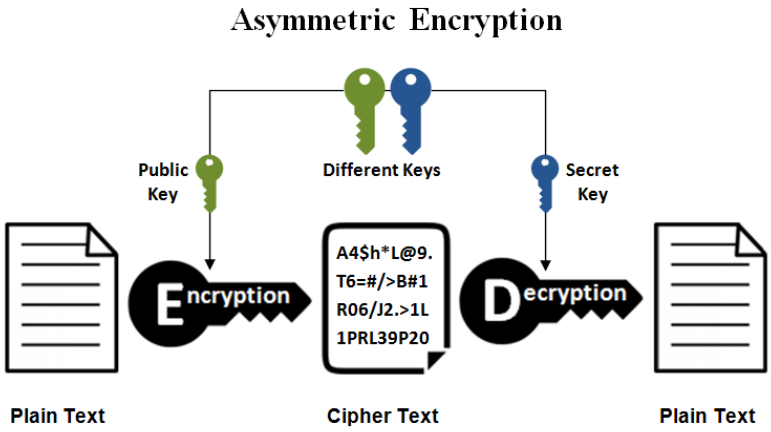


Figure 2.2: Schematic describing public key encryption. Retrieved from [25]

This method relies on the lack of processing power available to factorize a very large number in its prime factors in a short amount of time. However this could be changed in the future, especially with the appearance of quantum computers. While post-quantum computing algorithms are being developed to overcome this problem [4] - which could be useful for low-security applications - QKD provides a solid solution that guarantees a secure exchange of keys, allowing OTP encryption, and moreover, it is able to detect the presence of an eavesdropper.

2.2. QKD protocols

One can find two types of QKD protocols: DV-QKD (Discrete Variable) or CV-QKD (Continuous Variable). The difference betweent them is analogous to the particle-wave duality of light. DV-QKD works with the particle nature of light, encoding information in single photons while CV-QKD uses the wave nature of light to embed information onto the amplitude and the phase quadratures of the source light [20]. Despite CV-QKD having a promising future, at the moment only DV-QKD will be considered as its implementation in satellites is the norm [3]. When discussing DV-QKD two different sub-protocols are distinguished: prepare-and-measure, and entanglement-based. The entanglement-based one can allow the entangled photon source to be a non-trusted node in a double-downlink configuration, which entails more security. If the node is trusted, it will store all keys, making it vulnerable to a potential attack. This is, however, very unlikely to happen in the space scenario where the source can be on board of a satellite. Moreover, distributing pairs of entangled photons to different ground stations requires higher pointing capabilities and to overcome double the attenuation which

translates into a higher cost.

2.2.1. Prepare-and-measure protocols

The most used prepare-and-measure protocol is the Bennett-Brassard 1984 (BB84). Figure 2.3 describes a key generation process between Alice and Bob. Alice polarizes a source of light choosing randomly between the two bases shown. Bob will measure the incoming photons using randomly selected bases and registering their associated bit values - either 0 or 1. After all the photons have been sent, the choice of the bases is announced via a public channel. This is known as basis reconciliation. As shown in Figure 2.3, the bits registered by Alice and Bob when measuring the photons using the same base are the same, hence obtaining a private key between them. This is not the final secure key, as they still need to verify if the error rate is low enough on random subsets of the data. If the error rate stays under a certain threshold - set at 11% for this protocol [32] -, the secure key is finally obtained after the processes of error correction and privacy amplification. In an ideal process with no external perturbations, any errors would be caused by Eve. In the case of a man in the middle attack, Eve replaces the photons that she siphons off so Bob still receives them. However, since Eve does not know which base Alice is using for each one of the photons being sent, she has to randomly select the base she sends the replicated photon to Bob with. This will inevitably lead to errors once Alice and Bob compare their keys since statistically Eve will only get the base right 50% of the time. In reality, WCP sources are limited by multi-photon emissions and so decoy-states need to be introduced to trick the eavesdropper. This is discussed in Section 2.3.1.

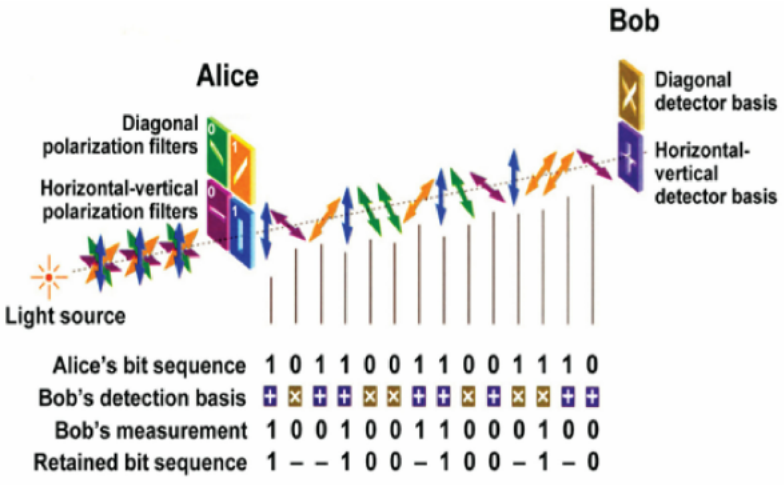


Figure 2.3: Schematic describing the BB84 protocol. Retrieved from [1]

2.2.2. Entanglement-based protocols

Two of the most widely used entanglement-based protocols are the BBM92 (Bennett-Brassard-Mermin, 1992) and the E91 (Arthur Ekert, 1991). As described in [18] , in E91 the source generates pairs of entangled photons: one photon of the pair is sent to Alice while the other one is sent to Bob. The generation of the entangled pair provides an intrinsic randomness regarding the base in which the photons are transmitted. Alice and Bob will measure the received photons using the two bases described in 2.3 in a random fashion. Once the process is finished, they will share the information about which basis was used for each photon, retaining the measurements of those photons when they used the same base, and obtaining the sifted key. Similarly to BB84, after an error correction procedure and privacy amplification - introduced in Section 2.2.3 - Alice and Bob will have a secret key.

2.2.3. Error correction and privacy amplification

Error correction and privacy amplification are two processes that are present regardless of the protocol chosen. The goal is to guarantee that the key shared between Alice and Bob has no - or minimal - errors and that it is totally secret, respectively. It has to be kept in mind that mismatches between Alice's and Bob's key can be due to both non-ideal transmission errors or to Eve intercepting information from the quantum channel and

then re-sending it. In addition, it is assumed that the whole process of public reconciliation is listened to by Eve. The error correction will first be done to get rid of errors in the final sifted key, while the privacy amplification will turn the final shared key into a shorter one, depending on estimations of how much information Eve possesses. How these two processes are carried on in the case of satellite QKD will be explained with an example in Section 3.2

2.3. Technology

From a high level perspective, the communication chain is formed by four elements: the sender, the receiver, the message and the channel. Applying this to QKD, it follows that the source sends polarization-encoded photons - characterized by their wavelength - through a certain channel. These elements are now analyzed to better understand the technology available to do QKD.

2.3.1. Source

There are important differences between QKD usin weak coherent pulses (WCP) and using entangled photons. Regarding WCP sources, "the average number of photons in one pulse is set to well below one, to minimize the probability of multiple photons according to poissonian statistics" [14]. It is important to keep the average photon number well below unit since there is a chance of multi-photon emissions, portraying copies of the same state. This will inevitably happen for some pulses, and it provides Eve with an opportunity to intercept one of those photons without altering the information received by Bob - what is known as a beam-splitting attack [27]. To solve this, the so called decoy-state is used. A fraction of the pulses - even up to half of them [24] - are sent with different intensity to make it possible to detect the presence of Eve siphoning off extra photons [26].

With an entangled photon source, a pair of entangled photons is distributed, one photon to each involved party. The generation of entangled photons makes the polarization of each pair truly random. One can have a double-downlink scenario where the photons are directly received by the two ground stations, or a single-downlink scenario where one of the photons is sent to the desired ground station while the other one is detected by the satellite itself. With the latter QKD can be performed using a protocol similar to the BB84. However, detecting photons on board might decrease the overall efficiency since the detectors need stringent cooling to perform adequately. On the other hand, the weak coherent pulse source generates photons with a polarization base chosen by a random number generator, as opposed to the intrinsic random nature of entanglement. However, no detector is then needed on board.

To simulate the QKD link between a satellite and a ground station, a MATLAB model has been developed at CQT, which will be used for this thesis. It follows the guidelines established in [5] where the results shown in Table 2.3.1 are published. In both downlink and uplink scenarios, the secure key obtained is larger when using a WCP source. Therefore, in the following work, a WCP source will be assumed.

	Secure key length obtained for the upper quartile satellite pass (kbit)			
Wavelength (nm)	Downlink, WCP source	Uplink, WCP source	Downlink, entangled photon source	Uplink, entangled photon source
405	68.5	3.5	6.2	0
532	264.5	33.1	119.3	12.1
670	465.6	87.7	324.7	67.4
785	458.3	111.3	272.9	75.7
830	317.3	82.1	136.1	39.7
1060	175.4	67.6	21.8	8.1
1550	123.9	94.8	12.8	14.4

Table 2.1: Comparison of secure keys obtained for downlink and uplink scenarios with a WCP and an entangled photon source. Retrieved from [5]

2.3.2. Wavelength

When designing a QKD-system, the wavelength chosen will determine its transmittance through the atmosphere.

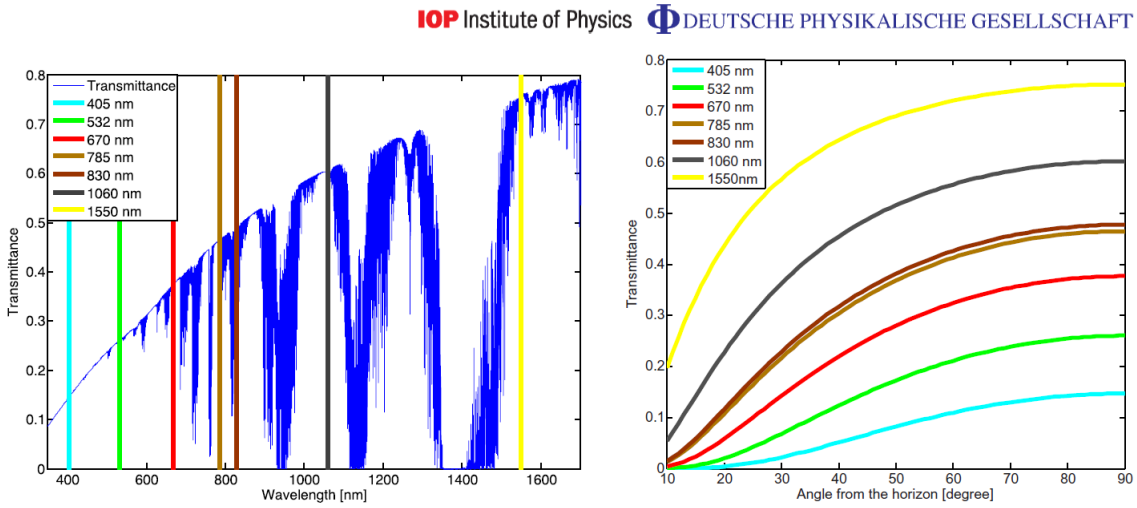


Figure 2.4: Simulated atmospheric transmittance for different commercially available laser system wavelengths. Propagation at zenith (left) and propagation for different elevation angles (right). Retrieved from [5]

An analysis of Figure 2.4 would suggest using the highest wavelength possible (λ = 1550 nm) as to maximize transmittance, as well as minimizing Rayleigh scattering, which is proportional to $1/\lambda^4$ [23]. However other aspects have to be considered, mainly the technology of sources and detectors. As of today, the sources with flight heritage have all used a wavelength in the range of 800 nm. These sources fall under the category of visible wavelengths, using as detectors Si Avalanche PhotoDiode (APD) technology. The other type of source corresponds to the infrared wavelength (such as the previously mentioned λ = 1550 nm). In this case the detectors available are InGaAs APDs, which perform poorly when compared to Si APDs, or superconducting single photon detectors, which need cryogenic cooling [5]. This type of thermal control is very costly hence not being considered for missions where SWaP is a constraint. There are attempts to overcome this barrier where a Si APD is used for a 1550 nm wavelength, converting it into visible wavelength right before the detection event. Using this approach, QKD has been demonstrated on ground over a distance of 53 km in daylight [23]. However, in the latest successful QKD downlink, the same research group sets as a condition to minimize noise that the satellite is in eclipse and the ground station at night time during the QKD link [22]).

2.3.3. Transmission

Two options are available to get the photons from Alice to Bob: using fibre cables or via free-space. Fibre has the inevitable problem of attenuation; with a typical loss of 0.2 dB/km, to register an event with a distance over a 1000 km would take 380 billion years [35]. To overcome this problem quantum repeaters are proposed to enable relaying of quantum states. Unfortunately this technology is still not available, needing elements such as a quantum memory [45]. Free-space provides a significantly reduced attenuation (0.07 dB/km at 2400 m above sea level [38]) but several limitations remain such as atmospheric turbulence and the curvature of the Earth limiting the possible line of sight between two distant parties. Space-based QKD effectively solves this issue, being able to establish links over longer distances thanks to the much lower attenuation in the vacuum of space. Figure 2.5 shows a comparison between the typical losses registered with fibre and the ones obtained in a satellite to ground link. Of course, QKD in space brings up a series of new challenges that have to be overcome. This will be discussed in Section 3.1.

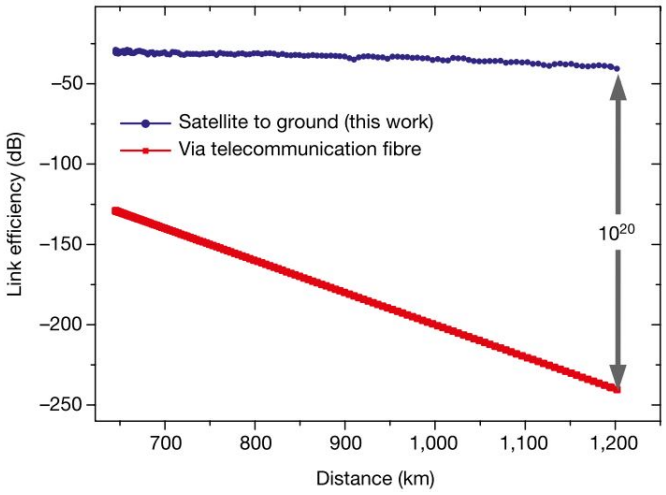


Figure 2.5: Losses comparison of QKD between fibre and the Micius satellite to ground. Retrieved from [21]

2.4. State-of-the-art

Space-based QKD is being developed by a number of entities around the world. Given its great commercial appeal, it is a matter of time before large missions conducted by agencies and private companies take place. However, as of today most of the missions are still at a technology demonstration level, being designed by research institutes. This section will go over the most relevant existing missions, starting by describing the role of CQT in this panorama and then what the other main actors are achieving and proposing for the near future.

2.4.1. Centre for Quantum Technologies at NUS

The Centre for Quantum Technologies (CQT) is a "national Research Centre of Excellence (RCE) in Singapore" [12]. It brings together experts in quantum physics, computer scientists and engineers to research and apply quantum mechanics to technology. One of these pieces of technology is the SPEQS instrument. Having completed its second version, this instrument is a compact and rugged source of entangled photon pairs. It was decided since the beginning to use the CubeSat standard as the bus for the missions, since it allows for cost-efficiency and flexibility. Also, developing a QKD source that can be fit inside a CubeSat can have a great commercial potential in the future.

Already having tested SPEQS-1 CS (correlated photon source) in space on-board the Galassia mission (more on this in Section 2.4.2), CQT is currently finishing the assembly of SPEQS-2. Its objective is to deliver a higher entangled-photon production rate to enable satellite-to-ground QKD. Once this instrument is tested in space, QKD performed by nanosatellites will come closer to reality and therefore constellations made up of nanosatellites are to be strongly considered. Table 2.4.1 sums up the path that CQT has followed during these years in the development of these instruments.

Figure 2.6 shows a CAD model and a diagram of the optics that an entangled photon source such as SPEQS is comprised of. The figure represents one of the earliest versions of the instrument (SPEQS-1 ES) but the functioning principle remains valid for the most recent ones, and for other entangled-photon sources. As a coarse description, the process is made of four steps [2]:

1. The source produces a high number of photons that pass through a filter and are diagonally polarised. This source will typically be a laser diode with a wavelength of around 400 nm.

2. The photons pass through two BBO crystals - horizontally and vertically polarised respectively - and this results in one original photon being converted in two polarisation-matched lower energy photons (wavelength of 760 nm and 860 nm in this case). This process is known as spontaneous parametric down conversion (SPDC) and has a very low efficiency, around 4 pairs per million pumped photons.

3. A dichroic mirror filters out photons that have not been converted, using them to feedback the system and control the source intensity consequently.

Timeframe	Goals and activities	Source	Missions
2012-2015	Miniaturisation and engineering developments.	SPEQS-1 CS	
2015-2016	Producing entangled photon sources and demonstrating them in space.	SPEQS-1 ES	High altitude balloons and 3rd party CubeSats
2015-2017	Satellite mission capability building and SPEQS performance developments.	SPEQS-2 v1	CQT SpooQy-1 CubeSat CQT
2017-2019	Space test of QKD-ready source.	SPEQS-2 v2	CQT SpooQy-2 CubeSat
Ongoing	Space to ground QKD demonstrations.	SPEQS-3	International collaborations

Table 2.2: Sources developed by CQT and their related missions. Retrieved from [2]

4. Another set of crystals makes sure that the pair of photons cannot be traced back to one of the two BBO crystals, hence not knowing their polarisation. This step achieves entanglement.

The rest of the optics depicted take the entangled photon pair and separate it to analyze the photons on board of the satellite. In a prepare-and-measure scenario using an entanglement source, one photon would be stored while the other one would be sent to ground.

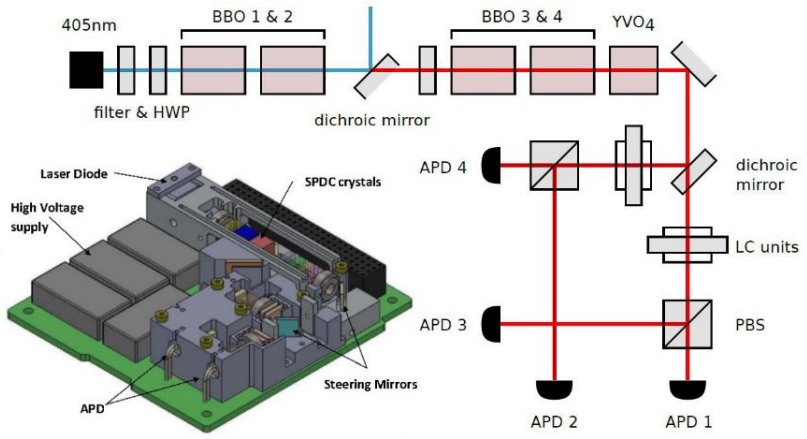


Figure 2.6: SPEQS-1 ES CAD model and optical layout diagram. Retrieved from [2]

As commented before, QKD has an important commercial appeal. It is not surprising that spin-offs are arising from the main QKD research institutes around the globe. An example is S15 Space Systems, whose service consists of selling secure keys based on QKD using the know-how developed at CQT. This combined expertise will be used in the development of the thesis, as most of the work will be done at CQT.

2.4.2. Other institutes

The need for QKD in space has been acknowledged by research institutes all over the world. First attempts have been conducted successfully, and have attracted the attention of private companies and governments. Once the technology has been shown to work, they will be ready to invest in larger missions.

Figure 2.7 shows the main current and future QKD space missions. It shows how almost every scenario shown in Figure 3.1 has already been demonstrated. It is no coincidence that the last scenario, corresponding to an ISL, is not present: it entails the most complexity. This is one of the reasons why this thesis will evaluate it for its potential use in a QKD network. The added value of enabling the satellites to distribute secret key with each other is not clear, thus ISL is an interesting research topic to explore in the case of QKD.

From the launched missions, the satellite Micius has achieved the most ambitious goal: it established a link between two distant ground stations sending pairs of entangled photons. It has also achieved a prepare-

and-measure link from LEO to ground and a teleportation experiment [3]. This mission can be considered the stepping stone for large-satellite QKD missions and one can expect a development of QKD missions alike by the main space agencies of the world. An example is the QUARTZ mission, a joint effort between ESA and SES Techcom S.A. [11]. In 2017 the same Chinese group would accomplish a successful QKD downlink using the Tiangong-2 Space Lab. It was achieved using a smaller 57.9 kg payload (integrating the QKD source along with the tracking system and the laser communication transmitter) [22].

Focusing on satellite-based missions, research institutes generally prefer using CubeSats to perform their experiments. This platform significantly reduces the costs, enabling this low-budget entities to carry out tests that bring affordable QKD in space closer to reality. The current goal of the missions being flown and being designed and proposed is to raise the TRL of the instruments and the link. From a cost point of view, it is clear how a constellation made of small satellites could be advantageous.

Most missions based on CubeSats place only the receiver on the satellite. Nanobob [18] and NanoQEY [17] intend to prove a QKD uplink. While these missions will help develop the technology, a source in space translates in better keyrates (the losses are approx. 10 dB higher in an uplink scenario) mainly due to the *shower-curtain* effect. This effect describes how the repercussion of the atmospheric losses is higher if they happen at the transmission end (uplink) instead of at the receiver end (downlink) [33]. The SpooQySats developed by the CQT embark the instrument SPEQS, which is a source of entangled photons. While only the first mission has flown, successfully demonstrating the functioning of a single-photon source, the next one is planned to launch in 2019 and it intends to prove the technology of an entangled-pair source of photons on board of a nanosatellite. As shown in Figure 2.7, no uplink or downlink will take place since the goal of the mission is just to test the correct functioning of the payload in space. In the same direction the proposed QUBE mission by the German QUTEGA funding scheme plans to embark a quantum payload with a number of sources on a Cubesat. However little information is available, placing CQT as the current leading institute developing small QKD sources.

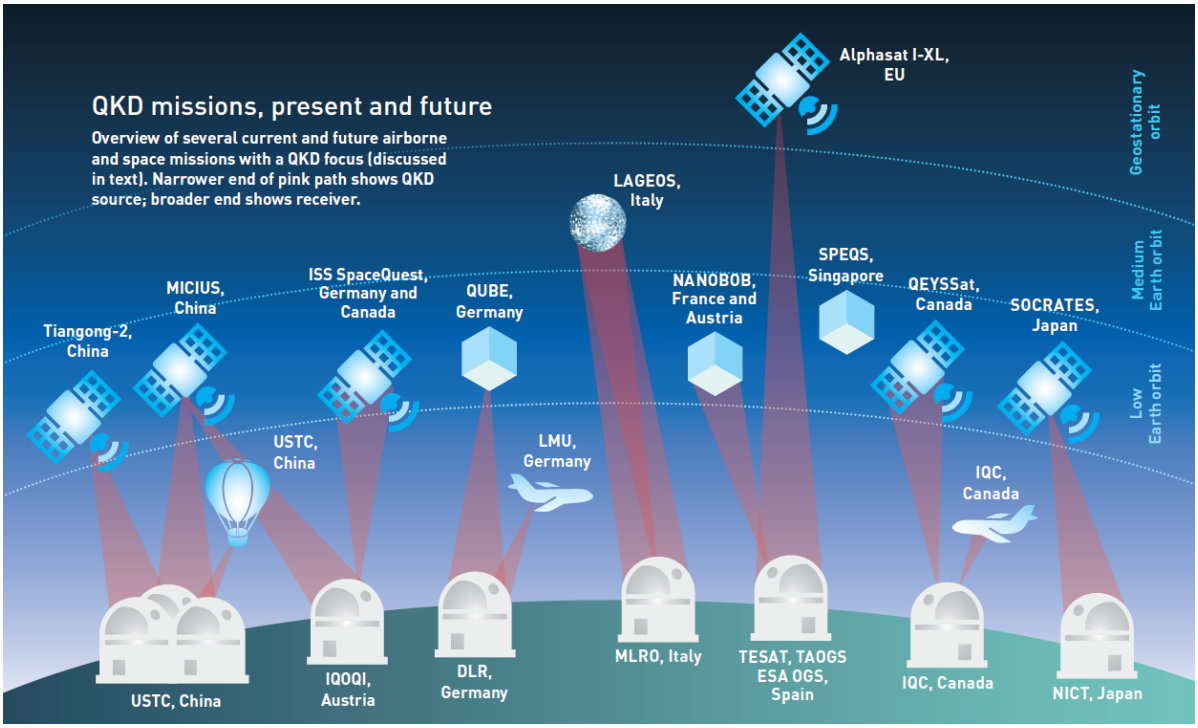


Figure 2.7: QKD space missions as of February 2018. Retrieved from [19]

Other missions have tested a source on board of satellites that could potentially enable QKD. The SOCRATES satellite was conceived with the goal of doing this QKD technology demonstration. The small Japanese satellite (48 kg) has proved successful transmission of non-orthogonal polarization states [41]. Another example is the Alphasat I-XL, a large GEO satellite embarking a laser communication terminal that was used to test quantum-limited coherent measurements of optical signals.

3

Assumptions and user requirements

3.1. QKD from space

Prior to the discussion about potential constellations, the operations of a single satellite doing QKD must be ascertained.

The goal of a QKD satellite will be to deliver key to a pair of ground stations - GS_A and GS_B - so they can communicate privately in a secure way. Delivering this key from space can be done following different concepts of operations, summed up in Figure 3.1

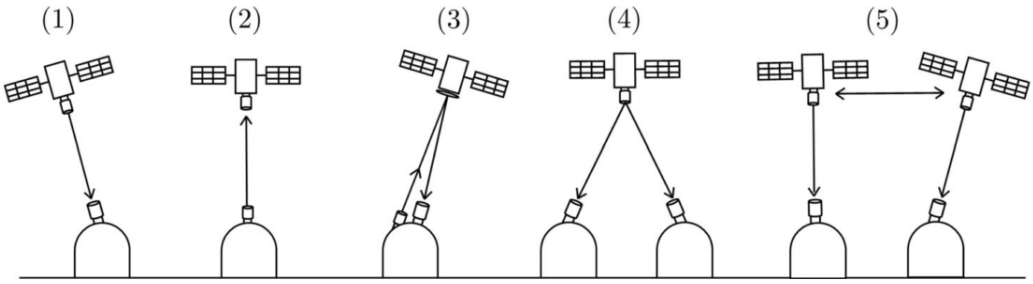


Figure 3.1: Possible scenarios for QKD in space. Retrieved from [3]

From scenarios 1 to 3, the most effective one is number 1. Downlink (1) will beat uplink (2) and reflection (3) in terms of keyrate since the atmospheric losses happening at the transmitter side of the link propagate along its length - the previously introduced *shower-curtain* effect. Furthermore, placing the source on the satellite will potentially allow scenario (5) to become a reality. Scenario (4) depicts an entanglement-distribution. The entangled photon pair gets split and each ground station receives a photon of said pair. The main advantage associated with this protocol is that the satellite does not store the key at any point in time, hence it does not need to be considered a trusted node. However, the complexity of the system is increased, the losses of the link are doubled and line of sight with both ground stations is required. A prepare-and-measure protocol does not have these disadvantages and can be performed with a less complex and therefore cheaper satellite. In this thesis a prepare-and-measure protocol is assumed and the satellites are considered trusted nodes. The logistics of the protocol will drive the design of the constellations, and ultimately, the functionality increase due to the possible inclusion of ISL. The process is depicted in Figure **??**. In step (a) the satellite flies over GS_A, exchanging a key with it. This process needs both an optical link and classical communication. Step (b) is identical, but with GS_B. Now the satellite possesses both K_A and K_B - which in virtually every case, will not be the same size due to different pass conditions. The final step will be to share $K_A \oplus K_B$ with either one of the two ground stations. Using its own key, GS_A will be able to obtain K_B and viceversa. Specifics of the logistics will be discussed in Section 3.2.3. This final step can be improved by introducing a relay, using for example an existing GEO constellation. This approach has been taken by several optical communication networks, enabling to greatly reduce the latency. Therefore, to simplify the study of

QKD constellations in this work, a GEO relay will be assumed. Whenever it is needed, the satellite will communicate $K_A \oplus K_B$ to the available GEO satellite via classical communication, which will then downlink it to the desired ground stations.

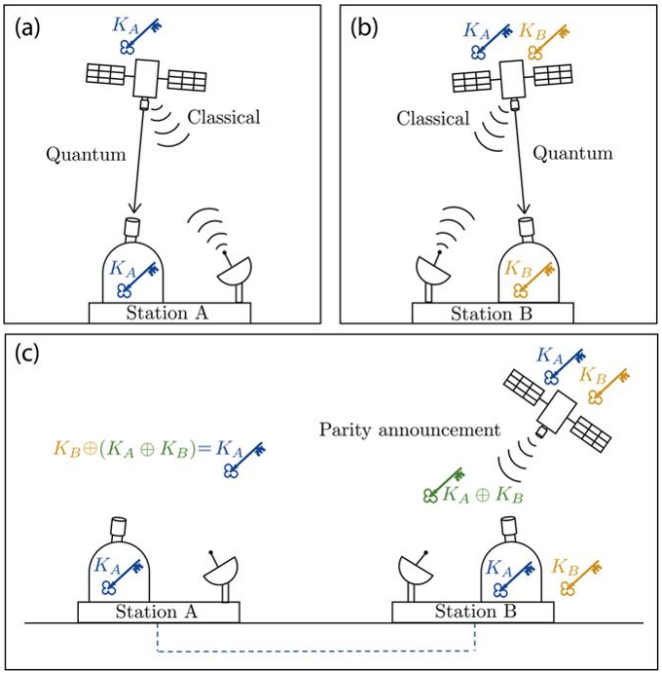


Figure 3.2: Prepare-and-measure QKD steps. Retrieved from [3]

3.2. QKD concept of operations

A successful key exchange with QKD between a satellite and a ground station entails a degree of complexity that requires a thorough definition of the operations to be handled. An example is therefore provided to have a better insight on how this would look in a real downlink prepare-and-measure scenario. This concept of operations is based on the Micius satellite and it corresponds to a planned future mission by CQT.

3.2.1. Tracking and preparation

QKD will be considered if the satellite pass has a minimum inclination larger than the one required by the ground station and the sky conditions are good enough. The latter is not completely defined since, contrary to standard optical communications where data packages are being transmitted, in QKD it is just a matter of getting key exchanged. Therefore passes with low visibility could still be useful even if only a small amount of key can be obtained, but where to set the threshold is left to a detailed trade-off performed by the involved ground stations.

The satellites will initiate the ground station central pointing several minutes ahead of the actual pass in order to achieve a certain pointing accuracy value in the first instants of the pass. Meanwhile, the payload gets ready to be used: the satellite will check the temperature and it will provide power to the instrument, which then will begin doing the relevant preparations for the QKD link (turning on the laser to the desired current, performing a self-test, etc.)

The ground station will point its beacon laser at 10 degrees above the horizon until the satellite passes. Once it does, the beacon will follow it according to the predicted pass curve. This allows the satellite to fine point to follow the beacon and it will reply pointing its beacon towards the ground station. After this step, the ground station is able to precisely track the satellite, achieving bi-directional tracking and locking.

3.2.2. QKD

At around 15 degrees of elevation angle, the QKD link begins. SPEQS is an entangled photon source, therefore for a prepare-and-measure scenario it will detect one photon of each pair, time-tagging the event while the other photon is sent down to the ground station. Intrinsic to this protocol is the basis reconciliation step where both parties share the base choice for each measurement. Firstly, the ground station shares this information over a classical communication channel. SPEQS will then generate the so called *sifted key*. It is equal to approximately half of the detected key, since it is comprised of those events where both satellite and ground stations chose to measure using the same basis.

The remaining procedures are required to ensure a totally secure and private key. Once the satellite determines which events are part of the sifted key, it will transmit this information to the ground station along with a portion of the key to be used for error correction purposes. Thanks to this reference key the ground station will be able to compute the Quantum Bit Error Rate (QBER) and initiate the error correction process - in this case, following the Cascade protocol [6]. After error correction the shorter resulting key is then subjected to a privacy amplification process at the ground station. This is done to eliminate information that a potential eavesdropper could have obtained. The resulting shorter key is the final secret key.

3.2.3. User scenarios

These scenarios represent two situations in which a key delivered by QKD would be needed. Once the ground nodes have a common secret key, they will choose how to use it accordingly to their purpose, let it be with a OTP or using some additional symmetric encryption algorithm such as the AES to obtain additional keysize. In the following work, when talking about encrypted messages it will be assumed that OTP is being used and hence the message will be the same size as the key encrypting it.

The first scenario represents one-to-one communication. Ground station A (GS_A) wants to communicate with ground station B (GS_B). The limitation on key size will be imposed by the fact that each satellite must downlink $K_A \oplus K_B$, and to perform this logical operation, K_A and K_B must be the same size. If Sat_1 has more K_A than K_B, only a piece of K_A as large as K_B will be used for this specific communication process. Therefore, the total key available for both ground stations will be $K_{A_{reduced}}$+K_B, or effectively, 2*K_B. This process is then repeated for every satellite of the constellation.

The second scenario consists in one ground station broadcasting a message to all the other ground stations. This is a scenario that could happen in the case of a country sending a message to its embassies around the world. Let's discuss the simplest case, with three ground stations: GS_A sends a message to GS_B and GS_C. Maximum security is again assumed, meaning that the piece of K_A used to encrypt the message sent to GS_B will be different from the piece of K_A used for GS_C. For each satellite, the amount of K_A will be evenly distributed amongst the other ground stations. In this example, this means distributing K_A in two halves. If both K_B and K_C aboard this satellite are larger than half of K_A, then the key available for GS_A to communicate with GS_B will be twice $(K_A/2) = K_A$ (similarly to what it was done in the previous case). It will be the same for GS_C. This case is depicted in Figure 3.3. However, if for example K_B is smaller than $K_A/2$, then the key size will be determined by K_B. This means that the key exchanged between GS_A and GS_B thanks to this satellite will be equal to $2 * K_B$, and therefore this will also be the case for GS_A and GS_C (even if more key could potentially be interchanged between these two other ground stations, the interest resides in finding the most restrictive couple of ground stations for each satellite, as this will determine the maximum size of the distributed message). This case is the one shown in Figure 3.4. This process is repeated for every satellite, yielding the largest message that GS_A can broadcast to the other ground stations using OTP.

3.3. Ground stations

The focus in this thesis relies on the study of the space segment of a QKD global network. However, the ground nodes of said network play a fundamental role in determining the requirements of the system. Therefore, two sets of ground stations have been devised, following a set of guidelines.

3.3.1. G20 network

A generic geographical distribution could be achieved by setting a grid of simulated ground nodes across the world. However this fails to replicate the real-life climate conditions that heavily affect the performance of

Figure 3.3: Diagram of the distributed message scenario. In this case, no ground station limits the final size of the message.

Figure 3.4: Diagram of the distributed message scenario. In this case, GS_D limits the final size of the message.

QKD in certain locations. Additionally, the potential users of QKD - at least in its first years - are expected to be major institutions highly concerned with security and privacy, e.g. governments or international banking institutions. To capture both this geographical diversity and this potential user database, a distribution of ground nodes based on the G20 is proposed. The countries belonging to this group represent the 85% of the global economy, and locating the ground nodes on their respective capital cities will result in a ground network adequately spread around the world. For simplicity Europe will be considered as a whole, setting its capital in Brussels.

Table 3.3.1 shows the countries and capital cities conforming this set of ground stations.

3.3.2. Indo-ASEAN network

An ongoing project for CQT is the establishment of a QKD network to deliver key to cities distributed in India and the ASEAN region. There is therefore an interest in studying this region as it represents a realistic case of a user. In addition, this distribution of ground nodes brings to light challenges that would not be encountered when treating with a scattered distribution such as the one present in the G20 case. The cities belonging to the Indo-ASEAN group are clustered together, having two interesting cases of ground stations pairs that interfere with each other (Bangalore with Chennai and Singapore with Kuala Lumpur, as seen in Figure 3.6). On top of that, most of these cities are located around the equator, with the maximum latitude belonging to Delhi, at approximately 29 degrees north. This will impact the design of a constellation specifically designed to suit these ground station network in an optimal way. The countries and cities chosen for this network are presented in Table 3.3.2.

G20 countries and capital cities			
Country	**Capital city**	**Country**	**Capital city**
Argentina	Buenos Aires	Japan	Tokyo
Australia	Canberra	Mexico	Mexico City
Brazil	Brasilia	Russia	Moscow
Canada	Ottawa	Saudi Arabia	Riyadh
China	Beijing	South Africa	Pretoria
European Nations	Brussels	South Korea	Seoul
India	New Delhi	Turkey	Ankara
Indonesia	Jakarta	United States	Washington, D.C.

Table 3.1: Countries and their capital cities that belong to the ground station set referred to as G20

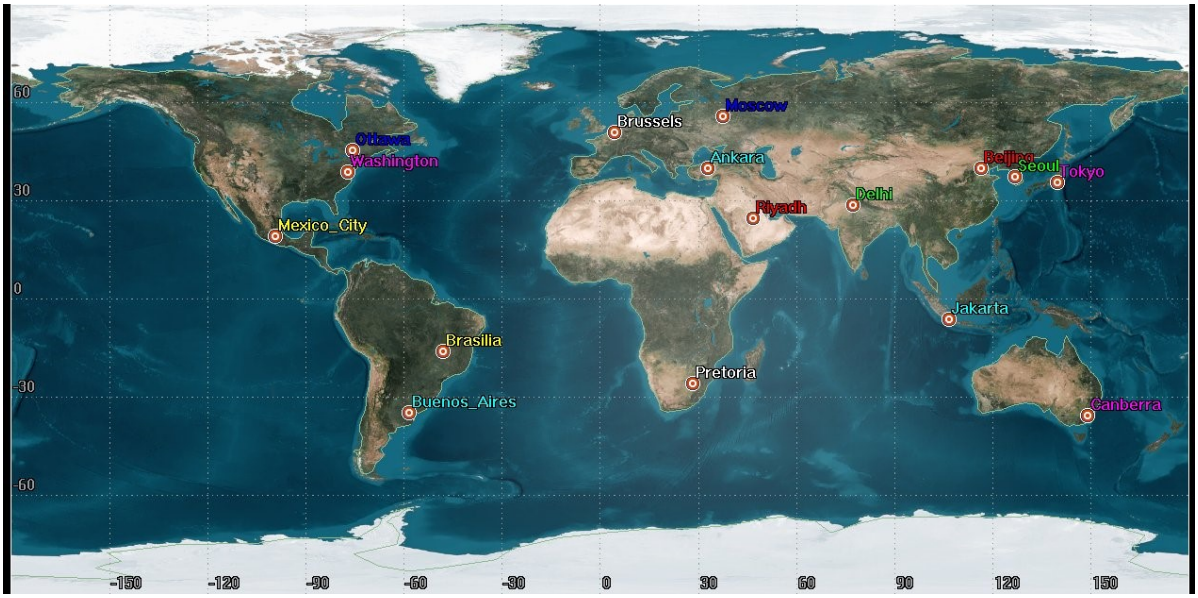


Figure 3.5: Geographic distribution of the capital cities being part of the G20 ground station network

3.4. User requirements and system evaluation

Before diving into the specifics of a QKD constellation design, one must take a step back and reflect on what the user requires from said system as well as how its performance is going to be evaluated. Nowadays, potential QKD users are entities for whom security and privacy in their communications are critical. At any point in the design, the key handling will be treated having this aspect in mind. This means that, for example, in a potential ISL scenario, satellites will not exchange non-encrypted key between them. It can be argued that this link is virtually secure, due to the operational complexity of hijacking it. However, in this thesis whenever key is exchanged, it will be done not only in a practical secure way but also in a theoretical secure way. In the previous example, this means that the key passed from one satellite to another will be encrypted using key previously generated between the two satellites.

With this aspect taken into account, the user then will wish to have as much key available as possible. The main driver to do QKD in space is to deliver key between two very distant points, but also to achieve higher key rates. Therefore, a constellation will be better if it delivers larger keys over a certain period of time.

Analogously to a communication constellation, the next factor one could think of is latency. While this could play a role if the satellite(s) would perform step (c) of Figure 3.2, as stated previously it is assumed that a GEO relay is used for the downlink of the key parity. Therefore latency will not be taken into account. However the temporal dimension is not completely disregarded for the study of a QKD constellation. The QKD application brings a specific parameter to the table: key renewal rate. This concept arises from the fact that a key being stored is considered less secure as time passes, due to the ever-increasing chances of being compromised. Therefore, the closest the key parity is downlinked with respect to the moment of generation

Indo-ASEAN countries and capital cities			
Country	**City**	**Country**	**City**
India	Bangalore	Indonesia	Jakarta
India	Calcutta	Malaysia	Kuala Lumpur
India	Chennai	Singapore	Singapore
India	Mumbai	Thailand	Bangkok
India	New Delhi	The Philippines	Manila
		Vietnam	Ho Chi Minh

Table 3.2: Countries and their respective cities that belong to the ground station set referred to as Indo-ASEAN

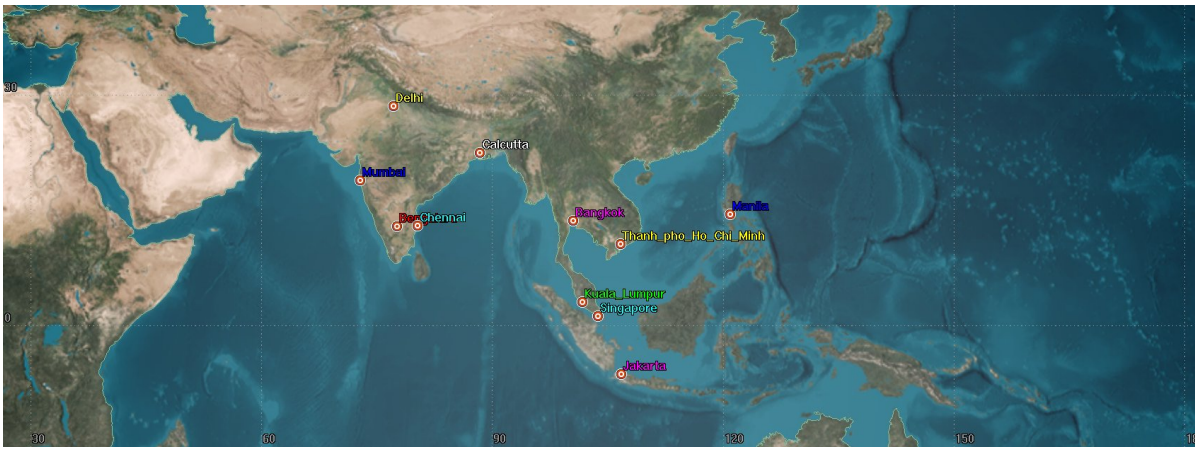


Figure 3.6: Geographic distribution of the capital cities being part of the G20 ground station network

of the two keys it is comprised of, the better. From the point of view of a satellite constellation design, this is translated into an effort to minimize the time periods between subsequent revisits for the ground nodes.

As one can imagine, a myriad of use cases can be thought of. Different ground stations, different specific requirements (e.g. discarding all exchanged keys that have not been used before 24 hours), etc. However, as a translation of user requirements into system requirements, these two guidelines will always be present:

1. The key size is to be maximized.

2. The time period between subsequent revisits is to be minimized.

These time periods between subsequent revisits or "access gaps" will be directly evaluated in a per-GS basis. To compare between different constellation configurations, the mean value amongst all the GSs can be computed, and the GS with the maximum gap will be of the most interest. Regarding the keysize, directly computing the value of the keysize exchanged between each satellite and GS will not give an accurate impression of the constellation performance for QKD purposes - at least using a protocol like the BB84 with the logistics that this implies. Directly computing the mean value of the keysizes exchanged for the satellite-GSs pairs could be misleading as a constellation where GS_A has 10Mb available and GS_B has only 2Mb available will be considered worse performing than one in which both GSs have 6Mb available each, even though the average value is the same. To fully express the distributed nature of the QKD constellations, in which the final goal is to let the ground stations communicate securely between them, the second scenario described in 3.2.3 will be used. This is the scenario named as "distributed message" in which the hypothetical case of one ground station sending a message to all the other ground stations is considered - never using the same key. Doing this exercise for every ground station will yield a graph that indicates much more accurately the performance of the constellation regarding the keysize exchanged. For a numeric value, it will now be appropriate to compute the mean value among the different ground stations, though one must be careful and avoid situations in which certain ground stations are clearly under-performing.

4

The model

4.1. Model structure

The flowchart of the code is depicted in Figure 4.1. The models have been developed using MATLAB. Additionally, STK has been used to initially determine the accesses between objects.

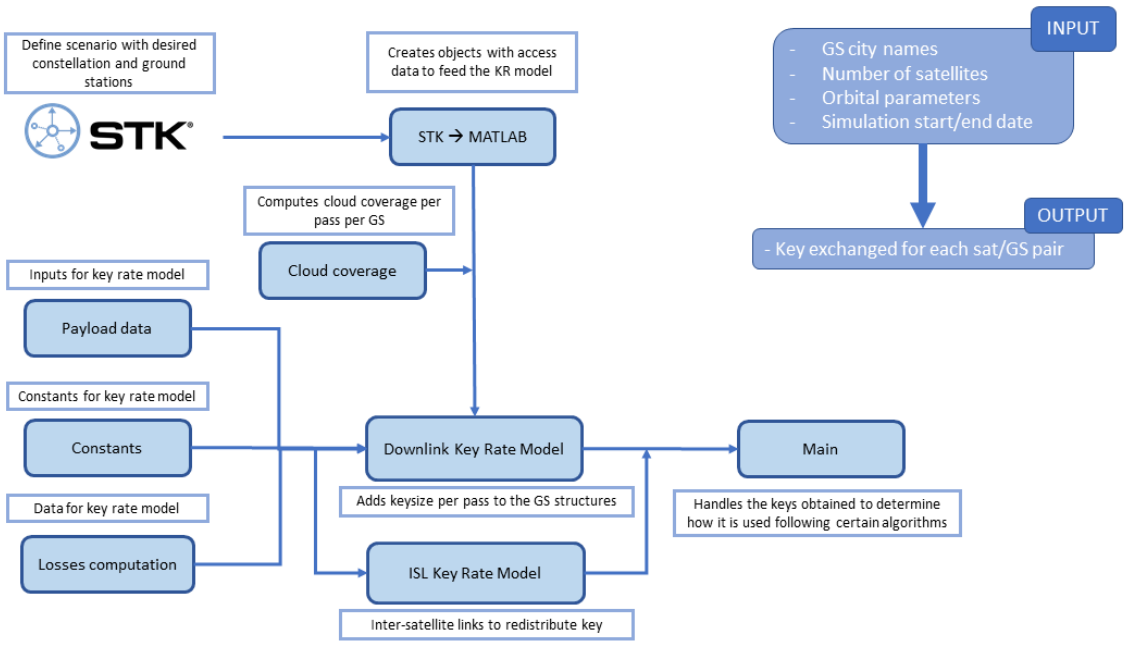


Figure 4.1: Flowchart of the QKD model

4.1.1. STK

The first step is to create the desired scenario in STK and to populate it. The required inputs are the start and end date of the simulation, the number of satellites on the constellation and their orbital parameters together with the location of the ground stations. Furthermore, the access constraints of satellites and ground stations can be characterized via customizing the relevant sensors. The sensor object is attached to each satellite or ground station, and it is responsible for characterizing the communication between them. For example, for the ground station sensors it is indicated that communication will only take place at night time and when the elevation angle of the satellite being observed is greater than a certain value. With the constellation and the

ground stations characterized, STK computes all the accesses between the objects (satellite-GS and satellite-satellite if ISLs are studied) and then outputs the data for each access with a chosen time step. The raw data gathers the instant of time being studied, the pass number, the distance between the two objects and the elevation angle of the satellite observed from the GS in the downlink case. This is easily exportable to MATLAB via a .csv report.

STK elements

To simulate the key-buffering, three basic elements are created in STK. These are ground stations, satellites, and the sensors that both ground stations and satellites use to establish the link between them. The following is a short description of the characteristics that define each of these elements, defined as structures in MATLAB.

- Ground station: Ground stations are set as Targets in STK. They are defined by their location, given by (*latitude, longitude, altitude*). Furthermore, each one of them is assigned a name, typically the city where the GS is located.
- Satellite: Each satellite is defined by the six keplerian elements of the orbit it is placed in. These are: semimajor axis (a), eccentricity (e), inclination (i), longitude of the ascending node (Ω), argument of periapsis (ω) and true anomaly at epoch zero (ν).
- Sensors: The sensor object will be attached to either a GS or a satellite and it will allow to define the constraints associated with satellite-based QKD. To model simple line-of-sight availability, both GS and satellite sensors are set as simple cones, with a 90° cone half-angle. A relatively conservative approach is taken by setting the minimum elevation angle of the sensors located in the GSs to 20° [21]. Another constraint to be set in every sensor is the lighting one, which in STK should be set to "Umbra". This means that the QKD link will only take place when the satellite is in eclipse and when the GS is in night time.

4.1.2. MATLAB

The *structure* data type is used to process and store in an organized fashion the raw data obtained from STK. Each satellite will store information about every ground station and, in the case of ISL, about every other satellite.

The key rate model was developed at CQT before this work took place. It is explained in Appendix A. Its inputs can be classified in:

- Model inputs. This includes the specifications of the instrument used to do QKD, the pointing capabilities of the satellite, the diameter of the receiver telescope, etc. They are detailed in Section 4.2,
- Model variables. The results of the STK access study, namely the distance between the objects and the elevation angle for each Δt.

Computing the amount of key exchanged during a certain pass is then achieved by integrating the keyrate obtained over the period of time covered by that pass.

It is assumed that the satellites have been flying for a certain period of time, doing QKD every time it was possible with the different ground stations, and accumulating the key on board.

A key element to consider in an optical downlink is the cloud coverage. This has been taken into account with a dedicated function that simulates the cloud coverage for a certain location in a certain time of the year (see Section 4.3). With this factor one can obtain the true key exchanged for each pass.

A heatmap provides a quick visualization of the performance of each satellite/ground station pair. An example is given in Figure 4.2. This shows the result of a month-long simulation, with a constellation of 12 satellites divided in 3 orbital planes in a Walker Delta pattern fashion - evenly distributed both in longitude of the ascending node and in true anomaly. The ground network case corresponds to the G20 case described in 3.3.

Once the amount of key is computed, the logistics to manage it have to be defined. Following the prepare-and-measure protocol, each satellite will communicate to GS_A and GS_B (any two ground stations of the network) the XOR operation of K_A and K_B. The two following factors are reminded:

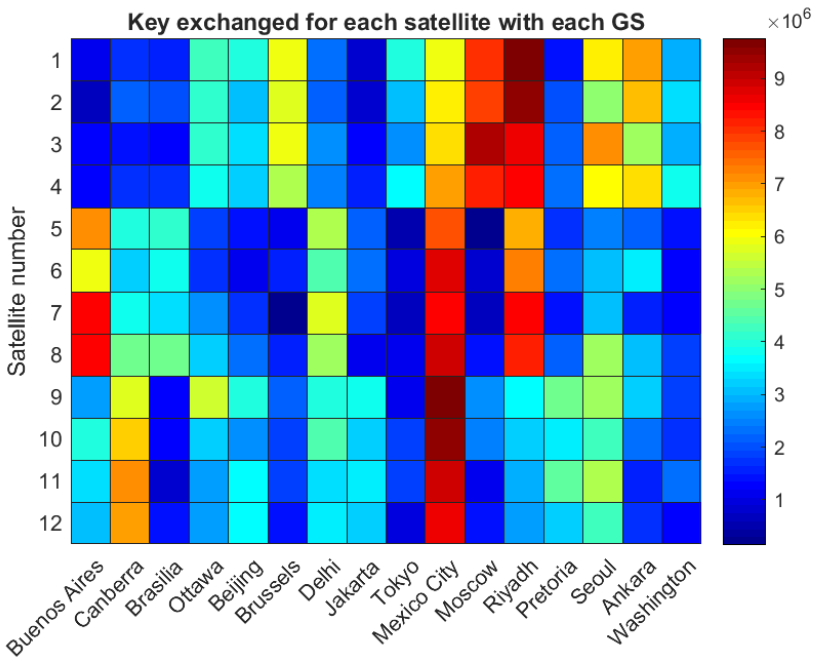


Figure 4.2: Example of heatmap displaying the amount of key exchanged between each satellite/ground station pair

- The satellite would downlink the result of the XOR operation via classic RF communication to either one of the two ground stations. As established, it is assumed that GEO satellites will be available to act as a relay, allowing for almost immediate downlink in any location of the globe. Downlink to only one of the ground stations is needed, since then the result of the XOR operation can be shared publicly via, for example, the Internet with the other ground node.
- For the XOR operation between K_A (the secret key exchanged between the satellite and the GS_A) and K_B (the secret key exchanged between the satellite and the GS_B), both elements shall have the same size. This means that if $K_A > K_B$, the amount of $K_A - K_B = K'_A$ will be left unused in the satellite. This opens up a new dimension on the research on how to do QKD in the most efficient way from space, as imbalances between keys exchanged with different ground stations will happen as a consequence of orbit geometry and local weather conditions.

In order to quantitatively study the performance of different constellations, the two generic use-case scenarios described in Section 3.3 are implemented.

4.2. Sensitivity analysis

A sensitivity analysis will help to understand how the different variables involved in the problem affect the final result (i.e. the key rate). In this particular case most of the variables being studied are not coupled, and if they are, their interaction is understood. It is therefore deemed enough to run a one-at-a-time (OAT) sensitivity analysis, which will serve the purpose of providing an insight on how each variable individually affects the key rate.

4.2.1. Parameters for the downlink scenario

Only parameters considered relevant for the scope of this thesis have been studied. This means that variables exclusively linked to the QKD protocols or to the optical instrument with little or no repercussion on the satellite and/or mission design have been left out of the study. The column named "Nom.val." is equivalent to the nominal value of each of the parameters used in the simulations of this work, which is the value set in the Micius satellite.

Sensitivity analysis parameters - Downlink scenario					
Name	**Description**	**Nom.val.**	**Range**	**Unit**	**Comments**
Range	Link distance	500	300 - 2000	km	Range of link distances correspond to circular LEO orbits design space
D_r	Diameter of receiver	100	15 - 200	cm	Commonly the receiver telescope diameter will be less than a meter, but larger ones are included for completeness
Err_{point}	Satellite pointing error	1.2	1.2 - 10	urad	Micius's value is exceptionally good, larger values are to be expected in other missions with worse ADCS
Divergence	Divergence of the Cassegrain telescope	5	1 - 20	urad	This value will depend on the transmitter telescope being used
Sky_{Br}	Sky brightness	0.4	0.25 - 20	$\frac{nW}{cm^2 sr}$	0.25 corresponds to pristine sky while 20 is a value that can be found in a city like Singapore at night
DCR	Dark count rate	25	20 - 100	counts/s	For receivers on ground, the detector is assumed to be appropriately cooled, hence the low DCRs considered

Table 4.1: Variables subject to the sensitivity analysis and their value ranges for the downlink scenario

4.2.2. Results for the downlink scenario

Figure 4.3 shows how the keyrate is affected by tweaking each one of the previously stated parameters within a plausible range.

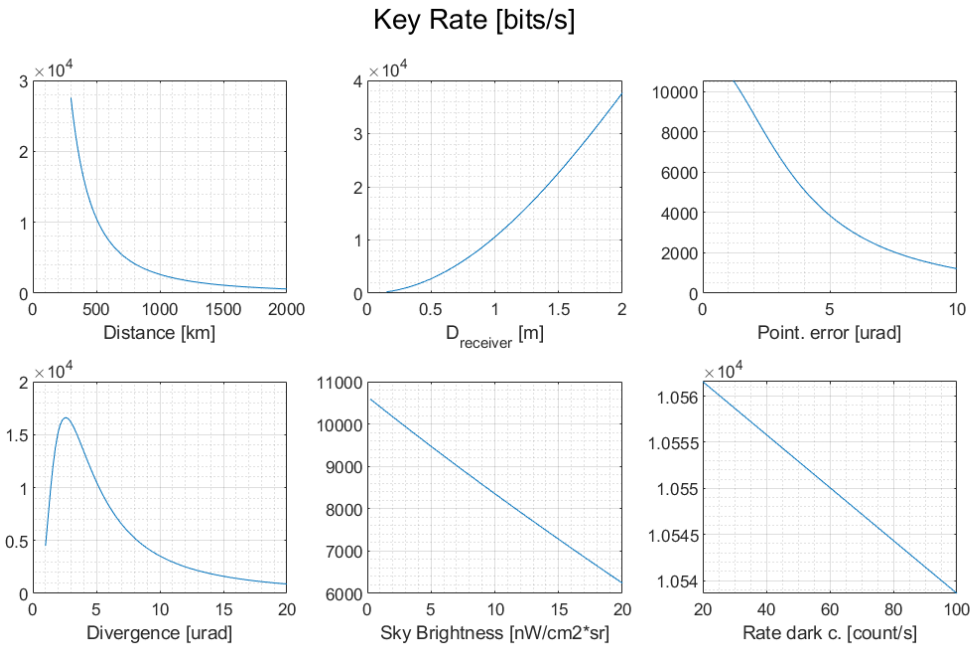


Figure 4.3: Sensitivity analysis results for the downlink scenario

An evaluation of Figure 4.3 shows how the keyrate increases or decreases with each parameter monotonically, except for the divergence. This is easily explained: with a very small divergence, the pointing error will play a crucial role, since all the photons are focused in a small area, therefore being more difficult to hit the receiver. However, if the divergence grows very large, it will be impossible to fit all the photons of the beacon

withing the diameter of the receiver, which explains why the keyrate value decreases after reaching a maxima for a certain divergence value. As shown in Figure 4.4, with a higher pointing error (five times higher in this example) the maxima for the divergence moves to the right, since to some extent is beneficial to have more divergence if the pointing error is larger.

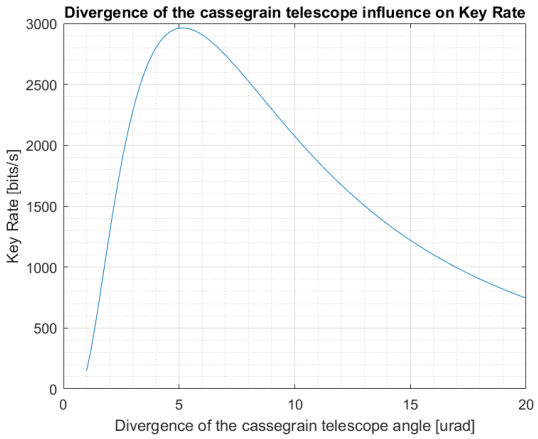


Figure 4.4: Sensitivity analysis results for the divergence when increasing the pointing error

4.2.3. Parameters for the ISL scenario

The parameters considered are very similar to those studied in the downlink case. Sky brightness is no longer taken into account as this sensitivity analysis is run for an intersatellite scenario. Furthermore, the distance parameter is separated in short and long range. The latter will define the maximum distance the satellites can be from each other to have above-null keyrate, which will condition the minimum number of satellites in a certain constellation to enable ISL. The range of other parameters are also accordingly adjusted to ISL, such as a maximum diameter of the receiver of 30 cm or a very high maximum dark count rate if the detector is not actively cooled, which dramatically decreases the keyrate as seen in Figure 4.5.

Sensitivity analysis parameters - ISL scenario					
Name	**Description**	**Nom.val.**	**Range**	**Unit**	**Comments**
Range	Link distance	2000	200 - 5000	km	For distances greater than 5000 km, the keyrate can be considered null for current satellite technology
D_r	Diameter of receiver	30	5 - 30	cm	Micius is a big satellite with room for a 30 cm telescope. For smaller satellites, this value will not be realistic
Err_{point}	Satellite pointing error	1.2	1.2 - 10	urad	Same logic as in the downlink scenario applies
Divergence	Divergence of the Cassegrain telescope	5	1 - 20	urad	Same logic as in the downlink scenario applies
DCR	Dark count rate	25	20 - 1000	counts/s	Counts will dramatically increase with no/less effective thermal control. It will be the case for small satellites where SWaP is a constraint

Table 4.2: Variables subject to the sensitivity analysis and their value ranges for the ISL scenario

4.2.4. Results for the ISL scenario

The results obtained follow the same trend as in the downlink scenario - though different parameter value ranges expectedly induce different keyrate values.

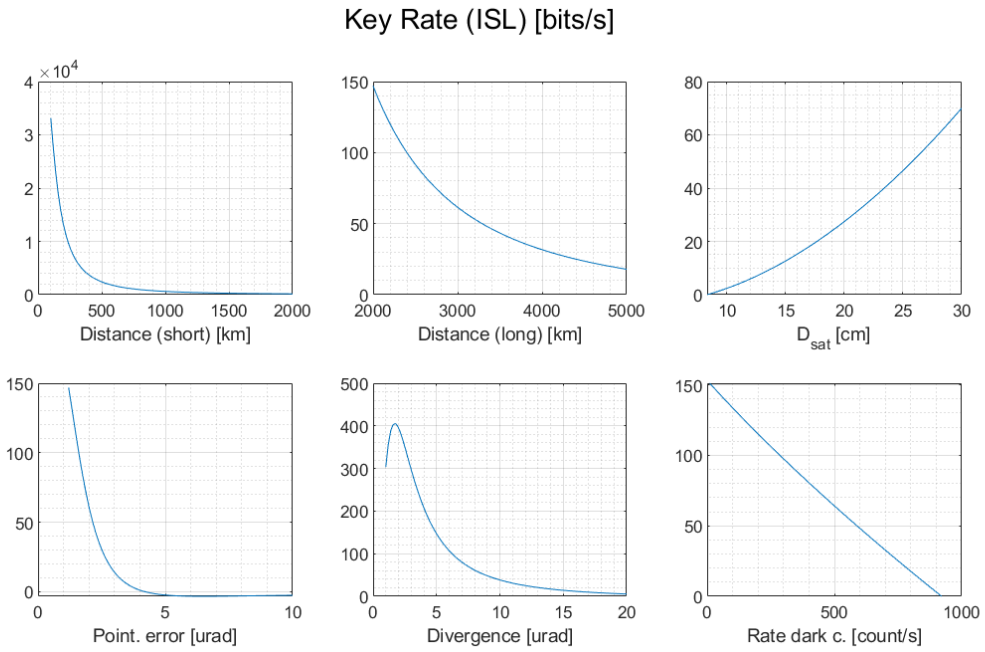


Figure 4.5: Sensitivity analysis results for the ISL scenario

4.3. Cloud coverage

Determining the cloud coverage of the location of a ground station plays a key role, as clouds impede the weak optical link. Using NASA's published values [31], inferred from the data collected by the MODIS instrument aboard NASA's Terra and Aqua satellites, a table with mean values and standard deviations is obtained for each location of the globe. Geographical granularity is equal to 0.1 deg, which roughly translates into 10 km for the areas being studied (with absolute latitude values typically lower than 60°).

For each location, the mean value is computed as the average monthly value (provided in the website) averaged for the last ten years. This characterizes the typical cloud coverage value of a given location during a specific month. Additionally, the standard deviation per month (and per location) has been computed from the daily average values provided. In the simulation, each time a satellite passes over a ground station, MATLAB's *normrnd* function is used to give a realistic cloud coverage value. This function randomly picks a value, following a normal distribution with the parameters previously determined.

The relevance of including a solid cloud model is understood by looking at Figure 4.6. In April, the Indian cities of the Indo-ASEAN scenario perform better in terms of amount of key exchanged since there tends to be a belt of clouds around the equatorial zone. However, in the summer India goes through the monsoon season, so in August it can be seen how, especially along the coast, clouds completely cover the Indian cities.

Given the high relevance of cloud coverage in this work, Figure 4.7 shows a map of the world with an average of the cloud coverage during three years. This map will be useful when analyzing the results obtained for different ground stations, which most of the times explain - at least partially - a delta-performance.

4.3.1. Very cloudy locations

Simulation runs with the previously explained cloud coverage model show that QKD would be close to impossible in locations with high cloud coverage factors, such as Singapore. To enable getting at least some key in these type of locations, it is assumed that QKD will be performed even at a 99% cloud coverage rate. It is common practice in optical communications to not initiate a link if the cloud coverage is beyond a certain value (e.g. 75%) but in the case of QKD one does not need to transmit complete data packages, hence making it worth it to get at least a small quantity of key per pass.

Additionally, a more detailed study would show that in some locations - again, such as Singapore - cloud coverage tends to be clustered around the same time of the day, and in fact the skies are usually clear at night

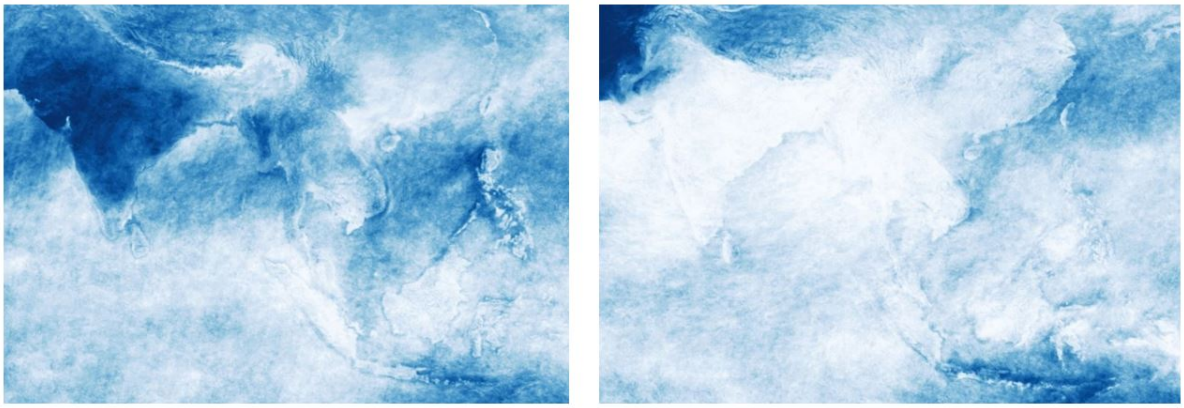


Figure 4.6: Cloud coverage in April (left) and August (right) for the Indo-ASEAN ground network. The lighter the blue, the more cloud coverage.

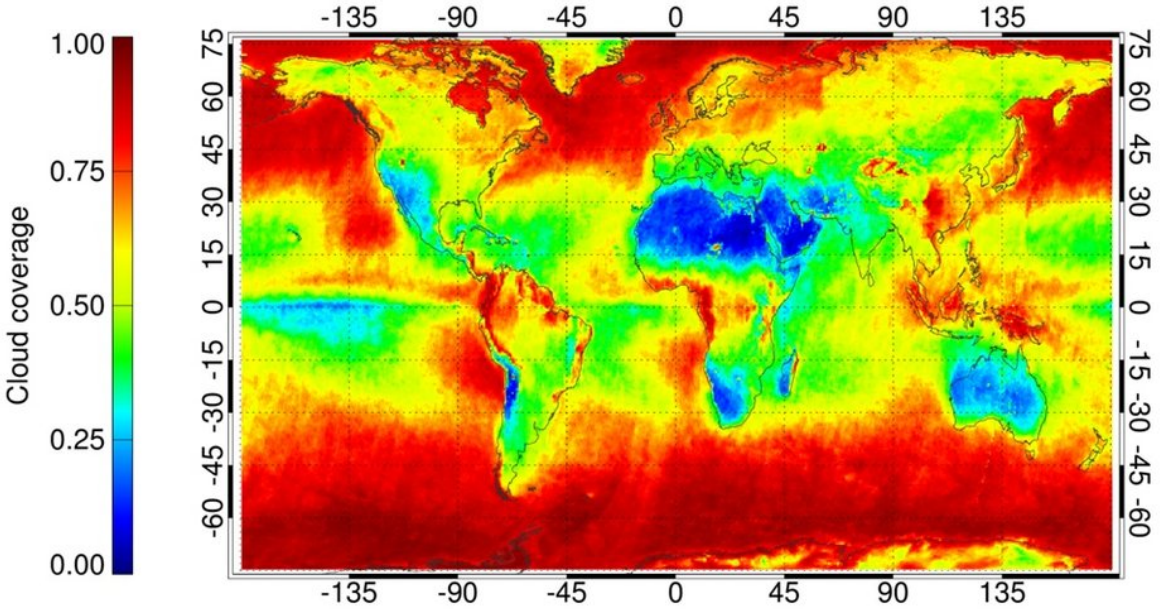


Figure 4.7: Global annual mean cloud cover derived from three years (2007–09) of Envisat data. Retrieved from [10]

time, when QKD is performed. Therefore, more detailed and even prediction models for clouds should be used for locations like this one or for potential commercial applications.

4.3.2. Cloud coverage timescale

With this model, a value for the cloud coverage is computed individually for each pass. A temporal relation between consecutive passes is missing. This is usually not a concern, except for cases when several different satellites pass over the same region (e.g. in a "string of pearls" configuration, with satellites evenly distributed over the same orbital plane). In these situations, cloud coverage for the pass of satellite i should be fairly similar to the one found for the next pass, of satellite $i+1$, if the time between the pass of both satellites is within the timescale of cloud coverage change. The conclusion remains the same: in the future accurate cloud prediction models should be implemented, especially if there is a greater interest in a determined region. Also, this issue applies in single-pass regime. As cloud coverage is computed from average values, the longer the simulation, the more realistic the key size values obtained will be - satellite i and satellite $i+1$ from the previous example will end up with practically the same keysize.

4.3.3. Results variability due to cloud randomness

Due to how clouds are simulated, results will vary from simulation to simulation. The goal of this section is to ascertain this variability, to allow for proper comparison between different configurations later in this thesis. The variability has been computed for the cases of interest studied here, namely yearlong simulations for the two proposed scenarios. The figure of merit studied is the one described in Section 3.4. Ten simulations have been run for each scenario, to analyze how this value fluctuates (the geometry of the constellation will be the same so the only variability between cases is due to the cloud simulation).

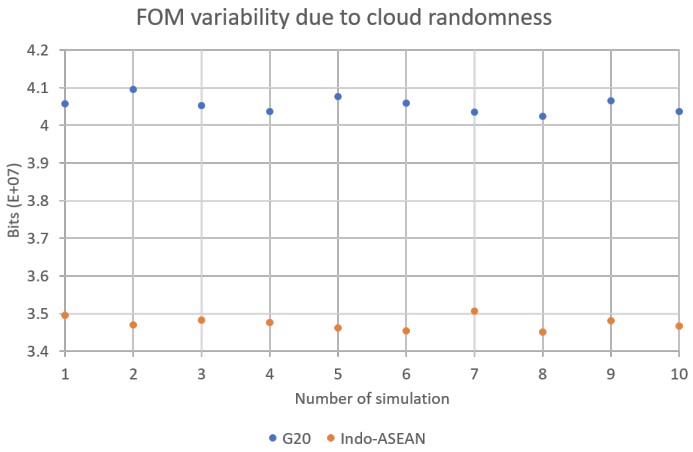


Figure 4.8: Variability on the FOM due to the randomness in the cloud coverage simulation

In both cases the average value practically coincides with the mean value obtained throughout the ten simulations. This short study intention is to have an estimation of the order of magnitude of this variability, in order to properly judge the results obtained when simulating different constellations. Based on the values obtained, fluctuations on the FOM smaller than ±0.4 Mbit will be attributed to the cloud randomness calculation.

4.4. Conflicting passes

If two ground stations are located close enough, the satellite will need to choose one to do QKD with (see Figure 4.9). The following assumptions are made when modelling the solution to this problem:

- The satellite will choose only one of the overlapping passes. This assumption works in the studied cases, where at most there is two ground stations close enough to find this problem. For a larger cluster of close ground stations, this condition would cascade and too many passes would be disregarded,

leading to an unrealistic result. In a regional model this should be taken account. Additionally, as a future step, the overlap duration could be computed and compared with the individual duration of the pass per ground station, to decide if it is worth it to start doing QKD with the first ground station and then initiate the process with the second one.

- The satellite will choose the ground station with the clearer skies.

To determine if two ground stations are close enough so the satellite has to choose, a minimum separation between ground stations is computed, as $d_{min} = h_{orbit} * cos(\epsilon_{min})$. The distance of every pair of ground stations is then determined, using the *haversine* formula 4.4 [16] that gives the distance of the greater circle linking two points on the surface of a sphere.

$$d = 2R_E sin^{-1}\left(\sqrt{sin^2\left(\frac{\phi_2-\phi_1}{2}\right) + cos(\phi_1)cos(\phi_2)sin^2\left(\frac{\lambda_2-\lambda_1}{2}\right)}\right) \tag{4.1}$$

Where (ϕ, λ) are the latitude and longitude of the ground station respectively.

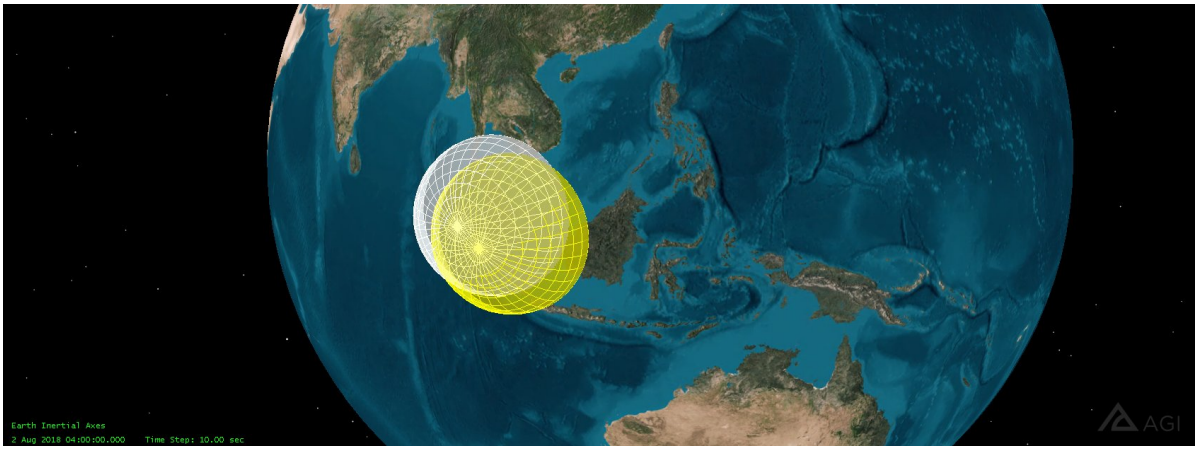


Figure 4.9: Graphic representation of Singapore (yellow) and Kuala Lumpur (white) ground stations areas of influence overlap

4.5. Validation

The only published data of a QKD mission in space is the one by the Micius satellite. This is the reason why it is considered sensible to use the inputs associated to this mission to carry out the desired simulations. In the same way, the published data allows to validate the model created here. For this purpose, the average sifted key rate is used as detailed in [21]. The same orbit is studied, a SSO with an altitude of 500 km exchanging key with the ground station located in Delingha.

Validation simulation input data	
Parameter	**Value**
Orbit perigee	490.9 km
Orbit apogee	507.1 km
Orbit inclination	97.3640 deg
Simulation period	23/Sep/2016 - 22/May/2017
Ground station	Delingha, China

Table 4.3: Values of input parameters for the validation study of the keyrate model

The real data corresponds to these same input parameters, with the difference that only 23 data points are disclosed in the publication. These are assumed to have been selected with the intention of showing how the key rate is affected by the weather conditions, obtaining very different values for passes with similar geometry.

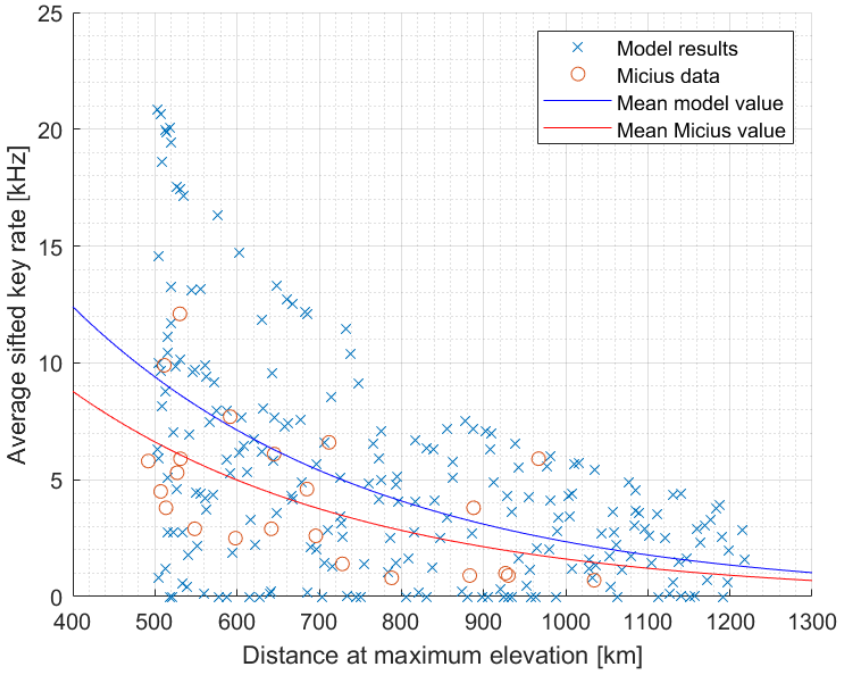


Figure 4.10: Validation of the key rate model (blue) with Micius data (red) and fitted curves

To exactly replicate the real values, cloud coverage data on the exact time of each pass would be needed. The model results are more optimistic than reality, as expected due to additional pass-dependent sources of key rate loss not being accounted for in the model. The best point from the Micius data (967 km, 5.9 kHz) agrees with the superior envelope of the simulation data, which corresponds to ideal conditions. Taking all this into account, this model is considered a valid representation of reality, and it will be used to perform further studies.

4.6. Graphical User Interface

With the goal of making the model user-friendly, a simple graphical user interface has been developed using MATLAB's app developer. Figure 4.11 shows the outlay of the interface. It lets the user choose the main parameters involved in the QKD constellation. For fine tuning of different elements (e.g. choosing different cities than the ones provided in the Ground Stations networks drop-down list) one must access the scripts. Therefore this tool is intended for quick analyses, including as default options the cases that have been shown to be the most interesting for research in this thesis.

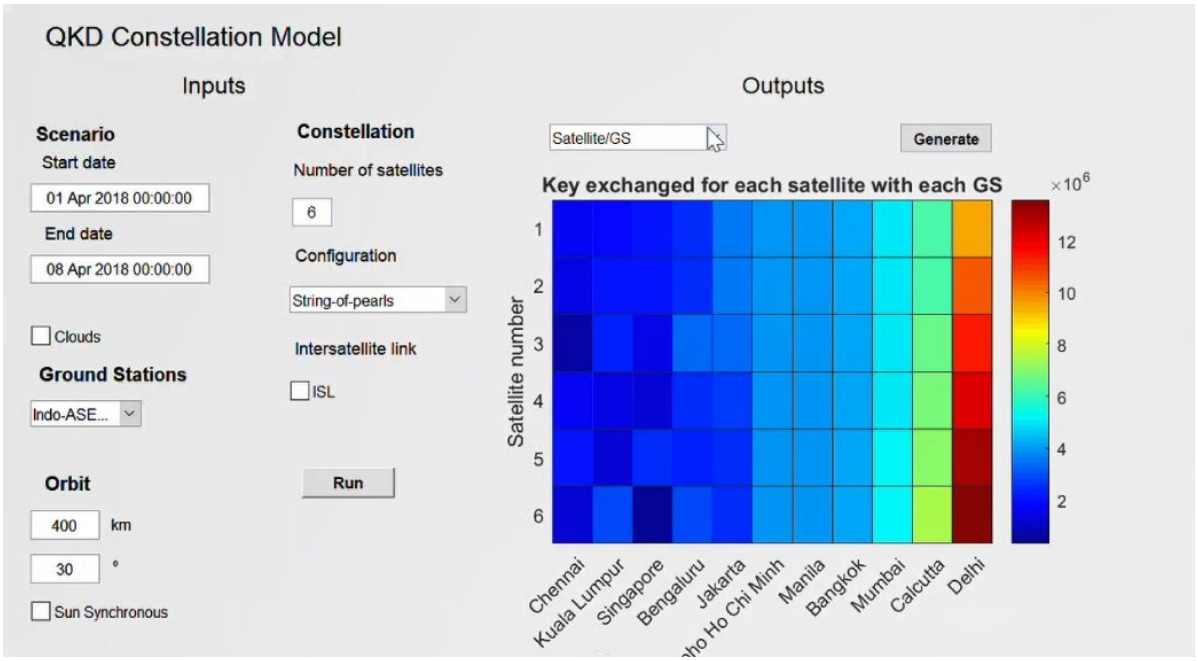


Figure 4.11: Graphical User Interface for the QKD constellation model

5

Constellation design

5.1. Initial considerations and assumptions

Throughout this work, the following assumptions will apply. These are mostly common sense that will make the results converge towards feasible and plausible configurations. Establishing these assumptions now will avoid ending up with configurations that maximize performance but are so complex or costly that they could never be implemented.

- Identical satellites: assuming that every satellite of the constellation will be identical simplifies both the analysis and the execution of the potential mission. Strictly speaking, not all the satellites involved will be identical as in this work a GEO relay is assumed. However, the GEO satellites are assumed to be already in orbit fulfilling a different primary goal, and helping the QKD satellite constellation as a secondary function.

- Same a, e, i orbits: this assumption will be discussed in detail in the following pages, but the orbital planes of the constellation will only differ in their longitude of the ascending node - while the satellites' position will also have the additional degree of freedom given by the true anomaly.

- GEO relay: as mentioned in Section 3.1, a relay comprised of GEO satellites will be used for near-immediate downlink of key whenever requested. This assumption will focus the study of this work in the key buffering itself, which is the part where the quantum link takes place. Downlink of the keys is done via classical communication, so the interest of its study with no GEO relay would be of merely logistic nature. The Inmarsat constellation is a valid example, currently comprised of twelve geostationary satellites.

- Small satellites: even though the analysis presented in this work is valid for any type of satellite, basic information about the spacecraft will be needed for certain mission design choices. Given the current QKD state-of-the-art and the future developments taking place [7] it is safe to assume that a 12U satellite would serve as an adequate bus for a QKD payload, especially with the copious choice of miniaturized technologies available nowadays.

5.2. Single orbit parameters

The first step to design a constellation will be the definition of the orbital plane that will be used. By the stated assumptions, the constellation design will have two degrees of freedom from the six keplerian elements - the longitude of the ascending node of the orbital plane and the true anomaly of each satellite within its orbital plane. The argument of the periapsis is undefined as circular orbits are assumed.

5.2.1. Eccentricity

Most LEO constellations existing and planned for the near future are made of circular orbits. The main reason for this choice is the constant set of distances between satellite and ground (the minimum distance being the orbit height, at an elevation angle $\epsilon = 90°$ and the maximum one corresponding to the minimum elevation angle of the ground station, ϵ_{min}). Fixing this design variable simplifies the overall design of the mission and has no drawbacks. In reality, if the desired result is a circular orbit, it will be better to opt for a frozen orbit, where some orbital parameters are slightly deviated from a pure circular orbit such as the higher-order potential harmonics of Earth's gravitational potential are compensated for. The result will be a sustainable quasi-circular orbit instead of an initially pure circular orbit, which due to its inherent instability would end up with a larger oscillating eccentricity value (assuming no in-orbit correction manoeuvres) [44].

In some scenarios, an elliptical orbit could be useful. In an elliptical orbit the satellite will spend more time in the region surrounding the apogee. Therefore, an orbit design in which the apogee is located above the Earth region of interest is an interesting choice for some specific cases. Satellites servicing Russia are a typical example. Satellites placed in a *Molniya* orbit spend a long time flying over the latitude region where Russia is located.

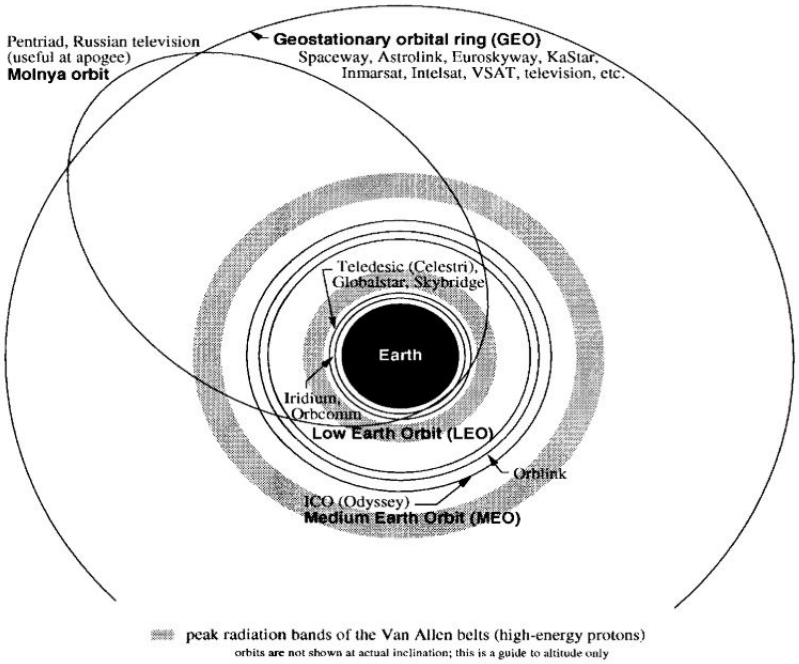


Figure 5.1: Schematic of different types of Earth-orbiting constellations. Retrieved from [13]

Figure 5.1 shows a schematic of different Earth orbits, ranging in altitude and also showing the aforementioned *Molniya* orbit.

For the sake of completeness, it must be mentioned that exotic configurations are being researched for Earth-orbiting constellations. They are usually made of elliptical orbits. An example are the *Flower constellations*, which are "special satellite constellations whose satellites follow the same 3-dimensional space track with respect to an assigned rotating reference frame" [37]. These constellations are still being researched and will not be considered for this thesis.

Assuming circular orbits also simplifies the study of the other orbital elements. By definition, the argument of periapsis is undefined for circular orbits [43] hence not being needed to consider it as a design variable. The semi-major axis will be equal to the semi-minor axis, so only the radius of the orbit will need to be defined - equal to the Earth radius plus the orbital height.

5.2.2. Semi-major axis

A maximum-possible height of the orbit can be inferred from the model due to its dependence on the height. When considering constellations, micro or even nanosatellites are the realistic candidates due to budget lim-

itations. Therefore, using the Micius satellite source as an upper boundary to determine the highest altitude seems an adequate approach. An analysis with the model shows that the QKD keyrate is zero at approximately 4000 km of distance between transmitter and receiver. Considering a minimum elevation of the ground station pointing equal to 20°, this translates in a circular orbit of approx 1368 km. In reality a LEO orbit will not go beyond 1000 km of altitude to avoid the inner Van Allen belt so that will be the maximum altitude considered.

QKD from higher altitudes would strictly speaking be possible, but impractical in reality with today's technologies.

To set a minimum boundary, the most stringent constraint will be lifetime. However lifetime is also a boundary for maximum altitude due to regulations by the IADC on LEO orbits not allowing a post-mission orbital lifetime greater than 25 years. Reentry systems can be considered, but it does not seem appropriate in this case since higher altitudes are not advantageous. The following brief calculation yields the approximate lifetime of a 12U. Figure 5.2 gives an approximate lifetime based on the ballistic coefficient. This coefficient is defined as $\frac{m}{C_D A_f}$ where m is the mass of the satellite, A_f is its frontal area (24 kg and 23x24cm respectively for a 12U [34]) and C_D is the drag coefficient, assumed equal to 2.2 for a regular spacecraft [44]. The result is a ballistic coefficient of approximately 200 kg/m^2.

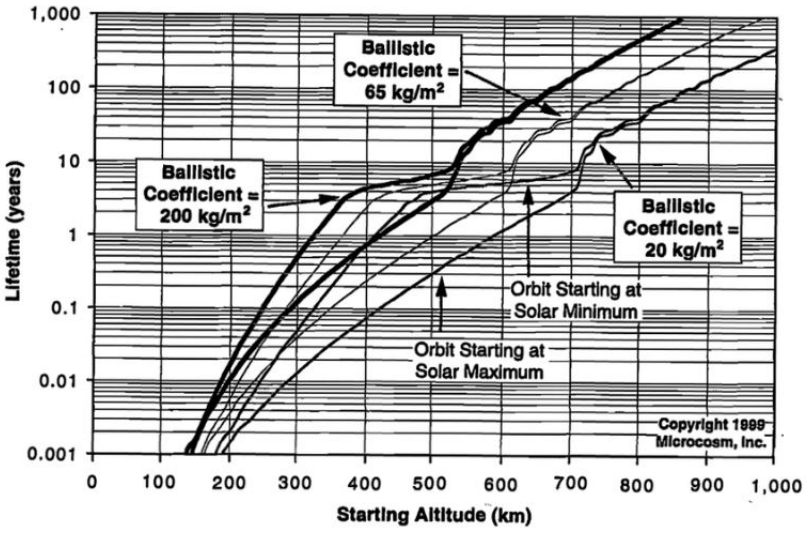


Figure 5.2: Satellite lifetime as a function of orbit altitude and ballistic coefficient. The solar activity influence is also shown. Retrieved from [44]

A satellite located in a higher orbit will have a lower relative velocity with respect to ground, and therefore it will have a longer time period pass over the ground stations. This difference is however barely noticeable in the range of altitudes being discussed here since $\frac{h}{R_e} \ll 1$.

Furthermore, cost will generally be reduced by lower orbits. If a coverage requirement is set, higher orbits would help meet said requirement with fewer satellites, hence potentially being a more cost-effective solution. Nevertheless, this would be a topic for a detailed case-by-case study that deviates from the general case that is sought after in this work.

For the case studies considered here, an orbit of 400 km of altitude will be chosen. Keyrate is prioritized, and the lifetime is still acceptable if it is in the order of several years. In each particular case this altitude would need to be optimized, which is a subject of discussion in Chapter 7.

5.2.3. Inclination

The inclination of the orbit will determine the maximum absolute value of latitude being covered. Two extreme cases are easily discerned. An equatorial orbit, with an inclination equal to 0° can be useful to maximize coverage for the regions surrounding Earth's equator. With no determined ascending node, the Ω parameter is undefined for these type of orbits [43]. On the other side of the spectrum, polar orbits are those whose inclination is set to 90°. They are used for its complete global coverage, and the ease of creating a uniform grid-like configuration when designing a constellation.

There is however a special case worth mentioning. It arises from the fact that the Earth is not a perfect sphere, hence introducing non-uniform effects in its gravitational attraction. Some of these perturbations in the gravitational potential induce very small changes in the orbit parameters. However, the largest one, known as J_2 and due to the Earth's oblateness, induces a constant effect: the rotation of the ascending node [44]. This rate of variation is known and it can be computed with equation 5.1 [29].

$$\dot{\Omega} = -\frac{3}{2}\frac{R_E^2}{a^2(1-e^2)^2} n J_2 \cos i \tag{5.1}$$

Where $\dot{\Omega}$ is the rate of variation of the ascending node, R_E is the Earth radius, a is the semi-major axis of the orbit, e is the eccentricity, i is the inclination, $n = f(a)$ is the orbit mean motion and J_2 the coefficient describing the Earth bulge around the equator causing the perturbation. With this equation one can fix certain values (assuming circular orbit, with fixed altitude) and design the orbit with an inclination such that the rate of rotation of the ascending node matches the angular speed of rotation of the Earth around the Sun. This type of orbit is well known and widely used, and it is called a *Sun Synchronous orbit* (SSO). Thanks to this property, the orbital plane preserves its orientation with respect to the Sun at all times. This makes the satellite cross the equatorial plane at the same local time in every orbital revolution. Approximately constant solar influx conditions will also result in simpler power and thermal subsystem designs. The calculation of the inclination value depending on the other parameters is automated in the model and just requires the user to state their choice of a SSO together with the desired orbital height.

Sun Synchronous orbits have been used mainly with EO purposes. A popular choice is the *dusk-dawn* orbit in which the satellite flies over the terminator line: at this local time the shadows cast by the Sun are the longest, thus providing good contrast, ideal for observation purposes [44]. As an example, most of ESA's Sentinel satellites are placed in a SSO.

In the context of QKD, it is easy to see how using a SSO could be appropriate. As discussed in Section 2.3.2, currently QKD must be done in eclipse circumstances: a SSO provides a steady fraction of eclipse time that could be attractive for QKD purposes. However, some configurations such as the dusk-dawn one will barely provide any eclipse time. The best SSO for QKD purposes will therefore be a *noon-midnight* SSO. In this orbit, the satellite always crosses the equatorial plane at noon, or midnight, regardless of the time of the year. This will yield the maximum steady eclipse time possible, increasing the keysize obtained. This is clearly shown in Figure 5.3.

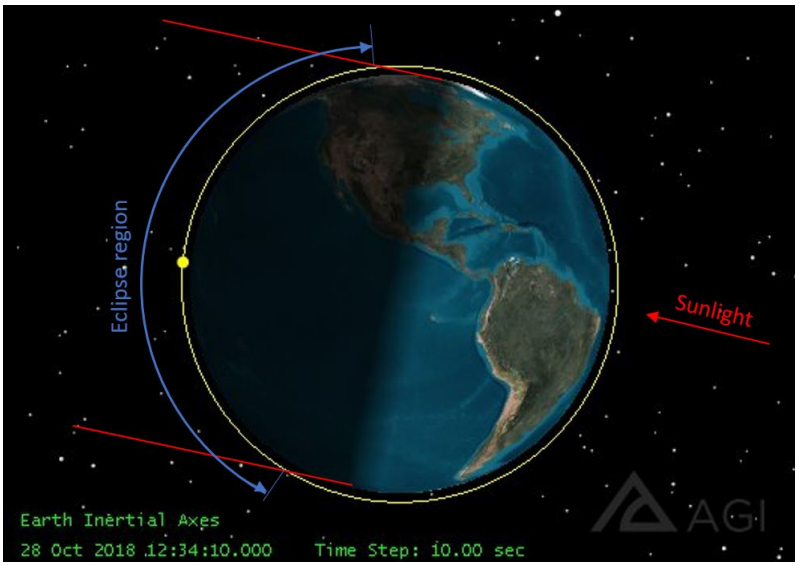


Figure 5.3: Schematic of the eclipse region in a noon-midnight SSO.

Overall, low-inclination orbits will not be considered as they cannot cover higher-latitude ground stations. Orbital planes with different inclinations could be a sensible choice for specific sets of ground stations, but in general it is a non-preferred solution as complexity and cost are increased. Therefore, as stated in the assumptions, all the orbital planes of the constellation will have the same inclination.

Minimum inclination

The most northern ground station sets the minimum inclination - approximately equal to its latitude. It will be useful to compute the range around this value where the orbit will still provide access to the ground station. With this value - from now on, θ - one can determine that the minimum inclination value to cover the ground station will be $GS_{latitude} - \theta$ while the inclination required to give complete coverage to said ground station will be $GS_{latitude} + \theta$.

Figure 5.4 shows the geometry sketch used to compute the desired angle θ. With the law of sines and cosines it can be obtained directly. A, B, C are generic angles of the triangle while a, b, c are generic sides of the triangle, ϵ_{min} is the ground station's minimum elevation, R_e is the Earth's radius and h is the orbital height.

$$a^2 = b^2 + c^2 - 2bc\cos A \tag{5.2}$$

$$\frac{\sin A}{a} = \frac{\sin C}{c} \tag{5.3}$$

Where:

- A = $90 + \epsilon_{min}$
- a = $R_e + h$
- b = R_e
- C = θ

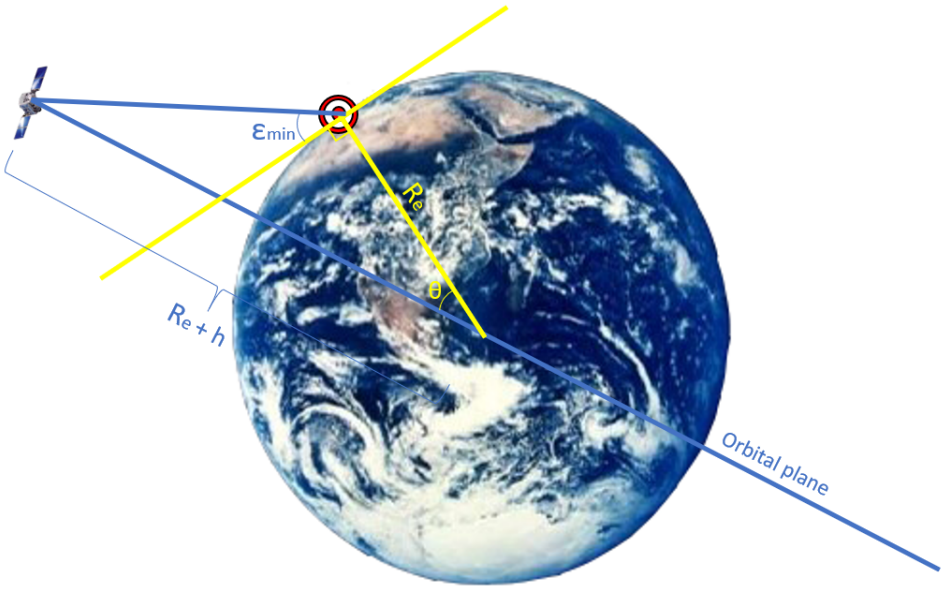


Figure 5.4: Minimum inclination case to cover a certain ground station

5.3. Orbit selection

As a summary, orbit selection for the QKD constellation is reduced to determining the inclination. Considering the guidelines stated in the previous section and the requirements outlined in Section 3.4, a study of the different inclinations can be performed for the two scenarios that will serve as an example for a QKD constellation throughout this thesis.

As a note for future sections, all the results presented in this work correspond to yearlong simulations. This avoids season-dependent effects and averages out the varying keyrates due to the J_2 effect.

5.3.1. Single-orbit results

In this stage of the analysis, each orbital plane is evaluated only on the access profile it has with the different ground stations throughout a year, without running the cloud coverage and QKD keyrate model. The keysize obtained is directly proportional to the access duration between satellite and ground station. Similarly, the rate of new key generation is determined by the gap between accesses for a certain ground station. These are the two figures studied here, computed as a mean for the values obtained for each ground station. Certainly, this only serves as an indication of how to proceed with the actual QKD analysis. Moreover, the "maximum gap" information - defined as the maximum revisit time over the studied period - is merely anecdotal, as in a constellation set up when one orbital plane is facing the sun - so no accesses are registered - the other planes will probably not be in such unfavourable situation, therefore obtaining much better values for this metric. This is better understood by looking at Figure 5.5 where the accesses of a constellation of satellites in a SSO orbit are compared to the accesses of a constellation formed by 30° orbital planes distributed in longitude of the ascending node. As it can be seen, the latter option presents bigger gaps at some points (i.e. when the orbital plane's normal vector is the most parallel to the sunlight) but the other planes can "cover" this gap.

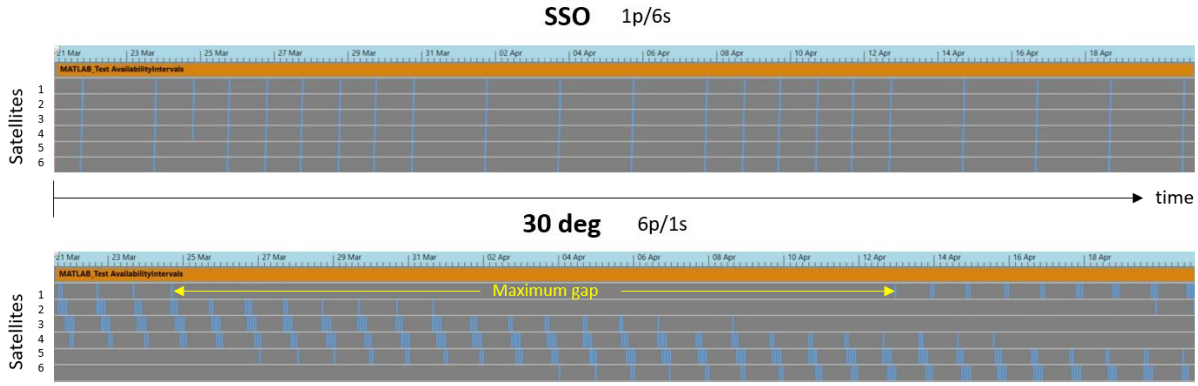


Figure 5.5: Access profile of one ground station for a *noon-midnight* SSO with six satellites and six 30° orbital planes evenly distributed in LAN with one satellite per plane

Regarding the inclination profile being studied, the minimum inclination is chosen approximately equal to the maximum latitude found on the set of ground stations. For the sake of completeness, retrograde orbits - those with inclinations larger than 90° - are considered in the analysis, though their use is limited due to cost reasons, requiring a larger delta-V injection. Therefore, the inclination profile will range between the minimum inclination to "180° minus the minimum inclination", using a reasonable number of sample points. Because of its special lighting conditions, a noon-midnight SSO will also be included in each analysis. The cost argument for retrograde orbits does not apply in this case as SSO are a popular choice for numerous missions, which translates in availability of launchers such as the Vega launcher. For the case study of an orbital height of 400 km, the inclination angle corresponding to a SSO is of 97.0347°.

Figure 5.6 and Figure 5.7 show the results obtained for this single-orbit analysis for the Indo-ASEAN ground station network. The main conclusion to be extracted is that it is beneficial for the keysize to have a constellation with the lowest inclination possible. As commented previously, this value is bounded by the city of maximum latitude. It is clear to see in Figure 5.6 how as the inclination increases, the access time decreases. Not surprisingly, this is not the case for the SSO due to its special properties that make it preserve its advantageous attitude towards the Sun throughout the year, maximizing the eclipse time and therefore having more useful passes over the different ground stations. Figure 5.5 illustrates the results depicted in Figure 5.7.

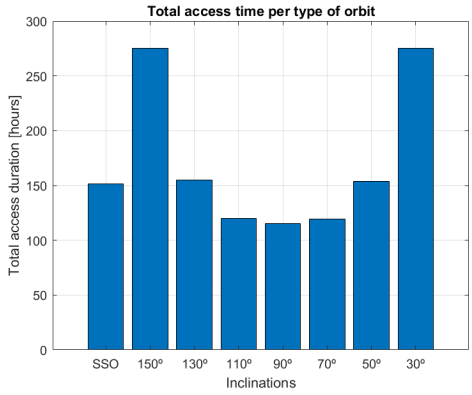


Figure 5.6: Total access time for the Indo-ASEAN network with different inclinations

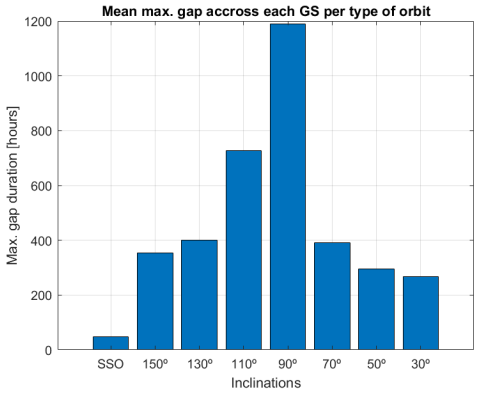


Figure 5.7: Maximum gap duration for the Indo-ASEAN network with different inclinations

For the G20 case, similar results are obtained. Lower inclinations and the SSO are the overall best performing orbital planes. Contrary to the previous case, the SSO now outperforms low inclination orbits, due to the ground stations being scattered around the globe. The detailed analysis for the constellations will be performed in Section 5.5.

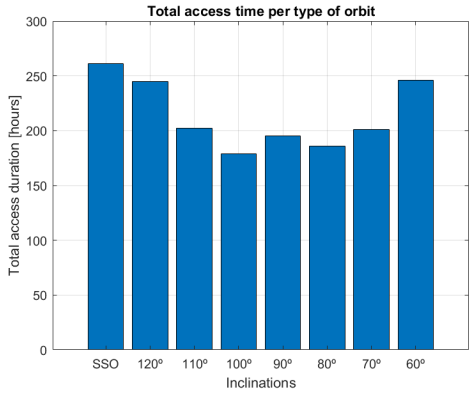


Figure 5.8: Total access time for the G20 network with different inclinations

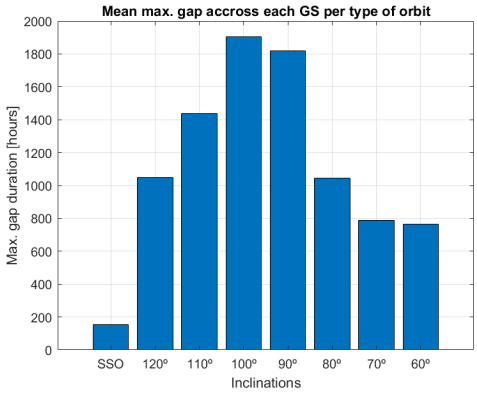


Figure 5.9: Maximum gap duration for the G20 network with different inclinations

5.4. Number of satellites

The number of satellites is a variable whose limit is purely cost-based. Technically, QKD service could be provided with only one satellite. This is however far from optimal and it defeats the purpose of studying the behaviour of QKD in a constellation. In the other extreme, adding satellites to the constellation will always improve its performance, but it is also not realistic beyond a certain point. The tool developed in this work enables the user to choose any number of satellites. For this work the number of satellites has been fixed in order to enable for comparison between cases. The number of satellites chosen - for the downlink-only scenario - is six. This choice follows a simple cost-based logic that can be easily understood with Figure 5.10. If one were to fix the cost of the Micius satellite (i.e. one satellite of the 500 kg category), drawing an isocost line would yield between 5 or 6 satellites belonging to the 20 kg category. As previously stated, a realistic bus for a QKD constellation has a dimension equal to 12U, which fits in that weight category. Following this rationale, 6 satellites have been chosen for the different cases.

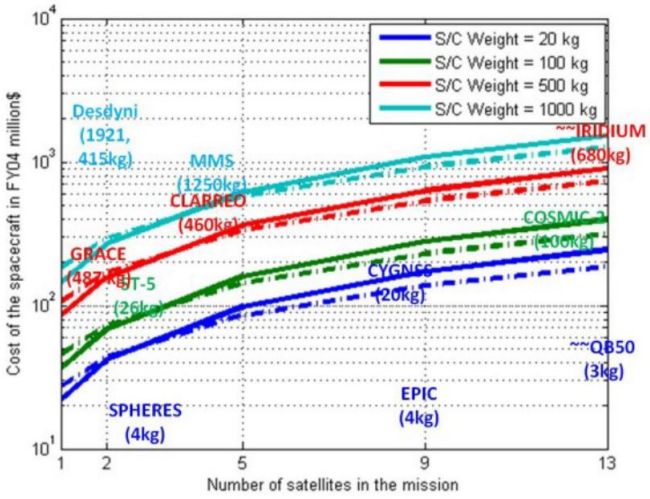


Figure 5.10: Cost model for different satellite weight categories. Retrieved from [30]

5.5. Applied cases and results

In this section the process of the QKD constellation design will be shown for the two sets of ground stations that have been introduced. Throughout the rest of this work, the following notation will be used to shortly describe the constellation: mp/ns. The parameter m is the number of different orbital planes in the constellation (i.e. the number of orbital planes with different longitude of the ascending node) and n is the number of satellites *per* orbital plane. It follows that the total number of satellites will be equal to $m * n$.

5.5.1. Indo-ASEAN results

Based on the results shown in Section 5.3, the 30° orbital plane and the *noon-midnight* SSO one were selected. For the latter, there is just one valid satellite arrangement for the SSO constellation: this is in only one orbital plane, with a LAN set to make the SSO a noon-midnight one. Regarding the distribution of the satellites within the orbit, an even distribution will make the most sense to maximize coverage. Therefore, the only SSO configuration to be studied can be noted as 1p/6s. The situation is different with the 30° orbital plane. In this case, placing all the satellites in the same plane (1p/6s) is clearly not a valid configuration as proved by the maximum gap study in a single orbital plane configuration. Figure 5.5 suggests that the greater the number of orbital planes, the better these "gaps" will be filled, avoiding situations where some ground stations would see no passes for long periods. However, placing satellites in different orbital planes will come at a delta-cost. This is why several configurations will be analyzed, to assess how keysize is affected by the different satellite distribution. In this case, the following configurations will be studied: 2p/3s, 3p/2s and 6p/1s. For the configurations with several orbital planes, the satellites will be distributed along the different planes following a Walker-Delta fashion. This results in an even distribution. The phase difference parameter 'f' will be set to 0 for these studies.

SSO case - 1p/6s

The following are the results obtained for a yearlong simulation corresponding to six satellites evenly distributed in a noon-midnight SSO, exchanging key with the cities that form the Indo-ASEAN network. A graph from each category will be shown to understand in future comparisons which results are obtained from each simulation.

Perhaps the most intuitive graph, Figure 5.11 shows how much key Satellite 1 has exchanged with each ground station.

For a compact visualization of the data, a heatmap plot is created, summarizing the the key exchanged by all satellite-GS pairs. The heatmap obtained in this case is shown in Figure 5.12.

Following a similar logic, but already introducing the communication between ground stations, a graph is produced for each ground station showing how much key it could potentially have with another certain

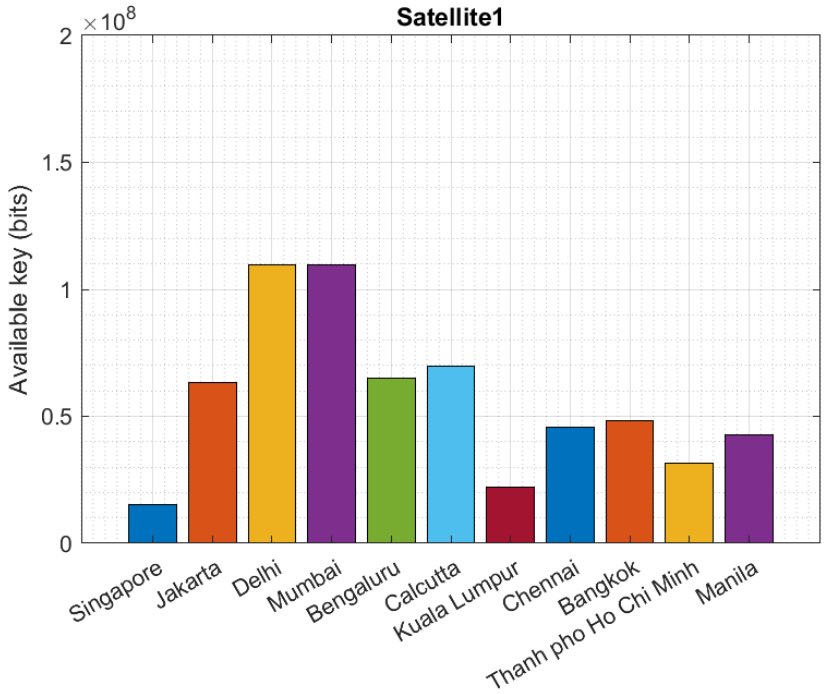


Figure 5.11: Keys stored on-board Satellite 1. SSO constellation for the Indo-ASEAN case.

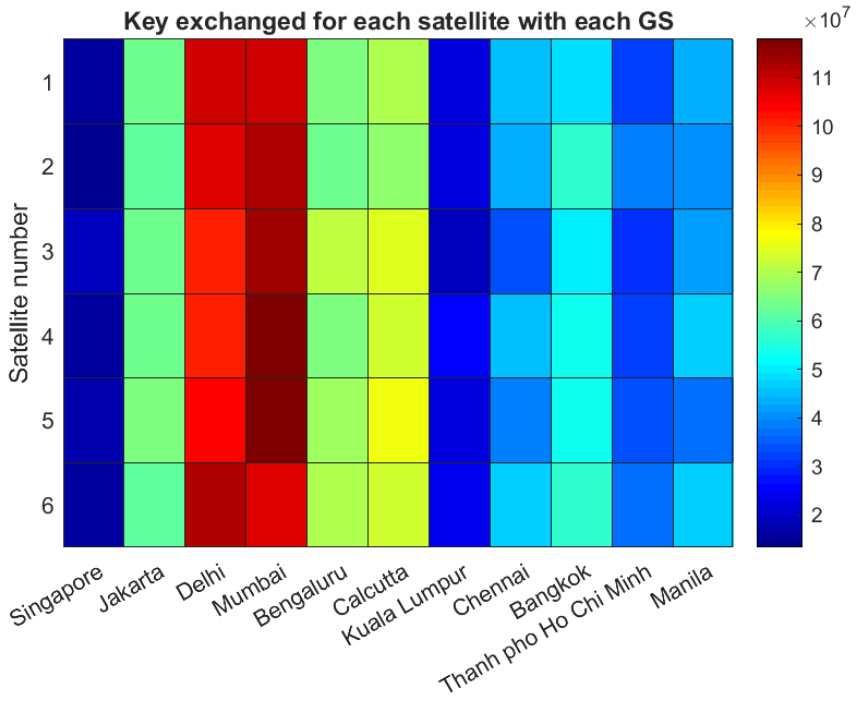


Figure 5.12: Heatmap of keysize exchanged between each satellite-GS pair. SSO constellation for the Indo-ASEAN case.

ground station. The limitation imposed by the ground station with the smaller key already comes into play. An example of this type of result graph is shown in Figure 5.13

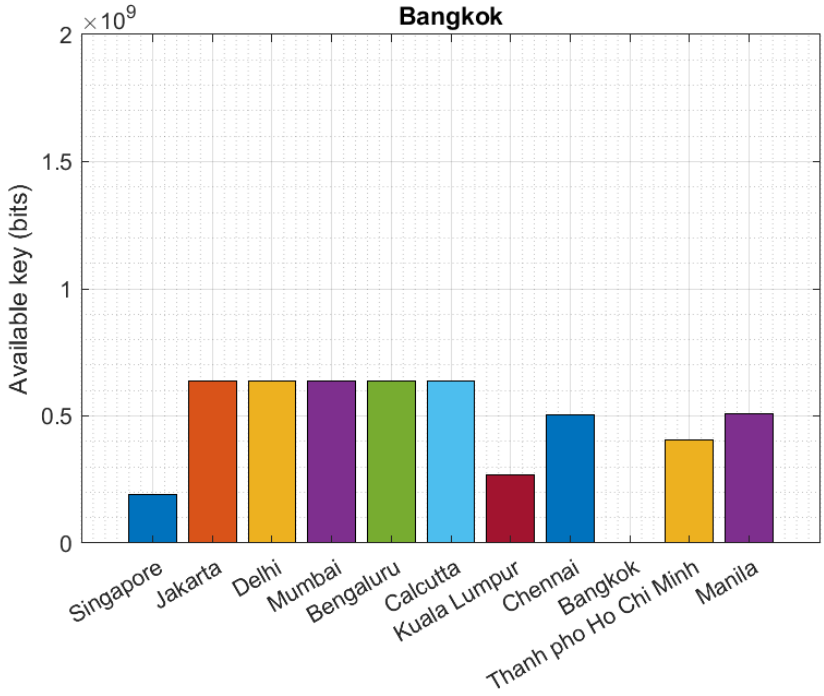


Figure 5.13: Bangkok's potential key available with each ground station of the network. SSO constellation for the Indo-ASEAN case.

There are two remarks to be made regarding this graph:

- The different bars are potential key between GS_m and GS_n. In this case, this means that Bangkok has 0.7x10^9 bits with Jakarta. But if in reality it uses this key with Jakarta, it will not have any more key to use with the rest of ground stations. That is why the graph is presented as *potential* key available.
- In this graph it is easy to see how the key between two different ground stations is limited by the ground station with the least key. Jakarta, Delhi, Mumbai, Bengaluru and Calcutta all have more key than Bangkok (see Figure 5.12). This is why in this graph they all have the same value, which is equal to twice the maximum keysize that Bangkok has available, as it was explained in Section 3.2.3. Equivalently, the ground stations with less keysize than Bangkok will be the limiting ones, showing a smaller value in this graph.

Analogously to the satellites, a heatmap can be plotted to better visualize the potential interactions between ground stations. This is shown in Figure 5.14.

Using this graph or the heatmaps the service each ground station gets can be assessed by identifying the stations that are lacking behind. Ideally the constellation is designed to minimize these differences, which improves the overall performance of the constellation.

From this one case alone a reflection can already be made on the different performance between the cities of the Indo-ASEAN group. The following factors are found when justifying a difference in obtained keysize between ground stations. They can be applied at a general level, for any set of ground stations.

- High cloud coverage. Ground stations located in cloudier areas will be noticeably affected. Figure 5.16 shows the yearly cloud coverage value - in a traditional RGB scale - for the Indo-ASEAN region. One can appreciate how cities like Delhi and Mumbai will end up with more key than Singapore or Kuala Lumpur.
- Ground stations near the equator. This is barely a differentiating effect within the ground stations of this network, as all of them have a reasonably low latitude and the orbit is almost a polar one. However

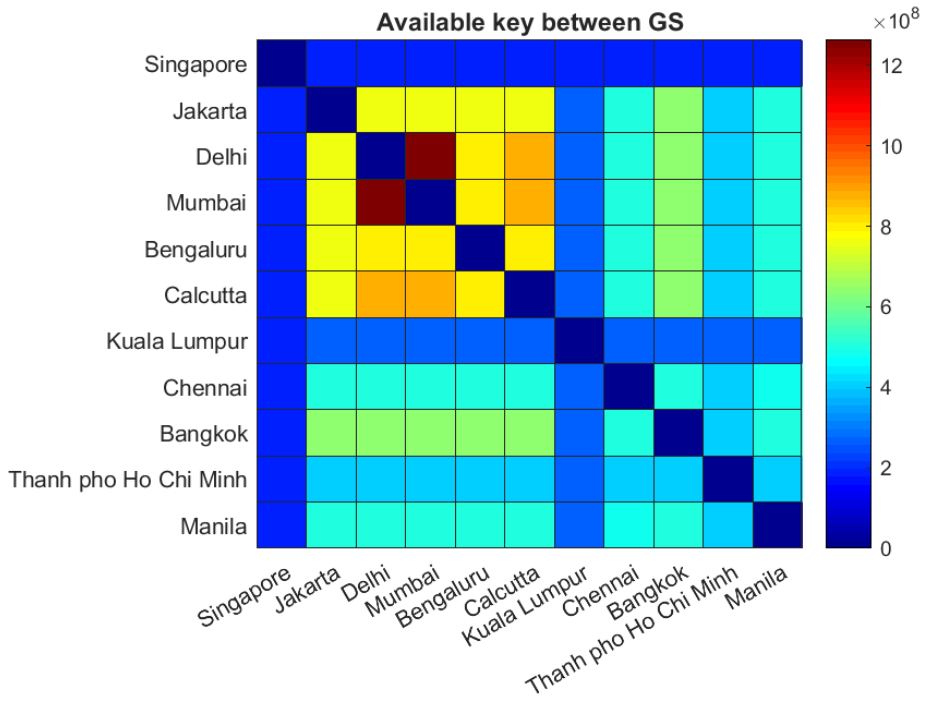


Figure 5.14: Heatmap of potential keysize between each GS pair. SSO constellation for the Indo-ASEAN case.

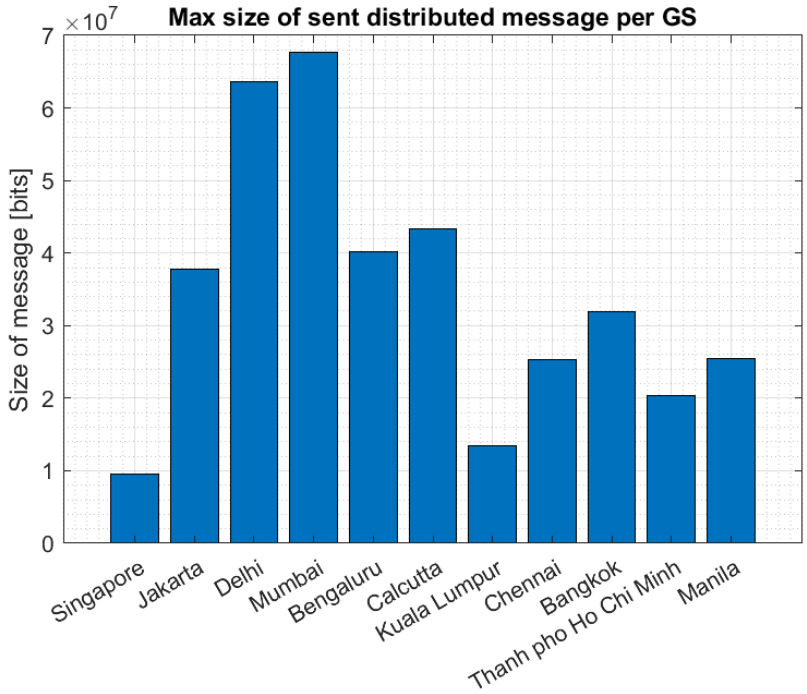


Figure 5.15: Maximum size of a potential distributed message sent by each GS, encrypted with OTP. SSO constellation for the Indo-ASEAN case.

for other inclinations, ground stations with a latitude close to the inclination of the orbit will benefit with respect to other ones, and in general ground stations in the equatorial area will have less access time [36].

- Conflicting passes. As explained in Section 4.4, when two ground stations are close enough, the satellite will need to choose which one it does QKD with. Taking into consideration the assumptions and modelling stated in the aforementioned section, the pairs of ground stations affected by this peculiarity will obtain approximately half of the keysize - as such close ground stations will have similar cloud coverage values.

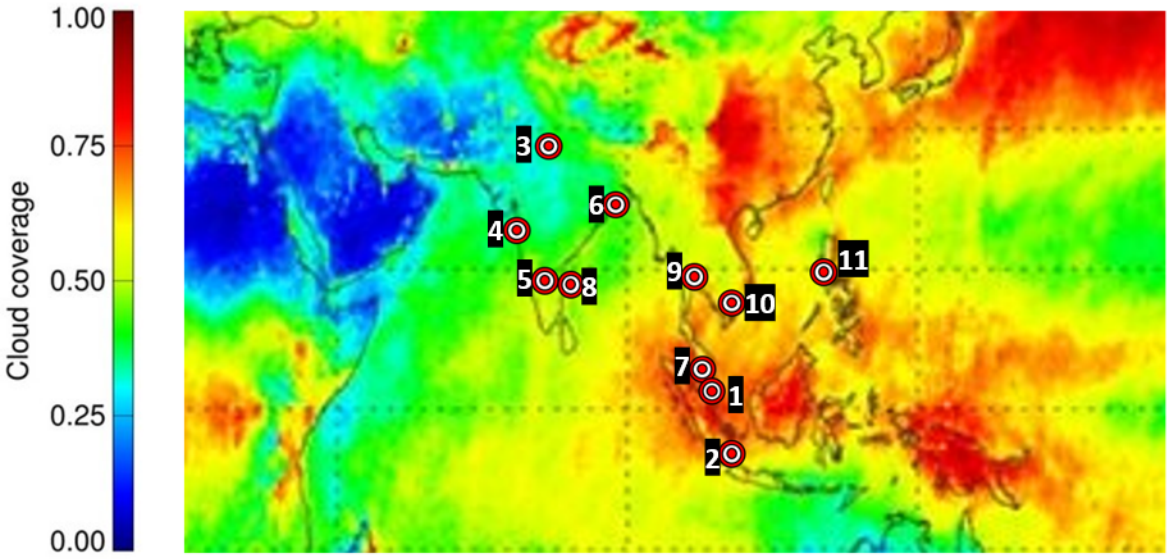


Figure 5.16: Indo-ASEAN ground stations on a cloud coverage map. Modified from Figure 4.7. The numbers refer to each city in the order shown in the result graphs.

30° cases

From the conclusions drawn in the single orbit study, the best orbit to use for a constellation will be the one whose inclination approaches the latitude of the most septentrional ground station. In this case, this translates in the 30° orbit. As previously discussed, one can expect an increase in performance with more orbital planes - especially regarding the maximum gap registered without an access for each ground station - but these configurations will be more costly.

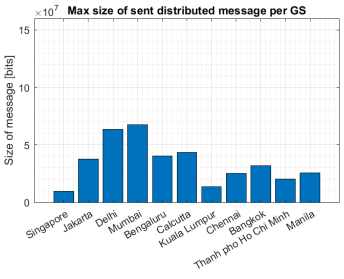
Results for Indo-ASEAN network					
Figure of merit		**SSO**	**30°**		
		1p/6s	**2p/3s**	**3p/2s**	**6p/1s**
Size	Mean size (Mbit)	34.44	66.55	66.55	66.49
	Min. size (Mbit)	9.6	15.56	15.18	15.01
Gap	Mean gap (hrs)	46.54	29.35	20.59	18.81
	Max gap (hrs)	46.54	56.53	21.70	19.45

Table 5.1: Results for the different downlink-only constellation configurations serving the Indo-ASEAN ground network

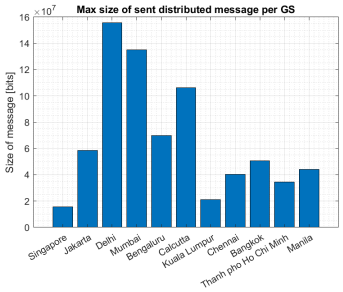
Results on Table 5.1 show how the SSO satellite constellation underperforms in terms of key size. This is due to the near-equatorial latitudes of this ground station network, that will benefit from orbits as close to null inclination as possible, as opposed to a SSO which is almost polar. Following the key size analysis, the three configurations studied with the 30° orbital planes offer the same performance. The variation of the values nicely agrees with the expected fluctuation due to the random calculation of the cloud coverage, quantitatively assessed in Section 4.3.

Regarding the maximum access gap for the different ground stations, it is clear how increasing the number of different orbital planes helps to lower this metric. If one were to choose a final configuration based on this analysis, the 3p/2s would be the wiser choice, as it virtually offers the same performance as the 6p/1s one, but at a lower cost.

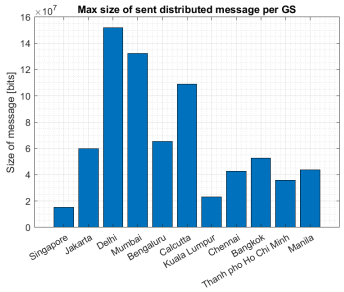
Cost has not been quantitatively analyzed in this work, but when comparing results it can act as a tie-breaker taking into account how deploying satellites in different orbital planes will always be more expensive than doing so in the same orbital plane.



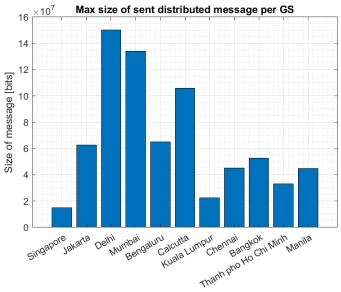
(a) SSO - 1p/6s



(b) 30° - 2p/3s

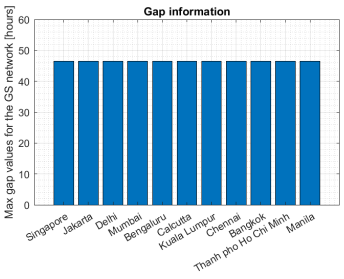


(c) 30° - 3p/2s

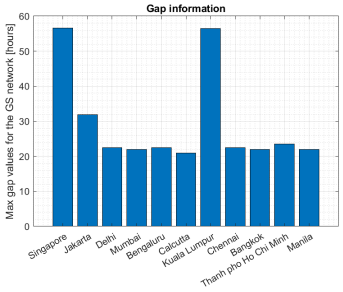


(d) 30° - 6p/1s

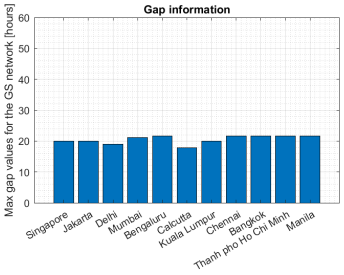
Figure 5.17: Summary of the key size obtained for the different cases for the Indo-ASEAN network



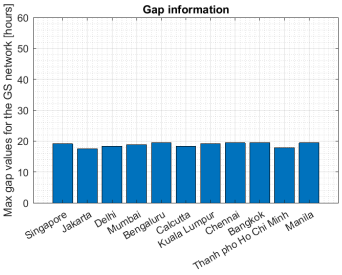
(a) SSO - 1p/6s



(b) 30° - 2p/3s



(c) 30° - 3p/2s



(d) 30° - 6p/1s

Figure 5.18: Summary of the maximum access gaps for the different cases for the Indo-ASEAN network

5.5.2. G20 results

The same type of graphs as the ones shown before are obtained for the G20 network. For the sake of conciseness, only the ones being used to compare between different constellations will be shown.

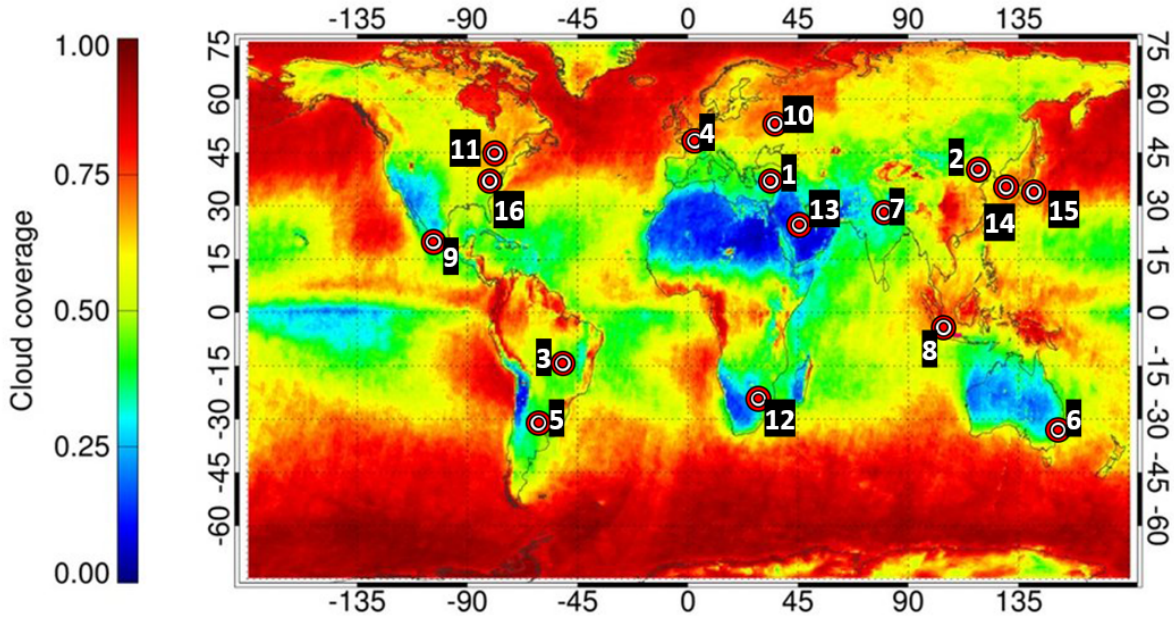


Figure 5.19: G20 ground stations on a cloud coverage map. Modified from Figure 4.7. The numbers refer to each city in the order shown in the result graphs

Again, Figure 4.7 gives an indication of the average cloud coverage for each ground station. It is easy to predict how ground station 13 - located in Riyadh - will perform the best in terms of key size. This is indeed true for every constellation studied, as can be seen in Figure 5.21.

The results for the maximum gap value shown in Table 5.2 do not take into account the figure obtained for Moscow. As it can also be seen in Figure 5.22, for every case Moscow has a dramatically larger maximum gap than the other ground stations. More precisely, this gap is one of 1248 hours, which equals 52 days. This anomaly happens due to the unfavourable situation of the satellites during the summer period. Earth's tilt will translate in the satellite not being covered by Earth's shadow when it flies over high-latitude ground stations, hence not registering valid passes during that time of the year. This is easily appreciated in Figure 5.20.

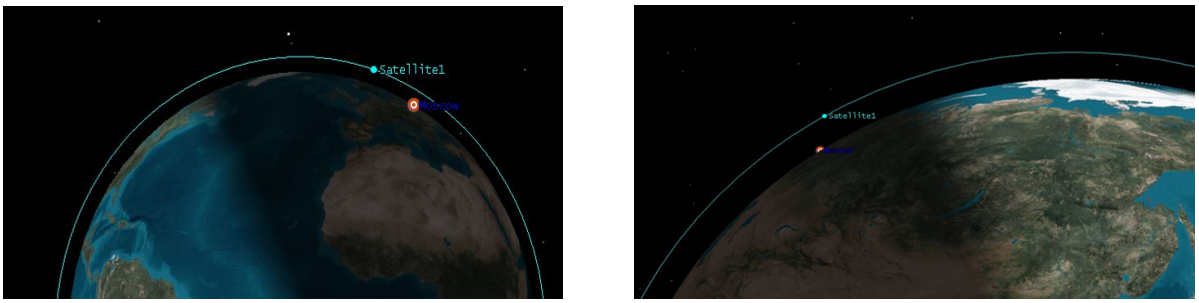
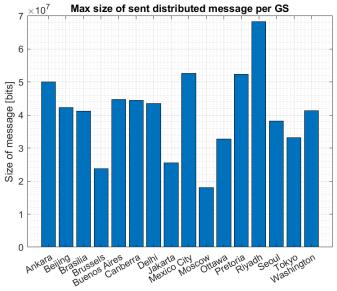


Figure 5.20: Moscow potential access in the winter (left) and in the summer (right)

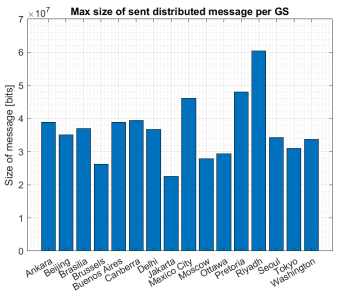
The results show how in this case, the SSO configuration performs slightly better than the different 60° ones in terms of key size. This is almost completely true as well for the maximum gap metric. The configuration 6p/1s shows a lower value for most ground stations when compared to the SSO one. This difference - and also the worst performance of Brussels, representing the centro-European region - might not justify the delta-cost associated with deploying the satellites in different orbital planes. Therefore, it seems that for a ground station network distributed around the globe, the best option will be to populate a *noon-midnight* SSO with the satellites of the constellation.

Results for G20 network					
FOM studied		SSO	60°		
		1p/6s	2p/3s	3p/2s	6p/1s
Size	Mean size (Mbit)	40.77	36.58	36.77	36.51
	Min. size (Mbit)	18.07	22.47	23.02	22.92
Gap	Mean gap (hrs)	45.03	188.14	65.82	29.24
	Max gap (hrs)	46.54	314	314	121.9

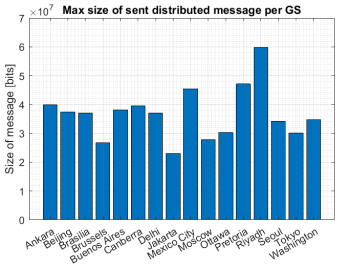
Table 5.2: Results for the different downlink-only constellation configurations serving the G20 ground network



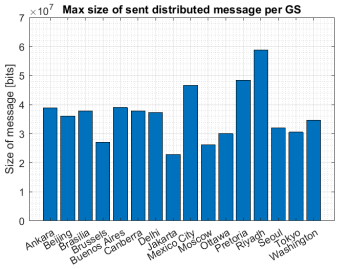
(a) SSO - 1p/6s



(b) 60° - 2p/3s

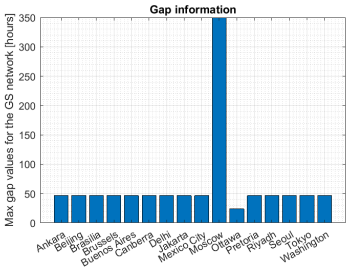


(c) 60° - 3p/2s

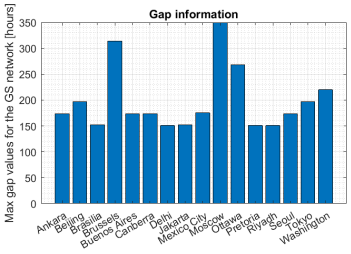


(d) 60° - 6p/1s

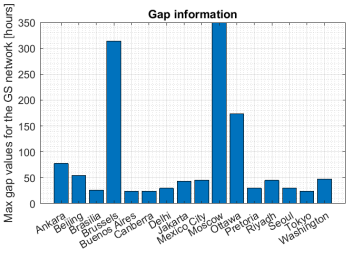
Figure 5.21: Summary of the key size obtained for the different cases for the G20 network



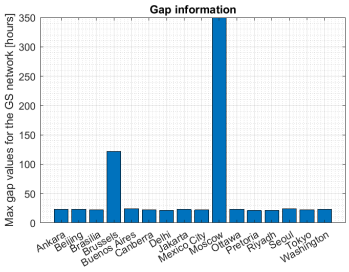
(a) SSO - 1p/6s



(b) 60° - 2p/3s



(c) 60° - 3p/2s



(d) 60° - 6p/1s

Figure 5.22: Summary of the the maximum access gaps for the different cases for the G20 network

6

Intersatellite link

6.1. ISL purpose

The purpose of ISL in a QKD constellation is not obvious. ISL is used in existing constellations usually to be able to deliver a service in real time, regardless of the users' location on ground. One could think this also applies for QKD, thinking of a hop-by-hop configuration in which two or more satellites connect distant ground stations. However this is not entirely true, because of the specific logistics of single-photon downlink QKD. Latency on the service provided in this case will depend on how fast a satellite, or a number of satellites, downlink the XOR of two ground stations keys to either one of them. The assumption of a GEO relay was made before, which drastically improves the latency. Furthermore, latency will not be considered a critical design driver since the foreseen applications are those that require a high level of security, bound to afford waiting a modest amount of time to obtain key. On top of this, the downlink of the XOR is done through a classical communication channel. Therefore, if a hop-by-hop architecture was devised between satellites to fulfill the purpose, no ISL QKD would actually be needed.

The parameters considered to assess the performance of each constellation are the key size and the revisit time, as commented previously. The revisit time between accesses cannot be changed via ISL. Therefore, key size should be the factor being improved. As explained in Section 3.4, it has to be understood that the key-exchange performance of a satellite cannot be solely measured looking at the keys it has exchanged with the different ground stations. Since the final goal of the QKD network is to share keys between two sites, when an excelling ground station wants to obtain key with any other ground node, it will be limited by its worse-performing counterpart.

A key-balancing strategy is therefore proposed in this work. If Sat_1 has exchanged a determined amount of key with every ground station except with GS_C, it will be helpful to get some of the key that adjacent Sat_2 has exchanged with GS_C and therefore increase the overall key that Sat_1 can deliver to two ground stations if GS_C is part of the ground nodes that wish to securely communicate. Security is to be kept in mind at all times, so the establishment of some initial guidelines is needed so security is not compromised for the sake of larger keys.

- Prior to the key exchange between two satellites, those satellites will have had to establish a QKD link between them, obtaining a secure key that allows them to encrypt the key that they are transferring.

- Since they key being sent will be duplicated, the key redistribution algorithm will be unidirectional. This means that Sat_1 will only give key to Sat_2, which will only give key to Sat_3, etc. This goes on until Sat_n which will only give key to Sat_1. Eventually an algorithm could be devised so the key being transferred is not retained in the sender satellite, but this would most probably translate in a minimal overall performance enhancement. It is considered that the proposed configuration has a minimal impact in security, if any at all.

6.2. Model

The key rate mathematical model needs to be updated to reflect the intersatellite scenario. From an environmental point of view, doing QKD between satellites will be beneficial for the key rate, since both the background noise and the atmospheric losses can usually be considered virtually null.

6.2.1. Inputs

Since the receiver is now on-board the satellite, a number of adjustments needs to be made. These adjustments will either decrease the keyrate or introduce technical/operational complexities in order to maintain a certain keyrate. To begin with, the diameter of the receiver will logically be smaller than the one used on ground. In this work the diameter used in the Micius satellite is assumed (30 cm) but this assumption will not be valid when considering smaller buses. A preliminary research of the commercially available technology will be shown in Section 6.5. Figure 6.1 shows the impact on the keyrate due to decreasing the diameter of the receiver.

Another crucial parameter is the rate of dark counts on the detector. Also shown in Figure 6.1, higher dark counts will translate in a heavily decreased keyrate. The rate of dark counts will be a function of the temperature of the detector. Therefore, cooling of this element will be needed for an acceptable ISL performance. This topic is discussed in Section 6.5.2.

Finally, not a technological but an operational constraint is added. The keyrate heavily depends on the distance between transmitter and receiver (see Figure 6.1). Therefore if the satellites need to exchange key between each other, they will have to spend a significant portion of their orbits within range from the satellites they are supposed to exchange key with. The key exchanged between satellites needs to be of a certain order of magnitude in order for ISL to be useful (see 6.3) so an additional constraint is added in the design of the constellations.

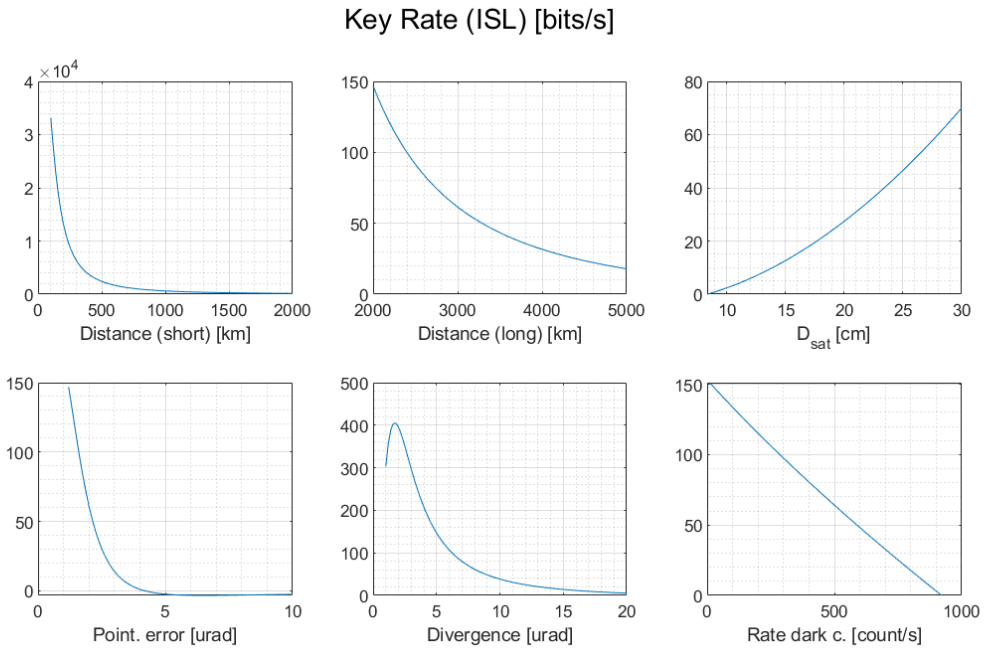


Figure 6.1: Figure 4.5, repeated for convenience. Sensitivity analysis results for the ISL scenario

6.2.2. Constellation design

Based on existing constellations, one can distinguish two different cases of ISL: *intraplanar* and *interplanar*. As the name suggest, in the intraplanar ISL the satellites establishing the link will be located in the same orbital plane. With the concept of operations proposed, in which the ISL is unidirectional, this configuration will end up looking like a "string of pearls". On the other hand, in the interplanar ISL the satellites will

be orbiting in different planes, which introduces additional complexity due to varying distances and angular accelerations. In this case, one satellite will be placed per orbital plane. This is the most advantageous configuration if considering interplanar ISL. Both options can be seen in Figure 6.2.

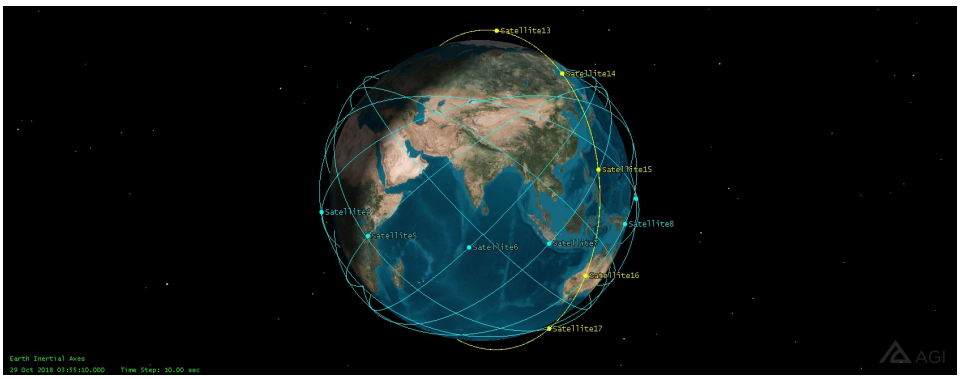


Figure 6.2: Generic case showing intraplanar (yellow) and interplanar (blue) ISL constellation configurations

6.2.3. Proposed algorithm

Figure 6.3 shows the different steps of the algorithm that defines how one satellite gives key to another satellite. The bar graphs correspond to the total amount of key these two satellites have available in order to communicate safely (top), the keys that the satellite acting as "giver" has exchanged with the ground nodes (left) and the keys that the satellite acting as "receiver" has exchanged with those same ground nodes (right).

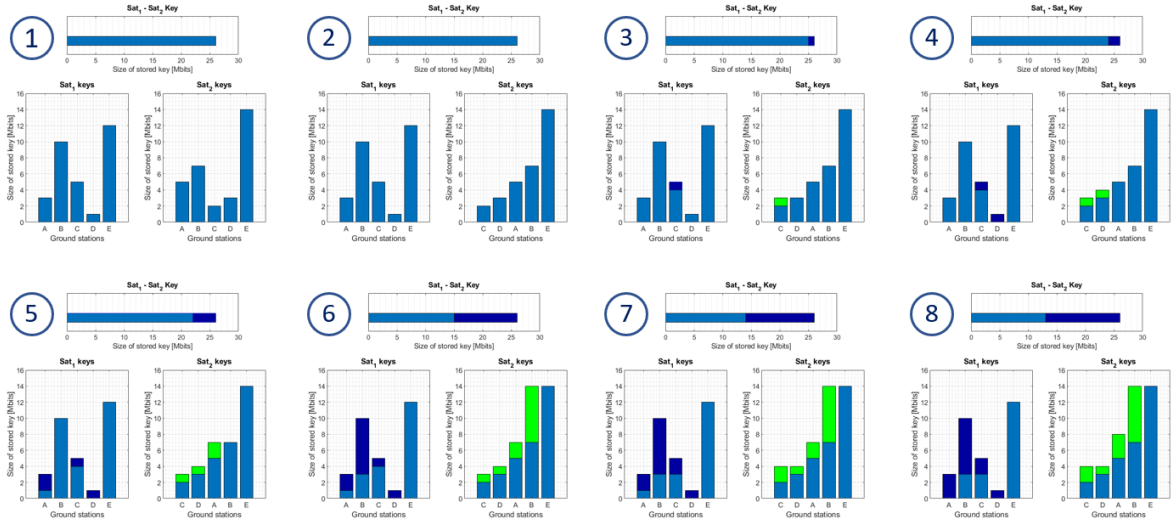


Figure 6.3: Step-by-step ISL key redistribution from Sat_1 to Sat_2. Dark-blue means key being sent from Sat_1 and key shared between both satellites being used. Green means key received by Sat_2.

The goal of the key redistribution will be to minimize the amount of key that is left unused when doing the XOR operation. Therefore, the ideal final situation would be for all the ground stations to have the same amount of key exchanged with the satellite - obviously, one will aim for making all of those key the same size as the largest one. First of all, they keys in the receiver satellite are sorted. Logically, the ground stations with less key will be prioritized. Then the first key exchange is planned: $K_C = 2$ Mbit will try to match $K_D = 3$ Mbit. Therefore, the receiver satellite requests the giver satellite to provide 1 Mbit of K_C. Once the request is made, two checks are done.

1. The two satellites must have enough common key to encrypt the key being transferred.
2. The giver satellite can only transfer as much key as it has.

In the example provided, K_{1-2} = 26 Mbit and $K_C|_{Sat_1}$ = 5 Mbit, therefore the 1 Mbit is successfully transferred to the Sat_2. In (3) this amount of key is colored in green for the receiver satellite and in dark blue for the giver satellite and the common key. From (3) to (4) the same logic is followed, now for the next pair of ground stations. In this case 2 Mbit are required for K_D equal K_A, but only 1 Mbit is available from Sat_1. The algorithm keeps running until the last pair (K_B with K_E) is reached. Then it starts again from the first pair, but now the last pair will be the one defined by K_A and K_B. The key exchange will proceed in this fashion until K_{1-2} is depleted, all the keys that Sat_1 has have been transferred, the ideal situation (all keys at Sat_2 equal to K_E) has been achieved, or the algorithm finishes it last loop when the last pair is set by K_C and K_D.

As it can be noted in this example, the last stopping criterion is the one that applies. It is the least optimal one since more key could be transferred, e.g. all of key C. However the implementation of this algorithm shows a robust increase in performance, and this example has been artificially generated to show its possible flaws.

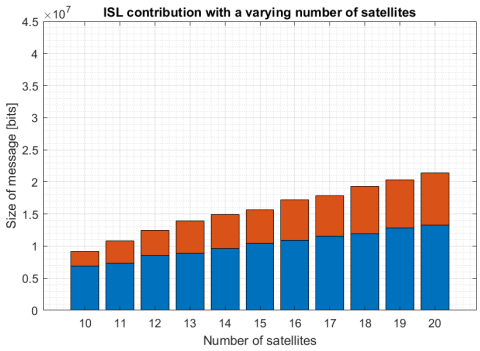
6.3. Number of satellites

For implementation of ISL in the two study cases a minimum numbr of satellites can be determined by considering the distance between them. The SSO provides the simplest case as the distance between satellites remains constant. For the other configurations, the satellites will always come closer at the bottom and top portions of their orbits. Running that preliminary SSO case yields a result of minimum 10 satellites needed for ISL.

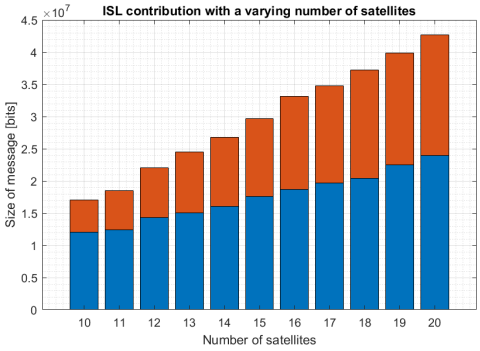
The algorithm described in Section 6.2.3 shows how ideally the end product of a successful key redistribution is for all the ground nodes to have the same key available as the best performing ground station. This will not be achieved with the minimum number of satellites required to begin this task, set at 10 satellites. However, due to the nature of this algorithm, one can predict a certain "law of diminishing returns", in which at some point adding more satellites to the constellation will barely yield any increase in performance.

To assess the increase in performance, the downlink-only performance will first be analyzed - based on the same FOM used until now -, and then the relative increase due to ISL key redistribution will be determined.

The four scenarios (G20 and Indo-ASEAN with intraplanar and interplanar ISL each) will be simulated, with a range of 10 to 20 satellites. These are the results obtained, shown in Figure 6.4 and Figure 6.5.



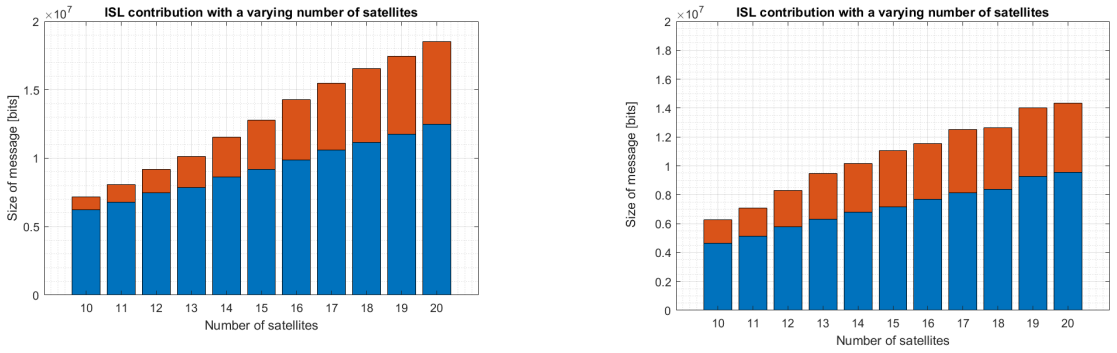
(a) SSO case



(b) 30° case

Figure 6.4: Downlink only (blue bars) and increase due to ISL key redistribution (additional red bars) for the Indo-ASEAN scenario with a varying number of satellites

One can see how the rate of increase of the red portion of the bar diminishes as the number of satellites is increased. To show it in a more clear way, Figure 6.6 presents the results obtained for the four cases, plotting in this case the relative improvement. The "diminishing returns" becomes in this case more clear: from 16 satellites on, the additional gains are less noticeable. In reality cost will be a constraint, while in the simulations, computational power represents the constraint. Introducing ISL dramatically increases the time of computation since a significant amount of additional accesses need to be processed. Therefore, a number of 16 satellites is chosen as representative to perform further analyses.



(a) SSO case **(b)** 60° case

Figure 6.5: Downlink only (blue bars) and increase due to ISL key redistribution (additional red bars) for the G20 scenario with a varying number of satellites

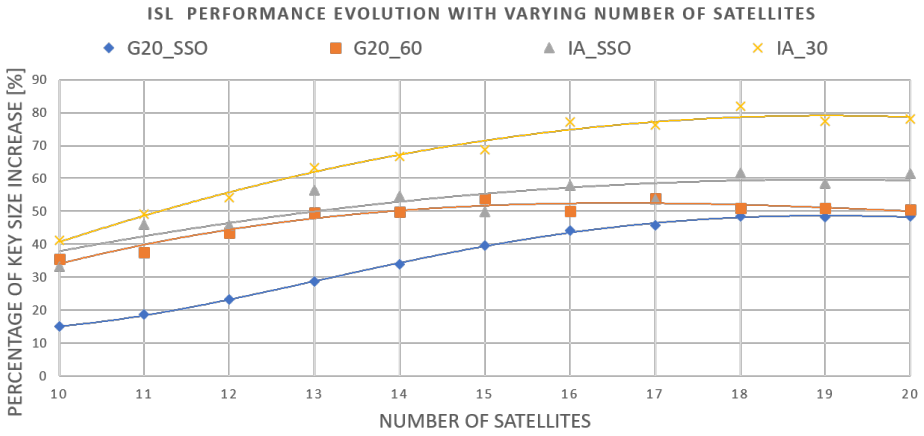


Figure 6.6: Improvement in key size FOM due to introducing ISL, as a function of the number of satellites in the constellation

6.4. Performance increase

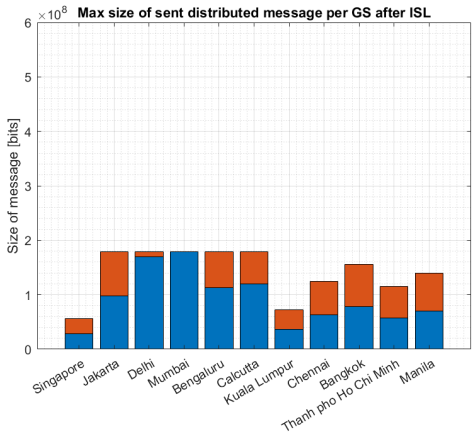
Yearlong simulations analogous to the ones run in the downlink-only scenario have been executed. The results regarding the key size are presented in the same format, now showing also the extra portion of key obtained thanks to the inclusion of ISL. Also the percentage of improvement per ground station is shown.

6.4.1. Indo-ASEAN ISL results

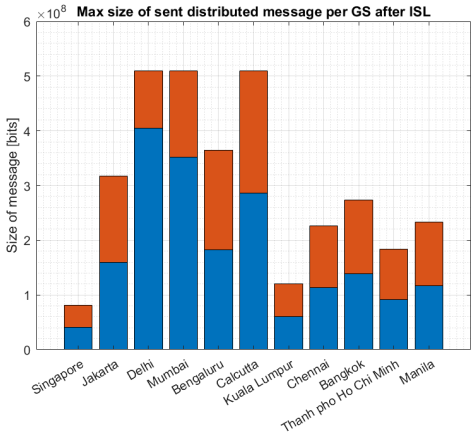
As previously stated, two cases have been run: the SSO case in which all satellites are placed in a noon-midnight orbital plane (1p/16s) and the 30° case in which each satellite is placed in its own orbital plane, with an angular phase of zero between them (16p/1s).

Results for Indo-ASEAN network			
FOM studied		**SSO**	**30°**
		1p/16s	**16p/1s**
Size	Downlink-only (Mbit)	92.1	177.0
	With ISL (Mbit)	141.7	302.5

Table 6.1: Results for the different constellation configurations serving the Indo-ASEAN ground network, with and without ISL

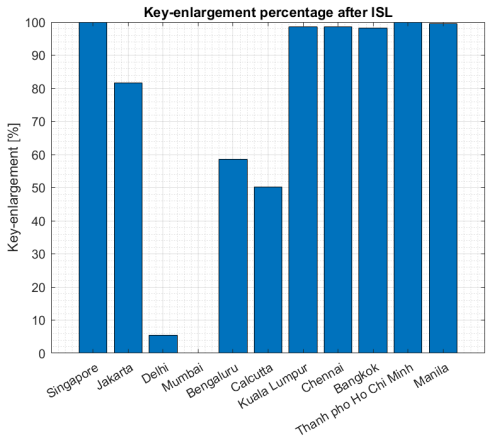


(a) SSO case - 1p/16s

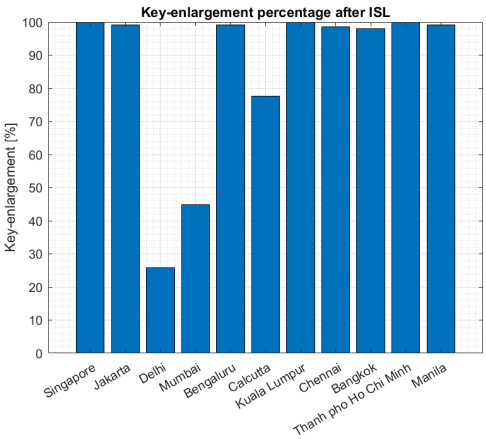


(b) 30° case - 16p/1s

Figure 6.7: Key size metric in the Indo-ASEAN network. The blue bars are the results of a downlink-only configuration while the red additional bars are the results once key redistribution via ISL has taken place



(a) SSO case - 1p/16s



(b) 30° case - 16p/1s

Figure 6.8: Relative key enlargement for each ground station of the Indo-ASEAN network after ISL key redistribution

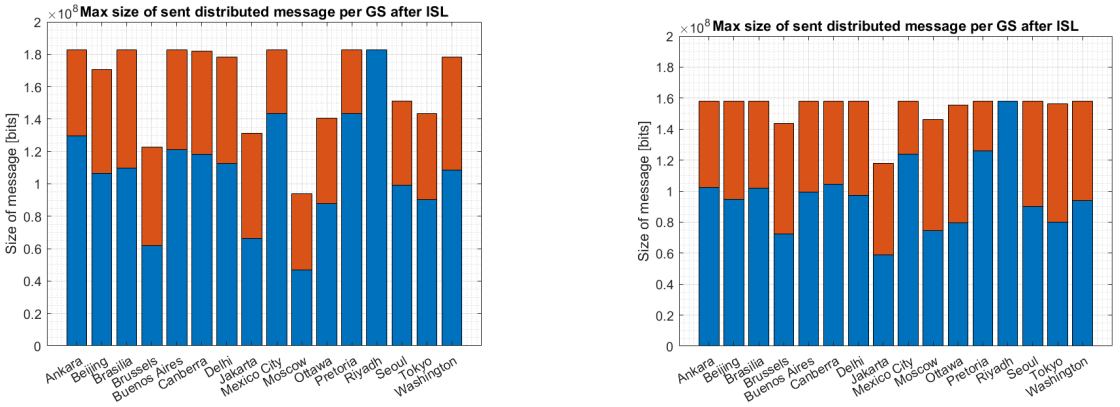
The design conclusion previously stated is here reaffirmed: a SSO design for a ground station network such as the Indo-ASEAN one is a poor choice. Even after the ISL redistribution of keys, the figure of merit obtained is lower than the one corresponding to the 30° configuration without ISL. Figure 6.7 does not seem to indicate a successful redistribution of the keys, especially in the 30° case. This is because this metric does not show the key obtained by each ground station, but the inter-connectivity between them. However in Figure 6.8 one can see that the algorithm indeed favors the worse-performing ground stations the most. As explained in Section 6.3, priority is given in the key redistribution to the ground stations with the least key.

6.4.2. G20 ISL results

The configurations analyzed are analogous to the ones seen in the Indo-ASEAN case. Table 6.2 sums up the obtained results.

Results for G20 network			
FOM studied		**SSO**	**60°**
		1p/16s	**16p/1s**
Size	Downlink only (Mbit)	108.02	97.32
	With ISL (Mbit)	161.84	153.54

Table 6.2: Results for the different constellation configurations serving the G20 ground network, with and without ISL



(a) SSO case - 1p/16s

(b) 60° case - 16p/1s

Figure 6.9: Key size metric in the G20 network. The blue bars are the results of a downlink-only configuration while the red additional bars are the results once key redistribution via ISL has taken place

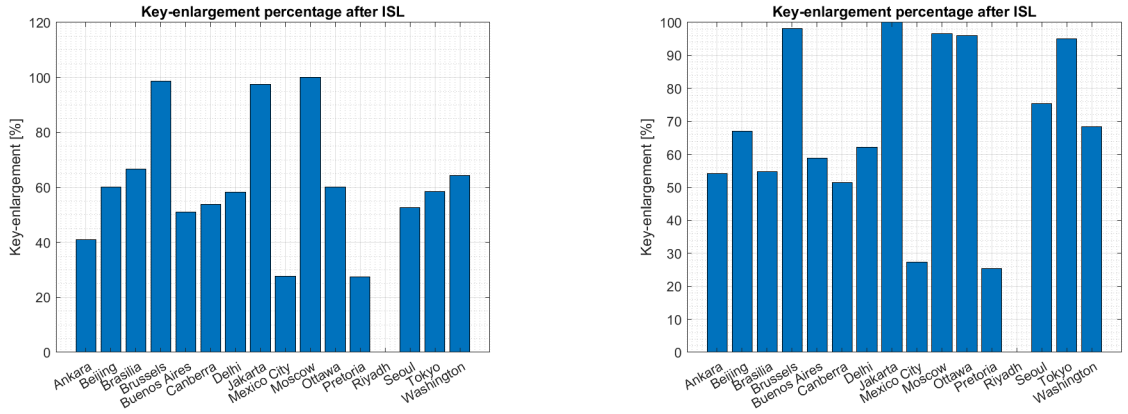
The SSO performs the best in this case, with a higher figure of merit than its counterpart. Figure 6.9 also suggests a more even result throughout the ground stations with the 60° constellation. Once more, in Figure 6.10 one can see how the worse performing ground stations are the ones receiving more key as end result, reaching the 100% increase in some cases.

6.4.3. Results discussion

The results obtained seem to agree with the proposed algorithm to redistribute key. There are however a few observations to be made that can be discussed upon.

Top-performing ground stations key-size increase

After analyzing both scenarios, one can see a considerable difference in the end result of implementing the proposed ISL key redistribution. It seems like the "balancing" effect is better achieved in the G20 constellations, while in the Indo-ASEAN scenario some of the best-performing ground stations FOM are further improved after implementing ISL, deviating from the initial intention. The explanation for this effect is the following. The FOM studied addresses the hypothetical case in which one ground station sends an OTP-encrypted message to all the other ones (e.g. a secret report sent to all member nations). Therefore, the key used will be equal to the key available over (n_{GS} -1). However they total key available by any other of those



(a) SSO case - 1p/16s

(b) 60° case - 16p/1s

Figure 6.10: Relative key enlargement for each ground station of the G20 network after ISL key redistribution

ground stations is less than the aforementioned quantity, that ground station will limit the size of the key used. In the G20 case, the difference between best and worse performing ground stations is not as great: therefore, when adding more key to the worse performing ground stations, their performance in terms of the FOM studied improves, but the performance of the best performing ground station (Riyadh in this case) does not because it was already able to use all its key. On the other hand, in the Indo-ASEAN case, some ground stations such as Singapore or Kuala Lumpur will limit the best performing ground stations. Therefore, when giving them more available key, the potential distributed message sent by the best performing ground stations will also be increased, explaining the increase in performance by these ground stations.

Cloud time correlation in SSO configuration

The SSO configuration is also known as a *string-of-pearls* configuration: the satellites are following each other. The algorithm proposed assumes that key is given only from Sat_i to Sat_{i+1}. Since the purpose is to redistribute key, it will be the most beneficial if the profile of keys between those two satellites is as different as possible. While the geometrical part of the problem is registered in this study, the cloud simulation does not properly account for the peculiarities of a string-of-pearls configuration. Especially true with a higher number of satellites, the access between Sat_i and GS_A will have a similar cloud coverage value as the one between Sat_{i+1} and GS_A. This time correlation is not implemented in the model, where the cloud coverage is computed randomly for each pass. However, because of the statistics used for the random computation, over a long-enough period of time, both Sat_i and Sat_{i+1} will have experienced, on average, the same cloud coverage when flying over GS_A. Therefore, while the cloud simulation strategy can be further improved, as discussed in Section 8.2, for this analysis the results obtained are considered valid.

6.5. Technology complexity increase

The purpose of this section is not to comprehensively go over the design of each satellite subsystem but to detect the key elements that will determine the ability of the spacecraft to be a functional node in the potential QKD constellation.

6.5.1. Attitude Control System

The attitude control subsystem will play a major role in the effectiveness of the QKD link. In a regular downlink scenario, pointing capabilities already greatly determine the keyrate obtained. But in an ISL case, attitude control becomes even more relevant as there will be an additional manoeuvring required to keep the QKD link with the neighbouring satellites. This is especially true in the case of interplanar ISL where the attitude control capabilities will be the most critical. The pointing requirements for an optically linked satellite system are computed in [9]. Configurations similar to the ones discussed in this thesis require a slew rate lower than 10deg/sec in the worst case scenario, as shown in Figure 6.11. This value, together with the pointing

capabilities taken as an input from the Micius satellite are achievable by the XACT-50 device developed by Blue Canyon Tech.

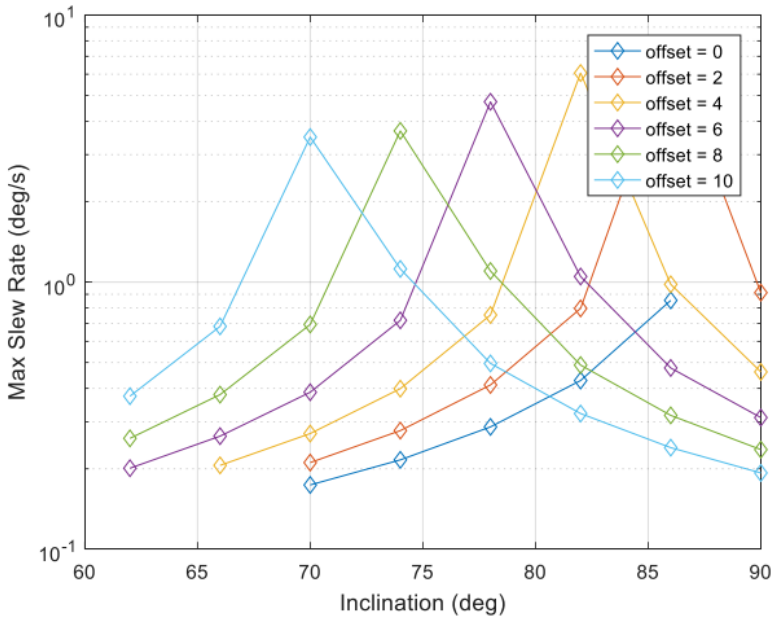


Figure 6.11: Peak slew rates for different inclination and true-anomaly offset configurations. Retrieved from [9]

6.5.2. Active cooling - ISL with receiver on board

In this thesis, a baseline downlink-only version of a satellite constellation is first studied. Then, ISL is introduced with the intention of improving the overall performance of the system. One of the hardware upgrades the satellite needs in order to be able to perform ISL is to incorporate a single photon detector - since in a downlink configuration and using a WCP source, there is no need for an on-board detector. Dark counts can severely affect the obtained keyrates, as seen on the sensitivity analysis in Section 4.2. These dark counts are inherent to the detector, and they are a direct function of the temperature. Dedicated thermal control for the detector will be needed; this topic shows a variety of approaches in literature. CQT proposes the inclusion of a thermoelectric cooler attached to the detector as part of its source of entangled photons, SPEQS, to bring it down to approx. -20°C [7] . This is a relatively rugged and power efficient solution, but it does increase the complexity of the system as well as its SWaP. For the Nanobob mission, with a 12U cubesat in an uplink configuration, no active cooling is said to be needed [18]. They rely on the heating of the detectors during daylight to 60-100°C, which has the annealing effect of later decreasing the dark counts, and then strategically placing the detector so it can be passively cooled via a radiator. Small heaters should be added to fine tune the operational temperature.

6.5.3. Telescope

Previous preliminary studies - such as the one presented in [33] - argue that it is possible to have a functioning QKD satellite in a downlink configuration using a 6U bus, with a rugged entangled-photon source such as SPEQS2. However when considering ISL, the receiving optics will heavily determine the key rate obtained. In the analyses carried on in this work, a receiving aperture of 30 cm has been considered. This was possible in the Micius satellite, which does not belong to the category of small satellites. Even with this value, the design of the constellations is severely constrained, so aperture dimensions much smaller than this one do not seem to be practical for QKD. There is therefore a need to use a larger bus than a 6U. There seem to be commercially available options for 12U satellites such as the one proposed by Apertureos, with a telescope based on a corrected Ritchey-Chrétien design, offering up to 25 cm in aperture for a 12U bus. Integration and further detailed analysis is out of the scope for this thesis, but as a conclusion it can be affirmed that a 12U satellite would be able to perform ISL QKD.

6.5.4. Overview

Though ISL introduces an additional complexity, it seems like most subsystems in a downlink-only configuration would already be capable of allowing ISL. If passive thermal control can be assumed, and an ACS of the characteristics of the XACT-50 is embarked to achieve the pointing capabilities assumed in this work, only a reasonably sized telescope needs to be added in order to achieve functional ISL.

7

Optimization

This chapter aims to provide an overview of the optimization process for the design of a QKD satellite constellation. The initial goal of the project was to design an optimal constellation to cover the Indo-ASEAN area, where the variable to be optimized was the number of satellites, and ultimately the cost. This goal has drifted towards a more academic, research-focused goal that addresses the wish to optimize the performance of the constellation with a fixed number of satellites. While optimization of satellite constellations is a topic widely discussed in literature, most research refers to continuous coverage, presumably motivated by commercial satellite constellations such as telecommunication ones where optimizing the configuration plays a major role. However, the problem studied in this thesis falls in the category of discontinuous coverage. To simplify the process and taking advantage of the fact that the model has been entirely developed in Matlab, the associated Optimization toolbox will be used.

From the optimization methods implemented in the toolbox, two are of interest for a problem such as the one presented here. These are non-gradient, stochastic methods: genetic algorithm (GA) and simulated annealing (SA). As shown in [8], thanks to these characteristics these two methods suit well the nature of the problem of a discontinuous-coverage satellite constellation. In their research, the goal is simply to minimize the maximum revisit time - not incidentally, one of the figures of merit used to assess the performance of the constellations throughout this thesis. The problem associated with these methods is how inefficient they are. They require a large number of function evaluations in order to achieve convergence. This proves to be especially true for the genetic algorithms since the number of function evaluations is not only equal to the iterations (generations) but that number times the members of the population. A detailed description of how each of these methods work is not needed, but Figure 7.1 shows the difference in function evaluations needed for convergence, where convergence is defined as a difference between the last two function evaluations smaller than a predefined tolerance value. It can be seen that for five satellites, GA reaches almost 25000 function evaluations while SA stays below 5000. Assuming that the simulations in this thesis had also five satellites - instead of six -, the approximate time needed for convergence based on this figure would be around 5000 hours for GA and 1000 hours for SA. This is based on an approximate run time of 20 minutes for a downlink-only six satellite configuration in the G20 scenario, during a year period. Given that 1000 hours translates to more than a month of non-stop optimization, this was not practicable with the resources available for this thesis.

7.1. Optimization goals

In these stochastic methods, a random initial input is used to generate the first guesses of the algorithm. Then, in one way or another, a random - but related to this first "seed" - set of variables will be evaluated, comparing it to the values obtained in the first function evaluation, and deciding to proceed in that direction or not depending on the inherent rules of the chosen method. In this case, the goal of implementing these optimization methods is not to come up with a totally new configuration, but to fine-tune the ones already found to perform better. More specifically, in the case of SA, the values of the variables explored will greatly depend on the seed given to the algorithm. The intention with this optimization process is therefore to feed

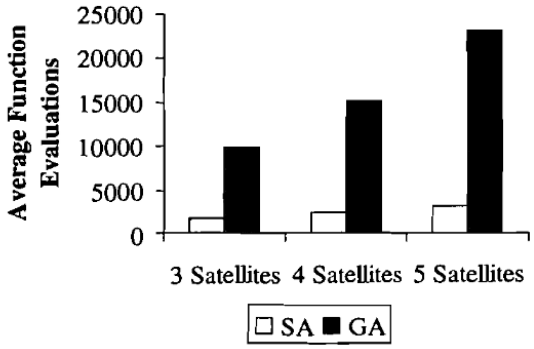


Figure 7.1: Function evaluations needed for convergence using both simulated annealing (SA) and genetic algorithm (GA) in a discontinuous, global coverage case. Retrieved from [8]

the optimization tool with a seed equal to the best-performing constellations found in Section 5.5 and obtain as a result a similar but better performing constellation.

7.2. Cost function

Ideally the cost function would gather the two figures of merit that have been used until now to assess the performance of each constellation. To keep the analysis simple, it has been decided to just optimize for key size, and then observe if the optimized configuration poses a problem in terms of maximum access gap for any ground nodes.

For easier interpretation of the function evaluations, the cost function will be defined simply as $\frac{FOM_{nom}}{FOM}$, where sought-after larger FOMs will lead to a decreased value of the cost function. FOMs refer to the figure of merit discussed throughout this thesis, and the nom subscript indicates the value of this parameter in the nominal case, used as a seed.

7.3. Variables

Since the goal is to achieve the best-performing constellation, the variables will be the orbital elements associated to the different satellites. Thanks to the assumptions made to simplify the design of the constellation, all satellites will have a common inclination and orbital height, greatly reducing the dimension of the variable vector. However one should leave the Ω and ν degrees of freedom to allow for configurations that deviate from a strict even distribution such as the one found in a Walker-Delta configuration. Good results have been achieved following this rationale in [8], where the output constellations outperformed the equivalent Walker-Delta options. To summarize, there will be 12 variables in the optimization process: orbit height and inclination, and then the Ω and ν value for each of the six satellites forming the constellation, except for one satellite that will be fixed at the values (Ω_1, ν_1) = (0,0).

7.4. Results

These are the results obtained for the two scenarios being discussed. An overview of the optimization settings is presented, together with the output of the optimization process and the results that the optimal configuration yields. For both cases the inputs for the Simulated Annealing optimization have been set as the default ones proposed by the Toolbox except for the stop criterion, where a maximum of a hundred iterations has been set due to time/processing power constraints.

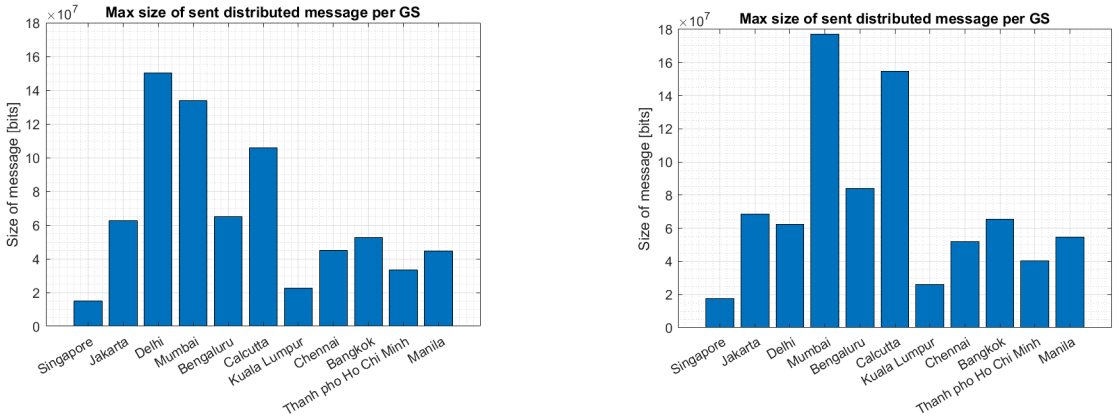
7.4.1. Indo-ASEAN case

The seed values are the ones corresponding to the 30° configuration, which showed the best performance. After running the optimization, the proposed configuration has an objective function value equal to 0.903. This means that the studied FOM is 10.7% larger in the obtained configuration. Table 7.1 shows the values of the variables before and after the optimization, together with the fixed boundaries established. The main interest resides in the longitude of the ascending node and the true anomaly, where interesting configurations that deviate from an even distribution can be found.

Optimization variables			
	Initial	Boundaries	Result
h [km]	400	[390 - 450]	440.799
i [deg]	30	[25 - 45]	25
Ω_2 [deg]	60	[0 - 359]	6.714
Ω_3 [deg]	120	[0 - 359]	107.833
Ω_4 [deg]	180	[0 - 359]	153.371
Ω_5 [deg]	240	[0 - 359]	214.828
Ω_6 [deg]	300	[0 - 359]	323.777
ν_2 [deg]	0	[0 - 359]	41.202
ν_3 [deg]	0	[0 - 359]	53.948
ν_4 [deg]	0	[0 - 359]	23.671
ν_5 [deg]	0	[0 - 359]	6.054
ν_6 [deg]	0	[0 - 359]	5.472

Table 7.1: Variables subject to the optimization process. Initial, boundary and final values shown for the Indo-ASEAN case.

While the FOM has been increased, it is needed to check whether all the ground stations of the network are still performing well at an individual level. Figure 7.2 shows how the major impact has been a loss in keysize by Delhi while Calcutta and Mumbai have increased their value. This is probably due to the value of inclination being lowered, which heavily benefits the two latter ground stations, and in general results advantageous for the rest of the near-equatorial locations. Contrary to intuition, the final configuration has a higher altitude than the initial one. Finally, Figure 7.3 shows how some cities now have a slight increase in their maximum access gap. For most of the ground stations this figure barely varies, hence considering the new configuration a valid improvement with respect to the "traditional" one presented before.



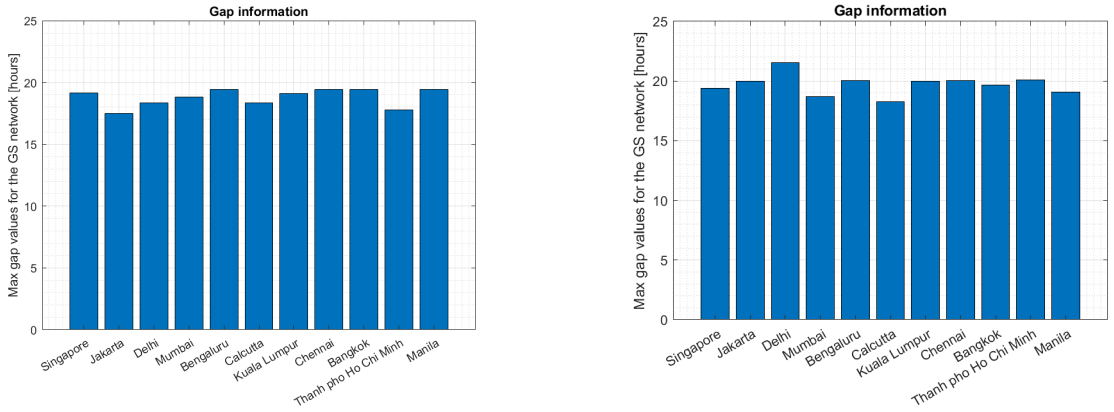
(a) 30° case - before optimization

(b) 30° case - after optimization

Figure 7.2: Key size performance metric per ground station, before (left) and after (right) the optimization process

7.4.2. G20 case

For the G20 case, an analogous process is carried out. In this case, the seed is the SSO configuration, which showed the best performance in this scenario. Table 7.2 shows in this case how the result of the optimization



(a) 30° case - before optimization

(b) 30° case - after optimization

Figure 7.3: Maximum access gap per ground station, before (left) and after (right) the optimization process

is the same configuration as the initial one. In principle, it can be expected that the specific combination in which all the satellites are located in a noon-midnight SSO is indeed the best one for this scenario. A potentially better configuration could have a lower altitude and the appropriate inclination to make it sun-synchronous, but probably that exact configuration has not been explored in this limited optimization analysis. Therefore, the conclusion is this case is straightforward, leaving the initial SSO configuration as the best-performing, even after the modest optimization that has been run.

Optimization variables			
	Initial	Boundaries	Result
h [km]	400	[390 - 450]	400
i [deg]	97.0347	[90 - 110]	97.0347
Ω_2 [deg]	0	[0 - 359]	0
Ω_3 [deg]	0	[0 - 359]	0
Ω_4 [deg]	0	[0 - 359]	0
Ω_5 [deg]	0	[0 - 359]	0
Ω_6 [deg]	0	[0 - 359]	0
ν_2 [deg]	60	[0 - 359]	60
ν_3 [deg]	120	[0 - 359]	120
ν_4 [deg]	180	[0 - 359]	180
ν_5 [deg]	240	[0 - 359]	240
ν_6 [deg]	300	[0 - 359]	300

Table 7.2: Variables subject to the optimization process. Initial, boundary and final values shown for the G20 case.

8

Conclusions and future work

8.1. Conclusions

This thesis constitutes a stepping stone towards the development of trusted-node satellite QKD constellations in the near future. Throughout this document the answers to the research questions initially proposed in Section 1.2 have been given or reflected upon. This final chapter collects them all together in an organized fashion.

QKD operations and technology choice

Compared to currently used public-key encryption, QKD provides a totally secure way to distribute a symmetric key between two parties. Due to high losses via optical fibre and the curvature of the Earth, the only way to deliver a key to nodes located far away is via satellite QKD.
There are several ways to establish a QKD link between a satellite and a ground station: downlink, uplink, reflection and downlink of two entangled photons. Reflection would imply great operational complexity and high losses for a constellation. Downlinking two entangled photons has the advantage of not having to consider the satellite as a trusted node, but the losses are doubled, and the satellite will only be able to deliver key to cities located simultaneously under its field of view. Uplink shows the advantage of not having to place a source on board, reducing complexity. However the keyrates obtained are lower when compared to a downlink configuration, mainly due to the *shower curtain* effect. Due to miniaturized entangled-photon sources being a reality at the moment – like SPEQS, developed at CQT – in this work a downlink configuration is chosen due to the higher keyrates obtained. With the purpose of maximizing keyrate, a WCP source is assumed, using a BB84 protocol. The detector limits the performance of the QKD system. Due to the current state of the art and the TRL of the different technologies, a Si-APD is assumed, together with a wavelength of 848.6nm. Though there is ongoing research to achieve successful QKD in daylight, the current technology to achieve practical keyrates from space implies that QKD will only be done when both satellite and ground station are in eclipse.
The operational concept of the constellation is therefore as follows: the satellites will exchange key via QKD with the ground stations whenever they have the chance to do so. This will build up a buffer of keys on board of each satellite. Whenever two ground stations want to obtain key to communicate securely with each other, the satellite will downlink to either one of them the result of the XOR operation of both keys exchanged. This last step is not considered in the simulation: one can assume that the downlink of the XOR operation result is just done whenever the satellite flies again over one of the two ground nodes. Since this step is done via a classical communication channel, if needed to minimize latency one can assume a relay between the satellites of the constellation or potentially a relay using existing GEO satellites. The last option is assumed in this work, though it is not relevant for the analyses carried out.

Ground stations

The ground stations should have a large enough aperture to guarantee sufficient keyrate. Furthermore, locations with low cloud coverage and low light pollution are preferred to host ground stations. Ideally these

ground stations will then be connected to the urban area nearby via optical fibre, distributing the key as needed. This work focuses on the space segment of the network, but one can see how a future global QKD network will also be comprised of these smaller fibre networks interconnecting urban areas.
Two scenarios have been proposed to analyze the constellation design using the model. The G20 case is formed by the capital cities of the countries belonging to this group (with Brussels taken as capital of Europe). This results in a set of cities that are bound to be potential customers of a QKD service in the near future. Furthermore, it is a global case where the cities are diverse both in location and climate. On the other hand, the Indo-ASEAN network has cities belonging both to India and southeast Asia. This is also a representative case that could be soon implemented due to its strategic nature. For this work, it is an interesting case since the cities are clustered around the equatorial region. Some ground stations severely suffer from cloud coverage, and two pairs of cities (Singapore/Kuala Lumpur and Bangalore/Chennai) are located so close together that the satellite will need to choose one of the two to do QKD with. The model dictates that the satellite will do QKD with the least cloudy city in the moment of the pass.

Matlab/STK model

Creating a model to simulate the QKD constellation has not only been a means to an end. In the end, it has constituted a research goal in itself. The model has been developed using MATLAB and STK integrated together. STK is used to compute the accesses between the different nodes, being able to set the desired conditions to do so such as the eclipse constraint, or the minimum elevation angle required, set at 20° in this work derived from literature. This information is then sent to MATLAB where different scripts compute the cloud coverage of each location and the keyrate of each pass. The result is the key size exchanged in each pass. The cloud coverage simulation is crucial to obtain realistic values. These values are derived from historical data from the last ten years and it is implemented with a granularity of 0.1 degrees, which translates in approximately 10 km, depending on the latitude of the location. The model has been validated with the results published by the QUESS mission, successfully recreating the key exchange process by the Micius satellite. Given that the theoretical model does not gather additional pass-dependent sources of keyrate loss, the results are slightly optimistic.
A sensitivity analysis has been run on the model. As part of the research conducted, intersatellite QKD has also been included in the model. The sensitivity analysis results are presented both for the downlink and the ISL scenario. The dependence of the keyrate with the distance between the two parties will be a constraint to design both downlink and ISL-capable constellations. Regarding the bus and the technology used, a large-enough receiver and low-enough dark counts have to be guaranteed. While these conditions are relatively easy to achieve on ground, they will be design drivers for the satellite in the ISL case. For the simulations shown in this thesis, the QUESS mission data was used as input.

Constellation design

For the constellation design, the guidelines established by existing Earth-orbiting constellations are followed. In all these constellations cost is an obvious driver. While cost has not been quantitatively analyzed in this thesis, it has been kept in mind throughout the different design choices. For example, the constellations are comprised of six satellites. Cost-wise, this is approximately equivalent to one Micius-sized satellite, and this number offers good versatility for the different constellation configurations. Also, all the satellites are identical. The constellations are formed by circular orbits: this is motivated by overall simplicity, since the distances between satellites and ground stations are constant. Again, for simplicity, all orbital planes have the same height and inclination. Different, more exotic configurations would require an additional orbital maintenance effort with no apparent increase in performance.
For both scenarios an orbital height of 400 km has been chosen. Based on a preliminary study, a 12U bus is deemed enough to embark a functional QKD source. Taking its ballistic coefficient into account, this orbital height offers an acceptable lifetime. On-board propulsion can be considered to further extend it, with an extensive range of options for cubesats in the market. With the current technology only a LEO constellation is considered to offer an acceptable key delivery service, due to the distance constraint.
The choice of the inclination value depends on the ground station network. The inclination has to be at least equal to the value of the latitude of the most septentrional ground station. A calculation on the exact value is presented in this work. The Sun-synchronous orbit represents a specific value of the inclination for which the orbital plane's attitude towards the Sun remains unchanged throughout the year. This property makes it attractive for QKD purposes as one can choose a *noon-midnight* orbit where the eclipse time is maximized

over a year and a steady stream of accesses is guaranteed. Around 97° for a 400 km orbit, its almost polar configuration makes it particularly suited for a global network with distributed cities across the world (a common constellation design is the Walker-Star one, formed by several polar orbits). However, it does underperform for low-latitude locations. This is why the lowest-possible inclination for each ground network has also been studied.
Regarding the orbital plane distribution, for the SSO it makes the most sense to locate all the satellites in the same orbital plane, the one corresponding to the *noon-midnight* configuration. This not only fully takes advantage of the favorable eclipse conditions, but it is also potentially cheaper due to lower deployment cost. The other inclinations (60° and 30° for the G20 and Indo-ASEAN case respectively) have been studied with different configurations: 2, 3 and 6 orbital planes. One orbital plane is discarded since at some point in time the orbital plane will be in an unfavorable attitude towards the Sun, where the satellites will barely experience any eclipse time.

Performance evaluation

To assess the performance of the constellations, two aspects have been taken into account. These are considered to effectively describe the usefulness of each constellation for a QKD service. The first one addresses they key size exchanged. However just evaluating the key size exchanged between satellites and ground stations ignores the interconnectivity dimension. As the end goal is to share key between two ground stations and the key delivered is limited by the underperforming ground station – due to the XOR operation – an additional management of the keys is done. The amount of key that each ground station can share with all the other ground nodes of the network is computed. Then, the mean value will provide a valid factor of merit to assess the key size available related to each constellation.
Furthermore, it is considered an advantage, from the point of view of maximizing security, to obtain recently generated key as opposed to key that has been stored for a longer time. Therefore, the maximum time gap between accesses is determined for each ground station. An average value will be obtained for the network, the lower the better. Evaluating this factor has brought up an issue with ground stations with a very high latitude. Due to Earth's tilt, when the satellite approaches these ground stations during the summer it will not be in eclipse. This is true for the case of Moscow, not being able to do QKD for 52 days.

Applied cases results

Results obtained for both scenarios encompass a series of lessons learnt. The SSO configuration performs the best in the G20 case in terms of keysize. The three configurations formed by 60° orbital planes obtain an equal final keysize value. This is due to the J_2 effects averaging out throughout the course of several months - all these simulations cover a period of a year. The value is not identical, due to the randomness associated to the cloud simulation. In a separated study this variability has been computed for these yearlong simulations, being equal to approximately ± 0.4 Mbit. As expected, opposite results are obtained for the Indo-ASEAN scenario, as these low-latitude ground stations benefit from lower inclination orbits. The maximum gap study shows how increasing the number of orbital planes improves this factor of merit. This is true to the extent of showing a lower average value for the six-plane orbital configuration when compared to the SSO configuration in the G20 case, though northern areas will still be better covered with the SSO. In the Indo-ASEAN case, both the three and the six plane configurations offer the best values, almost identical. With these results, it is safe to say that the best configuration for the G20 case is the one with the six satellites evenly distributed throughout a *noon-midnight* SSO while the best configuration for the Indo-ASEAN case is the one with three orbital planes, which performs virtually the same as the one with six planes but will have a lower cost. The detailed results for both scenarios can be found in Appendix C.

Intersatellite link

Intersatellite link has also been considered in the model. It introduces new challenges: constellation design constraints due to the need of the satellites to be closer together to effectively do QKD and added technological complexity. The optical aperture value in the simulation is taken from the Micius satellite, equal to 30cm. Though large for a CubeSat, there are commercial options available of 25cm of aperture for a 12U. Regarding dark counts, recent literature argues that passive thermal control could be enough to keep dark counts to a low enough level. CubeSat attitude control systems are also commercially available to provide the control

needed to perform interplanar links, more challenging than intraplanar ones due to varying distances and angular accelerations. The purpose of QKD ISL has been identified to redistribute keys between satellites to achieve a better overall performance of the constellation. It will not reduce latency as this parameter is determined by how fast the XOR result is downlinked via a RF channel. An algorithm has been designed that favors the worst-performing ground stations and minimizes the times that the key is shared between satellites. An analysis has been run showing the relative increase in performance of the constellation varying its number of satellites. Thanks to this analysis a law of diminishing returns has been found. This fact together with the wish to minimize the number of satellites used leads to a number of 16 satellites to form the ISL QKD constellations. Analyses for both ground station networks and both intraplanar and interplanar QKD have been run. The results are analogous to the ones obtained in the downlink-only scenario when it comes to choosing a configuration for each one of the scenarios. However intraplanar ISL will be favored due to a significant decreased complexity, thanks to constant distances between satellites and lack of angular accelerations between them. It can be concluded that ISL does indeed increase the performance of the QKD constellation, with the major impact being the constellation design constraint.

Optimization

As a final note, an optimization process is proposed to further improve the design of the constellation. Matlab's Optimization Toolbox has been used for this purpose. Stochastic optimization methods are used in literature for satellite constellations. While most research focuses in Genetic Algorithms, some authors address Simulated Annealing with similar or better results and far less function evaluations. Due to processing power and time constraints for this thesis, an optimization process using the Simulated Annealing method has been run. The goal of fine-tuning the best-performing constellation to provide global QKD service is met in both cases.

8.2. Future work

This model has been developed from scratch, therefore presenting copious future work opportunities. The proposed tasks follow both a further research drive - to characterize in a better way the QKD link - and a commercial interest - mainly focused in introducing the cost variable into both the design and the optimization process.

- Cloud coverage model. As discussed in the intraplanar ISL, the cloud model could be improved in a per-pass fashion. If two satellites pass over the same area within a certain period of time, the model should correlate those passes, creating similar cloud conditions for both of them. This is however a difficult task since the characteristic time of cloud coverage is not constant or uniform. Ideally, real time prediction would be implemented. This would be especially attractive for commercial purposes. If real time cloud prediction is added to the model, then accurate real time predictions of QKD links can be performed with the model presented in this thesis.

- Conflicting passes. As of today, the satellite behaviour is set to be quite simple when confronted with simultaneous access opportunities to several ground stations: it will just choose the least cloudy one, and completely disregard the other one. However, there could be potential scenarios in which the satellite would be able to perform partial accesses with both ground stations, (maybe) obtaining more key than if one of the ground stations was ignored. Ideally this could be analytically determined, quantifying the time needed for the satellite to switch the optical link from one ground station to the other one, and establishing certain rules of thumb as conclusions (e.g. redirecting will be possible with a certain minimum distance between the ground stations).

- ISL algorithm development. The algorithm developed to redistribute keys between satellites for the ISL case is fairly simple. The goal for the frame of this thesis was to develop a robust algorithm that would consistently show an increase on the overall performance of the constellation. However, stringent conditions have been applied such as one-way key exchange. There could be more complex algorithms to redistribute key between satellites, in order to optimize the ISL QKD behaviour.

- GUI further development. The GUI has been developed for an easy execution of the main cases analyzed in this thesis. It has been created using the Matlab in-built app tool, and it only shows the user the very basic input options of the model. A more complete and user friendly GUI can be developed to make the model accessible to a wider user base.
- Optimization. A first attempt on optimizing the QKD constellation has been made. However, time constraints have made it impossible to complete a full optimization analysis (both because of computing power and licensing issues). Therefore, an optimization study is recommended to properly assess the best configuration for a given set of ground nodes.
- Cost optimization. One of the main drivers of developing a QKD satellite constellation is its commercialization. This is the reason why cost will become a decisive factor when designing commercial QKD constellations. Cost should be in the future quantitatively assessed for QKD-capable satellites, as well as the expected revenue from a service of these characteristics. The optimization studies can also include cost as a variable, potentially leading to the determination of the needed number of satellites for a given ground station network.

A

Keyrate model

A.1. Link losses

In the downlink scenario, the total losses are computed as the sum of the transmission loss, free space loss and pointing loss.

The first step is the computation of the beam parameters, making use of the Gaussian beam theory. The waist of the beam at zero distance of the transmitter is a function of the wavelength and the divergence of the telescope:

$$w_{0_{down}} = \frac{\lambda}{\pi div} \tag{A.1}$$

A.1.1. Transmission losses

Transmission losses are due to the beam crossing the atmosphere. They are computed from the knowledge of their value at the closest approach of the satellite to the ground station (ϵ = 90 deg) which is divided by the sine of the elevation angle for each Δt. An extinction coefficient between 0 and 1 is additionally defined as a function of the transmission loss.

$$ext_{coeff} = 1 - 10^{L_{trans}/10} \tag{A.2}$$

A.1.2. Free space losses

Free space losses are a function of the beam itself, characterized by its beam waist and the diameter of the receiver's telescope. The distance between transmitter and receiver will also play a role, allowing to determine the width of the beam at the receiver. The beam waist (w_0) for Micius is determined from a known value of the telescope divergence. If computed using Gaussian beam theory, the divergence would be determined by the telescope diameter.

$$L_{fs} = 10 * log_{10}(1 - e^{-\frac{D_r}{w_d}}) \tag{A.3}$$

Where D_r is the diameter of the receiver telescope and w_d is the width of the beam at the receiver.

A.1.3. Pointing losses

Pointing losses take into account the pointing error (known value for both satellites and ground stations) as well as the divergence of the telescope and the diameter of the receiver telescope. There will be pointing losses concerning the transmitter as well as the receiver (satellite and ground stations respectively in the case of a downlink). The resulting value of the losses is normalized with respect to zero pointing error.

A.2. Noise

The next step is to calculate the the noise being received. In the case of the downlink, the noise on the detector is due to photons in the background and dark counts intrinsic to the detector.

A.2.1. Background noise

QKD is assumed to be performed only during nighttime and when the satellite is in eclipse. Therefore, the only photons creating noise are the ones due to artificial lightning, i.e. light pollution (and Moon and astronomical light – like the Milky Way). This will be determined by the light pollution in the region of the receiver, and the diameter and FOV of the receiver telescope.

$$Rate_{background} = \frac{\lambda}{hc} Sky_{Br} \pi^2 FOV_r^2 R_r^2 \tag{A.4}$$

Where SkyBr is the local value of the night sky brightness, FOV_r is the field of view of the receiver and R_r is the radius of the receiver telescope. The dark counts are a given value for APDs and they depend on the temperature of the detector.

A.3. QKD protocol

Lastly, after taking into account losses and noise, one should consider which protocol is using to generate key. A WCP source with the BB84 protocol will be described as it is the case studied in this thesis.

A.3.1. WCP with BB84 protocol

First of all, a transmittance value is defined as a function of the total losses already computed and including the values of the detector efficiency and the optical efficiency of the receiver optics.

$$\tau = 10^{\frac{Losses}{10}} \epsilon_{det} \epsilon_{opt} \tag{A.5}$$

The sifted key - term commonly used in QKD - will be the half product of this transmittance and the frequency of signal states (μ). This last term is equal to the fraction of photons being emitted that are part of the signal, the other ones being part of the decoy.

To calculate the gain of the signal state, both the noise and the transmittance are considered. The noise term is the probability of a background noise count, defined as the product of the noise rate previously calculated times the detection window time (t_{gate}).

$$Gain_{S.S.} = Rate_{noise} t_{gate} + (1 - e^{-\tau\mu}) \tag{A.6}$$

With these terms, the QBER of the signal state can be computed. The final keyrate is finally computed as a function of the previously computed values, source parameters and protocol values:

$$KeyRate = f(f_{DSP}, \mu, \nu, q, fE, Gain_{S.S}, QBER) \tag{A.7}$$

Where f_{DSP} is the source frequency, μ, ν, q and fE are parameters related to the protocol (signal state, decoy state, basis reconciliacion factor and error correction efficiency in the Cascade protocol respectively) and $Gain_{S.S}$ and $QBER$ have been computed previously.

B

Input values

```
 % Atmosphere
L_tr_down_0 = 3.2;                          % loss at closest approach downlink [dB]

% Downlink QKD
lambda_down = 848.6E-9;                              % downlink signal wavelength [m]
D_t_down = 0.3;                          % downlink transmitting telescope diameter [m]
D_r_down = 1;                             % downlink receiving telescope diameter [m]
Point_error_sat = 1.2E-6;                                    % pointing error [rad]
div_down = 5E-6;                          % divergence of cassegrain telescope [rad]

% Receiver optics
filter_width = 3;                                    % bandpass filter width [nm]
eff_optical = 0.16;
FOV_r = 130E-6/2;                                        % field of view receiver
bandpass_ratio = filter_width/400;
SkyBr = 0.4E-9 * bandpass_ratio;                     % sky brightness [W/cm^2/sr]

% Weak-coherent pulse source
f_DSP = 100E6;                                          % source frequency [Hz]
pulse_width = 0.2E-9;                                     % pulse width max [s]
mu = 0.8;                                          % signal state photon number []
v = 0.1;                                           % decoy state photon number []
f_mu = f_DSP*0.5;                                                  of signal states
f_v = f_DSP*0.25;                                    % frequency of decoy states
j_scl = 0.529E-9;                                    % in-orbit clock jitter [s]

% Ground station detector
j_total = 0.63E-9;                                                % total jitter [s]
j_dc = 0.35E-9;                                    % detector timing jitter [s]
t_dead = 1E-7;                                        % detector dead time [s]
eff_dc = 0.5;                                                % detector efficiency
e_0 = 0.5;                          % probability of noise count giving an error
e_d = 0.01;                         % probability photon hits erroneous detector
R_darkc = 25;                                    % rate of dark counts [count/s]
t_gate_WCP = 2E-9;                                          % detection window [s]

% Key extraction and privacy amplification
q = 0.5;                                                % basis reconciliation factor
fE = 1.4742;                       % error correction efficiency Cascade protocol
```

C

Results of chosen configurations

The detailed results in terms of key exchanged between each satellite and each ground station are presented in this appendix.

C.1. Downlink-only

These are the results obtained for the proposed constellations in a downlink-only configuration, both for the Indo-ASEAN network (Figure C.1) and for the G20 network (Figure C.2).

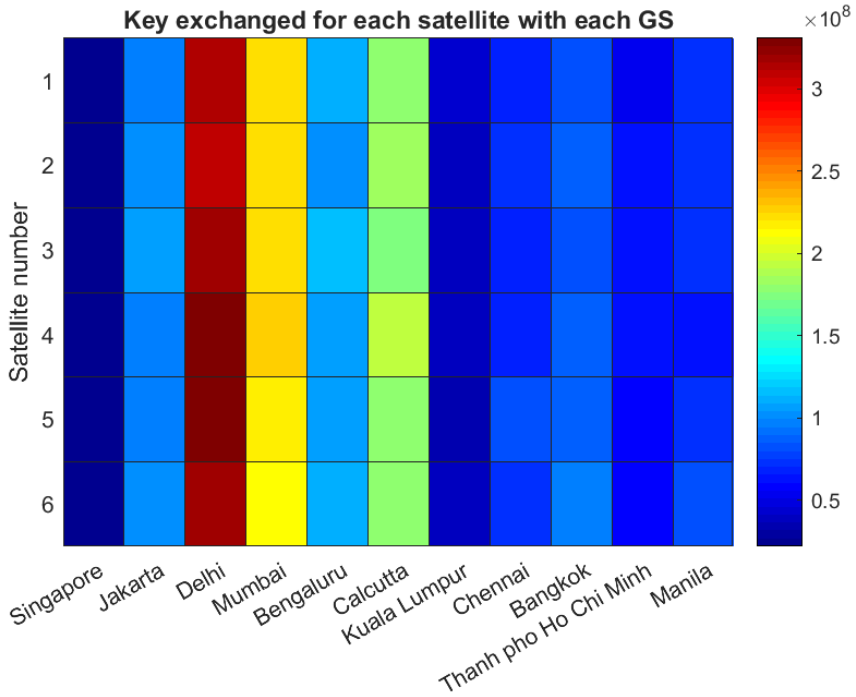


Figure C.1: Heatmap showing the key exchanged (bits) between each satellite/GS pair for the Indo-ASEAN network in a 30° 3p/2s downlink-only configuration, for a yearlong period

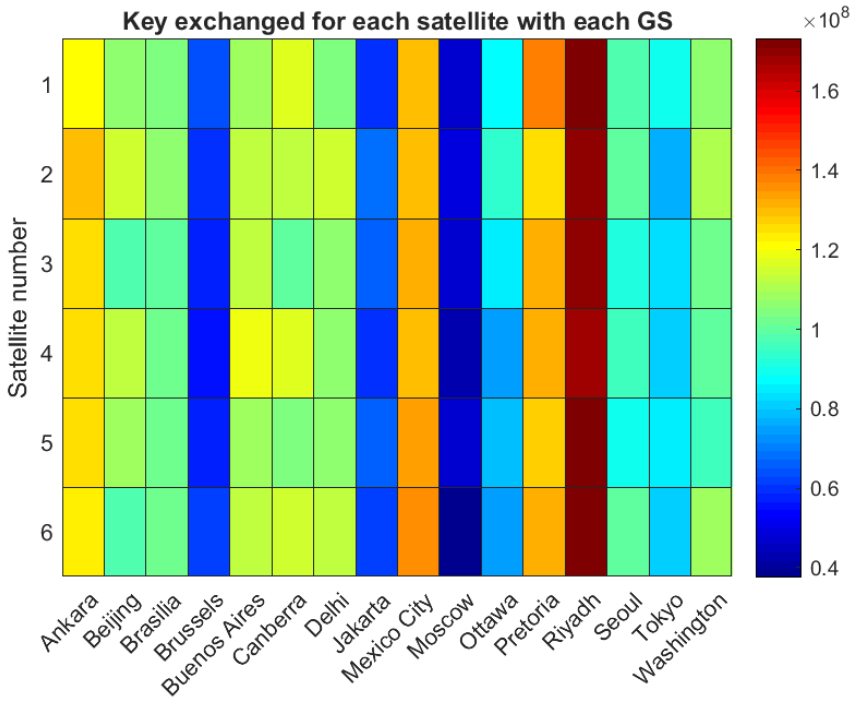


Figure C.2: Heatmap showing the key exchanged (bits) between each satellite/GS pair for the G20 network in a SSO 1p/6s downlink-only configuration, for a yearlong period

C.2. Intersatellite link

These are the results obtained for the proposed constellations in an ISL configuration, both for the Indo-ASEAN network (Figure C.3) and for the G20 network (Figure C.4).

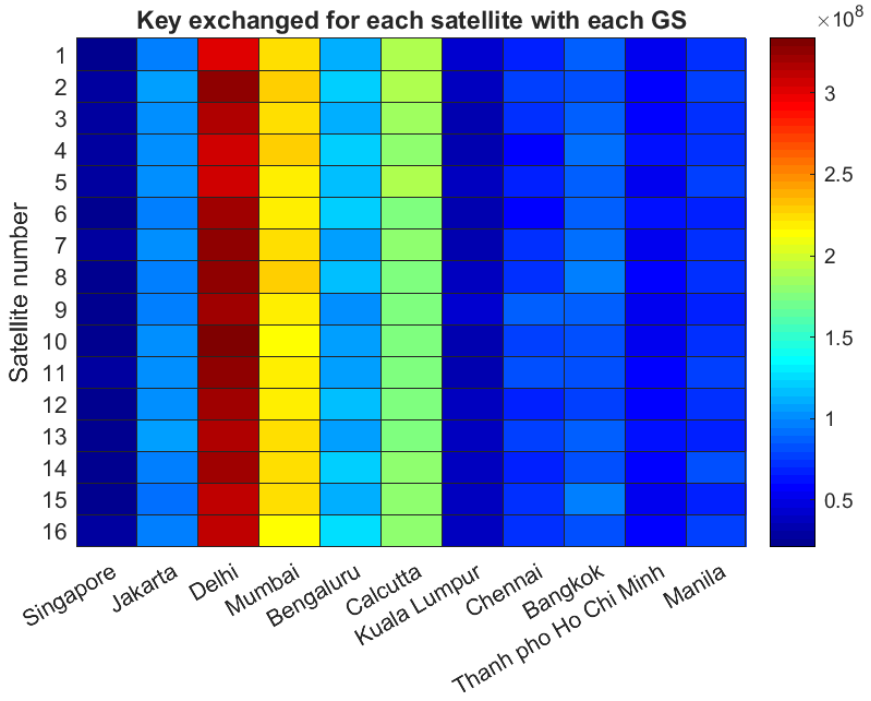


Figure C.3: Heatmap showing the key exchanged (bits) between each satellite/GS pair for the Indo-ASEAN network in a 30° 16p/1s ISL configuration, for a yearlong period

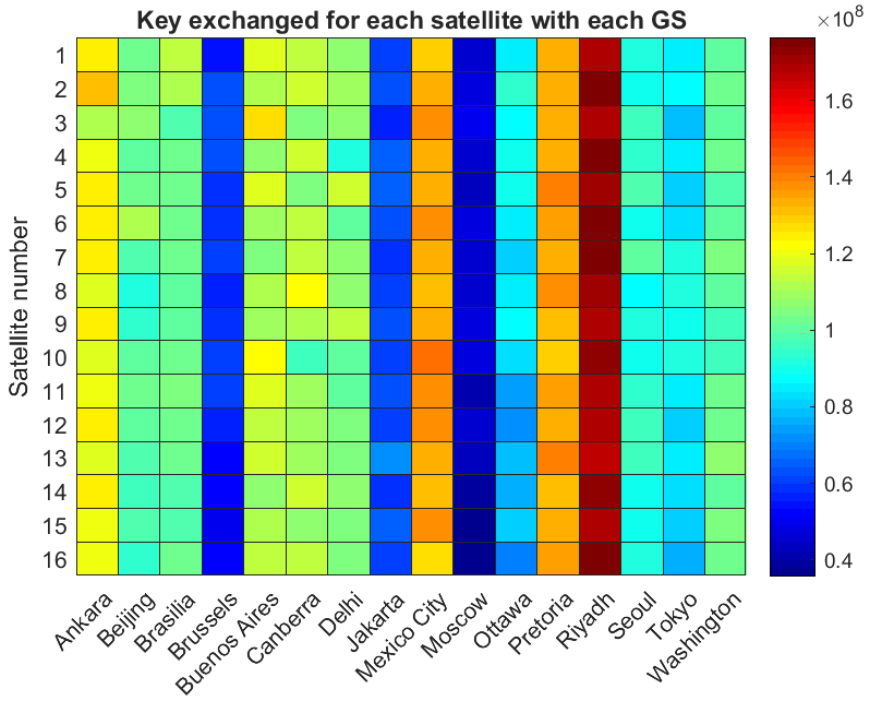


Figure C.4: Heatmap showing the key exchanged (bits) between each satellite/GS pair for the G20 network in a SSO 1p/16s ISL configuration, for a yearlong period

Bibliography

[1] Nadia Al-Saidi. Information security based nano and bio-cryptography. 05 2014.

[2] Robert Bedington, Tang Zhongkan, Rakhitha Chandrasekara, Cliff Cheng, Tan Yue Chuan, Kadir Durak, Aitor Villa Zafra, Edward Truong-cao, Alexander Ling, and Daniel Oi. Small Photon Entangling Quantum Systems (SPEQS) enabling space-based quantum key distribution. *Proceedings of the International Astronautical Congress*, pages 1–7, 2015. ISSN 00741795.

[3] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, (July):1–12, 2017. ISSN 2056-6387. doi: 10.1038/s41534-017-0031-5. URL http://arxiv.org/abs/1707.03613{%}0Ahttp://dx.doi.org/10.1038/s41534-017-0031-5.

[4] Daniel J Bernstein, Nadia Heninger, Paul Lou, and Luke Valenta. Post-quantum RSA. 2017.

[5] J-P Bourgoin, E Meyer-Scott, B L Higgins, B Helou, C Erven, H Hübel, B Kumar, D Hudson, I DSouza, R Girard, R Laflamme, and T Jennewein. Corrigendum: A comprehensive design and performance analysis of low Earth orbit satellite quantum communication (2013 New J. Phys. 15 023006). *New Journal of Physics*, 16(6):069502, 2014. ISSN 1367-2630. doi: 10.1088/1367-2630/16/6/069502. URL http://stacks.iop.org/1367-2630/16/i=6/a=069502?key=crossref.1aa19be2222fbfc55b45b5d0556ced3a.

[6] Gilles Brassard and Louis Salvail. Secret-Key Reconciliation by Public Discussion. pages 1–19, 1994.

[7] CQT. Private conversation with cqt staff.

[8] William A. Crossley and Edwin A. Williams. Simulated annealing and genetic algorithm approaches for discontinuous coverage satellite constellation design. *Engineering Optimization*, 32(3):353–371, 2000. ISSN 0305215X. doi: 10.1080/03052150008941304.

[9] Trevor A Dahl and Prof Brian C Gunter. An Evaluation of Spacecraft Pointing Requirements for Optically Linked Satellite Systems AE 8900 MS Special Problems Report Space Systems Design Lab (SSDL) Guggenheim School of Aerospace Engineering Georgia Institute of Technology Author : Advisor : An . 2017.

[10] ESA. Space for our climate - cloud cover. URL http://www.esa.int/Our_Activities/Observing_the_Earth/Space_for_our_climate/Highlights/Cloud_cover. Accessed: 06-11-2018.

[11] ESA. Space photons bring a new dimension to cryptography, may 2018. URL https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Space_photons_bring_a_new_dimension_to_cryptography.

[12] Centre for Quantum Technologies. About cqt, 2017. https://www.quantumlah.org/page/page.php?key=whatwedo, Last accessed on 2018-04-26.

[13] Y. Fun Hu, Gérard Maral, and Erina Ferro. Satellite Constellation Design for Network Interconnection Using Non-Geo Satellites. *Service Efficient Network Interconnection via Satellite*, 8, 2002.

[14] Johannes Handsteiner, Dominik Rauch, David Bricher, Thomas Scheidl, and Anton Zeilinger. Quantum key distribution at space scale. *2015 IEEE International Conference on Space Optical Systems and Applications, ICSOS 2015*, pages 1–3, 2016. doi: 10.1109/ICSOS.2015.7425062.

[15] Induced. Cover image 2 - highspeedsat satellite communication satellite. URL http://induced.info/?s=HighSpeedSat++Satellite+Communication++Satellite. Accessed: 06-09-2018.

[16] P.V Ingole and M.K Nichat. Landmark Based Shortest Path Detection by Using A* and Haversine Formula. *GH Raisoni College of Engineering and ...*, 1(2):298–302, 2013. doi: 10.1.1.300.5943. URL http://www.ijircce.com/upload/2013/april/17{_}V1204030{_}Landmark{_}H.pdf.

[17] T. Jennewein, C. Grant, E. Choi, C. Pugh, C. Holloway, JP. Bourgoin, H. Hakima, B. Higgins, and R. Zee. The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite. (September):925402, 2014. ISSN 1996756X. doi: 10.1117/12.2067548. URL http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2067548.

[18] Erik Kerstel, Arnaud Gardelein, Mathieu Barthelemy, and The Csug Team. Nanobob : A Cubesat Mission Concept For Quantum Communication Experiments In An Uplink Configuration. *arXiv*, (November): 1–37, 2017.

[19] Imran Khan. Satellite-based qkd. 010504(January):1–4, 2018.

[20] Andrew Lance and John Leiseboer. Quantum Key Distribution Systems Compared. (December):1–7, 2014.

[21] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 2017. ISSN 0028-0836. doi: 10.1038/nature23655. URL http://www.nature.com/doifinder/10.1038/nature23655.

[22] Sheng Kai Liao, Jin Lin, Ji Gang Ren, Wei Yue Liu, Jia Qiang, Juan Yin, Yang Li, Qi Shen, Liang Zhang, Xue Feng Liang, Hai Lin Yong, Feng Zhi Li, Ya Yun Yin, Yuan Cao, Wen Qi Cai, Wen Zhuo Zhang, Jian Jun Jia, Jin Cai Wu, Xiao Wen Chen, Shan Cong Zhang, Xiao Jun Jiang, Jian Feng Wang, Yong Mei Huang, Qiang Wang, Lu Ma, Li Li, Ge Sheng Pan, Qiang Zhang, Yu Ao Chen, Chao Yang Lu, Nai Le Liu, Xiongfeng Ma, Rong Shu, Cheng Zhi Peng, Jian Yu Wang, and Jian Wei Pan. Space-to-Ground Quantum Key Distribution Using a Small-Sized Payload on Tiangong-2 Space Lab. *Chinese Physics Letters*, 34(9), 2017. ISSN 17413540. doi: 10.1088/0256-307X/34/9/090302.

[23] Sheng Kai Liao, Hai Lin Yong, Chang Liu, Guo Liang Shentu, Dong Dong Li, Jin Lin, Hui Dai, Shuang Qiang Zhao, Bo Li, Jian Yu Guan, Wei Chen, Yun Hong Gong, Yang Li, Ze Hong Lin, Ge Sheng Pan, Jason S Pelc, M M Fejer, Wen Zhuo Zhang, Wei Yue Liu, Juan Yin, Ji Gang Ren, Xiang Bin Wang, Qiang Zhang, Cheng Zhi Peng, and Jian Wei Pan. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11(8):509–513, 2017. ISSN 17494893. doi: 10.1038/nphoton.2017.116.

[24] Sheng Kai Liao, Wen Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji Gang Ren, Wei Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng Zhi Li, Jian Feng Wang, Yong Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai Le Liu, Franz Koidl, Peiyuan Wang, Yu Ao Chen, Xiang Bin Wang, Michael Steindorfer, Georg Kirchner, Chao Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng Zhi Peng, Jian Yu Wang, Anton Zeilinger, and Jian Wei Pan. Satellite-Relayed Intercontinental Quantum Network. *Physical Review Letters*, 120(3):30501, 2018. ISSN 10797114. doi: 10.1103/PhysRevLett.120.030501. URL https://doi.org/10.1103/PhysRevLett.120.030501.

[25] SSL2BUY LLC. Symmetric vs. asymmetric encryption – what are differences? URL https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. Accessed: 16-12-2018.

[26] Hoi-kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy State Quantum Key Distribution. 230504(September 2004):15–18, 2005. doi: 10.1103/PhysRevLett.94.230504.

[27] X. Ma, B. Qi, Y. Zhao, and H. K. Lo. Practical Decoy State for Quantum Key Distribution. pages 1–15, 2005. ISSN 1050-2947. doi: 10.1103/PhysRevA.72.012326. URL http://arxiv.org/abs/quant-ph/0503005{%}0Ahttp://dx.doi.org/10.1103/PhysRevA.72.012326.

[28] Alfred J. Menezes, Jonathan Katz, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. 1996. ISBN 9788578110796. doi: 10.1017/CBO9781107415324.004.

[29] Daniele Mortari, Mp Wilkins, and Christian Bruccoleri. On Sun-Synchronous Orbits and Associated Constellations. *Paper of the 6-th Dynamics ...*, (January), 2004. URL http://mortari.tamu.edu/Flower-Constellations/MSSO.

[30] Sreeja Nag, Jacqueline LeMoigne, and Olivier de Weck. Cost and risk analysis of small satellite constellations for earth observation. *2014 IEEE Aerospace Conference*, pages 1–16, 2014. ISSN 1095323X. doi: 10.1109/AERO.2014.6836396. URL http://ieeexplore.ieee.org/document/6836396/.

[31] NASA. Cloud fraction (1 month - terra/modis). URL https://neo.sci.gsfc.nasa.gov/view.php?datasetId=MODAL2_M_CLD_FR. Accessed: 30-07-2018.

[32] Daniel K.L. Oi, Alex Ling, James A. Grieve, Thomas Jennewein, Aline N. Dinkelaker, and Markus Krutzik. Nanosatellites for quantum science and technology. *Contemporary Physics*, 58(1):25–52, 2017. ISSN 13665812. doi: 10.1080/00107514.2016.1235150. URL http://dx.doi.org/10.1080/00107514.2016.1235150.

[33] Daniel KL Oi, Alex Ling, Giuseppe Vallone, Paolo Villoresi, Steve Greenland, Emma Kerr, Malcolm Macdonald, Harald Weinfurter, Hans Kuiper, Edoardo Charbon, and Rupert Ursin. CubeSat quantum communications mission. *EPJ Quantum Technol.*, pages 1–20, 2017. ISSN 2196-0763. doi: 10.1140/epjqt/s40507-017-0060-1. URL http://dx.doi.org/10.1140/epjqt/s40507-017-0060-1http://arxiv.org/abs/1704.08707{%}0Ahttp://dx.doi.org/10.1140/epjqt/s40507-017-0060-1.

[34] Earth Observation Portal. Cubesat - deployer standards. URL https://directory.eoportal.org/web/eoportal/home. Accessed: 30-10-2018.

[35] Ji-gang Ren, Ping Xu, Hai-lin Yong, Liang Zhang, and Sheng-kai Liao. Ground-to-satellite quantum teleportation. *arXiv:1707.00934 [quant-ph]*, 2017. ISSN 0028-0836. doi: 10.1038/nature23675.

[36] Diane Roussel-Dupre. *Constellation Study for Optimized Target Access and Coverage*. PhD thesis, 2012.

[37] M Ruggieri, M De Sanctis, T Rossi, M Lucente, D Mortari, and Bruccoleri C. The Flower Constellation Set and its Possible Applications. 31(05-4108), 2006.

[38] Tobias Schmitt-Manderbach, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Henning Weier, Martin Fu, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. 010504(January):1–4, 2007. doi: 10.1103/PhysRevLett.98.010504.

[39] SemiElectronics. Cover image 1 - merits of hardware cryptography over software cryptography. URL https://semielectronics.com/merits-hardware-cryptography-software-cryptography/. Accessed: 06-09-2018.

[40] Gustavus J Simmons and Gustavus J Simmons. Symmetric and Asymmetric Encryption. 11(4), 1979.

[41] Hideki Takenaka, Alberto Carrasco Casado, and Mikio Fujiwara. Satellite - to - ground quantum communication using a 50 - kg - class micro - satellite. 2017.

[42] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental Satellite Quantum Communications. *Physical Review Letters*, 115(4):1–5, 2015. ISSN 10797114. doi: 10.1103/PhysRevLett.115.040502.

[43] Karel F. Wakker. *Fundamentals of Astrodynamics*. 1971. ISBN 0486600610. URL http://books.google.com/books?hl=en{&}lr={&}id=UtJK8cetqGkC{&}oi=fnd{&}pg=PR5{&}dq=FUNDAMENTALS+OF+ASTRODYNAMICS{&}ots=WB9rR9G1qc{&}sig=NnGuQtTUyWRsYRLwUMLa5l0Q2Sg.

[44] JR Wertz and Wiley J Larson. *Space Mission Analysis and Design, Space Technology Library*. Microcosm Press and Kluwer Academic Publishers, El Segundo, CA, USA,, 1999.

[45] Chao Yang, Hongqi Zhang, and Jinhai Su. The QKD network: model and routing scheme. *Journal of Modern Optics*, 64(21):2350–2362, 2017. ISSN 13623044. doi: 10.1080/09500340.2017.1360956. URL https://doi.org/10.1080/09500340.2017.1360956.