

UNIVERSITÀ DEGLI STUDI DI PADOVA

CISAS, Centro di Ateneo di Studi e Attività Spaziali
"GIUSEPPE COLOMBO" (CISAS)
Corso di Dottorato in Scienze Tecnologie e Misure Spaziali
Indirizzo: Astronautica e Scienze da Satellite, ASS
CICLO XXVI

BEAM PROPAGATION IN QUANTUM COMMUNICATION

Direttore del Corso di Dottorato: Ch.mo Prof. Giampiero Naletto

Coordinatore d'indirizzo: Ch.mo Prof. Giampiero Naletto

Supervisore: Ch.mo Prof. Giampiero Naletto

Co-Supervisore: Ch.mo Prof. Paolo Villoresi

Dottorando: Francesca Gerlin

Alla mia famiglia

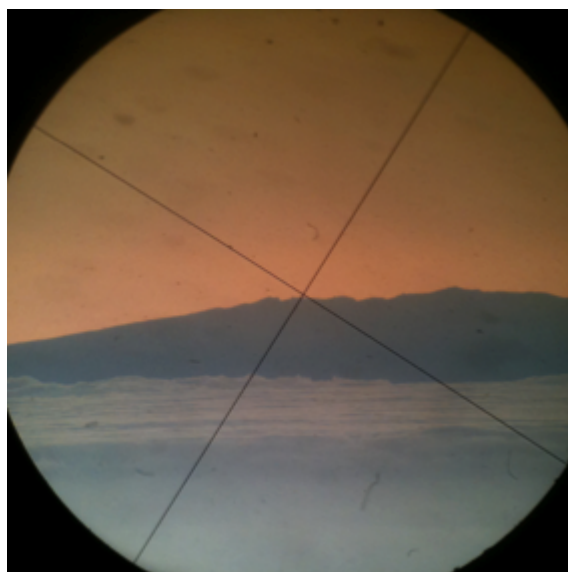


Figure 1: OGS secondary
At OGS secondary telescope (Izana, Tenerife), pointing JKT observatory in La Palma (Canary Islands)

Introduction

Quantum Mechanics has over hundred years of life. Since its introduction, its technological innovations are expected to lead to large-scale applications in the transmission field, making Quantum Communication (the art of sending quantum states from a place to an other) a fundamental topic of studies and researches.

Historically, Quantum Communication has been a test bed for the investigation of Quantum Mechanics properties (EPR paradox: the apparent violation of the classical principles of realism and location) [6].

Only after years, the researchers understood the potential of this new approach of Modern Physics in different fields of inquiry, such as Quantum Information (manipulation and transmission of the information employing quantum effects and Quantum Communication implies the transmission of Quantum Information) [64], Quantum Teleporting (the transfer of a quantum state at a point arbitrary far) [7], and Quantum Cryptography.

Quantum cryptography is one of the outstanding fields, promising absolute secure transmission of the key codes between two terminals according defined protocols (Quantum Key Distribution, with the development of protocols BB84, B92, Decoy state QKD,..), analyzing the information sent by a quantum channel: making use of the laws of Quantum Mechanics (no cloning theorem) the presence of an eavesdropper is detected with low error probability ensuring the security of shared keys. [74] [9] [8] [57].

Following the new quantum techniques reached in the laboratories -with favorable boundary conditions regarding the synchronization between transmitter and receiver and the reduced noise-, at the end of last century some scientists tried to bring their experiments outside of the laboratories, in the difficult outdoor conditions [16] [53] . In general, with the current technology, present optical fibers and free space are believed not faithful channels in order to devise a global scale quantum communication network.

In fact, the optical fibers present the drawback of the signal depolarization in addition to the limited propagation distance covered, slightly higher than 100km.

However, free space channel looks more promising. Owing to the non-birefringence of the Earth atmosphere, it allows the transmission of polarization states without serious alterations, and could be employed for low cost local networks; but it has the

disadvantage that an unconfined optical mode can suffer for the obstacle presence along the line of sight or of distortions caused by the atmospheric turbulence or the weather conditions.

In order to overcome these limitations, a solution could come trying to mitigate free space channel restrictions for ground applications and at the same time, going beyond the concept of free-space, to the space.

Taking advantage of the fact that the propagation in empty space leaves almost unchanged the characteristic of the beam, the space has the potential to be the primary quantum channel for the purpose of implementing an effective global Quantum Communication Network based upon ground and space segments. Thus, two remote sites on the planet surface could communicate by ground-space-ground links (using the satellites of the web as trusted nodes), with minimized losses and turbulence contributions strongly reduced to about ten kilometers of atmospheric layers (for a space-ground link).

Besides, the space channel could be used in support of the free space in a local ground network out-of-order for strongly adverse weather conditions.

Among the crucial quantum communication experiments, for free space let us recall the inter-island links between Tenerife (OGS telescope) and la Palma [96], [76], and the significant stepping stone of the single photon exchange between a space LEO satellite and a ground receiver (Matera Laser Ranging Observatory MLRO) [100].

Envisaging a global-scale quantum communication network, in the short and long term, the international interest of the science community is undoubtedly high [75] [104], both for terrestrial links [19] and spatial ones [3] [101] [38], due to the gain in terms of security for optical systems and in long distance communications.

The aim of my thesis is to demonstrate the feasibility of quantum communication in free space and space, highlighting how ESA Galileo constellation could be strengthened into an Optical Quantum Communication Network (OQCN), by the employment of a compact and low cost prototype (SaNe-QKD OPT). It will be the first step toward a real global-scale quantum communication web.

The work here presented follows three years of research at the Luxor Laboratory in Padova.

In the first part this work follows the strategic project Quantum Future "The shift in the communication paradigm" (Padova University), investigating about the impact of the atmospheric turbulence in long range quantum and classical communication. It deals with the **ground beam propagation** for quantum communication (in free space). (Chapters 1 and 2).

In the second part it deals with the **space beam propagation** for quantum communication and the Optical Quantum Communication Network (OQCN) devised for the Galileo constellation. (Chapter 3 and 4). In this part my thesis follows the ESA project "Application of Optical Quantum Links to GNSS" about devising and realization of the prototype (SaNe-QKD OPT), in which the University of Padova was involved for the quantum part SaNe-QKD (I was part of the team) and Thales Alenia Space for the realization of the "classical" optical part OPT.

Summarizing:

Chapter 1 introduces an overview of topics about Optics, Photonics, atmospheric models and turbulence parameters.

Chapter 2 proceeds with the ground beam propagation (free space horizontal experiments) between two sites in Canary Island, with data processing and results.

Chapter 3 reports about optical quantum communication systems, satellite orbital mechanics, focusing on Galileo constellation parameters, recalled uplinks and downlinks topics ¹, about simulations of space beam propagation between satellites, Quantum Key Distribution and decoy state.

Chapter 4 resumes the necessary topics in order to implement an OQCN for Galileo satellites, unfortunately a constellation based only on inter-satellite quantum communication links: the huge distances can be overwhelmed according a planned network topology, but with the current technology the simulations of up/downlinks of Chapter 3 have demonstrated the unfeasibility of space-ground quantum communication links, and vice versa, owing to the high constellation altitude above the Earth surface. At the end of the chapter SaNe-QKD prototype arrangements and the interface between Quantum and Optical part are shown.

For each part my thesis addresses an open issue:

Ground beam propagation: in this part we address the issue of the turbulence compensation for long distance quantum communication links, improving our knowledge on arrangement requirement definition and drivers in order to perform an effective quantum optical link.

The aim was the realization of the new equipment (called the Canary telescope). I was part of the team for arranging and testing the custom Canary telescope. The team performed two free-space propagation links with the telescope. The former, a ‘short’ local range (about 20 km) link between Asiago and Monte Grappa (Italy) in order to test the telescope and check the Communication equipment at the transmitting part [22]. The latter, a ‘long’ range (143 km long) link between La Palma and Tenerife (Canary Islands) for free-space propagation experiments with severe turbulence conditions. Developments and data analysis are in the resulting works [90] [18] [98] with in [19].

Highlighted the output methodologies for turbulence characterization in Ground Quantum Optical Links. New knowledge obtained about horizontal links beam propagation in free space and turbulence.

Space beam propagation: here we address channel models and simulations of inter-satellite links, up/down links and decoy state schemes in order to determinate the feasibility, the network topology and keeping the requested requirements (between the requirements, ESA requested a telescope aperture less then 20 cm and low burden and power consumption).

¹ Naming as uplink the optical communication channel established between a ground- based station and a satellite, and as downlink the optical communication channel established between a satellite to a ground-based station.

I was involved in the arrangement of the quantum optical prototype, SaNe-QKD, born implementing an existing prototype, Quake of UniPd, based upon Quantum Key Distribution B92 protocol. [5]

Crucial parts are the interfaces in order to fuse SaNe-QKD with the classical optical counterpart OPT by Thales Alenia Space.

Besides, I wrote reports, technical notes, being an active part at the evaluation steps of the projects (progress meetings between ESA, UniPd and Thales Alenia Space).

At that moment, SaNe-QKD is ready in each optic-mechanical part for the Proof of Concept Demonstration and only issues about the electronic interface between SaNe-QKD and OPT need to be further implemented by TAS and UniPd.

The resulting prototype will be positioned on board of Galileo satellite constellation for performing Optical Quantum Communication and part of this work is reported in [38].

Both the parts are set into a more general context expressed in [10].

As in last decades the international scientist community understood that Quantum Information Processing and Quantum Communication (QIPQC) has the capability to revolutionize many fields of science and technologies, being Quantum Information with immense computing power respect to the classical information, while Quantum Communication guaranteed of intrinsically security. Consequently, many non EU countries (as United States, China, Canada,...) allocated huge funding for dedicated researches.

So, helped by the coordinating guidelines of ERA-pilot QIST, Qurope, QUIE²T [70], Europe needs to join the researches about Quantum Information Processing and Communication (QIPC), into a unique more complex picture to coordinate and unify many national researches and studies. The aim is not to loose the international leading role being competitive and at the forefront of the field, at the cutting edge of Quantum science and technologies, under one common European umbrella of the Community research program. In the following table 1 it is reported the list of the short and long term goals for Quantum Information Processing and Quantum Information in [70].

These thesis embraces the exploited themes mainly of long term-goals of QIPQC: satellite Quantum Communication, multi-node Quantum network and (more than) 1000 kilometres of Quantum Cryptography.

Short term goals	Quantum Communication
	Build of a quantum repeater with two nodes Entangle two remote quantum memories Laboratory demonstration of Device Independent QKD
Long term goals	Quantum Communication
	Satellite Quantum Communication 1000 kilometres of Quantum Cryptography Multi-node Quantum Network Realization of new quantum protocols

Table 1: This table reports Qurope short and long term goals (within 10 years) for Quantum Communication [70]

Introduzione (in lingua italiana)

La teoria della Meccanica Quantistica ha alle spalle oltre cento anni di vita. Dalla sua introduzione, le innovazioni tecnologiche da essa apportate ne fanno prevedere applicazioni su larga scala nel campo delle trasmissioni, rendendo le comunicazioni quantistiche (l'arte di spedire stati quantistici da un sito ad un altro) un fondamentale argomento di studi e ricerche. Storicamente le comunicazioni quantistiche sono state il banco di test nell'indagine sulle proprietà della Meccanica Quantistica (il paradosso EPR: l'apparente violazione dei principi classici di realismo e località [6]).

Solamente dopo alcuni anni, i ricercatori hanno compreso il potenziale di questo nuovo approccio della fisica moderna in diversi campi di indagine, come nell'Informazione Quantistica (manipolazione e trasmissione dell'informazione impiegando gli effetti quantistici) [64], il Teletrasporto Quantistico (il trasferimento di uno stato quantistico ad un punto arbitrariamente lontano) [7] e la Crittografia Quantistica. La Crittografia Quantistica è uno dei sorprendenti campi di ricerca, che promette trasmissioni assolutamente sicure di codici fra due terminali secondo prestabiliti protocolli (la Distribuzione Quantistica di Chiavi, con lo sviluppo dei protocolli BB84, B92, Decoy state QKD, ..), analizzando l'informazione spedita lungo un canale quantistico: facendo uso delle leggi della Meccanica Quantistica (*No Cloning Theorem* -teorema di non clonazione-) la presenza di un ascoltatore indesiderato è rilevata con bassa probabilità di errore, assicurando la sicurezza delle chiavi condivise. [74] [9] [8] [57]

A seguito delle nuove tecniche acquisite nei laboratori di ricerca -con favorevoli condizioni al contorno riguardo la sincronizzazione fra trasmettitore e ricevitore e la riduzione del rumore- alla fine dello scorso secolo alcuni scienziati hanno cercato di portare i loro esperimenti (di comunicazione quantistica) fuori dei laboratori, nelle difficili condizioni esterne [16] [53].

In generale, con la tecnologia attuale, le fibre ottiche di ultima generazione e lo spazio libero non sono ritenuti affidabili canali per concepire un network di comunicazione quantistica su scala globale.

Infatti, le fibre ottiche presentano lo svantaggio della depolarizzazione del segnale in aggiunta alla limitata distanza di propagazione coperta, difficilmente poco superiore ai 100km.

Invece il canale di spazio libero risulta decisamente piu' promettente. A causa della non birifrangenza dell'atmosfera terrestre, la trasmissione degli stati di polarizzazione ha luogo senza serie alterazioni, e in tal modo il canale di spazio libero potrebbe essere impiegato per network locali a basso costo; ma, ha lo svantaggio che un modo ottico non confinato soffre la presenza di ostacoli lungo la linea di vista o di distorsioni causate dalla turbolenza atmosferica o dalle condizioni meteorologiche.

Al fine di superare queste limitazioni, una soluzione potrebbe venire cercando di mitigare le limitazioni del canale di spazio libero per applicazioni a terra e allo stesso tempo, andando oltre il concetto di spazio libero, allo spazio stesso.

Considerando che la propagazione nello spazio (vuoto) lascia quasi inalterati i parametri caratteristici del fascio (ottico), lo spazio ha il potenziale di essere il canale quantistico primario allo scopo di implementare un efficace network di comunicazione quantistica su scala globale basato su segmenti terrestri e spaziali. In tal modo, due siti lontani sulla superficie del pianeta potrebbero comunicare mediante collegamenti terra-spazio-terra (utilizzando dei satelliti della rete come nodi fidati), con perdite minimizzate e contributi di turbolenza notevolmente ridotti, a dieci chilometri di strati atmosferici (per un collegamento spazio-terra). Inoltre, il canale spaziale potrebbe essere utilizzato come supporto al canale di spazio libero in un network terrestre locale momentaneamente inutilizzabile in caso di condizioni meteorologiche fortemente avverse.

Fra i cruciali esperimenti di comunicazione quantistica, per lo spazio libero ricordiamo le connessioni fra le isole di Tenerife (telescopio OGS) e La Palma [96], [76], e l'esperimento che e' stato la pietra miliare, quello di scambio di singolo fotone fra un satellite spaziale LEO e un ricevitore a terra (Matera Laser Ranging Observatory MLRO) [100].

Nella prospettiva di un network di comunicazione quantistica su scala globale, a breve e a lungo termine, l'interesse internazionale della comunita' scientifica e' indubbiamente elevato [75] [104], sia per collegamenti terrestri [19] che spaziali, [3] [101] [38], a causa del guadagno in termini di sicurezza per sistemi ottici sia di comunicazione su grandi distanze.

Il fine della mia tesi e' di dimostrare la fattibilita' della comunicazione quantistica nello spazio libero e nello spazio, evidenziando come la costellazione Galileo di ESA (Agenzia Spaziale Europea) possa essere potenziata in un Network di Comunicazione Quantistica Ottica (OQCN), mediante l'impiego di un prototipo compatto e a basso costo (SaNe-QKD OPT). Rappresentera' il primo passo verso una rete reale di comunicazione quantistica su scala globale.

Il lavoro qui presentato segue a tre anni di ricerca presso i laboratori Luxor di Padova. Nella prima parte questo lavoro ripercorre il progetto europeo Quantum Future "Il salto nel paradigma quantistico" (Universita' di Padova), investigando l'impatto della turbolenza atmosferica nella comunicazione quantistica e classica su lunga distanza. L'indagine riguarda la **propagazione terrestre di fasci (Ground beam propagation)** per la comunicazione quantistica in spazio libero. (Capitolo 1 e 2).

La seconda parte riguarda la **propagazione nello spazio di fasci (Space beam**

propagation) di comunicazione quantistica e la realizzazione di un Network di Comunicazione Quantistica Ottica (OQCN) concepito per la costellazione Galileo. (Capitolo 3 e 4). In questa parte, la tesi segue il progetto ESA (Ente Spaziale Europeo) "Applicazione di connessioni Ottiche Quantistiche per GNSS" riguardo la progettazione e realizzazione del prototipo (SaNe-QKD OPT), in cui l'Università di Padova era coinvolta per la parte quantistica (facevo parte del team) e Thales Alenia Space per la realizzazione della controparte di ottica "classica" OPT.

Riassumendo:

Capitolo 1 introduce una panoramica degli argomenti di ottica, fotonica, di modelli atmosferici e parametri di turbolenza.

Capitolo 2 procede con la propagazione terrestre di fasci (ottici) (esperimenti di propagazione orizzontale su spazio libero) fra due siti nelle isole Canarie, con analisi di dati e risultati ottenuti.

Capitolo 3 riporta sistemi di comunicazione ottica quantistica, meccanica orbitale, focalizzando la nostra attenzione sui parametri della costellazione Galileo, richiamando concetti di connessioni "uplink" e "downlink" ², riguardo simulazioni di propagazione di fasci nello spazio fra satelliti, Distribuzione di Chiavi Quantistiche e schema "Decoy".

Capitolo 4 riassume gli argomenti necessari per implementare un OQCN per i satelliti Galileo. Purtroppo per il momento è una costellazione basata su connessioni di comunicazione quantistica solo di tipo inter-satellitare: le enormi distanze possono venire superate mediante un'accurata topologia del network, mentre con la corrente tecnologia le simulazioni di up/downlink del capitolo 3 dimostrano la non fattibilità dei collegamenti di comunicazione quantistica spazio-terra e viceversa, a causa dell'elevata quota della costellazione rispetto alla superficie terrestre. Alla fine del capitolo la realizzazione del prototipo SaNe-QKD e le interfacce fra la parte quantum e classica sono mostrate.

Per ciascuna delle due parti la tesi affronta alcuni argomenti aperti:

Ground beam propagation (Propagazione terrestre di fasci): in questa parte è affrontata la questione della compensazione della turbolenza per connessioni di comunicazione quantistica su lunghe distanze, migliorando la nostra conoscenza sugli allestimenti richiesti e sui requisiti (necessari) al fine di realizzare un efficiente sistema di comunicazione ottico quantistico.

Il fine era la realizzazione di un nuovo strumento (chiamato "Canary telescope") ed ero parte del gruppo che si occupava di allestire e testare il telescopio custom. Il gruppo ha inoltre realizzato due esperimenti di propagazione in spazio libero con il "Canary telescope". Il primo link locale di breve distanza (circa 20 km) fra Asiago e Monte Grappa (Italia) al fine di valutare il telescopio e controllare l'apparato di comunicazione al lato trasmettitore [22]. Come secondo link ha avuto luogo la connessione su lunga distanza (143 km) fra La Palma e Tenerife (Isole Canarie) per

² Chiamando uplink il canale di comunicazione ottica stabilito fra una stazione a terra e un satellite, e come downlink il canale ottico quantistico stabilito fra un satellite e una stazione a terra.

esperimenti di propagazione (di fasci ottici) nello spazio libero in condizioni di intensa turbolenza. Sviluppi ed analisi dati sono riportati nei lavori [90] [18] [98] e [19], evidenziando le metodologie risultanti in merito alla caratterizzazione della turbolenza.

Space beam propagation (propagazione di fasci (ottici) nello spazio): in questa parte affrontiamo modelli di comunicazione e simulazioni di connessioni intersatellitari, connessioni up/downlink e schemi di stato "decoy" al fine di determinare la fattibilità, la topologia del network mantenendo i requisiti richiesti (fra i requisiti, ESA richiedeva apertura del telescopio inferiore a 20cm e ridotto ingombro e consumi).

Sono stata coinvolta nell'allestimento del prototipo ottico quantistico, SaNe-QKD, realizzato implementando un prototipo esistente, Quake di Università di Padova (UniPd), basato sul protocollo B92 della Distribuzione di Chiavi Quantistiche. [5] Parte cruciale è stato l'allestimento delle interfacce al fine di fondere SaNe-QKD con la controparte di ottica classica OPT ideata da Thales Alenia Space.

Inoltre, ho redatto report, note tecniche e sono stata parte attiva nelle riunioni periodiche attestanti gli avanzamenti del progetto ("progress meetings" fra ESA, UniPd e Thales Alenia Space).

In questo momento, SaNe-QKD è pronto nelle parti ottico-meccaniche in vista del test "Proof of Concept Demonstration" e solo alcune questioni riguardanti l'interfaccia elettronica fra SaNe-QKD e OPT necessitano di essere ulteriormente approfondite da TAS e UniPd.

Il prototipo sviluppato sarà posizionato a bordo della costellazione di satelliti Galileo per realizzare comunicazioni ottiche quantistiche e parte del lavoro svolto fino ad ora è riportato in [38].

Entrambe queste parti vanno collocate in un contesto più generale espresso in [10].

Poiché nelle scorse decadi la comunità scientifica internazionale aveva compreso che l'Elaborazione dell'Informazione Quantistica e la Comunicazione Quantistica (QIPQC) presentano il potenziale per rivoluzionare tanti campi di ricerca e tecnologie, essendo l'Informazione Quantistica di immenso potere computazionale rispetto all'classica, mentre la Comunicazione Quantistica garante di sicurezza intrinseca. Di conseguenza, parecchi stati non europei (come Stati Uniti, Cina, Canada,...) hanno stanziato fondi per ricerche deicate.

Di conseguenza, aiutati dalle linee guida di ERA-pilot QIST, Quore, QUIE²T [70], l'Europa ha la necessità unire le ricerche su l'Elaborazione dell'Informazione Quantistica e la Comunicazione Quantistica (QIPQC), in un unico e più complesso quadro per coordinare ed unificare tanti studi e ricerche nazionali. Il fine è di non perdere il ruolo di leader internazionale restando competitivi in prima linea, un fronte unito all'avanguardia nelle applicazioni e tecnologie quantistiche, sotto la comune egida del programma di ricerca Europeo.

Obbiettivi a breve termine	Comunicazione Quantistica
	Costruire un ripetitore quantistico con due nodi memorie quantistiche entangle Dimostrazione in laboratorio di QKD con strumentazione indipendente
Obbiettivi a lungo termine	Comunicazione Quantistica
	Comunicazione Quantistica Satellitare 1000 chilometri di Crittografia quantistica rete Quantistica Multi-nodo Realizzazione di un nuovi protocolli quantistici

Table 2: Questa tavola riporta gli obbiettivi a corto e lungo termine (entro 10 anni) per la Comunicazione Quantistica [70]

Di seguito la tabella 2 che riporta la lista degli obbiettivi dell'Elaborazione dell'Informazione Quantistica e alcuni temi fra gli obbiettivi a lungo termine di QIPQC: il satellite di Comunicazione Quantistica, un quantum network a multi-nodo e (più di) 1000 chilometri di Crittografia Quantistica.

Abstract

Keywords: Quantum Communication (QC), space and ground beam propagation, Optical Quantum Communication Network (OQCN), Quantum Key Distribution (QKD), Galileo satellite constellation, atmospheric turbulence, feasibility studies, Quantum prototype SaNe-QKD

The aim of my thesis is to demonstrate the feasibility of Quantum Communication in free space and space, pointing out how ESA Galileo constellation could be strengthened into an Optical Quantum Communication Network (OQCN), by the employment of a compact and low cost prototype (SaNe-QKD OPT).

Considering table 2 according the guidelines of [70] (2012) for the European Quantum Information Processing and Quantum Communication, three crucial long term goals are fulfilled, (Satellite Quantum Communication, besides 1000 kilometres of spatial Quantum Cryptography, multi-node Quantum Network), with reference to Galileo constellation: the new devised OQCN will perform Quantum Communication between approaching satellites of the constellation in multi-node mode, and Quantum Key Distribution scheme will be employed over large distances, definitely above 1000 kilometers.

My thesis summarizes three years of researches at the Luxor Laboratories in Padova. It is dedicated to two core topics, which are twofold aspects of the same issue: beam propagation in Quantum Communication over ground and over space, with the final realization of a Quantum Communication Network in which concretized the acquired knowledge in Quantum field. And Inter-island Canary links have been chosen as representing a worse case scenario for Quantum Communication experiments, an ideal test bed to investigate beam propagation in view of the space applications, where crucial aspects are the huge distances that Communication beams have to cover.

The thesis is divided in two complementary parts:

Ground beam propagation

Beam propagation in free space along horizontal links in Canary Islands, performing long distances (143 kilometers) and aiming to exploit beam propagation through a turbulent medium. The results pointed out optical configurations and specifics in order to obtain an effective and stable communication link.

These researches are within of the strategic project Quantum Future of the University of Padova, "the shift in the Quantum paradigm"

Space beam propagation.

The second part is dedicated to space beam propagation, regarding design and arrangement of the Quantum prototype SaNe-QKD to fuse with the Optical Communication prototype OPT (by Thales Alenia Space). The resulting system, SaNe-QKD OPT, will be positioned on board of Galileo satellites for performing Quantum Optical Inter-satellite links.

Simulations about inter-satellite links, network topology features and key length evaluation, have allowed to obtain results and specifications about operative wavelengths and telescope apertures to use for inter-satellite communications. Then, the prototype SaNe-QKD have been arranged and is here shown in each part.

This researches are part of the project "Application of Optical Quantum Communication Links for GNSS" by the European space Agency (ESA).

My thesis is divided in four chapters, as follows

Ground beam propagation

Chapter 1 introduces an overview of main concepts of photonics, atmospheric models and turbulence parameters, optics and fiber-optics and telescopes, used throughout the treatment.

The Newtonian telescope is investigated in order to analyze the optical path arriving at the prototype SaNe-QKD for space purpose and the Canary Telescope in order to realize an optical system implementing the centroid spot following system. Zemax simulations are presented for both to check aberrations and for collimation issues. For Newtonian off-axis field, coma and field curvature are revealed. For Canary Telescope chromatic aberration is revealed and the arrangement scheme of the experiment of beam propagation in free space in Canary Islands with co-propagating beams control is described.

Kolmogorov atmospheric turbulence models with Hughnagel Valley model is then briefly reported too. It will be used in Canary experiments over 143 kilometers and in chapter 3 for up/downlink quantum communication simulations between a ground base transceiver and a satellite.

Chapter 2. It is known that an unconfined optical mode propagating in a turbulent medium suffers of distortions. In Quantum Communication the information is encoded and transmitted as a train of single photons with mean average of about

one photon for pulse; it follows that the link losses of a beam propagating in atmosphere increase with the distance; in contrast they cannot be reduced by increasing the signal power as in optical communication.

Consequently, it is crucial to exploit beam propagation over long ranges, in order to analyze photon statistics, the transformations on the beam due to the ground in order to prevent the unleashing of the beam between transmitter and receiver. The turbulence introduces two contributes according the eddies size [51] [52] respect to the optical beam:

- Beam wandering, which occurs when a laser beam is refracted by eddies with size larger than the beam diameter, causing a displacement of the beam center (centroid).
- Beam spreading, which is due to the laser beam being refracted by eddies smaller than the beam diameter. The short-term beam spread is an additional spread with respect to the standard spread due to the free space laser beam propagation (without turbulence effects).

These effects appears in relation to the exposition time: on short time scales the beam wandering is the dominant effect, while on long time scales the beam spreading is the dominant effect. Using turbulence as a resource, the research of beam propagation in free-space communication links opens to test a new equipment, the custom Canary telescope (Chapter1). The team performed two free-space propagation links with the telescope: the former, a ‘short’ local range (about 20 km) test link between Asiago and Monte Grappa (Italy) in order to examine the Canary Telescope and check the communication equipment at the transmitting part; the latter, a ‘long’ range (143 km long) link between La Palma and Tenerife (Canary Islands) for free-space propagation experiments with severe turbulence conditions. Developments and data analysis are presented, pointing out methodologies for turbulence characterization in Ground Quantum Optical Links.

The results of the propagation of single, double beams along 143 kilometers have demonstrated that it is possible to optimize an optical system in order to reconstruct the beam long-term diameter and by techniques of beam co-propagating technique, the loss link could be reduced. This is promising as link losses are crucial aspect in Quantum Communication, when in a noisy channel the quantum signal (the information encoded in single photons) cannot be improved by increasing the signal power.

Besides we observed that the statistic of arrival of single photons over a free-space 143 km optical link confirms that there is a transformation from Poissonian to log-normal distribution: There is still the evidence of consecutive subintervals of low losses allowing us to envisage the exploitation of turbulence as an SNR improvement technique.

Space beam propagation

Chapter 3 according the requests of the ESA project, a feasibility study for Quan-

tum Communication applications to Galileo constellation is shown.

The chapter starts with an overview of the merits of Optical Communication (data rate exchanging, lightness, compactness, low power consumption..) pointing out that the intrinsically secure is the added value that only the Quantum counterpart could supply. A brief part recalling orbital motion in space in order to check satellite orbital motion. Then we open to up/downlink simulations overview: recalling the simulations in literature of ground to space or space to ground beam propagation through the atmosphere, the feasibility study shows that unfortunately Galileo constellation can realize only intersatellite communication links, as the atmosphere and the altitude of the satellite constellation prevents any effective and real single photon transmission with the current technologies.

However, simulation results of intersatellite beam propagation show us that the huge distances can be overwhelmed (derived requirements are telescope diameters $>20\text{cm}$ and operating wavelength $<532\text{nm}$), and time interval within perform Quantum Communication can be calculated: respect to a reference satellite of different orbital plane, the time interval in which the intra-satellite distances are within 15000 kilometres are

- For satellite called three of about 176 minutes
- For satellite called two of about 168 minutes

Then exploiting the relative motion of satellites lying in different orbital planes, we show that it is possible to target communication between satellites that are closer in turns, and to achieve appreciable transmission rates: the distance intervals in which we calculated the raw key rate values are 6000, 10000 and 19000 kilometers, and the best values in raw key rates (18M bits/s at 6600 kilometers, related to lower attenuation values) are obtained for a telescope diameter of 50cm and wavelength of 50nm, while the worse values in raw key rates (2.2 Kbits/s at 6600 kilometers, related to higher attenuation values) are for a telescope diameter of 20cm and wavelength of 800nm.

Finally, today information-based society security is of paramount importance: Galileo Optical Quantum Network will guarantee intrinsically secure key exchanging, free of PSN attack, within a satellite distance signed by decoy scheme approach. After a brief review of a model for a Quantum Communication System, simulations about key rate are shown in the final section, showing that for same wavelengths and within same beam propagation distances, larger apertures present higher values of key rate[bit/s]. At the same time we have observed that shorter operating wavelengths presents higher values of key rate, assuring that in merit to Galileo OQCN decoy schemes could be applied in order to beat PNS attack over well defined communication links in relation to the link distance covered, the operative wavelength and the telescope aperture.

Chapter 4 We present a summary about the results of a feasibility study with reference to the architecture of Optical Quantum Communication links to a global

navigation satellite system (GNSS) Galileo: for an inter-satellite Quantum Key Distribution (QKD) network we have derived in the past chapter some specifications about the wavelength selection, by an analysis of the beam propagation outside the atmosphere for telescope radius and wavelength, showing that by decreasing the wavelength and increasing the telescope radius, the beam size at the receiver is reduced, and so is the attenuation, while the SNR increases. Given the GNSS motion, we have presented still some MATLAB simulations evaluating the time intervals in which two spacecraft reach the minimal intra-satellite distances, in order to investigate the feasibility of the OQL system and evaluate its expected performance in terms of achievable key lengths.

In this chapter the expected final secret key rate are derived (by taking into account raw key rate, the average number of photons per qubit at the transmitter output, the QKD efficiency, the free-space link attenuation, the attenuation due to devices at the receiver side, the QBER) and the number of required sifted key vs QBER that must be available to Alice and Bob, after the transmission on the quantum layer and the sifting phase, are evaluated too, in order for them to be able to extract a secret key of the desired key length. (Assumed attenuation between -40 dB and -45 dB for the quantum channel).

Then the quantum prototype SaNe-QKD is described in each part, the Quantum Key Distribution protocol used B92, the transmitter and receiver opto-mechanical arrangements with the dedicated interfaces to interface the Quantum module with the Optical one built by Thales Alenia Space.

Finally the Proof of Concept Demonstration tests for the quantum part described.

Sommario

Parole chiave: Comunicazione Quantistica (QC), propagazione di fasci ottici nello spazio e nello spazio libero, rete di comunicazione ottica quantistica (OQCN), Distribuzione di chiavi quantistiche (QKD), costellazione satellitare Galileo, turbolenza atmosferica, studi di fattibilit  prototipo quantistico SaNe-QKD

Il fine della mia tesi   di dimostrare la fattibilit  della comunicazione quantistica nello spazio libero e nello spazio, evidenziando come la costellazione Galileo di ESA potrebbe essere potenziata in una rete di comunicazione ottica quantistica (OQCN) dall'impiego del prototipo compatto e a basso costo SaNe-QKD.

Considerando la tabella 2 secondo le linee guida di [70] (2012) per l'analisi dell'Informazione Quantistica e della Crittografia Quantistica Europea, tre obiettivi a lungo termine e cruciali sono realizzati. (Comunicazione Quantistica satellitare, oltre 1000 chilometri di crittografia quantistica spaziale, rete quantistica multi-node), con riferimento alla costellazione Galileo: il nuovo new OQCN sar  in grado di realizzare comunicazione quantistica fra satelliti della stessa costellazione in avvicinamento in modalit  di multi-nodo, e uno schema di Distribuzione di Chiave Quantistiche Quantum Key Distribution sar  realizzato definitivamente su distanze superiori ai 1000 chilometri.

La mia tesi riassume tre anni di ricerca presso i Laboratori Luxor di Padova. E' dedicata a due argomenti centrali, che sono due aspetti duplici di uno stesso argomento: la Comunicazione Quantistica sia a terra che nello spazio, con la finale realizzazione di un OQCN (network di comunicazione quantistica) in cui concretizzare le conoscenze acquisite nel campo della quantistica. I collegamenti ottici fra le isole Canarie rappresentano il peggiore scenario per gli esperimenti di Comunicazione Quantistica, un banco di prova ideale per investigare le propriet  del fascio ottico in vista delle applicazioni spaziali, dove aspetti cruciali sono le enormi distanze che i fasci di comunicazione devono coprire.

La tesi si divide in due parti complementari:

Ground beam propagation (propagazione terrestre di fasci ottici)

la propagazione di fasci ottici nello spazio libero lungo link orizzontali alle isole Canarie, realizzando grandi distanze (143 chilometri) e avendo come scopo l'analisi (della propagazione del fascio) in un mezzo turbolento. I risultati evidenziano configurazioni ottiche e specifiche al fine di realizzare un efficace e stabile link di comunicazione. Queste ricerche sono parte del progetto strategico Quantum Future dell'Università di Padova, "il salto nel paradigma quantistico" (The shift in the Quantum paradigm)

Space beam propagation (propagazione spaziale di fasci (ottici)).

La seconda parte è dedicata alla propagazione spaziale di fasci ottici, riguardando design e allestimento del prototipo quantistico SaNe-QKD al fine di interfacciarlo con il prototipo di comunicazione ottica (realizzato da Thales Alenia Space). Il sistema risultante, SaNe-QKD OPT, sarà posizionato a bordo dei satelliti Galileo per realizzare link ottici quantistici inter-satellitari.

Simulazioni riguardo i link inter-satellitari, gli aspetti della topologia del network realizzato e la valutazione della chiave utilizzata, hanno permesso di ottenere risultati e specifiche come la lunghezza d'onda operativa e l'apertura dei telescopi da usare per le comunicazioni fra satelliti. Ne segue che il prototipo SaNe-QKD è stato allestito ed è qui mostrato in ogni sua parte.

Queste ricerche sono parte del progetto "Applicazione di Link di comunicazione ottica quantistica a GNSS" della Agenzia Spaziale Europea (ESA).

La mia tesi è divisa in quattro capitoli come segue:

Propagazione terrestre di fasci (Ground beam propagation

Capitolo 1 introduce una panoramica sui principali concetti di fotonica, modelli atmosferici e parametri di turbolenza, ottica, fibre ottiche e telescopi, concetti richiamati durante l'esposizione.

Il telescopio Newtoniano è analizzato al fine di indagare il fascio ottico che giunge al prototipo SaNe-QKD per fini spaziali e il telescopio Canario è analizzato per realizzare un sistema ottico capace di implementare un sistema di inseguimento del centroide. Simulazioni con Zemax sono presentate per entrambi i telescopi al fine di controllare le aberrazioni e per motivi di collimazione del sistema ottico. Per il Newtoniano il campo fuori asse, coma e curvatura di campo sono rivelati. Per il telescopio Canario aberrazione cromatica ed inoltre è descritto lo schema dell'esperimento di propagazione del fascio ottico in spazio libero nelle isole Canarie con controllo di fasci co-propaganti.

I modelli di turbolenza atmosferica e di Hughnagel Valley model sono poi brevemente riportati. Saranno utilizzati negli esperimenti alle isole Canarie su 143 chilometri e nel capitolo 3 saranno richiamati per simulazioni terra-spazio di comunicazione quantistica fra trasmettitore/ricevitore a terra e satellite.

Capitolo 2. E' noto che un modo ottico non confinato che si propaga in un mezzo turbolento e' soggetto a distorsioni. In Comunicazione Quantistica l'informazione e' codificata e trasmessa sotto forma di un treno di singoli impulsi con media di circa un fotone per impulso; segue che le perdite del link di un fascio che si propaga in atmosfera cresce con la distanza; di contro non possono essere ridotte aumentando la potenza del segnale (ottico) come nelle comunicazioni ottiche classiche.

Di conseguenza diventa cruciale investigare la propagazione di fasci ottici su grandi distanze, al fine di analizzare la statistica del fotone, le trasformazioni del fascio dovute alla propagazione terrestre al fine di precludere il disaccoppiamento del fascio fra trasmettitore e ricevitore. La turbolenza introduce due contributi rispetto alla dimensione dei vortici di turbolenza ("eddies" [51] [52]) in relazione al fascio ottico:

- "Beam wandering" (ballamento del fascio ottico), che ha luogo quando un fascio laser e' rifratto da vortici di turbolenza con dimensione maggiore del fascio ottico causando lo spostamento del centro del fascio (centroide).
- "Beam spreading" (allargamento del fascio), che e' dovuto al fascio ottico rifratto da vortici di turbolenza di dimensione inferiore al diametro del fascio. L' allargamento su breve termine ("short-term") e' un contributo addizionale all' allargamento tipico della propagazione in spazio libero (in assenza di effetti di turbolenza).

Questi effetti sono legati al tempo di esposizione: su scale temporali brevi il ballamento del fascio e' l' effetto dominante mentre su scale temporali lunghe l' effetto dominante e' l' allargamento del fascio. Utilizzando la turbolenza come una risorsa, la ricerca sulla propagazione di fasci ottici in link ottici di comunicazione su spazio libero apre i test del nuovo allestimento, il telescopio "custom" Canario (capitolo 1). Il gruppo di ricerca ha realizzato due esperimenti di link in propagazione in spazio libero. Il primo, un test a corta distanza (circa 20 chilometri) fra Asiago e Monte Grappa (Italia) per testare il telescopio Canario e controllare i sistemi di comunicazione alla parte del trasmettitore; il secondo , un link a lunga distanza (143 chilometri) fra le isole di La Palma e Tenerife (Isole Canarie) per esperimenti di propagazione in spazio libero con severe condizioni di turbolenza. Sviluppo e analisi dei dati sono presentati, evidenziando le metodologie e la caratterizzazione della turbolenza in link terrestri ottici quantistici.

I risultati della propagazione di singoli, doppi fasci lungo 143 chilometri hanno dimostrato che e' possibile attimizzare un sistema ottico al fine di ricostruire il diametro del fascio di "lungo termine" ("long term") e da tecniche di co-propagazione dei fasci le perdite dei link possono essere ridotte. Cio' e' promettente poiche' le perdite dei link sono un aspetto cruciale in Comunicazione Quantistica, quando in un canale "noisy"(rumoroso) il segnale quantistico (l' informazione codificata in singoli fotoni) non puo' essere migliorata mediante l' aumento della potenza del segnale. Inoltre abbiamo osservato che la statistica di arrivo dei singoli fotoni nello spazio libero (143

chilometri di link ottico) conferma la trasformazione da Poissoniana a log-normale della distribuzione (statistica della sorgente): c'è inoltre evidenza di sub intervalli consecutivi di basse perdite, cosa che permette di aprire uno scenario di ricerca sui fenomeni di turbolenza come miglioramento delle tecniche di ("signal to noise") miglioramento del rapporto segnale-rumore.

Propagazione spaziale di fasci (Space beam propagation)

Capitolo 3 secondo le richieste del progetto dell' Agenzia Spaziale europea (ESA) sono riportati gli studi di fattibilità per l' applicazione della Comunicazione Quantistica nella costellazione Galileo.

Il capitolo inizia con una panoramica sui meriti della Comunicazione Ottica (rate di scambio dati, riduzione peso e consumi, compattezza,..) evidenziando che la sicurezza (intrinseca) è un valore aggiunto che solo la controparte quantistica può fornire.

Il capitolo inizia con una breve parte che richiama la meccanica orbitale dei satelliti, In seguito si continua con simulazioni terra-spazio richiamando le simulazioni presenti in letteratura xi propagazione di fasci ottici terra-spazio e spazio-terra attraverso l', lo studio di fattibilità mostra purtroppo che la costellazione Galileo può realizzare solo link di comunicazione inter satellitare poiché l'atmosfera e quota dei satelliti ne impediscono ogni trasmissione di singolo fotone con la presente tecnologia.

Comunque i risultati delle simulazioni di propagazione di fascio ottico fra satelliti mostrano che le enormi distanze spaziali possono essere superate (i requisiti derivati sono di diametro del telescopio < 20 cm e di lunghezza d'operativa < 532 nm) e gli intervalli temporali entro cui realizzare la comunicazione quantistica possono essere calcolati: rispetto ad un satellite di riferimento di differente piano orbitale, l' intervallo temporale in cui le distanze interstellari sono entro 15000 chilometri sono

- Per il satellite chiamato tre di circa satellite 176 minuti
- Per il satellite chiamato due di circa satellite 168 minuti

In seguito i moti relativi dei satelliti che giacciono in differenti piani orbitali mostrano che è possibile comunicare fra due satelliti che sono a turno più vicini, ottenendo apprezzabili rate di comunicazione:

gli intervalli di distanza in cui calcolare i valori di "raw key rate" sono 6000, 10000 e 19000 chilometri, e i migliori valori sono (18M bits/s a 6600 km, relativamente a bassi valori di attenuazione) sono ottenuti per un telescopio di diametro di 50cm e lunghezza d' onda di 50nm, mentre i peggiori valori di "raw key rates" (2.2 Kbits/s a 6600 chilometri, in relazione a maggiori valori di attenuazione) si hanno per un telescopio di 20cm e lunghezza d' di 800 nm.

Infine, la sicurezza dell'odierna società basata sull' informazione è di fondamentale importanza: il Network Galileo (Optical Quantum Communication Network) garantirà la sicurezza intrinseca dello scambio di chiavi quantistiche, libero da attacco PN entro una distanza inter-satellitare definita dallo schema di Decoy. Dopo

un breve richiamo al modello per un sistema di Comunicazione Quantistica, simulazioni in merito al "key rate" (tasso di scambio di chiavi) sono mostrate nella sezione finale, mostrando che fissate lunghezza d'onda e distanze interstellari, maggiori sono le aperture dei telescopi maggiori sono i valori di "key rate" ottenuti. Allo stesso tempo abbiamo osservato che piu' corte lunghezze d'onda operative presentano maggiori valori di "key rate", assicurando che in merito alla costellazione Galileo OQCN (Optical Quantum Communication Network) gli schemi di decoy possono essere applicati al fine di battere l' attacco PNS, sui possibili link di comunicazione, in relazione al range di distanza (della comunicazione), alla lunghezza d'onda coperta e all' apertura del telescopio.

Dopo un breve richiamo al modello per un sistema di Comunicazione Quantistica, simulazioni in merito al "key rate" sono mostrate nella sezione finale, evidenziando che considerando le lunghezze d'onda e le distanze di propagazione del fascio, grandi aperture presentano elevati valori di "key rate". Allo stesso tempo abbiamo osservato che a corte lunghezza d'onda operativa presentano maggiori valori di "key rate". Allo stesso tempo abbiamo osservato che corte lunghezze d'onda operative presentano maggiori valori di "key rate" assicurando che in merito a Galileo OQCN (Optical Quantum Communication Network) gli schemi di decoy possono essere applicati al fine di battere l' attacco PNS sui possibili link di comunicazione in relazione alla distanza coperta, la lunghezza d'onda operativa scelta e l' apertura del telescopio.

Capitolo 4 Presentiamo un riassunto (introduttivo) riguardo ai risultati dello studio di fattibilita' sull' applicazione di link di comunicazione Ottici Quantistici in relazione al sistema globale satellitare (GNSS Galileo): per un network basato sulla Distribuzione di Chiavi Quantistiche inter-satellitare abbiamo derivato nel passato capitolo alcune specificazioni riguardo alla selezione della lunghezza d'onda mediante una analisi del fascio che si propaga al di fuori dell' atmosfera per telescopi di diametro fissato e per lunghezze d'onda determinate, mostrando che decrescendo la lunghezza d'onda e aumentando il raggio del telescopio la dimensione del fascio al ricevitore si riduce e cosi' l' attenuazione, mentre il rapporto segnale rumore SNR aumenta.

Considerato il moto del sistema Galileo GNSS, abbiamo anche mostrato alcune simulazioni in MATLAB per valutare gli intervalli temporali in cui due moduli spaziali raggiungono la minima distanza fra di loro, al fine di investigare la fattibilita' del sistema di Link di Comunicazione Ottico Quantistica (OQL) e valutare le attese performance (rese) in termini di lunghezze delle chiavi (crittografiche) raggiungibili.

In questo capitolo la chiave segreta finale attesa e' derivata (considerando il "raw key rate", il numero medio di fotoni per qubit in uscita dal trasmettitore, l' efficienza di Distribuzione di Chiavi Quantistiche, l' attenuazione dei link di spazio libero, l' attenuazione dovuta ai rivelatori dalla parte del ricevitore , il QBER) e il numero

di chiavi "sifted" (esaminate/analizzate) richieste contro il QBER che deve essere a disposizione del trasmettitore e del ricevitore, poi la trasmissione a livello quantistico e la fase di "sifting" (esame/analisi), sono anche valutate, al fine di poter esaminare la chiave segreta di desiderata lunghezza. (Assunti valori di attenuazione fra -40 dB e -45 dB per il canale quantistico).

Sono di seguito descritti il prototipo quantistico SaNe-QKD in ogni sua parte, il protocollo di Distribuzione di Chiavi Quantistiche utilizzato B92, il trasmettitore e il ricevitore nel suo arrangiamento opto-meccanico con le dedicate interfacce per mettere in comunicazione il modulo quantistico col modulo ottico costruito da Thales Alenia Space.

Infine i test di Proof of Concept Demonstration (Prova della Dimostrazione del Concetto) per la parte quantistica sono descritti.

Contents

Introduction	3
Introduzione(in lingua italiana)	9
Abstract	15
Abstract	21
Abstract	27
List of Tables	29
List of Figures	31
I Ground beam propagation	39
1 Optical Links	41
1.1 Classical Optics	42
1.1.1 Dall-Kirkham Cassegrain Telescope	53
1.1.2 Canary Telescope	54
1.2 Gaussian Beams	61
1.2.1 LASERs	61
1.2.2 Gaussian Beam	61
1.3 Atmospheric models and turbulence effects	65
2 Ground Links	71
2.1 Impact of turbulence in long range communication	76
2.1.1 Link Analysis	79
2.2 Conclusions	91
II APPLICATION OF OPTICAL QUANTUM LINKS TO GNSS	

93

3	Application of Optical Quantum links to GNSS: first phase	97
3.0.1	Orbital mechanics for Galileo Constellation	103
3.0.2	Circular orbit	103
3.0.3	Uplinks and Downlinks between Space and Earth	108
3.1	Intersatellite models for OQL	116
3.1.1	Galileo constellation	116
3.1.2	Space-based Global Quantum Network	127
3.2	Conclusions	135
4	APPLICATIONS OF OPTICAL QUANTUM LINKS TO GNSS: second phase	137
4.1	Optical Quantum link techniques for secure communications	137
4.2	Payload conceptual design	141
4.3	Secure communication for SaNe-QKD	143
4.4	Quantum Key Distribution for SaNe-QKD	147
4.5	Transmitter	153
4.6	Receiver	159
4.6.1	Expected parameters and key lengths for SaNe-QKD	164
4.6.2	Design	168
4.7	Proof of Concept Demonstration: quantum part test plan	173
4.8	Conclusions	175
	Bibliography	179

List of Tables

1	This table reports Europe short and long term goals (within 10 years) for Quantum Communication [70]	7
2	Questa tavola riporta gli obiettivi a corto e lungo termine (entro 10 anni) per la Comunicazione Quantistica [70]	13
1.1	The table shows the parameters of the Newtonian tube used for Optical Quantum Communication experiments.	50
1.2	Table about different focal lengths for test wavelengths.	55
2.1	Meteo Data on both sites (T=Teide R=Roque) for all the observing nights. Wind Speed is in Km/h, wind direction in degrees, humidity in percent whereas r0 in cm. The value of C_n^2 is to be intended as explained in the text multiplied by 10^{-14} for 1Km along the path and by 10^{-16} for the others 143Km. C is the validity index based on the number of seeing data: Poor, Medium, Good.	78
2.2	Output power measured at JKT.	78
3.1	The table briefly recalls the main pro and cons of optical communication compared to Radio Frequency (RF) technology	99
3.2	In the table the main parameters for Galileo satellite constellation are reported.	117
3.3	Chart showing the time interval in which the distance is lower than d_0	119
3.4	Table showing the minimum value distances for each couple of satellites, referring to the minimum values showed in figure 3.3	119

List of Figures

1	OGS secondary	1
1.1	The figure shows the conversion between power ratio P_{output}/P_{input} and attenuation coefficient α [dB] for a fiber of length 1km. An attenuation coefficient of 3dB corresponds to power ratio of $T = 0.5$, an attenuation of 10dB corresponds power ratio of $T = 0.1$, an attenuation of 20dB corresponds to a power ration of $T = 0.01$ and an attenuation of 30dB corresponds to a power ration of $T = 0.001$. . .	46
1.2	Example of Newtonian telescope VIXENRS200, used during the project application of Optical Quantum Links to GNSS, discussed in the second part of this thesis.	48
1.3	Zemax elaboration of the optical path. The Newtonian telescope VIXEN RS200 used for the Proof of Concept demonstration of the project "Optical Quantum Communication Links for GNSS". The simulation uses two fields, blue on axis, green out of axis.	49
1.4	The figure shows the Zemax elaboration about the Neutronian tube at the interface between SaNe-QKD prototype and OPT (project"Optical Quantum Communication Links for GNSS"). The image shows that the field curvature is visible at the interface and the calculated RMS radius is of 4.168um for the Field 1 (coassial) and RMS radius is of 5.007 um for field 2 (obtained putting a Y-field offset of 0.475). This image demonstrate that taking care of positioning a collimating lens with the right aperture at the interface between the UniPd system SaNe-QKD and the TAS system OPT, it is possible to interface the two optical systems. Note that it is present the coma pattern characteristic of off-axis images for Newtonian uncorrected telescopes . . .	51
1.5	Figure showing some Cassegrain telescopes with type of mirror and characteristics	53
1.6	"Reef" Dall Kirkham Cassegrain telescope used as support for laboratory with the Canary Telescope	54
1.7	With Ivan Capraro and Paolo Villoresi during tests of the Canary telescope at Asiago observatory (Italy) in April 2011, while performing a beam propagation experiment between Asiago and Monte Grappa (Italy).	55

1.8	Zemax simulation of the Zen lens.	56
1.9	Image of Zen lens mounted on the Canary telescope and in Zemax elaboration	57
1.10	Desktop images of Zemax software elaboration for the Canary Telescope. It uses 2 aspheric Thorlabs lenses (350420 and 350280) positioned at the first focus of the Zen Lens. The system is analyzed for 532nm and 808 nm.	57
1.11	The figure shows the telescope in September 2011 in La Palma site for some nights of ground beam propagation experiments between La Palma and Tenerife.	58
1.12	Figure (Up): Arrangement of the experiment of communication at the transmitter and at the receive showing the beam correction explained in point 1. Figure (Down): arrangement of the experiment of communication at the transmitter and at the receive showing the beam correction explained in point 2.	60
1.13	The figure shows Bufton velocity profile	68
1.14	The figures reports a Hufnagel Valley profile: the relation between $C_n^2 [m^{-2/3}]$ and the altitude $h[km]$	69
2.1	Canary telescope at JKT site, in La Palma pointing to OGS telescope, Tenerife.	72
2.2	Centroid Position night 19th – 20th 8:01 am. Averages at different times in order to eliminate the effect of short term turbulence.	74
2.3	Centroid distance from center (with minus sign) with respect to the collected power at OGS night 19th – 20th 6:19 am. It os shown that the collected power is nearly completely zero with a moment of about 2.5 pixels. From the system calibration it turns out that the focal spot moves of about $3\mu m/pixel$ corresponding to a displacement of about 70cm at OGS compatible with the observations.	75
2.4	Centroid Position X and Y with respect to the collected power at OGS night 19th-20th 8:01 am.	75
2.5	Images of power collected continuously by the co-propagating beam techniques.	76
2.6	Fitting of the profile in x and y on the transmitting aperture during the night of 23th. Notice how the $1/e^2$ criteria is met.	77
2.7	3D profile of the outgoing beam on sept. 23th.	77
2.8	Mean temporal scintillation variation versus the block size on which the SI is calculated. This is the effect of aperture averaging.	80
2.9	Spatial Scintillation Index v.s the exposure time.	80

2.10	Data obtained for different single photon acquisition compared to the background (first line). For each acquisition we report the total duration of the acquisition (Time), the temporal windows defining the counting interval (Window), the mean number of counts in the counting interval (Mean), and its the standard deviation (Std). We also report the scintillation index (SI) and the frequency bound defined in such a way that all the frequencies below the bound contribute to 95% of the scintillation index (Bound). With High (Low) we indicate acquisition with a high (low) mean photon number detected during 1 s. We notice that for the last two data sets the bound is higher due to the low signal compared to the background (having a flat frequency spectrum)	81
2.11	SPAD temporal distribution of count occurrences.	82
2.12	(color online). SPAD corresponding lognormal and Mandel curves. We can compare the data with the corresponding Poissonian distribution with the same mean value (234.1 ± 0.1) that would be obtained without turbulence.	84
2.13	(Color line). Photodiode temporal distribution intensity occurrences.	85
2.14	(color online). Photodiode temporal distribution intensity occurrences and corresponding lognormal curve.	86
2.15	(color online). SPAD power spectrum and cumulative power spectrum. Frequency bound (red vertical line): The frequencies below 51 Hz contribute to 95% of the scintillation index.	86
2.16	(color online). SPAD cumulative power spectrum. Frequency bound (red vertical line): The frequencies below 51 Hz contribute to 95% of the scintillation index.	87
2.17	(color online). Duration (in milliseconds) of events with overthreshold counting. In the different plots we considered a threshold of 1, 2, 4, and 6 dB above the average.	88
2.18	(color online). Counts that will be detected in the function of the threshold selection.	90
2.19	The image shows the Optical Quantum Communication Network (OQCN) for Galileo Constellation devised by University of Padova and Thales Alenia Space for ESA. Blue lines represent the communication channels performed between two optical transceivers on board of the satellites. Let us note that when two satellites approach each other, the Optical Link (Classical and Quantum) is accomplished. Earth and satellites are not built to scale in the figure.	95

3.1	The figure shows the architecture of an optical transceiver for space-to-space laser links. RX stands for Receiver, TX for Transmitter, ATD for Acquisition and Tracking Detector, PAA stands for Point Ahead Accuracy, FPA for Fine Pointing Assembly, CPA Coarse Pointing Assembly, ANT for Antenna.	100
3.2	The figure represents the estimation of the circular orbital period related to the distance from the Earth surface (the altitude interval is between 0 and 40000 km above the Earth surface).	104
3.3	The figure shows the estimation of the circular orbital speed related to the distance from the Earth surface	104
3.4	The figure represents the variation of the gravitational acceleration experienced by a satellite: the gravitational acceleration is here expressed in terms of ratio between the gravity value at the altitude z and at the sea level $g_0 = 9.807m/s$. The altitude interval performed is between 0 and 40000 km above the Earth surface	106
3.5	850nm: plot for up/downlink for long-term beam width $w_{LT}[m]$ vs. link distance [km] for Earth ESA telescope MLRO (diameter 1.5 m) in Matera. The satellite is supposed at the zenith of the ground station. The satellite telescope is supposed 20 cm of diameter [91]. The orbit altitudes of LEO, ISS, GLONASS, GPS NAVISTAR, Galileo and GEO orbit are shown.	109
3.6	850nm: plot for up/downlink for beam displacement β vs. link distance [km] for Earth ESA telescope MLRO (diameter 1.5 m) in Matera. The satellite is supposed at the zenith of the ground station. The satellite telescope is supposed 20 cm of diameter.[91] The orbit altitudes of LEO, ISS, GLONASS, GPS NAVISTAR, Galileo and GEO orbit are shown.	109
3.7	850nm: plot for up/downlink for short-term beam width $w_{LT}[m]$ vs. link distance [km] for Earth ESA telescope MLRO (diameter 1.5 m) in Matera. The satellite is supposed at the zenith of the ground station. The satellite telescope is supposed 20 cm of diameter [91]. The orbit altitudes of LEO, ISS, GLONASS, GPS NAVISTAR, Galileo and GEO orbit are shown.	110
3.8	For different telescope diameters[cm], the figure represents the day photon number collected vs. the field of view of the telescope [mrad]. It is assumed that the Earth albedo is 0.38, the Solar constant $S = 4.61 \cdot 10^{18} \text{ ph/s} \cdot \text{nm} \cdot \text{m}^2$ and bandwidth 1nm and detection time of 1ns. .	113
3.9	For different telescope diameters[cm] and assuming a full moon night, the figure represents the night photon number collected vs. the field of view of the telescope [mrad]. It is assumed that the Moon albedo is 0.12, the Earth albedo is 0.38, the Solar constant $S = 4.61 \cdot 10^{18} \text{ ph/s} \cdot \text{nm} \cdot \text{m}^2$ and bandwidth 1nm and detection time of 1ns. . . .	114

3.10	Galileo constellation simulated in MATLAB. The colored circles individuates three orbital planes, and the points along the circle indicate the satellites.	116
3.11	The figure shows the intra-satellite distance between a reference satellite and nine satellites positioned on a different orbital plane.	118
3.12	Simulations for different beam-size. The figure legend numbers are respectively the diameters in [m] and wavelength in [nm]: (up) trend for the intra-satellite distance [0, 60000] Km using for the Siegman's formula $W_0 = radius * 0,89$ [?]; (down) focus to the intra-satellite distance [1000, 10000] Km using the previous formula $W_0 = 2 * \frac{radius}{\pi}$	122
3.13	Simulations for different beam-size. The figure legend numbers are respectively the diameters in [m] and wavelength in [nm]: (up) trend for the intra-satellite distance [0, 60000] Km using for the Siegman's formula $W_0 = radius * 0,89$ [?]; (down) focus to the intra-satellite distance [1000, 10000] Km using the previous formula $W_0 = 2 * \frac{radius}{\pi}$	123
3.14	Simulations for different beam-size. The figure legend numbers are respectively the diameters in [m] and wavelength in [nm]: (up) trend for the intra-satellite distance [0, 60000] Km using for the Siegman's formula $W_0 = radius * 0,89$ [?]; (down) focus to the intra-satellite distance [1000, 10000] Km using the previous formula $W_0 = 2 * \frac{radius}{\pi}$	124
3.15	Figure: Simulations about key generation rate with 4 information wavelengths (350nm, 532nm, 850nm, 1550nm) and 3 telescope apertures (20cm, 30cm and 50cm). The key generation rate is reduced as the eavesdropper can perform multi-photon tagging (PNS attack). Thicker lines deal with the key generation for BB92, thinner lines deal with the key generation rate for BB84 scheme.	132
3.16	Figure: key generation rate for BB84 QKD protocol performed with decoy state scheme considering 4 wavelengths (350nm, 532nm, 850nm, 1550nm) and 3 telescope apertures (20cm, 30cm and 50cm). The decoy scheme uses mean photon number of $\mu = 0.4$ for information state, vacuum and weak decoy (with mean photon number $\nu = 0.27$).	133
3.17	The image show the relation between Mean Photon Number and QBER.	135
4.1	The figure shows the simulated SNR vs link distance for different telescope diameters and wavelengths (indicated in the legend as "diameter[m]@wavelength[nm]").	140
4.2	Working blocks for space segment and ground segment	142
4.3	The figure shows the block diagram for the B92 SaNeQKD transmitter (left) and receiver (right).	149
4.4	The image shows the laser source for B92 protocol. The polarization of the beam can still be optimized manually.	154

4.5	The figure shows the working board FPGA connected to the source breadboard. FPGA is driven the transmission of data during some tests in Thales Alenia Space, Turin in October 2013.	155
4.6	Primitive scheme about the transmitter part of SaNe-QKD.	156
4.7	The figures shows twofold aspects of SaNe-QKD interface. It works at sender for QKD and it works as beacon camera receiver for alignment issuesof SaNe-QKD OPT system. A focusing lens is positioned above the beam splitter (BST 70/30) in order to allow beacon camera use .	157
4.8	The figure shows the image of the SaNe-QKD "aerial module" positioned above OPT module. The signal coming from the source enters the interface, the telescope and is then transmitted outside. The fused module SaNe-QKD OPT is projected to be positioned on board of Galileo satellites.	158
4.9	SaNe-QKD mounted above Thales Alenia Space system. The original path have been modified and above the system it has been obtained a position for the beacon camera of OPT.	159
4.10	This figure reports the scheme of SaNe-QKD receiver. This is the primitive idea before we observed that a filter along OPT path cuts prevent 808nm to enter into SaNe-QKD. We are obliged to position APD and 808nm synchrony-path outside the module of SaNe-QKD for the test of the Proof of Concept Demonstration.	161
4.11	This figure reports the scheme of SaNe-QKD receiver. The beam enters the optical element BSS 11 and it is split in two. One part going to the Beacon camera of OPT, the second part of the beam going to the SaNe-QKD system, through the Beam Splitter, the Polarizers to the fibers.	162
4.12	This figure reports part of the SaNe-QKD receiver on the test bed mounted with the receiver interface. The polarizers and the beam-splitter are well observable at the center.	163
4.13	The figure shows the link switching sequence for satellite A1 that obtains the maximum balanced rate when only one telescope is available on each satellite. The shaded areas represent the total secret key length achievable in one period.	164
4.14	The figure shows the connectivity graph of the proposed QKD network scheme over the GNSS Galileo constellation, employing only one telescope per satellite. Red edges represent links that have a minimum distance of 6623 km, blue edges represent links that have a minimum distance of 7687 km.	165
4.15	Data frame structure. Quantum clock synchronization has been solved by a synchrony laser. Payload slots are used to send the synchronization beam between transmitter and receiver	166

- 4.16 The figure shows the secret key rate vs the number of sifted bits, for different values of the QBER. Again, dashed lines represent the optimal asymptotic bound, whereas solid lines represent the achieved rates given the finite-key analysis model described above. Here we see that there is a minimum number of sifted bits that needs to be exchanged in order to obtain a secret key and that this threshold is lower for lower QBERs. Furthermore, the asymptotic bound is approached faster, as the number of available sifted bits grows, with higher QBERs, although lower QBERs allow to obtain some secret key (non-zero secret key rate) with a lower number of sifted bits. . . 167
- 4.17 shows the number of sifted bits that must be available to the transmitter and the receiver after the transmission on the quantum layer and the sifting phase in order for them to be able to extract a secret key of the desired key length L_{key} . In particular, the dashed lines represent the asymptotic limit in the hypothesis of infinite key length, while the solid lines represent the values obtained by means of the finite-key analysis described above. Furthermore, these results assume an attenuation A_{link} of the quantum channel between -40 dB and -45 dB, and the Winnow protocol underlies the information reconciliation phase. Also the chosen information reconciliation protocol and privacy amplification parameters ensure a probability of error correction failure equal to 10^{-3} and a fraction of leaked bit of 10^{-3} , respectively. As an example, if we want to extract 2000 secret bits with a quantum bit error rate of 2 %, we need approximately 9000 sifted bits. 172
- 4.18 The figure represents the simulation for a multi-hop quantum communication between the reference satellite A1 and two satellites C7 and C6, approaching to the reference one and belonging to a same orbital plane. The blue curves represents the simulated hop between satellite A1 and C7, then the red curve represent the simulated hop between A1 and C6 satellite 173

Quantum Communication Roadmap

The following researches have to be collocated into a wider prospective, a European prospective.

As told above, European contribution in Quantum physics science and diversified branches as Quantum Information Processing and Quantum Communication (QIPQC) have been historically crucial and unprecedented, [100] [96] [39] [3] [13] and consequently many non EU countries (as United States, China, Canada,...) allocated huge funding for dedicated researches about Quantum science and applications.

ERA-pilot QIST, Qurope, QUIE2T [70] are European projects aiming at the collaboration over defined common goals, summarized into the table 1. Starting from a common objectives, it aims to collect the European developments into a unique more complex picture to coordinate and unify many national researches and studies.

The aim is to keep European researches competitive and at the cutting edge of Quantum science and technologies, under one common European umbrella of the Community research program.

According this point of view in my thesis three goals of the Qurope table 1 will be reached with the application of the Optical Quantum Communication Network to GNSS Galileo constellation:

- **Satellite Quantum Communication.** In chapter three and four will be devised and described the SaNe-QKD Quantum Communication model which permits (by the feasibility studies reported) to share secret keys between two space segments.
- **1000 kilometers of Quantum Cryptography** SaNe-QKD stays for Satellite Network with Quantum key Distribution technology and scheme. The working prototype comes from an implementation of a native B92 prototype of UniPd, Quake [?]. Besides the feasibility studies in space shows that there are the conditions for performing Quantum Cryptography over a **path > 1000 kilometers** (simulations performed for 2000, 6600 kilometers), as space keeps quite unchanged the characteristics of the transmitted mode. A proof of Concept Demonstration (Chapter 4) of free-space 400 meters is dated for late spring. Even this goal will be fulfilled
- **Multi-node Quantum Network.** The network topology of the OQCN (Optical Quantum Communication Network) for Galileo constellation considers that many connection can be performed. Even in the Proof of Concept scheme, two nodes of communications are performed: A first satellite with attenuations and relative motion approaching a second satellite. Switching test with two trusted nodes is represented in figure 4.14

Part I

Ground beam propagation

Chapter 1

Optical Links

1.1 Classical Optics

In this part we briefly recall the physical concepts necessary for beam propagation. First we will summarize optics for the telescopes, as in Quantum Communication suitable light collectors are necessary in order to gather the Quantum Information sent typically as single photon states. Fiberoptics are recalled too.

Then the treatment will follow with Gaussian beam physics as strongly attenuated lasers are the typical sources used in Quantum Communications experiments.

Finally, elements of atmospheric turbulence theory are recalled as crucial for Quantum Communication links performed through atmospheric layers: on next chapter (chapter 2) we will focus our attention on the atmospheric contribution of turbulence over a beam in free-space propagation.

Optics

According the Optics theory, the *relation for a spherical surface* between two media with n_1 and n_2 indices of refraction in paraxial approximation is given by: [43]

$$\frac{n_1}{p} + \frac{n_2}{q} = \frac{n_2 - n_1}{R} \quad (1.1)$$

with R the spherical interface radius, p position of the object and q position of the image along the optical axis.

Considering a thin lens (with thickness $d \simeq 0$ and refraction index n) in air ($n_1 = 1$) as an "intersection" of two spherical surfaces, the **Lensmaker's equation** obtained is:

$$\frac{n_1}{p} + \frac{n_2}{q} = \frac{n_2 - n_1}{R} \quad (1.2)$$

Considering the **Gaussian formula**:

$$\frac{1}{p} + \frac{1}{q} = \frac{1}{f} \quad (1.3)$$

The *focal length* f of the lens is defined as:

$$\frac{1}{f} = (n - 1) \left(\frac{1}{R_1} - \frac{1}{R_2} \right) \quad (1.4)$$

with R_1 and R_2 the radii of curvature of the lens.

- A lens is considered **convex (converging or positive)** if tends to decrease the radius of curvature of the incoming wave fronts: so it is thicker at the center and thinner at the edges. For a biconvex lens $R_1 > 0$ and $R_2 < 0$, for a planar convex lens $R_1 = \infty$ and $R_2 < 0$, for a meniscus convex lens $R_1 > 0$ and $R_2 > 0$.

- A lens is considered **concave (diverging or negative)** if tends to increase the radius of curvature of the incoming wavefronts: so it is thinner at the center and thicker at the eadges.

The trasverse (lateral) magnification M_T is the ratio of the transverse dimensions of the final image y_{im} respect to the dimensions of the object y_{obj} :

$$M_T = \frac{y_{im}}{y_{obj}} = -\frac{q}{p} \quad (1.5)$$

If $M_T > 0$ the image is erected, if $M_T < 0$ the image is inverted.

In a thin lens combination, [43][§ 5.2.3] it is defined **back focal length (BFL)** the distance from the last surface of the optical system to the second focal point of that system as a whole:

$$BFL = \frac{f_2(d - f_1)}{d - (f_1 + f_2)} \quad (1.6)$$

Moreover, in the same thin lens combination it is defined **front focal length (FFL)** the distance from the vertex of the first surface of the optical system to the first object focus of that system as a whole:

$$FFL = \frac{f_1(d - f_2)}{d - (f_1 + f_2)} \quad (1.7)$$

Recalling the relation for a mirror along the paraxial region [43] , the **mirror formula** is defined as:

$$\frac{1}{p} + \frac{1}{q} = -\frac{2}{R} \quad (1.8)$$

with $R > 0$ for a convex mirror and $R < 0$ for a concave mirror.

For an optical system, the **aperture stop** is any element (rim of lens or separated diaphragm) limiting the amount of light reaching the image. It determinates the light-gathering capabilities of the system. With the term **entrance pupil** we define the image of the aperture stop seen from an axial point on the object through those elements preceding the aperture stop itself. If no optical elements are positioned between object and aperture stop, the aperture stop itself becomes entrance pupil.

The **exit pupil** is the image of the aperture stop as seen from an axial point on the image plane through the eventually positioned interposed lenses. If such no lenses are present in the optical system, the aperture stop itself is the Exit Pupil.

The **Field Stop** is the element limiting the size or angular breadth of an imaged object, determining the *field of view* of the optical system.

The field (or angle) of view of an optical system is given by the relation

$$\alpha = 2 \tan^{-1} \frac{d}{2f} \quad (1.9)$$

with f the focal length of the system and d the detector size. As the amount of energy collected by a system is directly proportional to the area of the entrance pupil (area of the lens), the entrance pupil is proportional to the D^2 . At the other side the image area vary with the lateral dimension, which is proportional to f^2 . It is so useful define the **relative aperture** for an optical system, as:

$$A_R = \frac{D}{f} \quad (1.10)$$

The inverse of the relative aperture is known as **focal ratio (f-number)** of the optical system.

Fiberoptics and Beer-Lambert law

[71] [43] An optical fiber is a flexible and transparent cylinder, made of low loss dielectric materials (generally fused silica glass with high chemical purity).

The cladding (a transparent material) surround the core (the transparent inner part with a slightly higher index of refraction), and both are protected from the environmental by a buffer coating and a jacket.

A fiber acts as a waveguide, confining and transiting the light along the core axis by *total internal reflection*: the refraction index changing at the core-cladding boundaries keeps the light totally confined within the core, so electromagnetic waves can be guided into the fiber.

Let the refractive indexes for core, cladding and air be n_{core} , n_{clad} , n_0 respectively. So, for a considered fiber the fractional change of refractive index is

$$\Delta = \frac{n_{core} - n_{clad}}{n_{core}} \quad (1.11)$$

Because of refraction at the fiber-air boundaries, a ray -entering the fiber with an incident angle θ_{inc} - is bent according Snell law:

$$n_0 \sin \theta_{inc} = n_{core} \sin \theta_{ref} \quad (1.12)$$

With θ_{ref} the refraction angle with the fiber core axis.

If ϕ_{crit} is the complementary of the refraction angle θ_{ref} , , with $(\phi_{crit} + \theta_{ref} = \pi/2)$, then light rays satisfying the relation $\sin(\phi_{crit}) < (\frac{n_{clad}}{n_{core}})$ can be refracted into the fiber.

Moreover rays with angles larger than $\phi_{crit} = \sin^{-1}(\frac{n_{clad}}{n_{core}})$ at the core cladding boundaries, can experience *total internal reflection* and be guided within the core by multiple total internal reflections. The cone of angles larger than the critical one is called *cone of acceptance*.

For incident rays from the air into the fiber, the acceptance angle is defined by the relation: $\theta_{acc} = \sin^{-1}(NA)$, where

$$NA = \sin \theta_{acc} = \sqrt{n_{core}^2 - n_{clad}^2} = n_{core} \sqrt{2\Delta} \quad (1.13)$$

With NA the Numerical Aperture of the fiber.

Fibers support light propagation in the form of modes: each is a wave with a distant spatial distribution, polarization, propagation constant, group velocity, and attenuation coefficient. There is a correspondence between each mode and a ray that bounces with the core in a distinct trajectory.

Fibers supporting more paths through which the light can travel along the core are called *Multi Mode Fibers (MMF)*, while fibers supporting only a single-mode are called *Single Mode Fibers (SMF)*.

Fiber losses represent a limiting factor in communication science, as reducing the signal power while propagating it. The attenuation (or extinction) is the loss of intensity of a flux outgoing through a medium, and for a laser beam traveling across a fiber, the power typically decreases exponentially with the distance as result of scattering and absorption. Beer-Lambert law expresses the optical power variation dP for a signal propagating on a distance interval dz inside an optical fiber of total length z :

$$\frac{dP}{dz} = -\delta z \quad (1.14)$$

with δ the attenuation coefficient in units of km^{-1} . If P_{input} and P_{output} are respectively the input and the output power at the fiber ends, by Beer-Lambert relation, they are related by:

$$P_{output}/P_{input} = \exp(-\delta z) \quad (1.15)$$

With δ in dB/km .

In communication science the *attenuation coefficient* α is conventionally defined in units of decibels per kilometer (dB/km), according the further relation:

$$P_{output}/P_{input} = 10^{-\alpha z} \simeq \exp(-0.23\alpha z) \quad (1.16)$$

so the attenuation coefficient can be expressed as:

$$\alpha = \frac{1}{z} 10 \log_{10} \frac{P_{input}}{P_{outout}} \quad (1.17)$$

With α in dB/km .

The relation is represented in the figure 1.1 .

Telescopes

It is not clear who invented the telescope (from the Greek *telescopes*, device for seeing at a distance), but Galileo Galilei was one of the first to build a telescope using to positive lenses and an organ pipe as tube.

A telescope has the function to enlarge the retinal image of a distant object [43] .

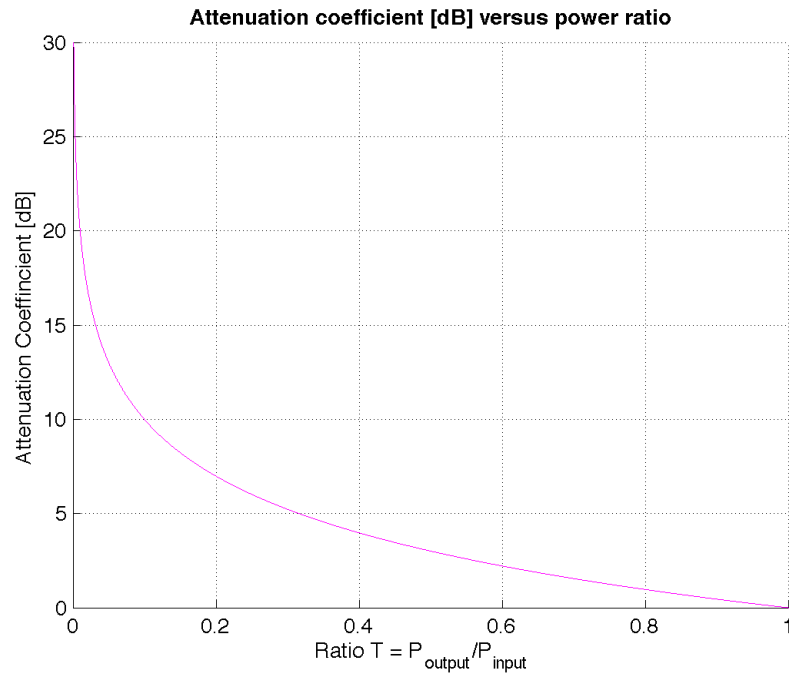


Figure 1.1: The figure shows the conversion between power ratio $P_{\text{output}}/P_{\text{input}}$ and attenuation coefficient α [dB] for a fiber of length 1km. An attenuation coefficient of 3dB corresponds to power ratio of $T = 0.5$, an attenuation of 10dB corresponds power ratio of $T = 0.1$, an attenuation of 20dB corresponds to a power ration of $T = 0.01$ and an attenuation of 30dB corresponds to a power ration of $T = 0.001$.

Refracting Telescopes

A telescope consisting of two lenses is said **afocal** (without focal length), when the two lenses are separated by a distance equal to the sum of their focal length. (In this case BFL and FFL of the configuration goes to infinity).

There are three types of telescopes.

- **Astronomical (or inverting) Telescope** . It has two positive lenses (objective and eyepiece) positioned in such a way that the second focal point of the first lens (objective) is with the first focal point of the second lens (eyepiece). For an object at infinity, the intermediate image positioned at the second focus of the objective lens is inverted as the final one.
- **Terrestrial (or erecting) Telescope**. It is an astronomical system with an erecting system usually located between objective lens and eyepiece lens. It requestes long tubes, so binocular telescopes usually use erecting prisms.
- **Galileian Telescope**. It is a constituted by an objective positive lens and a negative eyepiece lens according the relation $d = f_{objective} + f_{eyepiece}$ for afocal systems. The image is not inverted

The **angular magnification** of a telescope is defined as the ratio between the field of view in image space (the half angle of the apparent cone of rays) and object (the half angle of the actual cone of collected rays):

$$M_A = \frac{\alpha_{im}}{\alpha_{obj}} = -\frac{f_{objective}}{f_{eyepiece}} = \frac{D_{objective}}{D_{exitpupil}} \quad (1.18)$$

with $D_{objective}$ the diameter of the objective and $D_{exitpupil}$ the diameter of its image, the exit pupil. If $M_A > 0$ the image is erected, otherwise reversed.

Reflecting Telescopes

Reflective telescopes were conceived in the 17th century to allow large diameter objectives, as an alternative to refractive ones suffering mainly of chromatic aberration. here e recall the Newtonian reflecting telescope used during the experiments for "Application of Optical Quantum Links to GNSS".

Newtonian Telescope

Newtonian telescope was invented by Sir Isaac Newton in 1668.

It consists of a single concave primary paraboloid mirror and a secondary reflecting flat mirror. The single optical surface of the primary mirror creates the image, while



Figure 1.2: Example of Newtonian telescope VIXENRS200, used during the project application of Optical Quantum Links to GNSS, discussed in the second part of this thesis.

the flat one directs the light out to an accessible observing location.

Newtonian telescopes are between the world-wide most distributed telescopes for amateur astronomers; having only a parabolic mirror of complex shape, it is of much simpler fabrication and low costs than other telescope configurations (as Gregorian and Cassegrain).

In the experiments of Quantum Communications explained in the following (in chapter 3-4) we use a Newtonian telescope of 200mm of aperture with paraboloid primary mirror for the realization of the SaNe-QKD OPT prototype.

In the following figures we report the Newtonian telescope used (figure 1.2 and table 1.1) and Zeemax optical configuration design (figure 1.3 and 1.4).

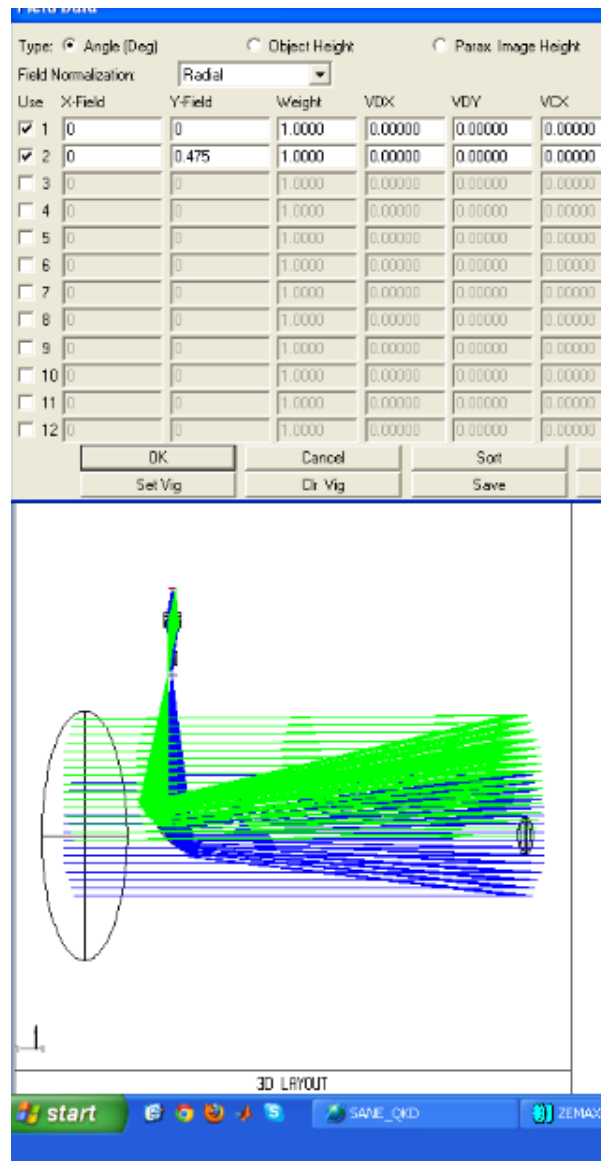


Figure 1.3: Zemax elaboration of the optical path. The Newtonian telescope VIXEN RS200 used for the Proof of Concept demonstration of the project "Optical Quantum Communication Links for GNSS". The simulation uses two fields, blue on axis, green out of axis.

Parameters	NEWTONIAN TUBE
Aperture	200mm
Focal Length	800mm
Diameter M2	54mm
Obstruction	31%
Diameter M2	54mm
Weight	5.3Kg

Table 1.1: The table shows the parameters of the Newtonian tube used for Optical Quantum Communication experiments.

Newtonian Telescope characteristics Newtonians are free of chromatic aberrations as all reflectors telescopes.

The following relations are valid for wavelengths of 550nm.

As the primary mirror of the Newtonian telescope is a parabolic one, it is free from spherical aberration when imaging distant objects: the **low order spherical aberration** of an object at infinity is given by [86]

$$W_z = \frac{(K + 1)D}{2048F^3} \quad (1.19)$$

with K the mirror conical value ($K = -1$ for our case of a parabolic mirror), D the aperture diameter, F the focal ratio.

The *RMS* wave front error for primary spherical aberration is given by:

$$w = \frac{W_z}{\sqrt{11.25}} \quad (1.20)$$

So, for a paraboloidal Newtonian telescope $W_z = 0$ and $w = 0$.

The concave mirror of the Newtonian configuration also produces **off-axis aberrations**: coma, astigmatism, field curvature and distortion.

The dominant off-axis aberration for Newtonian configuration is the coma. The astigmatism is present, but less important; the main aberration for image surface deformation is field of curvature. The distortion can be minimized positioning a stop at the telescope aperture.

If $\alpha = h/f$ the field angle (in radians), h the linear height of the image plane, f the focal length of the primary mirror, and F the focal ratio of the configuration, the **Low Order Coma** for an object at infinity is given by:

$$W_C = \frac{\alpha D}{48F^2} \quad (1.21)$$

The corresponding **Coma RMS wave front error** is

$$w = \frac{W_C}{\sqrt{32}} \quad (1.22)$$

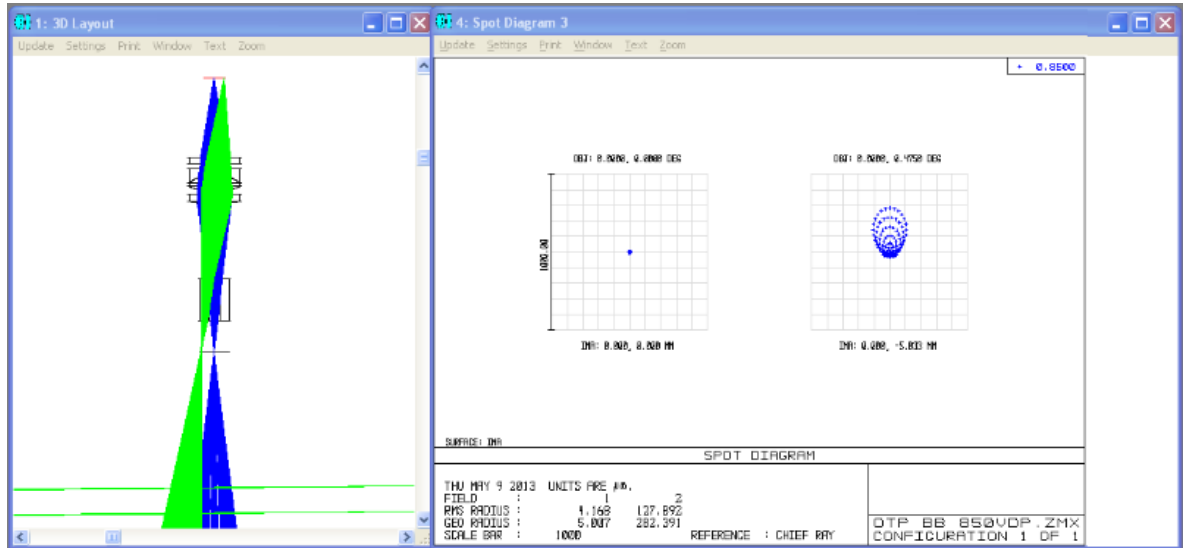


Figure 1.4: The figure shows the Zemax elaboration about the Newtonian tube at the interface between SaNe-QKD prototype and OPT (project "Optical Quantum Communication Links for GNSS"). The image shows that the field curvature is visible at the interface and the calculated RMS radius is of 4.168 μ m for the Field 1 (coaxial) and RMS radius is of 5.007 μ m for field 2 (obtained putting a Y-field offset of 0.475).

This image demonstrate that taking care of positioning a collimating lens with the right aperture at the interface between the UniPd system SaNe-QKD and the TAS system OPT, it is possible to interface the two optical systems. Note that it is present the coma pattern characteristic of off-axis images for Newtonian uncorrected telescopes

The previous relations of Low-Order Coma show that the Coma wave front error is inversely proportional to the square of the Newtonian focal ratio and decreases with the increase of it.

For our telescope

$$W_C = \frac{\alpha D}{48F^2} = \frac{h}{48F^2} = 0.26\alpha \quad (1.23)$$

If $f = 800mm$, and $h = 2.134mm$, $W_C = 0.0028$ [mm]

Low Order Astigmatism for wave front error for an object at infinity is given by:

$$W_a = \frac{-h^2}{8F^2f} = \frac{h^2}{8DF^3} \quad (1.24)$$

The corresponding RMS wave front error for the astigmatism is

$$w_a = \frac{W_a}{\sqrt{24}} \quad (1.25)$$

Finally, for our telescope the second main aberration is the astigmatism: the wave front error presents $W_a = 0.0001mm$ if $h = 2.134mm$, verifying that Coma aberration is the stronger extra-axial aberration.

Summarizing, the Newtonian telescope is free from spherical aberration, suffers severely of coma aberration, and of less intense astigmatism. The field curvature in our Newtonian telescope is present but relatively weak with no significant effect on visual observing. Coma and field of curvature for the VIXEN telescope are in figures 1.4.

Optical System	M1 Primary Mirror	M2 Secondary Mirror	Characteristics
Cassegrain	Paraboloid	Hyperboloid	Off-axis performance suffers of aberrations
Cassegrain Dall-Kirkham	Prolate ellipsoid	Sphere	Less expensive, degraded Off-axis errors
Ritchey-Cretien	Hyperboloid	Hyperboloid	Completely corrected Spherical Aberration and Coma

Figure 1.5: Figure showing some Cassegrain telescopes with type of mirror and characteristics

1.1.1 Dall-Kirkham Cassegrain Telescope

A Cassegrain (figure 1.5) is a telescope with a concave primary parabolic mirror and a convex hyperbolic secondary mirror in order to enlarge the focal length in a more compact configuration.

"Reef" (figure 1.6) is Dall Kirkham Cassegrain telescope with a spherical secondary mirror, used for tests, as laboratory support during the arrangement of the Canary Telescope for Ground beam propagation analysis.

For a Cassegrain configuration, if f is the Effective Focal Length EFL (the focal length of the system), f_1 the focal length of the primary (positive if concave), f_2 the focal length of the secondary (negative if convex), D_1 and D_2 the diameters of the primary and the secondary mirrors then the **secondary mirror aperture** is given by:

$$D_2 = D_1 \left(1 - \frac{d}{f_1}\right) = \mathbf{mf}_1 \quad (1.26)$$

and the **Effective Focal Length** f is:

$$f = \frac{f_1 f_2}{f_1 + f_2 - d} = \mathbf{mf}_1 \quad (1.27)$$

$\mathbf{m}$ is the **secondary mirror magnification**, given by the ratio between the effective focal length of the system and the focal length of the primary mirror:

$$\mathbf{m} = \frac{\mathbf{EFL}}{f_1} = \frac{f}{f_1} \quad (1.28)$$

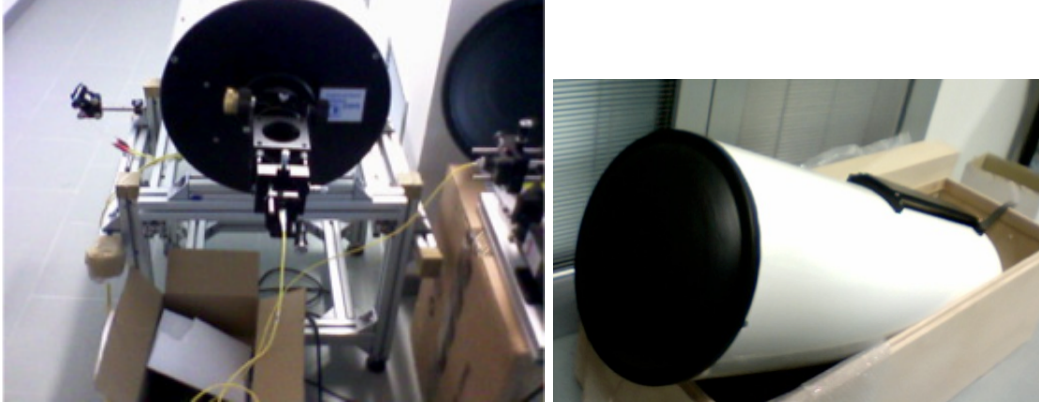


Figure 1.6: "Reef" Dall Kirkham Cassegrain telescope used as support for laboratory with the Canary Telescope

The *Back Focal Length (BFL)* for the Cassegrain configuration is given by the relation:

$$\mathbf{BFL} = \mathbf{d} + \mathbf{b} = \frac{(\mathbf{f}_1 - \mathbf{d})\mathbf{f}_2}{\mathbf{f}_1 + \mathbf{f}_2 - \mathbf{d}} \quad (1.29)$$

with b distance between Cassegrain focus and the primary mirror, d the distance between the two mirrors in the telescopes. Note that m and f are both positive in a Cassegrain configuration.

1.1.2 Canary Telescope

The "Canary Telescope" is a custom telescope used to investigate strongly-turbulent optical links in Canary Islands [19]. The scenario for performing such experiments was chosen between the Optical Ground Station (OGS) of the European Space Agency (ESA) in Tenerife and the Jakob Kapteyn Telescope (JKT) in La Palma Island, separated by about 143 km, both the sites above 2400m a.s.l.

We realized link-experiments using an optimized refracting transmitter, whose key component is the Zen singlet aspheric lens of 23 cm diameter, 220 cm focal length, F/9.5, manufactured by the Venetian *Officine Ottiche Zen*. Zemax optical configuration about the Zen lens are in figures 1.8 (surface characteristics and distortions) and 1.9

The Zen lens presents chromatic aberration: the focal lengths at different wavelengths are reported in table 1.2 . Two aspheric Thorlabs lenses (350420 and 350280) are then positioned at the first focus of the Zen Lens and the system is analyzed for 532nm and 808 nm in figure 1.10.

A first arrangement of the "Canary telescope" has been tested in Asiago Observatory



Figure 1.7: With Ivan Capraro and Paolo Villoresi during tests of the Canary telescope at Asiago observatory (Italy) in April 2011, while performing a beam propagation experiment between Asiago and Monte Grappa (Italy).

<i>Wavelength</i>	Focal Length [cm]
532nm	216.42
632nm	218.26
819nm	220.21

Table 1.2: Table about different focal lengths for test wavelengths.

during a beam propagation experiment to Monte Grappa in April 2011. Figure 1.7 .

The arrangement of the Canary Telescope

The telescope arrangement consists of three aluminum flanges aligned by four pipes (figure 1.11): the first flange is connected to a stabilizer, on the second it is placed the optical breadboard and the third flange holds the Zen lens.

The telescope orientation is achieved with two screws connected to the first flange in order to achieve easily the requested pointing; a XY stage was positioned at the third flange to move the telescope, too.

The laser sources were two. A 532nm laser coupled into fiber (40mW measured output power) and an 808nm IR diode laser coupled into fiber (6mW measured output

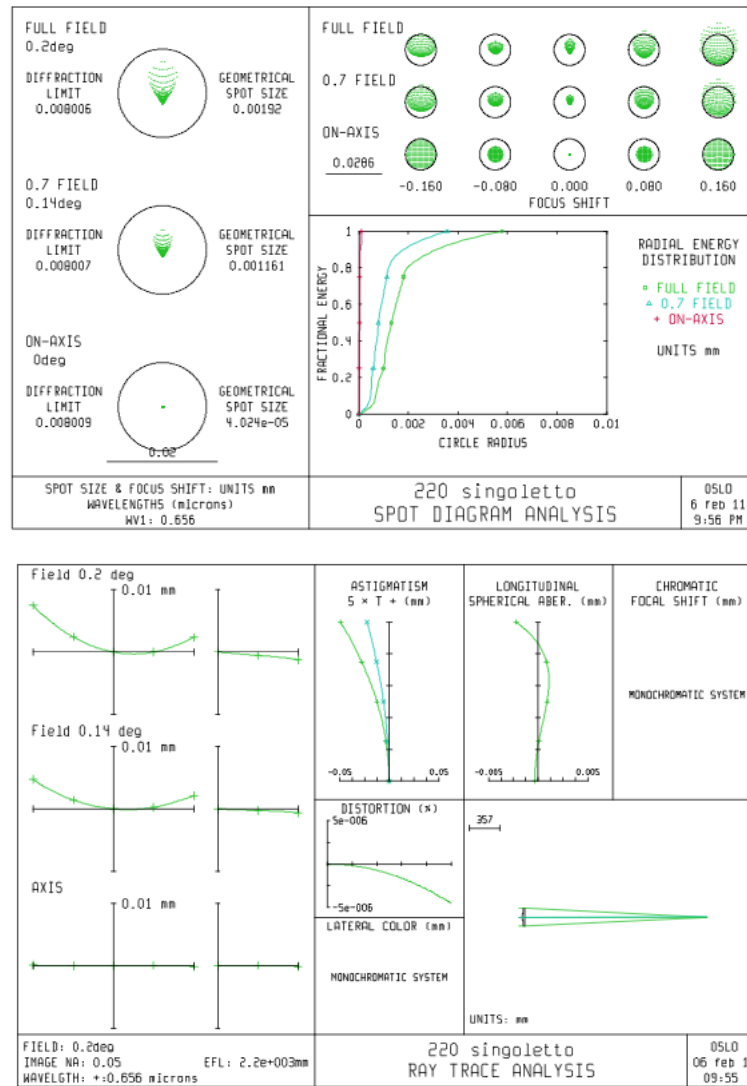


Figure 1.8: Zemax simulation of the Zen lens.

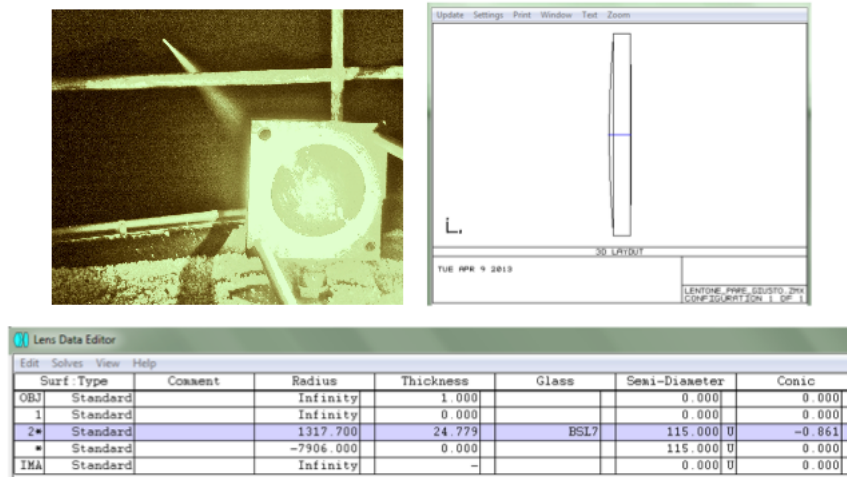


Figure 1.9: Image of Zen lens mounted on the Canary telescope and in Zemax elaboration

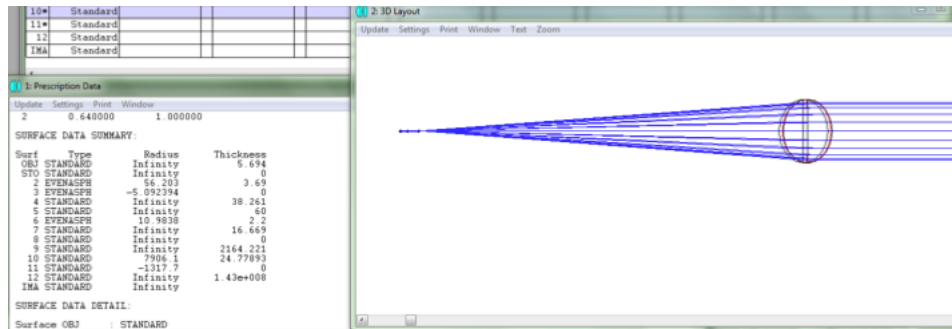


Figure 1.10: Desktop images of Zemax software elaboration for the Canary Telescope. It uses 2 aspheric Thorlabs lenses (350420 and 350280) positioned at the first focus of the Zen Lens. The system is analyzed for 532nm and 808 nm.

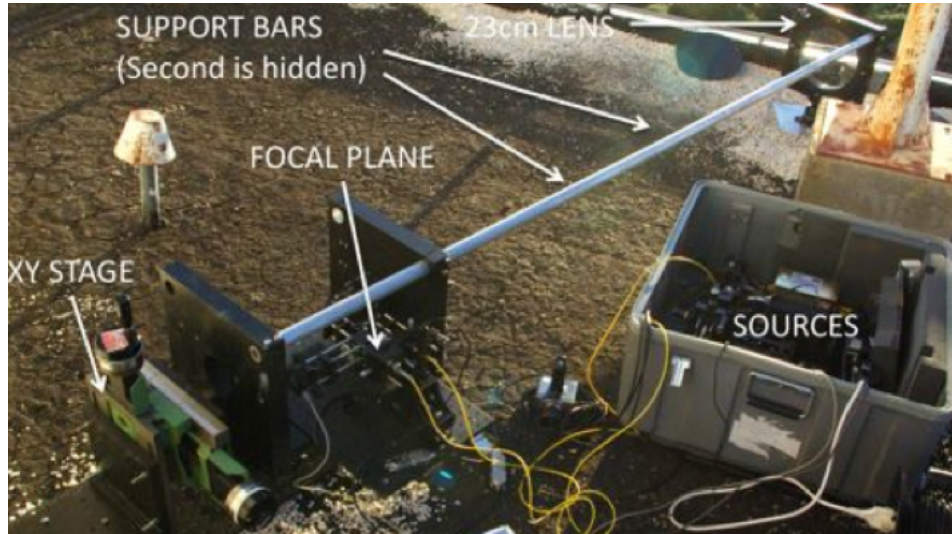


Figure 1.11: The figure shows the telescope in September 2011 in La Palma site for some nights of ground beam propagation experiments between La Palma and Tenerife.

power).

The laser sources have been aligned in order to share the output optical axis by a dichroic mirror, so the 532nm (Green) laser could be used for alignment issues and then switched off.

As told above, chromatic aberration is present: green and infrared wavelengths present two different focal lengths we need to be compensated by suitable lenses (figure 1.10). In the optical arrangement at the focal plane a CCD camera is positioned and a further 532nm Beacon Laser (150mW) sent during the experiments between OGS site (Tenerife) to Canary Telescope in JKT site (La Palma) for performing beam correction issues.

A *beam correction* is necessary in order to try to compensate all the atmospheric contributions due to the turbulence along the communication link between the two Islands. It was achieved in two ways during the experiments: A 532nm laser (called Green Beacon in the figure 6.2) is sent from the OGS observatory (RECEIVER) to the JKT (TRANSMITTER) and acquired in JKT site (travelling along approximately the same path of the Red and Green laser from JKT (figure). The Green Beacon signal is received by the CCD camera in the SENDER site (figure 1.12), and the acquired spot positions are sampled and averaged, in order to feed data to the control software, which apply calculated correction movements to the fine XYZ control stage of the Canary telescope, in order to compensate the slow drifts in beam directions (actions indicated by red arrows below).

In this way, by the real time analysis of the received Beacon laser deviations observed

at the CCD camera in SENDER site, it is possible to compensate immediately the turbulence contribution on the IR communication laser outgoing from the Canary telescope.

It is necessary to highlight that this beam correction strategy assumes that, along the same path, turbulence contributions in free space are about symmetric according the short time acquisitions of the CCD camera and the time delay of pointing correction.

A further correction system is based on the Thorlabs CCD camera positioned at OGS (RECEIVER site, figure 1.12), at the Coude focus of the telescope. A dichroic mirror divides the optical beams entering into two parts: the IR path for quantum communication acquisition issues is transmitted, the green path is reflected by the dichroic mirror and focused by optical elements at a Thorlabs camera. In real time a computer elaborates the received images, calculating the positions of the received laser spots, sending the error signals to the sender site (JKT) by a VPN connection. The Canary telescopes is then correct in real time by moving the fine XY stage accordingly.

This control strategy needs the beacon laser propagating in the same direction of the quantum signal.

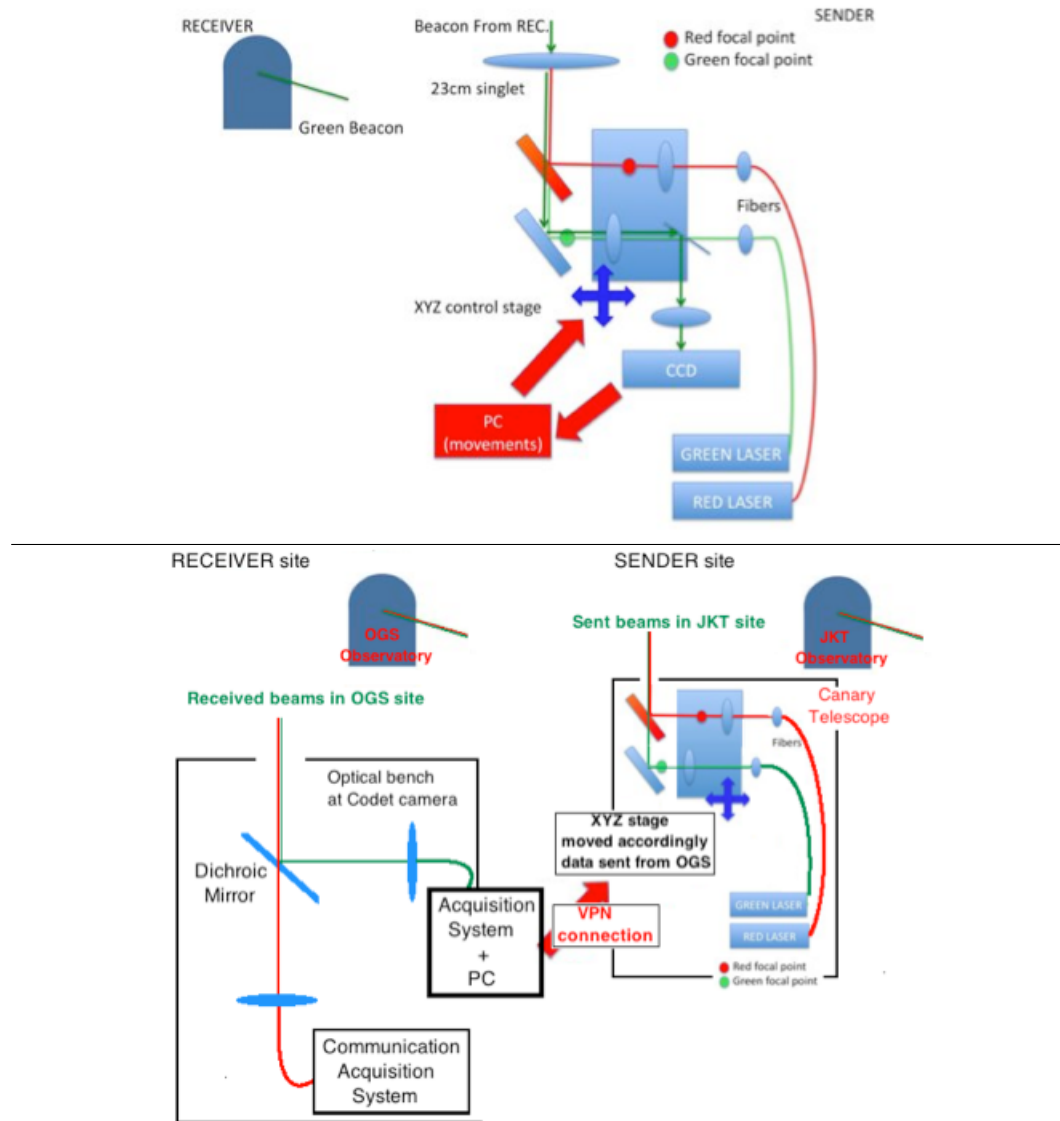


Figure 1.12: Figure (Up): Arrangement of the experiment of communication at the transmitter and at the receive showing the beam correction explained in point 1. Figure (Down): arrangement of the experiment of communication at the transmitter and at the receive showing the beam correction explained in point 2.

1.2 Gaussian Beams

1.2.1 LASERs

The LASER is a Quantum-device that produce light taking advantage of the way in which the atoms in medium interact with the electromagnetic radiation.

The physical principle [71] [83] of the **stimulated emission (SE)** allows a photon in a given mode to induce an atom, whose electron is in an upper energy level, to undergo a transition to a lower energy level and to emit a clone photon into the same mode of the initial photon.

The emitted clone photon has the same frequency, direction and polarization of the initial one. These two photons in turns serve to stimulate the emission of additional photons, and so on, while preserving these properties.

The result is a coherent light amplification.

Because the stimulated emission occurs only when the photon energy is nearly equal to the atomic transition energy difference, the process is restricted to a band frequencies determined by the atomic linewidth.

LASERs are devices that generate coherent light based on the physical principle of the stimulated emission discovered by Einstein in 1916.

The word *LASER* is an acronym for **Light Amplification by Stimulated emission of Radiation**.

The term *light* is here used in a broad sense, including radiation at frequencies in the Ultra Violet, Visible and InfraRed regions of the electromagnetic spectrum.

The three crucial elements of a *LASER* are:[83]

1. The amplifying medium (GAIN) consisting of charged carries with a pumping mechanism to excite these species to their higher energy states. The energy stored in the excitation can be emitted as light spontaneously or stimulated by pre-existing light leading to an amplification of light energy.
2. A suitable arrangement of optical elements (lens, mirrors, prisms,..) or some other mechanism to allow multiple passage of light through the gain medium.(feedback)
3. A loss mechanism to extract light energy from the device.

1.2.2 Gaussian Beam

[71] [80] A monochromatic wave $\Omega(\mathbf{x}, t) = U(\mathbf{x}) \exp(i\omega t)$ satisfies the wave equation if U satisfies the Helmholtz equation:

$$(\Delta - \frac{\delta^2}{c^2})U = 0 \quad (1.30)$$

that is, for $k = \frac{2\pi\nu}{c} = w/c$ wavenumber

$$(\Delta + k^2)U = 0 \quad (1.31)$$

with ν the wave frequency, c speed of light.

If we define $U(\mathbf{x}) = A\mathbf{x} \exp(-ikz)$, the Helmholtz equation becomes

$$\Delta_T A + \frac{\delta^2 A}{\delta^2 z} - 2jz \frac{\delta A}{\delta z} = 0 \quad (1.32)$$

Considering the paraxial approximation:

$$\left| \frac{\delta^2 A}{\delta^2 z} \right| \ll \left| 2k \frac{\delta A}{\delta z} \right| \quad (1.33)$$

The Helmholtz equation becomes:

$$\Delta_T A - 2jk \frac{\delta A}{\delta z} = 0 \quad (1.34)$$

The **Gaussian beam** is a solution of the wave equation in the paraxial approximation.

It is defined by the wave function:

$$U_w(x, t) = A_w(x) \exp[jw(t - \frac{z}{c})], \quad (1.35)$$

with

$$A_w(x) = \frac{A_1}{q(z)} \exp[-jk \frac{\rho^2}{2q(z)}], \quad (1.36)$$

$$\rho^2 = (x - x_0)^2 + (y - y_0)^2 \quad (1.37)$$

and

$$q(z) = z + jz_0 \quad (1.38)$$

The quantity $q(z)$ is called the **q-parameter** of the beam, while the z_0 is called **Rayleigh range**.

Two new functions are introduced by the following relation:

$$\frac{1}{q(z)} = \frac{1}{R(z)} - j \frac{\lambda}{\pi W^2(z)} \quad (1.39)$$

$R(z)$, the wave front curvature radius, and $W(z)$ the beam width at a generic z .

Finally, the crucial beam parameters for a Gaussian beam are summed up in the following four equations:

$$W_0 = \sqrt{\frac{\lambda z_0}{\pi}} \quad (1.40)$$

$$W(z) = W_0 \sqrt{1 + \left(\frac{z}{z_0}\right)^2} \quad (1.41)$$

$$R(z) = z \left[1 + \left(\frac{z_0}{z}\right)^2\right] \quad (1.42)$$

$$\zeta(z) = \arctan \frac{z}{z_0} \quad (1.43)$$

$\zeta(z)$ is the Guoy phase, while $2W_0$ is the spot size.

Gaussian Beam

The Gaussian beam [71] is the most frequent experimental condition.

The Gaussian beam optical intensity $I(\rho) = |U(\rho)|^2$ - with $U(\rho)$ the electric field - is a function of the axial position z and the radial position $\rho = \sqrt{x^2 + y^2}$.

For any value of the propagation axis z the beam intensity is a Gaussian function of the radial distance ρ , given by the following relation:

$$I(\rho, z) = I_0 \left[\frac{W_0}{W(z)} \right]^2 \exp\left(-\frac{2\rho^2}{W^2(z)}\right) \quad (1.44)$$

On the beam propagation axis ($\rho = 0$), the intensity (described by the previous relation) is reduced to

$$I(0, z) = \left[\frac{I_0}{1 + \left(\frac{z}{z_0}\right)^2} \right]^2 \quad (1.45)$$

The beam width $W(z)$ of the Gaussian distribution increases with the axial distance z .

At $\rho = 0$ the Gaussian function has a peak on the z axis, and decreases monotonically as ρ decreases.

Beam Width

The beam intensity assumes its peak value on the beam axis at any transverse plane, and decreases by a factor $1/e^2$ at the distance $\rho = W(z)$. the quantity $W(z)$ is called beam radius.

The relation of the beam width on z is given by:

$$W(z) = W_0 \left[\sqrt{1 + \left(\frac{z}{z_0}\right)^2} \right] \quad (1.46)$$

The beam waist W_0 is known as the *waist radius* and is the minimum value by $W(z)$, at the plane $z=0$. The waist diameter $2W_0$ is also called spot size. The beam width

increases monotonically with z and assumes the value $\sqrt{2}W_0$ at $z = \pm z_0$

Beam Divergence

For $z \gg Z_0$, the previous relation becomes

$$W(z) = \frac{W_0}{z_0} = \theta_0 z \quad (1.47)$$

with θ_0 is the half angle at which the cone of the beam diverges.

Depth of focus

Since the beam achieves its best focus at the plane $z = 0$, it has its minimum width at $z = 0$.

We define the *depth-of-focus* or the *cofocal-parameter* as the axial distance within which the beam width is no greater than a factor of $\sqrt{2}$ time its minimum value, (at this distance the area is within a factor of 2 of the maximum).

1.3 Atmospheric models and turbulence effects

The atmospheric turbulence is a critical issue in optical link experiments. From Kolmogorov turbulence theory, to Hufnagel-Valley model, to scintillation theory, crucial concepts will be focused in the following sections, recalling the main features about turbulence topics, in order to create a knowledge base for a best interpretation of the next chapter. [94] [45]

Kolmogorov turbulence model

Light propagation in atmosphere (for visible and IR wavelengths) experiences several phenomena, mainly:

- Absorption and scattering by air molecules
- *Clear air turbulence* inducing phase fluctuations, focusing and defocusing effects, local deviation in the direction of the electromagnetic propagation, scintillation (signal intensity fluctuations).

Owing to temperature and density variations in air atmosphere, the refractive index varies in random fashion in space and time, causing clear air turbulence effects. Considering the atmosphere as a fluid in continuous flow, the ratio between the fluid inertial forces and viscous forces is given by the Reynolds number,

$$Re = \frac{V_{scale} L_{scale}}{\nu} \quad (1.48)$$

with V_{scale} the characteristic velocity scale, L_{scale} the length scale, ν the kinematics viscosity. It permits to classify the nature (regime) of the flow: if laminar, the flow is stable, if turbulent, the flow becomes chaotic.

According Kolmogorov model small variations in temperature ($< 1^\circ C$) produce changes in wind velocity (**eddies**); so it is possible [51] [52] to describe the turbulent regime on the hypothesis that kinematic energy associated with large eddies is redistributed without loss to eddies of smaller size, until finally dissipated by viscosity.

The structure of turbulence according Kolmogorov theory is divided in three ranges:

- the *input range* characterized by bigger dimension eddies (L_0), and it represents the step when energy is injected into the turbulence and it depends on local conditions.
- the *dissipation range* which is characterized by smaller dimension eddies ($l_0 \ll L_0$). The energy is dissipated as heat and the viscosity energy losses dominates.

- In the *inertial sub range* the turbulent energy is transmitted from bigger dimension eddies L_0 to smaller dimension eddies l_0 .

In the inertial subrange, for a statistically homogeneous medium in turbulent regime, the *longitudinal structure function of wind velocity* between two observational points r_1 and r_2 at distance r is:

$$D_\nu(r_1, r_2) = \langle [\nu(R_1) - \nu(R_2)]^2 \rangle = C_\nu^2 R^{2/3} \quad (1.49)$$

with $l_0 \ll R \ll L_0$ and C_ν the **structural constant of the wind velocity**, indicating the strength level of the turbulence.

Moreover, the *three dimensional power spectrum of wind velocity* is given by:

$$\Psi_\nu(\chi) = 0.033 C_\nu^2 \chi^{-11/3} \quad (1.50)$$

with $\frac{1}{L_0} \ll \chi \ll \frac{1}{l_0}$.

In refractive index terms, according the Gladstone relation:

$$n - 1 \approx 79 \cdot 10^{-6} \frac{P}{T} \quad (1.51)$$

with T the Kelvin temperature and P the atmospheric pressure, the structure function of the refractive index is given by:

$$D_n(n(r)) = \langle [n(R_1) - n(R_2)]^2 \rangle = C_n^2 R^{2/3} \quad (1.52)$$

with $l_0 \ll R \ll L_0$ and C_ν and C_n^2 the **index of refraction structure parameter** indicating the strength of the turbulence.

C_n^2 is related to the **temperature structure parameter** C_T^2 by the following relation:

$$\left[\frac{n-1}{T} \right]^2 C_T^2 = C_n^2 \quad (1.53)$$

Refractive index structure parameter

The crucial parameter in turbulence theory is the Refractive index Structure Parameter, which depends on the site orography, location, altitude, time of day, season,... It is not a constant value: close to the ground, the largest temperature gradients associated with largest values of atmospheric pressures (and so air density), usually bring the refractive index structure parameter to high values.

At high altitudes, the decreasing temperature gradients (and so air density) usually bring the refractive index structure parameter to lower values. During the day, the refractive index structure parameter is usually stronger at noon, due to Earth surface

heating, while during the night it is usually expected lower.

Typical value for weak Refractive index Structure Parameter at ground level are expected as little as $10^{-17} \text{ m}^{-3/2}$, while in strong turbulence regimes, are expected values of $10^{-13} \text{ m}^{-3/2}$ or larger.

Considering short horizontal links, the refractive index structure parameter could be considered quite constant, instead for ground-space links the path crosses different layers in totally different conditions of temperature gradient, air pressure and density along the altitude.

A large number of parametric models have been formulated in order to describe the profile of the refractive index structure parameter $C_n^2(h)$. One of the most used is the **Hufnagel-Valley profile**, given by the following relation: [95]

$$C_n^2(h) = 0.00594 \left(\frac{\nu}{27}\right)^2 (10^{-5}h)^{10} e^{-\frac{h}{1000}} + 2.7 \cdot 10^{-16} e^{-h/1500} + A_0 e^{-h/100} \quad (1.54)$$

with h the altitude [m], A_0 the turbulence strength at the ground level, ν the wind correlation factor at high altitude [m/s].

The wind correlation factor is expressed by:

$$W = [(1/15km) \int v^2(h)dh]^{1/2} \quad (1.55)$$

this relation is valid in a range between 5 and 20 kilometers.

For the wind velocity can be used the Bufton model

$$v(z) = 5 + 30 \exp[-((z - 9400)/4800)^2] \quad (1.56)$$

where z and v are expressed in [m] and [m/s].

Below it is reported a wind velocity profile as a function of the altitude (Figure 1.14 (right)).

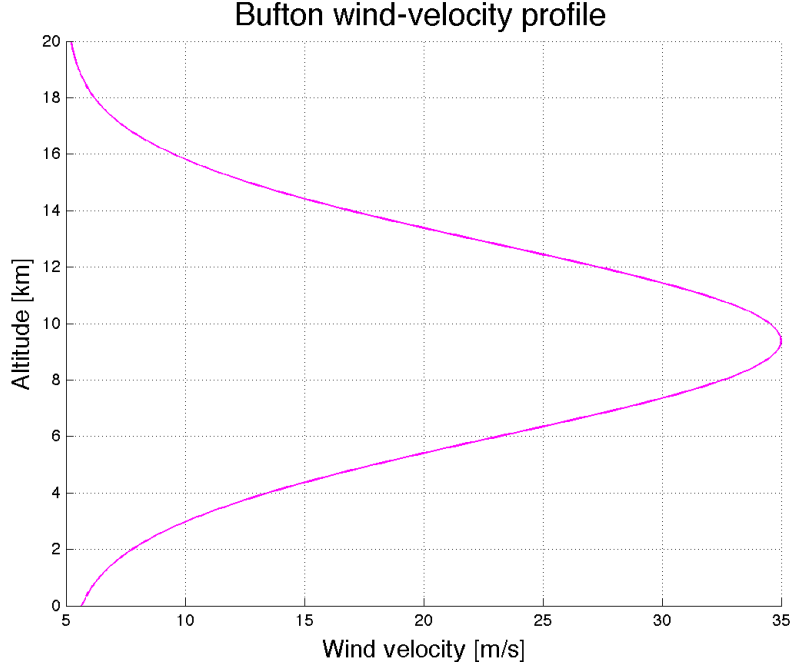


Figure 1.13: The figure shows Bufton velocity profile

The turbulence intensity is represented via the structural constant of the refractive index C_n^2 . Typically, in day-time, the *HV* model (*HV*5/7) is performed with $A_0 = 1.7 \cdot 10^{-14} \text{ m}^{-2/3}$ and $\nu = 21 \text{ m/s}$, realizing conditions for atmospheric coherence of 5cm and isoplanatic angle of $7 \mu\text{rad}$ at a wavelength of 500 nm .

Turbulent effects

Optical quantum links in free space are prone to the many channel impairments, since the information to be transmitted and retrieved is encoded into some quantum state (e.g., polarization) of only a few photons.

The physical effects observed on the optical beam propagating through the atmosphere are:

- *Beam wander* which occurs when a laser beam is refracted by an eddy with size larger than the beam diameter, causing a displacement of the beam center.
- *Short term beam spread* is due to the laser beam being refracted by an eddy smaller than the beam diameter. The short-term beam spread is an additional spread with respect to the standard spread due to the free space laser beam propagation (without turbulence effects).

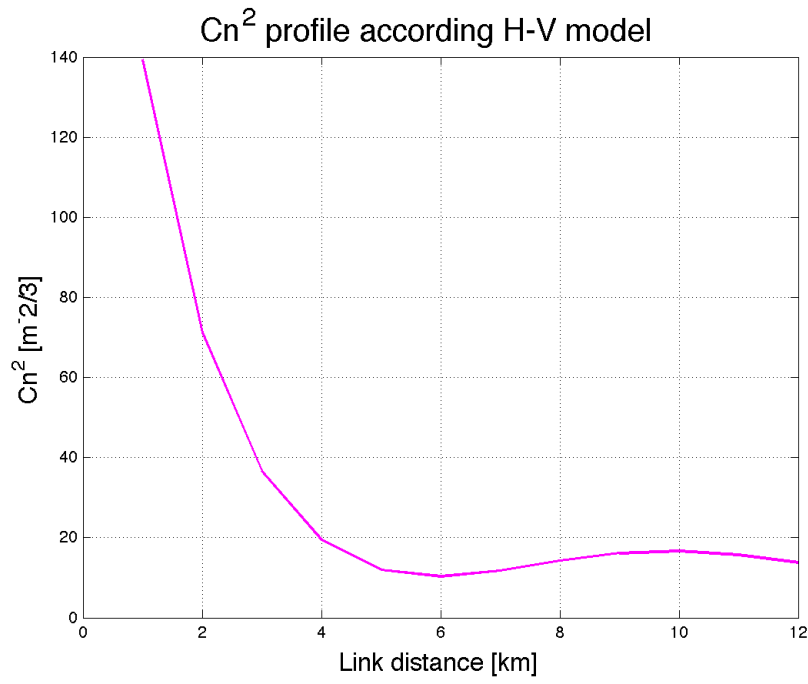


Figure 1.14: The figure reports a Hufnagel Valley profile: the relation between C_n^2 [$m^{-2/3}$] and the altitude h [km]

- *Long term beam spread* is the combination of the beam wander and the short-term beam spread leads to the long-term beam spread. The notation “long term” refers to the observation time that is much longer than for the “short term” beam spread. While the short-term beam spread represents the additional broadening at a certain instant, the long-term beam spread represents the area where at least 84 % of the intensity will be, as long as the turbulent environment parameters do not change. For the system loss calculations, the short term beam spread radius is more important than the beam wander, as the displacement of the beam center can be compensated by fast tracking systems but the short term turbulent spreading of the beam cannot.
- *Scintillation* the wave front is disturbed when it passes through turbulence, which leads to local changes of the electric field phase. When the wave impinges on the receiver, different parts of the wave interfere, resulting in a non-uniform distribution of the intensity that fluctuates about its average value. These spatial and temporal fluctuations in received irradiance are called scintillation.

Chapter 2

Ground Links

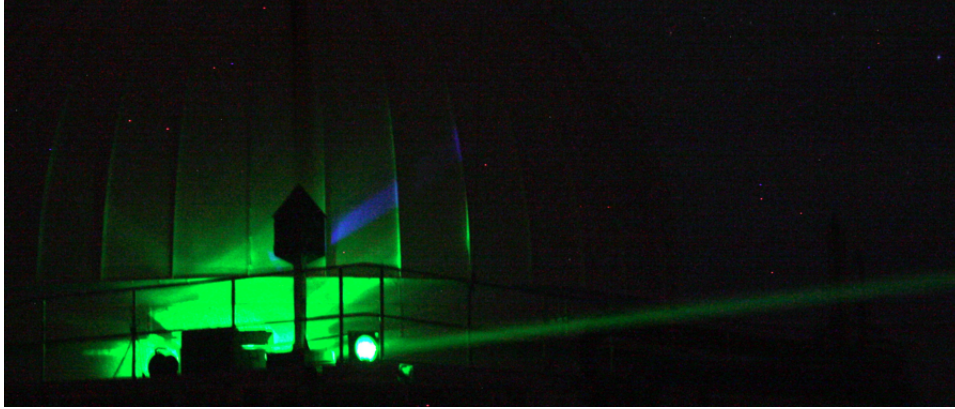


Figure 2.1: Canary telescope at JKT site, in La Palma pointing to OGS telescope, Tenerife.

The turbulence introduces on a propagating beam two contributes according the eddies size [51] [52]

- Beam wandering, which occurs when a laser beam is refracted by eddies with size larger than the beam diameter, causing a displacement of the beam center (centroid).
- Beam spreading, which is due to the laser beam being refracted by eddies smaller than the beam diameter.

The short-term beam spreading is additional respect to the standard spread due to the free space laser beam propagation (without turbulence effects).

These effects appears in relation to the exposition time: on short time scales the beam wandering is the dominant effect, while on long time scales the beam spreading is the dominant effect.

The atmospheric turbulence acts as a temporal and spatial variation of the air index of refraction. In particular, the losses on the transmitted photons are enlarged in a turbulent channel owing to beam wandering of the beam centroid or to scintillation [30], [31], [32], [24], [85]

To improve the communication quality and eventually the free space feasibility for ground-ground and space-ground links, it appears critical the understanding of the propagation effects induced by turbulence at the receiver and the temporal statistics of the collected photons, [100], [12].

Following these considerations, in this part we study the propagation of a free-space optical link over 143 kilometers between the Canary Islands Tenerife and La Palma [96] [33] reporting about the transmission, detection and optimization of the experiment.

The transmitter point was positioned at La Palma site at the Jacobus Kapteyn Telescope site and the receiving site at the OGS (Optical Ground Station) telescope at Tenerife.

The campaign was performed between the 17th and 25th September 2011.

The experiments had some aims:

- Testing the stability and pointing procedure for the optical system (Canary telescope) in order to perform quantum communication experiments over 143 kilometers between Tenerife and La Palma. The telescope arrangement is reported in chapter 1 section 1.1.2)
- Investigation about the effects of the atmospheric turbulence over long distance optical and near infrared links with the goal of understanding the optical beam parameter spoiling; estimating the link losses in order to characterize the channel and get data on turbulence and link properties.
- Check the pointing control based on the beacon beam coming from OGS site (two co-propagating beam technique, one used as reference for the single photon beam)

The link stabilization had been induced by the application of the technique of two co-propagating beams allowing to perform an effective communication link (avoiding any lost of the signal).

In order to investigate the feasibility of two co-propagating beams, the "Canary Telescope" had been first tested (one night in April 2011) for a point to point link experiment over 20 kilometres between Asiago Cima Ekar and Monte Grappa (Italy). According the previous images 1.1.2 of the telescope arrangement, figure 2.5 shows how a link experiment had been performed using two co-propagating coherent beams, with the aim of investigating the mutual displacement and wavefront transformation introduced by the turbulence.

Co-propagating beam: beacon control

The beacon for link stabilization issue was positioned at OGS site (on a little aperture) to JKT site: it worked as a pointing channel probe

It was recorded (after 143 kilometers of free space propagation) by a camera positioned along the focal plane of the Canary telescope, doing the opposite optical path of the information laser.

The information laser was an infrared beam transmitted from the JKT to the OGS telescope and measured at the Coude camera of OGS telescope in real time. The beacon laser is acquired with a complementary metal oxide semiconductor camera placed on the movable platform after the DM transmission.

The centroid of the beacon spot on the camera determines the correction on the outgoing IR laser by means of an error signal with respect to the reference position and the position of the spot at the camera is sampled about once a second and

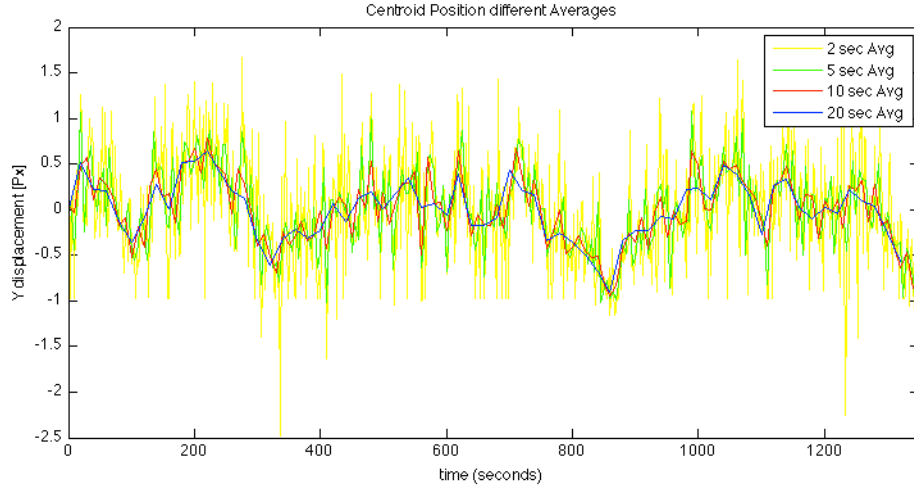


Figure 2.2: Centroid Position night 19th – 20th 8:01 am. Averages at different times in order to eliminate the effect of short term turbulence.

averaged for a number of frames; these data feed a control software that calculates the movement for the fine XY stage in order to compensate slow drift in the beam direction.

This scheme is based on the idea that the beacon laser arriving from OGS finder had spot dimensions that we expected similar to that the infrared spot at OGS site. The spot of the beacon at JKT was about 2 meters.

The analysis of the beacon signal and control system was scheduled only for the last night of the whole campaign. However, the calibration data were useful to understand pros and cons of such a control system, when compared with the collected power at OGS, even if the night weather turned foggy. Figures 2.3 and 2.4 show a correspondence between the average plot recorded in JKT, and the signal recorded by a power meter at OGS site. In figure 2.2 there are different averages of the beacon to overcome the atmospheric turbulence scintillation.

Finally, we can observe a strong correlation between the collected power and the position of the centroid distance (from best position).

There is indeed a strong dependence from the Y direction: it was observed such a dependence during all the nights, since the most frequent manual correction was done in that direction; during sunrise more stable time intervals were for the signal beam with a dependence almost all related to the Y axis. In conclusion, it is feasible in real time to counterbalance the propagation in free-space of the information beam, using a real-time probe analysis between receiver and transmitter.

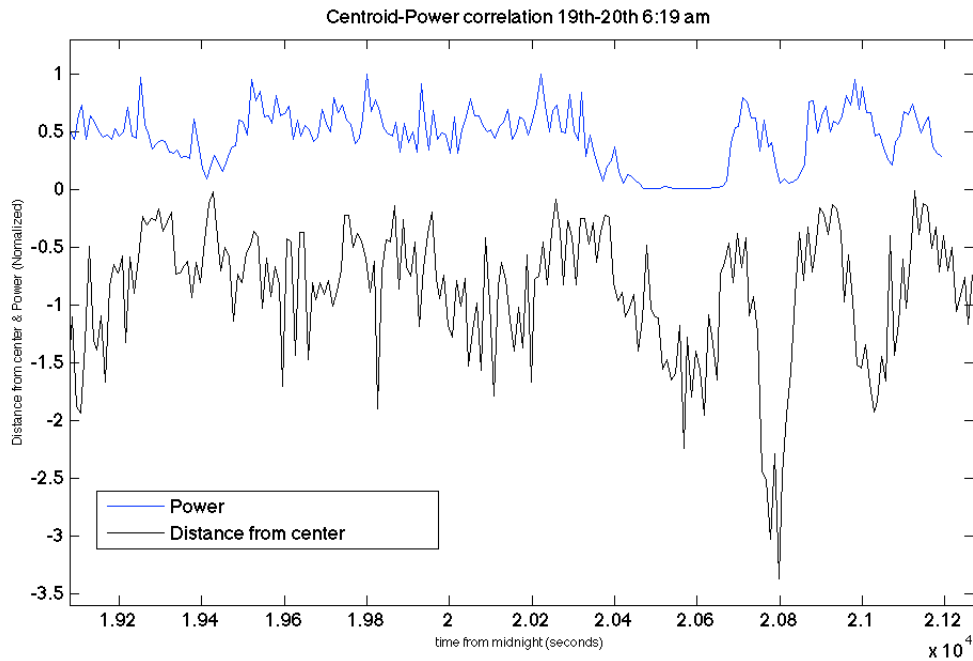


Figure 2.3: Centroid distance from center (with minus sign) with respect to the collected power at OGS night 19th – 20th 6:19 am. It is shown that the collected power is nearly completely zero with a moment of about 2.5 pixels. From the system calibration it turns out that the focal spot moves of about $3\mu\text{m}/\text{pixel}$ corresponding to a displacement of about 70cm at OGS compatible with the observations.

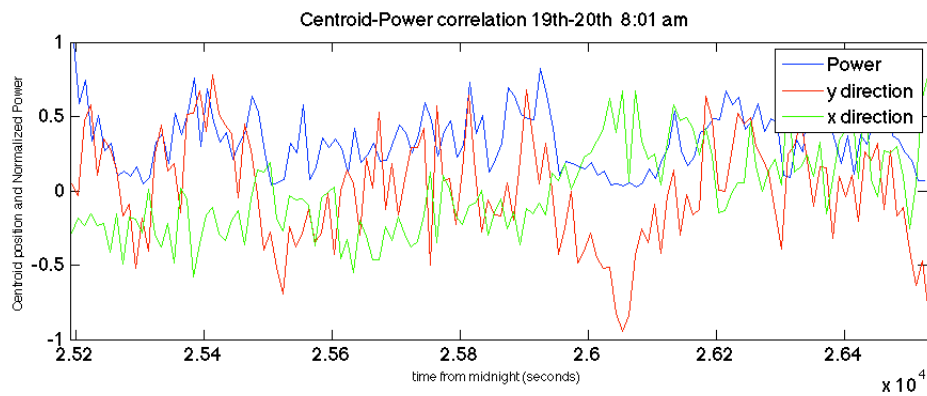


Figure 2.4: Centroid Position X and Y with respect to the collected power at OGS night 19th-20th 8:01 am.

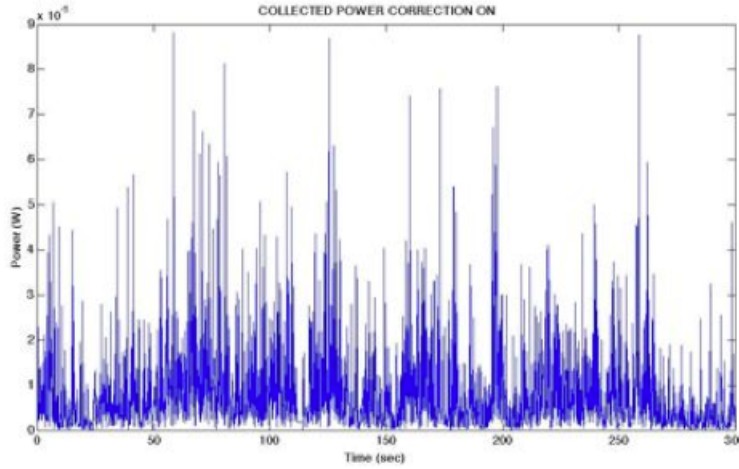


Figure 2.5: Images of power collected continuously by the co-propagating beam techniques.

2.1 Impact of turbulence in long range communication

The key element of the "Canary telescope" (section 1.1.2, figure 1.12) is the Zen lens, whose diameter is significantly greater than the estimated Fried parameter r_0 [36]. The basic idea is to acquire a beam spot similar to that reached at the primary mirror of the OGS telescope primary mirror, enhancing the power transfer between the two sites.

The optical arrangement had been previously implemented in Asiago-Grappa link in order to better stabilize it with a new XY stage with defining the Z direction as the optical axis of the system, able to move all the telescope (2.5m) in the XY plane. In the communication experiments two laser sources are used: a green source (532nm) coupled into fiber with a total output power of about 40mW; an infrared (IR) diode at 808 nm coupled into a single mode fiber with an output power of about 6 mW and suitable attenuators.

A dichroic mirror (DM) reflecting the 808 nm radiation had been introduced for alignment purposes, as the two sources shared the output optical axis by means of a mirror and a dichroic window. In this way the green laser can be used for a raw alignment and swathed off in a second moment if the IR needs to be operative.

The focal plane that comprises the focusing lens, the collimating lens and the fiber port for both green and IR can be moved by a fine XYZ system based on stepped Thorlabs motors. In this way the beam can be slightly steared by moving the focal spot at the singlet focus.

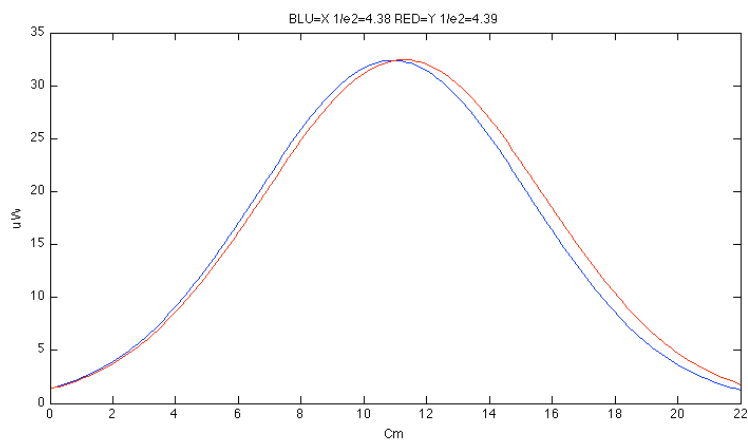


Figure 2.6: Fitting of the profile in x and y on the transmitting aperture during the night of 23th. Notice how the $1/e^2$ criteria is met.

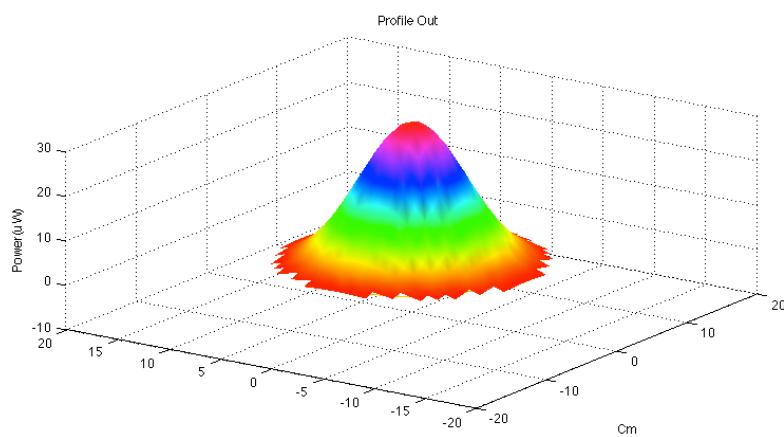


Figure 2.7: 3D profile of the outgoing beam on sept. 23th.

Table 2.1: Meteo Data on both sites (T=Teide R=Roque) for all the observing nights. Wind Speed is in Km/h, wind direction in degrees, humidity in percent whereas r_0 in cm. The value of C_n^2 is to be intended as explained in the text multiplied by 10^{-14} for 1Km along the path and by 10^{-16} for the others 143Km. C is the validity index based on the number of seeing data: Poor, Medium, Good.

Night	ws(T)	wd(T)	H(T)	ws(R)	wd(R)	H(R)	seeing(R)	r_0 (R)	Cn^2 (R)	C
17-18	14,31	328	4	23,55	271	0,5	0,9	3,4	0,19	G
18-19	15,17	186	6,5	31,6	221	6	1,165	2,6	0,3	G
19-20	5,9	129,5	4,5	12,4	151	3	1,75	1,7*	0,59	P
20-21	15,4	241,5	18,5	18,6	98,5	7,5	0,695	4,4	0,12	M
21-22	13,35	155	52,5	16	96,5	52	n.a.	-	-	
22-23	30,31	198	82	31,05	170	93	n.a.	-	-	
23-24	7,57	193,5	21	24,95	229,5	26	0,775	3,9	0,15	M
24-25	8,82	250,5	27	4,55	233	36	n.a.	-	-	

Table 2.2: Output power measured at JKT.

Night	Fiber Out	Lens Out	Optics Transmission
17-18	n.a.	n.a.	n.a.
18-19	4.5 mW	n.a.	n.a.
19-20	7.37 mW	4.98 mW	0.67
20-21	5.7 mW	3.86 mW	0.68
21-22	5.4 mW	4.23mW	0.78
22-23	n.a.(rain)	n.a.	n.a.
23-24	5.7 mW	3.99 mW	0.7
24-25	n.a.	n.a.	n.a.

During the nights between 21 and 24 September 2011, the experiments permitted to collect data at OGS site in Tenerife to measure the scintillation and the received power investigating about the temporal structure of the signal.

In the OGS Coude focus a photodiode and a power meter were placed, and, when the beam were suitably attenuated at the transmitter with a neutral filter, we also collected data at the receiver the a single photon (Excelitas SPCM-AQRH model) detector (SPAD).

We obtained an average attenuation of about 30 dB for many times during the best run with peaks of 27 dB averaged over 2 min.

The attenuation is calculated from the fiber and not from the singlet lens; the attenuation of the telescope is thus included in the measured attenuation.

Fried Coherence length r_0 . In the table 2.1 the average meteorological data of the two sites during the observing nights are shown.

The parameter r_0 is obtained from the vertical seeing: according the relation [2], the coherence length parameter r_0V for the vertical propagation is expressed as

$$r_0^{(V)} = 2.013 \times 10^5 \cdot \lambda / \text{seeing} \quad (2.1)$$

We estimated two C_n^2 following the Hufnagel-Valley (H-V) model, [95] the first for the first 100m (L_{v1}) and the second for the rest of the vertical propagation (L_{v2}), according:

$$C_{n(2)}^2 = \frac{(r_0^{(V)})^{-5/3}}{0.423(\frac{2\pi}{\lambda})^2(L_{v2} + C_{n(1)}^2 L_{v1})} \quad (2.2)$$

From the mean ratio of C_n^2 close to ground and above the ground in the H-V model.

$$C_{n(1)}^2 = 100C_{n(2)}^2 \quad (2.3)$$

At this point the value of r_0 for the horizontal propagation is reached with the standard formula using the two distances $L_{h1} = 1Km$ e $L_{h2} = 142Km$. In this way it is better taken into consideration the fact that for some chilimeters the beam travel close enough to the ground especially in Tenerife.

$$r_0 = 0.423(2\pi/\lambda)^2(L_{h1} * C_{n(1)}^2 + L_{h2} * C_{n(2)}^2)^{-3/5} \quad (2.4)$$

This approach looks good and the approximation of the C_n^2 can be considered valid even for horizontal propagation using the formulas above.

In table a *validity index* in three levels is reported indicating whether the r_0 approximation is a good or poor.

This coefficient takes into consideration the amount of seeing data available for the calculation. In that night we have recorded also a number of videos with our system that allow us to estimate directly the value of C_n^2 and r_0 directly from a measure of the spot size at the CCD and considering the optical setup.

These values are: $C_n^2 = 3 \times 10^{-17}$ and $r_0 = 3.76cm$.

Spot profile at transmitter . We measured the spot profile at the diameter during the night in order to see the mode and also the attenuation of the optics. The measured power data at the transmitter during the various nights are reported in table 2.2.

2.1.1 Link Analysis

Single photon detection acquisition. Setting the counting interval T to 0.1, 1 and 10 ms, we performed several measurements.

The *Mean Photon Number q* in a counting interval at the receiver should follow a lognormal probability distribution [62], because of the turbulence effects.

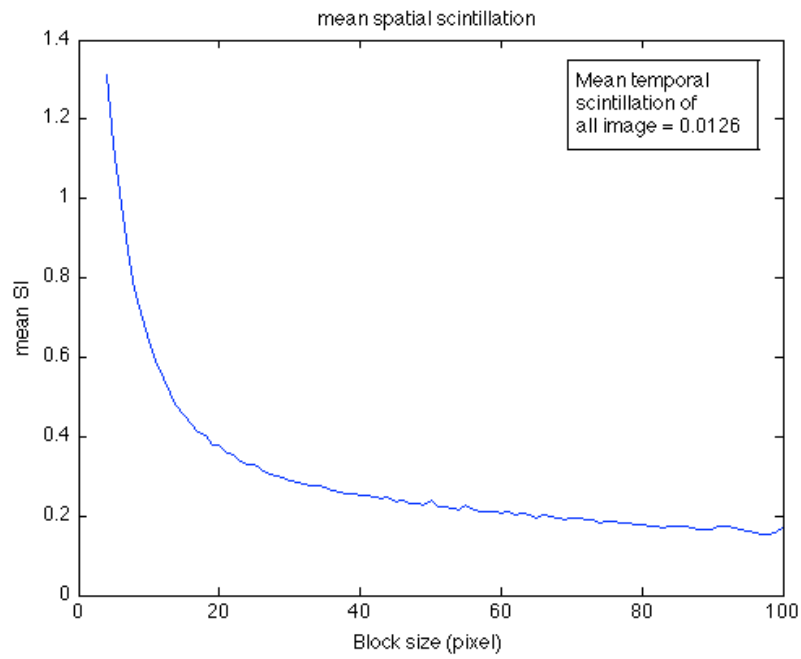


Figure 2.8: Mean temporal scintillation variation versus the block size on which the SI is calculated. This is the effect of aperture averaging.

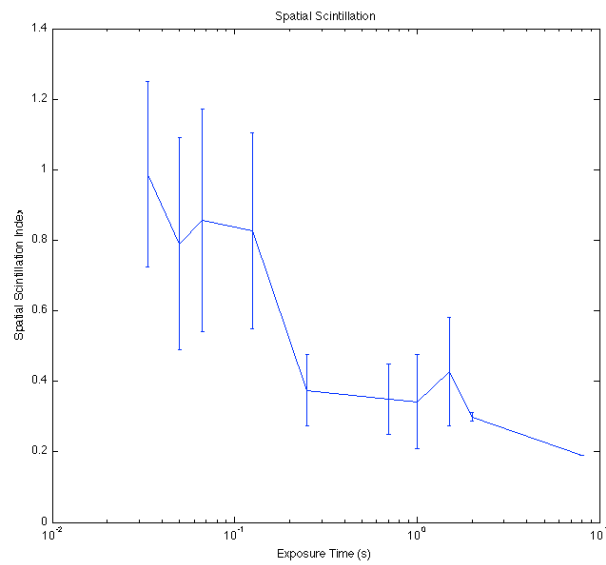


Figure 2.9: Spatial Scintillation Index v.s the exposure time.

	Mean	Std	Time (s)	Window (ms)	SI	Bound (Hz)
Backgr.	0.4732	0.7256	10	1	2.3515	475
Hi	5291	9135	650	10	2.9805	22
Hi	678.7	820.8	65	1	1.4626	43
Hi	510.4	751.9	65	1	2.1704	45
Hi	781.5	951.9	65	1	1.4834	42
Hi	180.2	312.0	65	1	2.997	39
Hi	234.1	349.2	65	1	2.2251	51
Hi	43.18	48.76	6.5	0.1	1.2748	81
Hi	21.17	26.34	6.5	0.1	1.5485	88
Hi	75.37	132.10	6.5	0.1	3.072	35
Hi	59.97	105.01	6.5	0.1	3.0659	37
Low	37.86	48.42	200	10	1.6355	35
Low	20.83	24.18	200	10	1.3479	35
Low	2.862	3.795	65	1	1.7578	384
Low	5.267	7.519	65	1	2.0383	258

Figure 2.10: Data obtained for different single photon acquisition compared to the background (first line). For each acquisition we report the total duration of the acquisition (Time), the temporal windows defining the counting interval (Window), the mean number of counts in the counting interval (Mean), and its the standard deviation (Std). We also report the scintillation index (SI) and the frequency bound defined in such a way that all the frequencies below the bound contribute to 95% of the scintillation index (Bound). With High (Low) we indicate acquisition with a high (low) mean photon number detected during 1 s.

We notice that for the last two data sets the bound is higher due to the low signal compared to the background (having a flat frequency spectrum)

$$P(q) = \frac{e^{-[(\ln(\frac{q}{\langle q \rangle}) + (\sigma^2/2))]^2/(2\sigma^2)}}{q \cdot [2\pi\sigma^2]^{1/2}} \quad (2.5)$$

where the scintillation index is $SI = \frac{\Delta q^2}{\langle q \rangle^2}$, $\sigma^2 = \ln(1 + SI)$ and the average is $\langle q \rangle$.

The probability of detecting an n photon in each interval follows the **Mandel**

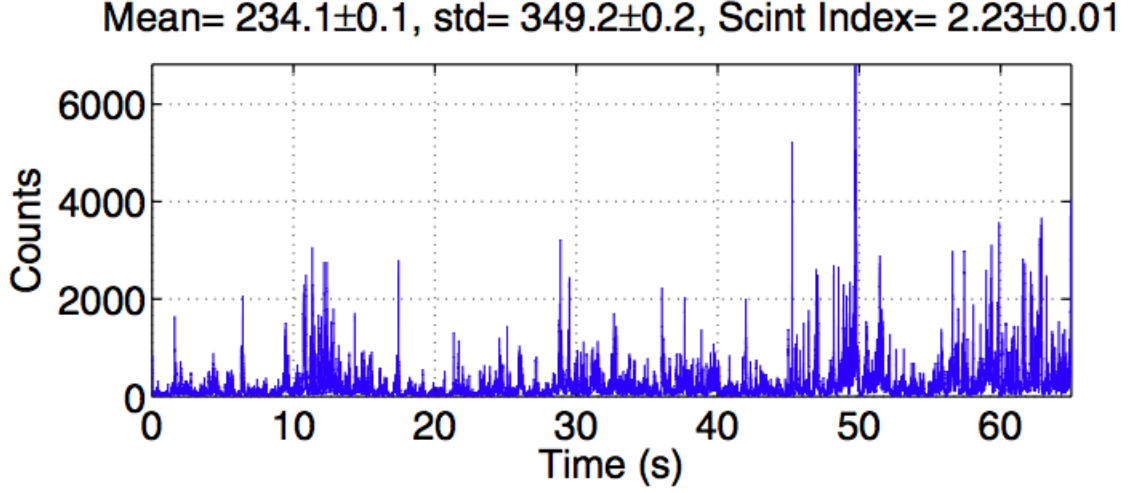


Figure 2.11: SPAD temporal distribution of count occurrences.

distribution if the counting interval T is large compared with the coherence time of the source and T is short compared with the turbulence time scale:

$$p_n = \int \frac{q^n \exp(-q)}{n!} P(q) dq \quad (2.6)$$

The mean number of detected photons is

$$\langle n \rangle = \sum_n n p_n = \langle q \rangle \quad (2.7)$$

We report the analysis of the temporal distribution of an acquisition with 1ms counting interval in Figure 2.11.

It is interesting to observe that when the average number of detected photons $\langle n \rangle$ is large (typically larger than 50) and the scintillation index bigger than 1, *the lognormal and Mandel distribution are quite similar.*

Given the experimental scintillation as 2.23 ± 0.01 and the mean value of detected photons as 234, we show the counting occurrences together with the corresponding lognormal distribution figure 2.12 ; for comparison, it is inserted the corresponding Mandel distribution with $\langle q \rangle = 234.1 \pm 0.1$ and $\sigma = 349.2 \pm 0.2$, parameters obtained from the raw data.

The similarity S between the lognormal or the Mandel curve and the experimental data is defined as

$$S = \frac{(\sum \sqrt{p_i q_i})^2}{\sum p_i \sum q_i} \quad (2.8)$$

with p_i the theoretical occurrence and q_i the experimental occurrence.

The *similarity S of the Mandel curve with the data* is of 0.9967 showing clear evidence of the statistic transformation.

The *similarity S of the lognormal curve with the data* is 0.9959.

The green curve represents 2.12 the Poisson distribution corresponding with the same observed mean value, to compare what would have been obtained if the statistic of the arrival photon were purely Poissonian.

The data of several different SPAD acquisitions are reported in Table 2.10

We measured the received light intensity with a fast photodiode by using an intense laser source.

Figure 2.13 shows the temporal distribution of the photodiode voltage of a data set covering 20s.

The intensities are recorded with 50kHz frequency.

The intensity occurrences follow a lognormal distribution as shown from the lognormal curve with a similarity of 0.9896.

In this case, the **scintillation index** evaluated from the experimental data is

$$SI = \frac{\Delta I^2}{\langle I \rangle^2} = 1.19 \pm 0.01 \quad (2.9)$$

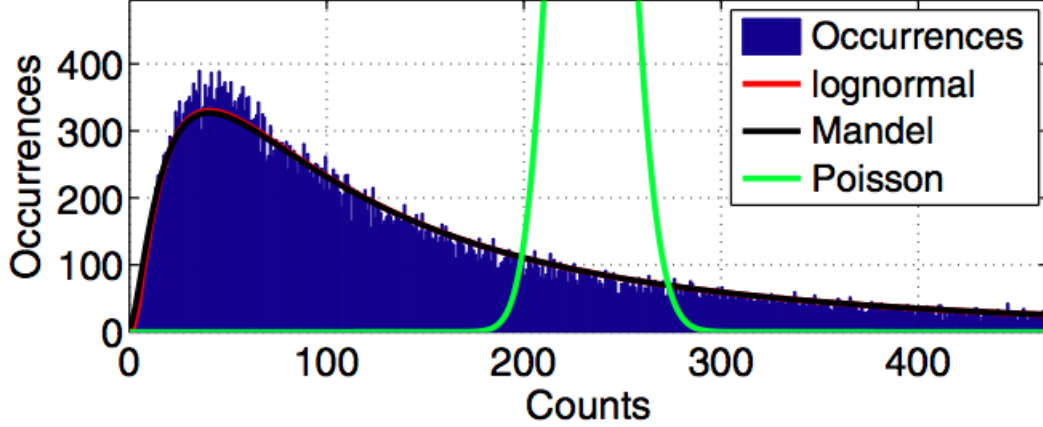


Figure 2.12: (color online). SPAD corresponding lognormal and Mandel curves. We can compare the data with the corresponding Poissonian distribution with the same mean value (234.1 ± 0.1) that would be obtained without turbulence.

Improving the SNR. For both quantum and classical communication, it is of paramount importance to achieve a high signal to noise ratio (SNR).

If a qubit state $|\psi\rangle$ encoded in the photon polarization must be sent between two remote locations, it is possible to determine the effect of (white) noise on the polarization fidelity. If $|\psi\rangle$ is the polarization state of the sent photon and ρ is the polarization density matrix of the received photon, the fidelity F

$$F = \langle \phi | \rho | \phi \rangle \quad (2.10)$$

is the probability of receiving the correct state.

If $|\psi\rangle$ is the polarization state of the sent photon and ρ is the polarization density matrix of the received photon, the fidelity $F = \langle \psi | \rho | \psi \rangle$ is the probability of receiving the correct state.

Measuring the Signal to Noise Ratio (SNR) in dB,

$$SNR = 10 \cdot \log_{10} \frac{N_s}{N_n} \quad (2.11)$$

with N_n the average amount of noise (coming from dark detections or background radiation) and N_s is the average number of detected photons.

The fidelity depends on the SNR as

$$F = 1 - \frac{1}{2(10^{SNR/10})} \quad (2.12)$$

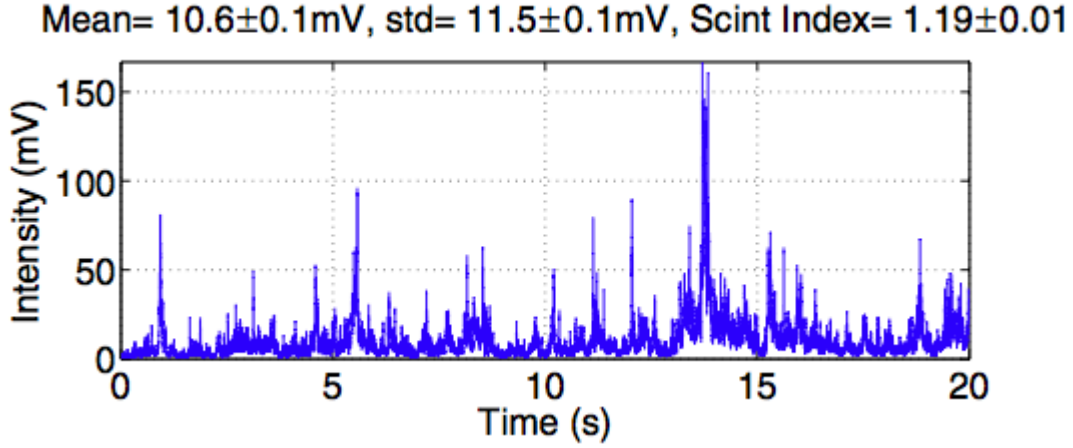


Figure 2.13: (Color line). Photodiode temporal distribution intensity occurrences.

Since the background photons are completely depolarized, the received quantum state are:

$$\rho = \frac{N_s - N_n}{N_s} |\psi\rangle \langle \psi| + \frac{N_n}{2N_s} \quad (2.13)$$

In order to improve the SNR for the transmission of single photons in a long distance free-space link as the present one, which uses a 1 m optical receiver, out of our findings we envisage the exploitation of the following procedure.

With a given frequency (slower than the single photon transmission rate), the free-space channel is probed by means of a classical signal that gives the information of the instantaneous transmission of the channel.

Only if the transmission is above a given threshold is the single photon signal acquired.

It is crucial for the protocol to be efficient to correctly identify the *probing* frequency and the threshold to be used.

This technique can also be used in the classical case, for instance, in on-off keying.

In Figure 2.15 it is reported the frequency spectrum.

The normalized plot of the power spectrum is obtained by normalizing the intensities by the average

$$I' = \frac{I}{\langle I \rangle} \quad (2.14)$$

The power spectrum is related to the scintillation index as follows.

We write the set of (normalized) acquisitions as I'_k with $k = 0, 1, \dots, N - 1$ and $N = \frac{20s}{20\mu s} = 10^6$ the number of intensity acquisitions over 20s.

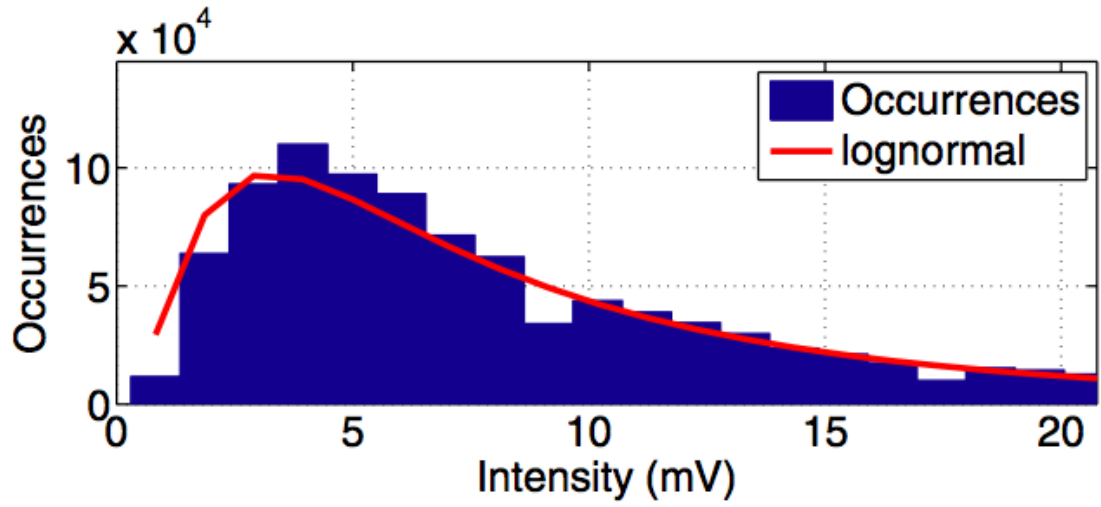


Figure 2.14: (color online). Photodiode temporal distribution intensity occurrences and corresponding lognormal curve.

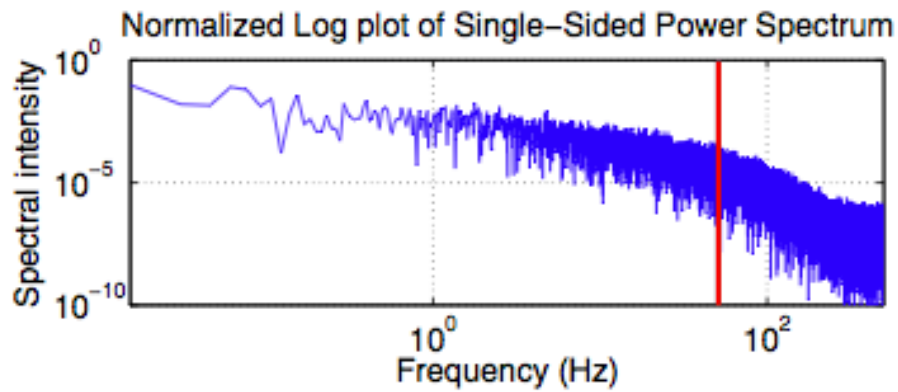


Figure 2.15: (color online). SPAD power spectrum and cumulative power spectrum. Frequency bound (red vertical line): The frequencies below 51 Hz contribute to 95% of the scintillation index.

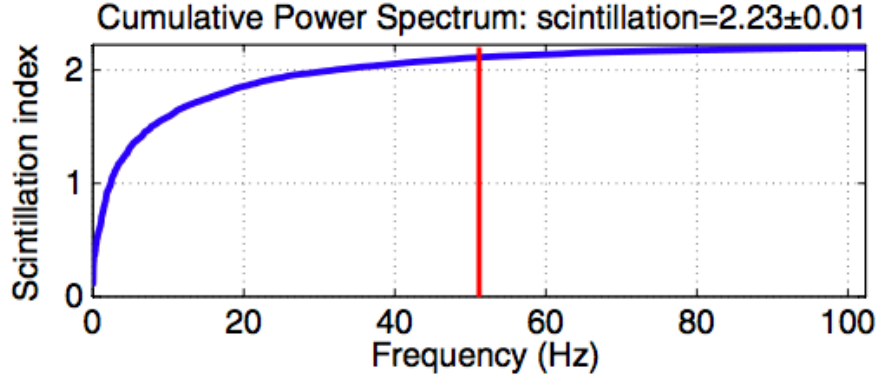


Figure 2.16: (color online). SPAD cumulative power spectrum. Frequency bound (red vertical line): The frequencies below 51 Hz contribute to 95% of the scintillation index.

The Fourier components are:

$$I_n = \sum k I' k \omega^k \quad (2.15)$$

with $\omega = \exp(-\frac{2\pi i}{N})$.

By Parseval's theorem it follows that

$$SI = \frac{2}{N^2} \sum_n = 1^N / 2 |I_n|^2 \quad (2.16)$$

Namely, it is the cumulative power spectrum without the zero frequency I_0 component.

We can notice that the frequencies contributing to the scintillation (up to 95%) are within (almost) 50 Hz.

For frequencies above around 500 Hz, the spectrum becomes flat, indicating that at this frequency the random noise is dominant. The typical fluctuations of the transmission channel due to the turbulence are within 100 Hz (see table in figure 2.10).

The frequency analysis of the temporal scintillation indicates that the probing frequency does not need to be higher than 1 KHz.

In order to obtain further evidence, we analysed the features of the counts above a given threshold of the signal represented in Figure 2.11.

By considering a threshold of 1, 2, 4, and 6 dB above the average, we considered the duration (in milliseconds) of events with over-threshold counting.

The results are shown in Figure 2.17.

The probability of obtaining an event above a given threshold q_0 can be predicted from the lognormal distribution (replacing the Mandel distribution with the lognormal distribution).

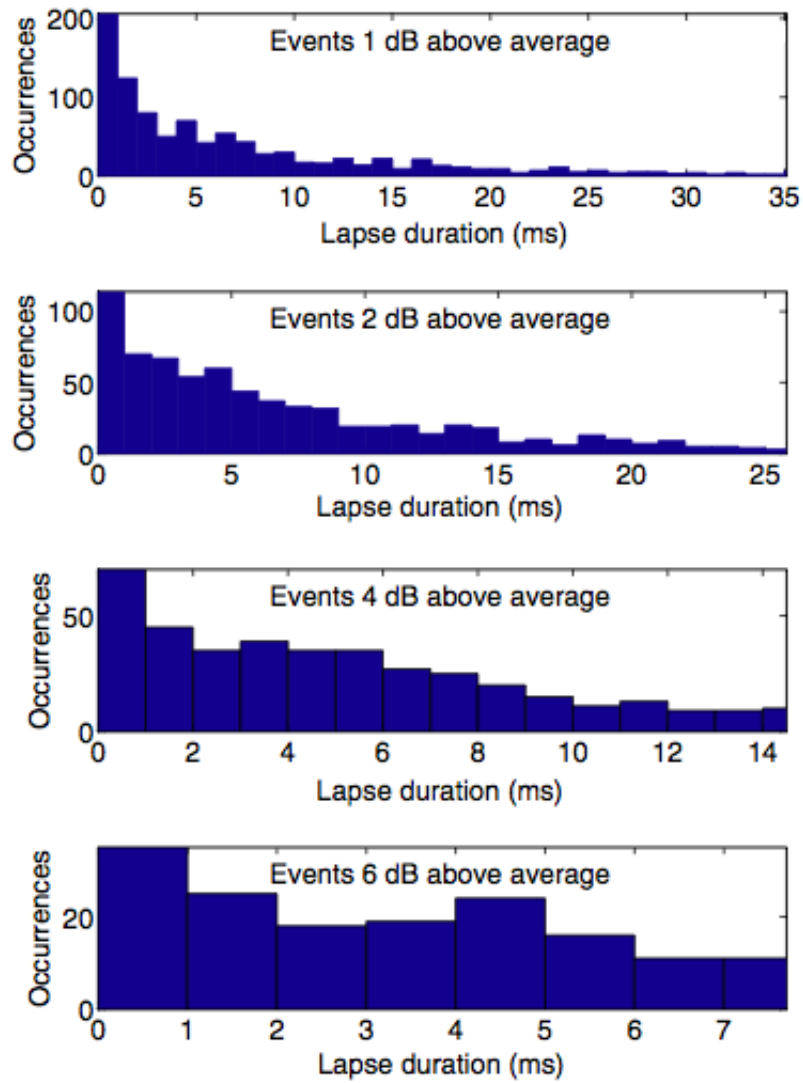


Figure 2.17: (color online). Duration (in milliseconds) of events with overthreshold counting. In the different plots we considered a threshold of 1, 2, 4, and 6 dB above the average.

$$p(q > q_0) = \frac{1}{2} - \frac{1}{2} \operatorname{erf} \left[\frac{\ln(q_0/q) + (\sigma^2/2)}{\sqrt{2\sigma^2}} \right] \quad (2.17)$$

where $\operatorname{erf}(x)$ is the Gaussian error function

$$\operatorname{erf}(x) = (2/\sqrt{\pi}) \int_0^x \exp(-t^2) dt \quad (2.18)$$

Acquiring the single photon channel only if the probed transmission is above a given threshold implies an increase of the average photon counts in each time slot. It is possible to show that, by considering only the events in which the transmission satisfy $T > T_0$, the new mean value $\langle n \rangle_{thres}$ is

$$\frac{\langle n \rangle_{thres}}{\langle n \rangle} = \frac{1 - \operatorname{erf}(\frac{x-y}{\sqrt{2\sigma^2}})}{1 - \operatorname{erf}(\frac{x+y}{\sqrt{2\sigma^2}})} > 1 \quad (2.19)$$

with $x = \ln(\frac{T_0}{\langle T \rangle})$ and $y = \sqrt{2\sigma^2}$.

Clearly, this threshold selection increases the SNR but at the same time decreases the overall counts in a given time.

In figure 2.18, we show the increase (in decibels) of the SNR and the percentage of the overall counts that will be detected.

In cases of strong turbulence and high noise, this technique could help the qubit transmission by “exploiting turbulence”, namely, considering only the particular moments in which the turbulence increases the channel transmission.

Finally, the statistic of arrival of single photons over a free-space 143 km optical link has been analyzed, demonstrating the transformation from Poissonian to lognormal distribution and thus expanding this investigation for more than an order of magnitude in length with respect to previous results.

[62] The evidence of consecutive subintervals of low losses allows us to envisage the exploitation of turbulence as an SNR improvement technique.

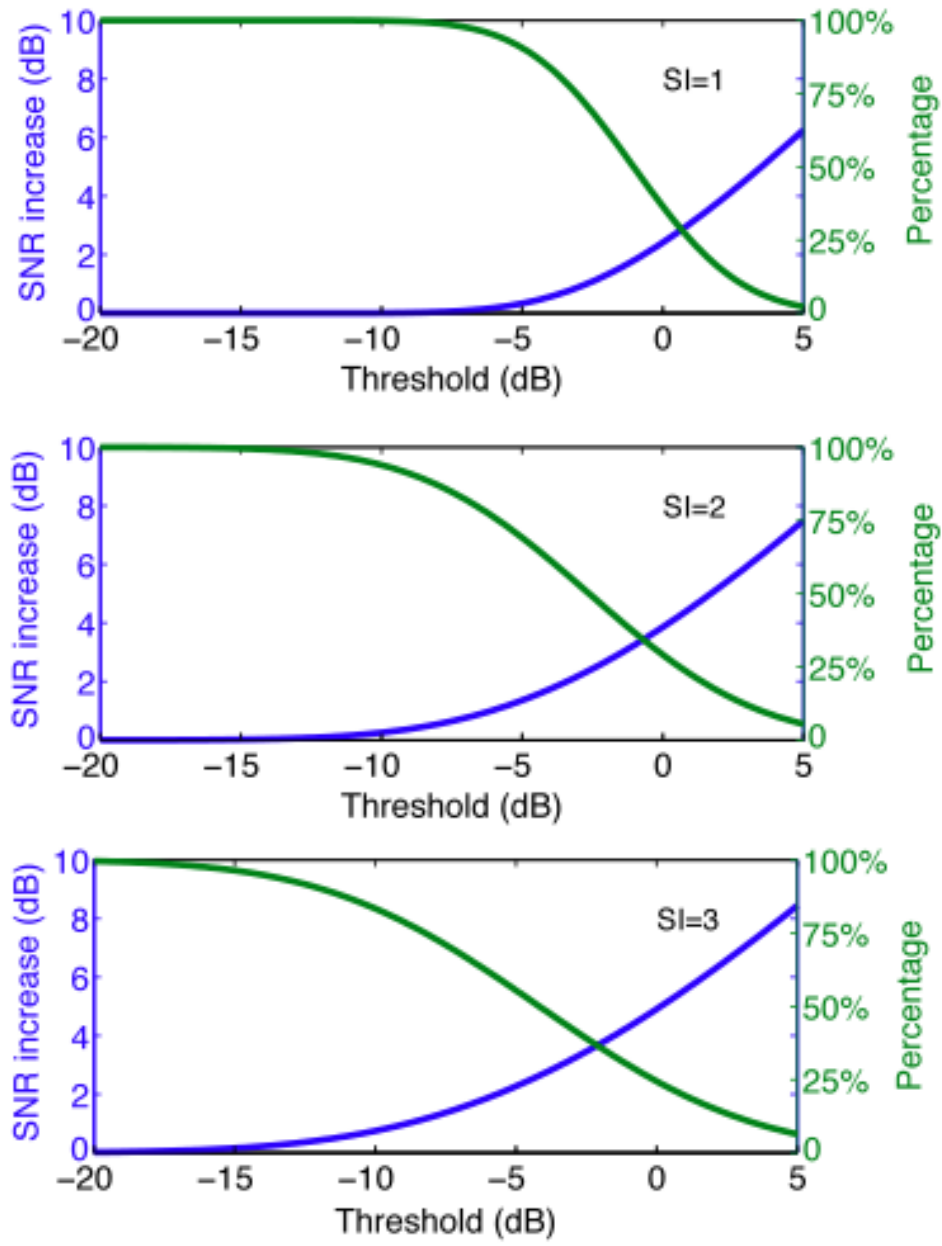


Figure 2.18: (color online). Counts that will be detected in the function of the threshold selection.

2.2 Conclusions

Two are the crucial results of this work. The studies of the propagation of single, double beams along 143 kilometers have demonstrated that

- At the receiver side the transmitted beam presents multiple spot features.
- By an optimized aplanatic refractive transmitter of large aperture (as our "Canary Telescope"). It is possible to reconstruct the beam long-term diameter as restricted into a spot (only a factor 3 to 5 the diffraction limit)

With the added value of *the beam co-propagating technique* This fact is of paramount importance as in a noisy channel the quantum signal (the information encoded in single photons) cannot be improved by increasing the signal power.

A solution could come iterating the data transmission until a sufficient data volume is received by the transmitter by performing a two beam co-propagating method.

Besides the statistic of arrival of single photons over a free-space 143 km optical link has been analyzed.

We have demonstrated that there is a transformation from Poissonian to log-normal distribution, expanding this investigation for more than an order of magnitude in length with respect to previous results.

Besides, there is the evidence of consecutive subintervals of low losses allowing us to envisage the exploitation of turbulence as an SNR improvement technique.

Part II

APPLICATION OF OPTICAL QUANTUM LINKS TO GNSS

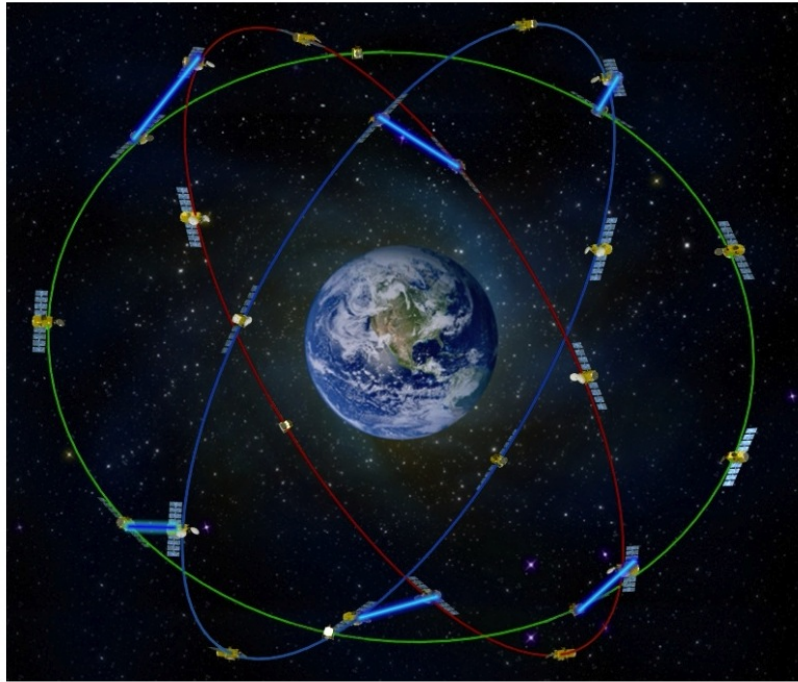


Figure 2.19: The image shows the Optical Quantum Communication Network (OQCN) for Galileo Constellation devised by University of Padova and Thales Alenia Space for ESA. Blue lines represent the communication channels performed between two optical transceivers on board of the satellites. Let us note that when two satellites approach each other, the Optical Link (Classical and Quantum) is accomplished. Earth and satellites are not built to scale in the figure.

Lasers will certainly be the communications medium of choice in future (Oerlikon-Space webpage)

The second part of my thesis reports about the project "Applications of Optical Quantum Links to GNSS", project of the European Space Agency for which the Quantum Group of Paolo Villorosi (Padua University) have devised and built the Quantum prototype SaNe-QKD. I was part of this team to design, accomplish and test the Quantum Communication system to position on board of Galileo satellite constellation.

At the same time, Alenia Space Turin team has worked for the Classical Optical Communication counterpart: starting from two different optical communication schemes the challenge was to interface each optical, mechanical and electronic part fusing

them into a unique working prototype.

The following chapters report about researches, simulations and optic-mechanical developments of the quantum transceiver for the ESA project.

Chapter three introduces quantum communication schemes for space applications, focusing our attention on MATLAB simulations for inter-satellite links in order to exploit the relative motion of satellites lying in different orbital planes. For Galileo constellation, we observed that it is possible to target communication between satellites that are closer in turns, achieving appreciable transmission rates and secret key lengths.

Finally, recalling elements of Quantum Mechanics MATLAB simulations for Decoy State scheme have been performed.

The fourth chapter reports about the design/arrangement of the Quantum transceiver in each part, before the Proof of Concept Demonstration (POCD) test.

Part of the work devised here is in [38]

Chapter 3

Application of Optical Quantum links to GNSS: first phase

In the fast evolving field of the optical communication technology, the challenging frontier is the space.

Last century, the space ascent has brought in orbit spacecraft, satellites and probes, to monitor and switch data with the Earth surface; nowadays these space-segments are facing a growing request in data volume exchanging, pointing out that their technology need to be implemented. [45] As observed in a US DoD (Department of Defence) document (2001) ([97]) a limit of frequency congestion for the RF (Radio Frequency) technology was expected above 10 Gb/s data transfer.

As the space is a privileged transmission channel preserving optical beam characteristics for extremely long distances, the optical communication systems have the potential to overcome the RF limit. The space experiments performed by satellites - equipped with laser communication terminals as ARTEMIS, TerraSAR-X, TanDEM-X, NFIRES, KIRARI (OICETS), LADEE (LLCD) [88] [93] [1] [54] [82] [72] [84] [87] [68] [46] [63] - have demonstrated the merits of the optical communication technology. Owing to lower system size, power consumptions, narrow optical beam divergence and small antenna (compared with RF competitors) the optical communication systems are crucial for satisfying the performances requested in terms of the increasing need in multi-gigabit data rate transfer, being effective when large quantities quickly sent back and forth between moving satellites.

Optical Communication Links

As told above, the optical communication technology is becoming a feasible alternative/integration to Radio Frequency communication for transmission of large quantities of data over long distances.

Three main blocks usually characterize an optical communication system: [20] [45]

- The **optical transmitter module OTM** that converts the electric communication signal into an optical one and send it through the communication channel, using the light (in visible and near infrared spectrum) to carry the information. Typical optical sources are lasers or LEDs (Light Emitting Diodes). For space OTM and compared to RF technology the less divergent lasers are the best solution. At shorter wavelengths and same antenna they present advantageous higher transmission performances, allowing *frequency reuse*¹ and reduced diffraction losses. Laser narrow beam width allows high accuracy of ranging too.
- The **communication channel** carries the optical signal from transmitter to receiver, that is a waveguide, or the non-birefringent atmosphere (in ground-ground or ground-space links), or the space (in space-space links).
- The **optical receiver module** that converts the signal (the information arrived through the optical channel and collected by the antenna) into an electric one.

The main drawback of optical communication technology is the perceive risk for the human eye due to the laser use, risk that is overtaken in space-space links (and mitigated in space-ground links using non-dangerous wavelengths and accurately weaker beams).

Other disadvantages of optical communication technology are the limited distances in terrestrial applications, reduced by the presence of obstacles, by Earth curvature (about 200km the major reachable horizontal extension) or weather conditions; humidity, clouds and fogs strongly attenuate the communication and strategies to mitigate weather restrictions are needed (see chapter two). Moreover, if performed in fiber-guided point-to-point terrestrial schemes it is necessary to improve the signal losses due to distortion and depolarization limiting the propagation distance covered (considerations to take in account for the Quantum counterpart application [12]).

As told above optical technology permits a competitive high data rate exchanging between two points with high efficiency and low power consumption.

The advantages of compactness and weightlessness of the optical communication systems are due to the lower size of the terminal components (light acquiring devices, optic-mechanical components and laser sources for the current technology developments in electronics and miniaturizing) and reduced antennas.

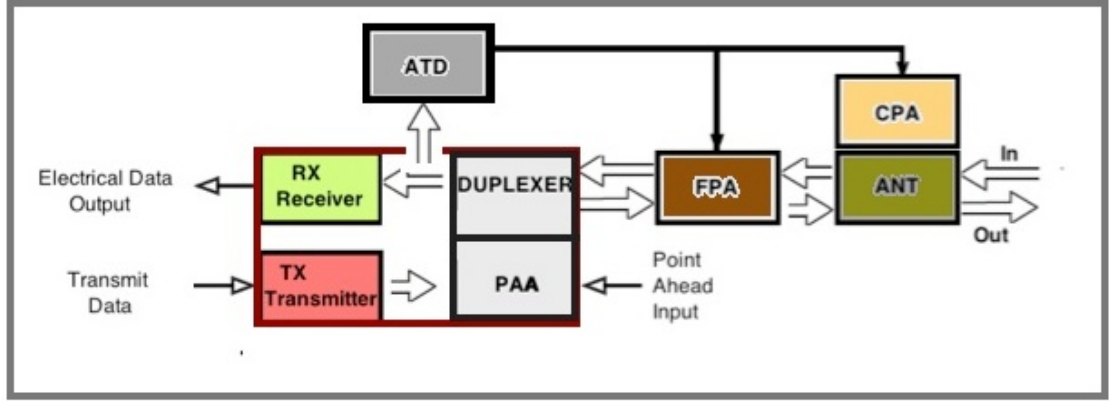
These merits make the optical communication systems definitely useful either for civilian or for military applications in space, where reduction in on-board burden means reduction in mission costs.

¹Frequency reuse: use of the same wavelength for multiple links owing to the small divergence angle of communicating beams

Optical communication advantages (compared to RF technology)
Transmitted narrow beam width
High data rate
Reduced system mass and size (antenna of 1/10)
Reduced power consumption and reduced costs
Frequency reuse
Intrinsically secure (by Quantum Key Distribution)
Optical communication drawbacks
Perceive risk for the human eye
Possible fails for obstacle presences
Limited by weather conditions

Table 3.1: The table briefly recalls the main pro and cons of optical communication compared to Radio Frequency (RF) technology

Figure 3.1: The figure shows the architecture of an optical transceiver for space-to-space laser links. **RX** stands for Receiver, **TX** for Transmitter, **ATD** for Acquisition and Tracking Detector, **PAA** stands for Point Ahead Accuracy, **FPA** for Fine Pointing Assembly, **CPA** Coarse Pointing Assembly, **ANT** for Antenna.



In order to reduce the payload burden, further, the optical transmitter and receiver modules can be integrated into a single *transceiver*, using a unique telescope. An example of optical communication transceiver is showed in the figure 3.1.

- The transmitter *TX* unit is part of the *optical transmitter module*, dealing with the optical signal generation.
- the *PAA (Point Ahead Assembly) unit* is necessary when the angular separation between transmitted and received beam due to fast terminal motion is larger than the associated beam divergence.
- the *Input-output duplexer unit* assures sufficient *isolation* between a transmitted signal and a received one. The isolation is achieved through the use of orthogonal polarizations or different wavelengths for transmitted and received beams in order to distinguish them into a unique transceiver. Besides, different portions of one telescope may also be used for transmitting and receiving optical signals, in order to spatially increase TX/RX isolation.
- the *FPA (Fine Pointing Assembly) unit* is used for beam tracking purposes.
- the *ANT (Optical Antenna) unit* is a telescope acting as an optical antenna that is connected to the *CPA (Coarse Pointing Assembly) unit* for pointing and tracking issues. In the **optical transmitter module** of a transceiver, the optical signal is generated in the optical transmitter unit TX by the electro-optical conversion; controlled by the PAA (Point Ahead Assembly) unit, by the input-output duplexer unit and the FPA (Fine Pointing Assembly) one, it

is sent from the telescope (ANT) to the **optical receiver module** across the **communication channel**.

Symmetrically for the **optical receiver module** of a transceiver, the optical signal propagating through the **communication channel** enters the telescope (ANT) and arrives at the RX receiver unit where it is converted into electrical signal (electrical data output).

- A small part of the received signal can be diverted to the *Acquisition and Tracking Detector (ATD) unit*, which provides information (for acquisition and tracking control) to the FPA (Fine Pointing Assembly) unit (checking the optical path after the telescope) and to the CPA (Coarse Pointing Assembly) unit able to correct the antenna position.

In addition to the high efficiency and low beam divergence, optical communication systems permit extremely secure point-to-point links: an hacker would have to be positioned in the immediate vicinity of the receiver, or would have to interfere with the laser beam. The **Quantum Mechanics** guarantees the security of the optical communication scheme, preventing the information theft by an eavesdropper: if performed by Quantum Key Distribution technique (described in the following sections) intrinsically secure ² optical links will be established.

The table ?? reports a brief summarizing about optical communication main pro and cons.

Finally, optical technology presents the potential of high-speed and long distance communication links in space, being advantageous when large quantities of data need to be transmitted quickly back and forth between satellites with the necessity of the *Quantum intrinsically security*.

²Intrinsic security means that there are no restrictions about the skills and the technologies available by an eavesdropper who is trying to jeopardize the communication scheme.

Quantum Communication

The aim of the science and the research is to improve the quality of life. In this sense in last decades, researchers have devoted strong efforts to study how Quantum Mechanics implications could be employed to manipulate the information leading to new information processing protocols (Quantum Information (QI)) [64] [21]), without any classical counterpart, as Quantum Computing (QC) [50], Quantum Key Distribution (QKD) [39] and Quantum Teleportation (QT) [7].

Recalling Quantum background, first quantum communication experiments were performed in laboratories or in local fiber-guided communications schemes between two points far only few tens of kilometers, as signal losses due to distortion and depolarization definitely limited the propagation distance covered. [77] [67] [28] [29]

During last decades the challenger has been extending the link distances [96] in performing terrestrial experiments of single photons exchanging; but as observed in the previous chapter, they suffer of beam distortion (due to atmospheric turbulence, weather conditions and presence of aerosols,...) and signal losses (due to obstacles positioned along the path).

However the Earth Atmosphere can still be used as an Optical Communication channel, as non-birefringence allows the transmission of polarization states without serious alterations; but the variable weather conditions can modify the quality/quantity of the received signal (rain, fog, clouds interposition can prejudice the communication) [2]. Besides inter-posed objects in the line of propagation of the transmitted beams, the limitations due to the Earth curvature, and the distortions caused by effects of atmospheric turbulence, still prejudice the communication.

Finally, it was early clear at the end of last century, that the concept of free-space need to be expanded beyond, to the space, devising Quantum Communication Systems, based upon optical technologies, on board of satellites, for a Quantum global network able to perform inter satellite links and space-ground ones. In order to cre-

ate and build an Optical Quantum Communication Network (OQCN) to position on board of Galileo constellation, it is necessary either to recall orbital mechanics topics of satellite motion (for inter-satellite links), or to introduce the Quantum Mechanics of cryptographic schemes, crucial argument to understand the working of the optical quantum communication prototype.

3.0.1 Orbital mechanics for Galileo Constellation

In this part we recall briefly orbital topics useful for future simulations and payload transceiver design [23].

3.0.2 Circular orbit

The *orbital equation* [23] defines the path of a body m_1 around a body m_2 , relative to m_1 , and it is given by the relation:

$$r = \frac{h^2}{\mu_{12}} \frac{1}{1 + e \cos \theta} \quad (3.1)$$

with h the angular momentum and $\mu_{12} = Gm_1m_2$ the gravitational parameter, θ the true anomaly and e the eccentricity.

Describing the circular orbit ($e = 0$) for a satellite at altitude z above the Earth surface, the orbital equation becomes

$$r = \frac{h^2}{\mu} = \frac{h^2}{GM_{Earth}} \quad (3.2)$$

with μ the Earth gravitational parameter: $\mu_{12} \equiv \mu = GM_{Earth} = 398600 km^3/s^2$ as the satellite mass is entirely negligible respect to the Earth mass.

As the angular momentum is $h = r\nu$, the velocity of the circular orbit around the Earth is

$$\nu = \sqrt{\frac{\mu}{r}} = \sqrt{\frac{\mu}{z + R_{Earth}}} \quad (3.3)$$

Finally, the period of the circular orbit is given by the relation

$$\Pi = \frac{\text{circumference}}{\text{speed}} = \frac{2\pi r}{\nu} = \frac{2\pi(R_{Earth} + z)^{3/2}}{\mu^{1/2}} \quad (3.4)$$

The following figures 3.2 and 3.3 reports the estimation of the circular orbital period Π and the estimation of the circular orbital speed ν for a satellite at different altitudes from the Earth surface.

Let us focus some interesting altitudes and gravity ratio values in the following table.

Altitude	Period Π [min]	Speed ν [km/s]
300km	90.52	7.613
1000km	105.1	7.35
2500km	138.7	6.701
5000km	201.3	5.919
10000km	347.7	4.933
20200km	718.5	3.873
23222km	844.4	3.670
35786km	1437	3.075

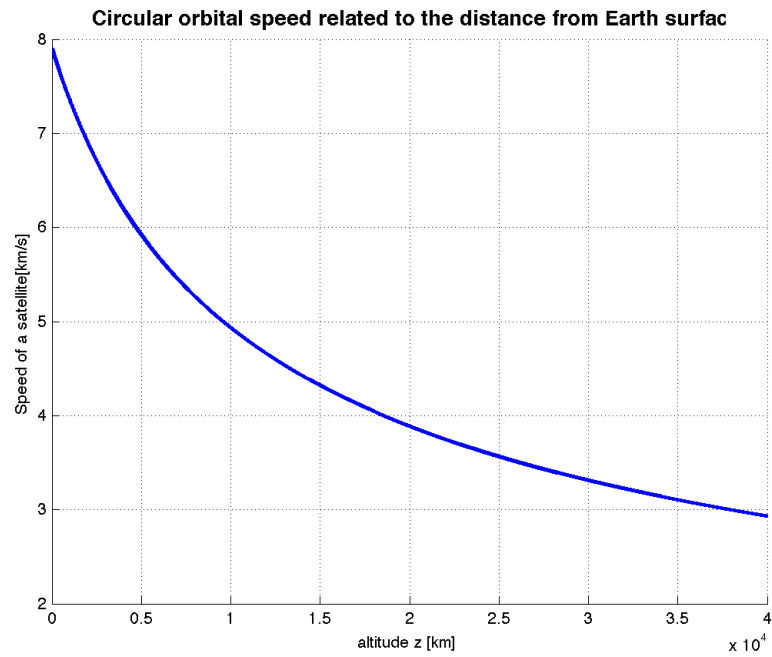


Figure 3.2: The figure represents the estimation of the circular orbital period related to the distance from the Earth surface (the altitude interval is between 0 and 40000 km above the Earth surface).

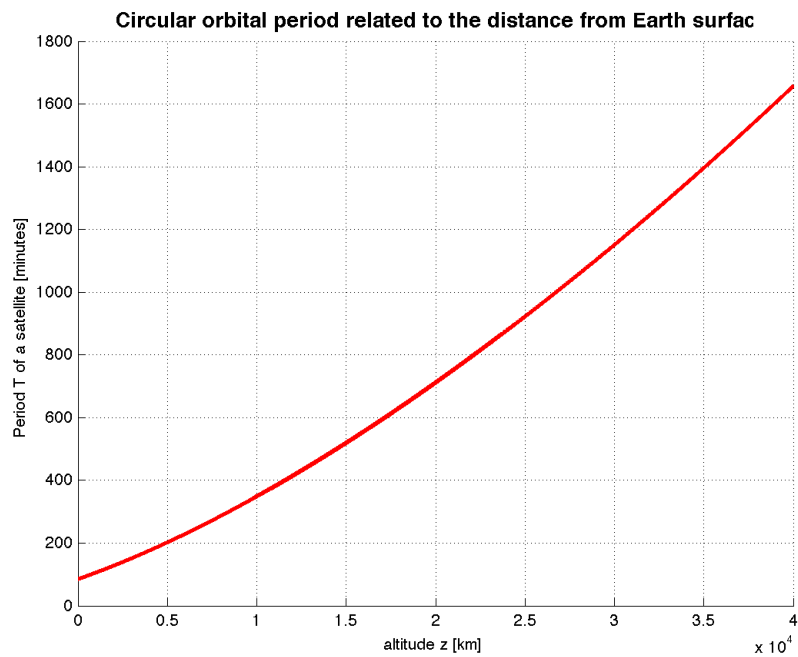


Figure 3.3: The figure shows the estimation of the circular orbital speed related to the distance from the Earth surface

The values reported in the table focus our attention on the fact that the circular orbital period of the ISS (International Space Station) is of about 90 minutes, with a circular orbital speed about $7.6km/s$. Even if based on a circular orbit approximation, the obtained values are similar to the real data. ($\Pi = 92'27''$ and $\nu = 7.706 km/s$) [81] The same observation can be done for **GPS NAVISTAR** and **GPS Galileo**. The calculated values of are similar to the real data. Finally, the circular orbital period and the circular orbital speed obtained for different altitudes are next to the real ones, even if based on a circular approximation orbit formula.

It is known [23] that a *Geostationary Equatorial Orbit* is a geosynchronous orbit above the Earth equator in which the satellite keeps always the same point in the sky as its period is equal to the Earth rotation one.

This orbit is useful for communication satellites, as they permits to the Ground stations to tracking easily the satellite antennas and to observe a large portion of Earth surface from a fixed privileged point in the sky, making geostationary orbits still interesting for weather or monitoring purposes.

The velocity of the geostationary radius is given by

$$r_{geo} = \sqrt{\frac{\mu}{w^2}} = 42164km \quad (3.5)$$

as the inertial angular velocity of a geostationary satellite is $w = 72.922 \cdot 10^{-6} rad$. So the Geostationary altitude above sea level of a geostationary orbit is $r_{geo} - R_{Earth} = 35786km$.

And the velocity along the circular orbit is

$$\nu_{geo} = \sqrt{\mu} r_{geo} = 3.075km/s \quad (3.6)$$

according the previous obtained values.

Appendix: Acceleration of gravity

Two masses m_1 and m_2 positioned at a distance r between their centers experience a gravitational force

$$F = G \frac{m_1 m_2}{R^2} \quad (3.7)$$

with G the gravitational constant ($G = 6.6742 \cdot 10^{-11} m^3/kg \cdot s^2$).

The gravity force is an inverse-square dependence on the distance, crucial if one of the two masses is significantly bigger then the other one: the *weight* W is the gravitational force of the Earth mass M_{Earth} on a mass m_{Sat} , many orders of magnitudes smaller

$$W = \frac{G m_{Sat} M_{Earth}}{R^2} = m_{Sat} \cdot \frac{G M_{Earth}}{R^2} = m_{Sat} \cdot g \quad (3.8)$$

So the satellite is forced to fall towards the Earth center of attraction by a free falling process, supposing the planetary force the only one force acting on the satellite.

The standard sea-level value for g_0 is $9.807m/s^2$ at the Earth surface radius $R_{Earth} =$

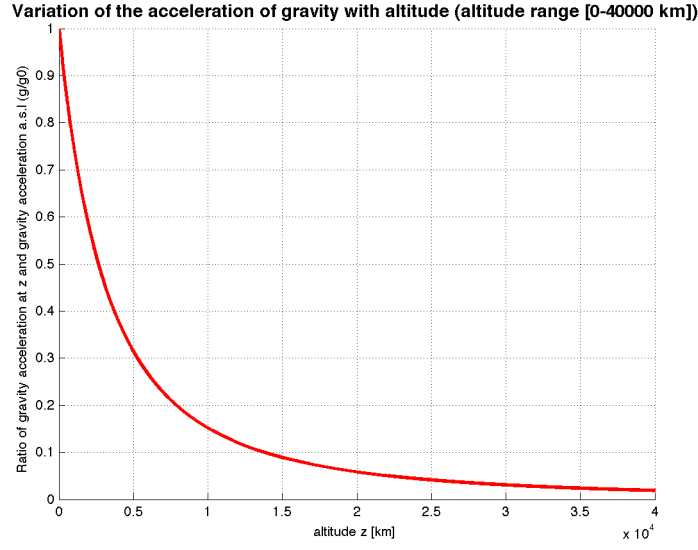


Figure 3.4: The figure represents the variation of the gravitational acceleration experienced by a satellite: the gravitational acceleration is here expressed in terms of ratio between the gravity value at the altitude z and at the sea level $g_0 = 9.807m/s$. The altitude interval performed is between 0 and 40000 km above the Earth surface

6378km. If the satellite altitude above the Earth surface is z , the distance between the center of Earth and the satellite is $r = z + R_{Earth}$.³

The satellite gravitational acceleration acting on the satellite is given by the relation

$$g_{Sat} = \frac{R_{Earth}^2 g_0}{(z + R_{Earth})^2} \quad (3.9)$$

so

$$\frac{g_{Sat}}{g_0} = \frac{1}{\left(\frac{z}{R_{Earth}} + 1\right)^2} \quad (3.10)$$

The figure 3.4 shows the estimation of the ratio $\frac{g_{Sat}}{g_0}$ between the gravity acceleration at the altitude z from the Earth surface and the gravity acceleration at sea level surface.

Let us focus some interesting altitudes and gravity ratio values in the following table.

³It is supposed that the corps have their masses concentrated on their center of attraction

Altitude	Gravitational ratio $\frac{g}{g_0}$	Notes
10km	0.997	Altitude for commercial airlines
300km	0.912	Altitude for International Space Station
1000km	0.747	Upper limit for LEO orbits
2500km	0.516	
5000km	0.314	
10000km	0.152	
20200km	0.058	Altitude for GPS NAVISTAR
23222km	0.046	Altitude for GPS Galileo
35786km	0.022	Geostationary satellites

The values reported in the table focus our attention on the fact that the astronauts weightless at the ISS (International Space Station) is not real, as Earth gravitational acceleration is present even if attenuated (it is about nine per cent less then the sea level value).

LEO upper limit orbital satellites (1000km) experience a gravitational acceleration about 25% less then the sea level value, while at 2500km it is about 50% of the sea level value.

A high altitudes, gravitational acceleration is significantly reduced. At 5000km this reduction corresponds to about 70%, while at 10000km it corresponds to about 85%; ever and ever strongly minimized (less then 6%) above 20000km, corresponding to the altitudes for GPS constellations. GEO satellites experience a gravitational acceleration about 98% less then the sea level value.

Communication Links

In this section, we present the results of a feasibility study on the application of optical quantum communication links to a global navigation satellite system (GNSS) network with reference to the Galileo architecture.

In this first subsection, beam propagation background and uplinks and downlinks between Space and Earth will be discussed.

Then, it will be pointed out the relevant case of inter-satellite links for the **Optical Quantum Communication Network (OQCN)** devised for Galileo Constellation, evaluating the expected performance in terms of achievable key lengths and quantum security (Decoy Scheme treatment).

Quantum Mechanics concepts and Quantum Cryptography schemes will be recalls, deriving specifications for the inter-satellite quantum key distribution (QKD) network.

3.0.3 Uplinks and Downlinks between Space and Earth

Naming as *uplink*, the optical communication channel established between a ground-based station and a satellite, and as *downlink* the optical communication channel established between a satellite to a ground-based station, in this section it is reported -for different satellite orbits- a summary of uplink/downlink feasibility study [89], [12], [91], a necessary background for future considerations about optical quantum link feasibility for Galileo Constellation.

The performances of a communication system are related to the SNR values (signal to noise ratio), refined reducing the link attenuation and the background noise, as the quantum communication schemes encode information into single photon states, the link performances cannot be improved increasing the signal level as for classical optical communication.

The atmospheric turbulence is the main limiting factor for quantum communication uplinks and downlinks: turbulence inhomogeneity increase the beam spreading to an extension significantly larger then what achieved by diffraction, depending on their size. So the turbulence eddies can cause two main effects [2] [45]

- Low spatial frequency beam wandering, if the dimensions are larger compared then beam size
- High spatial frequency beam spreading if the dimensions are smaller (then the beam size)

On short timescale, the beam is broadened and deflected in different directions; instead integrating over long timescales, the global effects is a spreading of the beam. It follows that the long-term spot tends to a Gaussian spatial distribution of intensity [2]

$$\langle I(r, L) \rangle = I_0 \exp\left(-\frac{2r^2}{w_{LT}^2}\right) \quad (3.11)$$

Figure 3.5: 850nm: plot for up/downlink for long-term beam width $w_{LT}[m]$ vs. link distance [km] for Earth ESA telescope MLRO (diameter 1.5 m) in Matera. The satellite is supposed at the zenith of the ground station. The satellite telescope is supposed 20 cm of diameter [91]. The orbit altitudes of LEO, ISS, GLONASS, GPS NAVISTAR, Galileo and GEO orbit are shown.

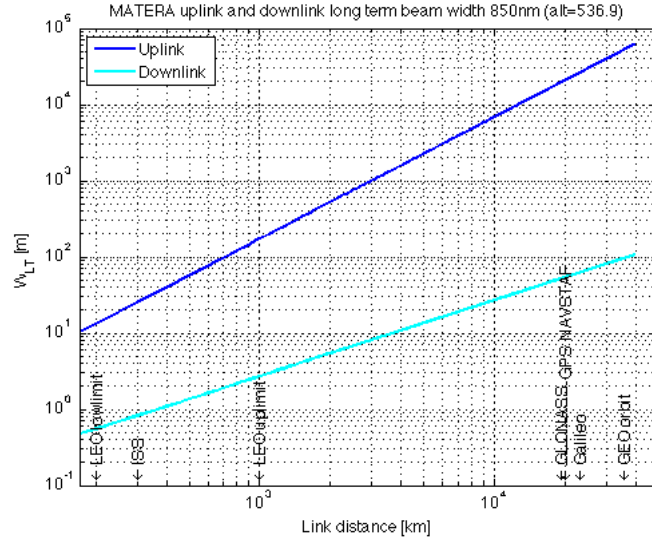


Figure 3.6: 850nm: plot for up/downlink for beam displacement β vs. link distance [km] for Earth ESA telescope MLRO (diameter 1.5 m) in Matera. The satellite is supposed at the zenith of the ground station. The satellite telescope is supposed 20 cm of diameter.[91] The orbit altitudes of LEO, ISS, GLONASS, GPS NAVISTAR, Galileo and GEO orbit are shown.

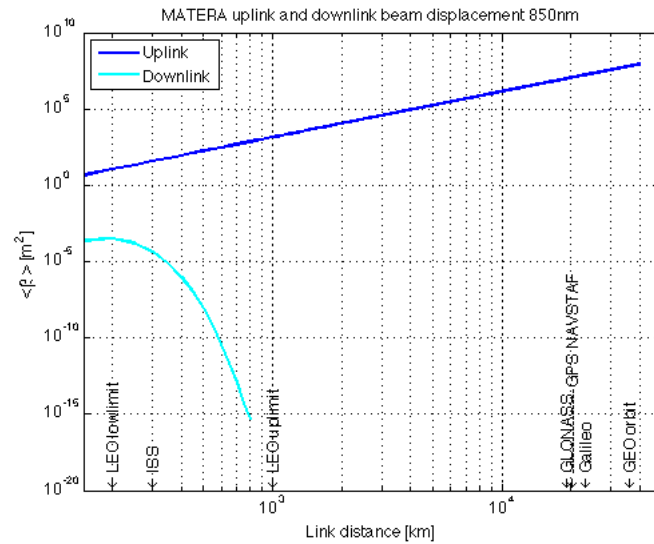
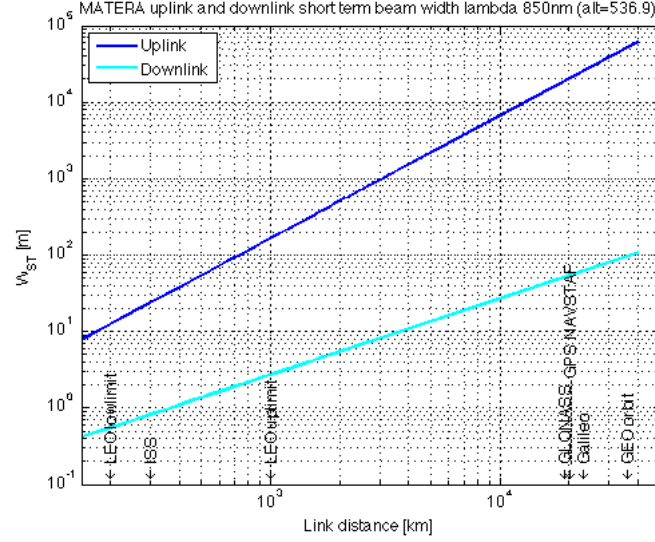


Figure 3.7: 850nm: plot for up/downlink for short-term beam width $w_{LT}[m]$ vs. link distance [km] for Earth ESA telescope MLRO (diameter 1.5 m) in Matera. The satellite is supposed at the zenith of the ground station. The satellite telescope is supposed 20 cm of diameter [91]. The orbit altitudes of LEO, ISS, GLONASS, GPS NAVISTAR, Galileo and GEO orbit are shown.



with L the propagation distance between sender and receiver, I_0 the beam intensity, r the beam radial distance from the center of the beam. w_{LT} is the long-term beam width, which is expressed by:

$$w_{LT}^2 = w_{ST}^2 + 2 \langle \beta^2 \rangle \quad (3.12)$$

The short-term beam width w_{ST} is given by:

$$w_{ST}^2 = w_0^2 \left(1 + \frac{Z_0^2 + L^2}{Z_0^2}\right) + 2 \left(\frac{4L}{kr_0}\right)^2 \left(1 - 0.26 \left(\frac{r_0}{w_0}\right)^{1/3}\right)^2 \cong w_0^2 \left(1 + \frac{Z_0^2 + L^2}{Z_0^2}\right) \quad (3.13)$$

with beam waist w_0 , r radial distance from the center axis of the beam, β the instantaneous displacement between the unperturbed position.

Calling Z_0 the Rayleigh parameter and r_0 the Fried parameter (discussed here below), for a collimated beam the long term beam width becomes

$$w_{LT}^2 = w_0^2 \left(1 + \frac{Z_0^2 + L^2}{Z_0^2}\right) + 2 \left(\frac{4L}{kr_0}\right)^2 \quad (3.14)$$

In cases of dominant beam displacement, accurate pointing system can compensate in order to equal 3.13 and 3.14, that is $w_{LT}^2 = w_{ST}^2$.

Supposing a satellite positioned above a ground-based station, it is seen rising, orbiting and setting down at different positions in the sky related to its orbit.

At each time, the satellite position, in relation to an Earth station, depends on a **three-component vector s (zenith angle θ_{zn} , site altitude h_0 , effective link distance L)** with the zenith angle θ_{zn} giving information about the thickness of the atmospheric layers crossed by the laser beam.

Naming with R_{Earth} the mean Earth radius and with R_{Sat} the satellite altitude and assuming (near) circular orbits, according the geometry of an Earth station looking at a satellite orbiting around the Earth surface, the **effective link distance L** is:

$$L = \frac{-2R_T \cos \theta_{zn} + [4((R_{Sat} + R_{Earth})^2 - R_{Earth}^2) + (2R_{Earth} \cos \theta_{zn})^2]^{1/2}}{2} \quad (3.15)$$

The Fried coherence length r_0 [2] measures the quality of the optical beam propagating through the atmosphere. It represents the maximum diameter for a collector before the atmospheric turbulence could prejudice the link performance.

For an Earth-Space link the Fried coherence length becomes

$$r_0 = [0.423k^2 \sec(\theta_{zn}) \int_{h_0}^L C_n^2(z) (\frac{L-z}{z})^{5/3} dz]^{-3/5} \quad (3.16)$$

with $k = 2\pi/\lambda$ the wave number.

Following the Hufnagel-Valley model, the Fried parameter is related to the parameter of structure (of the refractive index) $C_n^2(z)$ expressed for $z \in \{h_0, L\}$ by [45] [94]

$$C_n^2 = 0.00594 (\frac{v}{27})^2 (10^{-5}h)^{10} \exp(\frac{-h}{1000}) + 2.710^{-16} \exp(\frac{-h}{1500}) + A \exp(\frac{-h}{100}) \quad (3.17)$$

with $A = 1.7 \cdot 10^{-14}$ and $v = 21m/s$.

In terms of signal collector aperture (R the entrance aperture radius), the link efficiency η is:

$$\eta = \eta_0 (1 - \exp(\frac{-2R^2}{w_{LT}^2})) \quad (3.18)$$

and the received power P is given by:

$$P = 2\pi I_0 \int_0^R \rho \exp(\frac{-2\rho^2}{w_{LT}^2}) d\rho \quad (3.19)$$

and η_0 is assumed 0.1 at the zenith [3] [45]

Considering different satellite and probe/space module classes:

- **LEO Earth Orbit low limit** (about 200 km above Earth surface)
- **ISS, International Space Station** (300km above Earth surface)
- **LEO Up limit Orbit** (1000km)

- **GLONASS**, GLObal Navigation Satellite System, (19100 km) by the Russian Aerospace Defence Forces.
- **NAVSTAR GPS** NAVigation Satellite Timing And Ranging Global Positioning System, (20200 km) by US department of Defence.
- **Galileo**, a Global Navigation Satellite System (GNSS) currently built by the European Union and the European Space Agency (ESA) positioned at a mean altitude of 23222 km.
- **GEO stationary satellite orbit** (35786km) at which the satellite represents an apparent fixed point in the sky, ideal for communications,

The figures 3.5 3.7 3.6 shows the feasibility of Quantum uplink and downlink for 850nm operating wavelength for the OQCN, in terms of w_{LT} , w_{ST} and beam displacement $\langle \beta \rangle$ recalling [89].

[12] **Uplinks**. Considering the scheme of an optical link established between a ground-based station and a satellite with the telescope of radius R_{SpaceT} , *in day-time* the main source of background is the Sun, while *in night time* the main source of background is the Moon.

Generally, in terms of the background noise, the day conditions presents the worst case for the optical communication.

In day time conditions, we suppose a *Lambertian diffusion* of Sun light by the Earth (albedo a_{Earth} 0.38) and collected by the space telescope . The background is expressed in terms of the **number of collected photons**, which is a function of the telescope Field of View (*IFOV*) [rad], the *Solar constant* S ($4.61 \cdot 10^{18}$ *photons* $\cdot s^{-1}nm^{-1}m^{-2}$), in the time unit Δt [s] and bandwidth $\Delta \nu$ [nm] by the following relation:

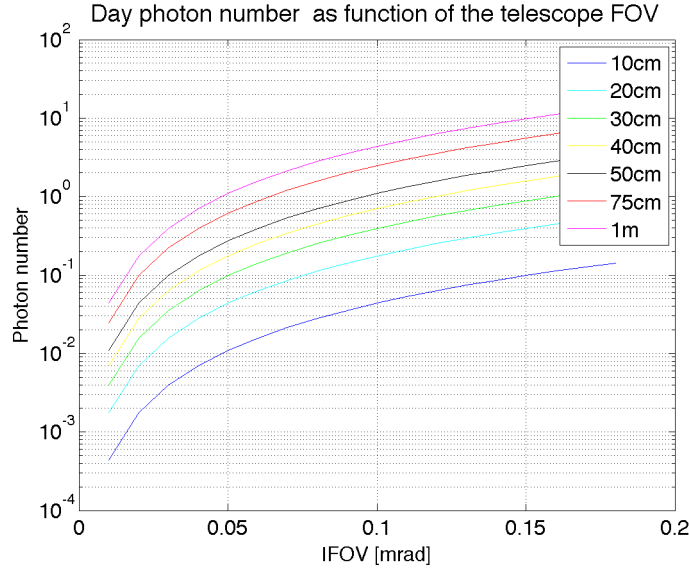
$$N_{Day} = Sa_{Earth}(R_{SpaceT} \cdot IFOV)^2 \sim 1.752 \cdot 10^{18}(R_{SpaceT} IFOV)^2 \quad (3.20)$$

In night time conditions, supposing a Lambertian diffusion of the Moonlight, (albedo a_{Moon} 0.12), the background noise is due to the Moon light diffused by the Earth surface and collected by the satellite telescope of radius R_{SpaceT} .

It is expressed in terms of the **number of collected photons**, which is a function of the telescope Field of View (*IFOV*) [rad], the *Solar constant* S , the time unit Δt [s], the bandwidth $\Delta \nu$ [nm], the Moon-Earth distance $d_{ME} = 384400 \cdot 10^3$ [m] and the Moon radius $R_{Moon} = 1738 \cdot 10^3$ [m] according:

$$N_{Night} = \frac{a_{Moon}a_{Earth}SR_{Moon}^2(R_{SpaceT} IFOV)^2}{d_{ME}^2} \sim 4.298 \cdot 10^{12}(R_{SpaceT} IFOV)^2 \quad (3.21)$$

Figure 3.8: For different telescope diameters[cm], the figure represents the day photon number collected vs. the field of view of the telescope [mrad]. It is assumed that the Earth albedo is 0.38, the Solar constant $S = 4.61 \cdot 10^{18} \text{ ph/s} \cdot \text{nm} \cdot \text{m}^2$ and bandwidth 1nm and detection time of 1ns.



and we observe that the ratio

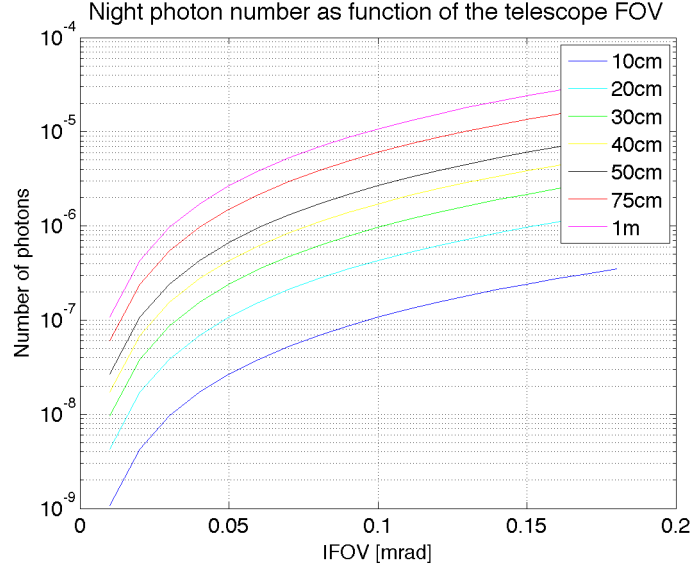
$$\frac{N_{Day}}{N_{Night}} = \frac{d_{ME}^2}{a_{Moon} R_{Moon}^2} \sim 2.758 \cdot 10^{-12} \quad (3.22)$$

Signal to Noise SNR. In the *night-time uplinks*, the SNR is the ratio between (single) signal photons 3.0.3 and noise photons at the receiver, for the bandwidth $\Delta\nu$ and the time of detection Δt and according [3] ($\eta_0 \sim 0.1$) at zenith:

$$SNR = \frac{\eta}{N_{Night} \Delta t \Delta \nu} \sim 2.327 \cdot 10^{-14} \frac{1 - \exp(\frac{-2R_{SpaceT}}{w_{LT}^2}) \Delta t \Delta \nu}{(R_{SpaceT} IFOV)^2} \quad (3.23)$$

We definitely observe in day-time and night-time uplink cases that *the value of background photons (and then the SNR) is directly dependent on the squared product between the telescope radius and field of view*. The figures 3.8 3.9 exploit equations 3.0.3 and 3.0.3 reporting the simulations of background noise supposing uplinks with different telescope radius in night-time and day-time.

Figure 3.9: For different telescope diameters[cm] and assuming a full moon night, the figure represents the night photon number collected vs. the field of view of the telescope [mrad]. It is assumed that the Moon albedo is 0.12, the Earth albedo is 0.38, the Solar constant $S = 4.61 \cdot 10^{18} \text{ ph/s} \cdot \text{nm} \cdot \text{m}^2$ and bandwidth 1nm and detection time of 1ns.



Downlinks. A space-telescope send the signal, collected by an Earth-telescope. The noise power received depends on the sky background brightness H_{Sky} (sky brightness of at least $1.5 \cdot 10^{-5} \text{ Wm}^{-2} \text{ Sr}^{-1} \mu\text{m}^{-1}$ requested for QKD [91]), on the telescope field of view $IFOV_{sr}$ [sr], on R_{EarthT} the Earth-telescope radius and the optical bandwidth $\Delta\nu$ μm according

$$P_{Night} = \pi H_{Sky} \cdot IFOV_{sr} (R_{EarthT})^2 \Delta\nu \propto IFOV_{sr} (R_{EarthT})^2 \Delta\nu$$

Signal to Noise. In night-time downlinks with bandwidth $\Delta\nu$ and time of detection δt , the signal to noise is the ratio between the signal single photons and the noise photons at the receiver $SNR = \frac{\eta h \nu}{P_{Night} \Delta t}$ with h the Planck constant.

Conclusions

For devising an Optical Quantum Communication Network (OQCN), it is necessary to analyze the feasibility of ground-space links.

As known in literature [91] [12], if a laser beam is affected by turbulence degradation at the beginning of its propagation, it arrives far from its unperturbed position.

Otherwise, if affected at the end of its propagation, it is barely modified in its final position. Consequentially, a downlink case is more promising than an uplink one at any orbit considered (in the link distance interval [200km:40000km]) (3.5).

The figure 3.6 shows that in uplinks the beam displacement β is a monotonically increasing contribution, while in downlinks, this contribution is quite negligible.

So, in general, long propagation up/down links are subjected mainly to beam spreading with wandering contribution quite inappreciable.

Beam width charts (figures 3.5, 3.7) show that (at 850nm) the ratio between the uplink and the downlink beam width (for Glonass-GPS-Galileo and GEO orbits) is of about 3 orders of magnitude higher, implying difficulties for quantum communication uplink applications at so high orbits, topic for researches and future technological developments. Besides, as SNR values are intrinsically related to the field of view and the radius of the receiving telescope, quantum communication schemes for uplinks to Galileo orbits, are quite unfeasible nowadays and implementations and new technology are requested for solving this lack. (As some LEO satellites to interface OQCN Galileo Network with the Earth for applying Quantum Key Distribution).

The feasibility of Quantum Communication uplinks and downlinks is so related to distances of order of LEO orbits, with the necessary of take care of the signal to noise (field of view and the telescope radius) and tracking/pointing accuracy issues. Day-time operations are often neglect during the previous discussion as Quantum Communication is unfeasible in day-time as it requests low values of background noise.

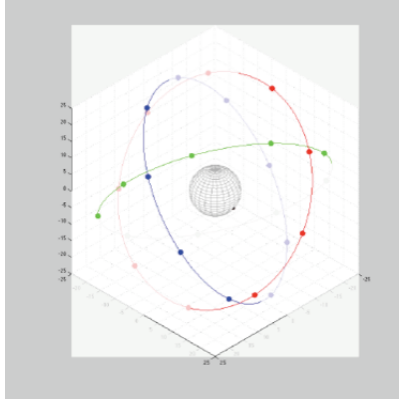


Figure 3.10: Galileo constellation simulated in MATLAB. The colored circles individuates three orbital planes, and the points along the circle indicate the satellites.

3.1 Intersatellite models for OQL

3.1.1 Galileo constellation

In this part we presents the MATLAB simulations for evaluating the time windows in which two spacecraft reach the minimal intra-satellite distance.

The aim is to understand the feasibility of the Optical Quantum Links and to evaluate the expected performance in its entirely and complexity.

GNSS architecture is constituted of nine satellites moving in three orbital planes inclined of 56 degrees. The space segments of the constellation are characterized by *phasing angle* (difference between the argument of latitude of two consecutive satellites, placed in adjacent planes) of $2\pi/27$ and *mean orbital radius* of 29600km.

To model GNSS orbiting satellites we choose a reference frame whose origin is the Earth centre and with z-axis orthogonal to the Earth Equatorial Plane. To simplify the simulation we assume satellite orbits to be circular.

We suppose:

- Satellites orbiting at 23222 km above Earth surface (Galileo altitude) establishing optical communication links propagating *in vacuum*.
- The beam radius function of the link distance according $w_{LT}^2 = w_0^2(1 + \frac{L^2}{z_0^2})$ [?] with z_0 is Rayleigh beam parameter and L the propagation distance.
- Link-efficiency $\eta = \eta_0(1 - \exp(\frac{-2R^2}{w_{LT}^2}))$ with R telescope radius. For theoretical simulation the factor $\eta_0 = 1$ and effective telescope diameter D is $D = \pi w_0$ [?]

Galileo constellation parameters
Number of satellites: 27
Number of planes: 3
Number of satellites per plane: 9
Inclination: 56°
Orbit radius: 29600 km
Node spacing: 120°
Satellite minimum distance: 19000km
Satellite maximum distance: 59000km

Table 3.2: In the table the main parameters for Galileo satellite constellation are reported.

- The SNR as ratio of signal (single) photons and noise photons at the receiver $SNR = \frac{\eta}{N}$.
- In the calculation of the performance of an optical Quantum Link the presence of a light source as the Sun or the Moon in the background could influence even crucially the performance of the link, as the SNR values result altered (in the simulations below the considered value of Noise is 10^6 photons $s^{-1}cm^2nm \cdot sr$) as observed.

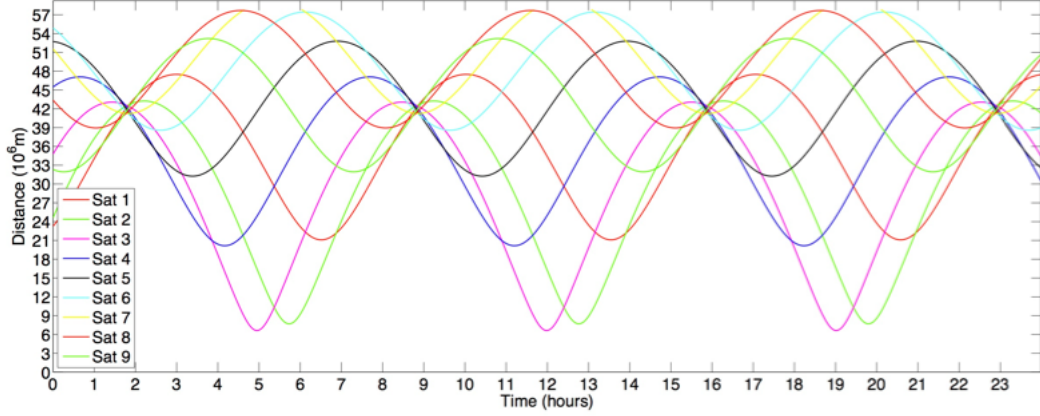
Noise sources in space scenario are zodiacal light due to sunlight reflected by interplanetary dust, and integrated starlight from direct starlight or starlight scattered by interstellar dust. The noise source and photons ratio depends on the observation direction (most of the sources are on the Galactic Plane); considering $1ns$ detection time, $1nm$ filter bandwidth, $100\mu rad$ the telescope field of view, then the number of noise photons collected is $\epsilon_N = H_b IFOV \pi R^2 \Delta\nu \Delta t$ with H_b is the brightness of the space background, $IFOV$ the telescope field ($[sr]$), R the telescope radius $[cm]$, $\Delta\nu$ the optical bandwidth $[nm]$ and Δt the detection time $[s]$.

To model GNSS orbiting satellites we choose a reference frame whose origin is the Earth centre and with z-axis orthogonal to the Earth Equatorial Plane. To simplify the simulation we assume satellite orbits to be circulars.

The following figure 3.11 represents the intra-satellite distance changing between a reference satellite and nine Galileo satellites belonging to a different orbital plane (not containing the reference satellite). Due to the symmetry of the system, the curves referred to the remaining orbital plane would be simply shifted in time.

We fixed the GNSS orbital mean radius at $R = 29600km$ (mean SMA) and show

Figure 3.11: The figure shows the intra-satellite distance between a reference satellite and nine satellites positioned on a different orbital plane.



in the following figure the intra-satellite distances (expressed in kilometers) during 24 hours between a reference satellite and the 9 GNSS satellites belonging to the a different orbital planes not containing the reference satellite.

Due to the symmetry of the system, the curves referred to the remaining orbital plane would be simply shifted in time.

We can also calculate the time intervals in which two satellites of different orbital planes are closer then a reference distance d_0 .

Again, due to the symmetry of the constellation, we show in the following graph only the time intervals between one satellite in one orbital plane and the nine satellites of a different orbital plane. From the figure below, it is shown that the nearest satellites approaches at distances lower than 10000 kilometers for about about 90 minutes, making the QO link feasible within this time window. The following table indicates the intra-satellite minimum distances between each of the nine satellites positioned in the same orbital plane respect to a probe satellite in a different orbital plane (in the configuration considered above).

Minimum distance reached between two closest satellites is 6630 km.

We can observe that the time intervals in which the intra-satellite distances (between one satellite and a second one probe satellite in a different orbital plane) are within 10000 Km is:

- For Satellite 3 (figure) the time-interval is about 96 minutes (5787 seconds) with the minimum intra-satellite distance reached at 6630 kilometers.
- For Satellite 2 (figure) the time-interval is about 82 minutes (4935 seconds) with the minimum intra-satellite distance reached at 7696 kilometers.

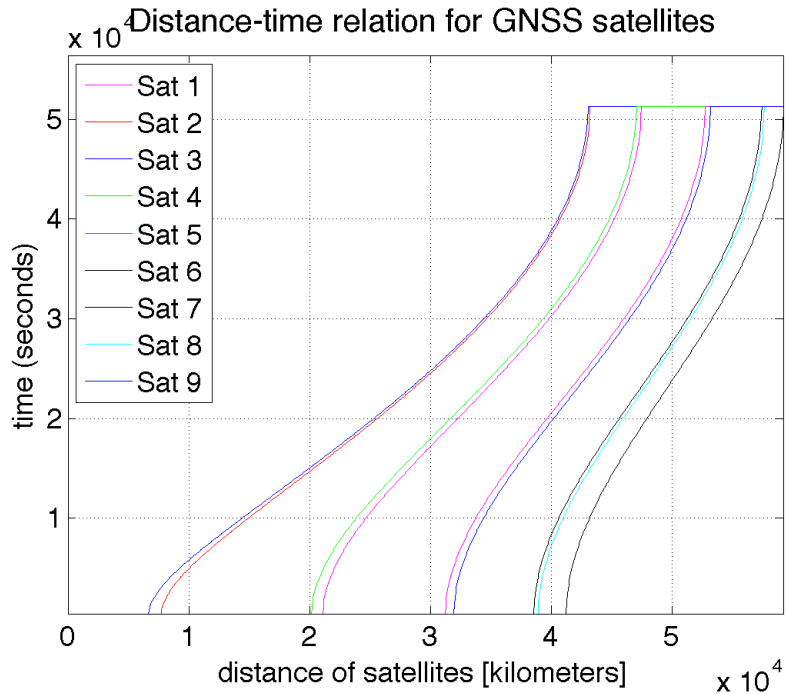


Table 3.3: Chart showing the time interval in which the distance is lower than d_0

Orbit radius	1min	2min	3min	4 min	5min	6min	7min	8min	9min
29600km	6630	7696	20190	21080	31260	31970	38540	38950	41260

Table 3.4: Table showing the minimum value distances for each couple of satellites, referring to the minimum values showed in figure 3.3

The time intervals in which the intra-satellite distances are within 15000 Km are:

- For Satellite 3 (figure) the time-interval is about 176 minutes (10560 seconds)
- For Satellite 2 (figure) the time-interval is about 168 minutes (10090 seconds)

Simulation results

The model previously presented has been used to investigate the link budget and set-up requirements.

In our simulation we consider 3 different telescopes diameters: $0.2m$, $0.3m$, $0.5m$, and a set of wavelength: $350nm$, $400nm$, $450nm$, $532nm$, $800nm$.

Simulations in the figures 3.12 : 3.14, for different laser wavelengths and telescopes radius, show that decreasing the wavelength and increasing the radius, the beam size at the receiver is reduced: this is due to the dependence of beam divergence with wavelength and telescope radius.

$$\theta \propto \frac{\lambda}{w_0} \quad (3.24)$$

In the following figures are reported the simulation results for different wavelength (fixing telescope diameter) and for different telescopes diameters (fixing wavelengths): laser beam radius at the receiver, link attenuation and signal to noise ratio (SNR).

Simulation comments and conclusions

In the following table are summarized the simulation results (using relation $D = \pi W_0$).

Table of simulation results for different distances

$\phi = 50cm$ $\lambda = 50nm$	6600 kilometers	10000 kilometers	19000 kilometers
Attenuation	6.2 dB	9.4 dB	14.7 dB
SNR	65.8 dB	62.7 dB	57.4 dB

$\phi = 30cm$ $\lambda = 532nm$	6600 kilometers	10000 kilometers	19000 kilometers
Attenuation	34.8 dB	38.4 dB	44.0 dB
SNR	41.7 dB	38.1 dB	32.5 dB

$\phi = 20cm$ $\lambda = 800nm$	6600 kilometers	10000 kilometers	19000 kilometers
Attenuation	45.4 dB	49.0 dB	54.6 dB
SNR	34.6 dB	31.0 dB	25.4 dB

As we can observe in the table the best conditions for a OQL in space are reached for $\psi = 50cm$, $\lambda = 50nm$, while the Ma et al. shown that quantum key distribution with entangled photon can tolerate up 35 dB attenuation per single photon channel; the SNR is sufficiently high in all situations and does not represent a problem for QKD realization.

Simulation results define two main conceptual requirements on telescopes diameter and sources:

- Telescope diameter > 20 cm
- Operating wavelength < 532 nm

According to these requirements, we can fix the telescopes diameter to 30 cm, even if it must be considered that others combinations of wavelength and telescope aperture can be interested, even if linked to technological limitations for the devices and optical element employed (let us remember that UV, X ray needs different (not so cheap) devices and optical elements).

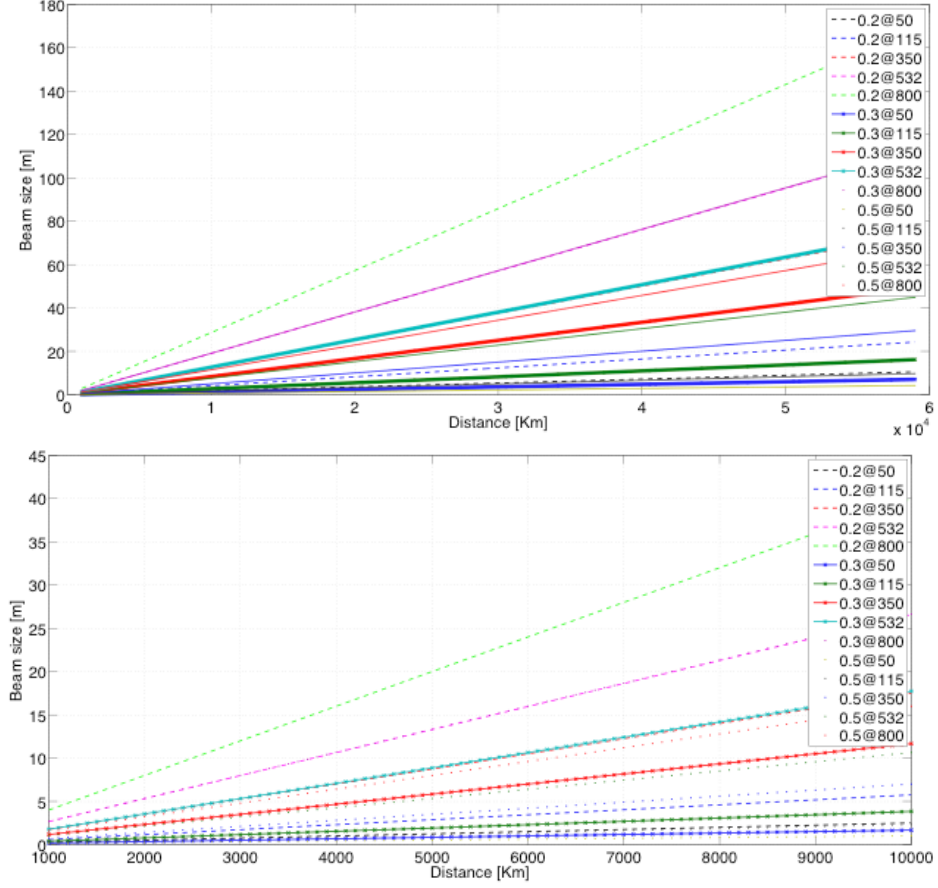


Figure 3.12: Simulations for different beam-size. The figure legend numbers are respectively the diameters in [m] and wavelength in [nm]: (up) trend for the intra-satellite distance [0, 60000] Km using for the Siegmán's formula $W_0 = radius * 0,89$ [?]; (down) focus to the intra-satellite distance [1000, 10000] Km using the previous formula $W_0 = 2 * \frac{radius}{\pi}$

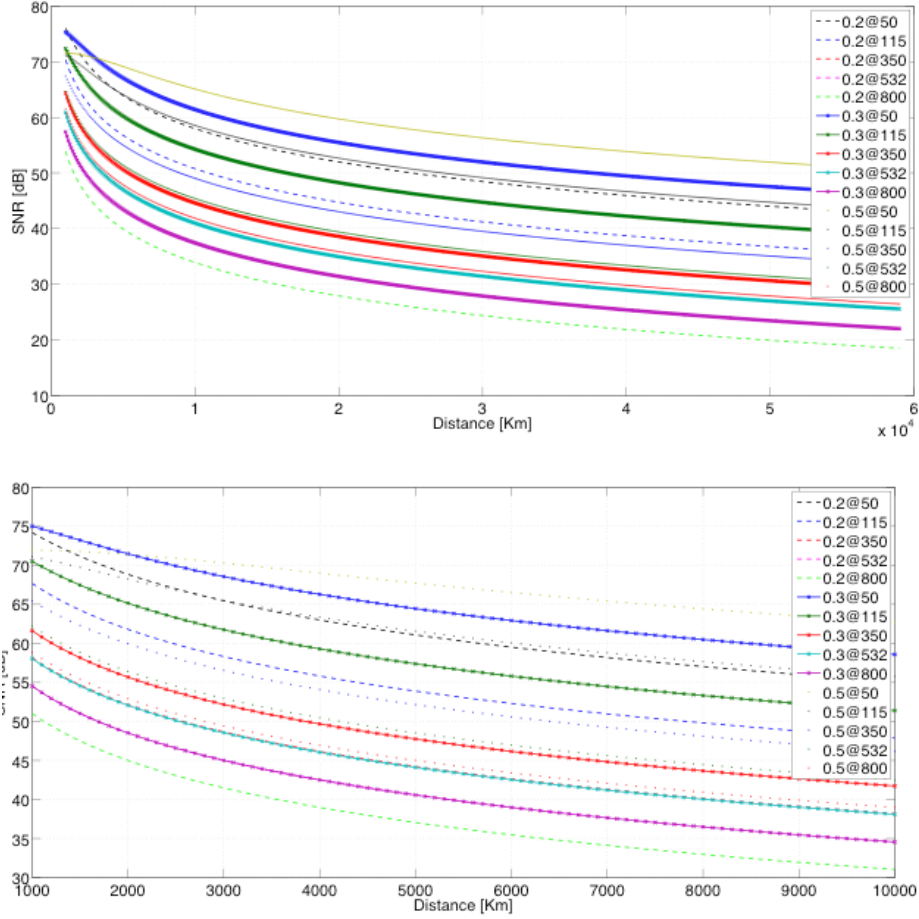


Figure 3.13: Simulations for different beam-size. The figure legend numbers are respectively the diameters in [m] and wavelength in [nm]: (up) trend for the intra-satellite distance [0, 60000] Km using for the Siegman's formula $W_0 = radius * 0,89$ [?]; (down) focus to the intra-satellite distance [1000, 10000] Km using the previous formula $W_0 = 2 * \frac{radius}{\pi}$

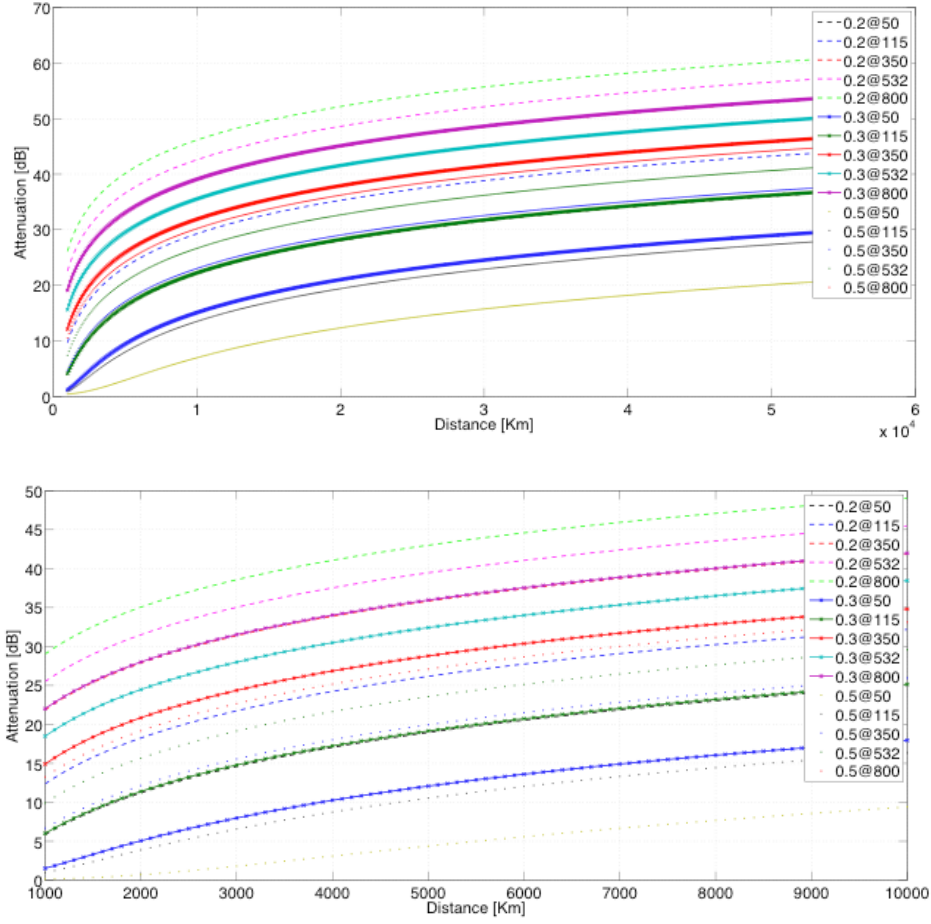


Figure 3.14: Simulations for different beam-size. The figure legend numbers are respectively the diameters in [m] and wavelength in [nm]: (up) trend for the intra-satellite distance [0, 60000] Km using for the Siegman's formula $W_0 = radius * 0,89$ [?]; (down) focus to the intra-satellite distance [1000, 10000] Km using the previous formula $W_0 = 2 * \frac{radius}{\pi}$

Secure Communications technical requirements and conclusions

For a rather general class of QKD systems the secure key rate can be approximately but effectively evaluated through the following relation:

$$R_K \simeq R_0 \mu \exp(-\mu) A \eta (1 - 2h_2(\epsilon)) \cdot P(A, \epsilon, \mu) \quad (3.25)$$

where

- R_0 is the **raw key rate** at which bits are output from the transmitter
- μ is the mean number of photon/bit at eavesdropper and the fraction of single photon/bits in Poisson statistics (in the faint laser regime) A are the losses depending on diameter of the receiver, wavelength and intra-satellite distance (see graph above) η is the protocol efficiency (0.5 for BB84 protocol and 0.25 for B92 protocol) ϵ is the Bit Error Rate over the quantum channel $1 - 2h_2(\epsilon)$ is the rate reduction due to error reconciliation with

$$h < -2(\epsilon) = -\epsilon \log_2 \epsilon - (\epsilon) \log_2 (1 - \epsilon) \quad (3.26)$$

[27]

- $P(A, \epsilon, \mu)$ is the compression factor for privacy amplification margin ($\geq 1/2$) [17].

Considering the previous table for OQL with different wavelengths and telescope apertures, the Secure Key Rate expected according the relation at different range in kilometers are:

$\phi = 50cm$ $\lambda = 50nm$	6600 kilometers	10000 kilometers	19000 kilometers
Attenuation	6.2 dB	9.4 dB	14.7 dB
Raw Key Rate	1.78E07 bit/s	8.64E06 bit/s	2.47E04 bit/s
$\phi = 30cm$ $\lambda = 532nm$	6600 kilometers	10000 kilometers	19000 kilometers
Attenuation	34.8 dB	38.4 dB	44.0 dB
Raw Key Rate	2.47E04 bit/s	1.08E04 bit/s	2.98E03 bit/s
$\phi = 20cm$ $\lambda = 800nm$	6600 kilometers	10000 kilometers	19000 kilometers
Attenuation	45.4 dB	49.0 dB	54.6 dB
Raw Key Rate	2.16E03 bit/s	9.41E02 bit/s	2.60E02 bit/s

The distance intervals in which we calculated the Raw Key Rate values are the following:

- 6600 Km: the minimum distance at which satellites of different orbital planes can approach each other.
- 10000Km: a reliable distance in which operate for the best performance of a Quantum Link between satellites of different orbital planes in GNSS constellation. (10000 Km)
- 19000Km: the minimum distance between two satellites positioned in the same orbital plane.

We can observe, from the above table, that the best values in raw key rates (18Mbits/s at 6600 kilometers, related to lower attenuation values) are obtained for a telescope diameter of 50cm and wavelength of 50nm , while the worse values in raw key rates (2.2Kbits/s at 6600 kilometers, related to higher attenuation values) are for a telescope diameter of 20cm and wavelength of 800nm .

3.1.2 Space-based Global Quantum Network

Finally the expected scenario for a space Quantum Key Distribution network is based on sharing a cryptographic random secret key (encoded by polarization of photons) by the quantum channel between a transmitting point and a receiving one.

For a (down)link scenario the Quantum Channel [?] performed by an Earth orbiting satellite can be devised in two ways: either establishing two independent quantum links simultaneously by entanglement correlations, or using the satellite as a trusted node between two Earth stations ⁴ The former case imposes some restrictions about the achievable distance between the receiving ground based stations on earth surface: for big zenith angle the links would experience too many atmospheric losses due to the increasing of atmospheric layers crossed by the laser beam. (As observed in section Quantum Communication Uplinks and Downlinks between Space and Earth). The latter case supposes two different secure key each established between the satellite and one ground station: it is supposed that the satellite orbits over the first ground segment establishing a secure key K_1 and then moving above the second ground station, establishing a different secure key K_2 in two different times. Then the key K_1 is encrypted with the second key K_2 , and so $K = K_1 \otimes K_2$ is sent to the ground station, allowing the first ground station to decrypt the second key K_2 .

This model has the advantage to establish simple single quantum links between space and ground at a time; but besides being more cost-effective, it has the drawback that the secureness of the scheme is based on the unassailability of the satellite, as the satellite possesses the secure key with which two ground stations communicate, supposing that an eavesdropper might violate the key storage of the satellite obtaining primary importance information.

⁴or eventually one Earth station and a further second satellite

Model for Quantum Communication system: source, channel and detector

Here we recall a general model of Quantum Communication Scheme.

- The optical transmittance of the channel of length L [m] in the fiber case is:

$$T_{Channel} = 10^{-\frac{L\alpha}{10}} \quad (3.27)$$

and α the loss coefficient [dB/m] If the internal transmittance of receiver optical components is T_{Rec} and the detector efficiency is $\eta_{Detector}$, the optical transmittance at the receiver becomes:

$$\eta_{Rec} = \eta_{Detector} T_{Rec} \quad (3.28)$$

So the overall efficiency η_{Sys} (transmission and detection) is given by the relation:

$$\eta_{Sys} = T_{Channel} \eta_{Rec} = 10^{-\frac{L\alpha}{10}} T_{Rec} \eta_{Detector} \quad (3.29)$$

Assuming at the receiver side a detector threshold and assuming the independence between the behavior of the photons in n-photon states, the transmittance of n-photon state η_n respect to a threshold detector is given by the following relation:

$$\eta_n = 1 - (1 - \eta)^n \quad (3.30)$$

for $n = 0, 1, 2, ..$

- The laser **SOURCE** of the QKD system is assumed to be a weak coherent state: the photon number of each pulse follows a Poissonian distribution with mean photon number μ . The density matrix of the emitted state is given by:

$$\rho = \sum_{n=0}^{\infty} \frac{\mu^n \exp(-\mu)}{n!} |n\rangle \langle n| \quad (3.31)$$

[?] with the density matrix of n-photon state $|n\rangle \langle n|$.

- Let us suppose that the background counts do not depends on the signal photon detection. The contributions of these two counterparts, background and true signal are dominant for the yeld of n-photon state Y_n . The Yeld is the conditional probability of a detection event at the receiver part given that the transmitter sends out an n-photon state.

$$Y_n = Y_0 - Y_0 \eta_n + \eta_n \simeq Y_0 + \eta_n \quad (3.32)$$

for $n = 0, 1, 2, ..$

- For a coherent state the **gain** is given by the relation [?] :

$$Q_\mu = \sum_{n=0}^{\infty} Y_n P_n(\mu) = \sum_{n=0}^{\infty} \frac{Y_n \mu^n \exp(-\mu)}{n!} = Y_0 + 1 - \exp(-\mu\eta) \quad (3.33)$$

The **Quantum Bit Error Rate (QBER)** for the signal state is given by the relation:

$$E_\mu = \sum_{n=0}^{\infty} \frac{e_n Y_n P_n(\mu)}{Q_\mu} \quad (3.34)$$

with $P_n(\mu)$ the Poisson distribution for strongly attenuated sources, Y_n the yield of n photon pulses.

The **Error Rate** of n -photon signal is

$$e_n = Y_0/2Y_n \quad (3.35)$$

Summarizing:

<i>Emitted state Density matrix</i>	$\rho = \sum_{n=0}^{\infty} \frac{\mu^n \exp(-\mu)}{n!} n\rangle \langle n $
<i>Overall system efficiency</i>	$\eta_{Sys} = T_{Channel} \eta_{Rec}$
<i>Yield</i>	$Y_n = Y_0 + \eta_n$
<i>Gain</i>	$Q_n = \frac{Y_n \mu^n \exp(-\mu)}{n!}$
<i>Overall gain</i>	$Q_\mu = Y_0 + 1 - \exp(-\mu\eta)$
<i>Bit error rate</i>	$e_n = \frac{\exp(-\mu)[e_0 Y_0 + e_{Detector} \eta_n]}{Y_n}$
<i>Overall QBER</i>	$E_\mu Q_\mu = e_0 Y_0 + e_{Detector} (1 - \exp(-\eta\mu))$

Key generation rate and Decoy state scheme

Here we present the model for evaluating the key generation rate [?] .

We evaluate the **lower bound for the key generation rate**:

$$R \geq q \left\{ -Q_\mu f(E_\mu) H_2(E_\mu) + (1 - \Delta) Q_\mu (1 - H_2(\frac{E_\mu}{\Omega})) \right\} \quad (3.36)$$

with q the protocol efficiency (1/2 for BB84 and 1/4 for B92), Q_μ the gain of the signal state, E_μ the Quantum Bit Error Rate of the signal state (QBER), $f(E_\mu) = 1.22$ the bidirectional error correction efficiency, H_2 the Shannon binary entropy expressed by the relation (for a variable x):

$$H_2 = -x \log_2 x - (1 - x) \log_2 (1 - x) \quad (3.37)$$

Δ is the portion of the tagged bits by the eavesdropper for Photon Number Splitting (PNS) attack.

Nowadays science research is not able to build single photon sources. So *attenuated weak sources* are generally uses as single photon sources in Quantum Key Distribution experiments. This is uncorrect, as occasionally they produce more that one photon, opening to the possibility of sofisticated eavesdropping attacks.

Photon Number Splitting (PNS) is one of them, as it is based to the fact that the eavesdropper is able to block all single-photon and multi-pulses photons coming from the transmitter; the eavesdropper splits them into two sets, each containing at least one photon: the former set contains groups of *only one single photon* that he sends to the receiver through a lesslossy channel. The latter contains groups of *at least single photons or more* that he kept for himself. In PNS attack, Δ represents the probability that an eavesdropper can obtain part of the transmitted bits and it is defined as the ratio between multi-photon pulses and non empty pulses detected by the receiver.

Let us note that in a high loss channel, multi-photon pulses have a higher probability to be received by Bob, and to exposed to eaversdropper attacks.

Δ depends on *the mean photon number of the state* μ and *the link attenuation* η according the relation:

$$\Delta = \frac{1 - \exp(-\mu) - \mu \exp(-\mu)}{1 - \exp(-\eta\mu)} \quad (3.38)$$

The result is that the key generation trends for QKD protocols with decoy states turns longer, as observed in the next sections.

Decoy State simulations for OQL

As exploited in the previous section, the two-decoy state protocol uses two decoy state (with mean photon numbers ν_1, ν_2) and one signal state with mean photon numbers μ , with $\mu > \nu_1, \nu_2$.

The transmitter chooses one of the decoy state intensities and send a train of pulses to the receiver, in order to probe the communication channel (obtaining information about the presence of an eavesdropper and about the channel attenuation).

Considering a two-decoy state scheme (vacuum and weak decoy state), the Key Generation rate formula is given by: [57]

$$R_{\geq q} \{-Q_{\mu} f(E_{\mu}) H_2(E_{\mu}) + (Q_1^L (1 - H_2(e_1^U)))\} \quad (3.39)$$

with the lower bound for Y_1 : [?]

$$Y_1^L \big|_{\nu_1 \rightarrow 0}^{\nu_2 = \nu} = \frac{\mu}{\mu\nu - \nu^2} (Q_{\nu} \exp(\nu) - Q_{\mu} \exp(\mu) \frac{\nu^2}{\mu^2} - Y_0 \frac{\mu^2 - \nu^2}{\mu^2}) \quad (3.40)$$

so the relation for the *gain of a single photon state* is given by:

$$Q_1^L \big|_{\nu_1 \rightarrow 0}^{\nu_2 = \nu} = \mu \exp(-\mu) Y_1^L \quad (3.41)$$

$$Q_1^L \big|_{\nu_1 \rightarrow 0}^{\nu_2 = \nu} = \frac{\mu^2 \exp(-\mu)}{\mu\nu - \nu^2} (Q_{\nu} \exp(\nu) - Q_{\mu} \exp(\mu) \frac{\nu^2}{\mu^2} - Y_0 \frac{\mu^2 - \nu^2}{\mu^2}) \quad (3.42)$$

The Δ fraction of tagged photons is: [?]

$$\Delta = \frac{\nu}{\mu - \nu} \left(-1 + \frac{Q_{\mu} \nu \exp(-\nu)}{Q_{\nu} \mu \exp(-\mu)} \right) + \frac{Y_0 \nu \exp(-\nu)}{\mu Q_{\mu}} \quad (3.43)$$

The *error rate* is given by the relation (upper bound):

$$e_1^U \big|_{\nu_1 \rightarrow 0}^{\nu_2 = \nu} = \frac{\exp(\nu) \cdot Q_{\nu} E_{\nu} - Y_0 e_0}{\nu Y_1^L} \quad (3.44)$$

$$e_1^U \big|_{\nu_1 \rightarrow 0}^{\nu_2 = \nu} = \frac{\exp(\nu) \cdot Q_{\nu} E_{\nu} - Y_0 e_0}{\nu \frac{\mu}{\mu\nu - \nu^2} (Q_{\nu} \exp(\nu) - Q_{\mu} \exp(\mu) \frac{\nu^2}{\mu^2} - Y_0 \cdot \frac{\mu^2 - \nu^2}{\mu^2})} \quad (3.45)$$

Assuming that an eavesdropper is able to intercept all the multi-photon pulses, the multi-photon tagging drastically reduces the key generation rate.

Assumuming that the mean photon number of the signal state is $\mu = 0.4$, and considering 4 information wavelengths (350nm, 532nm, 850nm, 1550nm) and 3 telescope apertures (20cm, 30cm and 50cm), the key generation rate is reduced according the figure 3.1.2:

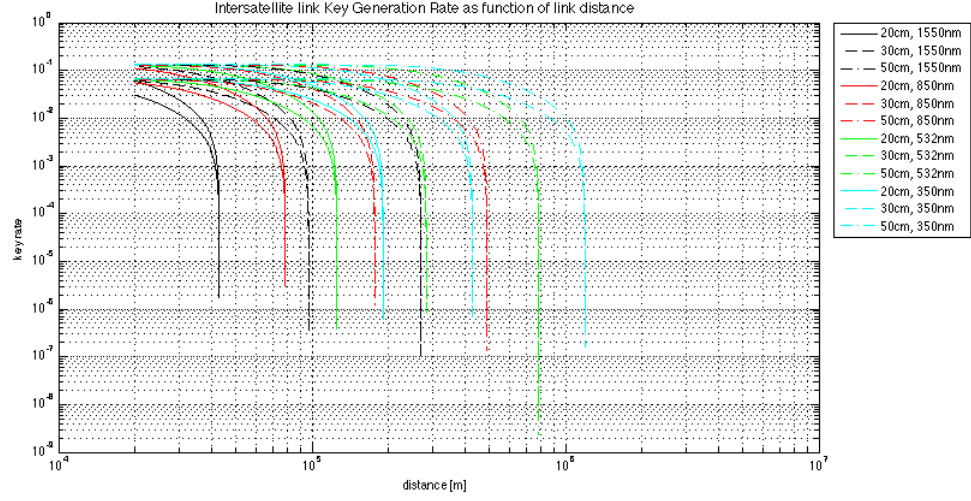


Figure 3.15: Figure: Simulations about key generation rate with 4 information wavelengths (350nm, 532nm, 850nm, 1550nm) and 3 telescope apertures (20cm, 30cm and 50cm). The key generation rate is reduced as the eavesdropper can perform multi-photon tagging (PNS attack). Thicker lines deal with the key generation for BB92, thinner lines deal with the key generation rate for BB84 scheme.

In the figures 3.16 we report the key generation rate simulated for intersatellite links, using a BB84 protocol with a two-decoy state (with $\mu = 0.4$ and $\nu = 0.27$). From the figure 3.16 we observe that the key generation trend for BB84 is longer in 3.1.2 as performed with decoy state scheme. In the following table, for a fixed telescope aperture (20cm) we report the corresponding key rate values [kb/s] at the distance d , supposing to perform BB84 scheme with two weak decoy schemes, with mean photon number of $\mu = 0.4$, decoy scheme based on vacuum and weak decoy (with $\nu = 0.27$).

$\phi = 20cm$	$d = 2E4$	$d = 1E5$	$d = 1E6$	$d = 2.5E6$
$\lambda = 350nm$	0.13	$5.64E - 2$	$7.86E - 4$	$1.37E - 4$
$\lambda = 532nm$	0.13	$2.98E - 2$	$3.61E - 4$	$6.13E - 5$
$\lambda = 850nm$	0.11	$1.30E - 2$	$1.45E - 4$	$2.46E - 5$
$\lambda = 1550nm$	$6.58E - 1$	$4.09E - 3$	$4.56E - 5$	$4.79E - 6$

The table shows that the key rate decreases according the link distance. And at same distance values, shorter wavelengths present higher values of key rate.

Analysing the relation between diameter and key rate, we can observe that for same

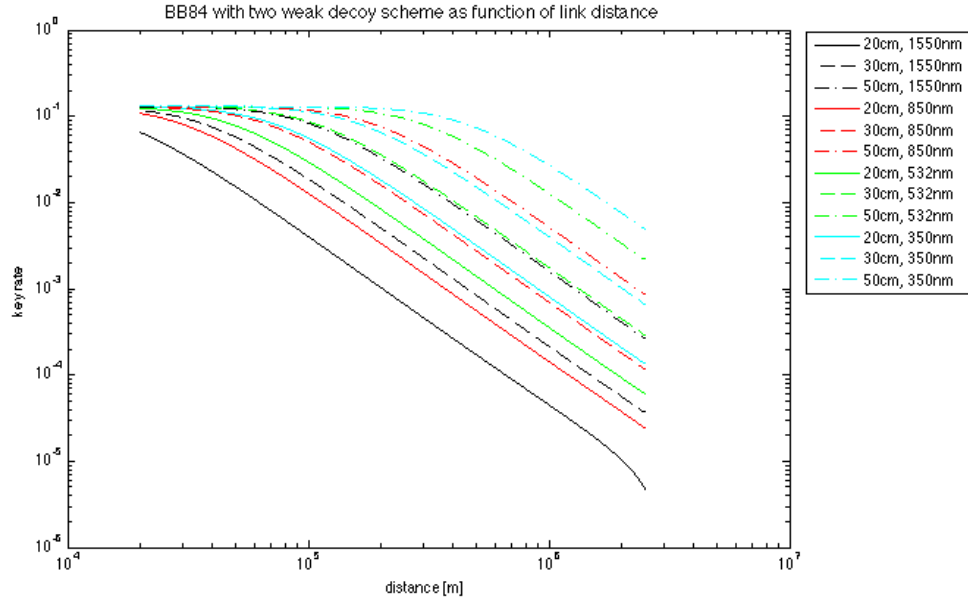


Figure 3.16: Figure: key generation rate for BB84 QKD protocol performed with decoy state scheme considering 4 wavelengths (350nm, 532nm, 850nm, 1550nm) and 3 telescope apertures (20cm, 30cm and 50cm). The decoy scheme uses mean photon number of $\mu = 0.4$ for information state, vacuum and weak decoy (with mean photon number $\nu = 0.27$).

wavelength and at same distance values, larger apertures present higher values of key rate. As observed in the following table.

$\lambda = 350nm$	$d = 2E4$ m	$d = 1E5$ m	$d = 1E6$ m	$d = 2.5E6$ m
$\phi = 50cm$	0.13	0.13	$2,69E - 2$	$4.99E - 3$
$\phi = 30cm$	0.13	0.11	$4.05E - 3$	$6.69E - 4$
$\phi = 30cm$	0.13	$5.64E - 2$	$8.24E - 4$	$1.37E - 4$

Galileo Optical Quantum Network will guarantee intrinsically secure key exchanging, free of PSN attack, within a satellite distance signed by decoy scheme approach. The decoy model applied to the Quantum Communication System shows that for same wavelengths and within same beam propagation distances, larger apertures present higher values of key rate[bit/s].

At the same time, we have observed that shorter operating wavelengths presents higher values of key rate. As Galileo operative wavelength in space will be chosen shorter than 800nm, decoy schemes could be applied with success to Galileo constellation in order to beat PNS attack over well defined communication links in relation to the link distance covered, the operative wavelength and the telescope aperture.

Note: Optimal Mean Photon Number vs QBER

In Quantum Communication, a clue issue is choosing a good mean photon number, as it is correlated to the Quantum Bit Error Rate.

For the determination of the optimal mean photon number reports the relation

$$\mu_{Opt} \simeq \frac{1}{2} [1 - \frac{h(Q)}{1-h(Q)}]$$

with that $h(Q)$ the Shannon binary entropy

$h(q) = -x \log_2(x) - (1-x) \log_2(1-x)$ The relation between QBER and Mean Photon Number is plotted below in the figure ?? : the mean photon number chosen for the previous decoy state simulations satisfies the Scarani relation.

For Decoy Scheme we choosed $\mu = 0.4$, according to [?].

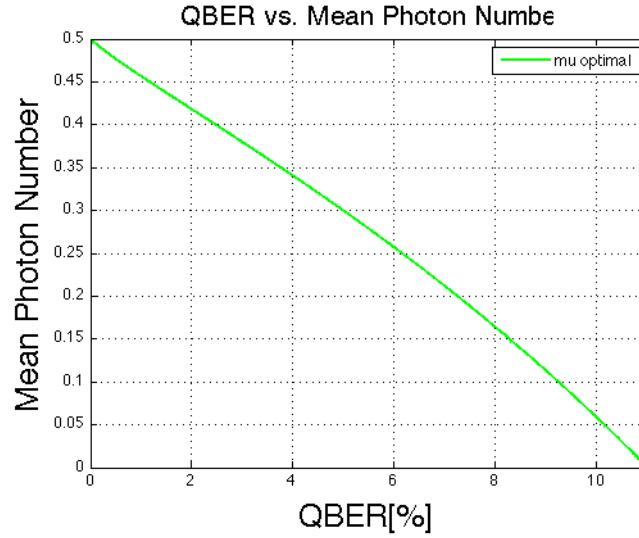


Figure 3.17: The image show the relation between Mean Photon Number and QBER.

3.2 Conclusions

In this chapter, according the requests of the ESA project, we have investigated about the feasibility of Optical Quantum Communication Links for Galileo constellation.

Finally, it is clear that Galileo has the potential to perform the Optical Quantum Communication, creating a unique satellite network, competitive in data rate exchanging, in security level, and at the cutting edge of technology and information science. A network which could be easily implemented for the merits of lightness, compactness and low power consumption (of the optical technology).

The simulations reported have exploited the relative motion of satellites lying in different orbital planes, showing that it is possible to target communication between satellites that are closer in turns, and to achieve appreciable transmission rates and secret key lengths. In this sense, Galileo network will be able to overtake the communication difficulties due to the huge space distances, by devising a spider web structure, an "ad hoc" topology of approaching satellites, communicating only within a chosen distance. (The topology will be discussed at the beginning of next chapter). Besides all, for today information-based society security issues are of paramount importance: Galileo quantum network will guarantee intrinsically secure key exchanging, free of PSN attack, within a satellite distance signed by decoy scheme approach. Unfortunately, the time is not ripe, yet, for Quantum Communication between space Galileo network and Earth: recalling previous studies and researches about uplinks and downlinks, we have shown that Quantum Communication can be devised within space LEO and Ground: atmospheric perturbations are the main source of limita-

tions, making unfeasible uplinks or downlinks between MEO satellite as GLONASS, GPS and Galileo and the Earth, with current technology.

A solution, in this sense, could be suggested. A supporting space segment in Low LEO orbit could reinforce the network.

In conclusion, we have seen that in some conditions the extension of quantum communications and technologies appears feasible in the new realistic scenario of the Galileo Optical Quantum Network.

Chapter 4

APPLICATIONS OF OPTICAL QUANTUM LINKS TO GNSS: second phase

4.1 Optical Quantum link techniques for secure communications

Today's economy and society is calling with ever growing needs for secure communications.

In this context, the quality of the key, its randomness, and the possibility to generate a perfectly matched key set remotely are techniques of paramount importance.

Quantum Key Distributions, *QKD*, is the only way to assure it by distributing keys for encryption at a global scale: making use of Quantum Mechanics the messages are surely encrypted, the presence of an eavesdropper is detected, and further, Quantum techniques applied in space may permit to increase the performances of intra-satellite communication or satellites-ground station communication.

The valuable features of Quantum Communication (science and technology of sharing a Quantum state of an elementary particle) and in particular of Quantum Key Distribution in the context of a satellite constellation are mainly to allow the increasing of the number of users of secure communication services, related to data transfer, telemetry, tele-command transfer and key distribution in order to protect navigation mission or navigation systems, while the merit of the optical link is to increase the available bandwidth and the aim is to move the initial step to extend Quantum Communication to secure communications in the context of GNSS.

Studies and experiments of QKD by the long range propagation of single photon, along a space quantum channel, even modelling up-link and down-link for ground-space communication have been performed, [12] [89] and from a security perspective, the free-space Quantum Communication approach proposed in this studies will provide the means to implement the exchange of quantum cryptographic keys with an

intrinsically secure protocol.

A breakthrough in mathematics or computer science could make current electronic money transfer encryption methods (such as *SSL* or *RSA*) instantaneously vulnerable. This is because the security of classical cryptography relies on the (currently unproven) classical computational difficulty of certain mathematical functions. Hence, classical cryptography does not guarantee absolute and unconditional security, and any future quantum computer would enable solving exactly the mathematical functions in use today to encrypt data in polynomial time: *QKD* implementation looks essential in order to avoid that any quantum computer would be able to capture the plain text from the encrypted message within a very short time frame compared to its classical counterpart.

QKD advantages are introduced here in a brief general description of cryptographic scheme.

The general and most intuitive scheme for secure communication in QKD is called *symmetric key cryptography*, symmetric, as the cryptographic key used at the transmitter is the same at the receiver. If a source S takes a secure key K , a key that must be shared with the receiver, and encodes the message x , called plain text, it obtains the cipher text y , the function that performs the encoding, called cipher. As was proven by Shannon, there is only one algorithm, so far, that is mathematically unconditionally secure, and it is the classical algorithm called **One Time Pad** (*OTP* or Vernam Code), a very simple one: take a message x , take a key k and sum them: *OTP* acts the sum modulus A , with A the dimension of the alphabet.

For unconditional security the key k has to satisfy the next properties:

- $k \in \text{Alphabet}$
- $k \in U$, perfectly random variable
- $\text{length}(k) = \text{length}(x)$
- k must be used only one time

The problem of security is shifted then to another issue: the distribution of random keys in a secure way.

Quantum Cryptography can help to solve the problem just mentioned of distribution of random keys in a secure manner: it cannot be used to communicate information in a secure way but it can indeed be used by two users to share a cryptographic key between each other (that is why we normally call quantum cryptography with the name of quantum key distribution).

Let's give a definition of quantum key distribution that resumes the main feature of the idea: a quantum key distribution system is a telecommunication system that can create a perfectly secure symmetric key at the transmitter and at the receiver. It needs two communication channels:

- 1 Quantum Channel, for the transmission of the quantum bits.
- 2 Classical Public Channel, for the communication of classical messages between the transmitter and the receiver.

The security of Quantum Cryptography relies on the fact that it uses the laws of Nature: each measurement on a quantum system perturbs the system itself; an innovative idea expressing that each measurement in some way perturbs the state that is traveling in the quantum channel, fundamentally based on the no-cloning theorem that states that it is not possible to perform a perfect copy of a quantum state.

Next generation navigation systems will be characterized by better (navigation performances in terms of accuracy, integrity, continuity, availability) and by the possibility to exploit dual use operation, thus increasing their robustness, resilience, security, as well as their autonomy features.

As observed in Chapter 3, free-space optical communications are an attractive alternative to RF communication links as they are characterized by higher antenna gain, higher data rates, better security, etc. Defense applications can exploit the intrinsic robustness offered by this technique against interception, eavesdropping and jamming, thanks to the narrow beamwidth [45].

A number of space missions have successfully tested optical communication techniques in space with excellent performances [88][93][1][11] [54] [82] [72] promising in the field of quantum communications, in which security applications are of particular interest.

Security issues are a key point in the development of GNSS system, not only with respect to the protection of the GNSS service signals against spoofing and/or jamming [66] [48] , but even more relevantly for the authentication, integrity and confidentiality of the control signaling traffic, and hence for the protection of the infrastructure itself.

The impact of a malicious adversary hijacking GNSS satellites and acquiring their control may prove catastrophic.

It should be noted that narrowbeam optics may not provide sufficient security, since the beam traveling over thousands of kilometres will still be spread by, say, a few hundred meters. Since its radius is far larger than the size of an attacking terminal, interception may not be detected as the legitimate receiver will not experience a significant loss.

Similarly, as the beam radius is also much larger than the legitimate receiver size, an attacker may eavesdrop or forge a transmission by simply positioning itself behind the receiver, or the transmitter, respectively, even at an appreciable distance.

A further advantage in the application of optical communication to space is that

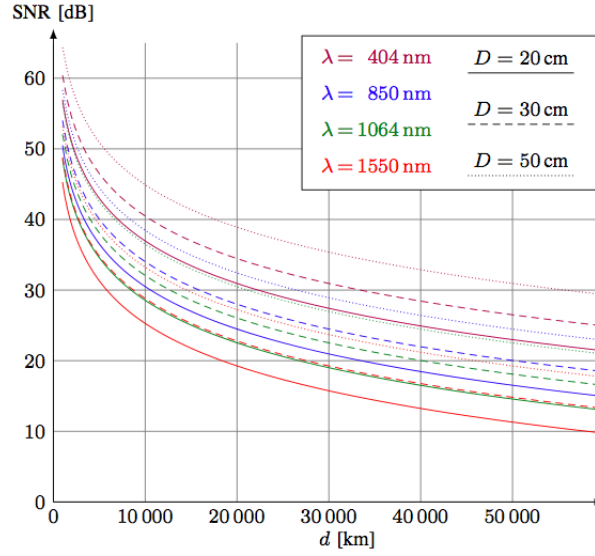


Figure 4.1: The figure shows the simulated SNR vs link distance for different telescope diameters and wavelengths (indicated in the legend as “diameter[m]@wavelength[nm]”).

the turbulence of the terrestrial atmosphere is completely removed, keeping almost unchanged the beam characteristics.

Recalling Chapter 3 analysis, we have observed that simulations of propagation outside the atmosphere for different laser wavelengths and telescope radii show that by decreasing the wavelength and increasing the telescope radius, the beam size at the receiver is reduced, and so is the attenuation, while the SNR increases: this is due to the dependence of beam divergence with wavelength and telescope radius. In the figure 4.1, it is reported a simulation about SNR results vs link distance for three different telescope diameters: 0.2m, 0.3m, 0.5m, and for the following wavelength values: $\lambda = 404$ (not yet proposed for space use), $\lambda = 800nm$ (see e.g., [93] [1]), $\lambda = 1064nm$ (as used in [11]), or $\lambda = 1550nm$ (proposed in [54] [82] [72]).

The wavelength selection is mainly dictated by the availability of sources and detectors and by their space qualification level, and within such constraints, a shorter wavelength provides lower diffraction losses along the free space channel.

Therefore, as observed in Chapter 3 analysis, although previous works have used longer waves, we aim to adopt $\lambda < 800nm$.

Considering the dimensions of current space optical terminals, it seems that a good compromise between achievable antenna gain and instrument size is given by telescope diameters around 0.2 m. As regards its optic configuration, this would ideally be of the Ritchey-Chretien type, but Cassegrain and Newtonian configurations are also appropriate.

4.2 Payload conceptual design

The working blocks of SaNe-QKD OPT are:

- Transmitter: Alice on satellite terminal or ground terminal
- Bob on satellite terminal or on ground terminal
- Auxiliary Functions and Electronics for both Terminals

Quantum Communication setup of the mission is composed of two terminals, the former located on board of the first GNSS satellite, the latter located on board of a second GNSS satellite in case of intra-satellite Quantum Communication, or in case of satellite-ground link on Laser Ranging Observatory at Earth (e.g. MLRO, Matera Laser Ranging Observatory).

Space and ground Terminals are characterized by some blocks, which constitute the conceptual payload of the GNSS satellite.

GNSS satellite payload is constituted of Telescope Block (TB), Alice-Bob Module (ABM), Ranging Module, Auxiliary Function ST (AFST), Electronics ST (EST) (or Electronics GT named for the ground segment).

- **Telescope Block (TB):** This is dedicated to the telescope (transmitting/receiving antenna).
- **Alice-Bob Module (ABM):** Alice Module is constituted of a QKD transmitter (in QKD Module) with the possibility to implement ground-satellite and intra-satellite decoy-state QKD by attenuators interposition on the output beam. Protocols BB84 or B92 can be implemented by the use of strongly attenuated lasers: four linearly polarized laser diodes, each one emitting a specific state (horizontal, vertical, $+45^\circ$, -45°), are used for the purpose. A photo-diode will be used to monitor the power of the four lasers, to check the performance of each laser in order to keep stable the mean photon-number on a long time scale.
Bob Module is constituted of a receiver for qubits implemented with polarization-encoded single photons (positioned in QKD Module). The input port receives a stream of photons, and passively distributes them at random between two measurement setups, one working in the horizontal-vertical basis, the other on the linear basis rotated at 45 degrees. The output is a click of one of the four single-photon detectors, which corresponds to a possible polarization state. Such detection events must be time-tagged and stored in memory.
- ranging Module is a block for performing classical ranging between satellites, or satellites and ground station.

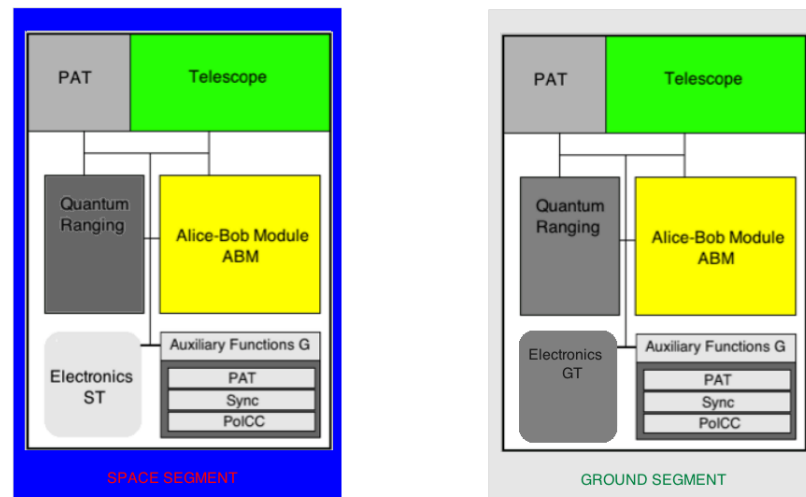


Figure 4.2: Working blocks for space segment and ground segment

- The Auxiliary Functions ST block (or GT for the Ground Segment), which contains all the functionalities needed to support the system operational: PAT (pointing, acquisition and tracking), synchronization and polarization control. For a Satellite-Terminal (ST) module, it is supposed to provide all the functions necessary to correctly perform the photon exchange between the Satellite and Satellite or Satellite and Ground Terminal. In particular it will take care of:
 - Pointing, acquisition and Tracking (PAT)
 - Temporal synchronization of the two terminals (Sync)
 - Polarization characterization, alignment and control of the ground and space terminals, (PolCC)

Pointing, Acquisition and Tracking (PAT)

The issues of Pointing, Acquisition and Tracking are very important for the mission, due to some contrasting aspects:

- The rapidity of the satellite passage – (if the satellite is seen from Ground Segment), with consequent fast change in the link length, and as rapidity in tracking and pointing is necessary too in Space-Space OQL (See simulations)
- The accurate pointing of the Space Segment or Ground Segment in the intra-satellite OQL
- The narrow field-of-view FOV necessary to minimize the background noise flux
- The asymmetrical effect of atmospheric turbulence in the down- or upward propagations,
- The correction of the satellite motion on pointing.

4.3 Secure communication for SaNe-QKD

Quantum Communication is the art of sending quantum states from one place to another, with the information encoded by Quantum states, hence Quantum Communication is the transmission of Quantum Information.[39]

One of the crucial results of Quantum Communication is Quantum Cryptography. Quantum Cryptography is one of the crucial results of QC, promising intrinsically secure communications. An encrypted scheme entails the distribution of a secret key between legitimated parties.

Secure Communications

Secure Communications (SC) aim at allowing confidential transmission of information between different parties performing privacy, authentication and confidentiality

issues between the users. History starts with one-time-pad encryption –invented by Vernam (1917) [99] - which uses a symmetric random secret key shared between sender and receiver. This scheme cannot be broken in principle if the parties do not reuse their key and the key is really random.

Three decades later, Shannon proved in addition that the Vernam scheme is optimal: there is no encryption scheme that requires less key length [78].

The users need only a secure method to share the key. In the 80s Bennet and Brassard [9] proposed a solution based on Quantum Physics for the key distribution issue; this idea, optimized by Ekert [26] in the early 90s was the beginning of the Quantum Key Distribution (QKD).

In an intriguing independent development, Shor [79] discovered that large integers can - in principle - be factorized efficiently performing coherent manipulations on many quantum systems. The factorization of a large numbers is a mathematical task considered classically hard to solve and for this reason forms the basis of a class of cryptographic schemes currently widely used. Although quantum computers have not been realized yet, the mere fact that they could be built might threaten the security of some cryptographic schemes.

QKD is the process to securely share cryptographic keys [39] [60] between terminals by exploiting information that is sent over a Quantum Channel: by making use of the laws of Quantum Mechanics, the presence of an eavesdropper can be detected with a small error probability, thereby assuring secrecy of the shared keys.

Discrete-Variable Quantum Key Distribution (DV QKD) and Continuous-Variable Quantum Key Distribution (CV QKD)

Discrete-Variable QKD protocol is the protocol recently applied to UniPd prototype [17] QuAKE (Quantum Advanced Key Exchanger), publicly demonstrated on October 3-4, 2011 at “Palazzo della Ragione” in Padua, over a 50 m distance and with indoor daylight conditions along the south wall of the Great Hall; and now applied to SaNe-QKD prototype for the project "Application of an Optical Quantum Link to GNSS". It is high performance and fit to space environment.

DV QKD infers that in a QKD protocol if two legitimated parties aim at sharing a theoretic secret key, via the Quantum Channel, they exchange single photons agreeing on a set of non-commuting bases for state measurements [74] [15].

Alice encodes a classical bit onto the polarization or the phase of a photon, and send it to Bob, which measures; repeating this process n -times, A. and B. share two n -bit strings, X and Y , which suffers discrepancies mainly due to losses in the channel, noise in Bob's detectors, but conservatively attributed to the action of an eavesdropper.

Therefore any QKD protocol must include a classical post-processing step in order

to extract a secret key from the correlated strings X and Y ; this is done through a noiseless authenticated but insecure classical communication channel and this secret key agreement is itself split in two parts: Reconciliation [60] (in which Alice and Bob correct the errors between their strings) and privacy amplification (in which Alice and Bob apply a random choose compression function to their mutual string, that, if well chosen, is uncorrelated with the random variable accessible to the eavesdropper). The simplest QKD protocol is the so called B92 protocol [8]

The majority of the QKD systems have been realized implementing Discrete Variable or Distributed Phase reference protocols, using the properties of the single photons in order to encode key information. In recent years, Quantum Communication protocols have been extended to the domain of Continuous Variable domain, representing a valid alternative, because of the promised high keyrate and security.

Continuous Variables quantum key distribution (CV-QKD) uses amplitude and phase of the second quantized model of radiation field characterized by infinite dimension of Hilbert space. If we suppose that a mode can be described by the conjugate operators p and q , satisfying the relation . This means that the principle of uncertainty must be satisfied by an arbitrary state of the system:

$$V(q)V(p) \geq 1/4 \quad (4.1)$$

where $V(\bar{x})$ is the variance of the arbitrary quadrature $\bar{x} = \bar{p}$ or $\bar{q}$. Moreover, coherent states satisfy $V(\bar{q}) = V(\bar{p}) \doteq \Delta$, where Δ is the Quantum Shot-Noise (QSN) [74].

A generic quantum state ρ is represented by the Wigner quasi-probability distribution

$W(q,p)$, whose continuous variables are the eigenvalues of the quadratures $x = \bar{p}$ or $\bar{q}$.

In the phase-space representation, states with Gaussian Wigner function are called *Gaussian state*.

For coherent states $|\alpha\rangle$, namely the eigenstates of the annihilation operator $a = (\bar{p} + \bar{q})/\sqrt{2}$, the detection of an arbitrary quadrature $\bar{x}$ provides outcomes x following the marginal distribution:

$$G(x - \bar{x}) = \frac{1}{\sqrt{2\pi}} e^{-\frac{(x-\bar{x})^2}{2\Delta}} \quad (4.2)$$

with $\Delta = 1$ for heterodyne detection and $\Delta = 1/2$ for homodyne detection.

The measurement scheme of CV-protocol is based on homodyne detection with outputs of real amplitudes instead of discrete events (e.g. clicks) as for photon counters [69] [34]: CV QKD protocols are based on p-i-n photodiodes, which are faster (GHz rate compared to MHz rate of single photon detectors) and more efficient (more than 80%). Furthermore, single photon detector rate is definitely limited by the detector dead time.

As light carries continuous information (the value of the quadrature of a coherent state), in the CV QKD protocols the key information is encoded by Alice in two

orthogonal quadratures X and P (amplitude and phase) as told above; according the protocol, the source can be squeezed light [40] or coherent light [34] [42], modulated in the X or P quadratures according to a centered bi-Gaussian distribution.

The receiver uses a homodyne detection setup to randomly measure one of the two quadratures. Other schemes [102], using at the receiver a 50/50 beam-splitter, allow the simultaneous measurement of the X and P quadrature and eliminate the need for Bob to randomly switch between measurement bases. This advantage comes with the fact that the two quadratures received by Bob are noisier than the single quadrature in the homodyne-based protocol.

One basic difference from CV and DV QKD comes from the detection scheme. In photon counters, post-selection is a necessity: if a photon does not arrive, the detector does not click and the event is simply discarded.

On the contrary CV protocol has an opposite feature: it always detects a result but the losses correspond to an increased noise in the signal, while in typical discrete variable protocols losses simply reduce the number of detected signals.

Two methods have been developed to face this situation at the protocol level: post-selection and reverse reconciliation. Post selection is fairly stable and realized using both one-way or two-way EC schemes. It is not performed at the Shannon limit and is not sure its degree of security: in fact its security is supposed only making assumptions about eavesdropper's interception. Reverse reconciliation is realized using a one-way EC scheme, mainly secure against collective attacks, but is sensitive to the efficiency.

[41] Finally for discrete modulation and Gaussian modulation protocols, a combination of post selection and reverse reconciliation looks to provide to obtain reasonable rates in a practical solution.

Discrete Variable protocols have the drawback that the raw key is made up of discrete variables for Alice, while Bob has a string of real numbers. In this framework the excess of signal is essential: the eavesdropper's attack is always simulated as observed loss, the corresponding key rates depend on the classical communication protocols chosen (with or without post-selection data, in reverse or direct reconciliation). And in this sense the best-known protocol involves a combination of post-selection and reverse reconciliation. Moreover in the presence of excess noise, the key rate formula is the object of ongoing research and entanglement verifications have been performed showing excess noise does not wipe out the quantum correlation within the experimental accessible domain.[44]

Continuous-Variable quantum key distribution (QKD) protocol based on coherent states and reverse reconciliation [34] can be realized for high-speed metropolitan-size networking with an average secret key distribution rate of 8 kbit/s over a 3dB

loss optical fiber (the prototype worked for 57 hours).

Transmission and detection of the signal and phase reference have been implemented by time and polarization multiplexing supported by sophisticated error-correction codes for reconciliation.

These protocols provide significantly higher secret key rates with increased bandwidths than previous schemes that only make single quadrature measurements. They also offers the further advantage of simplicity compared to all previous protocols which, to date, have relied on switching.

Then, Alice and Bob extract a secret common binary key from their data, by performing classical procedures for channel characterization, error correction and privacy amplification.

The security of these protocols come from the Heisenberg inequalities satisfied by the Quantum Continuous Variable system accessible to Alice Bob and the eavesdropper Eve. Recent developments of CV QKD systems [34] look to provide stable and automatic distribution of secret keys at high rates over relative long time intervals.

It was first implemented in a proof-of-principle experiment at near-infrared wavelength (780 nm) based on a pulsed shot-noise-limited homodyne detector. Subsequently the system went through successive phases of implementation of advanced error correction algorithms and the operation in IR 1550nm in order to enhance the performances of the system using standard product of telecommunication industry [42] . From a practical point of view the coherent state CV QKD protocol requires simple system architecture and eliminates the need for specific resources such as single photon sources and detectors.

The security against collective attacks rely on an entanglement-based description of the protocol which is formally equivalent to a PM scheme. If Alice is prepared by a bi-gaussian modulation by an EPR state of variance V . It has been recently theorized that CV protocols can be use in order to perform in a direct way secure communications, that is to say, without sharing any secret key. [69]. This procedure of directly communicating message bits is called Message Mode (MM).

4.4 Quantum Key Distribution for SaNe-QKD

[74] Quantum Key Distribution (QKD) is the process to securely share cryptographic keys (a random number key encoded in polarized states) between terminals by exploiting information that is sent over a Quantum Channel: Quantum Mechanics principles assures that an eventual eavesdropper attack to the communication will change instantaneously the transmitted signal states, so the presence of an eavesdropper can be detected with a small error probability, thereby assuring secrecy of the shared keys.

Security in QKD is related to the fundamental principles of Quantum Physics, as

any action by which a potential eavesdropper extracts information out of quantum states is a generalized form of measurements which modifies the state of the measured system.

Furthermore any action by the eavesdropper in order to obtain a perfect copy of the state -that Alice sends to Bob- is forbidden by the no-cloning theorem [103] .

One cannot duplicate an unknown quantum state while keeping the original intact.

Applying the QKD protocol to the space scenario of GNSS constellation, the two parties need to be connected by two channels (requirement for QKD). If Alice and Bob are the sender and the receiver parties, respectively, the two channels needed are:

- A **classical channel** on which they can send classical messages back and forth. A third person can listen to the conversation but cannot participate in it. The classical channel needs therefore to be authenticated (Alice and Bob need to identify themselves). The classical channel in SaNe-QKD OPT system is performed by the Thales Alenia Space OTP system working at a 1500nm wavelength.
- The **quantum channel** allows them to share quantum signals. The task of Alice and Bob is to guarantee the security against an eavesdropper tapping into the quantum channel and listening to the exchanges on the classical channel. In the whole SaNe-QKD OPT system, the quantum channel is performed by SaNe-QKD by UniPd.

Authorization is a request for QKD. If Alice and Bob (in QKD protocol) are the two authorized users, those who establish a secret key (a common list of secret bits known only to themselves) at a distance in the QKD communication protocol: a non-secret key is never used. After the transmission of a sequence of symbols, Alice and Bob must estimate how much information about their lists of bits has leaked out to a possible eavesdropper. Such an estimate is obviously impossible in classical communication as the communication is unmodified and leakage of information is quantitatively related to degradation of the communication.

Quantum Physics based intra-satellite links are within reach of current technology. In the last years, experimental and practical implementations of Quantum Key Distribution systems have been deployed (on Earth), over optical fiber links (the DARPA network in Boston and the SECOQC network in Wien) [67] [29] [28]

QKD networks are arguably the best known, and even commercial solutions are nowadays available. The advantages of such solutions lie in increased flexibility and lower costs for deploying the actual physical link: in this sense free-space QKD seems a possible solution to provide perfectly secure satellite-to-satellite and ground-to-satellite communication channels.

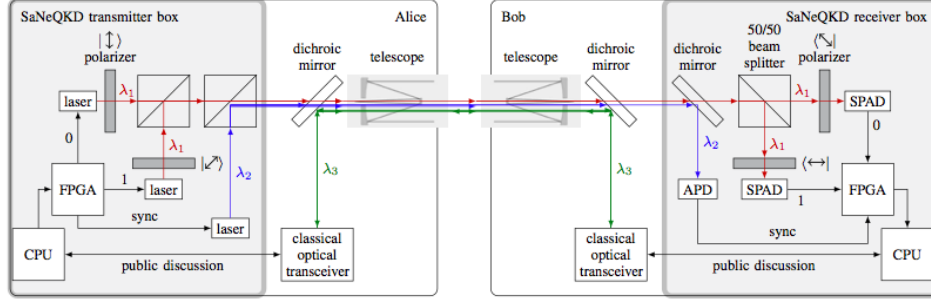


Figure 4.3: The figure shows the block diagram for the B92 SaNeQKD transmitter (left) and receiver (right).

Bit	Transmitter	Receiver
0	$ \uparrow\rangle$	$ \nearrow\rangle$
1	$ \searrow\rangle$	$ \leftrightarrow\rangle$

In recent years UniPd distinguished for the realization of a QKD architecture over a free space quantum channel [?] [100] . Furthermore, UniPd still supported developing challenging investigations about the effect of the atmospheric turbulence [?] (Chapter 2) in long distance optical and near optical infrared links in order to study the degradation of the beam properties and the methods for guiding and stabilizing the aiming, relevant point in case of single photon beams involved in Ground-Ground or Space-Ground Quantum Optical Links. This studies are crucial for space-to ground (or ground-to-ground) links as atmospheric effects can influence on the beam propagation, causing fluctuations in both the intensity and the phase of the received light signal, thus impairing link performance.

Protocol and transceiver

The corresponding receiver, employing a dichroic mirror, two polarizers and two single photon avalanche detectors (SPADs) for the information bits, and an avalanche photo-detector (APD) for the synchronization pulse is shown in 4.3 on the right. It should be noted that it is possible (although not trivial) to compensate for the satellite motion and keep the reference polarization axis on both terminals aligned [?] , even among satellites in distinct orbital planes.

Both the transmitter and receiver can be integrated with a classical optical transceiver system, employing a different wavelength, in general.

The same classical optical system can then be used for the public discussion channel in QKD.

SaNe-QKD stands for Satellite Network Quantum Key Distribution, and it is the UniPd QKD working system based on B92 (Bennet - Brassard) protocol. It consists of a transmitter (called Alice) and a receiver (called Bob) that are connected through a free-space quantum channel both driven by a field-programmable gate array (FPGA) driving the **transmitting mechanical system** in order to handle communications between PCs and laser devices or SPAD (Single Photon avalanche Diode) and APD.

Alice uses three laser diodes 2 attenuated lasers 850 nm for the key generation of optical power 3.5 mW and 1 laser for the synchronization (808 nm) of optical power 5m.

Only for the POCD tests, the synchrony laser will be repositioned outside the SaNe-QKD block, owing to the presence of a filter along the OTP BB optical path, preventing the use of the 808 wavelength. This momentaneous problem could be solved in future arrangements for SaNe-QKD, by substituting the native filter at the OTPBB interface, by an other one with a bandwidth larger (in order to permit the propagation of 808nm radiation).

The signal going out from the SaNe-QKD system, across part of the relay optic system of the OTPBB Optical counterpart for propagating outside through the 20cm-newtonian telescope.¹

Given the strong limitations on the satellite payload, we choose a QKD protocol that employs as few quantum states (and hence distinct sources) as possible. BB84 protocol employs four distinct, pairwise orthogonal, states, while the minimum is achieved by the B92 protocol that only employs two distinct, non-orthogonal states at the price of a further loss in the efficiency $\eta = \frac{1}{4}$.

Therefore we consider using B92, with polarization states and the encoding map: $0 \rightarrow |\uparrow\rangle, 1 \rightarrow |\nearrow\rangle$ and propose the transmitter scheme that is shown in 4.3, employing just two laser sources and two polarizers for the informative states and one laser for the synchronization pulse.

In fact while BB84 protocol need four linearly polarized laser diodes for each bread-board, each one emitting a specific states (horizontal, vertical, $+45^\circ$, -45°), B92 protocol (preferred) uses only two linearly polarized laser diodes, each one emitting a specific state (horizontal, $+45^\circ$); Why only two sources of coherent pulses in B92? The idea of B92 come from Bennett, who noticed (in 1992) [8] that the 4 states of BB84 were more than necessary for a Quantum Communication system: one could

¹The SaNe-QKD system is the Quantum counterpart - built by UniPd- of a more complex Optical Quantum Communication Network (OQCN).

Let remind to the reader that the classical part of the OQCN, the Optical Communication system called OTPBB, is built by Thales Alenia Space and it is connected to SaNe-QKD by an interface. The propagation wavelengths of OTPBB are 1530nm and 1560nm. In both transmitter and receiver the optical path of SaNe-QKD transmitter or receiver across part of the OTPBB relay optics, entering into the 20cm newtonian telescope and propagating outside. Symmetrically, for the receiving system.

use only two non-orthogonal states: Alice sends only two nonorthogonal states associated with the two values of the logical bit to-be-secretly-transmitted.

With the polarization encoding the source is composed by two linearly polarized laser diodes, each one emitting a specific state (e.g. horizontal, $+45^\circ$). The polarized laser pulses are attenuated to a single photon level by an attenuator. “Hence two states system are necessary, and if they are incompatible (not mutually orthogonal), then two states are also sufficient”. [8]. And in order to prevent from attacks by eavesdroppers, Alice and Bob would only need to monitor the attenuation of the quantum channel.

SaNe-QKD realize a QKD based on B92 protocol.

The system consists of a transmitter (Alice) connected to a 20cm Newtonian telescope. A receiver part (Bob) is connected to a further telescope.

A quantum channel is then established between Alice and Bob.

The transmitter (Alice) uses two infrared (850nm) attenuated diode lasers to send the bits 0 and 1, encoded in the vertical polarization and $+45^\circ$ linear polarization of the photons, respectively.

As recalled after in the section Design, a 808 nm laser beam is also used for synchronization issues. A raw key of 288 kbit is divided into 50 packets of 5760 bits each, which are in turn divided into 12 frames for the ease of synchronization. Each frame consists of 11 header slots and 240 payload slots, each with a duration of 800 ns. The header exhibits the pattern ‘100000xxxx1’, where ‘xxxx’ is the 4-bit frame number, encoded one bit per slot in a pulse-duration modulation of the synchronization beam (a 400 ns or 200 ns pulse encode the bit 1 or 0, respectively).

Concerning the payload slots, the first 200 ns are used to send the synchronization beam, then, after the synchronization laser, Alice waits 200 ns and then sends two bits separated by 200 ns 4.15.

Photons with $+45^\circ$ linear or vertical polarization correspond to 1 or 0 bit respectively.

The receiver (Bob) uses a dichroic mirror (DM) to separate the information qubits from the synchronization signal: the latter is reflected and detected by an avalanche photodiode, whereas the qubits, transmitted by the DM, impinge on a 50/50 beam-splitter (BS). On either output of the beam-splitter (BS), a polarizer and a single photon avalanche photodiode (SPAD) detect the 45° linear polarization or horizontal polarization photons.

Each click of either SPAD corresponds to the reception of a sifted 0 or 1, respectively.

Both transmitter and receiver are driven by a FPGA (field programmable array). The raw key obtained by photon exchange by the transmitter and the receiver is processed in four subsequent steps:

- sifting

- channel estimation
- key reconciliation
- privacy amplification

Finally a public discussion is implemented with the user diagram protocol (UDP) running over a public protocol (during the tests this public channel is IPN (Internet Protocol Network) and 802.11g underlines the physical layer transmission).

Sifting and Channel estimation step: in each round of the key-agreement protocol, Bob sends the positions of the received qubits over the public channel (the received qubits represent the sifted key) and discloses the value of a fraction of them, in order to allow to the transmitter to estimate the channel losses and the QBER.

The objective of the channel estimation is twofold: it predicts losses and the error rate introduced by the noisy quantum channel in order to properly perform the key reconciliation stage. Moreover, it is used to reveal the presence of eavesdropper, that is, to determinate the probability q that a photon has been observed by the eavesdropper, according to the Photon Number Splitting attack scheme.

A fairly low miss detection probability is assured where the miss detection event represents the case in which the eavesdropper is observing more photons than predicted by the channel estimation protocol.

Key reconciliation: errors introduced on the sifted key by the quantum channel (polarization degradation due to the atmosphere, noise in the devices are corrected by implementing the Winnow scheme: the probability of a reconciliation failure is kept below a fixed value P_{fail} , by guaranteeing a residual BER on the reconciled key smaller than P_{fail}/N_{rec} , where

$$N_{rec} = N_{sift} \sim N_{qber} \quad (4.3)$$

is the number of sifted.

Given these constraints, the number of iterations of the protocol and the block sizes for parity checking are chosen to minimize the number of bits N_{rev} revealed over the public channel **Privacy amplification:** The reconciled keys at Alice and Bob are compressed following a two steps procedure aiming at reducing the information leakage to a malicious party to the target value $I_{tar} = 1$ bit per key. First, N_{rev} out of the $N_{rec} = N_{sift} \sim N_{qber}$ bits of the reconciled key are deleted according to the procedure of bit deletion, in order to eliminate the information revealed over the public channel to perform key reconciliation. In this way, the information leaked to the eavesdropper during the key reconciliation stage is reduced exactly to zero. After bit deletion, privacy amplification is obtained by hashing with a full column rank, random, binary Toeplitz matrix, renewed at each round. The number of rows in the Toeplitz matrix is a design parameter for this phase of the key processing, depending on the amount of information on the key that Eve is estimated to have

gathered during the previous stages of the protocol.

There are two different methods for estimating the information gathered by Eve with IS attacks.

One method is linked to the number of errors revealed after key reconciliation with the information gained by the eavesdropper (Bennett). A second method defines an upper bound on Eve's Renyi entropy in the limit of long transmissions, that is when $N_{sift} \rightarrow \infty$. In QKD distillation protocols the public discussion channel is assumed to offer both high rates and high reliability.

In the intersatellite network this is a long distance free-space optical link yet to be designed.

In this part, by exploiting the results in the network communications, we describe objectives (drivers and goals) and conceptual design of the OQL Proof-of-Concept Demonstrator that will be developed by Thales Alenia Space and UniPd for GNSS secure networking.

We will highlight conceptual design, block diagrams, functional description and feasibility of the demonstrator.

The system represents a "Combined system" merging classical and quantum setup and will be used as a toolbox to study classical and quantum communications for links with varying parameters (distance, losses, background etc).

In the following sections we report the transmitter and receiver arrangements of SaNe-QKD for space.

The Quantum Communication system needs to be interfaced to the Classical Communication system (OPT developed by thales Alenia Space), with the added value that the two parts (classical and quantum) could work at the same time.

In order to interface the two systems, an optical-mechanical system has been devised. Challenges in low power and low weight have been considered in order to adapt the Quantum system for space.

4.5 Transmitter

The challenging points of this project are:

- to adapt the existing prototype of Quake (developed by UniPd) into the Quantum part of the Optical Quantum Communication system (SaNe-QKD) on board of ESA satellites.
- to interface SaNe-QKD transmitter and receiver with the optic-mechanical counterparts of OPT, the Optical Communication system by Thales Alenia Space.

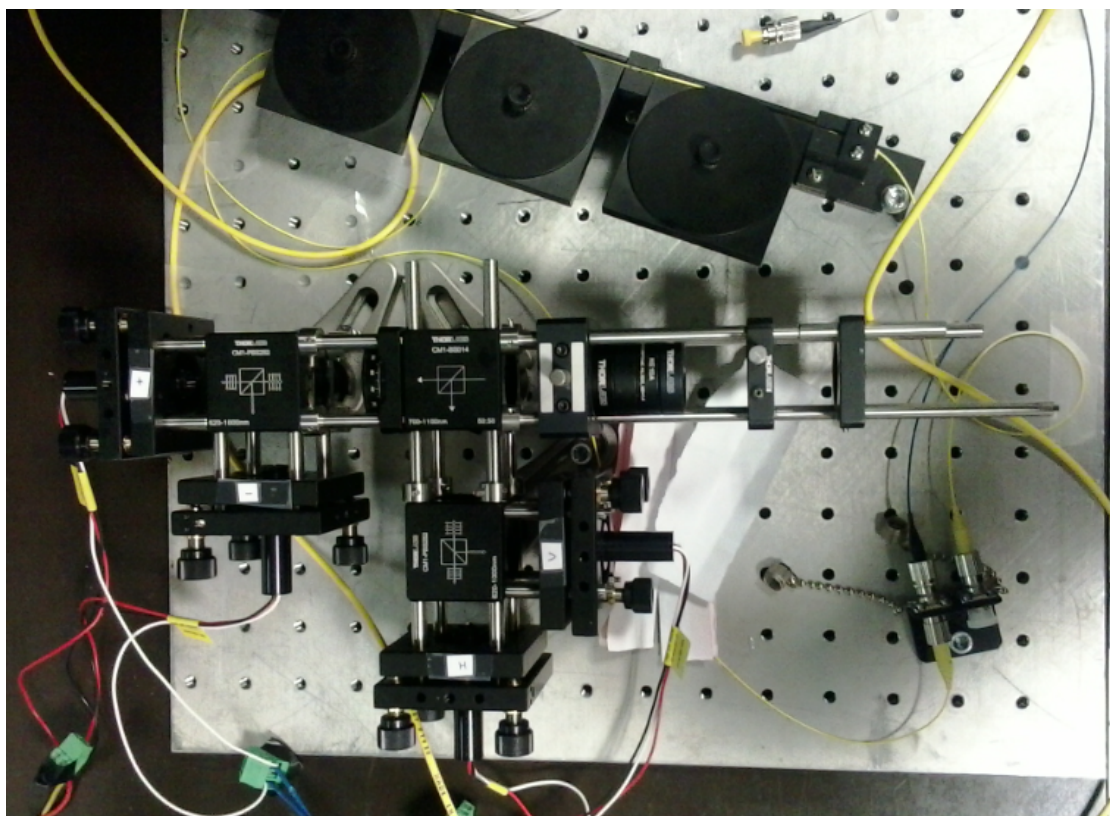


Figure 4.4: The image shows the laser source for B92 protocol. The polarization of the beam can still be optimized manually.

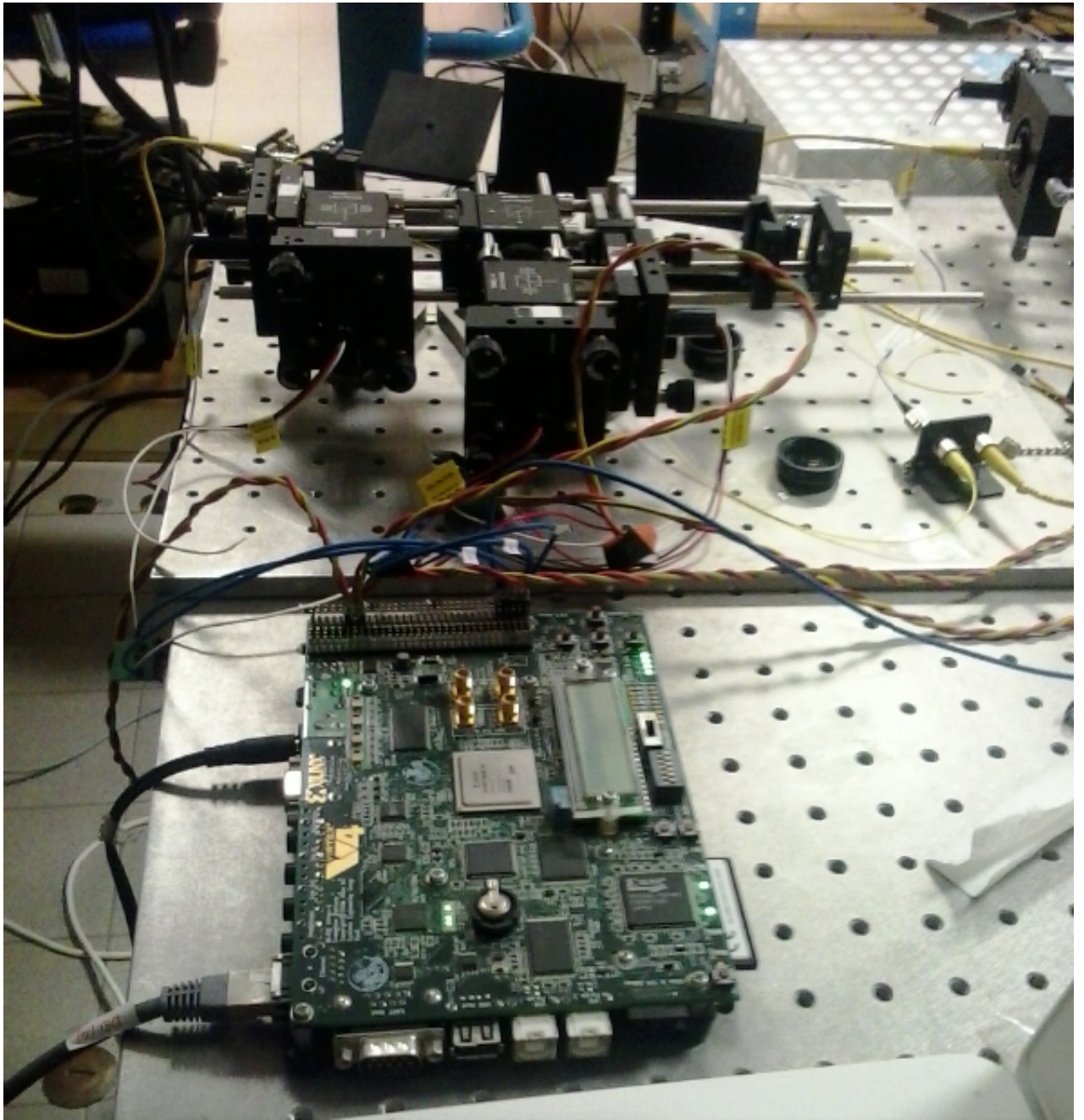


Figure 4.5: The figure shows the working board FPGA connected to the source breadboard. FPGA is driven the transmission of data during some tests in Thales Alenia Space, Turin in October 2013.

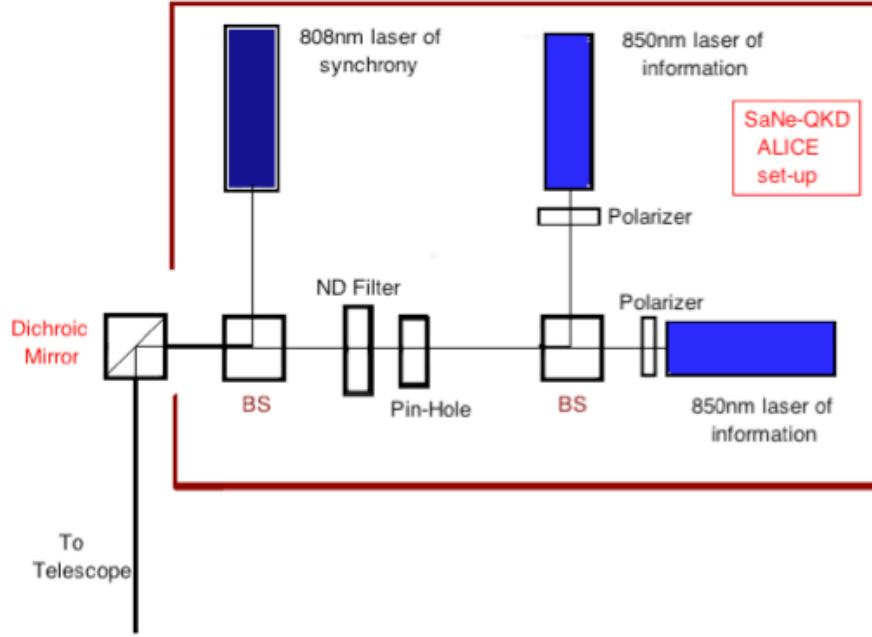


Figure 4.6: Primitive scheme about the transmitter part of SaNe-QKD.

For the transformation of Quake into the new module SaNe-QKD, optical and mechanical elements have totally changed, as the necessity of weightlessness and compactness prevent any use of heavy breadboards: we have been obliged to choose an "aerial arrangement" to position suspended above OPT system (see figure 4.9). A primitive plan 4.6 has been left because the wavelength path of 808nm was blocked by a filter into the OPT system. For the space the idea remains that presented in figure 4.6, but for performing the tests for the proof of Concept Demonstration, we will position the synchrony path of 808nm outside the SaNe-QKD box.

An important issue has been the fusion of saNe-QKD with the OPT module. As told above, an "aerial arrangement" was developed, with specifics interfaces, to position above the module of OPT, and using the same optical path of OPT. This fact has obliged us to position in a breadboard apart the SaNe-QKD source for performing the POCD tests.

Besides, OPT systems needs of two control camera at 850nm that have been integrated into SaNe-QKD receiver and SaNe-QKD transmitter.

SaNe-QKD transmitter system uses weak laser pulses received at the receiving box by single photon detectors (SPADs).

The source system observed in figure 4.6 consists in

- Four 850nm Laser of information World Star Tech (we uses only two of them

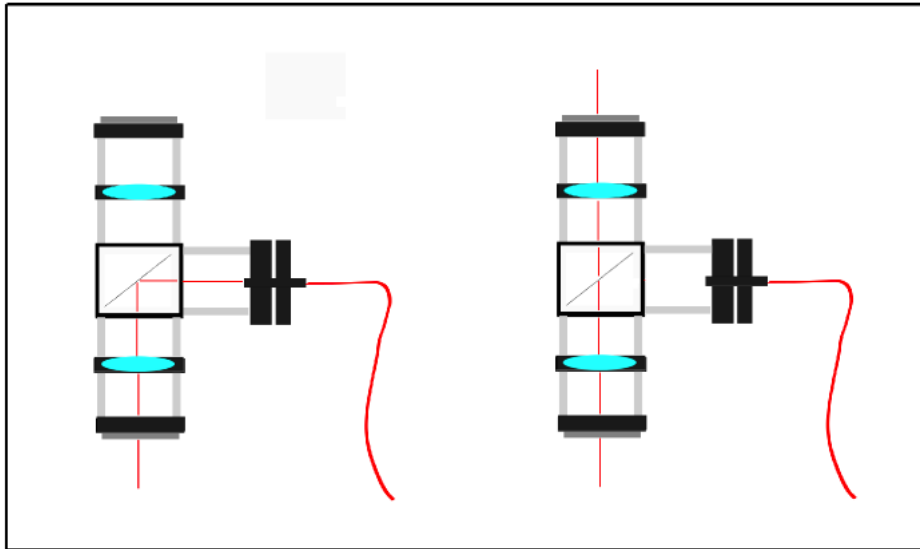


Figure 4.7: The figures shows twofold aspects of SaNe-QKD interface. It works at sender for QKD and it works as beacon camera receiver for alignment issues of SaNe-QKD OPT system. A focusing lens is positioned above the beam splitter (BST 70/30) in order to allow beacon camera use

according B92 QKD protocol)

- 808nm Laser of synchrony World Star Tech positioned outside the saNe-QKD box
- 2 Polarizing Beam Splitters and 1 Beam Splitter
- ND Filter
- Manual Polarization optimizer
- FPGA board
- Breadboard
- Dedicated cages and post, post-holder and forks
- C-mount adapter at the interface
- Collimating lens ($f=8\text{mm}$) at the interface
- A beam splitter (BST 70/30)
- A tip-tilt/XY cage
- Fiber adapter connector CFC-X-11

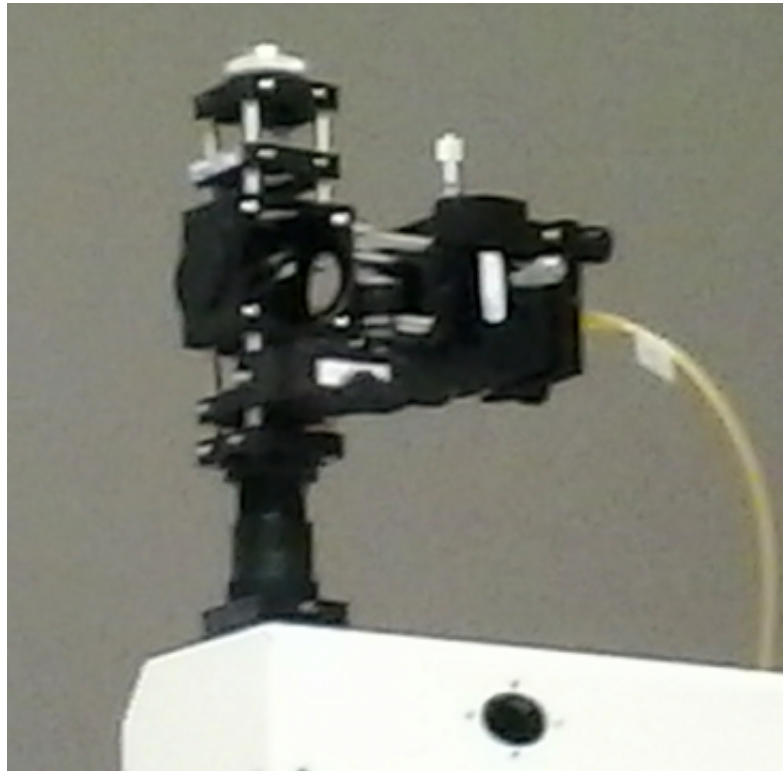


Figure 4.8: The figure shows the image of the SaNe-QKD "aerial module" positioned above OPT module. The signal coming from the source enters the interface, the telescope and is then transmitted outside. The fused module SaNe-QKD OPT is projected to be positioned on board of Galileo satellites.

- lens for Camera focusing

According B92 protocol the figure 4.6 the signal single state is generated at the source, sent along an optical fiber (MM) to the saNe-QKD inetrface, enters the telescope (leaves the first Galileo setellites) and is transmitted to a second telescope (positioned on a different Galileo satellite), follows the optical path to the SaNe-QKD interface (figure [?]), enters the polarizer, and is sent by the fiber to the SPAD for the single photon detection.

All the process is driven by the FPGA board at the transmitter point and at the receiver point.

The interface of SaNe-QKD has twofold as they works as QKD transmitter (or receiver), but they both work as beacon camera receiver for alignment issues of the whole SaNe-QKD OPT system. this is allowed by the beam splitter 70/30 of the interface and by a focusing lens above it.

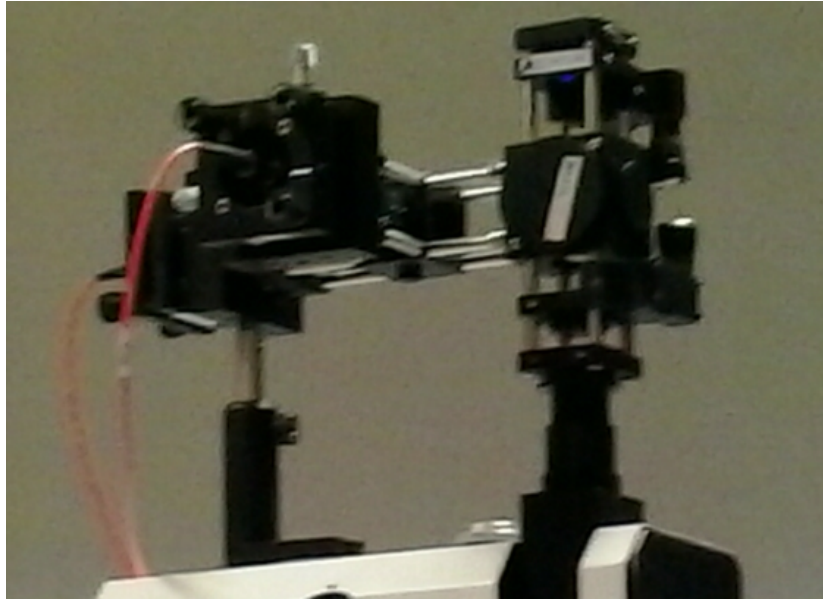


Figure 4.9: SaNe-QKD mounted above Thales Alenia Space system. The original path have been modified and above the system it has been obtained a position for the beacon camera of OPT.

4.6 Receiver

The receiving part of SaNe-QKD is often called "Bob".

Bob arrangement is shown (in the figure 4.12) and a list of the optical and electrical elements is reported here below:

- APD Avalanche Photon Diode
- one Polarizing Beam Splitters, 2 Thorlabs collectors CFC X11 B and a Beam Splitter (BSS 11 70/30 Thorlabs)
- 2 Polarizers Thorlabs
- two SPADs (Single Photon Avalanche Diode)
- one FPGA board
- Dedicated cages, 2 tip-tilt/XY cage and post, post-holder.
- C-mount adapter at the interface
- Collimating lens ($f=8\text{mm}$) at the interface
- A tip-tilt/XY cage

- Fiber adapter connector CFC-X-11
- lens for Camera focusing

SaNe-QKD the used sources are 850nm lasers for single photon generation and 808nm lasers for synchrony issues. In Alice block we use semiconductor lasers by World Star Tech, with nominal outgoing power of 3.5 mW (measured 3.45 mW), adjustable and focusing (by a lens into the dedicated cage). For the POCD the 808nm is substituted by a 850nm laser which will be positioned outside the system, as a filter in OPT prevent 808nm propagation.

Briefly, SaNe-QKD overall system works driven by FPGA (Field Programmable Gate Array) technology for building the SaNe-QKD electronic architecture.

A **FPGA** is an integrated circuit, which can be configured by a costumer or a designer after manufacturing – hence field-programmable. The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application specified integrated circuit (ASIC). The ability to update the functionality after shopping, partial re-configuration of a portion of the design and the low non-recurring engineering costs relative to an ASIC design (notwithstanding the generally higher unit costs), offer advantages for many applications. FPGA was chosen for SaNe-QKD for its characteristics of its flexible programmable chip and behaviour simulations.

A FPGA contains programmable logic components (logic blocks) and a hierarchy of reconfigurable interconnects that allow the blocks to be “wired together”. Logic blocks can be configured to perform complex combination functions, or merely simple logic gates.

In most FPGAs the logic blocks also include memory elements, which may be simple flip-flops or more complete blocks of memory. For SaNe-QKD we chose XILINX FPGA as bearing useful components for data acquisition, storage and elaboration and the requested hardware to be interfaced with a further board or a PC.

The APD (**Avalanche Photon Diode**) is a highly sensitive semiconductor electronic device that exploits the photoelectric effect to convert light to electricity. It is a high sensitivity photodiode that operates at high speed and high gain by applying a reverse bias. It delivers a higher S/N than PIN photodiodes and is widely used in optics. APDs photo detector provides a first stage of gain through Avalanche Multiplication. From a functional standpoint, they can be regarded as the semiconductor analogue to photomultipliers. By applying a high reverse bias voltage, APDs show an internal current gain effect (around 100) due to impact ionization (Avalanche Effect).

A SPAD (**Single Photon Avalanche Diode**) is a solid-state photo-detector based on a reverse biased p-n junction in which a photo-generated carrier can trigger an

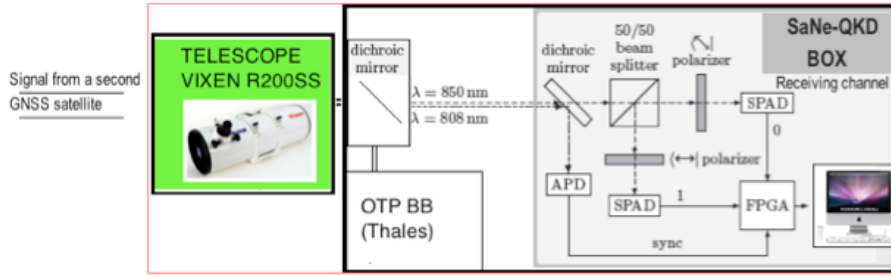


Figure 4.10: This figure reports the scheme of SaNe-QKD receiver. This is the primitive idea before we observed that a filter along OPT path cuts prevent 808nm to enter into SaNe-QKD. We are obliged to position APD and 808nm synchrony-path outside the module of SaNe-QKD for the test of the Proof of Concept Demonstration.

avalanche current due to the impact ionization mechanism. A SPAD can detect low intensity signals (down to the single photon) and can signal the arrival times of the photons with a jitter of a few tens of picoseconds. SPADs, as APDs, exploit the photon-triggered avalanche current of a reverse biased p-n junction to detect an incident radiation.

The fundamental difference between SPAD and APD is that SPADs are specifically designed to operate with a reverse bias voltage well above the breakdown voltage (on the contrary APDs operate at a bias lesser than the breakdown voltage). This kind of operation is also called Geiger mode.

FPGA, APD and SPAD, Polarized Beam Splitters and optical elements, used for SaNe-QKD, are described in [5].

We need to point out that the synchronization part of 808nm is at that moment positioned outside the SaNe-QKD box with the APD, as a filter in the OPT box prevent the 808nm propagation into the whole system.

808nm will be integrated in the system after the Proof of Concept Demonstration, by substituting the filter in OPT, so the system will return as in figure 4.12. (The APD is part of the synchronization issue) The basic system of SaNe-QKD has been modified too, in order to permit the positioning of the Beacon camera of SaNe-QKD at the top of it. A scheme with the interface is shown in figure 4.11 A receiving interface have been developed in order to permit to the optical path to enter correctly into the SaNe-QKD system. The current arrangement above OTP box is reported in figure 4.11 4.9

Network topology

It is necessary an efficient and secure connections among all satellites and we need to reach that the QKD network has a high degree of connectivity.

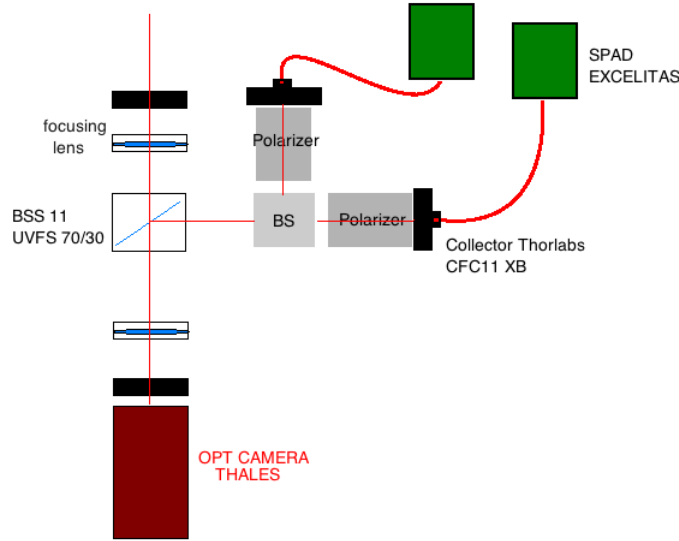


Figure 4.11: This figure reports the scheme of SaNe-QKD receiver. The beam enters the optical element BSS 11 and it is split in two. One part going to the Beacon camera of OPT, the second part of the beam going to the SaNe-QKD system, through the Beam Splitter, the Polarizers to the fibers.

However the mass and volume limitations on satellite payloads prevent equipping each node with several distinct transceivers. Therefore, a tradeoff must be sought between loading each satellite with the fewest possible transceivers and yet allowing sufficient connection redundancy for reliable, safe and secure QKD in the network. A possible solution in this respect is to exploit the relative motion between satellites in different planes, explained in the subsection *Galileo constellation architecture*. By alternately pointing transmitting and/or receiving telescopes towards the closer satellites, each terminal can share a sufficient amount of secret key bits with more than one node per transceiver in each revolution period. Following the above approach, we have considered two distinct feasible solutions.

- A minimal burden solution requires one quantum transmitter, one quantum receiver, one classical transceiver for the public channel and on telescope that can be pointed dynamically. By following a proper link switching sequence, 4.13 for satellite 1 of plane A, each node is connected with 4 other nodes as shown in 4.14 .

Such symmetry and redundancy in the network connectivity provides four completely disjoint paths to connect any pair of nodes. Thereby, it allows to cope with up to three (known) disrupted nodes. Also, through a properly devised threshold secret sharing scheme, it allows to exchange perfectly secret keys between two non adjacent nodes even if one (unknown) intermediate node is

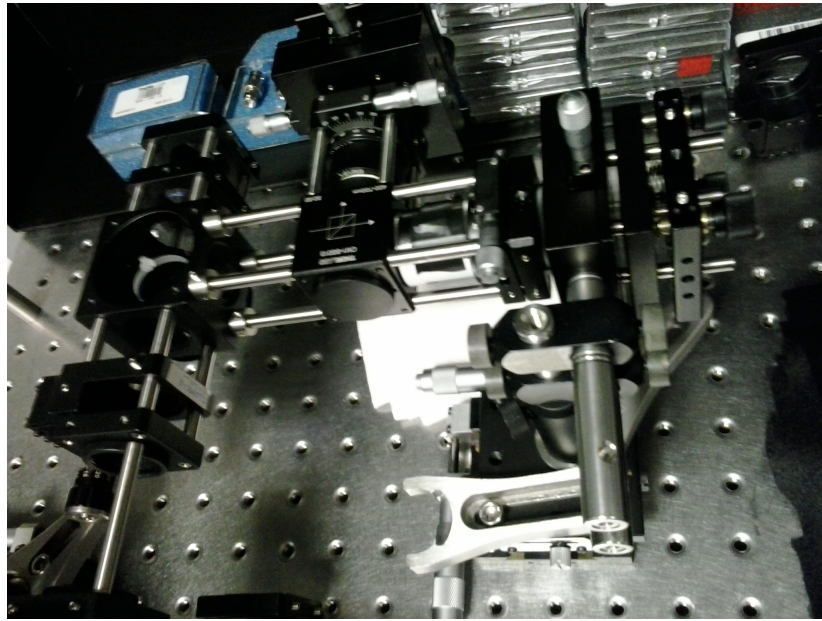


Figure 4.12: This figure reports part of the SaNe-QKD receiver on the test bed mounted with the receiver interface. The polarizers and the beamsplitter are well observable at the center.

hijacked and controlled by the adversary.

- Another, more complex solution, requires one quantum transmitter, one quantum receiver, two classical transceivers and two telescopes that can be independently pointed in different directions; and provides degree six for each node, and higher secret key length.

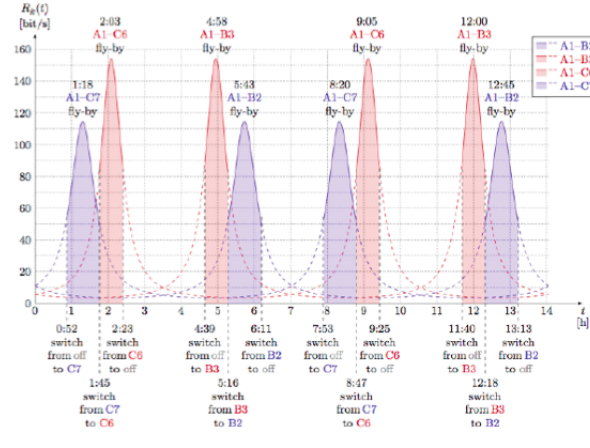


Figure 4.13: The figure shows the link switching sequence for satellite A1 that obtains the maximum balanced rate when only one telescope is available on each satellite. The shaded areas represent the total secret key length achievable in one period.

4.6.1 Expected parameters and key lengths for SaNe-QKD

In the design of the SaNeQKD system, the expected final secret key rate has to be derived by taking into account several parameters, that is:

- R_0 , the raw key rate;
- μ , the average number of photons per qubit at the transmitter output;
- η , the QKD protocol efficiency (e.g., $\eta = 0.25$ for B92, $\eta = 0.5$ for BB84);
- A_{link} , the free space link attenuation;
- A_{rc} the attenuation due to devices at the receiver side (Bob);
- ϵ , the quantum bit error rate (QBER).

Given these parameters, one could derive the sifted key rate as

$$R_{sift} = R_0 \eta A_{link} A_{rc} (1 - \exp(-\mu)) \quad (4.4)$$

That said, in order to compute the final secret key rate, some further processing of the sifted key is required, namely:

- channel estimation (for both QBER and link attenuation)
- information reconciliation
- privacy amplification

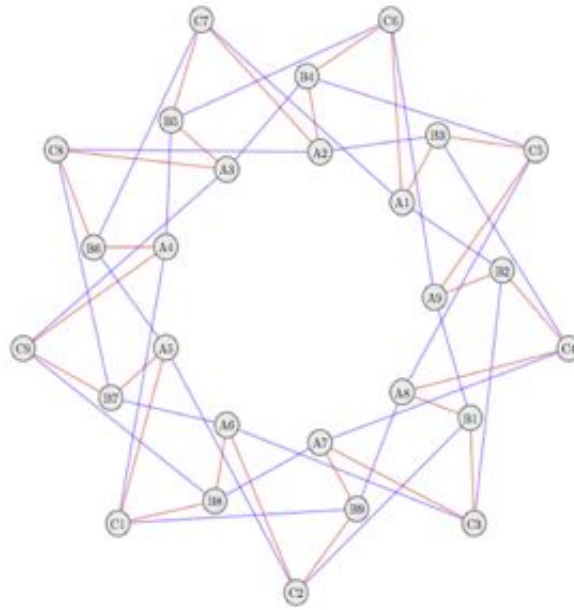


Figure 4.14: The figure shows the connectivity graph of the proposed QKD network scheme over the GNSS Galileo constellation, employing only one telescope per satellite. Red edges represent links that have a minimum distance of 6623 km, blue edges represent links that have a minimum distance of 7687 km.

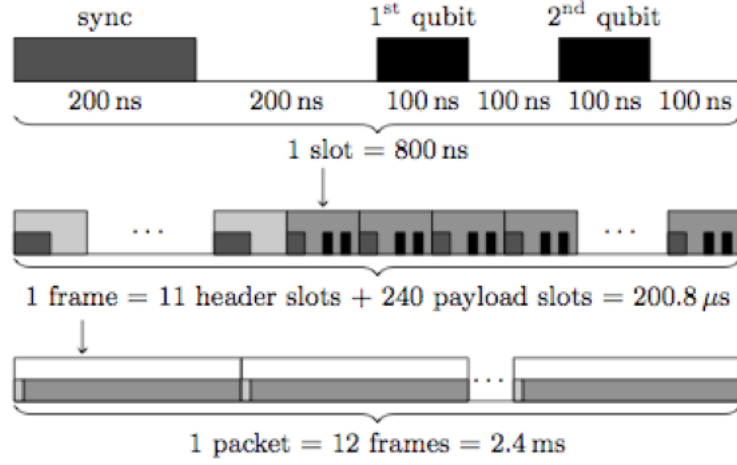


Figure 4.15: Data frame structure. Quantum clock synchronization has been solved by a synchrony laser. Payload slots are used to send the synchronization beam between transmitter and receiver

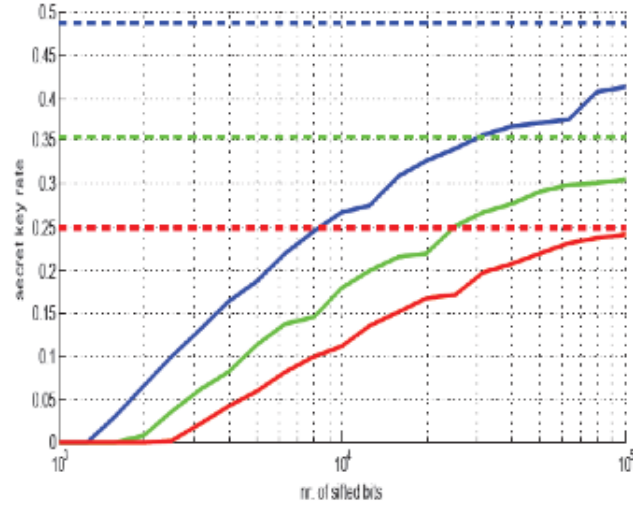
In the hypothesis of sifted keys of infinite length, it can be proven that the optimal upper-bound on the secret key rate is

$$R_{sec} = R_{sift}(1 - 2h_2(\epsilon)) \frac{\mu \exp(\mu)}{(1 - \exp(-\mu))} \quad (4.5)$$

where

$$h_2(\epsilon) = -\epsilon \log_2 \epsilon - (1 - \epsilon) \log_2 (1 - \epsilon) \quad (4.6)$$

the Shannon binary entropy function.



$$\text{QBER} = 1\%, 3\%, 5\%$$

Figure 4.16: The figure shows the secret key rate vs the number of sifted bits, for different values of the QBER. Again, dashed lines represent the optimal asymptotic bound, whereas solid lines represent the achieved rates given the finite-key analysis model described above. Here we see that there is a minimum number of sifted bits that needs to be exchanged in order to obtain a secret key and that this threshold is lower for lower QBERs. Furthermore, the asymptotic bound is approached faster, as the number of available sifted bits grows, with higher QBERs, although lower QBERs allow to obtain some secret key (non-zero secret key rate) with a lower number of sifted bits.

4.6.2 Design

The optical arrangement of SaNe-QKD uses three infrared (850 nm) attenuated diode lasers, controlled by a FPGA and it is implemented from the quantum prototype Quake of UniPd [17] [4].

The transmitted data structure is shown in figure 4.15.

For Quake, a raw key of 288 kbit is divided into 50 packets of 5760 bits each, which are in turn divided into 12 frames for the ease of synchronization.

Each frame consists of *11 header slots + 240 payload slots*; the slot duration is of 800 ns.

The *header* bears the frame number, encoded one bit per slot in a pulse-duration modulation of the synchronization beam (a 400 ns or 200 ns pulse encode the bit 1 or 0, respectively). As regards the *payload slots*, the first 200 ns are used to send the synchronization beam, then, after the synchronization laser, Alice waits 200 ns and then sends two bits separated by 200 ns.

The resulting *raw key rate* is therefore upper bounded as $R_0 \leq 2.39 \text{ Mbit/s}$.

The *measured sifted key rate* R_{sift} allows to estimate the total loss along the source-channel-detector chain $\alpha = R_{sift}/R_0$, including also the fraction of pulses that carry no photons, due to the Poissonian statistics of the faint source, and the B92 protocol efficiency $\eta = 0.25$.

With this arrangement it is allow to achieve a raw key rate $R_0 = 72 \text{ kbit/s}$ and a sifted key rate $R_{sift} = 4.6 \text{ kbit/s}$, although the FPGA would allow a nominal raw key rate $R_{raw,nom} = 2.4 \text{ Mbit/s}$ and a sifted key rate $R_{sift,nom} = 22.8 \text{ kbit/s}$.

With respect to Quake characteristics, some differences should be taken into account while designing SaNe-QKD for the Proof of Concept Demonstration experiment.

- The **link attenuation** is negligible in Quake experiments of Quantum Key Distribution along short distance [17], ($A_{link}, Q \sim 0$), but it is severe for the SaNeQKD one, being $A_{link}, S \in [40\text{dB}, 45\text{dB}]$. 4.18.

Hence, in this latter case, we need more raw key bits in order to get the same number of sifted bits over the time interval available for communication.

We need to choose the privacy amplification parameters according to the link attenuation, with higher attenuations yielding an increased amount of compression and a shorter length of the output secret key.

- The **wavelength used** by the SaNeQKD prototype is 850nm, whereas the one to be used in space by SaNeQKD is supposed to be 350 nm. Fortunately, this difference with 850nm has a negligible impact on the path loss, as the proof-of-concept experiment will be deployed on short distances (500 m) and the choice of filters and optical devices can be easily tailored depending on the chosen wavelength.

In order to mimic the link attenuation of the SaNeQKD scenario with our proof-of-concept experiment, we plan to use optical filters to reproduce both the higher attenuation and its variability. In particular, we consider **four test scenarios**:

- time down-scaling rate
- down-scaling
- attenuation matching
- power down-scaling

The target of each set-up is that of allowing the extraction of a secret key of a given length L_{key} , which translates into a constraint on the required sifted key length L_{sift} .

In order to get such sifted key lengths, we could use the maximum available raw key rate and derive the required amount of time (time down-scaling approach) or, vice-versa, set the available time interval and derive the corresponding raw key rate (rate down-scaling approach), or keep both time and raw key rate fixed and either introduce an additional (artificial) loss at the receiver side (attenuation matching approach) or reduce the average number of photons per bit (power down-scaling approach). While performing this analysis, we should also consider the constraint on the raw key rate achieved by our experimental setup, i.e., $R_0 = 72$ kbit/s. Also, the following parameters are given (when not differently specified):

- $\eta = 0.25$
- $\mu = 1$
- $A_{rc} = -12dB$

The communication on the public discussion channel between Alice and Bob will be implemented with the classical wireless optical transmissions.

Time down-scaling

Let us choose $R_{raw} = R_0 = 72$ kbit/s. This yields, in the POCD scenario, a sifted key rate

$$R_{sift} = R_{raw}\eta A_{rc}(1exp(\mu)) = 720bit/s, \quad (4.7)$$

given $A_{rc} = 12$ dB and $\mu = 1$. We can then derive the *time needed to distill a key* as

$$T_{key} = L_{sift}/R_{sift} \quad (4.8)$$

Example: As shown in figure in order to get $L_{key} = 10^2, 10^3, 10^4$, given $\epsilon = 1\%$, we need $L_{sift} = 10^3, 10^4, 310^4$, respectively, and we can derive the required T_{key} , as shown in the following table.

L_{key} [bit]	L_{sift} [bit]	T_{key} [s]
10^2	10^3	1.38
10^3	$5 \cdot 10^4$	6.94
10^4	$3 \cdot 10^4$	41.67

Rate down-scaling

Let us now fix the available time interval $T_{key} = 2400$ s. Given the required secret key length, this turns into a requirement on the sifted key rate and, consequently, on the raw key rate. More precisely,

$$R_{sift} = L_{sift}/T_{key} \implies R_{raw} = R_{sift}/(\eta A_{rc}(1 - \exp(-\mu))) \quad (4.9)$$

With respect to time-down scaling example, according to this approach we get the following requirements on the **sifted and raw key rates**:

L_{key} [bit]	L_{sift} [bit]	R_{key} [bit/s]	R_{raw} [bit/s]
10^2	10^3	0.42	42
10^3	$5 \cdot 10^4$	2.00	200
10^4	$3 \cdot 10^4$	12.50	1250

Attenuation matching

Let us fix T_{key} and R_{sift} as Rate down-scaling and $R_{raw} = R_0$. We want to find the additional attenuation A_{add} which should be introduced in the POCD system, by means of an optical attenuator at the receiver side, in order to reproduce the SaNeQKD scenario, i.e.,

$$A_{add} = R_{sift}/R_0 \eta A_{rc}(1 - \exp(-\mu)) \quad (4.10)$$

By referring to example of rate-down scaling, we get the following results.

L_{key} [bit]	L_{sift} [bit]	R_{sift} [bit/s]	A_{add} [dB]
10^2	10^3	0.42	-32.3
10^3	$5 \cdot 10^3$	2.00	-25.5
10^4	$3 \cdot 10^4$	12.50	-17.6

Power down-scaling

As in the previous case, let us fix the available time interval $T_{key} = 2400$ s, that, given the required secret key length, yields a sifted key rate $R_{sift} = L_{sift}/T_{key}$. Furthermore, we set $R_{raw} = R_0 = 72$ kbit/s.

According to the power down-scaling approach, we aim at finding the mean number

of photons per qubit η such that we can extract L_{key} final secret key bits in the available time T_{key} . In the POCD setup, this tuning on can be implemented by means of an optical attenuator at the transmitter side with attenuation A_{tx} . The following table shows the values of μ and A_{tx} for a QBER $\epsilon = 1\%$.

L_{key} [bit]	L_{sift} [bit]	μ [photon/qubits]	A_{add} [dB]
10^2	$9 \cdot 10^2$	$3 \cdot 10^{-4}$	-35
10^3	$2.7 \cdot 10^3$	$1 \cdot 10^{-3}$	-30
10^4	$1.6 \cdot 10^4$	$6 \cdot 10^{-3}$	-22

Classical channel specifications

The maximum length of the packets to be sent on the classical channel is $L_{pkt} = L_{sift} \log_2(L_{raw})$. In the followings, we show these packets lengths for two possible scenarios: the first one assumes $A_{link} \sim 0$ and $A_{rc} = 12$ dB, while the second one assumes $A_{link} = 40$ dB and $A_{dev} = 12$ dB.

L_{key} [bit]	L_{sift} [bit]	μ [photon/qubits]	A_{add} [dB]
10^2	10^3	10^5	$1.6 \cdot 10^4$
10^3	$5 \cdot 10^3$	$5 \cdot 10^5$	$9.4 \cdot 10^4$
10^4	$3 \cdot 10^4$	$3 \cdot 10^6$	$6.4 \cdot 10^5$

L_{key} [bit]	L_{sift} [bit]	μ [photon/qubits]	A_{add} [dB]
10^2	10^3	10^9	$3 \cdot 10^4$
10^3	$5 \cdot 10^3$	$5 \cdot 10^9$	$1.6 \cdot 10^5$
10^4	$3 \cdot 10^4$	$3 \cdot 10^{10}$	10^6

The figure 4.17 shows the number of sifted bits that must be available to transmitter and receiver after the transmission on the quantum layer and the sifting phase in order for them to be able to extract a secret key of the desired key length L_{key} . In particular, the dashed lines represent the asymptotic limit in the asymptotic infinite key length regime, while the solid lines represent the values obtained by means of the finite-key analysis described above.

Furthermore, these results assume an attenuation A_{link} of the quantum channel between $-40dB$ and $-45dB$ (corresponding to a wavelength $\lambda = 350nm$ and a telescope diameter of $0.2m$), and that the Winnow protocol [15] is used for the information reconciliation phase.

Also the chosen information reconciliation protocol and privacy amplification parameters ensure a probability of error correction failure equal to 10^{-3} and a fraction of leaked bits of 10^{-3} , respectively.

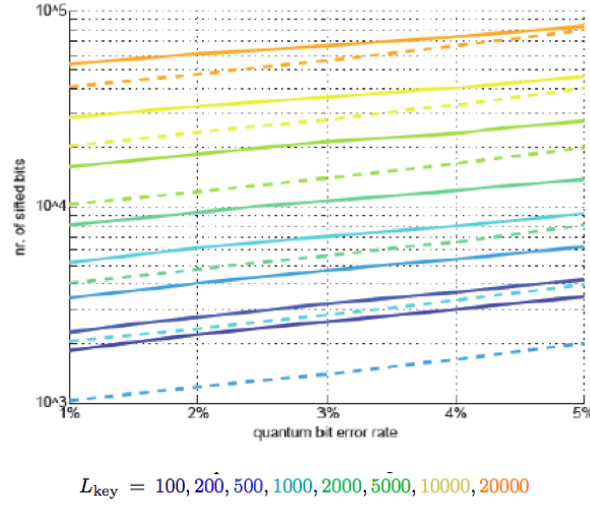


Figure 4.17: shows the number of sifted bits that must be available to the transmitter and the receiver after the transmission on the quantum layer and the sifting phase in order for them to be able to extract a secret key of the desired key length L_{key} . In particular, the dashed lines represent the asymptotic limit in the hypothesis of infinite key length, while the solid lines represent the values obtained by means of the finite-key analysis described above. Furthermore, these results assume an attenuation A_{link} of the quantum channel between -40 dB and -45 dB, and the Winnow protocol underlies the information reconciliation phase. Also the chosen information reconciliation protocol and privacy amplification parameters ensure a probability of error correction failure equal to 10^{-3} and a fraction of leaked bit of 10^{-3} , respectively. As an example, if we want to extract 2000 secret bits with a quantum bit error rate of 2 %, we need approximately 9000 sifted bits.

As an example, if we want to extract 2000 secret bits with a quantum bit error rate of 2%, we need approximately 9000 sifted bits.

With a flyby interval of approximately 40 mins, and a total attenuation $A_{\text{link}}A_{\text{rc}} = -50\text{dB}$, this would require the source to produce a raw key rate $R_0 \simeq 2.4\text{Mb/s}$, which is well in the range of currently available technology.

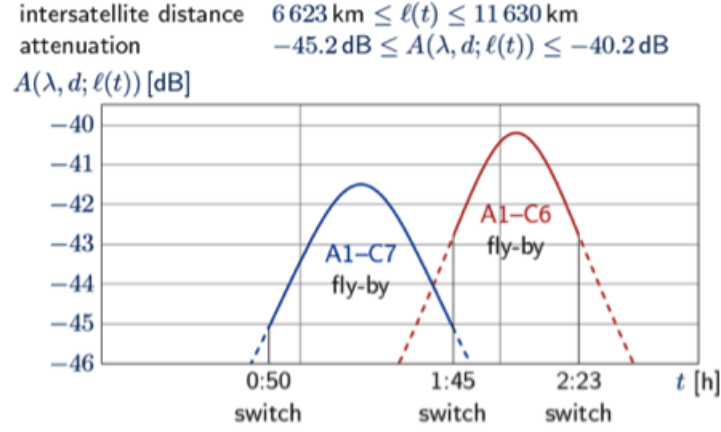


Figure 4.18: The figure represents the simulation for a multi-hop quantum communication between the reference satellite A1 and two satellites C7 and C6, approaching to the reference one and belonging to a same orbital plane. The blue curves represents the simulated hop between satellite A1 and C7, then the red curve represent the simulated hop between A1 and C6 satellite

4.7 Proof of Concept Demonstration: quantum part test plan

The Proof of Concept Demonstration will demonstrate the feasibility of the Optical Quantum Communication Network devised and built for the project "Application of Optical Quantum Links to GNSS". At that moment, the POCD date is dated for spring 2014.

The POCD tests (of the Quantum part SanNe-QKD) will be performed at Thales Alenia Space Headquarter in Turin. The transmitting prototype will be positioned at the top of the building 90, while the receiving prototype will be positioned in a next park. A terrestrial 400m downlink will be established during the night (low background is needed in order to perform QKD (Chapter 3)).

The list below briefly indicates the test plan for the POCD:

1 Demonstration of single-hop OQL.

The aim is to demonstrate a working Optical Quantum Communication prototype for Galileo constellation, in order to simulate multi-hop Quantum Key Distribution between more non adjacent satellites of the network, in realistic conditions of losses and link duration according the simulation of intersatellite links in chapter 3 and the test scenario discussed in 4.6.2. Time and loss varying single links will be simulated and single-hop mode experiments will be performed (according the blue and green line in the figure 4.18).

2 Demonstration of multi-hop OQL

The aim is to demonstrate a working Optical Quantum Communication prototype for Galileo constellation, in order to simulate multi-hop Quantum Key Distribution between two non adjacent satellites of the network, in realistic conditions of losses and link duration according the simulation of intersatellite links in chapter 3 and the test scenario discussed in 4.6.2. A transient switching is simulated between transmitter and receiver with rate adaption, which are typical aspects of OQCN in space between moving segments , simulating QKD with one time pad (figure 4.14)

In the following figure 4.18 it is represented the multi-hop simulation of an intersatellite communication between satellite A1 and satellite C7 flyby, for 1:16 seconds and between satellite A1 and C6, simulating the intersatellite attenuations in the interval $-45.2dB \leq A(\lambda, d, l(t)) \leq -40.2dB$.

The calculated approaching interval distance is between $6623km \leq l \leq 11630km$.

4.8 Conclusions

This is the concluding chapter of the second part of my thesis dedicated to the ESA project.

The quantum prototype **SaNe-QKD** have been developed following the guidelines of compactness and lightness of ESA requirements.

It can be fused by two optic-mechanical interfaces with the optical communication complex **OPT** developed by Thales Alenia Space, becoming a unique system (**SaNe-QKD OPT**) for the "Application of Optical Quantum Links to GNSS".

Besides, we have investigated about the motivations for introducing optical quantum communications on GNSS satellites. Feasibility studies have been developed in order to fix the telescope dimensions and the communication wavelengths.

As the primary limit to the deployment of optical quantum links are the huge distances between the satellites, by exploiting the relative motion of satellites lying in different orbital planes, it has been possible to target communication between satellites that are closer in turns, and to achieve appreciable transmission rates and secret key lengths.

Simulations (with MATLAB tools) for the time windows in which performing the optical quantum links for secure communications during GNSS satellite motions and about beam propagation in space have been reported in Chapter 3.

Finally, the project opens to a promising application field: to build an inter-satellite Quantum Communication Network (OQCN) offering the merits of the classical optical communication (which respect to the RF technology, guarantees high data volume exchange, reduced system mass and power consumption, transmitted narrow beam width,..) and with the added value of the Quantum Key Distribution (performed by SaNe-QKD prototype) aiming to the unconditional security against a computationally unbounded adversary, even one equipped with possible future quantum computational capabilities.

Conclusions

The aim of my thesis is to demonstrate that global-scale quantum communication networks are becoming true: the feasibility studies and the experiments performed in this work emphasize that there is the potential to implement quantum communication techniques in all the requested scenarios: ground and space.

For the **ground scenario** (Chapter 2) our studies confirm that it is achievable to reduce link losses devising a suitable optical system (as the Canary Telescope) able to use the analysis of the beam centroid to compensate the distortions due to the turbulence. An effective and stable free space quantum communication channel is possible and the link losses are contrasted. The system shown (Canary Telescope, Chapter 1) aims to be a reliable solution, using the transmission of an auxiliary beam in real time to probe and compensate the channel while the single photon exchanging is performed simultaneously (co-propagating beam scheme).

Besides, we report that in literature there is a lack of propagation models in atmospheric turbulence, although we have tried to contribute and help, confirming that the atmospheric turbulence changes the statistics of the source (Chapter 2). [62] [19].

The **space scenario** have been exploited (with analyses and simulations of satellites mutual distances for communication issues, quantum protocols used, network topology, key length evaluation); and the designed prototype (SaNe-QKD) have all the requirements to fulfil the demand of optical quantum communication links between ESA Galileo space segments.

However, owing to the constellation altitude (over 20000 kilometres above Earth surface), up/down links are unfeasible with the current techniques (Chapter 3).

In order to overcome this limit, we could suggest that a supporting space segment could be position in low LEO orbit, as a "trusted node" for uplinks and downlinks between the constellation satellites and ground bases. This is only an idea, supported recalling simulations and models in literature. ([12] [89]) They demonstrated that with the current technology only low LEO satellites have the conditions to perform up/down quantum communication links, which is what Chinese and European scientists are going to reach with the present technologies. [104] [75].

Following the feasibility studies and the experiments performed, the implementation of the Galileo constellation with the quantum optical communication prototype SaNe-QKD OPT, (devised by the University of Padova and Thales Alenia Space)

will allow to transform Galileo GNSS constellation into an inter-satellite Optical Quantum Communication Network (OQCN), establishing a stepping stone on the path to the future space communication techniques.

In the end we point out that according table 1 [70] my thesis has embraced topics of beam propagation over free space and over space, exploiting of themes of long term-goal table of QIPQC (satellite Quantum Communication, multi-node Quantum network and (more than) 1000 kilometres of Quantum Cryptography) in the view of giving a contributes to the developments of Quantum Communication over projects which open to a promising application field: to build an inter-satellite multi-node Quantum Communication Network (OQCN) with the added value of the Quantum Key Distribution performing long ranges Quantum Key Distribution, aiming to the unconditional security against a computationally unbounded adversary.

Bibliography

- [1] A. Alonso, M. Reyes and Z. Sodnik, “*Performance of satellite-to-ground communications link between ARTEMIS and the Optical Ground Station*,” *Proc. SPIE 5572, Optics in Atmospheric Propagation and Adaptive Systems, VII*, 372 (November 11, 2004);
- [2] L.C. Andrews, R.L. Phillips, C.Y. Hopen, “*Laser Beam Scintillation with Applications*”, *SPIE Press 2001*;
- [3] Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., et al. *Long distance quantum communication with entangled photons using satellites. IEEE J. Sel. Top. Quant. Electr.* 9 (6), 1541–1551, 2003;
- [4] D. Bacco, M. Canale, N. Laurenti, G. Vallone, P. Villoresi, *Experimental QKD with finite-key security analysis for noisy channels*, *Nature Comm.*;
- [5] D. Bacco, *Comunicazione quantistica finalizzata alla realizzazione di chiavi in spazio libero*, *Master thesis, Padova, 2011*;
- [6] J.S.Bell, “*On the Einstein Podolsky Rosen paradox*”, *Physics*, 1,3 (195), 1964;
- [7] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters “*Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*”, *Phys. Rev. Lett.* 70 1895 (1993);
- [8] C. Bennett et al. “*Quantum cryptography using any two nonorthogonal states*”, *Phys. Rev. Lett.* 68, 3121-3124 (1992) ;
- [9] C.H. Bennett, G. Brassard, “*Quantum Cryptography: Public key distribution and coin tossing*”, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175-179, India, (1984);
- [10] D. Binosi, “*Strategic report on current status , visions and goals for research in Europe*”, *QIPC Quantum Information Processing and Communication, QIST, London 2008*;
- [11] K. Bohmer, M. Gregory, F. Heine, H. Kampfner, R. Lange, M. Lutzer, R. Meyer “*Laser Communication terminals for the European Data Relay System*, *Proc.*

- SPIE 8246, free-space Laser Communication Technologies, XXIV, 82460D (February 9, 2012);*
- [12] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, P. Villoresi *Feasibility of satellite quantum distribution. New Journal of Physics 11, 045017; Arlington, 2009;*
 - [13] D. Bouwmeester, A. Ekert, A. Zeilinger, *The physics of quantum information: quantum cryptography, quantum teleportation, quantum computing. Springer Verla, 2000*
 - [14] G. Brassard, L. Salvail, "Secret-key reconciliation by public discussion," *Euro-crypt 1993, pp. 410-423;*
 - [15] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson *Fast, efficient error reconciliation for quantum cryptography, Phys. Rev. A, 2003;*
 - [16] W. T. Buttler, R.J. Hughes, P.G. Kwiat, S. K. Lamoreaux et al. "Practical free-space Quantum Key Distribution over 1 km", *Phys. Rev. Lett. 81 3283-3286, 1998;*
 - [17] M. Canale, D. Bacco, S. Calimani, F. Renna, N. Laurenti, G. Vallone and P. Villoresi *A prototype of a free-space QKD scheme based on the B92 protocol, ISABEL 2011, Barcelona, Spain, 29/10/11;*
 - [18] I. Capraro, A. Tomaello, A. Dall'Arche, F. GERLIN, R. Ursin, G. Vallone, P. Villoresi, *Free-Space Laser Communication Technologies, Proc. SPIE 8246, doi:10.1117/12.916078;*
 - [19] I. Capraro, A. Tomaello, A. Dall'Arche, F. GERLIN, R. Ursin, G. Vallone, P. Villoresi, *Impact of turbulence in long range quantum and classical communications, Phys. Rev. Lett., arXiv:120.6931,2012;*
 - [20] G. Cariolaro, C. De Angeli, N. Laurenti "Comunicazioni ottiche", *Edizioni Libreria Progetto(2006);*
 - [21] G. Cariolaro, "Telecomunicazioni Quantistiche", *(2008);*
 - [22] R. Corvaja, I. Capraro, A. Dall'Arche, N. Dalla Pozza, F. GERLIN, A. Tomaello, M. Zorzi, A. Assalini, A. Ferrante, G. Pierobon, F. Ticozzi, G. Vallone, P. Villoresi, *Engineering a Long Distance Free-Space Quantum Channel, Proceedings of Isabel 2011, Barcelona, Spain, 2011;*
 - [23] H.D. Curtis, *Orbital Mechanics for Engineering Students, Elsevier Aerospace Engineering series, 2005;*
 - [24] F. Dios, J.A. Rubio, A. Rodriguez, A. Cameron, *Appl. Opt. 43,3866 (2004);*

- [25] M. Dusek, M. Jahma and N. Lutkenhaus *Unambiguous state discrimination in quantum cryptography with weak coherent states*, *Phys. Rev. A* (62,2,022306,13/7/00);
- [26] A. K. Ekert, "Quantum cryptography based on Bell's theorem" *Phys. Rev. Lett.* 67,661 (1991)
- [27] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution" in *IEEE International Symposium on Information Theory, ISIT, 2009*, pp. 1879-1883;
- [28] C. Elliott "The DARPA Quantum Network" in *Quantum Communications and Cryptography*, ed. A. Segienko, M. Dekker, CRC Press, 2006;
- [29] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh "Current status of the DARPA quantum network" *Proceedings of the SPIE*, 5815:138-149 (2005);
- [30] R.L. Fante, *Proc. IEEE* 63,1669 (1975);
- [31] R.L. Fante, *Trans. Antennas Propag.* 23, 382 (1975) ;
- [32] R.L. Fante, *Proc. IEEE* 68,1424 (1980);
- [33] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, *Nat. Phys.* 5, 389 (2009);
- [34] S. Fossier, et al,
- [35] ;
- [36] D.L. Fried, *J. Opt. Soc. Am.* 56,1372(1966);
- [37] F. GERLIN, *Site-testing Astroclimatologico dell'Osservatorio Astronomico di Asiago*, Master degree thesis in Astronomy, University of Padua, 29 June 2009;
- [38] F. GERLIN, N. Laurenti et al. *design optimization for quantum communications in GNSS intersatellite network, Localization and GNSS, ICL-GNSS, 2013 International Conference, Turin, 2325-0747, p. 6, 25-27 June 2013*;
- [39] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography", *Rev. Mod. Phys.*, 74 145-95, 2002;
- [40] D. Gottesman and J. Preskill, "Secure Quantum Key Distribution using squeezed States", *Phys. Rev. A* 63, 022309 (2001) ;
- [41] F. Grosshans et al. *Proceedings of the sixth International Conference on Quantum Communications, Measurement and Computing (QCMC 02) Rinton Press, Princeton, NY, 2002*

- [42] Grosshans et al., "Quantum key distribution using gaussian-modulated coherent states", *Nature* 421, 238 (2003)
- [43] E. Hecht, *Optics, Addison-Wesley Longman, 1998*;
- [44] M. Heid, N. Lutkenhaus, *textit* 2006, *Phys. Rev. A* 73, 052316
- [45] H. Hemmati *Near-Earth Laser Communications, CRC Press, Taylor and Francis Group, 2009*;
- [46] J. Horwarth, F. David, M. Knappek, N. Perlot, "Coherent transmission feasibility analysis", *Free-Space Laser Communication Technologies XVII; G. S. Mecherle; Ed. Proc. SPIE Vol. 5712, p.13-23, April 2005*;
- [47] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson *Quantum cryptography for secure satellite communications, IEEE AERO, 1,191-200, 2000*;
- [48] T. E. Humphreys *Detection Strategy for Cryptographic GNSS Anti-Spoofing, IEEE Transactions on Aerospace and Electronic Systems, 49,2,1073-1090,4/13*;
- [49] B. Huttner, N. Imoto, N. Gisin and T. Mor *Quantum cryptography with coherent states Phys. Rev. A (51,3,1863-1869,3/95)*;
- [50] P. Kaye, R. Laflamme, M. Mosca, "An introduction to Quantum Computing", *New York Oxford University Press (2007)*;
- [51] A. Kolmogorov, *Turbulence, Classical papers an Statistical Theory, S. K. Friedlander, L. Topper, New York, 1961*;
- [52] A. Turbulence, "The local structure in an incompressible viscous fluid for very large Reynolds numbers", *C.R. (Dokl) Acad. Sci. USSR 30, 301-305, 1941*;
- [53] C. Kurtsiefer, P. Zarda, M. Hadler, H. Weinfurter, P.M. Gorman, P.R. Tapster, J.G. Rarity, "Quantum cryptography,: a step towards global key distribution", *Nature 419(6906): 450,10,2002*;
- [54] V. Kuzkov, D. Volovyk, S. Kuzkov, V. Caramia, Z. Sodnik, S. Pukha, "Laser Ground System for Communication Experiments with ARTEMIS," *Proc. IC-SOS, 9-12 October 2012*;
- [55] N. Lutkenhaus Security against individual attacks for realistic quantum key distribution *Phys. Rev. (61,5,052304,6/4/00)*;
- [56] X. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, A. Zeilinger *Quantum teleportation over 143 kilometres using active feed-forward, Nature, 489, 269, 2012*;

- [57] H.K. Lo, X. Ma, K. Chen "Decoy state quantum key distribution", *Physical Review Letters* 94 (23),230504;
- [58] X. Ma, B. Qi, Y. Zhao, K. H.K. Lo, "Practical decoy state for quantum key distribution", *Physical Review A* 72(1),012326;
- [59] Y. Zhao, B. Qi, X. Ma, H.K. Lo, L.Qian, "Experimental quantum key distribution with decoy state", *Physical Review Letters* 96(7),070502;
- [60] U. M. Maurer et al., *Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory.* 39,733 (1993)
- [61] E. Meyer-Scott, Z. Yan, A. MacDonald, J. Bourgoin, H. Hübel, and T. Jennewein *How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss*, *Physical Review A*, 84,6,062326,22/12/11;
- [62] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, *J. Opt. B* 6, S742 (2004);
- [63] <http://esc.gsfc.nasa.gov/267/278/279/LASER-COMMUNICATIONS-SET-FOR-MOON-MISSION.HTML>;
- [64] M.A. Nielsen, I.L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, (2000);
- [65] J.W.Pan et al., *Teleporting independent qubits through a 97km free-space channel*, *arXiv:1205.2024*,2012;
- [66] P. Papadimitratos and A. Jovanovic *Protection and fundamental vulnerability of GNSS*, *IEEE IWSSC*, 167-171, 2008;
- [67] M. Peev et al. "The SECOQC quantum key distribution network in Vienna", *New J. Phys.* 11 075001 (2009);
- [68] N. Perlot, M. Knappek, D. Giggenbach, J. Horwath, M. Brechtelsbauer, Y. Takayama, T. Jono, "Results of the Optical Downlink Experiment KIODO from OICETS Satellite to Optical Ground Station Oberpfaffenhofen (OGS-OP)", *SPIE Photonics West, Free Space Laser Communication Technologies XIX*, San Jose, Jan. 2007;
- [69] Pirandola, S. Braunstein, S.L., Mancini, S. Lloyd, S., *Secure quantum direct communication with continuous variables*, *Euro Physics Letters* 84, 20013-1/6 (2008)
- [70] <http://qurope.eu/content/qipc-roadmap/>
- [71] B.E.C. Saleh, M.C. Teich, *Fundamentals of photonics*, Wiley series in pure and applied optics. Wiley-Interscience. 2007;

- [72] M. Sans, Z. Sodnik, I. Zayer, R. Daddato, "Design of the ESA Optical Ground Station for participation in LLCD," *Proc. ICSOS, 9–12 October 2012*;
- [73] V. Scarani and R. Renner *Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post processing* *Phys. Rev. Lett.* (100,20,200501,23/5/08);
- [74] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev *The security of practical quantum key distribution* *Rev. Mod. Phys* 81,3,1301-1350,9/09;
 bibitemScheidl10 T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, and A. Zeilinger, *Proc. Natl. Acad. Sci. U.S.A.* 107, 19 708 (2010);
- [75] T. Scheidl, E. Wille, R. Ursin "Quantum optics experiments to the International Space Station ISS: a proposal, *New J. Phys.* 15043008, 2013"
- [76] T. Schmitt-Manderbach, *Experimental demonstration of free-space decoy-state quantum key distribution over 144km*, *Phys. Rev. Lett.* 98,010504,2007;
- [77] www.secoqc.net/;
- [78] Shannon C.E., 1949, *Bell Syst. Tech, J.* 28, 656
- [79] Shor, P. W., 1994 Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe (IEEE Computer Society, Los Alamitos)
- [80] A.Siegman, *Lasers, University Science Books, Mill Valley, 1986*;
- [81] Stazione Spaziale Internazionale, en.m.wikipedia.org/wiki/International_Space_Station;
- [82] X. Sun, D. R. Skillman, E. Hoffman, D. Mao, J.F. McGarry, L. McIntire, R. S. Zellar, F. M. Davidson, W. H. Fong, M. A. Krainak, G. A. Neumann, M. T. Zuber, D. E. Smith, "Free space laser communication experiments from Earth to the Lunar Reconnaissance Orbiter in lunar orbit," *Optic Express*, vol. 21, pp. 1865-1871 (2013);
- [83] O.Svelto, *Fundamentals of photonics, 1999*;
- [84] webpage http://space.skyrocket.de/doc_sdat/terrasar-x.html;
- [85] V.I. Tatarski, *Wave Propagation in a Turbulent medium* (McGraw-Hill, New York, 1961);
- [86] TelescopeOptics.net, website, www.telescope-optics.net/relecting.htm;
- [87] http://www.dlr.de/en/desktopdefault.aspx/tabid-78/7420_read-14120/;

- [88] T. Tolker-Nielsen and G. Oppenhauser, “*In-orbit test result of an operational optical intersatellite link between ARTEMIS and SPOT4, SILEX*,” *Proc. SPIE 4635, Free-Space Laser Communication Technologies, XIV, 1 (April 30, 2002)*;
- [89] A. Tomaello, C. Bonato, V. DaDeppo, G. Naletto, and P. Villoresi, “*Link budget and background noise for satellite quantum key distribution*,” *Advances in Space Research, 47(5): 802-810, 2011*;
- [90] Tomaello, A. Dall’Arche, A. Gerlin, F., Capraro, I. Vallone, G. and Villoresi, P. “*Experimental Studies toward the Quantum Communications with orbiting terminals*”, *OSA 2012, Quantum Information and Measurement2012*;
- [91] A. Tomaello, “*Quantum Communication channels between earth and space*” *PhD thesis (2012)*;
- [92] M. Tomamichel, C. C. W. Lim, N. Gisin and R. Renner *Tight finite key analysis for quantum cryptography, Nature Comm. vol. 3, art. 634, January 2012*;
- [93] M. Toyoshima, S. Yamakawa, K. Arai, M. Reyes, A. Alonso, Z. Sodnik, P. Lopez, B. Demelenne, “*Ground-to-satellite optical link tests between Japanese laser communications terminal and European geostationary satellite ARTEMIS*,” *Proc.SPIE 5338, Free-Space Laser Communication Technologies, XIV, 1 (June 16, 2004)*;
- [94] R.K. Tyson, *Adaptive optics engineering handbook, Optical science and engineering, Marcel Dekker, 2000*;
- [95] P.B. Ulrich, *Hufnaghel-Valley profiles for specified values of the coherence length and isoplanatic patch angle. WJSA/MA/TN-88-013, Arlington, Va, 1988*;
- [96] R.Ursin, S. Backus, K. F. Tiefenbacher, T. Schmitt- Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek et al. *Entanglement based quantum communication over 144km.Nat. Phys. 3,481-6, 2007*;
- [97] U.S. Office of the Secretary of Defence, *Unmanned Aerial Vehicle Roadmap, 2000-2025, p. 33, 2001*;
- [98] G. Vallone, P. Villoresi, I. Capraro, A. Dall’Arche, F. GERLIN, A. Tomaello, *Expeerimental Study of Free-Beam propagation for Single-photon Quantum OSA 2012*;
- [99] Vernam, G.S.,1926, *J. Am. Inst. Elect. Eng.* 55,109
- [100] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, *Experimental verification of the feasibility of a quantum channel between space and Earth, New J. Phys. 10, 033038 (2008)*;

- [101] P. Villoresi et al., *Space-to-Ground quantum communication using an optical ground station: a feasibility study. Quantum Communications and Quantum Imaging II, Proceeding SPIE 5551 113, 2004*;
- [102] C. Weedbrook, et al. "Quantum Cryptography Without Switching", *Physical Review Letters* 93, 1-4 (2004).
- [103] W Wootters, W. Zurek, *A single quantum cannot be cloned, Nature, 299:802-803, October 1982*
- [104] J. Yin, Y. Cao, S.-B. Liu, G.-S. Pan, J.-H. Wang, T. Yang, Z.-P. Zhang, F.-M. Yang, Y.-A. Chen, C.-Z. Peng, J.-W. Pan "Experimental single-photon transmission from satellite to Earth", 2013 [arXiv.org/abs/1306.0672](https://arxiv.org/abs/1306.0672)

Ringraziamenti

Vorrei ringraziare il Prof. Paolo Villoresi per avermi dato l'opportunità di lavorare nel gruppo di ricerca delle comunicazioni quantistiche e per avermi seguito in questi tre anni di dottorato. Grazie Paolo.

Ringrazio inoltre i Prof.ri Pino Giuseppe Vallone e Nicola Laurenti per la loro disponibilità a discussioni, correzioni, valutazioni in merito ai temi di ricerca affrontati; in particolare ringrazio Nicola per i caffè alla macchinetta del secondo piano nei lunghi pomeriggi pre-TN.

Non da ultimo desidero ringraziare il Prof. Giampiero Naletto per la sua continua disponibilità e per i tanti consigli e suggerimenti.

Ringrazio Zoran Sodnik di ESA (Agenzia Spaziale Europea), e, per Thales Alenia Space di Torino, Luciana Bonino e Sergio Mottini, coinvolti nel progetto "Application of Optical Quantum Link to GNSS".

Chiedendovi scusa se qualche nome verrà involontariamente dimenticato, ringrazio i tanti colleghi/amici (presenti e passati) di questi tre anni fra Luxor e DEI: Mattia, Andrea e Alberto, Stefano e Alberto, Marco e Davide Giacomo, Davide e Bacci, Alain, Marco e Vanessa, Lorenzo e Marcomattia, Matteo e Nicola, per i piacevoli pranzi al parco e per i quarti d'ora d'aria trascorsi assieme.

Un ringraziamento inoltre agli amici Quantum del Venerdì', al Prof. Luca Poletto (direttore dei Laboratori Luxor) e alle Prof.sse Paola Zuppella, Maria G. Pelizzo e Vania Da Deppo.

Grazie di nuovo a tutti voi per questi meravigliosi ed intensi tre anni di ricerca trascorsi assieme