DAVIDE BACCO

QUANTUM COMMUNICATIONS BETWEEN EARTH AND SPACE

Università degli Studi di Padova

Centro di Ateneo di Studi e Attività Spaziali "Giuseppe Colombo" (CISAS)

Sede Amministrativa: Università degli studi di Padova

UNIVERSITÀ DEGLI STUDI DI PADOVA

CISAS G. COLOMBO

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

SCUOLA DI DOTTORATO:
SCIENZE, TECNOLOGIE E MISURE SPAZIALI

INDIRIZZO:
SCIENZE E TECNOLOGIE PER APPLICAZIONI SPAZIALI E AERONAUTICHE (STASA)

CICLO: XXVII

Quantum communications between Earth and Space

Dottorando
Davide Bacco

Supervisore Interno
Ch.mo Prof. Giampiero Naletto

Supervisore Esterno
Ch.mo Prof. Paolo Villoresi
Dr. Mario Cosmo

DIRETTORE DELLA SCUOLA:
Ch.mo Prof. Giampiero Naletto

COORDINATORE D'INDIRIZZO:
Ch.mo Prof. Giampiero Naletto

Cielo, e non altro, cielo alto e profondo,
cielo deserto. O patria delle stelle!
O sola patria agli orfani del mondo!
— G. Pascoli

ABSTRACT

In this society people are always connected, and everyday they manage a lot of personal data also risking to be eavesdropped. Quantum science is one the most promising field of the next years, from quantum computing to quantum communications and above all quantum cryptography. Quantum cryptography is the first commercial application of quantum physics and moreover it results one of the most reliable solution for security problem. Using Quantum Physic law's it is possible to establish secure communications between two users, guaranteeing unconditionally security in the transmission of data. Unfortunately due to the intrinsic losses inside optical fibers, it is not possible to establish a quantum link over 300 km until quantum repeater will be achievable. The natural extension of terrestrial quantum links are space communications, where however the problems due to environment, temperature and pressure are totally new for quantum devices. The study investigated the possibility of sending quantum signals through atmosphere, in particular trying to realize quantum communications between Earth and Space. In this perspective we used Laser Ranging corner-cubes mounted into satellites to recreate a space quantum link. It was possible to prove that even with high losses, variable attenuation, and high backgorund a quantum key distribution system works, and an unconditionally secure key, needful for encryption, can be generated. With this experiments we demonstrate that not only free-space quantum key distribution is a ready technology, but also that quantum satellite communications is nowadays possible and realizable. Moreover these results open the way to look towards a global space quantum network, where optical station (OGS) could talk with satellite and vice-versa. This work was supported by the Strategic Project QUANTUMFUTURE of University of Padova, by ESAGNSS program and realized in Luxor laboratories in Padova. The principal tests were made at Telespazio (Matera) using the Matera Laser Ranging Observatory and into Thales Alenia Space (Torino).

SOMMARIO

Le persone al giorno d'oggi sono continuamente connesse e ogni giorno maneggiano dati sensibili, rischiando di venire intercettati e truffati. La fisica quantistica si inserisce in questo settore come uno dei campi più promettenti per gli anni futuri, dal computer quantistico, alle comunicazioni ottiche e in particolare la crittografia quantistica (QKD), aiutano lo sviluppo di sistemi incondizionatamente sicuri. La crittografia quantistica è stata la prima applicazione commerciale della fisica quantistica, rappresentando inoltre una soluzione versatile e sicura per la trasmissione di dati in modo incondizionatamente sicuro. Sfruttando le leggi della meccanica quantistica, come il teroema di non clonabilità e il fatto che ogni misura perburba lo stato, è possibile creare una chiave crittografica fra due utenti che consente, sotto alcune condizioni, di comunicare in modo cmatematicamente sicuro. Esistono già da alcuni anni sistemi commerciali di crittogafia quantistica in fibra ottica. Sfortunatamente a causa delle perdite intrinsiche della fibra non è possibile comunicare oltre i 300 km, fino a quando i ripetitori quantistici non saranno realizzati con alta efficienza. In questo settore si inserisce lo studio presentato in questa tesi, cercando una valida alternativa ai collegamenti in fibra ottica. La naturale estensione dei link quantistici terrestri è rappresentata dalle comunicazioni quantistiche satellitari, dove nonostante i problemi legati all'ambiente di utilizzo (temperatura, pressione, particelle ionizzate, etc) sono presenti parecchi risultati che lasciano ben sperare. Entrando in dettaglio lo studio presentato studia gli effetti della propagazione di un fascio ottico quantistico in atmosfera, in particolare nella condizione di un link quantistico fra Terra e Spazio. In questa prospettiva sono stati individuati come possibili dispostivi i retroriflettori utilizzati nelle misisoni di Laser Raanging, utilizzati solitamente per lo studio della geodesia spaziale. Sfruttando questi satelliti abbiamo ricreato un canale quantistico in downlink dove fosse possibile sperimentare i protocolli quantistici come la QKD. Nonostante le condizioni di lavoro molto sfavorevoli, (alte perdite, attenuazione variabile, puntamento instabile) è stato dimostrato che è possibile inviare nello Spazio un fotone, in un particolare stato quantistico e misurarne le sue caratteristiche. Questo risultato apre la strada alla crittografia quantistica in spazio libero, dimostrando come nonostante ci sia ancora molto strada da fare nell'ambito della fisica quantistica, alcune tecnologie sono mature e pronte per essere implementate in scala globale. In una prospettiva futura questo risultato dimostra come sia possibile immaginare una rete di satelliti quantistici in grado di comunicare con le stazioni base a terra ma anche fra loro. Questo lavoro è stato supportato dal progetto strategico di Ateneo QuantumFuture dell'Università degli studi di Padova, dai fondi ESAGNSS e realizzato sia nei laboratori Luxor del CNR UOS di Padova. I test principali sono stati eseguti nel Telespazio di Matera (ASI) e a Torino nella sede di Thales Alenia Space.

ACKNOWLEDGMENTS

Foremost, I would like to express my sincere gratitude to my advisor Prof. Paolo Villoresi for introducing me to the beauty of quantum mechanics and for introducing me inside the QuantumFuture Group.
Besides my advisor, I would like to thank the rest of my thesis committee, especially Prof. Giampiero Naletto for the advices always precise and correct, for his encouragement, insightful comments, and hard questions.
A particular thanks to Dr. Giuseppe Vallone, for the continuous support during my Ph.D study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me over all these years.
Last but not less important, my fellow labmates in Padova and every boys inside QF Group, that have supported me during this three years. Thanks also to all the people in Luxor laboratories for having chatted and discussed.
A great thank to my friend Davide Giacomo Marangon for helping me during my activities and above all for the continuous ideas and collaborations inside and outside the laboratory, it was a pleasure to work with you.
Last but not the least, I would like to thank my family: my parents Annalisa e Sergio, my brother Giacomo and especially to Chiara for helping and supporting me during these years, especially during the long missions in Matera or Torino.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

QKD Quantum Key Distribution

CS Computer Science

QRNG Quantum Random Number Generator

LEO Low Earth Orbit

MEO Medium Earth Orbit

GEO Geostationary Earth Orbit

MLRO Matera Laser Ranging Observatory

QC Quantum Communications

QM Quantum Mechanic

QP Quantum Physics

SNR Signal to noise ratio

IR Information Reconciliation

PA Privacy amplification

CC Classical cryptography

QCy Quantum cryptography

OTP One Time Pad

BER Bit error rate

PE Parameter Estimation

EB Entangled based

QRNG Quantum random number generator

WCP Weak coherent pulse

JKT Jacobus KapteinTelescope

OGS Optical ground station

ISS Internationl Space Station

ARTS Adaptive Real Time Selection

OQL Optical quantum link

GNSS Global Navigation Satellite System

CV Continuous Variable

DV Discrete Variable

PM Prepare and Measure

EB Entanglement based

IAs Individual attacks

IRs Intercept-and-resend

CAs Collective attacks

GAs General attacks

QBER Quantum bit error rate

RSA Rivest Shamir Adleman

CCRs Corner Cube Retroreflectors

SLR Satellite Laser Ranging

QWP Quarter wave plate

OQL Optical quantum link

APD Avalanche photo diode

INTRODUCTION

Quantum physics is one the most curios and interesting discoveries of the last 120 years. For a lot of time it was considered not only a useless science but too complicated to understand and impractical. Luckily more and more scientists began to look at Quantum Physics with a lot of interest. This fact bring the community to deal about quantum and the new theory about the completion of classical mechanic physic. Thanks to that and to other discoveries, Quantum Science became an important axiom in the physics field.

In particular the possibility to use Quantum Physics in order to establish secure communications was more attractive from various point of view.

Cryptography was one of the most interesting field from the ancient age to the present. The necessity of exchanging secret information between two users, without anyone else could look at the messages, has always passionate man.

The development of communications systems were quite slow until the World War II, when the discovery of the telegraph and subsequently of the phone, has laid the foundations of modern telecommunications.

Modern telecommunications grown up in a exponential way during the Twentieth century, defining the past century as "The information age". The strategic importance of communications has request the possibility of exchanging information in a secure way. In fact during the last 50 years the practice of secure link has become more and more frequently. In the case of governments institution, patents and discoveries from industry, to our daily lives, everyone need a way to communicate his restricted data in a secure way. Classical cryptography based its security on mathematical algorithms, in fact the difficulty that an eavesdropper has to extract information is directly proportional to the computing capacity. In the case of a quantum computer being built in the nearly future, the cryptographic system available today becomes in few time obsolete and insecure.

In this context QKD plays a crucial role allowing to establish a secure communication between two parties.

In fact QKD is a technique for sharing a random secure secret key, which will be used for Alice and Bob (respectively the transmitter and the receiver) for encrypting and decrypting the messages. For this purpose, an optical link is necessary to Alice and Bob to communicate using the principle of Quantum Mechanic (QM) and so permitting to discover a possible eavesdropper. Moreover QKD may be considered the first successful example of a quantum information protocol available in everyday applications. Indeed, commercial devices trough optical cables are already accessible worldwide. In the case of long distances, moving terminals and satellites space communications, the possibility of using free-space links is also very attractive.

In this perspective the aim of this thesis is to demonstrate that Quantum Communications (QC) is not only something bound to the laboratory research, but also a mature technology able to resolve some problems and helping the world in the struggle versus the enemies.

In this perspective, with the experiment presented, for the first time we proved the possibility to communicate through a quantum link with space satellites and moreover that in a near future it is possible to think about a global quantum network.

Let's now introduce the chapters description and a small resume of the argument described and studied.

In Chapter 1 we report a brief summary of the basic principles of QM, in particular paying attention to qubit definition and to all the tools necessary to understand real applications of theory concepts.
From Chapter 2 to Chapter 7 we describe our activities and experiments in the field of quantum communications.
Chapter 2 we introduce the concept of QKD, we explain the basic principles of the system, some protocols and moreover we define security from mathematical point of view.

Furthermore in order to create a secure communication between Earth and Space, we researched and worked in finite key regime, where the work conditions are limited by environment constraints. We demonstrate that also in presence of high level of noise and finite key regime it is possible to create a secure key: this results will be very useful for satellites link because the good time for acquisition is very limited to decades of minutes.
In Chapter 3 we study the propagation of a quantum beam in atmosphere, trying to understand which are the principal effects and how they could be mitigated. In this perspective we reported an experiment made in 2012 in Canary Archipelago, where we demonstrated how it is possible to take advantage from atmosphere effects in secure key generation rate.
Chapter 4, 5 and 6 we leave terrestrial links looking towards satellite communications. Nowadays there are not orbiting quantum transmitter or receiver available for QC, so we recreate a quantum space link between satellites and Earth. In this perspective we used corner-cube retroreflectors mounted on satellites to simulated a downlink quantum channel and realizing a quantum link between satellites and an Optical ground station (OGS).

In satellites communications, the estimation of the channel parameters is a fundamental request.In fact in Chapter 4 we present the theory about the estimation of the link, explaining how it was possible to calculate all the constants appearing in the experiments.
In Chapter 5 we introduce Polarimeter, an instrument useful for studying the polarization of photons sent into Space. This have been very useful for QKD experiment because it permits a primary verification of which satellites are available for QC.
In Chapter 6 we report the principal results obtained in Matera 3 experiment, realizing the outcomes of this task. Moreover we point out a new record for single photon qbit transmission, where it was possible to receive a single photon from a distance of 7000 km.
In Chapter 7 we report an experiment in collaboration with TASI (Thales Alenia Space) regards a quantum payload for Global Navigation Satellite System (GNSS) satellite. In fact we studied and realized an OQL system, where a complete optical QKD transmitter and receiver were implemented and tested in order to demonstrate the feasibility of QC between satellite in Space. Moreover this experiment opens the way for a global network of QKD where Earth-satellite and even satellite to satellite communications could be possible.

Finally in Chapter 8 we summarize the main results of the thesis and we propose some new experiments that could be implemented and realized with the know-how acquired during these years.

INTRODUZIONE

La fisica quantistica è una delle scoperte più interessanti e affascinanti degli ultimi 120 anni. Per molto tempo gli scienziati l'hanno ritenuta pressoché inutile, teorica e incomprensibile. Inoltre, non riuscivano ad intravedere possibili applicazioni nella società. Per questi motivi è sempre stata considerata una materia di nicchia. Tuttavia negli anni, gradualmente, la comunità scientifica si è approcciata allo studio della Fisica Quantistica, capendone e cominciando ad esplorarne l'enorme potenziale. Grazie alle successive scoperte la Fisica Quantistica assunse una valenza internazionale, fino a divenire un punto fermo del XX secolo. In particolare, è possibile giustificare la suddetta affermazione grazie alle leggi fondamentali della Meccanica quantistica e alle loro applicazioni, quale ad esempio la possibilità di scambiare informazioni in modo completamente sicuro.
La ricerca di metodi per rendere un messaggio nascosto, così da renderlo non comprensibile ai non autorizzati, ha da sempre appassionato l'uomo. Si ritrovano esempi antichi di crittografia a partire dai Mesopotamici.
Lo sviluppo dei sistemi di comunicazione è stato piuttosto lento fino alla seconda guerra mondiale, quando le scoperte del telegrafo e, successivamente, del telefono hanno posto le basi delle moderne telecomunicazioni. Esse sono cresciute in modo esponenziale nel corso del XX secolo, definito da alcuni come "L'era dell'informazione".
La società odierna basa la sua importanza sulla possibilità di scambiare le informazioni in modo sicuro e riservato. Infatti, negli ultimi 50 anni l'uso della crittografia è divenuto sempre più radicato. Innumerevoli sono gli esempi quotidiani in cui è necessaria la massima riservatezza e integrità. Si pensi, per fare alcuni esempi, ai governi europei e mondiali, alle istituzioni, ai brevetti delle scoperte industriali e, per finire, ai nostri dati sensibili.

La crittografia oggi utilizzata (classica), basa la sua sicurezza su algoritmi matematici, e sulla difficoltà che un eventuale attaccante incontrerebbe se venisse a conoscenza del messaggio cifrato.
Possiamo definire la sicurezza garantita dalla crittografia classica come una sicurezza legata alla potenza di calcolo dell'attaccante. È stato dimostrato che nel caso (non ormai così remoto) i cui fosse disponibile un computer quantistico, gli attuali sistemi crittografici sarebbero da considerare insicuri. Infatti, l'esecuzione e il compimento di operazioni molto complesse, come la fattorizzazione di numeri primi, da parte di un computer moderno può durare anche decenni. La stessa operazione eseguita da un computer quantistico potrebbe essere ultimata in tempi molto rapidi. A causa di questa problematica, da anni gli scienziati cercano una tecnica che possa fornire un modo completamente sicuro di scambiare informazione indipendentemente dalla potenza di calcolo dell'attaccante. In questo contesto, la crittografia quantistica svolge un ruolo fondamentale che permette di stabilire una comunicazione sicura tra due parti. Infatti la crittografia quantistica è una tecnica per la condivisione di una chiave casuale, in seguito utilizzata da Alice e Bob (rispettivamente il trasmettitore e il ricevitore) per codificare e decodificare i messaggi. La comunicazione sicura è basata su un link ottico fra i due interlocutori dove, grazie alle leggi della meccanica quantistica, siamo

in grado di capire se la trasmissione è stata intercettata o meno. Inoltre la crittografia quantistica può essere considerata come il primo esempio di un protocollo di informazione quantistica disponibile nelle applicazioni di tutti i giorni. In effetti, esistono già da alcuni anni dispositivi commerciali in fibra ottica che implementano alcuni protocolli di crittografia quantistica. Tuttavia, a causa delle perdite intrinseche della fibra ottica non è possibile superare la distanza di 300 km mediante un solo link. In questo contesto la propagazione quantistica in atmosfera è divenuta molto attraente negli ultimi anni, soprattutto considerando la possibilità di creare una comunicazione sicura tra terminali mobili.
Alla luce di questa affermazione, il lavoro di tesi si propone di dimostrare che le Comunicazioni Quantistiche non sono solamente un campo di ricerca sperimentale, ma si stanno affacciando come tecnologia matura potenzialmente applicabile nella società. Riportiamo ora una breve descrizione degli argomenti trattati in ogni capitolo, sottolineando gli scopi iniziali e i risultati ottenuti.
Nel Capitolo 1 è riportata una breve sintesi dei principi di base della Meccanica Quantistica, in particolare prestando attenzione alla definizione di qubit e a tutti gli strumenti necessari per comprendere gli esperimenti presentati.
Dal Capitolo 2 al Capitolo 7 sono descritte le attività di ricerca ed alcuni esperimenti nel campo delle comunicazioni quantistiche.

In particolare nel capitolo 2 viene introdotto il concetto di crittografia quantistica, spiegando i principi base del sistema, i protocolli più utilizzati e introducendo la definizione di sicurezza dal punto di vista matematico. Essendo inoltre il nostro obiettivo l'estensione delle attuali comunicazioni quantistiche, mediante un collegamento Terra e Spazio, ci siamo concentrati nel regime di "chiave finita", dove le condizioni di lavoro sono limitate da vincoli ambientali.

Grazie a questo esperimento abbiamo dimostrato come, anche in presenza di alti livelli di rumore e di un numero limitato di bit, sia possibile creare una chiave incondizionatamente sicura: questo risultato è molto utile nel caso di link satellitari dove il tempo disponibile per l'acquisizione è limitato a decine di minuti.
Nel Capitolo 3 invece, viene studiata la propagazione di un fascio ottico in atmosfera, cercando di capire quali sono gli effetti principali e come potrebbero essere mitigati. In questa prospettiva riportiamo un esperimento realizzato nel 2012 nell'Arcipelago delle Canarie, dove si dimostra come sia possibile sfruttare gli effetti dell'atmosfera nella generazione di una chiave sicura. Nello specifico abbiamo utilizzato le fluttuazioni intrinseche dell'atmosfera per sondare il canale e sfruttare questo fenomeno, sia per diminuire gli errori, sia per aumentare il numero finale di bit ricevuti. Questo metodo è applicabile negli attuali sistemi di crittografia quantistica in spazio libero, permettendo così di migliorare l'efficienza e il rate di chiave.
Nel Capitolo 4, 5 e 6 i protagonisti non sono più i collegamenti terrestri, bensì le comunicazioni Terra satellite. Al giorno d'oggi, non sono presenti in orbita trasmettitori o ricevitori quantistici. Per questo motivo abbiamo ricreato un collegamento quantistico tra i satelliti e la Terra utilizzando i retroriflettori montati su alcuni satelliti, utilizzati dalla comunità di Laser Ranging spaziale. Siamo quindi stati in grado di simulare sperimentalmente un link quantistico fra un satellite e una stazione base ricevente.

Nelle comunicazioni a lunga distanza e soprattutto in quelle satellitari, la stima dei parametri del canale è molto importante.
In particolare nel Capitolo 4 sono presentati alcuni concetti di teoria alla base delle moderne telecomunicazioni sia terrestri che spaziali, spiegando in particolare come sia stato possibile calcolare tutti i parametri presenti negli esperimenti.
Nel Capitolo 5 introduciamo il Polarimetro, uno strumento utile per studiare la polarizzazione dei fotoni inviati nello spazio. Questo si è dimostrato molto valido perché ha permesso una verifica primaria di quali satelliti fossero utilizzabili per le comunicazioni quantistiche.
Nel Capitolo 6 invece vengono riportati i risultati ottenuti nell'esperimento Matera 3. In questo esperimento è stato possibile inviare per la prima volta dei singoli fotoni polarizzati da un satellite e misurarne la loro polarizzazione. Questa misura apre la strada verso la crittografia quantistica satellitare, dimostrando come sia possibile trasmettere e ricevere singoli fotoni a grandissima distanza. Siamo inoltre riusciti a far propagare un singolo fotone da una distanza maggiore ai 7000 km. Questo pone un nuovo limite per le trasmissioni quantistiche.
Nel capitolo 7 invece viene riportato un esperimento in collaborazione con THALES Italia riguardante un payload quantistico per il sistema di navigazione satellitare GNSS. Abbiamo infatti realizzato un sistema completamente ottico in grado di simulare il comportamento di due satelliti nel processo di scambio e riconciliazione di chiavi quantistiche. Il sistema inoltre è stato testato, con risultati positivi, in un link in spazio libero di 500 m. Questo esperimento apre la strada ad una rete globale di crittografia quantistica in cui saranno possibili sia comunicazioni terra-satellite, sia collegamenti intra satellitari.
Infine nel capitolo 8 vengono riassunti i principali risultati della tesi e proposti alcuni possibili esperimenti futuri, potenzialmente attuabili utilizzando il prezioso il know-how acquisito in questi anni.
Riteniamo che i nostri piccoli contributi alla comunità scientifica siano invece di grande interesse per le Comunicazioni quantistiche, dove i nostri esperimenti possano in parte contribuire ad una futura una rete quantistica globale.

1 QUANTUM MECHANICS AND QUBIT

Quantum information science is a combination of Computer Science, Quantum Physics and Information Theory. It is a completely interdisciplinary field, combining together the physics model and axioms of QM, the protocol and algorithm of Computer Science (CS) with the aim of exchanging and manipulate information. In this Chapter we report some basic concepts of QM. The aim is to introduce the necessary equation, theorems and postulates in order to completely understand the content of this thesis. For major detail see [34].

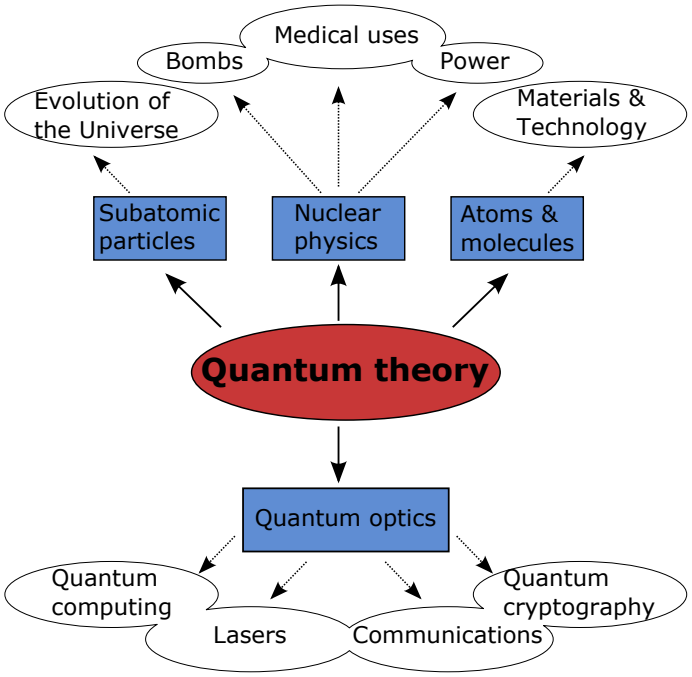


Figure 1.1: Representation of some research field and applications born from Quantum theory.

1.1 POSTULATES OF QUANTUM MECHANICS

Quantum theory ia a mathematical model of the physics world. In order to define this model it is necessary to introduce mathematical formalism on which are based the fundamental concepts of QM. In particular QM is ruled by few postulates, which for the aim of this works can be summarized in four core hypothesis:

Postulate 1. *In QM a state of a physical system is described by a complex wave function or equivalently from a vector in an Hilbert Space* $\Psi(r,t)$*. The function* $\Psi(\cdot)$ *is completely integrable and normalizable (*$\int_{allspace}|\Psi|^2 = 1$*).*

Postulate 2. *The evolution of a quantum closed system is described by a unitary transformation. The state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by an operator U which depends from t_1 and t_2 time:*

$$|\psi'\rangle = U|\psi\rangle \tag{1.1}$$

This definition doesn't give any information about a particular state, but it only describes the evolution of the quantum system. Another more precise definition and where the variable t, time is described by a continuous variable is the Schrödinger equation:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \tag{1.2}$$

depending on th Hamiltonian operator H[1]. The equation could also be written as:

$$\frac{d}{dt}|\psi(t)\rangle = -iH|\psi(t)\rangle \tag{1.3}$$

The knowledge of the Hamiltonian of the system describes completely the system dynamics.

Postulate 3. *All the dynamical variables in a system can be represented by a linear hermitian operator with eigenvalues λ_i and eigenvectors $|\lambda_i\rangle$. The outcome of a measure will be one of the eigenvalues with probability $|\langle\lambda_i|\Psi\rangle|^2$ and the measurement will reduce the state of the system from $|\Psi_i\rangle$ to $|\lambda_i\rangle$.*

Postulate 4. *Interactions and composite of quantum systems are completely described by the tensor product of the single component states: $|\Psi_{12}\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$.*

1.2 QUANTUM COMPUTATION AND QUBITS

Before defining what are the basic elements of a quantum system, we would like to introduce the general criteria useful for exploring quantum computing and in general quantum system. We report here the David DiVincenzo principles explaining the needful criteria in order to successfully implement a quantum information process [34]. The five core requirements for the implementation of quantum computing are:

1. a scalable physical system with well characterized qubits (memory)
2. the ability to initialize the initial state of the qubits, such as $|000\cdot\rangle$
3. a long relative decoherenece times, much longer than the gate operations time
4. a "universal" set of quantum gates with high fidelity for speedy operations
5. qubit-specific measurement capabilities without modify other neighbors qubits

He also added two supplementary criteria relating to the transmission and movement of information:

1 The average value of Hamiltonian operator describes the system energy.

6. The ability to interconvert stationary and flying qubits
7. The ability to faithfully transmit flying qubits between specified location.

These 7 criteria represents a complete set of operations necessary for exploring a QC physical system. However, before considering the complexity of the entire system, it is necessary to introduce some basic concepts of QM.

1.2.1 *Qubit*

The Qubit word means literally quantum bit. It represents the information as a quanta, thus the smallest part where can be encoded data. As in the classical system, based on operation between bits, from a quantum point of view, the core of the system are based on qubits.
In a more stringent definition, the qubit symbolize the state of a vector Hilbert two-dimensional space. A generic qubit $|\psi\rangle$, represents in a vector space V, with $|0\rangle$ and $|1\rangle$ orthogonal can be symbolized as:

$$|\psi\rangle = a|0\rangle + b|1\rangle\,. \tag{1.4}$$

The main difference between classical bit and qubit rely in the fact that a classical bit can be represented only in two values 0 or 1, while a qubit can assumes infinite values, thanks to the superposition of the base state $|0\rangle$ and $|1\rangle$. It is not possible with a single measure recover the value of the parameters a an b, in fact a measurement on a qubit return $|0\rangle$ with a probability a^2, and the state $|1\rangle$ with probability b^2. Moreover after the qubit measurement, the state will collapse in one of the two base states, so we can say that after the measurement we know, with a probability equal to one the state of the system. Some examples of qubits are: polarization of photons, electron spin, spin of core atom, ions in resonant cavities, etc.
A useful representation for a generic qubit, is the Bloch sphere (Figure 1.2), where a qubit is represented by a single vector into an unit sphere.

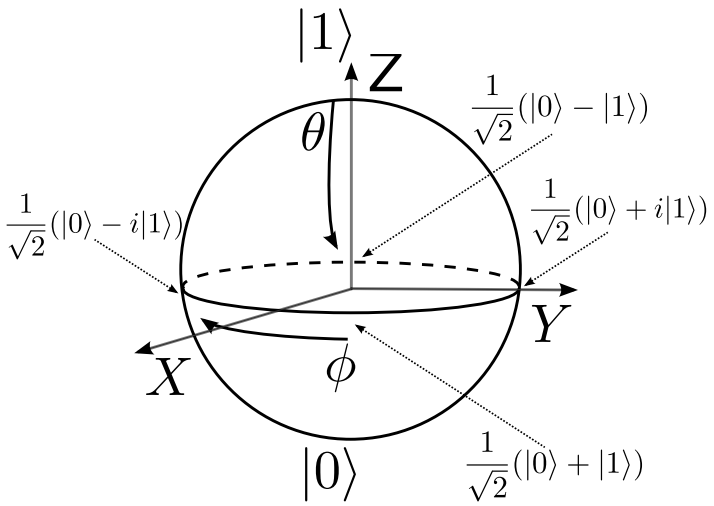


Figure 1.2: The Bloch sphere is a graphical representation of the state of a single qubit.

1.2.2 *Copy of a qubit*

In the classical system the copy of a bit is a simple operation, while in the case of a quantum state a perfect copy of a qubit is not allowed. The *no-cloning theorem* proves as a generic quantum state cannot be copied. Here we report a small proof of the famous theorem: let's consider a physical state $|\psi\rangle$ that we would clone, and the generic state $|s\rangle$ where we carry the copy. The total state state of the system is based on two qubits, so the output values are given by the tensor product $|\psi\rangle \otimes |s\rangle$. The linear operator that describes the copy operation works as follows:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\,; \tag{1.5}$$

and in the same way for a state $|\phi\rangle$:

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle\,. \tag{1.6}$$

Then calculating the internal product between the two equation results:

$$(U(|\psi\rangle \otimes |s\rangle)) \cdot (U(|\phi\rangle \otimes |s\rangle)) = (|\psi\rangle \otimes |\psi\rangle) \cdot (|\phi\rangle \otimes |\phi\rangle)\,. \tag{1.7}$$

and using linearity property we have:

$$(|\psi\rangle \otimes |s\rangle) \cdot (|\phi\rangle \otimes |s\rangle) = (|\psi\rangle \otimes |\psi\rangle,\, |\phi\rangle \otimes |\phi\rangle) \tag{1.8}$$

$$\langle\psi|\phi\rangle\langle s|s\rangle = \langle\psi|\phi\rangle\langle\psi|\phi\rangle \tag{1.9}$$

Considering the fact that the vector $|s\rangle$ has unitary norm, the equation become:

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2 \tag{1.10}$$

and the only solution are $\langle\psi|\phi\rangle = 0$ and $\langle\psi|\phi\rangle = 1$, thus only in the case that the two states are equal or orthogonal. this means that copy operator could works only in the above written cases. This theorem will be very useful for our experiments and in particular it is one of the basic principle of QKD.

1.2.3 *Qubit manipulation and Gates*

One important characteristic in an physical system is the possibility of controlling the variables, in particular the possibility of making operations, changing the states and processing information. In fact the second DiVincenzo criteria tells us how to initialize our qubits, moving our qubit in a particular position of the Bloch sphere.

From a mathematical point of view, using 4 unique rotations, it is possible to transform any input state into another qubit. The 4 rotations don't alter the final vector and they works along each Cartesian axis.
The Pauli matrices, as a result of the exponential Hamiltonian operator deriving from Schrödinger equation $|\Psi\rangle = \exp(-i\hat{H}t/\hbar)|\Psi(0)\rangle$, can perfectly represent one rotation about the respective axis. They are defined as:

$$\hat{\sigma}_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \hat{\sigma}_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \hat{\sigma}_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \hat{\sigma}_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.11}$$

It follows:

$$R_I(\theta) = e^{-i\theta\hat{\sigma}_I/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{bmatrix} \tag{1.12}$$

$$R_X(\theta) = e^{-i\theta\hat{\sigma}_X/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{1.13}$$

$$R_Y(\theta) = e^{-i\theta\hat{\sigma}_Y/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{1.14}$$

$$R_Z(\theta) = e^{-i\theta\hat{\sigma}_Z/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{bmatrix} \tag{1.15}$$

An example of unit transformation $\theta = \pi$, corresponding to a single rotation about the y axis, should intuitively flip the qubit from 0 to -1. Using the definition $|0\rangle = \begin{bmatrix} 0\,1 \end{bmatrix}^T$ and $|1\rangle = \begin{bmatrix} 1\,0 \end{bmatrix}^T$ we obtain:

$$R_Y(\pi)|0\rangle = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix} = -|1\rangle \tag{1.16}$$

The physical concept behind this operations is that using an Hamiltonian with Pauli operators permits to initialize and control a single qubit state. There exist also 4 simple operations deriving from special rotation: they are known as Pauli gates, X, Y, Z and the Hadamard gate. The Pauli gates are simply transformation matrices equivalent to the original Pauli matrices. The Pauli Y gate, known as a conjugate bit flip, maps the state $|0\rangle \to i|1\rangle$ and $|1\rangle \to -i|0\rangle$. It corresponds to a π rotation about the Y axis on the Bloch sphere. The Pauli Z gate is a phase flip gate, it leaves the $|0\rangle$ state unchanged but $|1\rangle \to -|1\rangle$. This is also a π rotation about the Z axis on the Bloch sphere.

The Hadamard gate instead[2] puts the qubits onto the equator of the Block sphere in a superposition state. Specially, $|0\rangle \to 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|1\rangle \to 1/\sqrt{2}(|0\rangle - |1\rangle)$. This is equivalent to π rotation about the $(1, 0, 1)$ axis or the $(\vec{x} + \vec{z})/\sqrt{2}$. Finally the Pauli X gate represents the NOT operation and maps the states $|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$. Examples of how it is possible to obtain a not gate:

$$B = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.17}$$

1.3 MULTIPLE QUBIT

As natural extension of the presented analysis in the case of a single qubit, it is possible to deal also multiple qubits. We must distinguish two possibilities:

- the qubits are uncorrelated (one operation made in one qubit, didn't modify the other one)

2 The Hadamard transformation matrix is $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

- the qubits are correlated (the state of one qubit is bound to the other, and moreover from the knowledge of a state it is possible to recover information about the other)

From a mathematical point of view, in the case of two space vectors V and W with the respective basis $\{v_1, v_2\}$ and $\{w_1, w_2\}$ from the tensor product we have:

$$\{v_1 \otimes w_1,\, v_1 \otimes w_2,\, v_2 \otimes w_1,\, v_2 \otimes w_2\} \tag{1.18}$$

and the space dimension becomes $\dim(V \otimes W) = \dim(V) \times \dim(W)$. In a system with two qubits, each one with its own base ($\{|0\rangle, |1\rangle\}$), we will obtain:

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \tag{1.19}$$

As reported for two qubit, can be extended for n qubit, and the state representation becomes:

$$|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle \tag{1.20}$$

where $|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1$. In the case we want to measure a quantum state based of n qubit, and reminding that the measurement process is a probabilistic, the obtained result of the first qubit in $\{|0\rangle, |1\rangle\}$ base will be:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \tag{1.21}$$

highlighting the first qubit we have:

$$|\psi\rangle = |0\rangle \otimes \big(a|0\rangle + b|1\rangle\big) + |1\rangle \otimes \big(c|0\rangle + d|1\rangle\big) = \tag{1.22}$$

$$\begin{aligned} &= \sqrt{n}\,|0\rangle \otimes \left(\frac{a}{\sqrt{n}}\,|0\rangle + \frac{b}{\sqrt{n}}\,|1\rangle\right) + \\ &+ \sqrt{m}\,|1\rangle \otimes \left(\frac{c}{\sqrt{m}}\,|0\rangle + \frac{d}{\sqrt{m}}\,|1\rangle\right) \end{aligned} \tag{1.23}$$

where $n = |a|^2 + |b|^2$ and $m = |c|^2 + |d|^2$. At the end of the process, a measure of the first qubit give the following result:

- $|0\rangle$ with a probability n, and the final state will be:
  $|0\rangle \otimes \left(\frac{a}{\sqrt{n}}\,|0\rangle + \frac{b}{\sqrt{n}}\,|1\rangle\right)$
- $|1\rangle$ with a probability m, and the final state will be:
  $|1\rangle \otimes \left(\frac{c}{\sqrt{m}}\,|0\rangle + \frac{d}{\sqrt{m}}\,|1\rangle\right)$

1.3.1 *Quantum entanglement*

In previous paragraph we report examples of correlated system, where the alteration of one qubit is bound to the other and vice-versa. It is possible to define *Entanglement state* a state where it is not possible to go back at a_1, a_2, b_1, b_2 parameters describing the state:

$$|\psi\rangle = \big(a_1|0\rangle + b_1|1\rangle\big) \otimes \big(a_2|0\rangle + b_2|1\rangle\big)\,. \tag{1.24}$$

An example of an entangled qubit is:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{1.25}$$

It is worth to note that any measure in one qubit change also the state of the other qubit. From a mathematical point of view, if we measure the first qubit, without having already measured the second one, it results that:

$$P[qubit_1 = |0\rangle] \mid qubit_2 \text{ non measured}] = \frac{1}{2}$$
$$P[qubit_1 = |1\rangle] \mid qubit_2 \text{ non measured}] = \frac{1}{2}$$

The result change completely in the case that the second qubit was already measured with a $|0\rangle$ result:

$$P[qubit_1 = |0\rangle] \mid qubit_2 \text{ measured}] = 1$$
$$P[qubit_1 = |1\rangle] \mid qubit_2 \text{ measured}] = 0$$

In the case where the measurement made on the second qubit was $|1\rangle$, the probability values will be inverted.

BELL STATES Usually entangled state is created by particular interactions between subatomic particles. There are more ways to produce an entangled state. One of the most famous and used method is the SPDC down-conversion[3] to generate a pair of entangled photons in polarization [49]. Other methods include the use of the Hong-Ou-Mandel effect: by the use of a fiber coupler to confine and mix photons, the use of quantum dots to trap electrons until decay occurs, are all method that permits the creation of an entangled state [48]. A particular protocol, know as *entanglement swapping* permits to create entangled photons using quantum systems never interacting directly [28, 81].

HADAMARD GATES One important way to create an entanglement state using one simple transformation, is to perform an Hadamard gate (see 1.2.3. By applying on a 0 qubit an Hadamard rotation and then using the output state as the control bit of a CNOT [4] gate, it follows that:

$$|\Psi_1\rangle = U_{Had}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1.26}$$
$$|\Psi_{12}\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{1.27}$$
$$|\Psi_{ent}\rangle = U_{CNOT}\,|\Psi_{12}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.28}$$

3 SPDC: spontaneous parameter down conversion is optical quantum process where a non linear crystal is used to split one photon into pairs of photons. These photons generated have combined energies and momenta equal to the energy and momentum of the original photon. Moreover they are phase-matched in the frequency domain, and have correlated polarizations.

4 The CNOT gate can be represented by the matrix $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

In this way it is possible to create the 4 maximally entangled states called Bell states, defined as:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.29}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{1.30}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{1.31}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1.32}$$

QUANTUM TELEPORTATION One of the most fascinating thing of QM is the possibility to perform a quantum teleportation of the state information. In 1993 C. Bennet and colleagues invent a protocol where a maximally entangled qubits, in addition to some classical information, could effectively *teleport* an unknown state of a qubit between two distant and different locations.
Our aim it to transmit a generic quibit from A to a different location B. In order to achieve this teleportation scheme, it is necessary three qubits, the transmitted qubit a, the messenger b and the receiver qubit c. The first step is to create a maximally entangled state between the qubit b and c. After this operation c is sent toward the location B, using a quantum channel as optical-fiber or free-space link. Then applying a CNOT gate between the qubit a and b and subsequently an Hadamard rotation on a the preparation process is completed. When we measured the qubit a and b collapsing their state, instantaneously information about qubit a is teleported to qubit c.
In this process qubit a will be destroyed after the measurement, and in according with the no-cloning theorem no copies are created. It should be noted that qubit b never leaves the location A and the teleportation happens between qubit a and qubit c.

The qubit b and c are prepared in the Bell state $\frac{1}{\sqrt{2}}(|0_b\,0_c\rangle + |1_b\,1_c\rangle)$ while the unknown qubit a, which we want to teleport from location A to B is in the state $|\Psi_a\rangle = \alpha|0_a\rangle + \beta|1_a\rangle$. From the property reported in the above paragraphs, it results that the entire system is in the state:

$$|\Psi_\Sigma\rangle = |\Psi_a\rangle|\Psi_{bc}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right) \tag{1.33}$$

When it is applied the CNOT gate to the first qubit, we obtain:

$$U_{CNOT_{(a,b)}}\,|\Psi_\Sigma\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right) \tag{1.34}$$

now applying the Hadamard transformation, see equation (2) to qubit a so that $|0_a\rangle \to \frac{1}{\sqrt{2}}(|0_a\rangle + |1_b\rangle)$ and $|1_a\rangle \to \frac{1}{\sqrt{2}}(|0_a\rangle - |1_b\rangle)$ the system becomes:

$$U_{Had_{(a)}}U_{CNOT(a,b)}|\Psi_\Sigma\rangle = \frac{1}{2}[\,|0_a0_b\rangle\,(\alpha|0_c\rangle + \beta|1_c\rangle) + |1_a0_b\rangle\,(\alpha|0_c\rangle - \beta|1_c\rangle) + |0_a1_b\rangle\,(\beta|0_c\rangle + \alpha|1_c\rangle) + |0_a1_b\rangle\,(\beta|0_c\rangle + \alpha|1_c\rangle)\,]$$

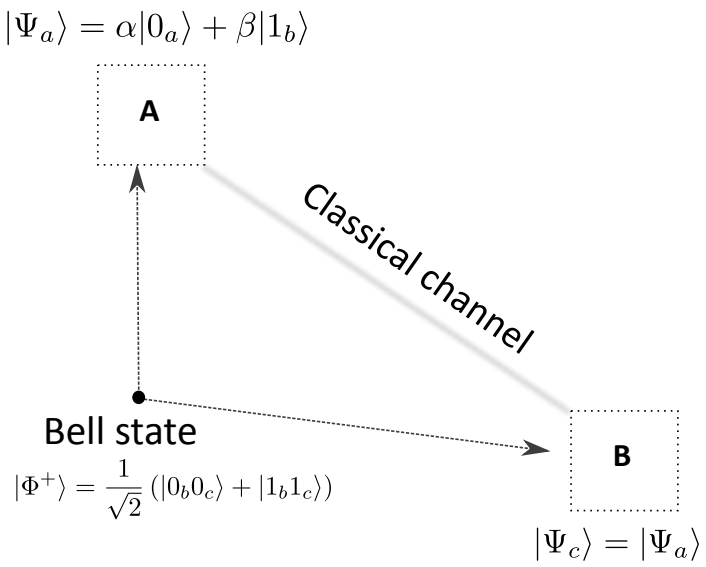


Figure 1.3: Teleportation scheme: an entangled Bell state is created. The photons b and c are sent to the location A and B respectively. After the rotation, transformation and measurement process between the qubit a and b, we have teleported the qubit a into the qubit c. The classical channel is necessary to transfer information about the measured make in location A.

We can note that $|\Psi_c\rangle$[5] looks nearly identical to $|\Psi_a\rangle$ except a rotation. Once the measurement in location A of qubits a and b is made, the result of this measure is sent classically to location B. In this way it is known the exact rotations to perform into qubit c in order to obtain the original state a. The term of teleportation, sometimes abused, consist on the transport of information about a quantum state, located in a place A to a different place B without direct interaction. During the last years it was proved that it is also possible to teleport a quantum state using electrons and entangled diamonds respect to photons [84]. Maybe in future the scientists will discover more information about entanglement state, but until now we have to use it and this process represents one good use of this phenomenon. Moreover teleportation or other protocol using entangled state would be very useful looking to a future mixed quantum network based on satellite, base stations and repetition node.

5 $|\Psi_c\rangle = |0_a 0_b\rangle(\alpha|0_c\rangle + \beta|1_c\rangle) + |1_a 0_b\rangle(\alpha|0_c\rangle - \beta|1_c\rangle) + |0_a 1_b\rangle(\beta|0_c\rangle + \alpha|1_c\rangle) + |1_a 1_b\rangle(\beta|0_c\rangle - \alpha|1_c\rangle)$

2 QUANTUM KEY DISTRIBUTION

Nowadays telecommunications play a crucial role in our daily lives, everyone is always connected and during all the day there are a continuous exchange of information. In this scenario, Secure communications become more and more important in many areas, e.g. on-line purchases, emails and video chats. Quantum cryptography (QCy) or QKD applies fundamental laws of quantum physics to guarantee secure communications. The security of quantum cryptography was proven in the last 30 years. The security analysis of the QKD system is usually based on the assumption that the component parts are considered ideals. From a practical point of view instead, the device imperfections and usury of the components must be taken into account for a completely investigation of the system. In this chapter we present the fundamental of QKD, introducing the layered model of the system and explaining how it is possible to implement a completely quantum cryptography working system.
A particular section will be dedicated to finite key analysis. This kind of analysis will offer a novel approach against the classical one, allowing an improvement of the final rate especially in a very bad scenario like satellite communications, where the attenuation of the channel is very high.

2.1 CRYPTOGRAPHY AND QUANTUM CRYPTOGRAPHY (SOA)

The discovery and the theory formalization of QM in the XX century has opened new horizons in science and techniques. Governments and scientific community made a lot of effort in QM field, in fact in the last 15 years it was possible to appreciate big ideas and results. However before this technology becomes present in our daily lives a lot of work is still considerable. The research is very closely linked to the technological development, in fact a lot of idea are not yet implemented for the lack of mature technology, but in the last two year quantum devices have become more and more important (e.g. quantum memory, quantum repeater, etc).
QKD was the first practical QM idea implemented in the 1984 thanks to Charles H. Bennet and Gilles Brassard [15]. This idea, thought by Stephen Wiesner in the 1970 [115], was realized only fourteen years later. Even though the concept was very simple and a lot of devices were available in those years, the idea met resistance also in the scientific community. Only ten years later, Information community was ready to understand the infinite potentially of QM. Here we resume the basic history of QCy:

- 1970, Stephen Wiesner, "Conjugate coding:" noisy transmission of two or more "complementary messages" using single photons in complementary polarization bases
- 1984, Bennet and Brassard, BB84 Protocol: the first QKD system was realized

- 1991, Artur Ekert EPR-Ekert protocol: it was invented the E91 protocol using maximally entangled state to distill quantum keys

These three discoveries encase all the science about QKD development in the last 30 years. Obviously during all this time a lot of advancements were made in QM field, but the basic principles of all the protocols can be extracted from there.

2.1.1 *Classical cryptography*

From the ancient age cryptography was one the most important fields of interest, above all in war context where the messages and the news about the enemy were very important to to take advantage in the battle.

The basic scheme of Cryptographic system is reported in Figure 2.1, there are a sender and a receiver and sometimes an eavesdropper. The sender in order to communicate in a secret way with his own partner, must hide or modify the plain text so that it becomes very difficult for an eavesdropper to extract information about the message.
In cryptography, one of the classical famous method to encrypt information was a cipher, historically very used (Caesar or Napoleon cipher) but now abandoned for its few security.
A cipher is a sort of secret alphabet, where every letter (or groups of letters) are substituted with another one, so that it is possible to rewrite the message in an secret way. In this case, obviously also the other partner must known the cypher dictionary.

This ciphers are not very reliable, above all after the development of modern computer, where the scheme like cipher cryptography becomes very simple to decrypt using tools such as frequency analysis. However mechanical or electro-mechanical classical ciphers were used until modern years and Enigma was one of the most known cypher.

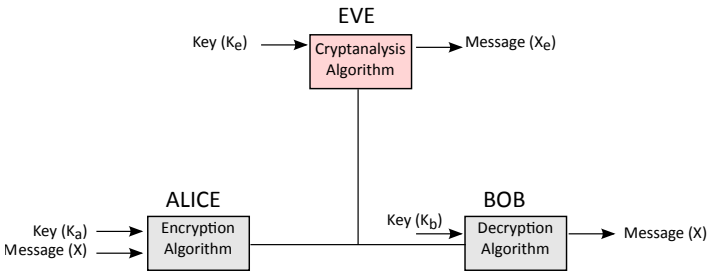


Figure 2.1: Base scheme of classical cryptography system: the sender Alice encrypts the message and sends it to Bob through a communication channel. Eve tries to extract information about the message using cryptanalysis methods. Bob once he received the message from Alice is able to decrypt the ciphertext and recover the message.

2.1.2 *RSA cryptosystem*

From the birth of Information science and of the computers, Rivest Shamir Adleman (RSA) algorithm is one of the most used public-key cryptosystems for secure data transmission. In this particular scheme the encryption key

is public (accessible by everyone), while the encryption key is secret. This asymmetry in the protocol guarantees the security algorithm, in fact the difficulty of an eavesdropper to factoring the product of two large prime numbers is very huge, and an analysis with a nowadays computers will take also a lot of years [87].

A user that would use RSA encryption must choose two large prime numbers, and then publish only the second one. This number represents the public key, that anyone can use to encrypt messages. In the conditions that the public key is large enough, only who knowns the prime (secret) number could decrypts the message.

The method of RSA encryption can be subdivided in three steps: the key generation, the encryption of the message and the decryption.

- *key generation*: the public key, known by everyone is used for encrypting messages. Messages encrypted with the public key can only be decrypted with the private key.
- *encryption*: once Bob receive the public key from Alice, he will send the message M to Alice. Before doing this operation, Bob has to turn M into an integer m, such that $0 \leqslant m < n$ using a reversible protocol known as a padding scheme. Then he computes c as $c \equiv m^e (\mod n)$ and transmits the ciphertext to Alice.
- *decryption*: Alice can recover the integer number m from the ciphertext c using her private key d and computing $c \equiv c^d (\mod n)$. Once she knows the parameter m, she can recover the original message M by reversing the padding scheme

2.2 THE FUNDAMENTAL OF QKD

Let's now see how QM is the basic core for QKD. A QKD system is based on two different communications channels, a quantum channel ruled by QM laws, useful for key exchange with photons, and a classical channel used for error correction and privacy amplification actions.
The quantum channel is confidential and restricted to Alice and Bob users, while classical channel may be realized with a public communication links (e.g. Internet network, LAN, free-space optical classical link, optical fiber, etc) and it is accessible to everybody. In fact an important characteristic of classical channel is that everyone could read the encrypted message, however from Shannon's proof if it was used One Time Pad (OTP) (see 2.3.1) encryption, it would have been impossible for an eavesdropper to recover the message.
In Figure 2.2 it is reported the base scheme of a QKD system, where Alice and Bob exchange keys through quantum channel and use a secure part of these keys for encrypting data and sharing through classical channel.

The big difference between classical and quantum cryptography resides in the way they protect information: Classical cryptography (CC) uses theory codes to improve the complexity of the algorithm through which it is possible to encrypt data; from the other point of view QCy uses the laws of Quantum Physics (QP) in order to achieve a unconditionally security on the keys that will be used to encrypt data with OTP[1] method. From the theoretical point of view it is possible to imagine a uncrackbable cryptographic

1 see OTP paragraph 2.3.1

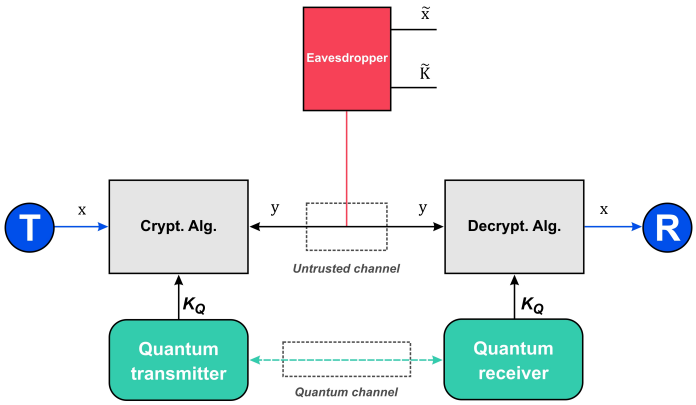


Figure 2.2: Base scheme of QKD system.

system based on the simple scheme presented in Figure 2.2. However from an experimental vision the situation is quite different: it is necessary to decide the trade off between the security that your system require and how many information Eve could access. This problem is not due to the limitation of QM but only to technical imperfections of the instruments used in the QKD system. This is very important looking to the future where the transmission of secure data will be more and more precious and QKD will be one of the easiest and the secure way to do it.
In this chapter we analyzed into details the concept of quantum security, unconditionally security and in particular we will show the mathematical models behind these concepts.

2.3 DEFINITION OF THE SECURITY ANALYSIS OF QKD

The basic laws of QP presented in Chapter 1 are here recalled in order to explain how QCy works. The idea that every measure perturbs the quantum state of the photons and moreover that is not possible to obtain a perfect copy of a generic quantum state plays good for us. In fact if an eavesdropper would measure our photons, during the transmission through the quantum channel and then resend them, we are able to detect the difference thanks to the principles of QM.

Otherwise on the transmission trough the classical channel, Alice and Bob could be intercepted, but before this action the channel must be authenticated (with a pre-shared key) in order to escape every loss of information. Moreover also in the case that Eve is able to obtain information about the encrypted message, it would not be a problem if all the steps of QKD were performed in the correct way.
The first step of a QKD protocol is the exchange and the measurement of quantum states on the quantum channel.

Depending of the protocols Alice, must specify which quantum state she send ($|\psi(S_n)\rangle$) for the sequence of n symbols $S_n = \{S_1, \ldots, S_n\}$. The other user, Bob has to measure and decode the signals but above all he has to estimate the total losses in order to evaluate the presence of a possible eavesdropper.

An important characteristic of Alice encoding is that the chosen states of the protocol must be non-orthogonal, otherwise Eve could decode the sequence without introducing errors but only measuring the qubits in the right bases [51].
It is possible to subdivide QKD protocols in two big groups: Prepare and Measure (PM) scheme, where Alice prepares the states and then sends to Bob, and Entanglement based (EB) scheme where a couple of entangled photons are sent simultaneously to Alice and Bob. Once the users have received photons, they can measured and establish a secure key. The principle of this protocols relies in the entanglement phenomena, in fact the measures made by Alice and Bob are perfectly correlated, in the sense that the results of the measurement of the two particles are surely in one orthogonal base. In this way if Eve try to extract information about the quantum state, she destroys these correlations so that Alice and Bob can detect.
Depending on the conditions of the channel, from the final key rate requirements and obviously from the final use of the system, one can choose which is the best configuration. Moreover the security proof for EB protocol translates immediately to the corresponding PM one and vice-versa.

Once Alice an Bob has exchange enough data (N symbols), they can start the processing step, sending some important information through the classical channel. In all QKD protocols the statistic of the data transmission must be estimated by Alice and Bob: error rate in decoding (QBER), loss of coherence, loss of the channel, transmission rate, detection rates, etc.
The most important parameter is the Bit error rate (BER), because depending on the measured value the data could be good or unusable. Due to the chosen protocol the level of the threshold is different. This step is called Parameter Estimation (PE) and usually it is preceded by a sifting phase, where Alice and Bob exchange through the classical channel the measured base or the detection position's, in order to share the same $l \leqslant N$ symbols. This symbols all together make the key; it is in part correlated and only partially secret. Now we are going to see how create a perfect secure key starting from sifted bits. The length of the secure key (k of length l) depends on how much information Eve has extracted from the raw key.

2.3.1 *One Time Pad*

OTP is the unique method to encrypt message in the unconditional secure way. Invented by Gilbert Vernam in 1917, and demonstrated by Shannon in the '50 years, this technique uses one time a completely random pre-shared key. In particular at least the dimension of the key must be of the same length of the message to encrypt [98]. Vernam cipher works as follow:

- the two users share an identical key. The length of the key at least equal to the dimension of the plain text [2]
- Alice can encrypt the message only adding the plain text to the key [3]
- Bob deciphers the encrypted message and then he destroys the key

2 plain text is information a sender wishes to transmit to a receiver.
3 $\oplus$ sum using XOR operation.

This method works only under some restrict conditions: Alice and Bob must share a secret identical key composed by true random bits.[4] It was proved by Vernam that it is impossible, from the mathematical point of view, that an eavesdropper can decrypts the cypher text, if all the hypothesis written above are respected. The main problem in this method is the difficulty of creating a shared key between the two users, because classical method didn't allow this kind of operation. However in the past, usually during the wars period, a lot of spies and soldiers had small textbooks, with insignificant words that they used for exchanging secure messages using this encryption method. This technique becames more important when in year 1984 Bennett and Brassard invent the QKD, thus associating OTP encryption with a quantum channel it was possible to create an unbreakable communication system [15].

2.4 LAYERED MODEL

In the next sessions we will introduce the Layered model of QKD. This definitions were written by Ueli Maurer, and we will give a short summery of the main postulates useful for our experiments. For a more detail descriptions, we remand the reader to consult the seminal paper [73].
The author propose in his work a practical scheme for generating a secret key in the case of realistic noisy channel also in the presence of an eavesdropper. It proves that this kind of analysis is completely in accord with the information-theoretic approach. The model, reported in Figure 2.3 could be divided in six steps:

- two parties, Alice and Bob aim to create a secret shared key
- these keys could be represented as random variables S_A and S_B, so that $S_A = S_B = S$
- in this scenario Eve has negligible information
- Alice transmits a random sequence X
- a part of information is collected by Bob Y, however also Eve eavesdrops the channel and obtained the sequence Z
- X and Y are called raw keys and they are obtained without no post-processing

In the case where the information extracted by Eve is bigger than the information between Alice and Bob, from a mathematical point of view it is possible to write:

$$\mathbb{I}(X;Z) > \mathbb{I}(X;Y) \tag{2.1}$$

where $\mathbb{I}(X;Z)$ represents the mutual information between Alice and Eve, and $\mathbb{I}(X;Y)$ between Alice and Bob.
However, also in this particular scenario, it is show by [73] that is possible to extract secret key thanks to post-processing action. In this particular case the following conditions must be satisfied:

4 The goodness of the random bits can be identified with some particular criteria. If the generated numbers are not completely random, the security of the process could be compromised.

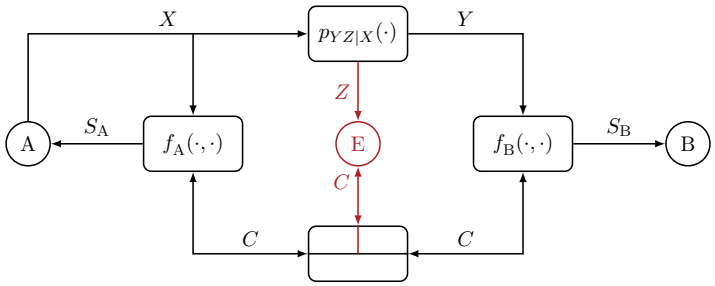


Figure 2.3: Information-theoretic secret key agreement system model.

$$\text{(correctness)} \qquad P[S_A \neq S_B] < \varepsilon_{\text{cor}} \tag{2.2}$$

$$\text{(secrecy)} \qquad \mathbb{I}[S_A, S_B : Z, C] < \varepsilon_{\text{sec}} \tag{2.3}$$

where ε_{cor} and ε_{sec} are usually very small (e.g. $10^{-9}, 10^{-10}$). Then Alice and Bob communicate using a public authenticated channel in order to exchange information about the raw keys. In this hypothesis Eve has a completely access to this channel but she cannot modified the message or substitutes Alice or Bob.

Once that Alice and Bob have created and distilled the keys, they start with post-processing function. From Alice side she applies a $f_A(\cdot)$ functions, while from Bob side he executes $f_B(\cdot)$ in order to extract the secret key pair (S_A, S_B). To fix the base steps of a QKD system let's take an overview of the main actions, see Figure 2.4.

- physical transmission over an insecure channel
- public discussion to obtain sifted keys: X_S at Alice's side and Y_S at Bob's side (advantage distillation $\mathbb{I}(X_S, Y_S) > \mathbb{I}(X_S; Z, C')$)
- Alice and Bob apply post-selection functions:$(f'_A(\cdot,\cdot), f'_B(\cdot,\cdot))$
- information reconciliation to correct the errors, denoted by the functions: $(f''_A(\cdot,\cdot), f''_B(\cdot,\cdot))$
- reconciled sequences pair, (X_R, Y_R) guarantees the inequality $P[X_R \neq Y_R] < \varepsilon_{cor}$
- privacy amplification step with the aim to decrease the information of Eve about the key (S_A, S_B)
- privacy amplification is performed using $(f'''_A(\cdot,\cdot), f'''_B(\cdot,\cdot))$ functions
- at the end of this process Alice and Bob shared the same identical secure key $S = S_A = S_B$

An intuitive plot, showing how the crucial quantities involved in the different phases of the described secret key agreement scheme change, is shown in Figure 2.4.

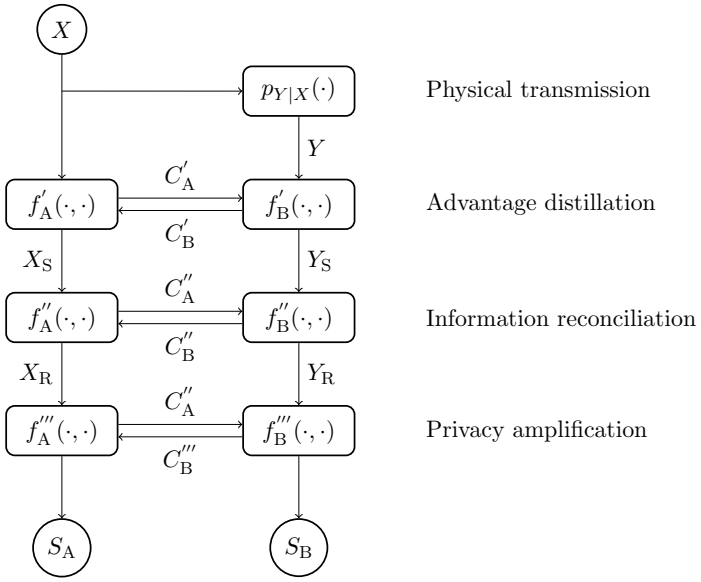


Figure 2.4: Information-theoretic secret key agreement procedure.

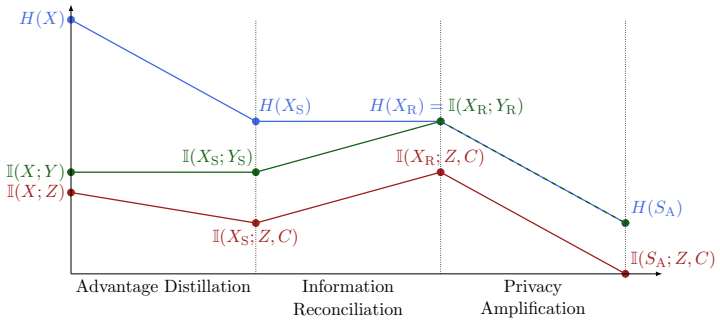


Figure 2.5: Evolution of information-theoretic measures involved in a secret key agreement protocol.

2.5 SECURITY OF QKD

In a theoretical scenario where the symbols N (numbers of sifted bits) stretch asymptotically to infinite, the secret key rate follows the expression: r =

$$\lim_{N\to\infty} l/n$$

From the other side in a realistic case, another important parameter must also be taken into account: the raw-key rate (R): the number of raw bits generated per unit time.
This number in part depends form the protocol, but above all it strictly correlated to the real devices are you adopting and to the environmental conditions. It is possible to define the secret key rate as

$$K = R \cdot r \tag{2.4}$$

For a detailed of this quantity see [92] section III. Another analysis will be take into account when the dimension of the key N is finite. In particular a reduction of the final secret key rate is expected principally for two reasons:

the parameter estimation is less precise due to the fixed bits, and above all because some hypothesis are true only in the case of asymptotic limit. In the next section we will discuss more precisely the finite key analysis, showing our results in term of the final key rate.

2.5.1 *Unconditional security and its conditions*

The main difference between CC and QCy arises in the fact that theoretically using QKD it is possible to achieve an unconditionally secure transmission. In technical term it means that security can be proved without imposing restriction on the computational resources by an eavesdropper. As reported and explain in Chapter 1 QM achieve a perfect check of the system and the possibility to detect the presence of an eavesdropper through the intrinsic laws of QP.

However this axiom must be made quantitative; in other words we must define before the key agreement how much information Eve can extract. From a mathematical point of view the observed perturbation, made by Eve allows the computation of a bound. In this perspective security QKD is guarantee only under some conditons:

- Eve cannot be inside Alice's or Bob's apparatus
- the Quantum random number generator (QRNG) must be trusted
- the classical channel use for PE must be authenticated
- the power of Eve il limited to the physics laws

If one of these requirements will not be satisfied the security of the system could be compromised [92].

2.5.2 *The concept of security*

We used the definition of security made by *Scarani et al* in [92]. One of the easiest way to define the security of a system is to measure the difference between a perfect key and the generated key. We can assume that the quantity ε is the unit of measure of the secrecy of the key.
A key is defined as "*ε-secure*" when the created key and the perfect one differs from a ε quantity. One important characteristic of a criteria definition is the possibility to add more requirements without any contradiction or loss of value. In particular the definition of security reported by Scarani in [92] satisfy the composability criteria. If a key with security ε is used on a ε' task, the composability property assume that the whole procedure is at least $\varepsilon + \varepsilon'$ secure.
An example of a composable definition of security is the following equation:

$$\frac{1}{2}\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \oplus \rho_E\|_1 \leqslant \varepsilon \tag{2.5}$$

where $\rho_{\mathcal{K}E}$ represents the state with correlation between the final key and Eve and τ_k the completely mixed state on the possible final keys $\mathcal{K}$. The ρ_E variable can be assumed as whatever state of Eve. The maximum failure probability in this security criteria is defined by the variable ε. Once defined the security of our key, it is desirable derive a proof of that definition. In our case several techniques have been used:

- a first proofs, made by Mayers and base on the uncertainty principle [75]. Recently reviewed by Koashi [62]
- some security proofs were based on the generalized techniques, made by Shor and Preskill ([99]), on the correspondence between entanglement and classical post processing
- the most recent techniques use information-theoretical notions [85, 11].

The core of the proof, relies on a strict relationship between the security requirements and the dimension of the secret key. In other words, it results very simple to write a relationship of the form:

$$P(\|\rho_{KE} - \tau_k \oplus \rho_E\|_1 > 2\varepsilon) \lesssim e^{l - F(\rho_{KE}, \varepsilon)} \tag{2.6}$$

The security requirements will be satisfied in all the cases which $l \gtrsim F(\rho_{KE}, \varepsilon)$.

2.5.3 *Attack model*

The objective of QKD is providing an unconditionally secure cryptographic keys. In particular, depending on the assumption made toward Eve, different bounds on the secrecy level can be derived. According to the traditional classification, three attacks categories, with increasing generality, can be distinguished:

INDIVIDUAL ATTACKS Individual attacks (IAs) are one of the most constrained attacks on a QKD system; they assume that:

IA.1 the eavesdropper uses always the same attack strategy and considers each qubit independently from the others

IA.2 all the quantum measurements made by the eavesdropped on the qubits are performed before the classical post-processing [71, 89]

One of the most famous individual attacks are the Intercept-and-resend (IRs) attacks. In a IRs Eve independently intercepts, measures and then retransmits qubits. This is one of the simplest attacks, in fact Eve has to measures each qubit, with a black machine like Bob receiver and depending to the obtained results, she sends the new qubit to the real Bob.

COLLECTIVE ATTACKS Collective attacks (CAs) are a generalization of IAs, and characterized by the following properties:

CA.1 the eavesdropper uses always the same attack strategy and considers each qubit independently from the others (as (IA.1))

CA.2 this time Eve can uses devices as quantum memories to store the qubits and postpone the measurement in a later convenient time [16]

GENERAL ATTACKS The family of General attacks (GAs) fall down the assumption made in the IAs and in CAs that is the eavesdropper considers each qubit independently from the others (IA.1) and (CA.1). In fact in literature this kind of attack is known by the name of joint or coherent attack, because it does not impose any restriction on the attack strategy, except those defined in security definition 2.5.1.

2.5.4 *QKD protocols*

In this section, we report some remarkable examples of QKD protocols, useful for the complete understanding of the work and above all because some of them are implemented in the experiments presented in this work. The most famous and one the most implemented protocol was the BB84 [15], but we will introduce also the simplest version B92 [14] and a revision of the BB84 useful in the finite key regime [104]. All these protocols use a polarized encoding technique, thus the polarization of the sent qubits determines which bits we have sent. There exist other schemes, such as the six-states [20], the SARG [90] protocols or Time-Bin protocols [72] which exploit other degrees of freedom like phase delay. For a complete overview of QKD protocols both Continuous Variable (CV) and Discrete Variable (DV), the interested reader can refer to [43] and [92].

BB84 PROTOCOL The Bennett-Brassard 1984 protocol [15] was the first QKD scheme that has been proposed and realized. In this scheme information is encoded into single polarized photons, in particular there exist two polarization bases, hereby denoted by **X** and **Z**, each one define by a pair of orthogonal polarization states. As it is possible to see from Table 2.1 **X**-basis is called horizontal-vertical basis, linked to the quantum state $|\leftrightarrow\rangle$ or $|\updownarrow\rangle$ states. From the other side **Z**-basis is called diagonal basis and it is specified by $|\nwarrow\!\!\searrow\rangle$ or $|\swarrow\!\!\nearrow\rangle$ states.

Table 2.1: Example of bit-qubit mapping of BB84 protocol

Bit	$\mathbb{X}$-Basis	$\mathbb{Z}$ -Basis
0	$\leftrightarrow$	$\swarrow\!\!\nearrow$
1	$\updownarrow$	$\nwarrow\!\!\searrow$

The protocol works as follow:

- Alice choose randomly, using a QRNG[5] which bit of the two basis send to Bob $\{x_m\}$ i.i.d in $\{0,1\}$
- Alice prepares the state to be sent throughout the quantum channel $\{A_m\}$, i.i.d. in$\{\mathbb{X},\mathbb{Z}\}$
- Alice send a sequence of polarized photons (qubits) to Bob, for each random bit x_i Alice send $|\psi_i\rangle$
- Bob for each qubits choose randomly in which basis measure the state; every measure corresponds to a bit, $\{B_m\}$, i.i.d. in$\{\mathbb{X},\mathbb{Z}\}$
- after the measure, Alice and Bob hold different key, named *raw key*
- using classical channel Alice and Bob compare basis used in the transmission and detection. Different basis have to be discarded, while bits obtained with same basis form the key
- at the end of this process Alice and Bob share the same key

5 Quantum Random Number generator

$$Y_S = \{y_i : A_i = B_i\} \tag{2.7}$$

When the two basis are identical, it is known that there are a strong correlation between sent and receive qubits; from the other point of view when the two qubits results different and obviously discarder, the result is uncorrelated and it could be due to an Eavesdropper presence or a very noisy channel. The procedure describe above take into account a PM-scheme distribution protocol, where Alice before sending quantm bits to Bob have to prepare photons in the correct state. Moreover the states that Alice sends to Bob are decided a priori. From the other side there exist EB-scheme where the protocols use entanglement properties to create quantum states. In the following paragraphs we will describe in detail also EB-scheme.

Table 2.2: Example of BB84 protocol

Random bits Alice x_i	0	0	1	0	0		1	1	0
Random basis Alice A_m	✣	✣	⤫	⤫	⤫	✣	✣	⤫	✣
Sent photons $\|\psi_{x_m}\rangle$	↔	↔	↘	↗	↗	↕	↕	↘	↔
Random basis Bob B_m	⤫	✣	✣	✣	⤫	✣	⤫	⤫	✣
Raw key y_m	1	0	1	0	0	1	1	1	0
Basis publication	⤫	✣	✣	✣	⤫	✣	⤫	⤫	✣
Basis comparison		OK			OK	OK		OK	OK
Sifted key $y_{S,m}$		0			0	1		1	0

Error estimation Bob or Alice, once they have exchanged a sequence of qubits (or viceversa), sends to the other a random subset C of sifted key bits for estimating the bit error rate Q in the quantum channel (Quantum bit error rate (QBER)). More specifically, the estimated qber $\hat{Q}$ is defined as:

$$\hat{Q} = \frac{\sum_{c \in C} x_{S,c} \oplus y_{S,c}}{|C|} \tag{2.8}$$

The estimated QBER is a crucial parameter for the classical post-processing phase, that is, for information reconciliation and for privacy amplification, and affects the final secret key rate.

In the ideal case that the quantum channel is ideal and no adversary is attacking the system, the BB84 protocol directly produces a secret key. On the contrary, if an attacker is present, she obviously interact with the quantum channel before she knows the chosen state-preparation and state-measurement bases. Hence, the sifting procedure applied to QKD, enables the legitimate parties to get an advantageous position with respect to the eavesdropper. This operation however reduces the final rate, since, on average, only $1/2$ of the times Alice's and Bob's basis choice will match. The efficiency of the BB84 protocol, in the absence of losses, is $\eta_{BB84} = \frac{1}{2}$. The final key rate in the assumption of asymptotic key rate results: (derived in

$$r_{BB84} = R[1 - 2h_2(Q)] \tag{2.9}$$

where $h_2(p)$ represents the binary entropy function[6] and R represents the sifted key rate. Let us now describe what happens if an eavesdropper independently attacks each sent qubit with probability p, by first measuring and resending it to Bob; this attack is known as *intercept-and-resend* attack (IA.2). In this example Eve has to choose which bases use for the quantum projection, in order to extract the information encoded in the photon. It was demonstrate by Shor in [99] that the best way for Eve to get information is to mimic a legitimate receiver, thus to to choose uniformly at random the measurement basis, $\mathbb{E}$. In this situation, Eve guess the state preparation basis with probability $1/2$, and she takes the wrong basis with probability $1/2$. When she picks the correct basis, she gets the right result, whereas when she picks the wrong basis, she gets a uniformly random result, thanks to the complete non-orthogonality of the states in the $\mathbb{X}$ and in the $\mathbb{Z}$ bases. Then she have to retransmit the qubit in order to confuse Bob, by preparing it in the same basis she used for the measurement. In a realistic hypothesis of quasi-fixed QBER Q and of and ideal setup (no errors and losses introduce by Eve), it is possible to derive the bit error rate in the case of IRs:

$$Q_{IR}(q) = (1-q)Q + q\left(\frac{Q}{2} + \frac{1}{4}\right) = \left(1 - \frac{q}{2}\right)Q + \frac{q}{4} \tag{2.10}$$

whereas losses will not be affected. Therefore, the QBER measured at Bob linearly increases with the attack rate q, up to its maximum value

$$Q_{IR}(1) = \frac{Q}{2} + \frac{1}{4} \tag{2.11}$$

Hence, it results very clear that Eve has to find a trade-off for getting as much information as possible without been revealed. At the same time, Alice and Bob have to estimate as precisely as possible the attack rate q, in order to compensate for the eavesdropped information during the privacy amplification phase.

EFFICIENT BB84 PROTOCOL As seen in section 2.5.4, the BB84 protocol has a raw-sifted efficiency $\eta_{\text{BB84}} = 1/2$ that is, in the absence of losses, only half of the raw bits sent by Alice yields a sifted sequence at Bob. Looking toward an higher efficiency of this protocol , a variant of the BB84 protocol, that we refer to as *efficient* BB84 (e-BB84), has been proposed in [104]. In standard BB84, both polarization bases are used for raw key transmission and for attack estimation, and their choice is unbiased. In e-BB84, instead, one basis (say $\mathbb{X}$) carries the raw key sequence, whereas the other basis (say $\mathbb{Z}$) is used for eavesdropping detection. Also, the choice of the two bases at Alice and Bob is biased: intuitively, the basis carrying the raw key is chosen with higher probability, while the detection basis is chosen less frequently. Let us describe it in more detail. The e-BB84 protocol is characterized by the sifted key length n and by the number of bits used for parameter estimation k; both parameters can be chosen according to the required secret key length and channel conditions as described below. Also, the choice of n and k yields the probability of picking each of the two bases, namely,

$$p_{\mathbb{X}} = \frac{1}{1 + \sqrt{k/n}}\,, \; p_{\mathbb{Z}} = 1 - p_{\mathbb{X}} \tag{2.12}$$

The protocol consists of the following subsequent steps:

6 $h_2(x)\; h_2(p) = p\log(p) - (1-p)\log(1-p)$

- quantum transmission
  1. Alice randomly generates a sequence of bits, $\{x_m\}_{m\in[1,M]}$ i.i.d. in $\{0,1\}$
  2. a biased sequence of state-preparation bases $\{A_m\}_{m\in[1,M]}$ in $\mathbb{X},\mathbb{Z}$, chosen with probabilities $p_{\mathbb{X}}$ and $p_{\mathbb{Z}}$, respectively where M is such that the condition in the sifting phase is met.
  3. for each random bit x_i, Alice prepares a qubit $|\psi_{x_i}\rangle$, in the form of a single photon polarized in the A_i basis, and sends it through the quantum channel.
  4. Bob randomly generates a biased sequence of state-measurement bases, $\{B_m\}$ in $\{p_{\mathbb{X}},\mathbb{Z}\ \}$, chosen with probabilities $p_{\mathbb{X}}$ and $p_{\mathbb{Z}}$, respectively
  5. Bob measures each received qubit, $|\psi_{x_i}\rangle$, in the B_i basis and gets the measured bit y_i.

- Sifting (advantage distillation) Alice and Bob exchange the state preparation and the state-measurement bases through the public channel , $\{A_m\}$ and $\{B_m\}$, and discard the bits for which their choice differs. Also, they distinguish the bits measured in the $\mathbb{X}$ basis and the ones measured in the $\mathbb{Z}$ basis, thus defining the following subsets:

$$\mathcal{X} = \{i\ :\ A_i = \mathbb{X}, B_i = \mathbb{X}\} \tag{2.13}$$
$$\mathcal{Z} = \{i\ :\ A_i = \mathbb{Z}, B_i = \mathbb{Z}\} \tag{2.14}$$

  The quantum communication is repeated as long as either $|\mathcal{X}| < n$ or$|\mathcal{Z}| < k$. Then, Alice and Bob pick the same n and k indexes, randomly chosen, in $\mathcal{X}$ and in $\mathcal{Z}$, respectively, thus defining the subsets $\mathcal{X}_n$ and in $\mathcal{Z}_k$. Finally the following sifted sequences are defined:

$$\mathbf{X}_{\mathbb{X}} = \{X_{\mathbb{X},i}\} = \{x_i : i \in \mathcal{X}_n\},\ \text{(sifted key at A)} \tag{2.15}$$
$$\mathbf{Y}_{\mathbb{Y}} = \{X_{\mathbb{X},i}\} = \{y_i : i \in \mathcal{X}_n\},\ \text{(sifted key at B)} \tag{2.16}$$
$$\mathbf{X}_{\mathbb{X}} = \{X_{\mathbb{X},i}\} = \{x_i : i \in \mathcal{Z}_k\},\ \text{(estimation bit at A)} \tag{2.17}$$
$$\mathbf{Y}_{\mathbb{X}} = \{Y_{\mathbb{X},i}\} = \{y_i : i \in \mathcal{Z}_k\},\ \text{(estimation bit at B)} \tag{2.18}$$

- Error estimation Bob sends to Alice the whole sequence of estimation bits $\{\mathbf{Y}_{\mathbb{Z},m}\}$ in order to compute the bit error rate $Q_{\mathbb{Z}}$ on the eavesdropping detection basis, yielding:

$$\hat{Q} = \frac{\sum_{c\in\mathcal{Z}} X_{\mathbb{Z},c} \oplus Y_{\mathbb{Z},c}}{|\mathcal{Z}|} \tag{2.19}$$

  Again, this QBER is a crucial design parameter for the classical post-processing phase, and, in particular, for the privacy amplification phase. On the other hand, the QBER on the $\mathbb{X}$-basis, $Q_{\mathbb{X}}$, is the main design parameter for the information reconciliation phase, and should be known to the legitimate parties. As it can easily be seen, the efficiency of the protocol e-BB84 results: $\eta_{e-BB84} = p_{\mathbb{X}}^2$ and is therefore higher than the efficiency of BB84 (see (2.5.4)) as soon as $p_{\mathbb{X}} > 1/2$. Also, the asymptotic (secret to sifted) key rate for the efficient BB84 directly follows from the one of BB84, that is:

$$r_{e-BB84} = R[1 - h_2(Q_{\mathbb{X}}) - h_2(Q_{\mathbb{Z}})] \tag{2.20}$$

B92 PROTOCOL The Bennett 1992 protocol [15] is a DV PM protocol, where information is encoded in two non-orthogonal quantum states. In particular, a state-preparation basis, $\mathbb{P}$, and a state measurement basis, $\mathbb{M}$, are defined, so that the following map is defined:

Table 2.3: Example of bit-qubit mapping of B92 protocol

Bit	$\mathbb{P}$-Basis	$\mathbb{M}$ -Basis
0	$\updownarrow$	$\nwarrow\!\!\searrow$
1	$\nearrow\!\!\swarrow$	$\leftrightarrow$

The protocol works as follow:

- Alice generates randomly, using a QRNG[7] a sequence of bits $\{x_m\}$ i.i.d in $\{0,1\}$
- For each random bit $\{x_i\}$, Alice prepares a qubit $|\psi_{x_i}\rangle$, in the form of a single photon polarized in the corresponding $\mathbb{P}$-basis state, and sends it through the quantum channel. The choice is now deterministic, whereas in the BB84 protocol it was random.
- Bob randomly generates a sequence of $\mathbb{M}$-basis states, $\{B_m\}$, i.i.d. in $\{\mathbb{P}, \mathbb{M}\}$.
- Bob projects each received qubit, $|\psi_{x_i}\rangle$, onto the B_i polarization, and gets the measured bit yi. If $|\psi_{y_i}\rangle$ is orthogonal to B_i, then no detector clicks; otherwise, the right detector clicks with probability $1/2$ and does not click with probability $1/2$.
- Bob sends to Alice, through the public channel, the indexes D of the the qubits that produced a click at the receiver
- at the end of this process Alice and Bob share the same key

$$X_S = \{x_i : i \in D\} \tag{2.21}$$
$$Y_S = \{y_i : i \in D\} \tag{2.22}$$

Table 2.4: Example of B92 protocol

Random bits Alice x_m	0	0	1	0	0	1	1	1	0
Sent photons $\|\psi_{x_m}\rangle$	$\updownarrow$	$\updownarrow$	$\nearrow\!\!\swarrow$	$\updownarrow$	$\updownarrow$	$\nearrow\!\!\swarrow$	$\nearrow\!\!\swarrow$	$\nearrow\!\!\swarrow$	$\updownarrow$
Random basis Bob B_m	$\leftrightarrow$	$\nwarrow\!\!\searrow$	$\nwarrow\!\!\searrow$	$\nwarrow\!\!\searrow$	$\leftrightarrow$	$\leftrightarrow$	$\nwarrow\!\!\searrow$	$\nwarrow\!\!\searrow$	$\leftrightarrow$
Sifted key y_m		0		0		1			

The efficiency of the B92 protocol (in the absence of losses) immediately follows from the described scheme

$$\eta_{B92} = \frac{1}{2}\left(P[x_i = 0, B_i = |\nwarrow\!\!\searrow\rangle] + P[x_i = 1, B_i = |\nearrow\!\!\swarrow\rangle]\right) = \frac{1}{4} \tag{2.23}$$

7 Quantum Random Number generator

Hence, results that B92 protocol has a lower efficiency as compared with BB84, and a fortiori, with e-BB84. On the other hand, B92 relies on a simplified setup, which requires just two non orthogonal states at both the transmitter and the receiver side, that is, half of the complexity of BB84.
Unfortunately, the described setup also comes with a significant security threat. Due to the deterministic coding of qubits, in fact, an eavesdropper who plays the man-in-the-middle can mimic Bob's receiver, and re-transmit the qubits which produced a click. This attack, known as unambiguous state discrimination (USD) [35], introduces significant losses, yielding an overall efficiency of $(1/4)^2$ if each qubit is attacked, but does not affect the measured QBER at the receiver.

In the original paper by Bennett [14], the use of a strong reference was suggested to avoid this problem, but this enhanced protocol becomes insecure as soon as the channel losses get higher than a given threshold which depends on the non-orthogonality of the signal states [36]. A further solution for making the B92 protocol more robust against losses and noise is the one presented in [69], where the decoy-states principle is extended to B92 by using additional uninformative states. Finally, the asymptotic (secret to sifted) key rate for the B92 protocol is:

$$r_{B92} = R[1 - \text{leak}_{EC} - I_E] \tag{2.24}$$

where $\text{leak}_{EC}(Q) \geqslant h_2(Q)$ and $I_E = \min(I_{AE}, I_{BE})$.

2.5.5 *Single photon remarks*

All the protocols presented above assume one strong hypothesis, thus that each sent qubit trough the quantum channel is composed by a single photon. On this way Eve cannot measures the incoming photon without perturbing it, and giving the possibility to Bob to understand that the measure is distorted. In the case of multiple photons associated to a single qubit, an attack like Photon Number Splitting (PNS) works in a very efficient way, in fact Eve could measure one of the qubit photons without perturbing the measured made by Bob [91]. In a experimental scenario, where usually the sources for Alice are faint laser, this assumption is not often verified. It is possible to study the static of the emitted photon in order to better understand an prevent this kind of attacks. The probability of emission follows a poissonian statics, while the probability of multi-photon emissions can be calculated as:

$$P[n_{ph} > 1 | n_{ph} > 0] = \frac{1 - e^{-\mu}(1 + \mu)}{1 - e^{-\mu}} \tag{2.25}$$

Usually to prevent this problem, in the choose about the transmission rate of Alice, it is decided that a lower emission rate could be allow in order to decrease the probability of multi-photon emission. In other word we must choose the parameter μ (mean photon number per pulse) lower than 1. Usually in a realistic QKD scenario typical values are $0.1 \leqslant \mu \leqslant 0.4$.

Due to the low performance of the final key rate (in the case of low μ), scientist propose solutions to overcome this limitation, the best known protocol (with the same security of the others) are reported in [56, 67, 90] and propose a decoy state method.

The decoy state method works as follow: in addition to the encoded qubits, Alice sometimes sends pulses with different level of μ which carry no information about the key, but they are only useful for checking Eve's presence. Eve could not know the intensity of the qubits, and she can't recognize if such qubit is for key creation or for security check, in this case she measures the qubit and for Alice and Bob result very simple to detect her presence.

Decoy state method was demonstrated in several works, both considering optical fiber link [88] both in free-space scenario [109]. Also in the case of finite key analysis it was proved that decoy state method works [46].
In all the experiment presented in this thesis, we never include decoy states method both, but it would be better if all the analysis was made in the also against PNS attack.

2.6 FINITE KEY ANALYSIS

In the last years, great efforts from the quantum communication community were directed to this subject, due to its relevance for a number of application scenarios [4, 92, 24]. We would like to underline that all previous published experimental work on finite-size key security were based on a far more inefficient bound as compared with the one obtained in Tomamichel [104]. In this work, we study the security and the generation rate of a protocol for key exchange in the finite-key regime and in presence of noise, whose value is experimentally varied up to the top limit [9]. The security is assessed with reference to a recently introduced theoretical result [104], for which "almost tight bounds on the minimum value" of exchanged qubits "required to achieve a given level of security" were obtained [104], as well as for a realistic bound described below. In particular, by leveraging the optimal design of the prepare-and-measure scheme complying with the above mentioned tight theoretical bounds, we evaluate how the secret key rate scales in different channel conditions, depending on the protocol parameters. We consider two possible attack models, referring to two different levels of secrecy: *pragmatic secrecy*, which ensures resiliency against individual attacks, and *general secrecy*, which ensures resiliency against the most general quantum attacks.

2.6.1 *Protocol for quantum key distribution.*

We will adopt here the protocol described in [104], a derivation of the well known BB84 protocol [15] and reported in 2.5.4.
According to this protocol, one of the two bases is used to encode the raw key bits while the other basis is used to test the channel for the presence of the eavesdropper. Moreover, the two bases are selected by Alice and Bob in the preparation of the qubits and in their measure, respectively, with non equal probabilities, unlike the standard BB84.
In order to obtain the final sifted keys, Alice and Bob keep the same n bits, randomly chosen, from the $\mathbb{X}$ bits to form the sifted key strings $\mathbf{X} = \{x_i\}$ and $\mathbf{X}' = \{x_i'\}$. Similarly they choose k random bits from the $\mathbb{Z}$ bits to obtain the parameter estimation strings $\mathbf{Z} = \{z_i\}$ and $\mathbf{Z}' = \{z_i'\}$. Differently from [104], we defined the sifted key as $\mathbf{X}$ and not as the union set of $\mathbf{X}$ and $\mathbf{Z}$. The $\mathbb{X}$ bits will be used to build the final secret key and the expected number of errors between $\mathbf{X}$ and $\mathbf{X}'$ is the crucial parameter in the design of the information reconciliation protocol. The $\mathbb{Z}$ bits will be used to test

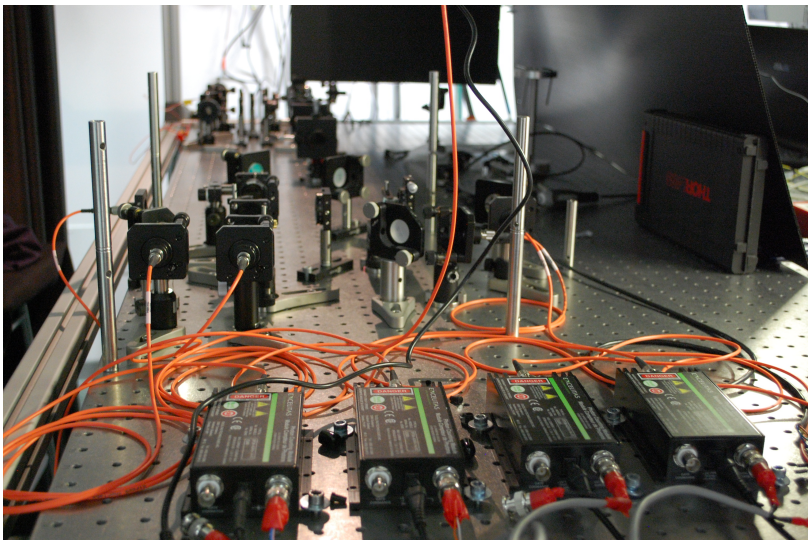


Figure 2.6: The experiment was realized in the Luxor Laboratory of CNR IFN where Alice and Bob was mounted in a stabilized optical table. It is possible to see the four SPAD detectors used for the state measurement and the optical fibers (orange cables) used both for collecting photons both for introduce different noise light into the channel.

the presence of the eavesdropper and the number of errors between $\mathbf{Z}$ and $\mathbf{Z}'$ is used for dimensioning the privacy amplification procedure. Note that the probabilities $p_{\mathbb{X}}$ and $p_{\mathbb{Z}}$ are chosen to satisfy $p_{\mathbb{Z}}^2/p_{\mathbb{X}}^2 = k/n$ in order to minimize the number of exchanged photons before the quantum communication is stopped. After the quantum transmission and the sifting of the raw data, four subsequent tasks take place: parameters estimation, information reconciliation, error verification and privacy amplification. The first task, parameters estimation, is required to measure the QBER on the $\mathbb{Z}$ basis, $Q_{\mathbb{Z}}$. Furthermore, we assume that the quantum channel is stable, i.e., that QBER on the $\mathbb{X}$-basis, $Q_{\mathbb{X}}$, is constant in time (note that, in general, $Q_{\mathbb{X}} \neq Q_{\mathbb{Z}}$). If $Q_{\mathbb{X}}$ increases (for instance because an attacker is tampering with the channel), then the information reconciliation will fail. The failure will be detected during the error verification phase, and the protocol will abort. On the other hand, the empirical QBER in the $\mathbb{Z}$ basis is dynamically computed at each protocol run as $\hat{Q}_{\mathbb{Z}} = (\sum_{i=1}^{k} z_i \oplus z_i')/k$, to check for the presence of an eavesdropper. The protocol aborts if $\hat{Q}_{\mathbb{Z}} > Q_{\text{tol}}^{\mathbb{Z}}$, where $Q_{\text{tol}}^{\mathbb{Z}}$ is a given channel error tolerance on the $\mathbb{Z}$ basis which has been determined a priori based on the expected behavior of the quantum channel and the required level of security.

Information reconciliation allows Bob to compute an estimate $\hat{\mathbf{X}}$ of $\mathbf{X}$ by revealing L_{EC} bits (L_{EC} represents the classical information leakage). We define P_{fail} as the upper bound to the probability of a reconciliation failure and ε_{cor} as the upper bound to the probability that $\hat{\mathbf{X}}$ differs from $\mathbf{X}$. We fixed a threshold $Q_{\text{max}}^{\mathbb{X}}$ such that the empirical QBER $\hat{Q}_{\mathbb{X}}$ in the sifted key is higher than $Q_{\text{max}}^{\mathbb{X}}$ with probability less than $P_{\text{fail}}/2$.

2.6.2 *General and pragmatic secrecy*

In this work we consider two possible attacker models, which in turn entail two different notions of secrecy, which we call *general* and *pragmatic*, respectively. General secrecy, as defined in [104], requires that the final shared keys are secret with respect to the most GAs, and it is based on the secrecy criterion provided in [63]. We say that the distilled key $\mathbf{S}$ is ε_{sec}-GS (general secret) if for any attack strategy

$$\min_{\sigma_E} \frac{1}{2}\|\rho_{SE} - \omega_S \oplus \sigma_E\|_1 \leq \frac{\varepsilon_{\text{sec}}}{(1 - p_{\text{abort}})}, \tag{2.26}$$

being $\|\rho\|_1 = \text{Tr}\sqrt{\rho\rho^\dagger}$, p_{abort} the probability that the protocol aborts, ρ_{SE} the quantum state which describes the correlation between Alice's classical key $\mathbf{S}$ and the eavesdropper, ω_S the fully mixed state on $\mathbf{S}$, and σ_E a generic quantum state on the eavesdropper's Hilbert space. Then, if the bases $\mathbb{X}$ and $\mathbb{Z}$ are chosen as described above and assuming that Alice uses an ideal single photon source, the authors of [104] show that an ε_{sec}-GS key can be extracted out of the reconciled key, with length:

$$\ell \leq n(1 - \widetilde{h}_2(Q_{\text{tol}}^{\mathbb{Z}} + \mu)) - L_{\text{EC}} - \log_2 \frac{2P_{\text{fail}}}{\varepsilon_{\text{sec}}^2 \varepsilon_{\text{cor}}} \tag{2.27}$$

where $\mu = \sqrt{\frac{n+k}{nk}\frac{k+1}{k}\ln\frac{2}{\varepsilon_{\text{sec}}}}$, $h_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, $\widetilde{h}_2(x) = h_2(x)$ for $0 \leq x \leq 0.5$ and $\widetilde{h}_2(x) = 1$ for $x > 0.5$.

On the other hand, pragmatic secrecy [25] ensures that the final key is secret with respect to IRs attacks [55], i.e., a specific class of selective individual attacks, which, however, represents the most realistic and feasible attack strategy based on the experimental technology nowadays available: collective or more general attack models (see [92]), in fact, require ancillary qubits and quantum memories in order to be deployed. While in a long-term perspective (more than 50 years) general security is the goal, in the near future ($5 - 10$ years), we know that an ideal IRs attack is the best option that an eavesdropper can choose because the quantum memory needed for a general or coherent attack is not yet available.
In the Experimental Results subsection, we will show that there are situations in which no key can be extracted if general security is required, while a pragmatically secure secret key can be obtained. In these cases, requiring general security, a protection far above actual possibilities of an eavesdropper, prevents key generation. Also, we would like to stress that pragmatic secrecy, unlike computational secrecy, offers forward security: if a key is produced today with pragmatic secrecy (without quantum memory available for Eve), the key or a message encrypted with it will be secure for any future use.

As a criterion for pragmatic secrecy, we use a bound on the classical equivocation at the eavesdropper, namely we say that the distilled key $\mathbf{S}$ is δ_{sec}-PS (pragmatic secret) if, for any IRs attack strategy and in the case that the protocol is not aborting,

$$H(\mathbf{U}_S) - H(\mathbf{S}|V) \leq \frac{\delta_{\text{sec}}}{1 - p_{\text{abort}}} \tag{2.28}$$

being $\mathbf{U_S}$ the uniform key with the same length as $\mathbf{S}$, V the classical random variable which summarizes all the information available to the eavesdropper and $H(\mathbf{S}|V)$ the equivocation (conditional entropy) of $\mathbf{S}$ given V. Note that eq. (2.28) implies the uniformity and the security conditions

$$\begin{cases} H(\mathbf{S}) \geq H(\mathbf{U_S}) - \frac{\delta_{\text{sec}}}{1-p_{\text{abort}}} & \text{(uniformity)} \\ I_{\text{acc}}(\mathbf{S};E) \leq \frac{\delta_{\text{sec}}}{1-p_{\text{abort}}} & \text{(security)} \end{cases} \tag{2.29}$$

where the accessible information I_{acc} is the maximum mutual information $I(\mathbf{S};V) = H(\mathbf{S}) - H(\mathbf{S}|V)$ that can be extracted from the quantum system E [63]. Moreover, choosing $\delta_{\text{sec}} = \frac{2}{\ln 2}\varepsilon_{\text{sec}}^2$ in (2.28) implies condition (2.26) for non-coherent attacks (see Methods section 2.7). It should be noted that, as for incoherent individual attacks, eq. (2.28) guarantees composable security, as the eavesdropper, without a quantum memory, cannot exploit the "locking property" of the accessible information (see [63]). The pragmatic security of the distilled key can be assessed through the following result, the proof of which is provided in the Methods section. The distilled key $\mathbf{S}$ is δ_{sec}-PS if

$$\exists\, a \in \mathbb{N} : \quad f(a,\ell) \leq \delta_{\text{sec}} \tag{2.30}$$

where

$$f(a,\ell) = \ell \max_q \left[I_q(a+1, n-a) I_{1-q/2}(k(1-Q_{\text{tol}}^{\mathbb{Z}}), kQ_{\text{tol}}^{\mathbb{Z}}+1) \right] + \frac{2^{-(n_{\text{EC}}-\ell-a)}}{\ln 2}, \tag{2.31}$$

with $n_{\text{EC}} = n - L_{\text{EC}} - \lceil \log_2(P_{\text{fail}}/\varepsilon_{\text{cor}}) \rceil$ and $I_x(a,b)$ denoting the regularized incomplete beta function

$$I_x(a,b) = \frac{B(x;a,b)}{B(1;a,b)}, \quad B(x;a,b) = \int_0^x t^{a-1}(1-t)^{b-1}\, dt. \tag{2.32}$$

Based on (2.30), we can therefore choose the optimal secret key length as

$$\ell = \max\left\{ b : \min_a f(a,b) \leq \delta_{\text{sec}} \right\} \tag{2.33}$$

Please note that, in order to allow a comparison with the tight bound (2.27), we have derived the secure key length in the hypothesis that Alice uses a single photon source.

Finally, given the probability ε_{rob} that the protocol aborts even if the eavesdropper is inactive [104], we can compute the final secret key rate for both general and pragmatic secrecy as

$$r(\ell, n, k, \varepsilon_{\text{rob}}) = (1-\varepsilon_{\text{rob}}) \frac{\ell}{M(n,k)} \tag{2.34}$$

where $M(n,k) = n + k + 2\sqrt{nk}$ is the expected number of qubits that have to be sent until n sifted key bits and k parameter estimation bits are collected.

2.6.3 *Experimental results*

We conducted experiments with different noisy channels yielding different values for the average QBER $Q_{\mathbb{X}}$ and $Q_{\mathbb{Z}}$, each of them realized with different encoding probabilities $(p_{\mathbb{Z}}, p_{\mathbb{X}})$. We varied the noise value in the channel by

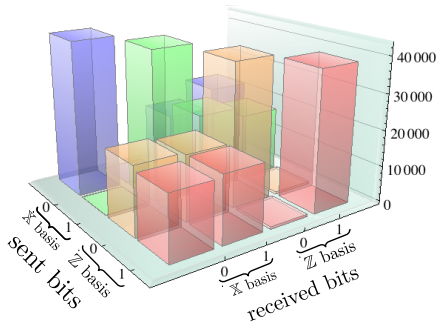


Figure 2.7: Experimental bits: Joint empirical distribution of sent and received bits, as obtained in one experiment with the best channel conditions (corresponding to $Q_{\mathbb{X}} = 0.33\%$ and $Q_{\mathbb{Z}} = 1.48\%$). The probabilities of sending and measuring in the $\mathbb{X}$ and $\mathbb{Z}$ basis were $p_{\mathbb{X}} = 0.51$ and $p_{\mathbb{Z}} = 0.49$, respectively.

coupling to the receiver an external unpolarized source of suitable intensity, that increased the background signal. It is worth noting that by this operation we are modelling the following depolarizing channel

$$\mathcal{C} : \rho \to (1 - P)\rho + \frac{P}{4} \sum_{j=0}^{3} \sigma_j \rho \sigma_j, \tag{2.35}$$

where σ_j are the Pauli matrices, being σ_0 the identity and P the parameter representing the probability that any detected photon is coming from the background.

In Figure 2.7 we show the joint empirical distribution of the transmitted and received bits on the $\mathbb{X}$ and $\mathbb{Z}$ bases obtained in one run with the best environmental conditions (i.e., with additional background), for the case $p_{\mathbb{Z}} = 49\%$ and $p_{\mathbb{X}} = 51\%$. As expected, in this case the QBER is very low: the main source of errors are imperfections in the waveplates used in the measurement, yielding $Q_{\mathbb{X}} = 0.33\%$ and $Q_{\mathbb{Z}} = 1.48\%$ on average. In Figure 2.8 we show the measured experimental key rates for each data set and for both general and pragmatic secrecy. First of all, let us recall that, in order to consistently compare the secrecy rates obtained with general and pragmatic secrecy, the security parameters ε_{sec} and δ_{sec} have to be chosen so that $\delta_{\text{sec}} = \frac{2}{\ln 2}\varepsilon_{\text{sec}}^2$. As a performance reference, we plot the asymptotic theoretical bound $r = 1 - h_2(Q_{\mathbb{X}}) - h_2(Q_{\mathbb{Z}})$, holding in the limit of infinite length keys (labelled as "asymptotic" in Figure 2.8) and the optimal theoretical bound for ε_{sec}-GS keys (labelled as "numerically optimized $p_{\mathbb{Z}}$" in Figure 2.8). The experimental key rates are obtained by the following procedure: for each data set the n-bit sifted key $\mathbf{X}$ and the k-bit parameter estimation string $\mathbf{Z}$ ($\mathbf{X}'$ and $\mathbf{Z}'$) at Alice's (Bob's) side are obtained by the experiment. The error correction is performed on $\mathbf{X}$ and $\mathbf{X}'$ by using the Winnow scheme; in particular, the Winnow parameters were chosen so that a maximum of 6 subsequent iterations is allowed with block sizes up to 256 bits. We then performed privacy amplification by compressing the error-free keys by multiplication with a random binary Toeplitz matrix. The amount of compression depends on ℓ, the secret key length, given by eq. (2.27) and (2.33) for general and pragmatic security, respectively. On the other hand, the optimal bound for ε_{sec}-GS keys is numerically derived by maximizing the secret key

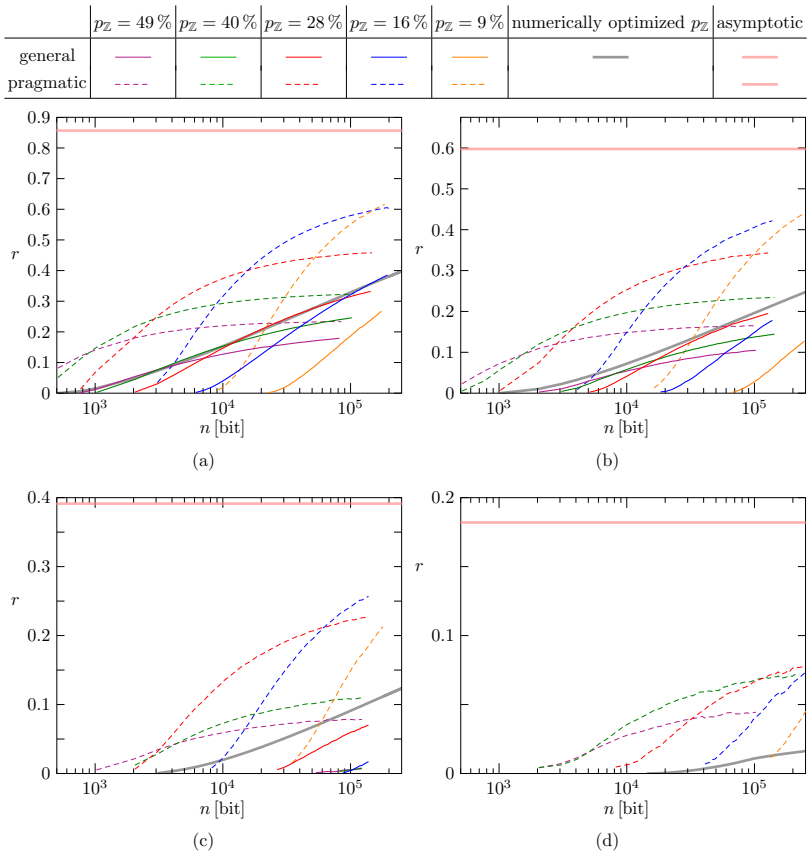


Figure 2.8: Experimental secret key rates r vs. sifted key length n for different probabilities of encoding and measuring on the two bases $p_{\mathbb{Z}}$, $p_{\mathbb{X}} = 1 - p_{\mathbb{Z}}$ and for different channel conditions (values of the average QBER $Q_{\mathbb{X}}, Q_{\mathbb{Z}}$): (a) $Q_{\mathbb{X}} = 0.3\,\%$, $Q_{\mathbb{Z}} = 1.5\,\%$; (b) $Q_{\mathbb{X}} = 2.4\,\%$, $Q_{\mathbb{Z}} = 3.9\,\%$; (c) $Q_{\mathbb{X}} = 4.9\,\%$, $Q_{\mathbb{Z}} = 6.0\,\%$; (d) $Q_{\mathbb{X}} = 8.3\,\%$, $Q_{\mathbb{Z}} = 8.1\,\%$. For each case we report the key rates obtained for ε_{sec}-GS (solid lines) and δ_{sec}-PS (dashed lines) keys with $\varepsilon_{\text{sec}} = 10^{-10}$, $\delta_{\text{sec}} = \frac{2}{\ln 2}\varepsilon_{\text{sec}}^2$, $P_{\text{fail}} = 10^{-3}$ and a correctness parameter $\varepsilon_{\text{cor}} = 10^{-10}$. The standard deviation of experimental rates are on the order of 10^{-3} for both ε_{sec}-GS and δ_{sec}-PS keys. Error bars are not reported in the plot for the sake of clarity. For comparison, we also report the asymptotic key rate in the infinite length limit, and the ε_{sec}-GS bound achievable by optimizing the probability $p_{\mathbb{Z}}$ and the thresholds $Q_{\text{tol}}^{\mathbb{Z}}, Q_{\text{max}}^{\mathbb{X}}$ for each value of n.

rate r (eq. (2.34), with ℓ given by eq. (2.27)) over p_Z, $Q^{\mathbb{Z}}_{\text{tol}}$ and $Q^{\mathbb{X}}_{\text{max}}$ for each n.

In the numerical procedure used to find the optimal bound for ε_{sec}-GS keys, since an analytical expression is not available for L_{EC} or ε_{rob}, L_{EC} is approximated as $L_{\text{EC}} = 1.1 \cdot n \cdot h_2(Q_{\mathbb{X}})$ and, similarly, ε_{rob} is replaced by the following upper bound [**?**]:

$$\varepsilon_{\text{rob}} \leq \exp\left[-\frac{k(Q^{\mathbb{Z}}_{\text{tol}} - Q_{\mathbb{Z}})^2}{1-2Q_{\mathbb{Z}}} \ln\left(\frac{1-Q_{\mathbb{Z}}}{Q_{\mathbb{Z}}}\right)\right] \tag{2.36}$$

Experimental values obtained for ε_{rob} show that such bound is rather loose. On the other hand, as $Q_{\mathbb{X}}$ increases, the approximate expression for L_{EC} is lower than the average value for the Winnow scheme. As a consequence, the experimental secret key rates may slightly exceed the optimal bound in some low QBER cases, as we can see in fig. 2.8.

As a further comment, we note that, for an asymmetric channel with $Q_{\mathbb{X}} < Q_{\mathbb{Z}}$, using the $\mathbb{Z}$ basis for key encoding and $\mathbb{X}$ for eavesdropper detection provides a higher optimal secret key rate (2.34). However, when the two error rates $Q_{\mathbb{X}}$ and $Q_{\mathbb{Z}}$ have similar values, a minor gain in r is obtained. For instance, when $n = 10^6$, $\varepsilon_{\text{cor}} = \varepsilon_{\text{sec}} = 10^{-10}$, with $Q_{\mathbb{Z}} = 4\%$ and $Q_{\mathbb{X}} = 2\%$, we can achieve $r = 0.31$; by exchanging the role of $\mathbb{Z}$ and $\mathbb{X}$, $r = 0.33$ can be achieved.

In situations such as satellite quantum communications, the amount of sifted bits is expected to fluctuate as it depends on the variable channel conditions during the passage. From the experimental point of view it is easier to fix the values of $p_{\mathbb{Z}}$ and $p_{\mathbb{X}}$ and accumulate data as long as possible. The value of $p_{\mathbb{X}}$ will constrain the ratio between k and n according to the relation $p_{\mathbb{X}} = \frac{1}{1+\sqrt{k/n}}$. In the performed experiments, we thus fixed the value of $p_{\mathbb{Z}}$ and $p_{\mathbb{X}} = 1 - p_{\mathbb{Z}}$. For each value of the background noise we run different acquisitions with $p_{\mathbb{Z}}$ belonging to the discrete set $\{9\%, 16\%, 28\%, 40\%, 49\%\}$. Experimental results for the ε_{sec}-GS key rates are plotted with thin solid lines, while δ_{sec}-PS key rates are plotted with thin dashed lines; different colors correspond to different $(p_{\mathbb{Z}}, p_{\mathbb{X}})$. We used $P_{\text{fail}} = 10^{-3}$, $\varepsilon_{\text{cor}} = 10^{-10}$ and $\varepsilon_{\text{sec}} = 10^{-10}$. As expected, pragmatic secrecy always allows the achievement of higher secret key rates with respect to general secrecy, which pays the price for the higher level of secrecy it provides. The gain becomes more evident when the channel becomes noisier and the QBER increases. We also observe that with $Q_{\mathbb{X}} = 4.9\%$ ε_{sec}-GS keys secure are obtained for $p_{\mathbb{Z}} = 16\%$, $p_{\mathbb{Z}} = 28\%$, $p_{\mathbb{Z}} = 40\%$ and $p_{\mathbb{Z}} = 49\%$ and not for $p_{\mathbb{Z}} = 9\%$, whereas, when $Q_{\mathbb{X}} = 8.3\%$, only keys secure against pragmatic secrecy can be extracted with the parameters we used.

We point out that the bounds derived for the general and pragmatic secrecy do take into account statistical fluctuations: if the measured $\hat{Q}_{\mathbb{Z}}$ is greater than $Q^{\mathbb{Z}}_{\text{tol}}$ the protocol aborts, while for $\hat{Q}_{\mathbb{Z}} < Q^{\mathbb{Z}}_{\text{tol}}$ the protocol gives a secure key with security parameter ε_{sec}. As an example, given $Q_X = 4.9\%$, $Q_Z = 6.0\%$, $n = 100000$ and $p_{\mathbb{Z}} = 9\%$, the parameter μ which takes into account these fluctuations for general secrecy (see eq. (2.27)), is approximately equal to 0.15, a value which, for an experimentally realistic number of bits disclosed during the information reconciliation procedure, and even without the contribution of $Q^{\mathbb{Z}}_{\text{tol}}$, yields the impossibility of producing a secret key.

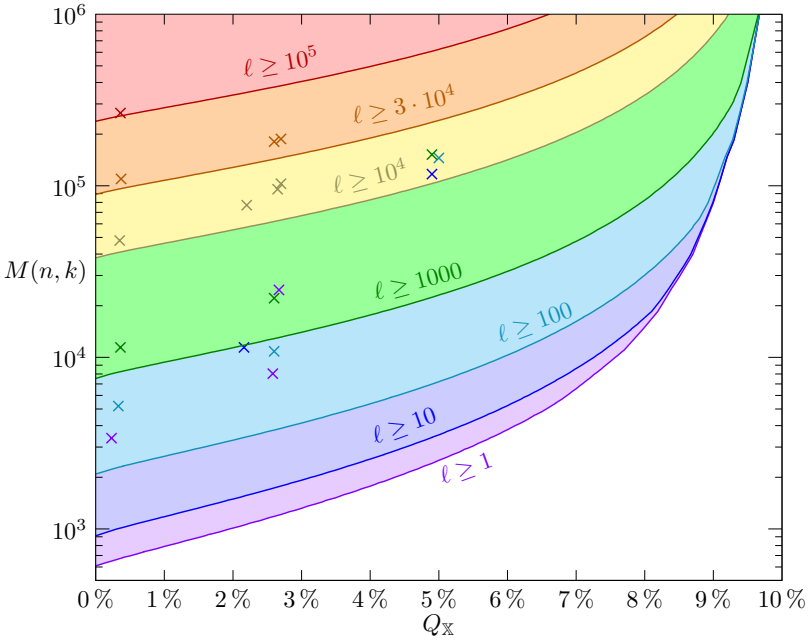


Figure 2.9: Minimum number of received bits $M(n,k)$ needed to obtain a ε_{sec}-GS key of a given length ℓ (as labelled on each curve) versus the quantum BER $Q_{\mathbb{X}}$. Different colors divide the regions with different secret key lengths. Crosses represent our experimental results, the colored regions and the solid lines that delimit them are derived from the numerically optimized bound, assuming $Q_{\mathbb{Z}} = Q_{\mathbb{X}}$.

Moreover, we notice that higher values of $p_{\mathbb{Z}}$ ($\sim$ 50%) better suit lower values of n for both general and pragmatic secrecy in all considered cases: for instance, when $Q_{\mathbb{X}} = 0.3\%$ in the general secrecy case, $p_{\mathbb{Z}} = 49\%$ is optimal for $n < 3 \cdot 10^3$; on the other hand, as n increases, it is possible to decrease $p_{\mathbb{Z}}$ and when $n \simeq 10^5$ the highest rate is obtained with $p_{\mathbb{Z}} = 16\%$. This feature can be understood in the following way: for a short sifted key $\mathbf{X}$, an almost equally long string $\mathbf{Z}$ ($k \sim n$) is needed to reliably detect eavesdropping; when n grows, less bits of $\mathbf{Z}$ (in percentage) are necessary. In fact, in the large n limit, it is possible to choose k so that k/n vanishes as n goes to infinity and the secret key rate approaches the asymptotic bound, $r = 1 - h_2(Q_{\mathbb{X}}) - h_2(Q_{\mathbb{Z}})$.

It is worth noting that, in the asymptotic limit, a biased choice of the bases gives a higher secure key rate with respect to the BB84 protocol [15] whenever $p_{\mathbb{X}} > \sqrt{1/2}$. In fact, in the infinite limit, the fraction of secure over sifted bits is given by $1 - 2H(Q)$ in both cases (for simplicity we here assume $\hat{Q}_{\mathbb{X}} = \hat{Q}_{\mathbb{Z}} = Q$); however, a biased choice of the bases gives a number of sifted bits that is approximately $p_{\mathbb{X}}^2 > 1/2$ of the sent bits (also in the finite size regime), while for the BB84 protocol the sifted bits are $1/2$ of the sent bits. In particular, by using a large $p_{\mathbb{X}}$, namely $p_{\mathbb{X}} \sim 1$, in the infinite key limit we approach a double secret key rate with respect to BB84.

With the obtained data we also estimated the minimum number of received qubits M that are needed in order to obtain a key of given length ℓ. In figure 2.9 we show this quantity as a function of the QBER (in this case we assumed that $Q_{\mathbb{X}} = Q_{\mathbb{Z}}$). Solid lines represent the theoretical minimum M necessary to obtain a general secret key for different lengths ℓ. With mark-

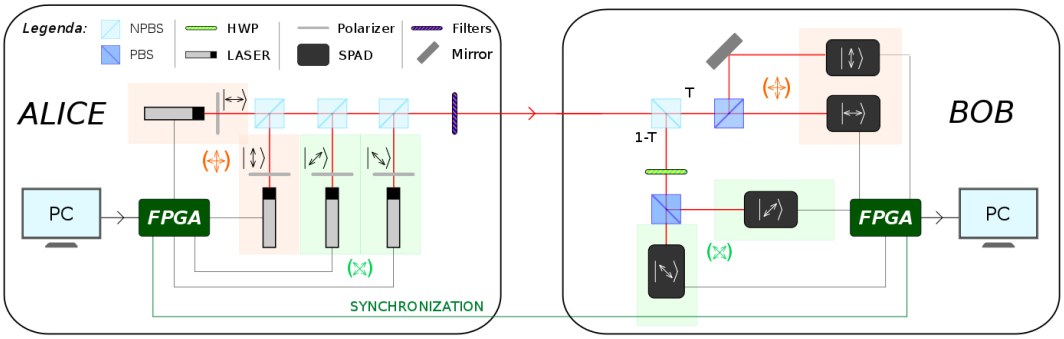


Figure 2.10: The qubits are generated by attenuating four differently polarized lasers. The FPGA board controls which laser should be turned on in each qubit transmission. At the receiver side, by a beam splitter with transitivity T, Bob perform the measurement in the $\mathbb{X}$ (with probability T) or $\mathbb{Z}$ basis (with probability $1-T$). NPBS, beam splitter; PBS, polarizing beam splitter; HWP, half wave plate; Filters, neutral density filters, SPAD, single photon avalanche diode.

ers of different colors we indicate the experimental received qubits for the different values of ℓ. Clearly, as the QBER grows, it is necessary to increase the number of exchanged qubits to obtain a given key length ℓ. On the other hand, when the channel is almost noiseless, a secret key of reasonable length can be extracted by using a relatively small number of qubits: for instance, more than 1000 secure key bits can be obtained by exchanging less than 20000 photons (see Figure 2.9).

2.7 METHODS

The optical setup of our prototype implementing the quantum communication is shown in Figure 7.2. The transmitter (Alice) uses four infrared (850nm) attenuated diode lasers driven by a Field Programmable Gate Array (FPGA) to send the bits 0 and 1 encoded in the different polarization bases of the photons. By properly configuring the FPGA, it is possible to set the probabilities $p_{\mathbb{X}}$ and $p_{\mathbb{Z}}$. The receiver (Bob) uses a variable beam splitter (BS) with transmission T to send the received qubits to the measures in the two bases. The probability $p_{\mathbb{X}}$ is equal to the transmissivity T of the BS. On one BS output, a polarizing beam splitter (PBS) and two single photon avalanche photodiodes (SPAD) measure the photons in the $\mathbb{X}$ basis; on the other side a half-wave plate (HWP) is positioned before the PBS to allow the measurement in the $\mathbb{Z}$ basis. The counts detected by the four SPAD are stored on a second FPGA. A cable between the two FPGA is also used along for synchronization. Concerning the transmitted qubits, we used the same data structure of a recent free-space QKD implementation [25] based on the B92 protocol [14]. A raw key is composed into N packets of 2880 bits each, which are in turn divided into 12 frames for the ease of synchronization. In fact, 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). As regards the payload slots, the first

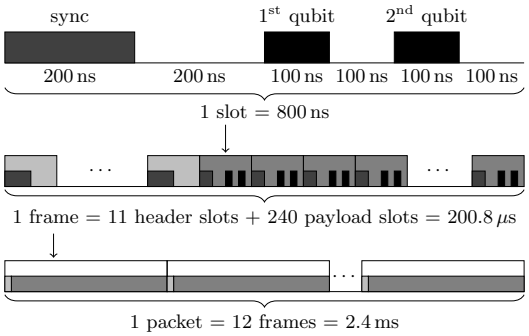


Figure 2.11: A raw key of 288 kbit is divided into 50 packets of 5760 bits each, which are in turn divided into 12 frames for the ease of synchronization. In fact, each frame consists of 11 header slots and 240 payload slots, each with a duration of 800 ns. The header exhibits the pattern '100000xxxx1', 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 or0, respectively). The first 200 ns are used to send the synchronization beam, then, after the synchro-laser, Alice waits 200 ns and then sends the two qubits separated by 200 ns. The resulting raw key rate is therefore upper bounded as $R_{raw} \leq 2.39\text{Mbit/s}$.

200 ns are used to send the synchronization signal; then, Alice waits 200 ns and sends two bits separated by 200 ns. It is worth noting that the experimental setup of this protocol is very similar to the original BB84: the main difference lies in the interpretation of received bits in the two different bases.

2.8 DISCUSSION

In conclusion, we have experimentally demonstrated the feasibility of key distillation according to the finite-key analysis proposed in [104] and compared it with a less stringent definition of security, called pragmatic, that protects the protocol against intercept and resend attacks. We compared the two analyses for different amounts of depolarizing noise added to the quantum channel. With pragmatic security, a significantly secret key rate with finite keys is demonstrated, even in conditions near the theoretical $Q_{\mathbb{X}}$, $Q_{\mathbb{Z}}$ bound of 11%. Its drawback is the insecurity against collective attacks, which however are not presently available. We stress that, when the channel is very noisy ($Q_{\mathbb{X}} = 8.3\%$) no key that is secure against the most general quantum attack could be extracted up to $2 \cdot 10^5$ sifted bits; however, by considering only intercept and resend attacks, in this case a secrect key rate up to 7.5% was obtained. When $Q_{\mathbb{X}}, Q_{\mathbb{Z}} > 11\%$ it is not possible to obtain a secure key even in the asymptotic large n limit. This shows that, for highly noisy channels, the use of pragmatic secrecy is a viable solution to obtain some secret bits for a experimentally realistic number of exchanged photons. We believe that our work can have important application for free-space quantum communication and for all QKD scenarios in which the number of exchanged qubits is limited by physical constraints, such as in the inter-satellites link scenario.

3

FREE-SPACE LONG DISTANCE OPTICAL LINK

In this chapter we study the propagation of a quantum beam through the atmosphere, paying attention to some particular effects, like beam wondering, beam spreading and scintillations. We demonstrate in Chapter 2 how it is possible to establish secure key also in presence of noise and in the case of finite key regime. In order to bring laboratory experiment in real life conditions we perform a free-space link in 2012, where it was possible to establish a QKD experiment between two islands in the Canary archipelago. It represent one of the most interesting scenario for a possible quantum link, because the proximity of Sahara desert and badly weather conditions make the environment very particular. From the astronomical point of view, the blanket of clouds that hide the scattering of city light, create a perfect conditions for space study and exploration; from the other side this clouds creates a very turbulent channel once you look for an horizontal link, where a sender, positioned in the Jacobus KapteinTelescope (JKT) telescope communicates with a receiver situated in OGS telescope. We explored atmosphere's effects, and we proved that polarized photons sent through 143 km of atmosphere have not be degraded. Moreover we introduce a new method of analysis in order to use as a resource the atmospheric effects, so that to increase the Signal to noise ratio (SNR) ratio and to be able to make QC also in a very worst case conditions.

3.1 GAUSSIAN BEAM PROPAGATION

The treatment will be focused on Gaussian beam because it is one of the most frequent case in experimental condition. We can define the optical intensity of a Gaussian beam $I(\rho) = |U(\rho)|^2$, where $U(\rho)$ represents the electric field in the function of the axial and radial position, z an $\rho = \sqrt{x^2 + y^2}$.

$$I(\rho, z) = I_0 \left[\frac{w_0}{w(z)} \right]^2 \tag{3.1}$$

The peak of the function obviously is represented by the point $\rho = 0$ in the z axis, and decreases monotonically as ρ increases. In the case of $(\rho = 0)$ the intensity reduces to:

$$I(0, z) = \frac{I_0}{1 + (z/z_0)^2} \tag{3.2}$$

In the condition of any transverse plane, the intensity of the beam assumes its peak value on the beam axis, and decreases by a factor $1/e^2$ at the radial distance $\rho = w(z)$. The relation of the beam width in function of the parameter z is given by:

$$w(z) = w_0 \sqrt{1 + \frac{z}{z_0}^2} \tag{3.3}$$

the minimum value assumed by $w(z)$, at the plane $z = 0$ is known as *beam waist* o *radius* w_0. Usually in optics a term very used is the *spot size*: $2w_0$. In the hypothesis that $z >> z_0$, the first term of the equation (3.3) become neglected, in fact $w(z)$ could be approximately at:

$$w(z) \simeq \frac{w_0}{z_0} = \theta_0 z \tag{3.4}$$

where θ_0 represents the half angle at which the cone of the beam diverges.

3.2 ATMOSPHERIC MODEL

Beam propagation in atmosphere is subject principally to many effects given by temperature, wind, atmospheric conditions and many others. Small variations in temperature ($< 1°C$) give rise to local random changes in the wind speed, so that generations of whirls is amplified. Due to the continuous change of temperature, the density of the atmosphere varies and hence its refractive index. Usually these small variations are inconsistent, but in the case that they can accumulate they become important in the study of an optical beam propagation in atmosphere. The front wave of a propagated optical beam (not only quantum), will be subject to variations related to the refractive index. This can lead to effects of:

- beam wandering
- intensity fluctuations ("scintillation")
- enlargement of the beam ("beam spread")

These small variations on the refractive index, have a similar effects like a series of small lenses positioned through the direction of propagations.
The consequences due to the small variations in the refractive index, have a similar effect like a series of small lenses. The latter, focus and redirect the beam, and possibly through interferential phenomena causes variations in intensity.

It could be assumed from theory that, every single "lens" focus and redirects the beam in different position. This phenomena explain the intensity fluctuation of the bundle. Moreover the dimension of these lenses could be approximated to the dimension of the vortex that generated it. Given the complexity of this kind of study, the theory of turbulence is based on statistical analysis. Statistical description of the process, makes possible the generalization of useful models describing the average effects, such as: total beam wandering, beam spread, scintillation [112].

3.2.1 *Structural constant of the refraction index*

One of the most method to represents turbulence intensity, is structural constant intrinsic of the refraction index C_n^2. It is related with the geographic position and altitude, but also it changes with the seasons, days and the hours. From experimental observations, Hufnagel suggested the following relation [61]:

$$C_n^2 = \{[2.2 \cdot 10^{-53} h^{10} (W/27)^2] e^{-} h/1000 + 10^{-16} e^{-h/1500}\} e^{r(h,t)} \qquad [m^{-2/3}] \tag{3.5}$$

where h is the height of the station in meters above sea level, W is the wind correlation factor and $r(h,t)$ is a zero mean Gaussian random variable; v(h)

is the wind velocity at the height h. The correlation factor of the wind could be expressed by the equation:

$$W = \left[\frac{1}{15\,\mathrm{km}} \int_{5\mathrm{km}}^{20\mathrm{km}} v^2(h)\, dh \right] \tag{3.6}$$

For what concerns the wind velocity it can be used the Bufton's model

$$v(z) = 5 + 30e^{-[(z-9400)/4800]^2} \tag{3.7}$$

where the distance z and the velocity v are expressed respectively in [m] and [m/s].

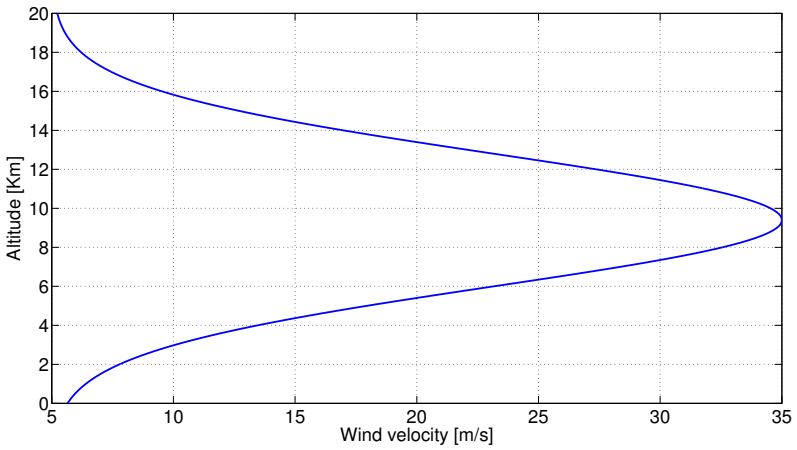


Figure 3.1: A plot of the average wind profile versus the altitude using Butfon's model.

3.2.2 *Turbulence effect*

We concentrate our analysis in the regime of weak turbulence, where weak phase perturbations occur, due to variations of the atmospheric density, along the beam trajectory.

In this regime all the perturbations effects could be refer to a phase perturbation $\phi(r)$, where $\mathbf{r_i} = (r_i, \theta_i)$ represents the polar coordinates. This hypothesis constitutes a significant conceptual simplification. Our interest is based in the time-evolution of the phase correlation between two points r_1 and r_2. In mathematical terms it can be formalized as:

$$C(\mathbf{r_1}, \mathbf{r_2}) = \langle e^{i\Phi(\mathbf{r_1}) - \Phi(\mathbf{r_2})} \rangle \tag{3.8}$$

where our aim is to find a final explicit expression for the phase structure function. In the case of a beam propagation of distance L the phase difference accumulated can be written as:

$$\Phi(\mathbf{r_1}) - \Phi(\mathbf{r_2}) = k \int_0^L [n(\mathbf{r_1}, z) - n(\mathbf{r_2})] dz \tag{3.9}$$

where $k = 2\pi/\lambda$ denotes the wave vector. From "Kolmogorov's two-thirds law", the structure function for the phase results [70]:

$$D_\Phi(|\mathbf{r_1} - \mathbf{r_2}|) = 6.88 \frac{|\mathbf{r_1} - \mathbf{r_2}|^{5/3}}{r_0} \tag{3.10}$$

The r_0 parameters, usually named as *Fried parameter*, is correlated to the optical consequences of the phase distortions. In fact without turbulence the r_0 parameter stretch to ∞.
Considering the propagation of a Gaussian beam in atmosphere, and using the above theory concepts, it is possible to determine a relation between the beam waist and the Fried parameter:

$$\frac{w_o}{r_0} = \frac{\sqrt{(w_{le}/w_{dl})^2 - 1}}{3} \tag{3.11}$$

where w_{dl} and w_{le} are the $1/e$ far field radius of the diffraction-limited beam.

In the case of horizontal line of sight transmission, the atmosphere is relatively uniform, in fact the the Fried parameter can be expressed as:

$$r_0 = 3.02\,(k^2 L C_n^2)^{-3/5} \tag{3.12}$$

typical values of the refractive index are in the range $10^{-17}$to 10^{-12} in a very good case. For night-time operation and in the case of a good astronomical sites we can use the following formulation, based on the Hufnagel-Valley profile [107, 108]:

$$C_n^2(h) = 8.16 \cdot 10^{-54} h^{10} e^{-h/1000} + 3.02 \cdot 10^{-17} e^{-h/1500} + 1.90 \cdot 10^{-}15 e^{-h/100}$$

From a vertical line of sight the Fried parameter could be approximated to:

$$r_0 = \left[0.423\, k^2 \sec\varepsilon \int_0^1 h C_n^2(h)\, dh\right]^{-3/5} \tag{3.13}$$

where ε indicates the zenith angle. As reported in the above paragraphs, the atmospheric turbulence is source of spread on the range of high spatial frequency, wander for low spatial frequency and intensity variations. In fact eddies smaller than the beam size are cause of beam spreading, whereas eddies larger than the beam size cause wander. Intensity fluctuations are due to eddies of the order of $\sqrt{\lambda L}$ where λ is the wavelength of the radiation and L is the propagation distance.

SCINTILLATION The intensity variations are usually expressed as the log amplitude fluctuations. In an optical experiments with a small dimension of the receiver telescope, the scintillations effects must be take into account, while for a big receiving area these effects are mediated in all the aperture. The scintillation could be expresses as:

$$\sigma_I^2 = A[e^{4\sigma_x^2} - 1] \quad [W/cm^2] \tag{3.14}$$

where A is the aperture average factor which in the hypothesis of weak turbulence and small value of eddies l_0 ca be estimated as:

$$A = \left[1 + 1.07\left(\frac{kD^2}{4L}\right)^{7/6}\right]^{-1} \tag{3.15}$$

in the case of a plane wave the parameter σ_x^2 is approximated to the value $0.307\, k^{7/6} L^{11/6} C_n^2$, and for a spherical wave it becomes $0.124\, k^{7/6} L^{11/6} C_n^2$. L represents the link distance, while D is the aperture diameter.

BEAM WANDER A propagation of an optical beam in a turbulent atmosphere, is affected by deviation from its nominal position. Depending on the velocity of this effect we could divide wandering in *jitter* effect in the case of fast movements and *drift* as a slow shift effect. It is possible to estimate the tilt variance as:

$$\alpha^2 = 0.364 \left(\frac{D}{r_0}\right)^{5/3} \left(\frac{\lambda}{D}\right)^2 \tag{3.16}$$

The tilt movement can be subdivided in:

- G-tilt through the mean gradient of the wave front (it represents what is seen by a quadrant detector)
- Z-tilt through the normal to the plane that minimize the wave front distortion (it represents the tilt terms on the Zernike's expansion)

3.2.3 *Space channel*

In the previous sections we have understood that the sky is not transparent for optical frequency. In Figure 3.2 we present a simulated atmospheric transmittance for a propagation at zenith angle. We underline the wavelengths of commercially available laser system using colored lines. As you can see, the transmittance is better at higher wavelengths, but unfortunately other factors (e.g. detectors efficiency, diffraction, source repetition rate) limits the performance of the link .

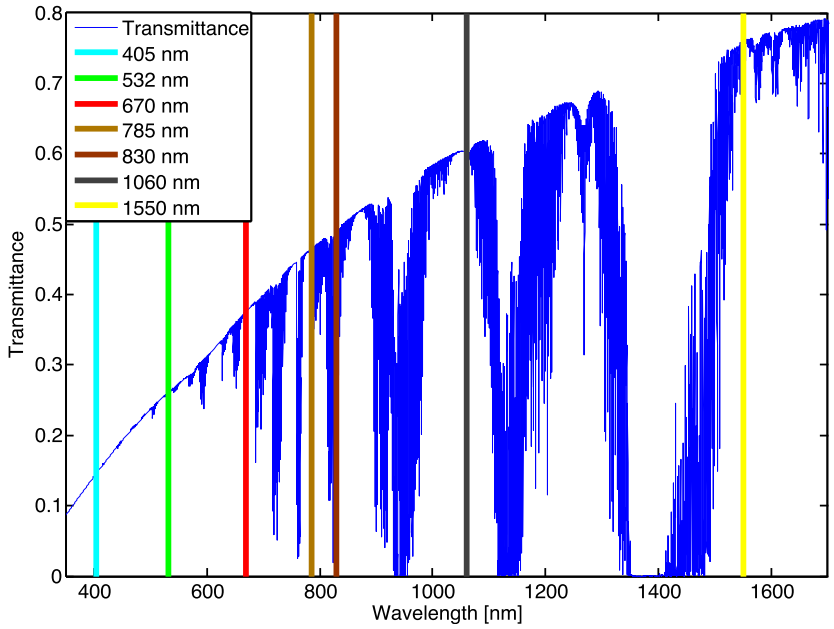


Figure 3.2: Simulated atmospheric transmittance at a typical rural location, for propagation at zenith. Colored lines represent wavelengths of commercially available laser systems. Courtesy of ICQ Waterloo.

As we saw from the above paragraphs, the transmission in atmosphere of an optical beam will be affected by diffraction, systematic pointing error

and atmospheric turbulence, which degrades the quality of the wave front and obviously affecting the result of the transmission. Moreover the beam diffraction depends on the working wavelength and in order to mitigate this problem bigger telescope and particular optical design of the system must be done. In this kind of scenario a trade-off between the working wavelength and the dimension of the telescope is necessary to ensure acceptable results. From other QKD experiments due in free-space channel, it is clear that turbulence has no negative effect on polarization-based [52, 109]. Looking at vertical link, and in particular to satellites communications, turbulence predominantly occurs in the lower 10 km of the atmosphere [40].

The total dimension of the beam size, comes from the combination of diffraction and turbulence. Because turbulence is not correlated with the transmitter aperture, this imposes a limitation on the aperture size of the transmitter telescope.
As above explained, the transmittance of the atmosphere is dependent on both wavelength (see 3.2) and angle, and it includes the concentrations of molecules and particles present [19].

3.3 CANARY EXPERIMENT

As we report in the above paragraphs, the effects of the free-space channel (losses and background light) on quantum signal, in particular in presence of atmospheric turbulence, impair the security of the QKD system. We introduce a method to exploit the atmospheric turbulence as a resource for QKD. An Adaptive Real Time Selection (ARTS) technique at the receiver allows to take advantage of the fluctuating transmissivity of the channel, giving rise to an increase of the secure key rate. QKD pioneering demonstrations in free-space were realized generally during dark nights or by using very narrow spectral filters that generally impose a low key rate already on urban scale [57, 22, 109, 37, 83, 68]. On the contrary, in ordinary conditions the QBER will be higher than the secure threshold except for high channel transmission. However, in the case of QKD over long links and in realistic conditions, including daylight, a breakthrough in the protocol is needed to limit background noise.
Here, we devise a method that exploits the atmospheric turbulence for secret key generation, even in the conditions in which the average QBER is too high for secure communication. In a link with fluctuating transmission coefficient and a significant attenuation, due to turbulence and to the combination of optical diffraction and scintillation, respectively, it is possible to devise a solution to the high QBER problem on the basis of a sound characterization of the channel transmission. A recent study pointed out that the temporal profile of the transmissivity typically has peaks lasting a few milliseconds, distributed in a low transmissivity background [26]. A post-selection technique based on estimating the QBER in short time frames would be ineffective here because the QBER value cannot be reliably estimated in such short time scale [38]. Indeed, using current or even realistic transmission rates e.g. 100 MHz of repetition rate, the QBER statistics results too limited due to the moderate rate. Moreover, such use of the received qubits further reduces the key rate and has to be avoided.
The CAD1 and CAD2 distillation schemes discussed in [10] represent a generalization of Maurer's advantage distillation technique [73] and presented

in Chapter 2. Sequences of correct (possibly non consecutive) sifted bits are joined together and one single secure bit is distilled out of each sequence. The length of each sequence should be chosen according to a trade-off scheme, because longer sequences allow to distill keys with higher channel QBER, but provide a lower key rate in the case of low QBER. However, in a turbulent, rapidly time-varying channel, the effectiveness of such solutions would be limited by the difficulty of choosing the suitable parameters of the distillation strategy according to the varying QBER.
Another generalization of the advantage distillation of [74] was proposed in [113]: parities for many pairs of bits are shared between Alice and Bob along the public channel. Those pairs with non matching parities are discarded, while the remaining ones (over which the QBER is lower) are syndrome decoded. However, the above presented distillation methods do not take advantage of the intrinsic QBER variability of the channels, but they rely on the assumption that the channel maintains its QBER stable long enough to allow optimization of their parameters. On the contrary, the technique proposed in [38] exploits the transmissivity peaks in the channel by observing variations of the sifted bit rate on a millisecond time scale, and can hence be quite effective in dealing with turbulent channels [95, 94].
Here we propose a ARTS scheme where transmissivity peaks are instantaneously detected. The scheme is based on the estimation of the link transmissivity in its intrinsic time scale by an auxiliary classical laser beam copropagating with the qubits but conveniently interleaved in time.

In this way the link scintillation is monitored in real-time and the selection of the time intervals of high channel transmissivity corresponding to a viable QBER where a positive key generation rate is available.

3.3.1 *Preliminary analysis*

The link used in our demonstration is the 143 Km free-space channel between La Palma and Tenerife islands shown in Figure 3.3. At the transmitter we generate the quantum bits by strongly attenuated lasers at 850 nm. In the same location we also use a 30 mW[1] classical laser beam (probe) at 808 nm to estimate the link transmissivity. We used two different wavelengths to easily separate, by a dichroic mirror, the two signals at the receiver. The quantum and probe signals are coupled into the same optical path of a customly designed telescope (see Figure 3.3).

In order to test the ability of estimating the link transmissivity, we first sent on the same free-space channel, two signals: the classical probe, detected with a fast photodiode at the receiver, and a single strongly attenuated laser. The classical signal featured pulses of 100 μs duration at 1 kHz repetition rate, while the attenuated laser at 850 nm was a continuous beam. At the receiver, the quantum signal was detected by a Single Photon Avalanche Photodiode (SPAD) and acquired in packets with duration of 1 ms.
We would like to test the correspondence between the intensity of the received classical beam and the photons received on the quantum channel. As shown by the 11 s of acquisition time reported in Figure 3.4, there is a strong

1 At the transmitter the beam diameter size is of the order of 20 cm, guaranteeing class-1M eye-safe beam.

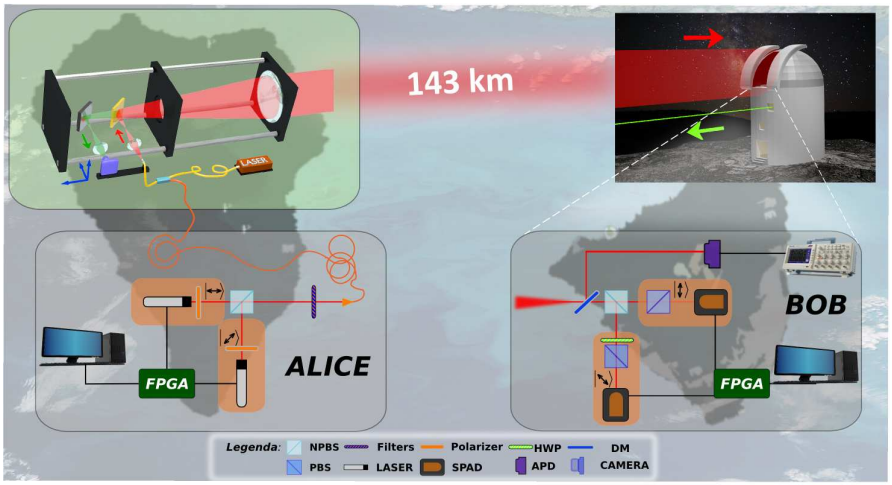


Figure 3.3: Experimental setup: Alice, located at JKT observatory in La Palma, sends qubits by using two 850 nm FPGA-controlled attenuated lasers with different polarization. Qubit photons are combined with an atmospheric probe laser (30 mW @ 808 nm) and transmitted through a suitably designed telescope. The Alice telescope is also used to collect the beacon laser sent by Bob, located at the Optical Ground Station in Tenerife, and required for tracking the pointing of the transmitter. Bob receives both the signals through the OGS telescope: the probe is monitored by an APD and the qubits are detected with two SPADs. FPGA: Field Programmable Gate Arrays; HWP: half-wave plate; NPBS: non-polarizing beam splitters; PBS, polarizing beam splitter; SPAD, single-photon avalanche photodiode; DM: dichroic mirror.

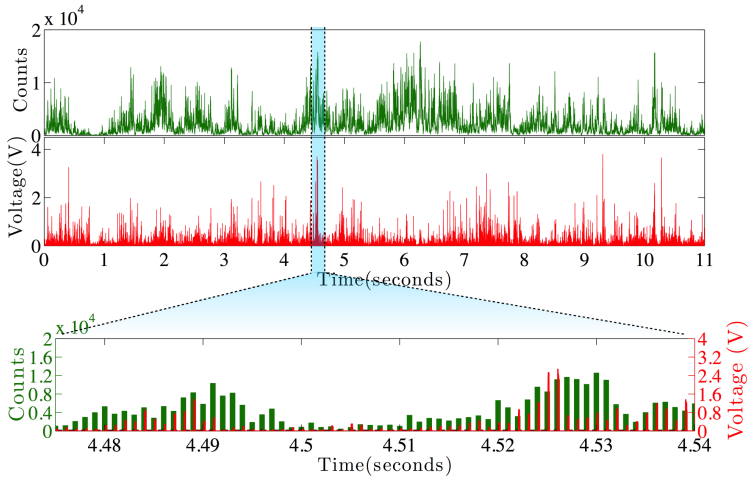


Figure 3.4: Comparison between the counts detected by the SPAD (green line) and the voltage measured by the fast photodiode at the receiver (red line). In the inset we show a zoomed detail of the acquisition (between 4.48 s and 5.54 s) in order to better appreciate the correlation between the quantum and classical signal. We chose a particular inset but in all the acquisition the two signals are correlated.

correlation between the photon counts detected in each packet (green line) and the voltage registered with the fast photodiode (red line).

To demonstrate the correlation we performed the ARTS method, consisting in the following procedure. Given a set of L packets (each of 1 ms length), we let V_i be the probe signal amplitude and S_i the number of detected photons in the quantum signal for the i-th packet, respectively. We set a threshold value V_T for the probe voltage and post-select only those packets such that $V_i > V_T$; in particular, we denote by $\mathcal{I}(V_T) = \{i \in [1, L] : V_i > V_T\}$ the indexes of the packets for which the above condition holds and by $N_P(V_T)$ the corresponding number of packets, that is, $N_P(V_T) = |\{\mathcal{I}(V_T)\}|$. Furthermore, we define the following quantities:

$$S(V_T) = \sum_{i \in \mathcal{I}(V_T)} S_i, \qquad \overline{S}(V_T) = \frac{S(V_T)}{N_P(V_T)} \tag{3.17}$$

with $S(V_T)$ representing the total number of detected bits and $\overline{S}(V_T)$ the mean number of detection per packets after the post-selection performed with threshold V_T.

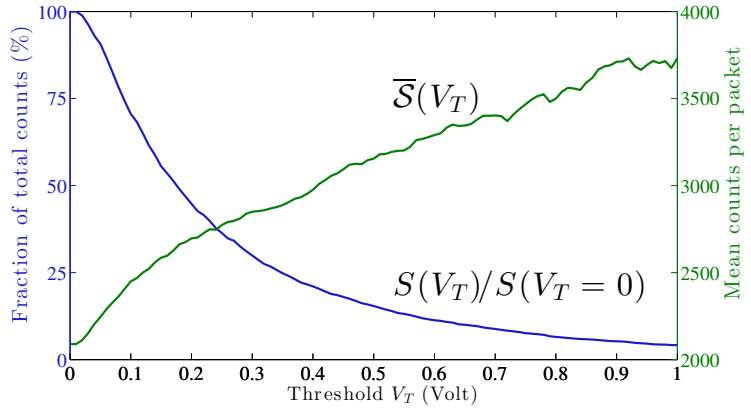


Figure 3.5: Mean counts per packet $\overline{S}(V_T)$ (normalized to the mean counts obtained without thresholding) and fraction of total count $S(V_T)/S(V_T = 0)$ in function of the probe threshold.

The effect of the ARTS procedure can be clearly appreciated in figure 3.5, where $\overline{S}(V_T)$ (normalized to the mean counts obtained without thresholding) is plotted (green line) as a function of the threshold: a higher threshold value corresponds to a larger mean number of counts per packet. This demonstrates that the probe and quantum signals are strongly correlated and one can significantly improve the SNR by thresholding[2]. As side effect, we have that the pre-selection also decreases the overall number of detections in the transmission $S(V_T)$ as can be noticed by considering the ratio $S(V_T)/S(V_T = 0)$ (blue line).

3.3.2 *Application of ARTS method to QKD*

We then apply the results previously described to a QKD experiment. In particular, we will show that, increasing the SNR by thresholding gives, in some

2 Here we define the SNR as the ratio between the overall signal (true signal plus background) and the background

cases, benefits in terms of the secret key length, even if the total number of sifted bits will decrease. Indeed, when the QBER is above the maximum value tolerable for QKD (11 % for the BB84 protocol) is not possible to produce secure key. However, by the ARTS method we will reduce the QBER below the limit, allowing secure key generation. We point out that at the receiver the beam has a mean photon number per pulse below 1, namely it is the single photon level. At the transmitter side, due to the 30 dB average attenuation of the channel we are not working in the single photon regime.
First, given the number of errors E_i in the i-th packet, we define the overall number of errors $E(V_T)$ and the quantum bit error rate $Q(V_T)$ in the post-selected packets as

$$E(V_T) = \sum_{i \in \mathcal{I}(V_T)} E_i\,, \qquad Q(V_T) = \frac{E(V_T)}{S(V_T)}. \tag{3.18}$$

For evaluating the impact of the ARTS procedure on the performance of a quantum key distribution system, it is important to study the two complementary effects of thresholding: on one side, the ARTS will increase the mean detected bits per packet $\overline{\mathcal{S}}(V_T)$. On the other side it will decrease the total detections $S(V_T)$. Both effects influence the achievable secret key rate of the system, and an optimal trade-off should be found.

Being the length of the output secret key dependent on the number of available sifted bits and on their bit error rate, as a first step we need to derive an expression for both of these quantities. As demonstrated in [26], the statistics of the transmission of a long free-space channel follows a log-normal distribution. The measured probe voltage at the receiver, being constant the transmitted intensity, follows the same distribution, given by

$$p(V; m_V, \sigma^2) = \frac{1}{\sqrt{2\pi}\sigma}\frac{1}{V} e^{-[(\ln \frac{V}{m_V} + \frac{1}{2}\sigma^2)]^2/(2\sigma^2)}. \tag{3.19}$$

In the previous expression σ^2 is defined as functions of the mean m_V and of the variance v_V of the probe intensities distribution, that can be reported as: $\sigma^2 = \ln\left(1 + (v_V/m_V^2)\right)$. As an example, we show in Figure 3.6, the distribution of the measured voltages of the data used in Figure 3.4, that, according to the theory [36, 26], follows a log-normal distribution.

In the following analysis, we assume that the number of detected photons and the probe intensity have completely correlated log-normal distributions [26]. This hypothesis implies that both distributions have the same parameter σ^2. Then, we can predict the number of packets above threshold $N_P(V_T)$ and the number of sifted bits surviving the thresholding $S(V_T)$ in case of null background by:

$$\begin{aligned} S(V_T)/S(0) &= \int_{V_T}^{+\infty} \frac{V}{m_V} p(V; m_V, \sigma) dV \\ N_P(V_T)/N_P(0) &= \int_{V_T}^{+\infty} p(V; m_V, \sigma) dV. \end{aligned}$$

By taking into account the background clicks we get:

$$\begin{aligned} N_P(V_T) &= N_P(0)\frac{1}{2}\left[1 - \operatorname{erf}\left(\frac{\ln \frac{V_T}{m_V} + \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right)\right] \\ S(V_T) &= n_b N_P(V_T) + \frac{1}{2}[S(0) - n_b N_P(0)]\left[1 - \operatorname{erf}\left(\frac{\ln \frac{V_T}{m_V} - \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right)\right] \end{aligned} \tag{3.20}$$

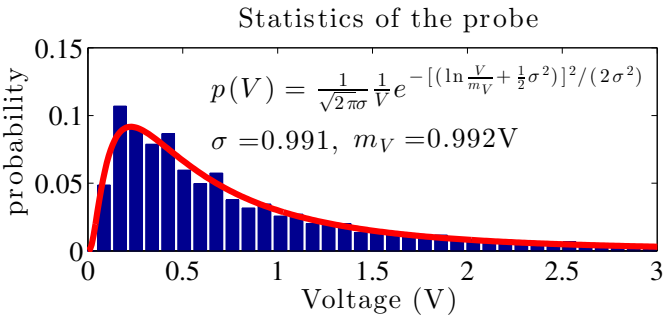


Figure 3.6: Experimental occurrences of probe intensities (measured by photodiode voltages) and lognormal fit. We show the experimental probabilities of occurrence of different photodiode voltages corresponding to different probe intensities. We also show the corresponding lognormal curve that fits the experimental data. In the figure we report the lognormal parameters obtained in the fit.

where n_b is the average background count per packet. Indeed, experimental data suggest that the hypothesis of complete correlation between quantum and probe signal is not strictly satisfied, and equation (3.20) turns out to be an approximation of the measured values. Still, it allows to derive a post-selection threshold that allow to increase the secure key rate, as will be seen in the following (e.g., in Figure 3.7).

We now define a further predictive model for estimating the bit error rate on the quantum channel as a function of the probe threshold. Let us assume that the average bit error rate on the quantum channel is m_Q and that the number of counts per packet due to background noise is n_b. Now, since background photons are not polarized, the corresponding bit error rate is $1/2$, and we can write the predicted quantum bit error rate Q_{th} as a function of the threshold V_T, namely,

$$Q_{th}(V_T) = m_Q\left(1 - \frac{n_b}{\overline{S}(V_T)}\right) + \frac{1}{2}\frac{n_b}{\overline{S}(V_T)} \tag{3.21}$$

where the predicted value for $\overline{S}(V_T) = S(V_T)/N_P(V_T)$ is obtained by using equation (3.20). Given these quantities, the asymptotic key rate of a QKD system based on the BB84 protocol and the ARTS procedure (namely the probe thresholding mechanism) reads as follows:

$$R(V_T) = \frac{S(V_T)}{S(0)}\left[1 - 2h_2\left(Q(V_T)\right)\right] \tag{3.22}$$

It is worth noting that considering the asymptotic rate instead of the finite-lenght one [8, 104], may be considered a restrictive approach, especially because the post-selection further reduces the number of available sifted bits. However, it is sufficient to choose the size of the blocks before key distillation (i.e., information reconciliation and privacy amplification) large enough such that, without loss of generality, the asymptotic bound provides a reasonable approximation of the actual rate.

In Figure 3.7, we finally compare the theoretical (solid lines) and the experimental values (circles and crosses) of the measured QBER and the asymptotic key rate as a function of the probe intensity threshold in a data acquisition. The theoretical curves for the QBER and for the key rate were obtained

by substituting in equation (3.21) and in equation (3.22) the estimates for the log-normal parameters m_V and σ^2 of the probe signal distribution. The other two parameters, $S(0)$ and $N_P(0)$, needed for predicting $S(T)$ and $N_P(T)$, are directly measured (they correspond to the total sifted bits and the total number of packets received respectively).

The data shown of Figure 3.7 correspond to an acquisition of $5 \cdot 10^5$ sifted bits in condition of high background, simulated by a thermal light source turned on in the receiver laboratory. The intensity of the background was chosen in order to obtain a mean QBER larger than 11%. In particular, we measured an average value of $n_b = 35.17$ for the background clicks per packet and we assume $m_Q = 5.6 \cdot 10^{-2}$. As clearly shown in the figure, equation (3.21) provides a good approximation of the experimental curve.

As shown by the same Figure, there is a strong correspondence between the shape of the theoretical rate, R_{th}, and the measured rate, R_{exp}. The fact that the experimental points do not fit the expected curve can be ascribed to the discrepancy in the empirical joint distribution of probe intensities and counts with respect to the model; in particular, we measured the following fitting parameters for the normalized log-normal distributions: $\sigma_V^2 = 0.967$ for the probe intensities and $\sigma_S^2 = 0.716$ for the photon signal. However, the derivation of the optimal threshold for maximizing the secret key length (magenta dashed line) from the probe distribution yields the optimal V_T also for the experimental data. In particular, the optimal threshold inferred from the probe distribution is $V_{T,\text{opt}}^{(\text{th})} = 375$ mV, and coincide with the one resulting from optimization on the experimental data, yielding a rate of $R(V_{T,\text{opt}}^{(\text{th})}) = 5.55 \cdot 10^{-2}$.

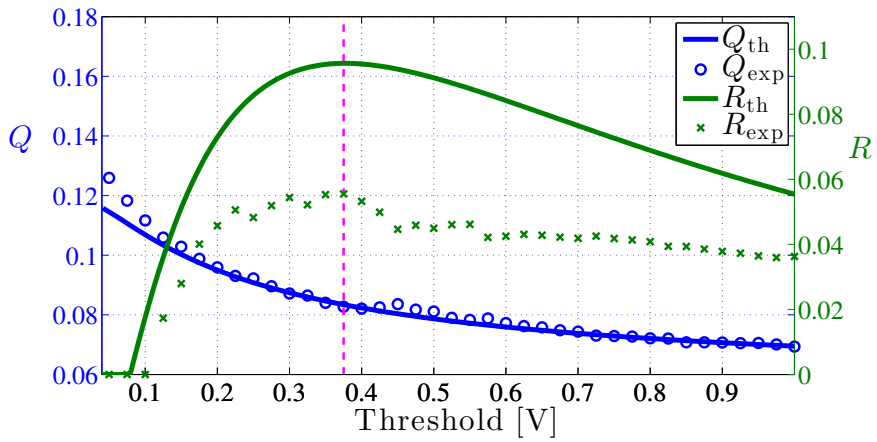


Figure 3.7: Experimental QBER (Q_{exp}) and secure key rate (R_{exp}) in function of the probe threshold (measured by the photodiode voltage). With solid lines with show the corresponding theoretical predictions (Q_{th} and R_{th}).

We observe that, in the case of $V_T < 70$ mV, is not possible to generate a secure key, being the QBER higher than the theoretical maximum (i.e., $Q = 11\%$). By increasing the threshold value above 70 mV a non-zero secret key rate is achieved. With the optimal threshold value, the measured QBER is $Q(V_{T,\text{opt}}^{(\text{th})}) = 8.38 \cdot 10^{-2}$; a significant improvement with respect to the initial value, $Q(0) = 13.14 \cdot 10^{-2}$ is therefore achieved. Finally, we observe that

for increasing values of $V_T > V_{T,\text{opt}}^{(\text{th})}$ the QBER still decreases, but so does the rate, since the reduction in the residual number of sifted bits does not compensate the advantage obtained from the lower QBER.
This result is of absolute practical relevance, as it shows that leveraging the probe intensity information is an enabling factor for quantum key distribution, since it allows to distill a secret key even when without the post-selection it would not be possible.

As for the security of this post-selection approach as applied to a QKD system, no advantage is given to a potential attacker in the true single photon regime, being the thresholding nothing but a further sifting step on the received bits [10, 114]. If the attacker tried to force Alice and Bob to post-select a particular bit, in fact, she would alter the probe signal before the disclosure of the preparation bases on the public channel, and, therefore, before she could actually know if her measured bit is correct. On the other hand, altering the probe statistics or interrupting the probe transmission would not yield any advantage to the attacker, as it would just break the correlation between the quantum and the classical signal and would thus result in a denial of service attack. The security analysis gets more involved if we allow photon number splitting (PNS) attacks. In that case, the attacker may force Bob to receive just the qubits for which the PNS attack was successful, i.e., only those pulses with multiple photons. A decoy state protocol may counteract this strategy, but its effectiveness with a turbulent and loss varying free-space channel has to be investigated.

Finally we report a simulation where the ARTS method can be compared with the technique introduced in [38], where a post-selection is performed when the number of received sifted bits is above a given threshold, determined by the mean QBER of the channel. The post-selection is effective only when the threshold is set in order to get at least several bits for coherence time of the channel (typically of the order of few milliseconds): in fact, only in this condition it is possible to post-select the correct instants of high transmissivity. In the case of very turbulent channel and extreme environmental conditions (say mist or high humidity), the number of received bits per coherence time of the channel can be lower (or of the order) than 10: in this case, the post-selection cannot be implemented and only the ARTS method becomes effective.

In order to compare the two techniques we assume that the probe and the signal statistic are perfectly correlated. The rate achievable in the two cases are shown in figure 3.8, demonstrating that the ARTS methods outperform the post-selection on the received sifted bits when the number of mean sifted bits received per coherence time of the channel are below ~ 10 and the SNR is below 20.

EXPERIMENTAL SETUP The transmitter (Alice) was located at the JKT observatory in the island of La Palma where two 850 nm attenuated lasers provided the quantum signal and a 808 nm laser was used as atmospheric probe. The polarization of the 850 nm lasers was set to the two different bases by means of half wave plates and quarter wave plates. The encoding of the quantum signal was then obtained by controlling the lasers with an FPGA. Classical and quantum lasers were coupled into mode fibers and injected into a fiber beam splitter. One of the two beam splitter output was delivered toward to a suitably designed Galilean telescope whose main char-

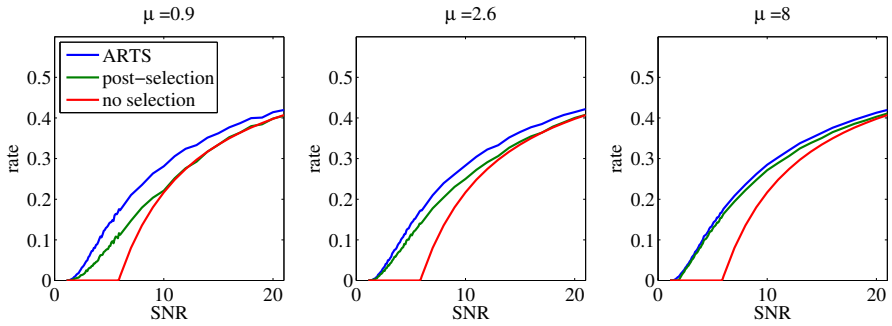


Figure 3.8: Comparison between the rates achievable by the ARTS, the post-selection and the standard QKD technique (no selection). We assumed that the channel QBER is 3% and the lognormal parameter is $\sigma = 1$, similar to the parameter we measured in the tested free-space channel. The parameter μ is the mean sifted bits per coherence time of the channel.

acteristic is a singlet aspheric lens of 230 mm diameter and 2200 mm of focal length. This lens allowed us to get, after 143 km of propagation, a beam spot comparable to the dimensions of the primary mirror of the receiving telescope in order to maximize the power transfer between the two parties. To compensate the beam wandering induced by the atmosphere, we implemented a feedback loop for controlling the transmitting direction: the fiber delivering the signal to the transmitter was mounted on a X-Y-Z movable stage placed close to the focal place of the 230 mm lens, with computer controlled stepped motors. On this same stage, we mounted a CCD sensor which acquired a green (532 nm) "beacon" laser sent by Tenerife toward Alice telescope. The camera is placed in order to measure an image of the singlet focal plane: the wandering of the beacon on the CCD was then analyzed in real time by a software that moves the X-Y-Z stage to compensate the movement of the beacon spot on the camera.

At the receiver part (Bob), in Tenerife, we used the 1 m aperture telescope of the ESA Optical Ground Station to receive the signals. After the Coudè path, we collimated the beam and the classical and quantum signal (at different wavelength) were divided by a dichroic mirror. The qubits were measured in two bases, using PBS and waveplates. T he counts detected by the two single-photon avalanche photodiodes(SPAD) were stored on a FPGA. The probe beam is detected by an high-bandwidth APD (avalanche photodetector) and then registered and stored by an oscilloscope.

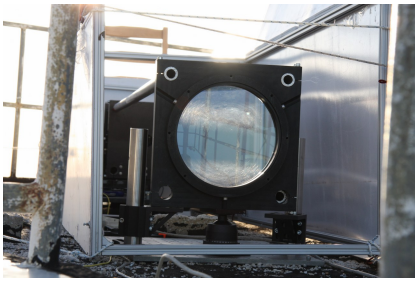
For what concerns the transmitted qubits, in order to measure the QBER of the channel, we used the same data structure of a recent free-space QKD implementation based on the B92 protocol (see Chapter 2). A raw key is composed into N packets of 2880 bits each, sent at the rate of 2.5 MHz; as regards the payload slots, Alice sends two qubits separated by 200 ns. Due to communication with the FPGA, each packets is sent every 20 ms resulting in an average sending rate of 150 kHz. The two FPGAs are synchronized every second by a pulse-per-second (pps) signal equipped by two GPS receivers located in the two islands.

We want to point out that at the transmitter side, the pulses contain in average more than one photon, while at the receiver side we work in the single photon regime. Our aim, in fact, was to simulate a possible realistic scenario where one would employ fast (hundreds of MHz to GHz) free-space QKD

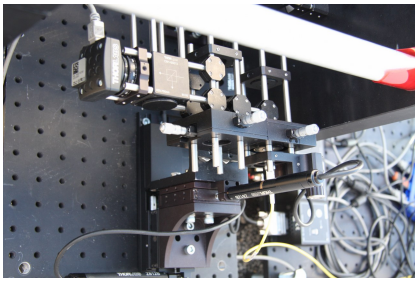
systems which are nowadays commonly available. Since our system has a transmission rate of 2.5 MHz, the detected rate is comparable to the rate observable with a transmitter emitting true single photon pulses with a repetition rate of about 1 GHz, considering fixed the amount of optical and atmospheric attenuation.

3.4 CONCLUSIONS

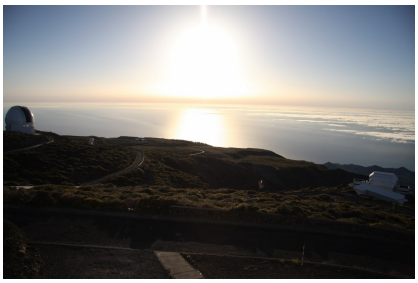
We have presented a proof of principle demonstration of a method exploiting the atmospheric turbulence as a resource for QKD. The turbulence will implies a fluctuating transmissivity of the channel used for quantum communication. The ARTS method, easily integrable in current QKD systems, is based on the sampling of a classical beam (probe signal) sent on the same channel of the quantum bits. By measuring the intensity of the probe at the receiver, it is possible to select in real time the best time slots of high channel transmissivity. We demonstrated that with the ARTS method we were able to decrease the measured QBER; moreover, this method allows to extract secret key in extreme conditions, namely when the initial QBER is above the security threshold of 11%.



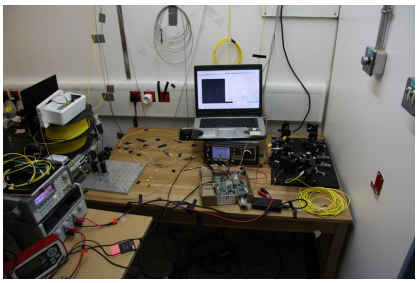
(a) *Transmitter telescope.*



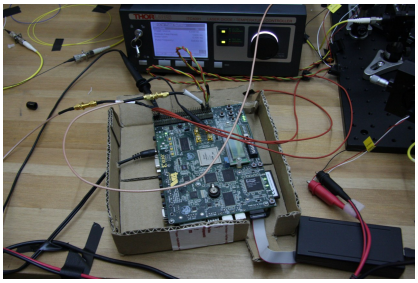
(b) *X-Y stage.*



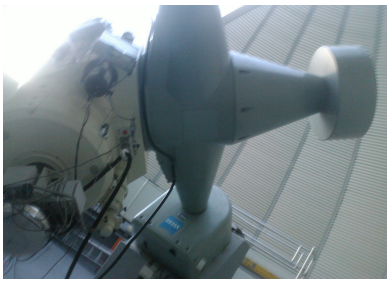
(c) *Sunrise.*



(d) *Laboratory setup.*



(e) *FPGA.*



(f) *Receiving telescope.*

(g) *Telescope detail.*

(h) *OGS.*

Figure 3.9: Pictures of the experimental Canary setup.

4 LINK BUDGET EARTH-SPACE

The most promising application of QKD is the generation of a provably unconditionally secure key at distance, which is not possible with classical cryptography. The use of satellites allows QC on a global scale, an impossible task on ground with current optical fiber technology, in which the signal loses intensity at long distances. One of the fundamental requirement in order to do QC in a Earth-Space channel, is that the degree of polarization is maintained during all the communication process.
Previous works made by Paolo Villoresi's group demonstrate its feasibility [17, 18, 111]; on the basis of these results, in this chapter we present available simulation about the achievable key rate, and a small review about the complexity of the experiment due to the intrinsic limit of the devices. The formulas and formalism used in next sessions were introduced by John J. Degnan [32]. The most important parameter in a communication system is the attenuation factor, also known as link-budget, which depending of his value introduces limitations in the final performance.

A link budget is the accounting of all the gains and losses from the transmitter, through the medium (free space, cable, waveguide, fiber, etc.) to the receiver in a telecommunications system. In the next sessions we take in exam a possible link budget between Earth and satellite, intersecting knowledge of classical optical communications with radio telecommunications. Considering the fact that we works with very distant targets, it is not possible to be sure of the value of all the parameters. In fact in the case of very large losses, small variations of them (e.g. in the weather conditions) could cause significant differences in the parameters and consequently in the attenuation factor.

4.1 LINK EFFICIENCY

As for any classical communication scheme, to analyze and model the setup, it is necessary to known the attenuation factor of the link and the noise introduced in the system. In particular QC are weaker than classical, in fact information is coded at single photon level [96], and in this way the signal cannot be increased: therefore a sufficient SNR can be achieved only reducing the link attenuation and the background noise.

As discussed in Chapter 3 on page 45, the main factor limiting the free-space optical communication link is atmospheric turbulence. The refractive index inhomogeneities induced by turbulence increase the beam spreading to an extent significantly larger than what caused by diffraction.

Depending on their size, the turbulence eddies can cause two main effects: beam wandering, if their dimension is large compared with the beam size; beam broadening on the contrary [33].

In a real orbiting scenario, from an Earth station point of view (OGS), the satellite is seen rising, orbiting and setting at different positions in the sky, related to its orbit. At each time the satellite position can be defined, in the Earth station reference system, by zenith and azimuth angles and

by link distance. The thickness of the atmospheric layers crossed by the beam depends on the zenith angle and, as we will show in the following, influences the beam propagation and the link budget.

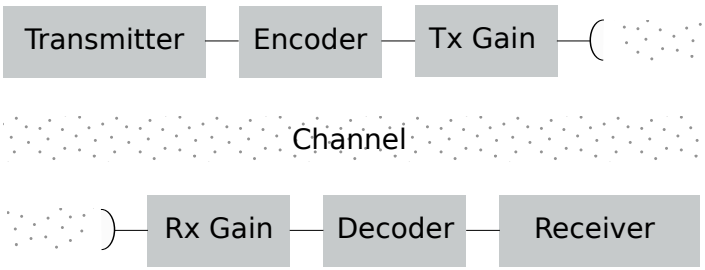


Figure 4.1: Base scheme of a telecommunications system.

4.2 UP-LINK AND DOWN-LINK SCENARIO

The communication systems can be subdivide in three principal group: unicast, multicast and broadcast. The difference is based on how many users attend to the same communication.

- Unicast: communication between one source and one user
- Multicast: communication between one source and many users
- Broadcast: communication between one source and all the users.

In addition to this type of division, it is possible to distinguish between the choice of the transmission medium in:

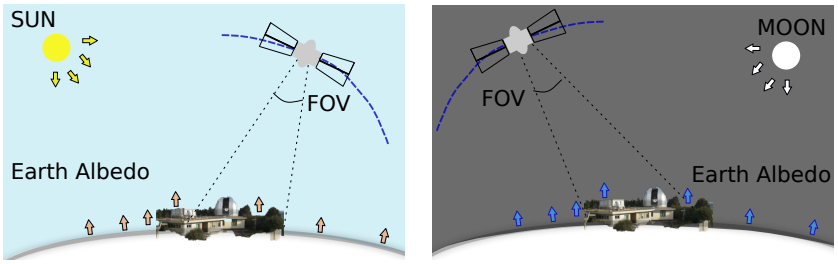
- Half-duplex it is not possible to send and receive contemporary messages
- Full-duplex: it is possible to send and receive contemporary messages

In the case of satellite communications, it is possible to differentiate two different scenario: the first one where the transmitter is in space and the base stations are positioned at Earth. This case is known as *down-link scenario*. The other case take into account a receiver satellite orbiting around the Earth and the base stations work as transmitter. This possibility is known as *up-link scenario*. In the following section we describe the pro and cons of the two cases, highlighting which could be the best choice for a future quantum satellite.

4.2.1 *Beam size distortions*

To investigate the feasibility of QC, we have to take into account the distortions introduced by the atmosphere that could downgrade the performance of the link. A more detailed analysis is reported in Chapter 3. A Gaussian beam of waist w_0 and intensity I_0, has an average spatial distribution of intensity, given by [33, 17]:

$$\langle I(r,L)\rangle = I_0 e^{-2r^2/w_{LT}^2} \tag{4.1}$$



(a) *Daytime operation.* (b) *Nightime operation.*

Figure 4.2: Model for the uplink day-time and night-time background noise estimation considering the two different sources of noise.

where r is the radial distance from the center of the beam, L is the link distance and w_{LT} is the long-term beam radius defined as: $w_{LT}^2 = w_{ST}^2 + 2\langle\beta^2\rangle$. Here β is the instantaneous beam displacement from the unperturbed position, while w_{ST} is the short-term beam width. The long-term beam width, for a collimated beam, is:

$$w_{LT}^2 = w_0^2\left(1 + \frac{L^2}{Z_0^2}\right) + 2\left(\frac{4L}{Kr_o}\right) \tag{4.2}$$

where Z_0 is the Rayleigh parameter of the beam, and r_0 is the Fried parameter (for the uplink scenario), see Chapter 3.

$$r_0 = \left[0.423\sec(\theta_{zen})k^2\int_{h_t}^{L} C_n^2(z)\left(\frac{L-z}{L}\right)^{5/3} dz\right]^{-3/5} \tag{4.3}$$

For a circular or a near circular orbit, the effective link distance, also known as slant range L, considering the geometry formed by an orbiting satellite and an Earth station is given by the equation:

$$L = -(R_E + h_t)\cos\theta_{zen} + \sqrt{(R_E + h_t)^2\cos^2\theta_{zen} + 2R_E(h_s - h_t) + h_s^2 - h_t^2} \tag{4.4}$$

where R_E is the Earth radius (6378 km), h_t is the station height above sea level, h_s is the satellite height above sea level, and θ_{zen} is the zenith angle of the satellite as observed from the station.
Using these formulas, the short-term beam radius can be estimated as:

$$w_{ST}^2 = w_0^2\left(1 + \frac{L^2}{Z_0^2}\right) + 2\left\{\frac{4.2L}{kr_0}\left[1 - 0.26\left(\frac{r_0}{w_0}\right)^{1/3}\right]\right\}^2 \tag{4.5}$$

It appears very clear that the turbulence effect has to be summarized by an additive factor to the Gaussian beam. In order to compensate the turbulence effect with an accurate pointing system, it could works also if the beam displacement β is higher than w_{ST}. In the present simulation we deal with a worst-case scenario, where the β is uncompensated. The effects of turbulence could be summarized in a redistribution of the beam energy, in fact the power P collected by a receiver can be estimated as:

$$P = \int_0^R \rho e^{-2(\rho^2/w_{LT}^2)} d\rho \tag{4.6}$$

where R is the radius of the telescope. The probability of photons detection could be derived from the ratio between the transmitted and received power as:

$$\eta = \eta_0 \left(1 - e^{2R^2/w_{LT}^2}\right) \tag{4.7}$$

considering the detection efficiency, the pointing losses and the atmospheric attenuation: the factor η_0 can be approximable set to 0.1 at the zenith [7, 47]. More in general η_0 can be related to the zenith angle by the following equation that is an accurate approximation up to 70°.

$$\eta_0 = \eta_P \, \eta_{TX} \, \eta_{RX} \cdot 10^{\left(-\frac{4.34\,\tau(0)\sec(\theta_{zen})}{10}\right)} \tag{4.8}$$

where η_P , η_{TX} , η_{RX} are the pointing losses, the transmitter losses and the receiver losses. τ is the depth of path at the zenith, that given the atmospheric transmittance ($\simeq$ 0.8 at 800 nm) $T = e^{-\tau}$. In a downlink scenario, where the source is orbiting and considering an optical beam it encounters the atmosphere only in the last path of the channel.
This fact is very important because the effects of the turbulence are weaker than up-link or horizontal link; in fact the turbulent eddies affecting the beam are much smaller than beam diameter. Beam wandering become negligible compared to the beam spreading due to the short-term effect. Moreover in this case, beam spreading are less strong than the uplinlk. All this considerations, de facto implies a lower attenuation factor in a downlink scenario respect to the up-link one.

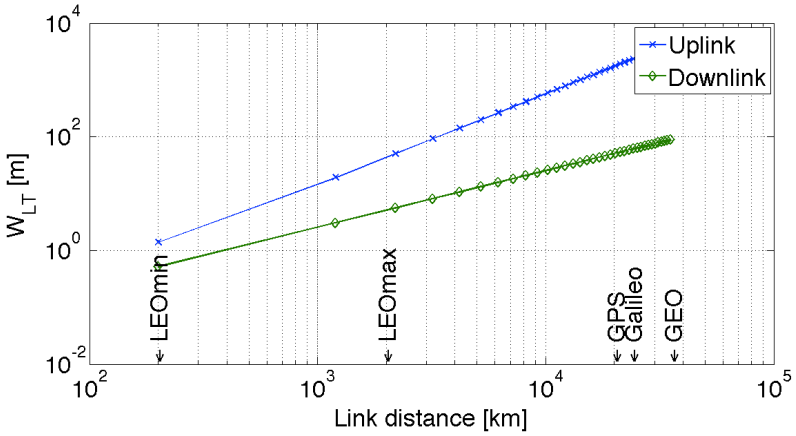


Figure 4.3: Long term beam width w_{LT} as a function of the link distance L. Simulation with an Earth telescope radius $r_T = 75$ cm and a space telescope radius $R = 10$ cm.

In the next sections we will report a method to investigate the background noise and the major sources of noise, in the case of down-link and up-link scenario.

4.2.2 *Up-link daytime operation*

In the case of uplink scenario during daytime operation, Sun represents the major source of background noise. Scattered light (assuming a Lambertian

diffusion model) diffused by the Earth is collected by the telescope [17]. In Figure 4.2 is reported a generic scheme of an up-link Earth satellite communication. It is possible to estimate the number of background photons collected by the receiver system, as a function of bandwidth units and time units $\Delta\nu[nm]$, $\Delta t[s]$.

$$N_{B_{day}} = a_E \frac{A_t}{\pi} (\text{IFOV}^2) H_{sun} \tag{4.9}$$

where a_E is the Earth albedo; A_t is the area of the telescope in space; IFOV is the telescope field of view; H_{Sun} is the solar spectral irradiance (photons s^{-1} nm^{-1} m^{-1}).

4.2.3 *Up-link nightime operation*

In the same way, it is possible to analyze the background noise for an up-link scenario during night-time operation. The dominant sources of noise are the Earth black-body emission, scattered light from human activities and diffused moonlight. The noise related by moonlight can be evaluated by:

$$N_{B_{night}} = a_E \, a_M \, R_M^2 \frac{A_t}{\pi} \frac{\text{IFOV}^2}{d_{EM}^2} H_{sun} \tag{4.10}$$

where a_M is the Moon albedo; R_M is the Moon radius; d_{EM} is the Earth–Moon distance. It can be assumed that the noise due to Earth black-body radiation can be negligible for a real QKD system. Numerical estimation shown that it is three order of magnitude less that of moonlight [17].

4.2.4 *Downlink background noise*

From the equation above reported and following the articles [17] and [19], the noise power received by the telescope is:

$$Pb = H_{bk} \, \Omega_{fov} \, A_t \, \Delta\nu \tag{4.11}$$

where H_{bk} is the brightness of the sky background [W m^{-2} sr^{-1} μm^{-1}]; Ω_{fov} is the field of view of the telescope in [sr]; A_t is the receiving telescope area at the Earth station; $\Delta\nu$ is the optical bandwidth [μm].

4.2.5 *Signal to noise ratio*

One the most important parameter in a communication system is the SNR, because depending of his value it is possible to estimate the number of expected errors introduced in the transmission. The SNR is defined as the ratio between the single photons of signal and the noise photons at the receiver:

$$SNR = \frac{\text{Signal}}{\text{Noise}} = \frac{\eta}{\epsilon_N} \tag{4.12}$$

where ϵ_N is the number of noise photons with a detection time Δt for a bandwidth Δv.

We can distinguish two different formulas for uplink and downlink scenario:

$$SNR = \frac{\eta_0(1-\exp(-2A_t/(\pi w_{LT}^2)))d_{EM}^2}{a_E a_M R_M^2 IFOV^2 H_{sun}} \tag{4.13}$$

$$SNR = \frac{\eta_0(1-\exp(-2A_t/(\pi w_{LT}^2)))h\nu}{H_b \Omega_{fov} A_t \Delta v \Delta t} \tag{4.14}$$

where h is the Planck constant. The contribution due to an imperfect QKD system is neglected in this definition. We omit the formula in the case of daytime operation, because due to the high level noise and it results unfeasible a positive SNR.

4.3 RADAR EQUATION

Each equation written until now, was based on the hypothesis that a orbiting satellite, equipped with a transmitter or a receiver is nowadays available. Unfortunately, we have mentioned a lot of times the lack of a quantum satellite. Although we decide to experimentally simulate a quantum transmitter using the Corner Cube Retroreflectors (CCRs) mounted in SLR satellites. In this perspective we are going to introduce some basic principle, useful to understand the experiments presented in Chapter 5 and in Chapter 6. For the complete description on how a SLR system works and a more detailed analysis we invite the reader to see [32].

Thanks to the SNR equation it possible to estimate the expected number of photons in the case of uplink and downlink:

$$\eta_p = \eta_{det}\left(E_T\frac{\lambda}{h\nu}\right)\eta_{tx}G_t\Sigma\left(\frac{1}{4\pi L^2}\right)A_t\eta_{rx}T_a^2T_c^2 \tag{4.15}$$

where η_{det} represents the detector quantum efficiency, E_T is the laser pulse energy, λ is the laser wavelength, h the Planck's constant, c the speed of light in vacuum, η_{tx} and η_{rx} the optical efficiency of transmitter and receiver, Σ is the satellite cross section, L is the distance between satellite and base station, A_t the effective area of the telescope receive aperture, T_a is the one-way atmospheric transmission and T_c is the one way transmissivity of cirrus clouds (if present).

In the following subsections we will enter into detail, reporting from Degnan paper [32], the individual terms of the link equation (4.15) . Every single terms should be discussed for a complete description and analysis of a SLR system, but we will describe only the important terms for our experiments.

4.3.1 *Transmitter gain*

Usually a SLR station is equipped by a mode-locked laser which produce a quasi-gaussian spatial and temporal profiles of the wave front. The transmitter gain for a gaussian beam is given by the expression:

$$G_t(\theta) = \frac{8}{\theta_t^2}\exp\left[-2\left(\frac{\theta}{\theta_t}\right)^2\right] \tag{4.16}$$

where θ_t is the half-angle far field divergence, between the beam center and $1/e^2$ intensity point and θ is the beam pointing error[1]. Pointing stability can

1 Pointing Error is the angular rotation from the desired pointing direction, or in other words it is the difference between the actual pointing direction and the desired pointing direction.

be affected both by internal and external number of factors (e.g. physical motion, heat buildup, cavity instability, air currents). Typical values for θ_t in SLR system fall between 50 and 75 mircoradians ($10 - 15$ arcseconds) which implies a transmitter gain about $G_t = 1.4 \cdot 10^9$.

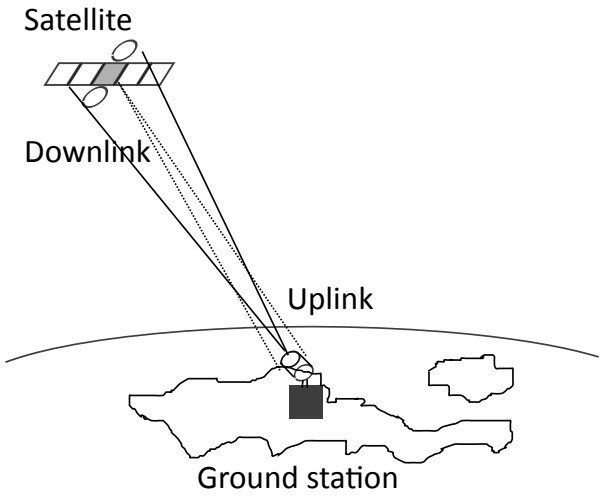


Figure 4.4: Sketch of SLR facilities defining uplink and downlink channel.

Atmospheric turbulence, describe in Chapert 3, introduce particular effects to the beam and also set a lower limit to the minimum bundle divergence that can be achieved. In propagation trough the amount optical system, in our case trough the Coudé path, the beam profile is usually radially truncated by some limiting aperture and sometimes centrally obscured by the secondary mirror. In a far field analysis the loss due to the secondary mirror, produces secondary rings around the main central lobe. In order to consider this phenomena in our experiment, a general expression for the transmitter gain is given by:

$$G_t = \frac{4\pi A_t}{\lambda^2} g_t(\alpha_t, \beta, \gamma_t, X) \tag{4.17}$$

where $A_t = \pi a_t^2$ is the area of the transmitting aperture and $g_t(\alpha_t, \beta, \gamma_t, X)$ is a geometric factor. Usually if the target is in the far field of the transmitter the expression become:

$$g_t(\alpha_t, \beta, \gamma_t, X) = \left(\frac{2}{\alpha_t^2}\right)(e^{-\alpha_t^2} - e^{-\gamma_t^2 \alpha_t^2}) \tag{4.18}$$

where $\alpha_t = a_t/w$ and $\gamma_t = b_t/a_t$ and a_t is the radius of the primary transmitting aperture, w is the gaussian beam waist, and b_t is the radius of an obscuring secondary mirror.

The transmitter gain, as it is possible to see from (4.17) is proportional to the inverse square of the wavelength. This factor implies a higher degree of collimation for shorter wavelengths and must be taken into account in the phase of design of the optical experiments.

4.3.2 *Cirrus Cloud*

The presence of smog, fog and low clouds prevents the optical transmission; moreover also in the case of very high humidity good data is not guarantee. However, even when skies appears clear and weather conditions seems good, sub-visible cirrus clouds are overhead about 50% of the time at most locations. A global study of cloud thickness compute a mean cirrus cloud thickness, when present of 1.341 km [45]. Experimentally it is proved that cirrus transmittance is given by the equation

$$T_c = \exp[-0.14(t \sec \theta_{zen})^2] \tag{4.19}$$

where t is the cirrus cloud thickness and θ_{zen} is the zenith angle.

4.3.3 *Retroreflector characteristics*

In order to characterize the reflected optical beam, we have to study the internal structure of the CCRs. For normally incident light, a single unspoiled retroreflector has a peak optical-cross section Σ_{cc} defined by:

$$\Sigma_{cc} = \rho A_{cc} \left(\frac{4\pi}{\Omega} \right) = \rho A_{cc} \left(\frac{4\pi A_{cc}}{\lambda^2} \right) \tag{4.20}$$

where ρ is the cube corner reflectivity (decreases with the passage of time), $A_{cc} = \pi R_{cc}^2$ is the light collecting area of the corner cube, and $4\pi/\Omega$ is the on-axis retroreflector gain. Ω is the effective solid angle occupied by the far field diffraction pattern (FFDP) on the retroreflector.
For a circular entrance aperture, the FFDP of the reflected wave is the familiar function given by:

$$\Sigma(x) = \Sigma_{cc} \left(\frac{2J_1}{x}(x) \right)^2 \quad x = kR_{cc} \sin(\theta) \tag{4.21}$$

and θ is the angle from the cube face normal. At arbitrary incidence angle, the area A_{cc} is reduced by the factor

$$\eta(\theta_{inc}) = \frac{2}{\pi} \left(sin^{-1}\mu - \sqrt{2} \tan \theta_{ref} \right) \cos \theta_{inc} \tag{4.22}$$

where θ_{inc} is the incident angle and θ_{ref} is the internal refracted angle as determined by Snell's law: $\theta_{ref} = sin^{-1}[\sin(\theta_{inc}/n)] \quad \mu = (1 - 2\tan^2 \theta_{ref})^{1/2}$ where n is the cube index refraction. Thus the peak optical cross-section in the center of the reflected lobe falls off as:

$$\Sigma_{\text{eff}}(\theta_i nc) = \eta^2(\theta_{inc})\Sigma_{cc} \tag{4.23}$$

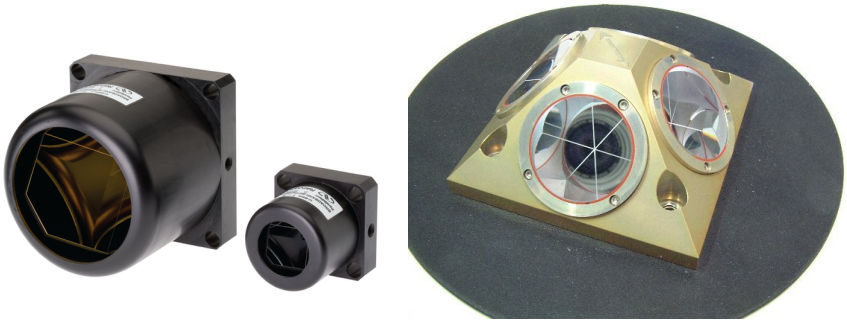
One can further limit the effective incidence angle over which the retroreflecter responds by recessing the retroreflctor in its holder. It can be easily shown that the effective are of the elliptical entrance aperture, as limited by the recess, is given by:

$$A_{eff}(\theta_{inc}) = A_{cc} \left(1 - \frac{\tan \theta_{inc}}{\tan \theta_{max}} \right) \tag{4.24}$$

where $\theta_{max} = \cot^{-1}(d/D_{cc})$ and $D_{cc} = 2R_{cc}$.

Table 4.1: Current and revised cross section for the SLR satellites.

Satellite	Altitude [km]	Current [$10^6 m^2$]	Revised [$10^6 m^2$]
Starlette	815	0.65	1.8
Lageos-1	5850	7	15
Lageos-2	5625	7	15
Etalon-1	19105	60	65
Etalon-2	19135	60	65
BeaconC	927	3.6	13
Ajisia	1485	12	23
Stella	815	0.65	1.8
Jason-1	1336	0.3	0.8
GPS	20030	40	19
Envisat	800	0.3	0.85
Larets	691	0.5	0.6
Lares	1450	3.2	3



(a) *Spoiler CCR.* (b) *Unspoiler CCR.*

Figure 4.5: Example of spoiling and non spoiling satellite CCRs. On the left it is possible to see the spoiling retroreflector, in fact the mirrors are positioned inside the ring of the structure. On the right it is possible to note that there aren't any structure before the CCR.

4.3.4 *Velocity aberration*

The far field diffraction pattern (FFDP) of a cube corner with a circular entrance pupil consists of a principle main lobe surrounded by low intensity rings. In the case of no relative motion between the satellite and the target, the retroreflected FDFP should be centered in FOV of the telescope. Due to the relatively motion between satellite and the base station the FFDP results in a different position respect to the ideal one. The magnitude of the angular displacement in the FFDP is given by the equation: The

$$\alpha(h_z, \theta_{zen}, \omega) = \alpha_{max}(h_z)\sqrt{cos^2\omega + \tau^2(h_z, \theta_{zen})\sin^2\omega} \tag{4.25}$$

where the maximum value, α_{max} and $\tau^2(h_z, \theta_{zen})$ is given by the expression

$$\alpha_{max} = \frac{2}{c}\sqrt{\frac{R_B^2 g}{R_E + h_s}}$$
$$\tau^2(h_z, \theta_{zen}) = \sqrt{1 - \left(\frac{R_E \sin\theta_{zen}}{R_E + h_s}\right)^2}$$

and R_E is the Earth radius, $g = 9.8\ \mathrm{m}/s^2$ is the gravitational acceleration at the surface, h_s is the satellite height above sea level, c is the speed of light and the angle $\omega = \cos^{-1}[(\hat{r}x\hat{p}) \cdot \hat{v}]$ where $\hat{r}$ is the position vector in the satellite direction, $\hat{p}$ the line-of-sight from station to satellite, and $\hat{v}$ the satellite velocity vector respectively.

4.3.5 *Retroreflector spoiling*

In the case we want to decrease the loss due to the velocity aberration effect, there exist a "spoiler" for CCRs (see Figure 4.5). The goal of spoiling is to concentrate more reflected energy into the annular region bordered by α_{max} and α_{min}. Ideally an optimum cross-section is given by:

$$\Sigma_{ideal} = \rho A_{cc}\left(\frac{4\pi}{\Omega_{cc}}\right) = \rho A_{cc}\left(\frac{4\pi}{\alpha_{max}^2 - \alpha_{min}^2}\right) \tag{4.26}$$

where $4\pi/(\alpha_{max}^2 - \alpha_{min}^2)$ is the ideal effective target gain and ω_{cc} is solid angle subtended by the annular ring of interest. A particular behavior of the spoiler is that it introduces a slight variations into the cube corner dihedral angles, complicating the FFDP. In fact in the case of normal incident beam the initial single main Airy breaks into $2N$ lobes distributed within an angular annulus. Each of the $2N$ lobes are created from a different sector of the CCR entrance aperture. Because the distribution of energy within this "annulus" is therefore highly nonuniform, the effective area for each lobe is reduced to:

$$A_{eff} = \eta(\theta_{inc})\frac{A_{cc}}{2N} \tag{4.27}$$

We can obtain an approximate expression of the peak intensity centered in one of the $2N$ lobes, substituting the latter equation into the (4.20):

$$\Sigma_{peak}(\theta_{inc}, N) = \eta^2(\theta_{inc})\frac{\Sigma_{cc}}{4N^2} \tag{4.28}$$

4.3.6 *Satellite optical cross-section*

The satellites cross section Σ, from a theory point of view achievable with a single CCR must take into account the limitation due to the velocity aberration effects. The received signals can be approximated as a sum of all the contribution of several CCRs. Also for this reason modern geodetic satellite, like Starlette, Lageos and Etalon are sphere in order to avoid the spreading caused by the reflection of the flat panel array. The array size of a SLR satellite is above determined by the orbiting distance, in order to achieve a reasonable SNR value. Let's consider a spherical satellite uniformly covered

with CCRs. The density of CCRs as a function of incidence angle could be approximated to:

$$N(\theta_{inc}) = d\theta_{inc} = \frac{N}{2} \sin\theta_{inc} d\theta_{inc} \tag{4.29}$$

where N is the total number of CCRs on the satellite. An approximated relation is given by the following integral:

$$\Sigma = \Sigma_{cc} \int_0^{n/2} d\theta_{inc} N(\theta_{inc}) \eta^2(\theta_{inc}) \tag{4.30}$$

If the CCRs are not recessed in their holders, $\eta(\theta_{inc})$ is given by (4.22). If their angular response is limited by the recess, (4.24) suggests that the variation can be well-approximated by the expression $\eta(\theta_{inc}) = 1 - (\theta_{inc}/theta_{max})$ where θ_{max} is given by (4.3.3). Substituting the equations (4.29) and (4.3.6) into (4.30) and evaluating the results integral yields a simple expression for the target cross-section:

$$\Sigma = \frac{\Sigma_{cc} N}{2} \left[1 - \frac{sin^2(\frac{\theta_{max}}{2})}{(\frac{\theta_{max}}{2})^2} \right] \tag{4.31}$$

4.4 CONCLUSION

In this chapter we present a sort of a review equations about satellite optical communications and radar link. They would be very useful for a complete description of the next experiments, reported in Chapter 5 and Chapter 6. We would like to underline that these formulas are not derived by me, but they are reported from a paper made by John Degnan [32] which has studied for years SLR facilities.

5 POLARIMETER

In order to achieve QKD through a Earth-Space channel, in the case of polarization encoding protocols (simplest) the degree of polarization of the transmitted radiation must be preserved. It allows the exchange of cryptographic keys from a sender (Alice) to a receiver (Bob). A possible way to verify this fundamental requirement is to study the space channel using Laser Ranging system and a polarimeter. In a SLR system the reflection is done by optical components called CCRs, which ensure that the laser beam is reflected back to the telescope direction.
At present time, the behavior of polarization reflected by a CCRs is well known, in particular it has been widely proved that devices with a metal coated reflecting surface maintain the degree of polarization, while the ones without it cause a depolarizing effect on the incident beam. This was also verified experimentally at LUXOR CNR laboratory in Padova. For these reasons, satellites equipped with CCRs are expected to maintain the polarization state of the laser ranging pulse.

In addition to the above descriptions, the Mueller matrix of the telescope was measured at different positions, in order to study how it affects the polarized laser pulse that passes through it. Secondly, using Jones' formalism, a model of the overall system (telescope-satellite-telescope- polarimeter) was made, so as to create a reference for the observations. If one assumes a Jones matrix for the CCRs mounted on satellite equal to the one of a plane mirror, it can be demonstrated that the considered experimental setup should maintain the chosen polarization state from one end to the other, regardless of the telescope position.

5.1 POLARIZATION LIGHT

The first part of this chapter is only propaedeutics for a complete description of an optical polarized beam, and for the complete understanding of the presented experiment. The classical concept of polarized light refers to the wave polarization state as a time evolving function of its electric field vector **E**. If the extremity of the vector describes a stationary curves during the observation time, the wave is defined as *polarized*, otherwise if the vector takes random positions the wave is defined *unpolarized*.
Polarization is a property of electromagnetic radiation, describing the shape and orientation of the locus of electric field vector extremity as a function of time, at a given point of space.
When light passes through a medium or in the case that it is reflected by a target, its polarization is modified. Variations in the state of polarization of a wave enable the possibility to characterize every component of optical systems. The electric field vector of a monochromatic or quasi-monochromatic wave, can be expressed in terms of three orthogonal components in the

right-handed Cartesian coordinate system. For a wave propagating over the z direction, the instantaneous electric field vector, can be expressed as:

$$\mathbf{E}(z,t) = \begin{bmatrix} E_x(z,t) \\ E_y(z,t) \end{bmatrix} = \begin{bmatrix} E_{0x}\,\cos(\omega t - kz + \varphi_x) \\ E_{0y}\,\cos(\omega t - kz + \varphi_y) \end{bmatrix} \tag{5.1}$$

From (5.1) we can obtain the locus of the extremities of the electric filed vector:

$$\left(\frac{E_x}{E_{0x}}\right)^2 + \left(\frac{E_y}{E_{0y}}\right)^2 - 2\frac{E_x\,E_y}{E_{0x}\,E_{0y}}\cos\varphi = \sin^2\varphi \tag{5.2}$$

where $\varphi = \varphi_x - \varphi_y$. The above equation can degenerate in a circle or in a line depending on which polarization are we considering. The corresponding polarization will be defined as: elliptical right-handed ($\pi < \varphi < 0$), elliptical left-handed ($0 < \varphi < \pi$), circular ($\varphi = \pm\pi/2$) and linear ($\varphi = 0, \pi$).

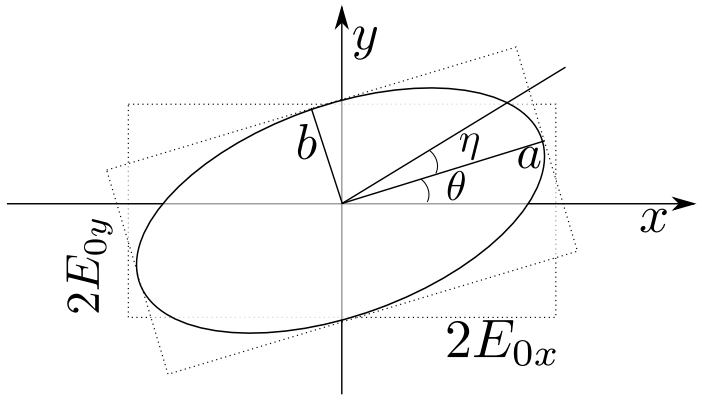


Figure 5.1: Ellipse of polarization.

In the Figure 5.1 the elliptical polarization is reported. It lies in a rectangle of dimension $2E_{0x} \times 2E_{0,y}$. Each polarization state can be unequivocally described:

$$\begin{cases} \eta = \text{ellipticity} \\ \theta = \text{azimuth} \\ \nu = \tan\nu = \frac{E_{0y}}{E_{ox}} (0 \leq \nu \leq \pi/2) \end{cases} \tag{5.3}$$

This parameters are related to the electric field vector by the following equation:

$$\begin{cases} \tan 2\theta = \tan 2\nu \cos\varphi \\ \tan 2\varepsilon = \pm \sin 2\theta \tan\varphi \\ \tan\varepsilon = \pm\frac{b}{a} \quad (-\pi/4 < \varepsilon \leq \pi/4) \end{cases} \tag{5.4}$$

where $\tan 2\nu = 2(E_{0x}E_{0x})/(E_{0x}^2 - E_{0y}^2)$, $a^2 + b^2 = E_{0x}^2 - E_{0y}^2$ and $\pm ab = E_{0x}E_{0y}\sin\varphi$.

5.1.1 *Jones formalism*

A very common representation of the electric field vector, can be obtained using column complex vector: $\mathbf{E} = \begin{bmatrix} E_{0x}e^{i\varphi_x} & E_{0y}e^{i\varphi_y} \end{bmatrix}^\dagger$ with this math structure, each optical system can be modelled trough 2×2 complex matrix, called Jones representation matrix. If $\mathbf{E_i}$ denotes the Jones vector of an incident wave to an optical system, described by its Jones matrix J, the outgoing waves $\mathbf{E_o}$ is related to that by: $\mathbf{E_0} = J\mathbf{E_i}$. In the case of a series of optical system, the total electric field can be expressed by the product of every single Jones matrices. Following the wave propagation direction: $\mathbf{E_0} = J_n \cdot J_{n-1} \dots J_2 \cdot J_1 \cdot \mathbf{E_i}$. where J_1 is the first device and J_n represents the n^{th}.

5.1.2 *Stokes parameters*

Jones representation does not take into account the depolarization channel. To extend and complete the model we need to introduce Stokes parameters. A Stokes vector is structured by four parameters: S_0 proportional to the total density of power of the wave, S_1 proportional to the density power in the vertical and horizontal polarization, S_2 proportional to the density power in the $+45°$ or $-45°$ polarization degree, S_3 is proportional to the left-handed and right-handed polarization. They represent the amplitude, phase and polarization of a wave and are defined by:

$$\begin{cases} S_0 = \langle E_x^2 \rangle + \langle E_y^2 \rangle \\ S_1 = \langle E_x^2 \rangle - \langle E_y^2 \rangle \\ S_2 = 2\langle E_x E_y \cos\varphi \rangle \\ S_3 = 2\langle E_x E_y \sin\varphi \rangle \end{cases} \tag{5.5}$$

where $\varphi = \varphi_x(t) - \varphi_y(t)$ represents the difference in phase between x and y components. The $\langle\rangle$ operator is the temporal average on the measurement time. In the case of a completely polarized wave, the parameters vector (5.5), becomes:

$$\begin{cases} S_0 = \langle E_x^2 \rangle + \langle E_y^2 \rangle \\ S_1 = \langle E_x^2 \rangle - \langle E_y^2 \rangle \\ S_2 = 2E_x E_y \cos\varphi \\ S_3 = 2E_x E_y \sin\varphi \end{cases} \tag{5.6}$$

where $S_0^2 = S_1^2 + S_2^2 + S_3^2$.
For an unpolarized wave, the position of the electric field vector is undetermined. Considering a temporal average on the measurement time we can write:

$$\langle E_{0x}^2 \rangle = \langle E_{0y}^2 \rangle \tag{5.7}$$

$$\langle E_{0x}\, E_{0y} \cos 2\varphi \rangle = \langle E_{0x}\, E_{0y} \rangle \langle \cos 2\varphi \rangle \tag{5.8}$$

$$\langle E_{0x}\, E_{0y} \sin 2\varphi \rangle = \langle E_{0x}\, E_{0y} \rangle \langle \sin 2\varphi \rangle \tag{5.9}$$

the phase variation are equally distributed between $-\pi$ and π. It follows that: $\begin{bmatrix} S_0 & S_1 & S_2 & S_3 \end{bmatrix}^\dagger = S_0 \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}^\dagger$

DECOMPOSITION THEOREM As reported in the previous paragraph, the Stokes vectors can be used both with polarized and unpolarized waves. The formalism enables to express the incoherent superposition of two light waves. The vector S^i of a partially polarized waves (PP) can be decomposed into two parts: a completely polarized (CP) wave, and a non-polarized wave (CD); this decomposition is unique:

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} S_0 - \sqrt{S_1^2 + S_2^2 + S_3^2} \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} \sqrt{S_1^2 + S_2^2 + S_3^2} \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} \tag{5.10}$$

$$PP = CD + CP$$

COHERENCE MATRIX AND DEGREE OF POLARIZATION The coherence matrix (polarization matrix) is defined as the temporal average of the product of a Jones vector by its Hermitian conjugate:

$$\Phi = \langle \mathbf{E} \otimes \mathbf{E}^\dagger \rangle = \begin{bmatrix} \langle E_x E_x^* \rangle & \langle E_x E_y^* \rangle \\ \langle E_y E_x \rangle & \langle E_y E_y \rangle \end{bmatrix} \tag{5.11}$$

In order to define the degree of polarization on an electric field, we have to connect polarization matrix with the Stokes parameters. It can be done by the following relationship:

$$\Phi = \frac{1}{2} \sum_{i=0}^{3} S_i \sigma_i \tag{5.12}$$

where σ_i represents the Pauli matrices. We can define the degree of polarization as:

$$P = \frac{I_{\text{pol}}}{I_{\text{tot}}} = \sqrt{\left[1 + \frac{4 \det(\Psi)}{T_r(\Phi)^2}\right]} = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0}, \quad 0 \leq P \leq 1 \tag{5.13}$$

If the measured $P = 0$, it means that the wave is not polarized, otherwise if $P = 1$ the wave is completely polarized.

5.1.3 *Poincaré sphere*

An useful graphical representation of the polarization states is the Poincaré sphere. Each point of the sphere is uniquely associated to a Stokes vector. The Stokes parameters S_1, S_2, S_3 correspond to the coordinates of the 3-axes of the sphere. For a completely polarized wave the radius of the sphere results unitary. In the case of optical device where it has a deflated or squeezed sphere, with a radius less than one the polarization parameter will be lower than < 1. The linear polarization state are reported in the equatorial line, while circular states are positioned to the poles of the spere. North hemisphere corresponds to elliptical left-handed states, whereas in the South hemisphere there are right-handed elliptical states.

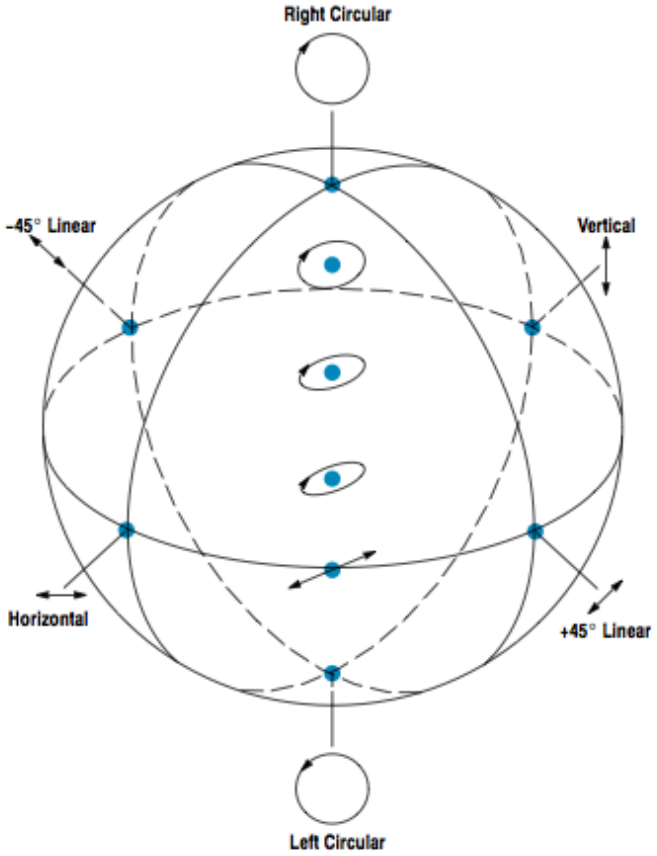


Figure 5.2: Representation of the Stokes vector on the Poincaré sphere.

5.1.4 *Mueller matrix*

We are going to define the last formalism matrix useful for polarization study of an electromagnetic wave. Mueller matrix is a 4×4 matrix, that describes completely the polarimetric behaviour of an optical device. It can be seen as an operator that maps each polarization input state, represented by a Stokes vector, to an output Stokes vector, corresponding to a defined polarization output state: $S_0 = M S_i$. Each Jones matrix, defined in 5.1.1 section, can be rewritten as a Mueller matrix by:

$$m_{ij} = \frac{1}{2} \mathrm{Tr}(J\sigma_j J^\dagger \sigma_i) \tag{5.14}$$

As for the Jones matrices, also in the case of Mueller matrix, a series of optical components can be represented via the products of each matrices: $M = M_n M_{n-1} \dots M_2 M_1$. The Mueller formalism permits better experimental analysis, thanks to the fact that the terms are perfectly measurable. The equation (5.14) can be rewritten as:

$$M_J = A(J \otimes J^\dagger)A^{-1} \tag{5.15}$$

where A is the matrix:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & i & -i & 0 \end{bmatrix} \tag{5.16}$$

5.2 LASER RANGING

The global SLR network station measures the flight time of ultrashort light pulses retroreflected by satellite in order to study the Earth, Atmosphere, Oceans from a geodetic point of view. This technique is very precise in fact it is possible to find out also millimeters changed in the Earth's crust. Moreover it is one of the most accurate method to determine the geocentric position of the satellites around the Earth. Finally but not minor, Laser Ranging results very useful in the study about the variations of the gravity field of the Earth and it allows a very precise modeling evaluating the long-term climate change. The SLR stations joint together with VLBI, GPS, DORIS and PRARE represents an important part of the international network of space geodetic observatories.

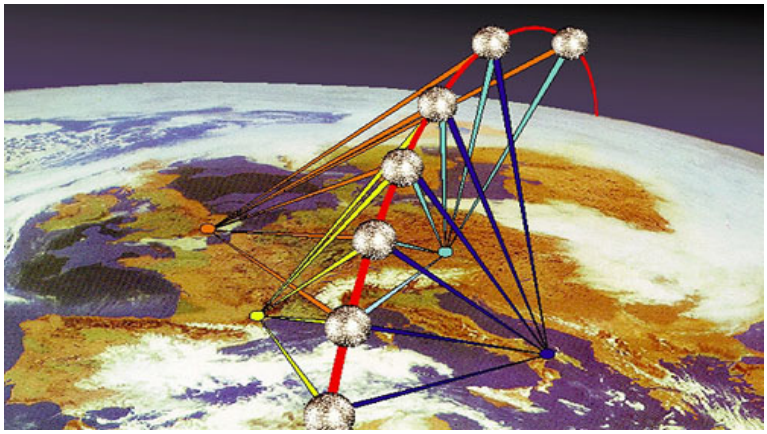


Figure 5.3: Sketch of of Satellite Laser Ranging system. Figure from [2].

5.2.1 *Laser Ranging Operation*

In order to study and implement a quantum space link, a transmitter/receiver on space is needed: this requires an hosting satellite. Due to the lack of this payload, one can use SLR network system to recreate a downlink channel from satellite to Earth. Usually a laser ranging station is equipped with:

- high-speed telescope, able to point and track the laser ranging satellite, normally orbiting in Low Earth Orbit (LEO) range
- high energy pulsed laser
- efficiency detector to receive the retro-reflected laser pulses
- pointing and tracking system

- data logger system to collect the ranging data

The specifics of the Matera Laser Ranging Observatory (MLRO), site of the space link experiments are reported in table 5.1. The parameters are given from NASA in [2]. More information on laser ranging and previous quantum experiments can be found in [100]. Laser ranging satellites are provided with corner cube reflectors, this because of their property of reflecting the incident beam in a counterparallel way, regardless of the angle of incidence.

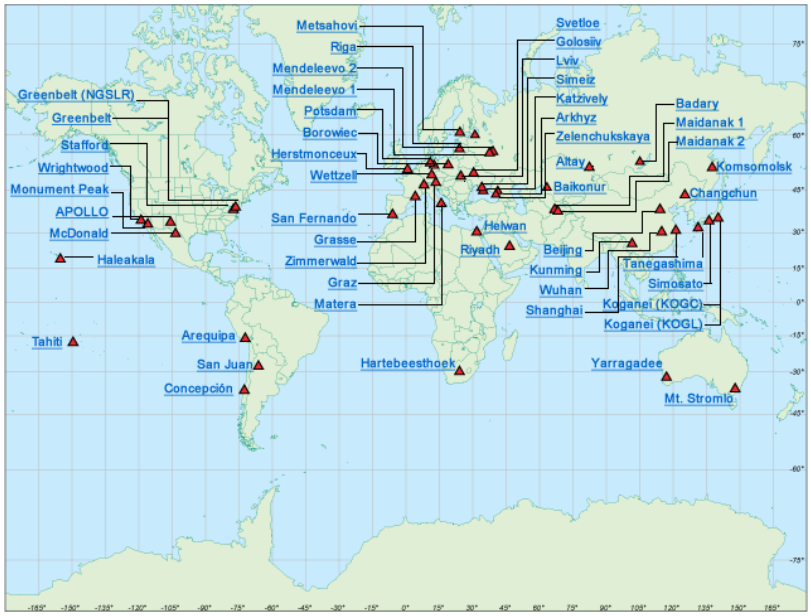


Figure 5.4: Maps of active SLR stations, more informations available at [2].

5.3 EXPERIMENTAL STUDY OF QUANTUM SPACE CHANNEL

The purpose of this experiment is to evaluate the properties of a quantum channel in space within the QKD. The main feature, necessary to develop such a technique, is that the electromagnetic wave used for the signal transmission keeps its polarization state during all the time of propagation. Previous works demonstrate its feasibility [111, 18]; on the basis of these, an instrument capable to measure the state of polarization, in its Stokes vector description, has been developed. The experiment was carried out in Matera, inside the ASI facility, that includes a laser ranging station, MLRO. In order to study the quality of the quantum channel it was used satellites of the International Laser Ranging System, equipped with corner cube reflectors: if the CCRs are metal coated they reflect the incoming beam without modifying its polarization.

5.3.1 *Preservation of polarization*

The corner cube reflector is a structure consisting of three mirrors that are mutually orthogonal so as to constitute a corner of a hollow cube, see Figure 5.6. This structure has the property of retroreflection, so the radiation incident on the CCRs from any direction is eventually reflected back in the

Table 5.1: Specifications of the Matera Laser Ranging Observatory.

Specifications	Measure
Telelscope aperture	1.5 m
FOV	0.016°
Focal length primary mirror	2250 mm
Radius of curvature primary mirror	−4500 mm
Focal length secondary mirror	148.5 mm
Radius of curvature secondary mirror	−297 mm
Back focal length	15 m
Effective focal length	225 m
Laser pulse energy	100 mJ
Laser pulse repetition rate	10 Hz
Laser wavelength	532 nm
Beam divergence angle	45μ rad
Transmission optical efficiency	0.75
Receiving optical efficiency	0.39 (with pass-band filter)
Elevation	536.9 m
Telescope effective area	1.7662 m^2

counterparallel direction. For this reason it is widely used for many applications such as in laser resonators, long-path interferometry, ranging, atmospheric absorption measurements and in road traffic visibility applications. For more complex applications, i.e. plasma polarimetry and interferometry or quantum laser ranging, it is necessary to know how the CCRs modify the state of polarization of the incident radiation. Metal coated corner cubes tend to preserve polarization in contrast to uncoated ones. The mirror symmetry of the trihedral planes (facets) of the corner cube give rise to six regions in the cube. In a glass corner cube, the output beamlet of each region presents a different polarization state, whereas in a metal coated corner cube the output polarization states in all six parts can become identical as in an ideal planar mirror [59, 60]. In non-normal incident irradiation, the polarization properties of the corner cube become more complicated because six Mueller reflection matrices are required instead of the single Mueller matrix for the normal incidence case (collimated beam collinear to the major diagonal of the cube). Other than polarization preservation, a metal-faceted cube tends to reduce the intensity loss encountered by uncoated cubes when the range of the incidence angle is extended appreciably [77, 80, 97].

5.3.2 *Experimental setup*

Through the rotation of a quarter-wave plate, a known polarization state has been given to the SLR pulse coming out from the telescope. The reflected one then has been analyzed deflecting the incoming radiation toward the polarimeter, with a beam splitter. All the instrumentation was integrated with the MLRO facility, so as to receive half of the incoming beam from the

Figure 5.5: Picture of the MLRO telescope system and coudè path.

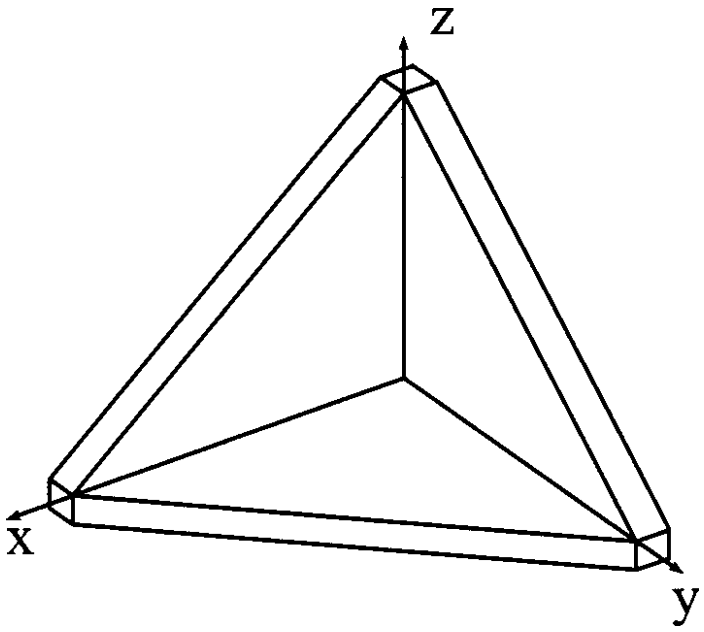


Figure 5.6: Perspective view of a corner cube retrorelfector.

telescope. Then after the first beam splitter the beam is divided into four directions in order to analyze the polarization state. A detailed diagram of the device is exposed in Figure 5.11. The device was built to best-fit the characteristics of the laser ranging station, mostly related to its technology and limits:

- dimension of the laser ranging beam (45 mm);
- velocity aberration: the tilt of wavefront of the ranging beam compared to the telescope optical axis.

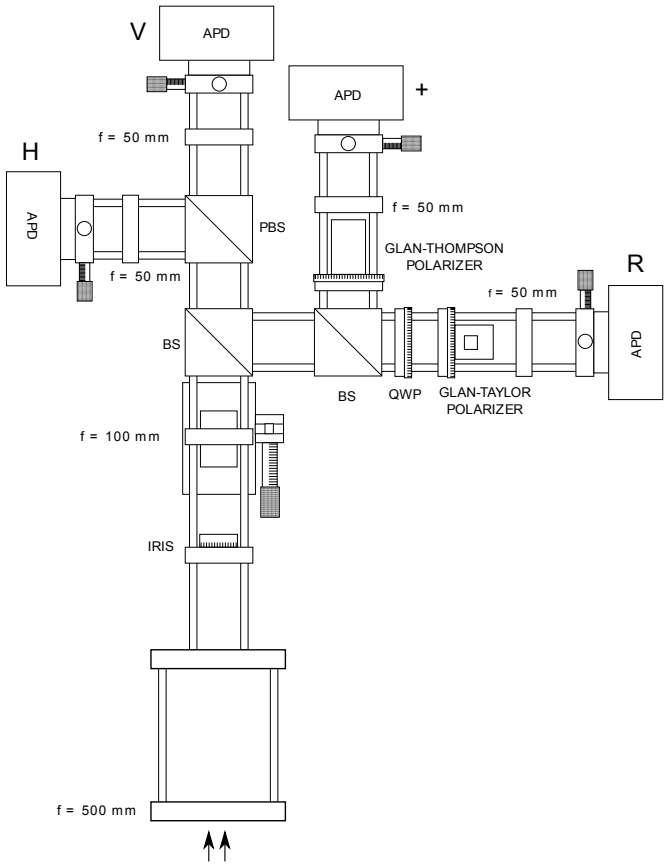


Figure 5.7: Polarimeter optical setup.

This effect is induced by the satellite movements that require a continuous tracking. A continuous tracking causes a tilt on the wavefront that generates a movement on the detector. To evaluate the image quality of the optical system we simulate the Matera Cassegrain telescope 5.5 using the real values of the telescope. As we show in table 5.1 the primary mirror has an aperture of 150 mm and a focal length of $f = 2250$ mm; we are able to determine the radius of curvature of M_1 (primary mirror) from:

$$f_1 = \frac{-R_1}{2} \Longrightarrow R_1 = -4500\,\text{mm} \tag{5.17}$$

Likewise from $f_2 = 148.5$ mm we obtain $R_2 = -297$ mm for the M_2 (secondary mirror). M_1 is a parabolic mirror, while M_2 is a convex hyperboloid

with conicity parameter about -1.0281. This kind of telescope is not affected by chromatic aberrations because it is been composed by two main mirrors, that are quite irrelevant to the wavelength. Chromatic aberrations cannot be considered because Matera telescope works only at 532 nm, and the other visible and invisible spectrum are thrown away by dichroic mirror. Another important parameter about the telescope is the b.f.l (about 15 m); this allows us to determine the secondary magnification M by:

$$M = \frac{-\text{b.f.l.}}{f_2} + 1 = 100 \tag{5.18}$$

So now we are able to calculate the equivalent focal length of the system:

$$M = \frac{\text{focal length of the system}}{\text{focal length of primary}} \Longrightarrow f_{eq} = 225\,\text{m} \tag{5.19}$$

Other important information of the telescope are reported in 5.1. Now let's take in exam the optical layout of the polarimeter designed to fit on the Cassegrain $f/150$ focus of the telescope; it will works primarily in the 532 nm wavelength. The incoming beam is reduced in size by a $5\times$ Galilean beam reducer formed by two positive lenses ($f = 500$ mm, $\phi = 2''$, $f = 100$ mm $\phi = 1''$). In the final setup the lenses distance has been set to $l = 450$ mm in order to get a collimated beam of $d = 3$ mm from the uncollimated one coming from the telescope [78]. A non polarizing beam splitter sends the collimated beam into two orthogonal directions: the transmitted part into the horizontal-vertical channels and the reflected one into the right circular linear channels. In the former case a Glan-Taylor polarizer splits the beam into horizontal and vertical polarization. In the latter, the reflected portion is splitted again by another NPBS for the circular right-handed and linear $\pm 45^\circ$ channels, respectively formed by a Quarter wave plate (QWP) followed by a Glan-Taylor polarizer and by a Glan-Thomson polarizer. In the last part of the optical system, the light of each channels is focused with a $f = 40$ mm, $\phi = 1''$ lens into Avalanche photo diode (APD). All the system is assembled in a cage system that simplifies assembly, alignment and operations and improve the portability of the instrument. Figure 5.12 show optical results of the system. We can appreciate the geometrical performance of the scheme besides a lot of aberrations. Also we can note how the point spread function (PSF)[1] for the cetral ray is very good and satisfies the contrast requirement. Analyzing more precisely the aberrations, we note that the only one present on the spots diagram and confirmed by the ray fan plot is coma. This kind of aberrations is very annoying if your system is designed for imaging, while in our case where we are concentrated to detect photons returned by satellite, and so it can be omitted. In Figure 5.12 we can see the total simulated system, including the seven mirrors that composed the optical coudè path. An important feature we must underline is that this system was designed to collect all the photons retroreflected by satellites without interfere with the normal operation of Matera Laser Ranging system, positioning a 50/50 beam splitter at the end of the coudé path. This total system present a FOV very small, increasing the reception problems and this is confirmed both from the real experiments also from the simulations. This fact makes very difficult the alignment of the polarimeter with the telescope and also decreases the number of photons received in every detector.

1 can be described as the response of an imaging to a point source.

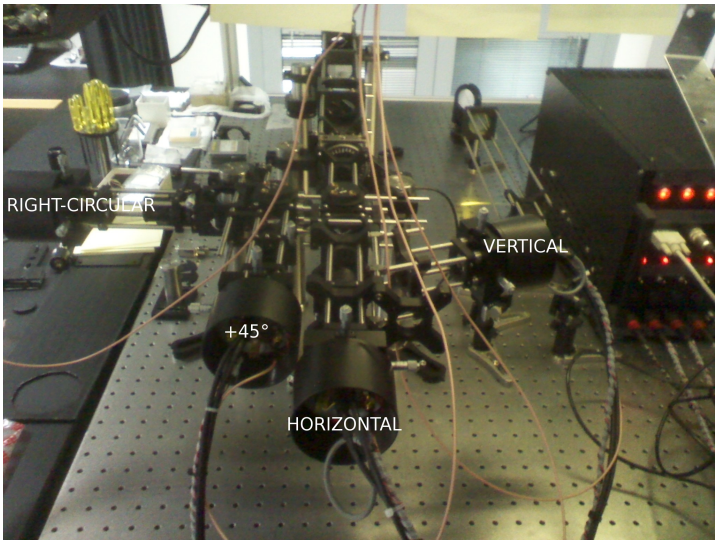
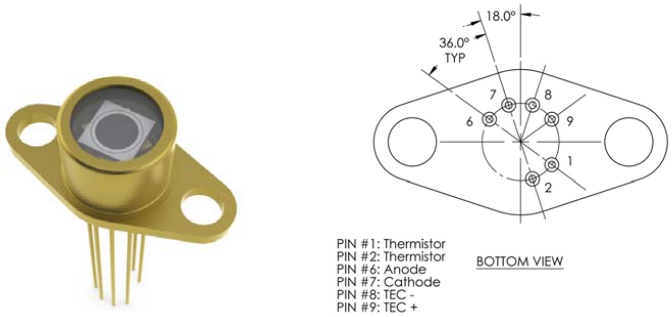


Figure 5.8: Picture of the Polarimeter.

ELECTRONIC SCHEME OF THE EXPERIMENT For each channel of the polarimeter we have a laser pulse whose intensity is proportional to the level of polarization of the incoming light. In order to reconstruct the polarization



(a) Picture (b) Pin out

Figure 5.9: APD SAR3000T6.

states, we need measurements of intensity of the four channel. The chosen detectors satisfied these characteristics:

- high sensitivity to detect the faint signal retroreflected from the satellite
- high bandwidth to detect the short pulses of the laser (80 ps)
- large active area to compensate the velocity aberration

The avalanche photodiodes are the solution that meet all these requirements. We chose the SAR3000 T6 from Laser Components [1] for their short rise time of 500 ps and a nominal bandwidth of 700 MHz. These detector present

a large sensitive area (3 mm of diameter) in order to mitigate velocity aberration problem. A screen shot of the acquisition oscilloscope TDS 6124C, displaying the signals of the four APDs is reported in Figure 5.10. Every detector has a temperature stabilization implemented inside the base chip and controlled in feedback by a loop. For more details regard APD characteristic and implementations for this experiment, we advise the reader the reference [5, 79, 102].

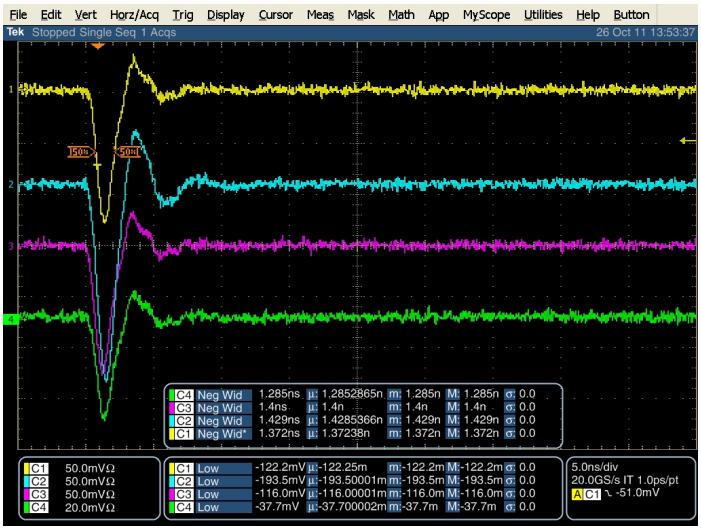


Figure 5.10: APDs signals on TDS 6124C Oscilloscpe.

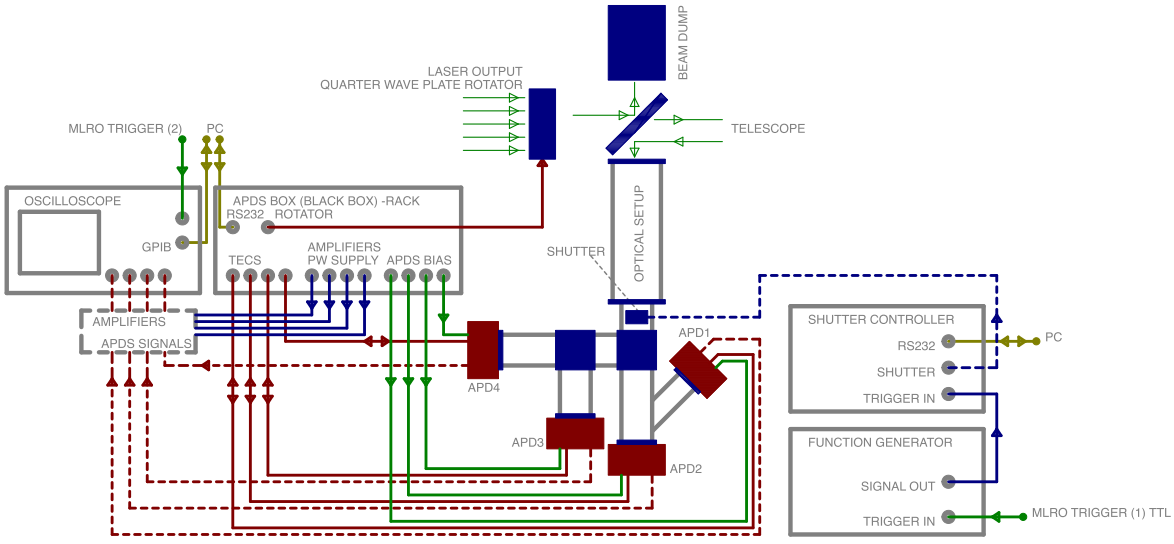
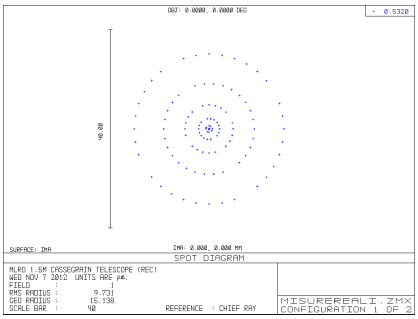
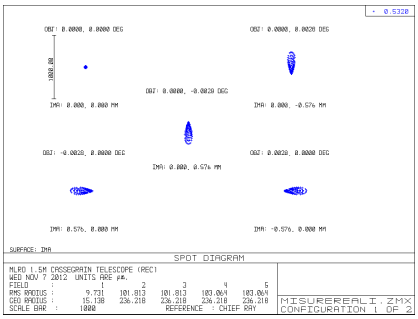


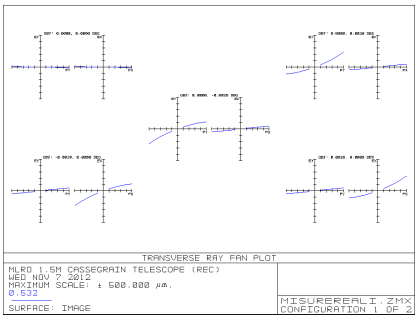
Figure 5.11: Base scheme of the polarimeter experiment implemented in T/R optical bench available at MLRO station.



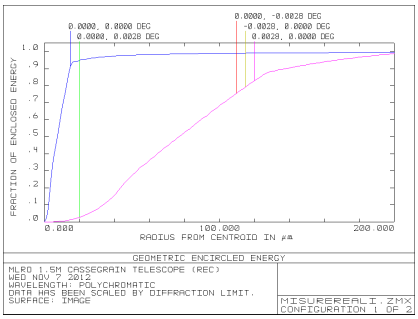
(a) *Spot Diagram.*



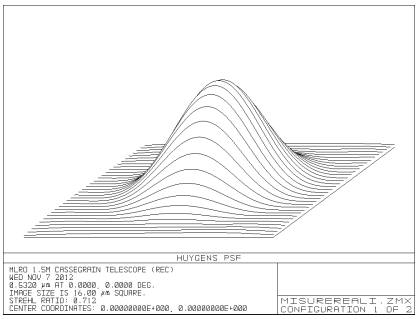
(b) *Spots diagram .*



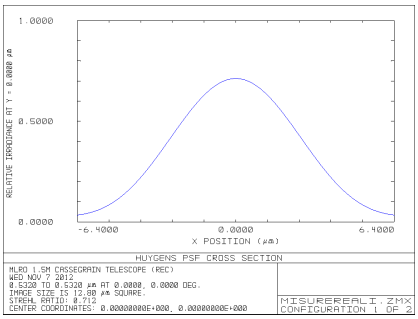
(c) *Ray Fan.*



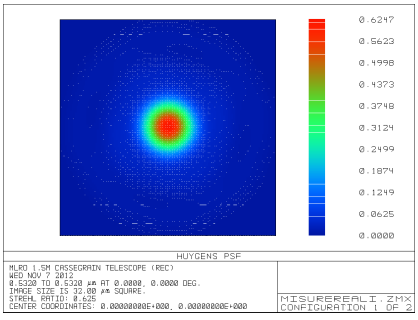
(d) *Encircled Energy.*



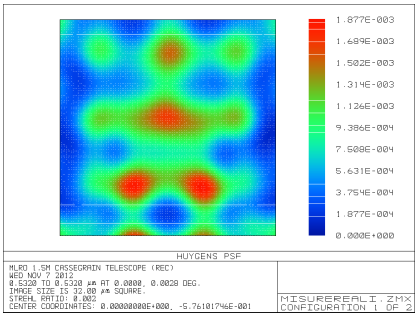
(e) *Huygens PSF.*



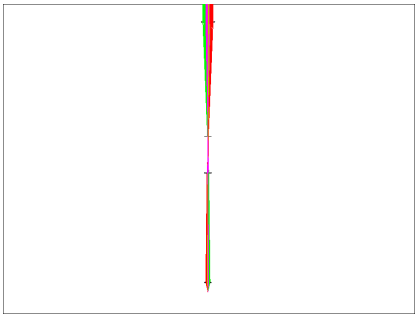
(f) *Huygens PSF cross section.*



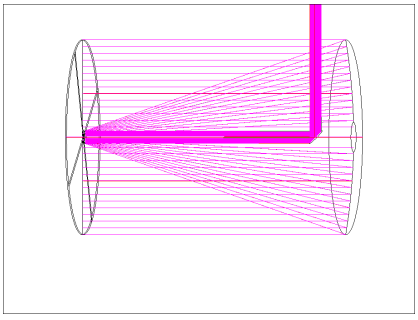
(g) *Huygens PSF.*



(h) *Huygens PSF off axis.*



(i) *Beam reducer.*



(j) *Cassegrain telescope.*

Figure 5.12: Image obtained by Zemax simulation.

5.4 SPACE QUANTUM COMMUNICATION

The polarization analysis for an Earth-Space link starts with the problem of modeling a real quantum link on space. Physically, one have to deal with a free-space dynamic optical link through the atmosphere. Another problem is due to the relative motion between transmitter and receiver. The main problems for QC are:

- effects due to atmospheric turbulence (as seen in Chapter 3)
- background noise: due to the light pollution, sunlight and moonlight every source of noise is detected by the receiver
- the relative motions between transmitter and receiver (source of misalignment in the polarization references of the transmitter and receiver)
- non ideal optics devices (cause of depolarization, attenuation and distortion)

From the Stokes and Muller formalism, introduce in the above sections of this chapter, a simple way to verify the correctness of the transmission is to minimize the norm of the difference between the sent state and that expected one:

$$\min_{\theta_Q,\theta_h} \|S - M\, M_q(\theta_q)\; M_h(\theta_h) H\|_F \tag{5.20}$$

In this way, knowing the Mueller matrix of the channel, one can compensate any distortion effect to the polarization introduced by the channel itself. In a typical transmitting system, channel probing and information exchanging share the same medium. This implies that the Mueller matrix measurement should not affect the single-photon exchange in the quantum channel. Two possible solutions are time-multiplexing and wavelength-multiplexing [17].

5.5 CHANNEL POLARIZATION ANALYSIS

Although this experimental setup would allow one to estimate four different polarization states, in the presented case only three of the four channels were used (corresponding to states V ,H, $-$, respectively). This was due to an electronics-related problem that caused the fourth detector (placed at the R-arm end) to have less signal amplification capability. Before carrying out the experimental measures, a calibration measure was performed by calculating the total Mueller matrix of telescope and polarimeter. This procedure allowed us to verify its behaviour on the polarization that passes through it and also to calibrate the response of the APD. Figure 5.13 represents the Mueller matrix obtained from this procedure. In particular we send classical polarized light from the pupil of the telescope and we analyzed it using polarimeter, creating the Mueller matrix of the telescope. This measure was performed with different polarization states and with different angles (azimuth and elevation) of the telescope.

5.5.1 *Data analysis*

The data used for this experiment were acquired during two night of observations (17 and 18 October 2012) at the MLRO. Several satellites were tracked,

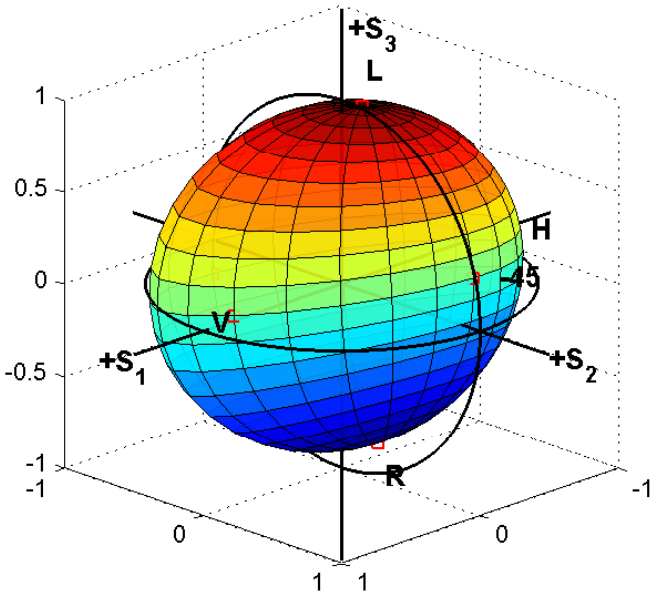
Table 5.2: Most relevant satellites used in this experiment

	Lageos	Etalon-1	Etalon-2
Ownership	USA-Italy	Russia	Russia
Launch date	Oct, 22th 1992	Jan, 10th 1989	May, 31th 1989
Reflectors	426	2146	2146
Reflectors type	uncoated	coated	coated
Perigee	5620 km	19120 km	19120 km

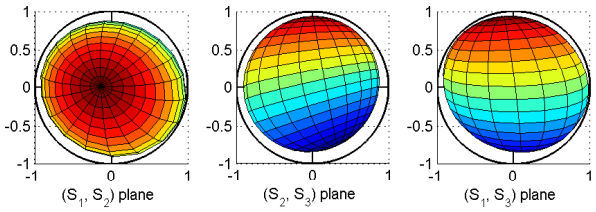
both with metal-coated CCRs and uncoated ones, with the aim to characterize their behaviour on different polarization states. In order to keep the telescope pointed at the spacecraft, continuous corrections were made to the position of the former by the facility operator. These corrections had an impact on the data acquisition time, which decreased with the satellite orbit. For this reason, only two polarization states were sent, in order to ensure enough data for every satellite passage, precisely only H and R were generated through the quarter-wave plate rotation. Table 5.2 shows the satellites used for the experiment with some critical characteristics, such as the type of retroreflectors and perigee, which is crucial for signal losses estimations.

While for Lageos-2 satellite the intensities read at the four arms of the polarimeter were very high, its CCRs type make it unusable for the realization of QKD in Space. On the contrary, Etalon satellites are suitable candidates to demonstrate the polarization preservation, since their retroreflectors are Aluminum coated.
In figures 5.15 are reported examples of the oscilloscope waveforms of several measures for both type of satellites. Each color represent the signal read from one channel of the polarimeter, which are named $CH\,1, 2, 3, 4$ and measure states $V, H, -, R$ respectively. The vertical lines limit the time interval useful for the measure of the incoming signal, which is approximately 1 ns; the number at the bottom describes the QWP rotation angle, hence, the polarization state outgoing from the telescope. Overall, it can be noticed that the signal received from Lageos-2 is more intense than the one from the Etalons. Moreover one can see that both type of satellites behave almost like what the simulations predicts. In fact, if the reflected laser pulse is completely depolarized, the intensity read from the four channels should be slightly different, regardless the sent state.

This phenomenon was clearly seen by considering the signal provided by the former satellite, which can be noticed by looking at the last frame of the Figure 5.15. The expected behaviour of the latter type of space-crafts instead, should show the conservation of polarization degree over the whole communication channel, i.e. the measured state should be equal to the sent one. In this case it means that the intensities read on the four channels change, depending on the polarization outgoing from the ground station: if the generated state is H, then signal is supposed to be present only in the H-arm of the polarimeter $(CH2)$; whereas, when R is sent to the satellite, H and V detector should provide a similar value of intensity, which are half respect to the one read from R-channel $(CH4)$. These phenomena are showed in the first and in the second frame of Figure 5.15: for the reasons explained in section 5.3.2 and for the distance from Earth of Etalon-1, 2, no



(a) *Perspective view.*



(b) *Projected view.*

Figure 5.13: Mueller matrix of the telescope at position $el = 0$, $az = 45$, this matrix was obtained by sending six different polarization states through the telescope and then measured with the polarimeter.

signal was detected in channel four, even when it was expected to be the highest, and despite this fact, the data related to $CH1$ and $CH2$ readings are consistent with theory.

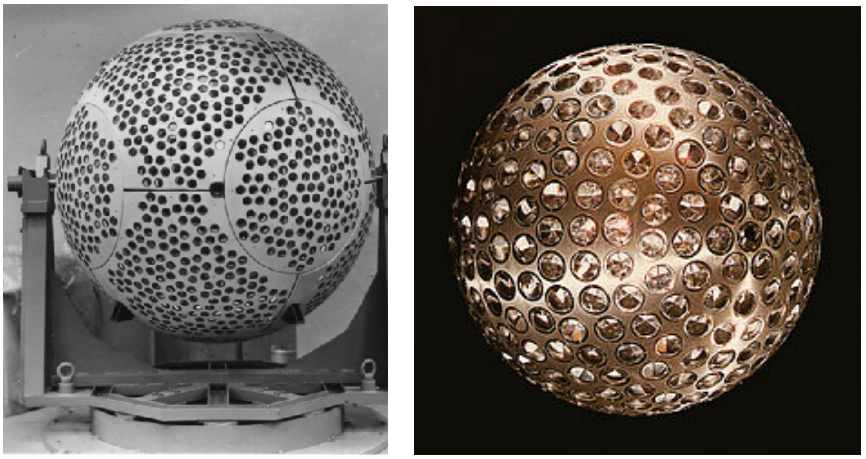
5.5.2 *Discussion*

The data acquired during this observations campaign at MLRO facility permitted us to verify the behaviours of two different type of satellite's corner cubes retroreflectors, metal-coated and uncoated ones, from the polarization point of view. In particular, it was observed that satellites with un-

coated CCRs have a clear depolarization effect on a polarized laser pulse. On the other hand, although the data set lacks of direct measures of the right-handed polarization state, the information provided by the other three channels of the polarimeter, give us indications about the behaviour of metal-coated CCRs. In particular, the intensity reads from the three linear polarization arms are consistent with the expect one in the case when H and R are sent to the satellite. Unfortunately this work was unfinished for various reasons. We try to resume the main problems encounter during one year of experiments and test campaigns.

- very noisy detectors, due to the high intensity of the sent pulse
- unstable detectors, oscillate waves owning to the electromagnetic interference
- difficulties to align the Polarimeter, very different angle between the internal reference CCRs and satellites
- velocity aberrations problems (difficulties to align and to see the return pulse from very close satellites)
- different response from the APD and above all not stable during the nightime
- pointing error of the telescope

Due to all this problems it was decide to discard this kind of experiment because in order to obtain publishable results it would be necessary to change a lot of the existing setup. It may seems that this experiment wasn't useful for the final aim of the thesis, but during the campaigns it was possible to improve our know-how about the space optical communication and understand what were the main problems of this kind of technique. Moreover

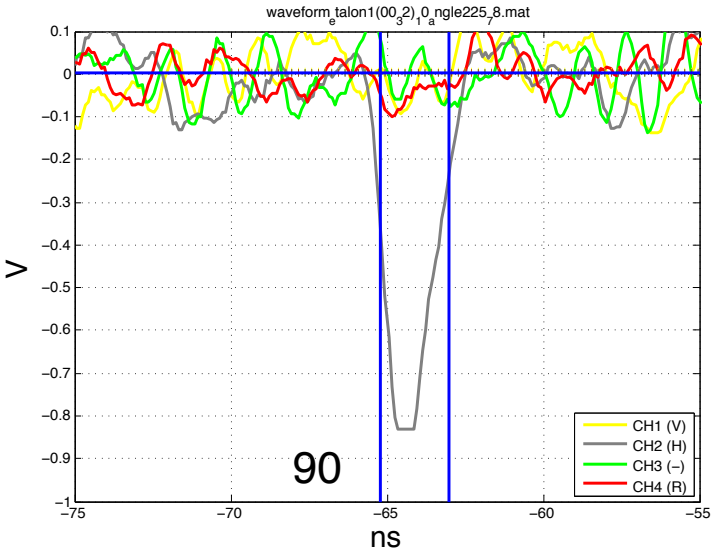


(a) *Etalon*. (b) *Lageos*.

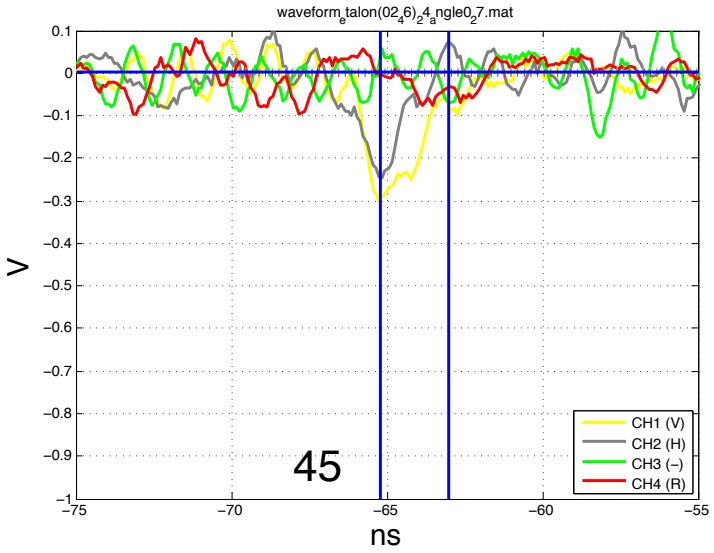
Figure 5.14: Picture of SLR satellites.

even if data were not so clear, a first demonstration of the feasibility of sending and receiving polarized photons from satellite was proved. In particular it was possible for the first time to measure the polarization of a SLR beam with a polarimeter and detect signal with a detector (not designed for SLR)

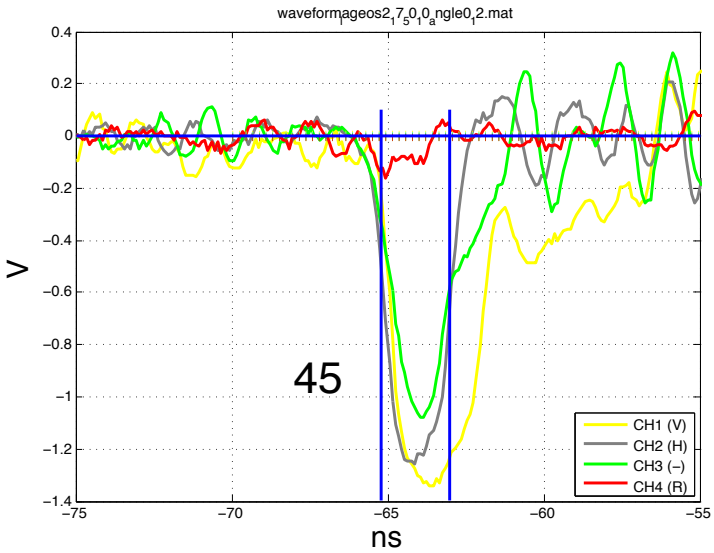
of LEO and Medium Earth Orbit (MEO) satellites. A minor issue but the same important was that we were able to synchronize two different system with a precision about 1 ns.



(a) *Waveform example for Etalon-1 satellite, H state sent.*



(b) *Waveform example for Etalon-1 satellite, R state sent.*



(c) *Waveform example for Etalon-1 satellite, R state sent.*

Figure 5.15: Waveform examples of the signal read by the APD at the end of the polarimeter. The first two pictures are referred to the satellite Etalon-1, whereas the last one is from Lageos-2.

6 SPACE QUANTUM COMMUNICATIONS

When we talk about QKD and quantum communications it's natural to look forward a future scenario where a global network of quantum cryptography will be present. In this kind of project satellite communications will be the base for every intercontinental possible link. Furthermore, QC along satellite links are crucial for the realization of quantum protocols on a global scale and for fundamental tests of QP [86]. In particular, QKD [12, 66, 50, 9], quantum teleportation and entanglement swapping [118] as well as the measurement of Bell inequalities in a relativistic scenario[44], require QC over long distances.

However, the absence of orbiting terminals equipped with quantum transmitters or receivers precluded so far the demonstration of satellite to ground quantum state transmission thus impairing the development of satellite quantum link.

We start from the results of Chapter 5 to exploit QC using satellite corner cube retroreflectors as a quantum transmitter in orbit. A stable quantum link has been established between several low Earth orbit satellites and the Matera Laser Ranging Observatory (MLRO) of the Italian Space Agency in Matera (Italy) by transmitting different qubit states encoded in the photon polarization.
The QBER has been kept steadily low for a total transmission time of 85 s. Indeed, we measured an average value of QBER $= 4.5\%$, a level that is suitable for several QKD protocols and for the violation of Bell inequalities. The mean photon number per pulse leaving the satellites was estimated to be of the order of one, as required in QKD [92]. We demonstrated that QC from an orbiting terminal to a base station is not only a promising idea but is nowadays realizable. Moreover we proposed a new protocol, where by exploiting modulated retroreflectors our communication scheme could easily be turned into a fully operational satellite QKD system. Our results pave the way to the implementation of future QC worldwide networks, setting a new record on the distance of single photon transmission.

6.1 TOWARDS SATELLITE QC

The first satellite Sputnik 1, launched in 1957, was put into an geocentric orbit orbit around the Earth. From these years an approximately number of 2456 artificial satellites were launched. Satellites can be classified by their geocentric orbits in altitude, inclination and eccentricity category. For our interest we describe only the altitude classifications, the most common classifications of the orbit:

- Low Earth orbit (LEO): Geocentric orbits ranging in altitude from $0 - 2000$ km
- Medium Earth orbit (MEO): Geocentric orbits ranging in altitude from $2000 - 35786$ km. Also known as an intermediate circular orbit

- Geosynchronous Orbit (GEO): Geocentric circular orbit with an altitude of 35786
- High Earth orbit (HEO): Geocentric orbits above the altitude of geosynchronous orbit 35786 km

Our experiment, due to the high losses of the channel take into account only LEO an MEO satellite, but in future also QC with Geostationary Earth Orbit (GEO) satellites would be possible. The envisaging and modelling of Space QC started a dozen years ago [7, 18, 103, 19, 93], but completely payload system have not been placed in orbit yet. Therefore, since 2008 the experimental studies of Space-to-ground links simulated a source of coherent pulses attenuated at the single photon level by exploiting satellites for geodetics laser ranging, which are equipped with CCRs [111, 117]. However, a full quantum transmitter for polarization encoded QKD in Space also requires qubits prepared in different polarization states. Here we show the operation of such quantum transmitter. We sent toward selected satellites a train of laser pulses at the repetition rate of 100 MHz paced with an atomic clock. The qubit signal is obtained by the pulses reflected by the CCRs (6.1). From simulating process and an high accuracy measures (4) we set the outgoing laser intensity such that, after the attenuation occurred in the uplink, the qubit signal has an average photon number per pulse (μ_{sat}) close to one. Moreover we prove the feasibility of the BB84 protocol [15] with the qubits encoded in four different polarization states, corresponding to two mutually unbiased basis. A secret key can be established between the transmitter and the receiver when the average QBER is below 11%[1].

As proved from the polarimeter analysis (5), the exploitation of CCRs with metallic coating on the three reflecting faces is crucial for preserving the polarization state during the reflection and thus obtaining low QBER. For this reason we could not use satellites mounting uncoated or dielectric coated CCRs. We focus our interest in five LEO satellites (below 2000 km): Jason-2, Larets, Starlette and Stella with metallic coated CCRs and Ajisai, with uncoated CCRs, for comparison.

6.1.1 *QC with polarized photons*

The first proof of QC using generic polarization states from two mutually unbiased bases, were realized with a single passage of Larets. The passage was divided in four intervals of 10 s in which we sent horizontal $|H\rangle$, vertical $|V\rangle$, circular left $|L\rangle$ and circular right $|R\rangle$ states. At the receiver the state analysis is performed by two single photon detectors measuring two orthogonal polarizations, from which the QBER is extracted. Indeed, in a transmission with polarization encoded qubits, the QBER can be estimated as

$$Q = \frac{n_{\text{wrong}} + 1}{n_{\text{corr}} + n_{\text{wrong}} + 2} \tag{6.1}$$

where n_{corr} and n_{wrong} are the number of detections in the sent and orthogonal polarization respectively[2]. The results are summarized in 6.2. In the four intervals, we obtained 199 counts in the correct detector and 13 wrong

1 By using the post-selection techniques introduced in[10], QBER up to 15% can be tolerated for (reasonable) secret key generation.

2 We used the Bayesian estimator of the QBER.

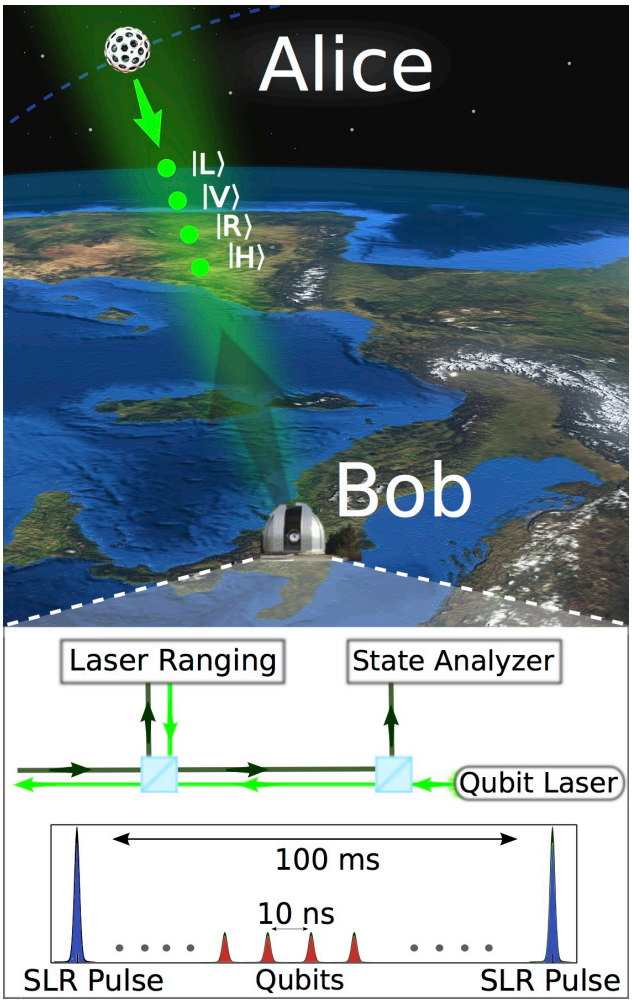


Figure 6.1: Qubit pulses are sent at 100 MHz repetition rate and are reflected back at the single photon level from the satellite, thus mimicking a QKD source on Space. Synchronization was performed by using the bright SLR pulses at repetition rate of 10 Hz.

counts, giving an average QBER of 6.5% $\pm$ 1.6% suitable for a secret key extraction. Once considered the average 3.6% duty cycle of our setup, the mean return rate in the selected intervals is 147 $\pm$ 10 cps. Such rate corresponds to $\sim 10^4$ bits for each Satellite passage in the case of perfect condition if very fast shutters are implemented.
A further analysis has been carried out to prove the preservation of the polarization state for the other coated satellites. In this analysis we divided the detection period in intervals of 5 seconds: for each interval the data were analyzed only if the signal of at least one detector was 5 standard deviations above the background. The QBER resulting from this analysis are shown in 6.6 for Ajisai, having non polarization preserving CCRs, and for the polarization preserving satellites Jason-2, Larets, Starlette and Stella. We achieved low QBER for several tens of seconds in all the polarization maintaining satellites, with an average value for each passage not exceeding 7%. By combining together the results of all the polarization maintaining satellites we achieved an overall communication period of 85 s, with an average

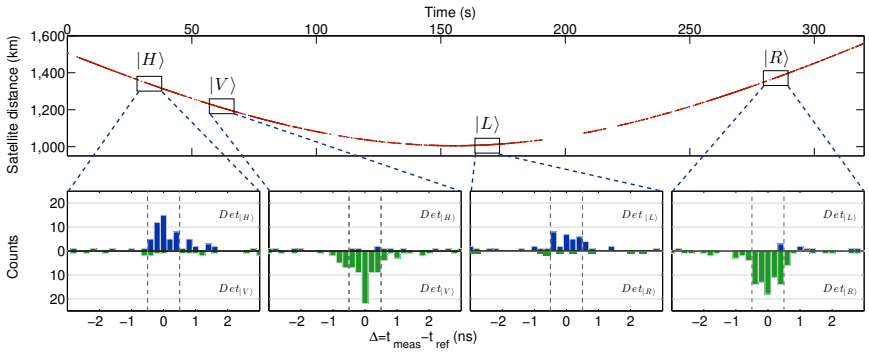


Figure 6.2: Top: Larets trajectory measured by the 10 Hz SLR pulses. The four selected 10 s intervals correspond to four different polarization input states. Bottom: the four histograms report the obtained counts at the receiver for each single photon detector in function of the measured detection time t_{meas}, demonstrating an average estimated $QBER$ of 6.5%. The signal on the two detectors is blue for H/L polarization and green for V/R. Gray dashed lines represent the $1\,\sigma$ selection interval around the expected time of arrival t_{ref}.

QBER=4.5% $\pm$ 0.8%. These results prove that faithful transmission of different polarization qubits can be obtained in different conditions and satellite orbit and show the stability and the reliability of our approach. In 6.6 we also report the experimental detection rates achieved with the different LEO satellites.

6.1.2 *Single photon investigation*

A real earth-satellite QKD system is based on faint laser pulses with a mean photon number of the Poisson process μ close to 1. Indeed the BB84 protocol with decoy states [67] in a realistic scenario requires [92] $\mu \lesssim 2$ and decoy signals with mean photon number close to 1 [106] (see Appendix B). In this section we demonstrate that our experiment was carried out in this regime by providing a quantitative estimate of the mean photon number of the downward pulses. The value of μ_{sat} can be estimated by the radar equation [32] introduce in Chapter 4 and now suitably used:

$$\mu_{rx} = \mu_{sat} \frac{\Sigma}{\rho A_{\text{eff}}} \left(\frac{1}{4\pi L^2} \right) T_a A_t \eta_{rx} \eta_{det} \tag{6.2}$$

with μ_{rx} the received mean photon number per pulse, Σ and A_{eff} respectively the satellite cross-section and effective retroreflective area, ρ the CCR reflectivity, L the slant distance, T_a the atmospheric transmissivity, A_t the telescope area, η_{rx} the optical receiving efficiency and η_{det} the single photon detector efficiency. The values of the parameters used in the μ_{rx} estimation are reported in the Methods section. Concerning the satellite cross-sections, we used those given in [6, 110, 21] and reported in table 4.1. For the Larets passage of 6.2 we obtained $\mu_{sat} = 3.4 \pm 0.2$ and a corresponding downlink transmissivity of $\sim 4.3 \cdot 10^{-7}$ (63 dB of attenuation). The values of μ_{sat} for the remaining satellites are reported in 6.6. The resulting μ_{sat} is of the order

of unity for the four satellites with metallic CCRs. The reflectivity ρ of the CCRs was taken as unitary, setting a higher bound on μ_{sat}.

In order to have an additional confirmation that the obtained values of μ_{sat} are correct, the full radar equation was used to estimate the number of received photons in several passages of the different satellites. The theoretical predictions and the experimental data are compared in Figure 6.3. The results show that radar equation model [32] and eq. (6.2) provide a precise fit for the measured counts and the μ_{sat} values derived in Figure 6.6.

To estimate μ_{sat} it is necessary to factorize the radar equation into an uplink and a downlink factors. While most of the parameters of the radar equation can be easily separated into uplink and downlink factors, the satellite cross section Σ plays a role in both and must be split according to $\Sigma = \rho A_{\text{eff}} G_{down}$. The parameters ρ and A_{eff}, corresponding to the CCRs reflectivity and the effective satellite retroreflective area, contribute to the uplink, while G_{down} gathers all the downlink contributions into an effective downlink gain. Then, the downlink factor

$$\eta_{\text{down}} \frac{\Sigma}{\rho A_{\text{eff}}} \frac{1}{4\pi L^2} T_a A_t \eta_{rx} \eta_{det} \tag{6.3}$$

can be used in equation (6.2) to obtain an estimate for μ_{sat}. The values of the parameters used to evaluate μ_{sat} are the following: $\eta_{det} = 0.1$, $P_s = 0.11W$ P_s is the laser power, corresponding to $\mu_{tx} \simeq 2.946 \cdot 10^9$), $\eta_{tx} = 0.1$, $A_t = 1.73m^2$, $\eta_{rx} = 0.13$. For the cross-sections, we used the following values (we report the min- and max- values used to draw the shaded ared in Fig. 4): $\Sigma = 23$ for Ajisai, $\Sigma = 0.2 \div 1.7$ for Jason, $\Sigma = 1 \div 2.5$ for Starlette and Stella, $\Sigma = 0.2 \div 0.8$ for Larets.
The atmospheric absorbance is proportional to the air-mass (AM), defined as the optical path length through atmosphere normalized to the zenith. In our model we considered 87% of transmissivity at the zenith for all the days. This value refers to good sky conditions [32] which were effectively selected for the experiment.

For a consistency check of our μ_{sat} estimation, the full radar equation has been used to extrapolate the transmitter gain, given by

$$G_t = \frac{8}{\theta_t^2} \exp\left[-2\left(\frac{\theta}{\theta_t}\right)^2\right]. \tag{6.4}$$

In the previous equation θ_t is the divergence angle of the up-going beam (including beam broadening due to turbulence), while θ is the pointing error. Since the two parameters θ and θ_t cannot be directly and separately measured, we obtained an estimate for G_t by comparison the data obtained in different passages of the several LEO satellites. As a consequence of the pointing error, the detection frequency of the 100 MHz laser varies strongly with time, thus producing localized peaks of detection for few tens of seconds, followed by the absence of signal. Because of this several periods of at least 10 seconds, in which the detection frequency was significantly above the background, have been isolated and only the peak frequency within these periods has been taken into account.

To best approximate of G_t, we averaged the most stable data taken for Ajisai, Jason and Starlette, thus obtaining an effective gain of $G_t = 1.1 \times 10^9$. The resulting value of G_t has been used in the radar equation to estimate the number of received photons. The theoretical predictions and the experimental data are compared in Figure 6.3. The results show that radar equation

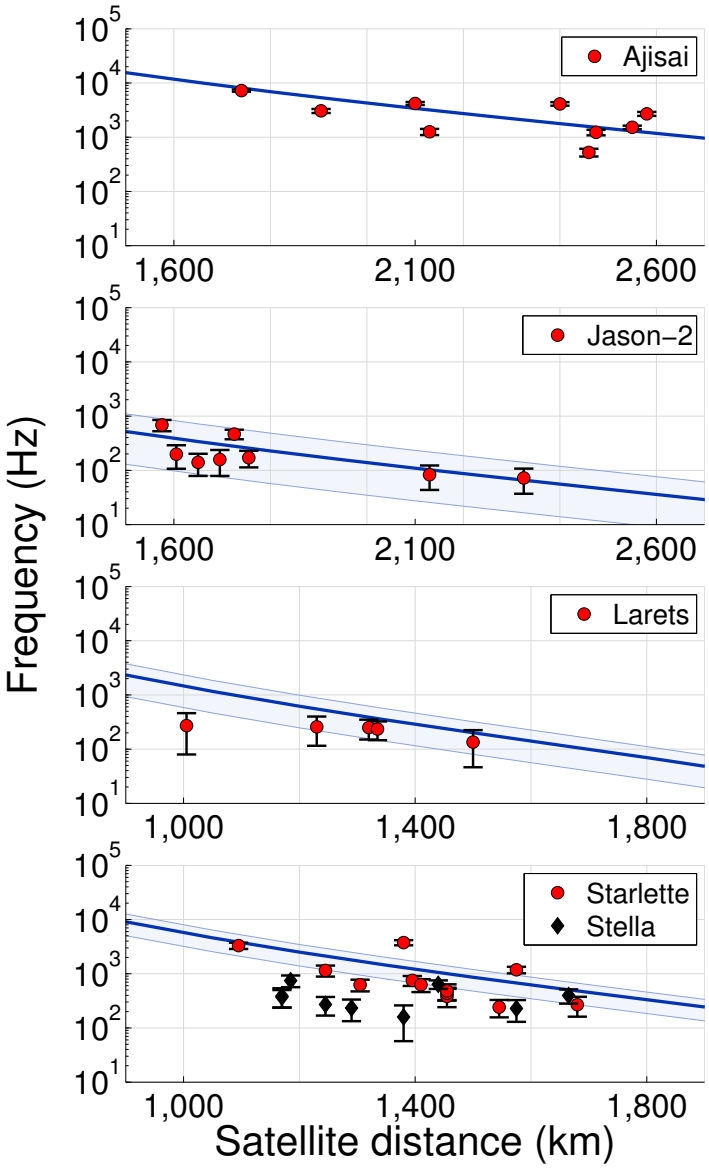


Figure 6.3: Points represent the return frequencies of the qubits for different satellites along the orbit, compared with the prediction of the link budget provided by the radar equation model (continuous line). Error bars account for Poissonian errors only while shaded area comes from the available uncertainties of the satellite cross-sections $\sum$. Uncertainties in the orbital parameters and beam pointing affect trend of the return rate beyond shot noise. The twin satellites Stella and Starlette show different behaviour despite similar characteristics, but in line with the SLR statistics

model [32] and eq. (6.2) provides a precise fit for the measured counts and the μ_{sat} values derived in 6.6.

QKD SATELLITE PROTOCOL USING RETROREFLECTORS We now show that our QC scheme could be turned into a practical satellite QKD system. Indeed, we note that, if the outgoing and incoming beams travel through the same optical path, the polarization transformation induced in the uplink by

the telescope movements is compensated in the downlink (see Appendix B). Therefore, by transforming the state during the retroreflection, it is possible to change the qubit sends from satellite to the ground. On this base, we propose a two-way QKD protocol, working as follows:

- in the ground station, a horizontal polarized beam is injected in the Coudé path and will exit the telescope rotated by an angle depending on the telescope pointing
- the outgoing beam is directed toward a satellite with CCRs having a polarization rotator, such as a Faraday Rotator, mounted at the entrance face
- it is possible to rotate the returning polarization by a suitable angle θ by using the polarization rotator
- in the CCRs a suitable attenuator lowers the mean photon number to the single photon level
- a measure of the intensity of the incoming beam is desirable in order to avoid Trojan horse attack [42] and to guarantee the security of the protocol
- the retroreflected beam then propagates toward the ground telescope, and thanks to the properties of the Coudé path, a polarization qubit will be received (see Appendix B).

By this scheme, a decoy state BB84 protocol can be realized between satellite and ground. The experimental results shown above demonstrate that such protocol is currently realizable using few centimetres CCRs and that the MLRO station is suitable for Space QC.

Obviously this is only an idea for a future experiment, but the possibility to have something very small and integrated as payload is completely different from a quantum transmitter or receiver in space, where optical components and the pointing error would be a big issue. Moreover this device could work both for SLR both for QKD and the integration of a quantum transceiver in SLR stations would be quite easy.

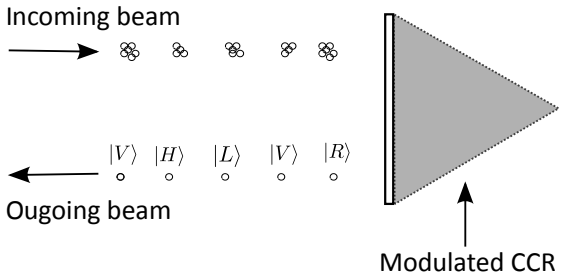


Figure 6.4: Idea of QKD with modulated CCR: the multi-photons pulses arriving from Earth is measured, attenuated and modulated by the CCR and retroreflected to the Earth. In this way it is possible to create a two-way QKD scheme.

6.1.3 *Setup*

The detailed scheme used in the experiment is shown in B.1. A mode-locking master laser oscillator subjugated at the MLRO atomic clock is used as events generator. It produces pulses of 100 ps duration at the wavelength of 1064 nm, with a repetition rate of 100 MHz and about 400 mW of average power. The master laser beam is split to provide the seed for the SLR signal and the pump pulse for the qubits. The high intensity SLR pulses are obtained by selecting with a pulse picker one pulse every 10^7 and then using a regenerative amplifier and two single-pass amplifiers followed by a Second Harmonic Generation (SHG) stage, obtaining pulses at 532 nm with 100 mJ energy and 10 Hz repetition rate. The beam used to generate the qubits is obtained by sending the rest of the master oscillator laser to a suitable SHG unit, whose output is 110 mW. The beam divergence is controlled by a collimator, while the polarization state is changed by two waveplates and a modulator. Two non-polarizing beam splitters (NPBS) are used to combine SLR and qubit pulse-train in the upward beam that is directed via the Coudé path to the MLRO telescope, from which it propagates toward the satellite.

The beams coming from the satellite and received by the MLRO telescope propagate backward via the Coudé path and are split by the same two NPBS used in the uplink. The qubit receiver is composed by a focalizing lens, a rotating waveplate, an optical shutter and two single photon photomultipliers (PMT) placed at the outputs of a Polarizing Beam Splitter (PBS). The signals detected by the PMT are fed into a time tagger with 81 ps resolution. The rotating waveplate, controlled by software, is used to change between two receiving bases, $\{|H\rangle, |V\rangle\}$ and $\{|L\rangle, |R\rangle\}$.

The pulses generated by the transmitter, passing through the first NPBS produce a scattering that elevates the background noise at the quantum receiver. To prevent this effect, we implemented a time division protocol by using two fast mechanical optical shutters. In the first half of the 100 ms slot between two SLR pulses, the transmitter shutter is opened in order to send the qubit pulses toward the satellite, while the reception shutter is closed to protect the receiver PMT.

In the second half of the slot the transmitter shutter is closed, and, once the receiver shutter is fully open, the detection phase begin. By using this protocol, the effective transmission time during a slot cannot be larger than the round trip time (RTT); however, since the shutters require about 2 ms to fully open and 2.5 ms to fully close, the effective period is further reduced by 4.5 ms. Considering that for a LEO satellite the RTT varies between 5 and 20 ms, the effective duty cycle can vary between 0 and 15% . Moreover, the effective duty cycle varies also in a single satellite passage, approaching its minimum when the satellite reaches its maximum elevation (see 6.5).

In order to reject the background and dark counts, a precise synchronization is needed. For this purpose we exploited the SLR signal. The latter is generated in a coarse pulse-train of strong pulses (10 Hz repetition rate and 100 mJ pulse energy) whose seed is taken from the same oscillator locked to an atomic clock used to generate the 100 MHz qubits. The atomic clock guarantees that the qubit pulses are all separated by 10 ns and that 10^7 qubit pulses exactly correspond to 100 ms, the time between two SLR pulses. Two non-polarizing beam splitters were used in the optical path in order to merge and split the outgoing and incoming SLR signal and qubit stream (see Figure 6.1 and Figure B.1 in Appendix B on page 129). For qubits discrimi-

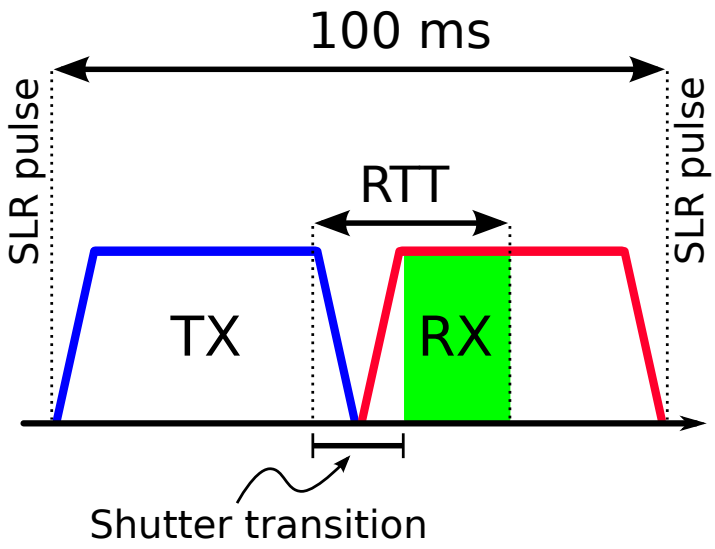


Figure 6.5: Schematic demo of shutter operation.

nation, we synchronized the state analyzer by using the time-tagging of SLR pulses provided by the MLRO unit, which has few picosecond accuracy. Indeed, by dividing the intervals between two consecutive SLR detections in 10^7 equidistant subintervals, we determined the sequence of expected qubit times of arrival t_{ref}. This technique compensates for the time scale transformation due to satellite motion with respect to the ground. Our detection accuracy σ was set equal to the detector time jitter (0.5 ns), as other contributions to time uncertainties coming from detection electronics or laser fluctuations are negligible. Counts registered within $1\,\sigma$ interval around t_{ref} were considered as signal, while the background has been estimated from the counts outside $3\,\sigma$.

6.2 SINGLE PHOTON LINK WITH MEO SATELLITE

Once we have obtained the results presented in the above paragraphs, we decided to improve the limit of single photon transmission in space, fixed at LEO orbits. From our simulation and with the same setup of the QBER measurement, a single photon transmission from a MEO satellite had to be possible. We focus our experiment on Lageos satellite because it is very brilliant and relative easy to center with SLR station. The high signal loss, due to the satellite slant range exceeding 7000 km, imposes stringent limitations to the background level tolerable by the receiver. To minimize the effect of the stray light, the incoming beam has been filtered spatially, reducing the detector field of view down to 40 μrad, and on the basis of the wavelength, with a 3 nm wide band-pass filter. This reduced the stray light effect to a negligible level compared to the $\sim$ 50 Hz intrinsic detector dark count frequency.

To further reduce the background a second filtering stage, based on the time synchronization, has been implemented. This technique requires the determination of photons expected the times of arrival t_{ref} and it must take into account the "Doppler-like" squeezing and expansion effect of the 100 MHz pattern as the satellite goes toward or away from the MLRO station

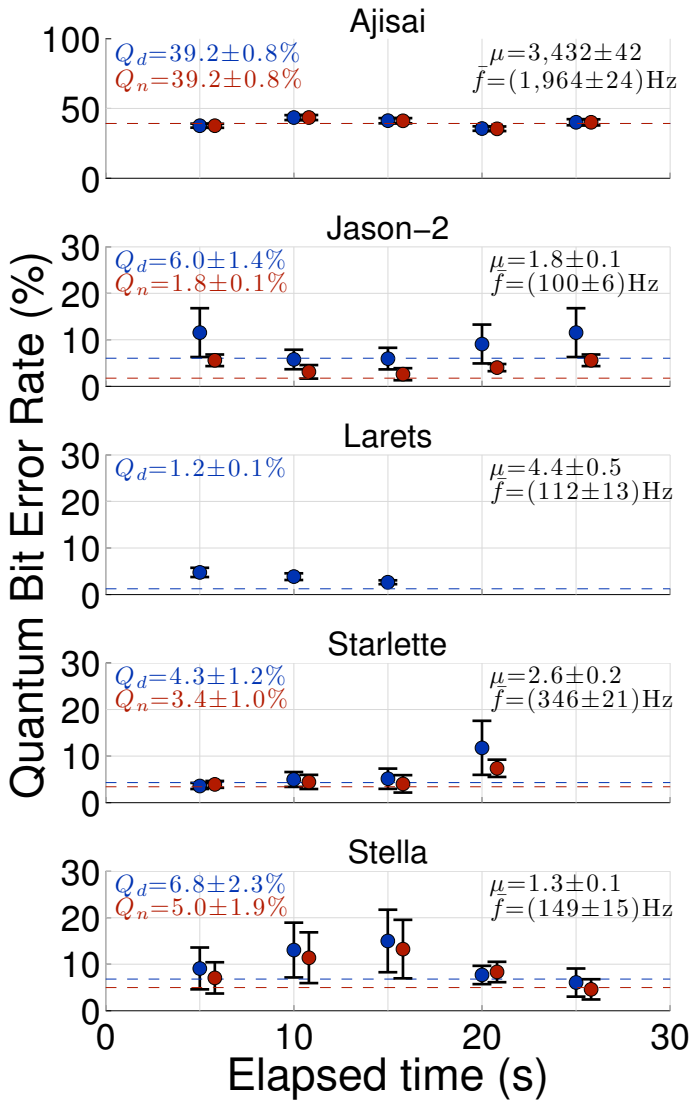


Figure 6.6: We fixed the sent polarization to $|V\rangle$ and measured in two orthogonal polarization $|H\rangle$ and $|V\rangle$. For each satellite we show the bare QBER (blue dots) calculated according to (6.2), and the QBER calculated after the background subtraction (red dots). Error bars represent Poissonian errors. Q_d and Q_n represent the bare and background subtracted QBER for the whole satellite acquisition. For Larets we observed no detection in the wrong state, and we did not estimate the QBER with background subtraction. The coating of Ajisai retroreflectors depolarizes the qubits, while the other satellites preserve the photon polarization. We also indicate the mean detection rate and the average photon number per pulse at the satellite.

(see Figure 6.7). The estimate of t_{ref} was obtained by dividing the interval between the detection of two consecutive 10 Hz pulses by 10^7. This procedure relies on the fact that the two laser patterns are locked one to the other, with a fixed phase relation. Therefore a single calibration is needed to measure the offset of the 100 MHz pattern with respect to the 10 Hz pulses,

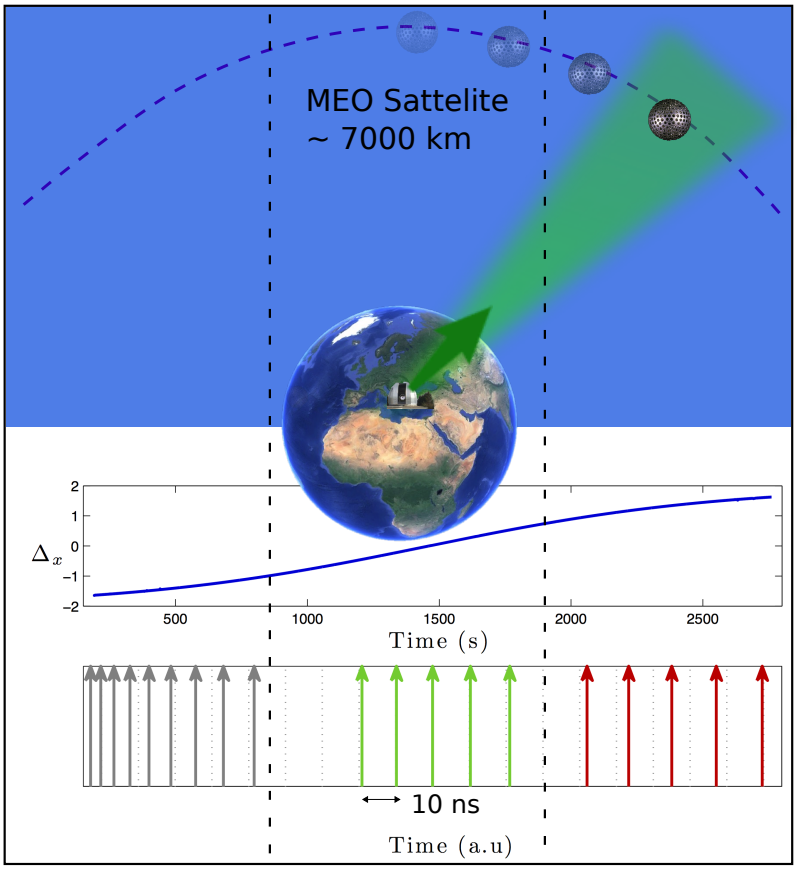


Figure 6.7: Experimental setup: two 532 nm beams are sent towards satellites, one for Laser Ranging observations and the other one for quantum communications. SLR pulse is a 10 Hz 532 nm beam combined with a train pulses at 100 MHz 532 nm. Photons are collected with two different system: a more precise PMT (Photomultiplier) was used for SLR in order to achieve a better resolution on datas. This characteristic was also useful for QC because we were able to control more precisely the Doppler effect and the velocity aberration due to the trajectory of the satellites.

which results form the different optical path of the two beams. This procedure automatically compensate for the "Doppler-like" distortion, as both beam undergoes the same transformation.

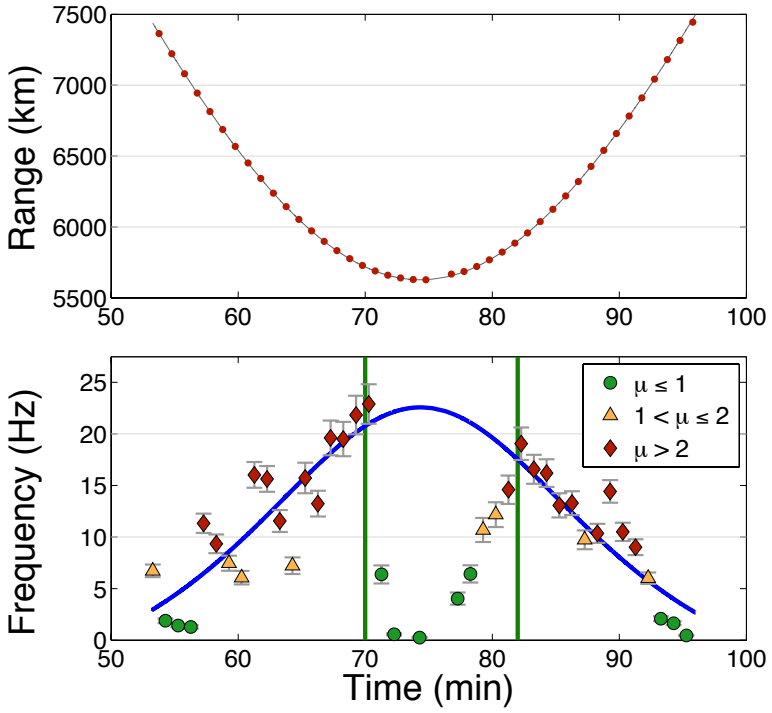


Figure 6.8: Estimation of mean number of photons per pulse.

As discussed in [32] and presented in paragraph 6.1.2, the radar equation (6.2) can be used to estimate the average photon detection frequency at the receiver starting from the average photon transmission frequency.

The return frequency depends on the instantaneous satellite slant range both directly, due to the factor $1/L^4$, and through T_a, which. In fact T_a assumes the form

$$T_a = exp(-\sigma\, h_s\, sec(\,\theta_{zen}\,)\, e^{-h/h_s}) \tag{6.5}$$

with σ the attenuation coefficient, h the altitude over the sea level of the ground station and $h_s = 1.2Km$ a scaling height.

All the parameters of (6.2) are known with the exception of the transmitter gain G_t which can be expressed as:

$$G_t = \frac{8}{\theta_t^2} \exp\left[-2\left(\frac{\theta}{\theta_t}\right)^2\right].$$

where θ_t is the time independent divergence angle of the upgoing beam (including beam broadening due to turbulence), and θ is the time dependent telescope pointing error, due to satellite fluctuations from the ideal trajectory. These two parameters are not known separately, however, it is possible to gather their effects on the beam widening into an effective divergence angle θ_{eff} defined as $G_t = \dfrac{8}{\theta_{eff}^2}$. Since both parameters are unknown, it is possible

to compute a mean value of G_t from the parameter a obtained from the fit. From this we can extract an effective divergence angle θ_{eff} defined as $G_t = \frac{8}{\theta_{eff}^2}$.

The obtained value of θ_{eff} is 52 μrad, which is lower than that computed in the above paragraphs. If we compare this value with the ones obtained in the case of LEO link, we can see that this value is lower. We can explain this with the fact that a MEO has a higher perigee compared to a LEO satellite, that lead to a lower angular velocity and thus makes the tracking more stable over time.
Figure 6.8 shows a good agreement of the measured frequencies with the overall fit, with the exception of the interval between minute 75 and 76. This is due to a temporary problem with the telescope pointing and because of that those points where not used in the analysis.

It's important to note that due to the telescope instantaneous pointing error the mean number of photons per pulse hitting the satellite varies over time, as the uplink attenuation is higher in instants with worse pointing and viceversa. This effect is evident in the deviation of the measured detection frequency from the global fit. Because of this an estimation of the μ_{sat} based on the mean uplink attenuation would produce high errors as it would not consider local fluctuations of the pointing error.

For this reason we computed μ_{sat} as the average number of received photon per pulse μ_{rec} divided by the downlink part of the radar equation. With this method it's possible to get the μ_{sat} corresponding to each return frequency point precisely.

With this method we computed μ_{sat} for each analysis slice, distinguishing those where $\mu_{sat} \leq 1$, $1 < \mu_{sat} \leq 2$, and $\mu_{sat} > 2$. The first two cases are the ones that have a μ that can be considered practical to be used in protocols such as BB84 with decoy states (Appendix B). As we can see in 6.8, we were able to receive pulses with less than unitary photons per pulse in the moments when the satellite was in the farthest points from the the ground station, which corresponds to the maximum geometric attenuation. Moreover the intervals which lead to the useful μ_{sat} correspond to periods of bad telescope pointing, which increase the uplink losses even more.

We analyzed two satellite passages, one for the Ajisai satellite, a LEO with perigee of 1478 km, and one for Lageos-2, comparing the timestamp of each photon detection with the nearest t_{ref}. In both cases we identified a peak with strong statistical significance (more than 15 σ over background in both cases), corresponding to the detection of the 100 MHz pattern (see Figure 6.8). On the basis of a Gaussian fit we extracted both the residual offset (Δ_0) and the full width at half maximum (FWHM) of the distribution. The measured Δ_0 is 0.04 ± 0.03 ns for Lageos and 0.02 ± 0.02 ns for Ajisai, resulting in both cases compatible with the values that obtained during the calibration, thus demonstrating the reliability of the synchronization technique for LEO and MEO satellites. The FWHM measured for the two passages is 1.20 ± 0.08 ns for Lageos and 1.28 ± 0.05 ns for Ajisai, a value that allows a background reduction of a factor 10 while maintaining $\sim$ 70% of the data. Moreover, the fact that the two values are compatible, within the experimental errors, indicates that the synchronization procedure doesn't depend on the slant range, and can be effectively applied to any satellite distance. It is worth noting that the FWHM is dominated by the time jit-

ter of the single photon detector, from datasheet 1.5 ns . The 80 ps pulse width of the 100 MHz laser is thus not significantly broadened during the transmission through the atmosphere as well as during the reflection on the corner cubes. As a consequence the adoption of a lower jitter detector, such as single-photon avalanche diode or microchannel plate with a FWHM $\sim$ 50 ps, would improve the efficiency of the whole synchronization system allowing a further enhancement of the SNR amplification by more than one order of magnitude.

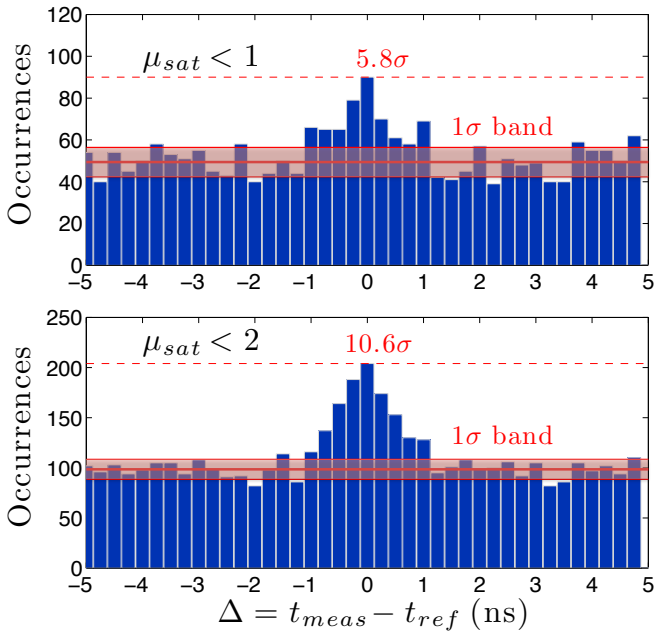


Figure 6.9: Return from Lageos satellite with different μ value

We selected the intervals with $\mu_{\text{sat}} \leq 1$ and $\mu_{\text{sat}} \leq 2$ which resulted in an integrated acquisition period of 360 s and 720 s respectively. For all the data in these intervals, we compared the timestamp of each photon detection with the nearest t_{ref}. As shown in 6.9, in both cases we observed the reception peak with a strong statistical significance over the background. For the data with $\mu_{\text{sat}} \leq 1$ we measured a peak signal to noise ratio SNR= 1.8 with a mean reception frequency of 1.4 Hz, while for the data with $\mu_{sat} \leq 2$ we measured a SNR= 2.1 with a mean reception frequency of 4.3

6.3 DISCUSSION

In conclusion from the plots reported above it results very clear that we experimentally demonstrated the preservation of single photon polarization over a channel with unprecedented length, showing QC from several satellites acting as quantum transmitter and with MLRO as the receiver. Moreover we perform the first measure of QBER from photons coming from satellites and we found that it was low enough to demonstrate the feasibility of quantum information protocols such as QKD along a Space channel. In addiction, we propose a new protocol with a very simple trusted device in orbit, formed by active CCRs mounted on a spacecraft and operated in the two-way scheme. This solution may provide a simple alternative to a full space

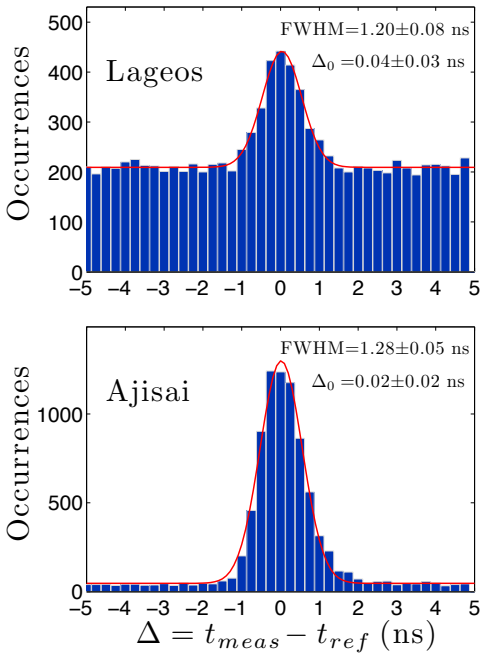


Figure 6.10: Comparison of the actual time of detection with the expected time of photon arrival. The peak centered at $\Delta = 0$ represents the detection of the 100 MHz beam. The compatibility of the fit parameters for LEO and MEO satellites demonstrates the robustness of the analysis method independently from the satellite distance.

terminal since all the existing SLR facilities can be turned into QC stations with minor upgrade, fostering a faster expansion of QC around the planet and beyond. We improve the actual limit of single photon transmission, performing an experiment where Alice was positioned about 7000 km from Bob. it was possible to demonstrate out technique works both for LEO and MEO, allowing a good detection of the quantum signal over the noise counts. Unfortunately being Lageos an uncoated aluminium satellite, it was not possible to measure the QBER in the case of MEO satellite, but near future also this kind of experiment will be done. All the experiments and simulation was perform in the regime of photon encoding polarization, where the information about the bit is encoded in the state of polarization of the photon. However we must pay attention to other protocols, like time-bin encoding where using a non balanced Mach-Zender (MZ) interferometer it is possible to delay the phase between the wave-packet of the photons and so encoding our information in the phase delay of the qubit.

7 INTERSATELLITE LINK

The space-to-ground quantum key distribution, as demonstrated in Chapter 5 and in Chapter 6 can be considered feasible. A future different scenario for the QC are the inter-satellite links between two or more satellites exchanging informations among them. In this chapter we focus our attention on the extension of inter-satellite communications into the quantum domain. Classical optical communication in a very long distance link between two moving terminal is already a great effort, but several missions (LLCD, LCRD) demonstrated that is achievable. A further request introducing quantum light in this context is of enormous interest, but also a very challenging project. We present a scheme for a quantum payload based on B92 protocol, which could be used in a future GNSS satellite mission. In fact we realized, in collaboration with TASI (Thalens Alenia Space Italia) a space QKD terminal whole based on optical communications. Both the quantum channel, for the key generation, both the classical channel for the information reconciliation process were realized in a free-space link. This system was implemented and tested in a line of sight terrestrial link in order to demonstrate that a quantum payload application is available and possible for GNSS constellation.

7.1 OPTICAL LINK MODEL

For an optical characterization of the beam, the propagation through vacuum of a laser beam can easily be modeled. Better, in the case of inter-satellite link the background noise is lower than considering downlink or uplink scenario(presented in Chapter 4). The propagation equation of a Gaussian beam in vacuum has at least the divergence:

$$\theta = \frac{\lambda}{\pi w_0} \tag{7.1}$$

obviously the lower is the beam waist at the receiver side, the more energy can be collected by the telescope increasing the total efficiency of the link. The divergence factor, from equation (7.1) can be decreased depending on the color (λ) of the laser and also increasing the beam waist w_0 of the beam. Another good point of an optical propagation in vacuum is the absence of the broadening effects due to atmosphere [65, 39], which simplify the propagation equation:

$$w_{LT}^2 = w_0^2 \left(1 + \frac{L^2}{Z_0^2}\right) \tag{7.2}$$

where L is the propagation link distance and $Z_0 = \pi w_0 / \lambda$ is the Rayleigh parameter of the beam. The total power P collected by the receiver of radius R can be estimated as:

$$P = 2\pi I_0 \int_0^R \rho e^{-2(\rho^2 / w_{LT}^2)}\, dq \tag{7.3}$$

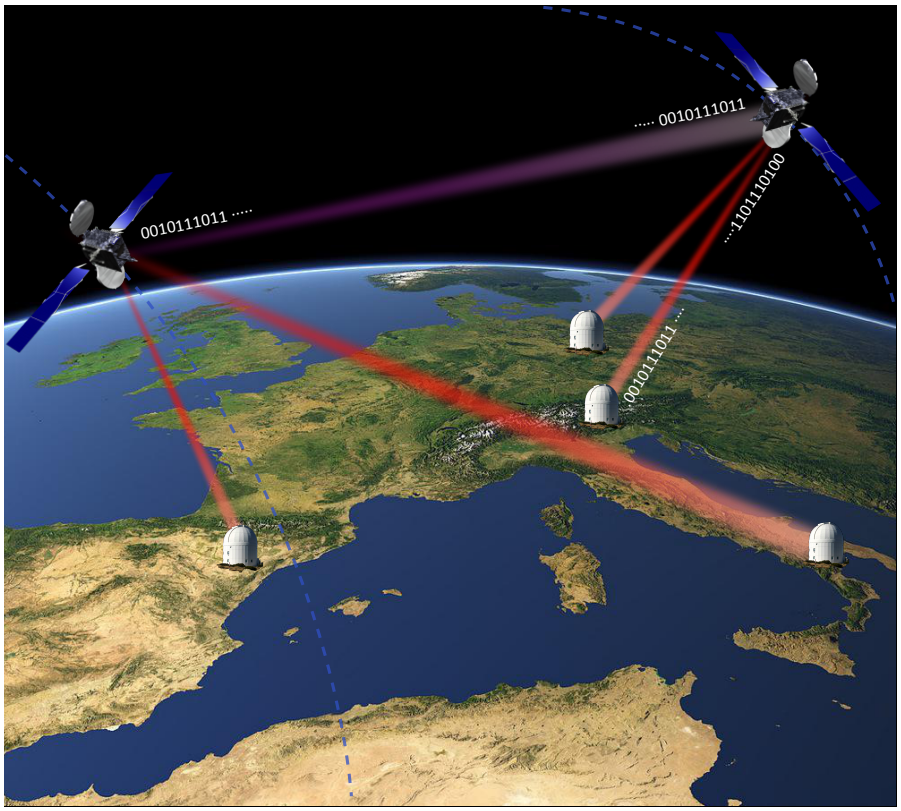


Figure 7.1: Future scenario of satellite QC network. Every satellite can exchange quantum and classical information both with other spacecrafts, both with OGS. This quantum network will allow to exchange information in an unconditionally secure way.

To get a quantitative idea of the link energy-transfer we introduce the η parameter, defined as the ratio between the transmitted over received energy as:

$$\eta = \eta_0 \left(1 - e^{-2R^2/w_{LT}^2}\right) \tag{7.4}$$

In a real scenario where satellites are moving, limitations like optical efficiency and pointing error are present. In order to establish secure communications, the SNR achieved in all the transmission must be greater than fixed threshold value, depending on how much informations we allow to Eve. As reported in Chapter 4, SNR ratio can be defined as:

$$SNR = \frac{\eta}{N} \tag{7.5}$$

where for a fixed detection time $\Delta t = 1$ ns and a bandwidth $\Delta\lambda = 1$ nm, the number of noise photons N of an optical quantum receiver results:

$$N = H_b \Omega_{fov} \pi R^2 \, \Delta t \, \Delta\lambda \tag{7.6}$$

where H_b is the brightness of the space background $[photons \cdot s^{-1} \cdot cm^{-2} \cdot nm^{-1} \cdot sr^{-1}]$, Ω_{fov} is the field of view of the telescope in $[sr]$, R is the telescope radius in $[cm]$, $\Delta\lambda$ is the optical bandwidth $[nm]$ and Δ_t is the detection time $[s]$.

The principal noise sources in inter-satellite link are the Zodiacal light (ZL)[1] and integrated starlight (ISL) that comes from direct starlight and from scattered light by interstellar dust. The highest noise level in the milky-way are on the Galactic Plane, but obviously the intensity and the numbers of source depending on the chose direction.

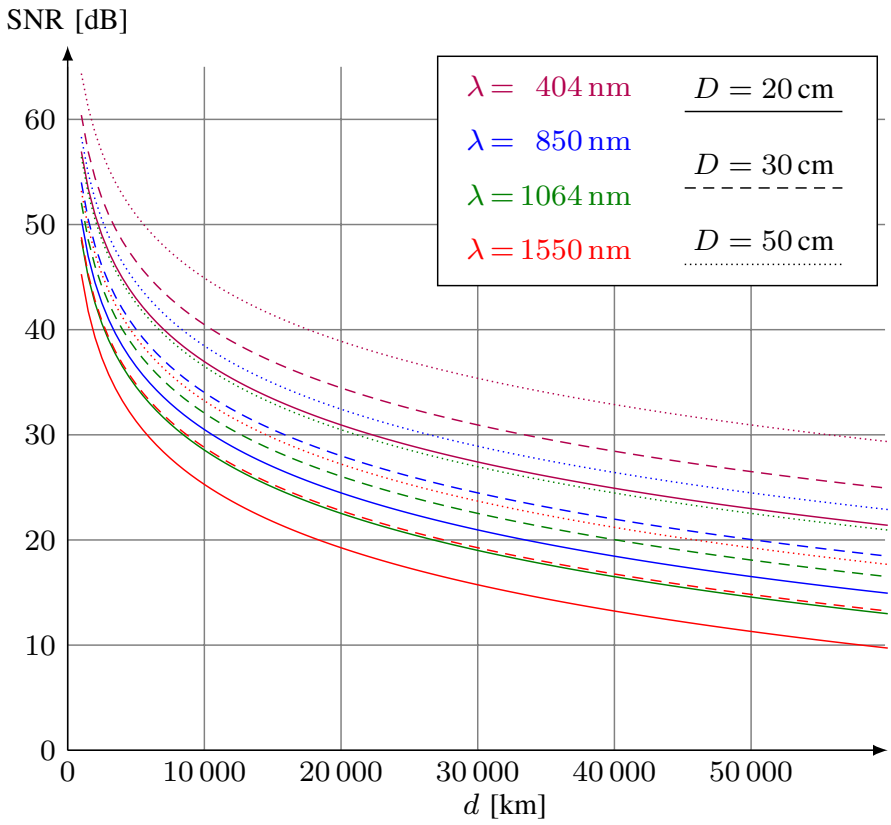


Figure 7.2: Simulated SNR versus link distance for different telescope diameters and wavelengths. The background noise level N (7.6) is assumed to be $10^6 ph/(s \cdot cm^2 \cdot nm \cdot sr)$. The source bandwidth is 1 nm, and the detection time is 1 ns.

7.2 HYBRID NETWORKS

7.2.1 *Navigation system*

The possibility of determining the relative position into the Earth with a very precise measure, is provided by the GNSS satellite network. The next generation of European navigation systems will be better both in terms of accuracy, availability and integrity, but also it will have the possibility of a dual-use in terms of more robustness, resilience and security. As saw in the previous Chapter 6, a good number of space missions have successfully tested optical communications techniques in space [101, 64, 105, 58]. This fact encourages additional developments of new devices for security applications looking to

1 Zodiacal light is sunlight reflected by interplanetary dust

a global network of secure and robust satellites. Security issues are a key point in the development of GNSS system, not only looking at the protection of the GNSS service signals against spoofing and/or jamming5 [54, 82], but even more relevantly for the authentication, integrity and confidentiality of the control signaling traffic. The impact of a malicious adversary hijacking GNSS satellites and acquiring the control may prove catastrophic implications.
The use of optical satellite-to-satellite and satellite-to-ground quantum links will allow unconditionally secure generation of cryptographic keys over satellite links and the construction of a secure key distribution space network [76, 53]. In fact most of the protocols that offer secure communication services (such as confidentiality, message authentication, access control, message integrity, ...) rely on cryptographic mechanisms (encryption, digital signature, etc.) that require the communicating parties to share secret keys. In this context QKD schemes offer unconditional security ensuring an high level of safety independently from the computation capabilities of the eavesdropper [41].

GALILEO CONSTELLATION ARCHITECTURE The GNSS Galileo architecture is formed by 27 satellites, 9 in each of three different orbital planes (called A, B, C), with a 56° inclination. Due to the relative motion of the satellite, the time windows available for the OQL transmission is a very crucial parameter. QC for key generation, pointing operation and time for transfer data are all necessary operations taking a slot time which have to be considered in the design analysis. Here we report the result of a simulation evaluating the slot time intervals depending the distance between the satellites, in order to evaluate the performance of a possible OQL like [41].

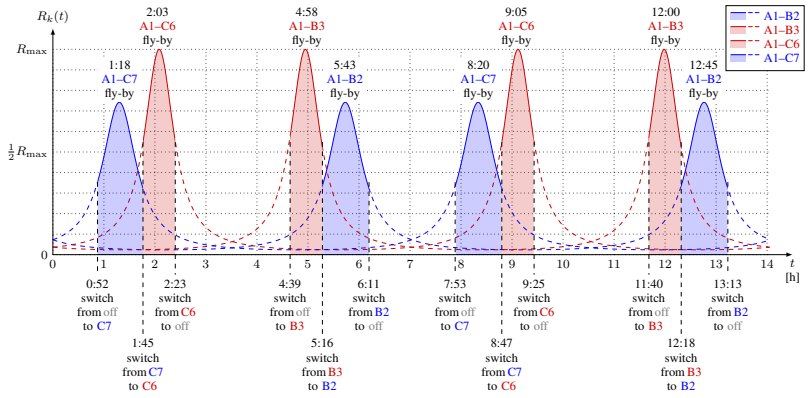


Figure 7.3: Simulation of link switching sequence for satellite $A1$. The shaded areas represent the total secret key length achievable in one period.To simplify the simulation it was assumed that orbits are circulars with a mean radius of $R = 29634$ km.

NETWORK TOPOLOGY Looking towards a satellites network, a natural trade-off between an high degree of connectivity and the volume of the payload must be sought. However a certain level of redundancy for reliable, safe and secure QKD is required. By alternately it is possible to think a different scenario where each satellite point, transmit and/or receive 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. There are two different feasible ways: a minimal one where is required one quantum transmitter, one telescope (suitably pointed) and one receiver over a classical communication system for exchanging public data. In figure 7.3 it is reported an example of this solution, where the satellite A1 can connect with other 4 satellites. The second way requires two quantum transmitter, one quantum receiver, two classical transceiver and two telescopes which can be pointed in different positions independently. This more complicated solution offers more possibilities of connection and higher secret key rate.

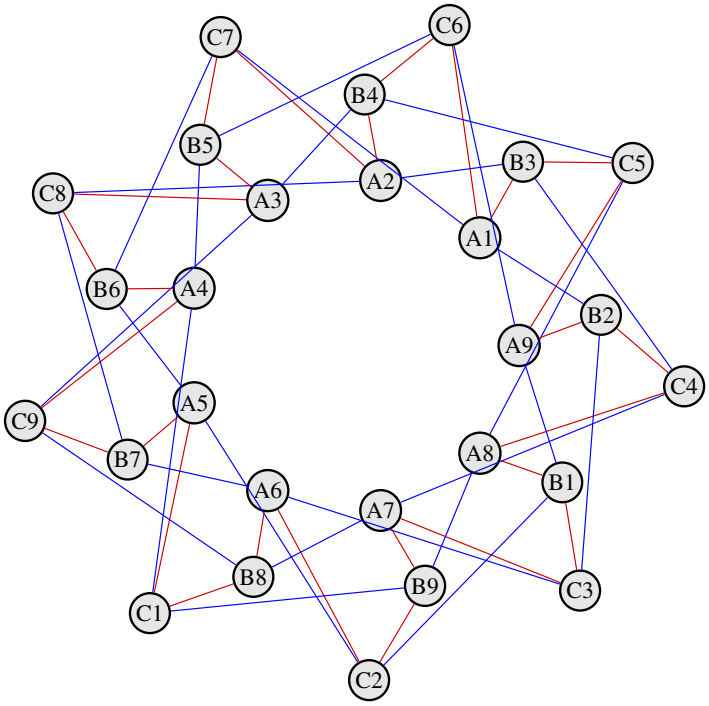


Figure 7.4: Connectivity graph of the proposed QKD network scheme over the GNSS Galileo constellation, employing only one telescope per satellite. Red edges represent links that have a minimum distance of 6623 km, blue edges represent links that have a minimum distance of 7687 km

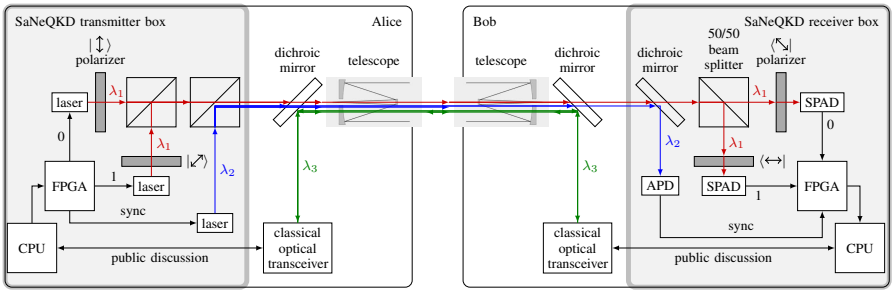


Figure 7.5: Block diagram for the B92 SaNeQKD transmitter (left) and receiver (right).

QKD PROTOCOL Due to the limitation impose by the dimension of satellite, the quantum payload must be chosen as light as possible, obviously ensuring reliability and security. In this context, the easiest QKD protocol which employs as few quantum state as possible is the B92, introduced in Chapter 2. From a security point of view, it is well known that the B92 protocol can be assumed insecure over a threshold channel efficiency, mostly in the case of a simplest implementation without a decoy-state method. Unfortunately in our experiments we adopt this protocol to demonstrate the perfect integration of a QKD system with an optical classical communication one (provided by Thales) without focusing on the security of the QKD protocol. In our implementation of B92 protocol we choose the following encoding maps: $0 \rightarrow |\updownarrow\rangle$, $1 \rightarrow |\nwarrow\searrow\rangle$ for Alice and $|\leftrightarrow\rangle \rightarrow 1$, $|\swarrow\nearrow\rangle \rightarrow 0$ for Bob. The scheme of the used setup, is reported in figure 7.2.

7.2.2 *Expected parameters and key length*

In order to allow a comparison between the theoretical rate and the experimental one, we introduce the main parameters playing a crucial role in the final rate. In the design of the SaNeQKD system, the expected final secret key rate is influenced by:

- 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. $\eta = 1/2$ for BB84 and $\eta = 1/4$ for B92)
- 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)

the sifted key rate can be written as:

$$R_{sift} = R_0 \eta A_{link} A_{rc} (1 - e^{-\mu}) \tag{7.7}$$

It is worth to note that in order to compute the final secret key rate, some further processing of the sifted key is required, channel estimation (for both QBER and link attenuation) information reconciliation and privacy amplification. We remand the reader to Chapter 2 for discussion about infinite and finite key regime, and in particular for the correct selection of the parameters according to the QKD chosen protocol.

7.3 EXPERIMENTAL RESULTS

Once we have designed and simulated the behavior of the OQL system, we proved experimentally in THALES (Torino) the entirely system. In Figure 7.5 is reported the implemented scheme for the free-space link experiment. Two Newtonian telescopes, with a primary mirror of 200 mm, were used for the pointing and for the link establishment. In particular in Figure 7.6 is reported an optical diagram of the principals components of the telescopes. A consideration about the telescope design must be done: in Chapter 3 we proposed an atmosphere turbulent model based on the Gaussian beam. This

choice was made both for simplicity but above all because the propagation of Gaussian beam is less prone to the degradation thanks to the greater amount of energy locked up in the center of the beam. The Newtonian reflector telescope however presents an obscuration (mirror M2) in the center of the spider. This leads to lose about half of the transmitting power, increasing the total loss of the channel. Moreover this fact affects also the average mean photons leaving the transmitter, reducing the security of the system. Here we report a preliminary analysis of the data, having just finished the experimental part in Torino during the last days of December. From a principle point of view, we created an entirely QKD system only based on optical communication (see section 7.4 for more details) able to generate and process keys. Moreover it was proven how our QKD system can be very portable and easily integrable. All the data reported in Figure 7.11 were collected in different run with different noise and attenuation conditions.
We obtain an average QBER of 5.7% in the case of quasi single photon transmission with an average sifted key length of 144 counts per packets. From a more mathematicians point, a further analysis in order to perfectly match the simulation system with the experimental one must be done. In addition we only reported the sifted key rate, that as we known from Chapter 2 is only the first step of QKD layer.

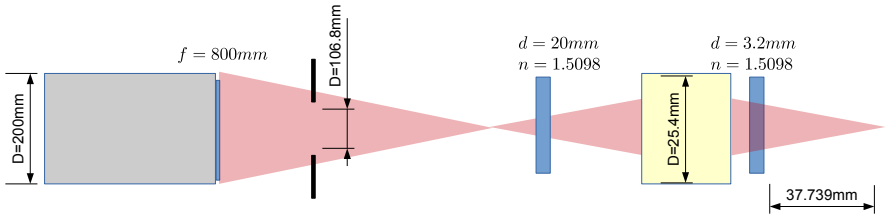


Figure 7.6: The completely optical scheme of the Newtonian reflector OQL telescope can be summarized with a system composed by three lenses. This permits to study the beam propagation inside the telescope and to estimate the intrinsic lossy.

Another important parameter in a QKD system is the errors introduced by the channel and from the depolarization of the photons. In Figure 7.8 we reported the experimental QBER as a function of the attenuation factor. In addition we plotted the theoretical expected QBER function calculated as:

$$Q = \frac{Q_0 + (1 - 2Q_0)N/S}{1 + (1 - 2Q_0)N/S} \tag{7.8}$$

where Q_0 represents the intrinsic QBER of the channel.

7.4 EXPERIMENTAL SETUP

A B92 protocol based on the Weak coherent pulse (WCP) laser is implemented in the OQL system. The lasers are controlled by a Virtex 6 FPGA, which permits a maximum theoretically rate about 2.4 Mbit/s. More details about the FPGA structure are reported in 2.11 on page 44. The two 850 nm single photon laser are injected in an optical fiber, to facilitate the integration between Alice part and the optical classical transceiver. In order

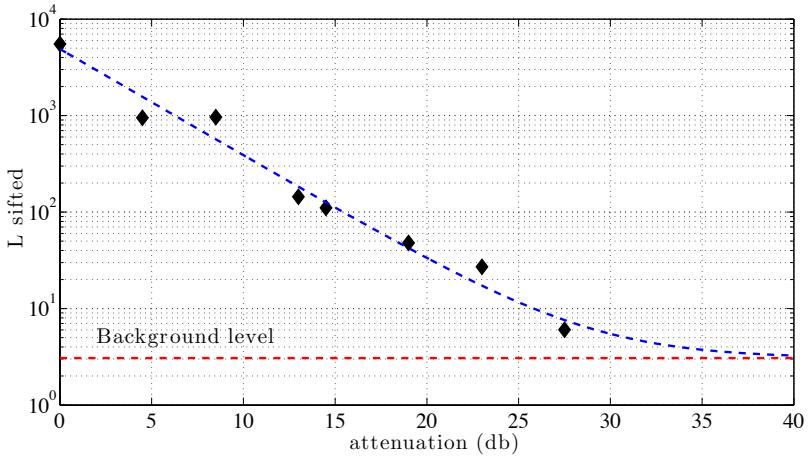


Figure 7.7: Sifted bit versus attenuation factor. Black diamonds is the measured experimental data, while the dotted blue line represent the theoretical rate in function of the attenuation of the channel. Red dotted line et the average background level for the experiment.

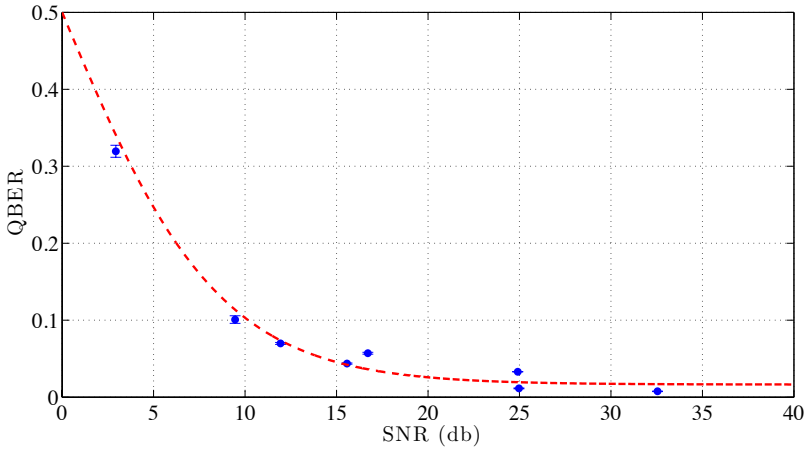


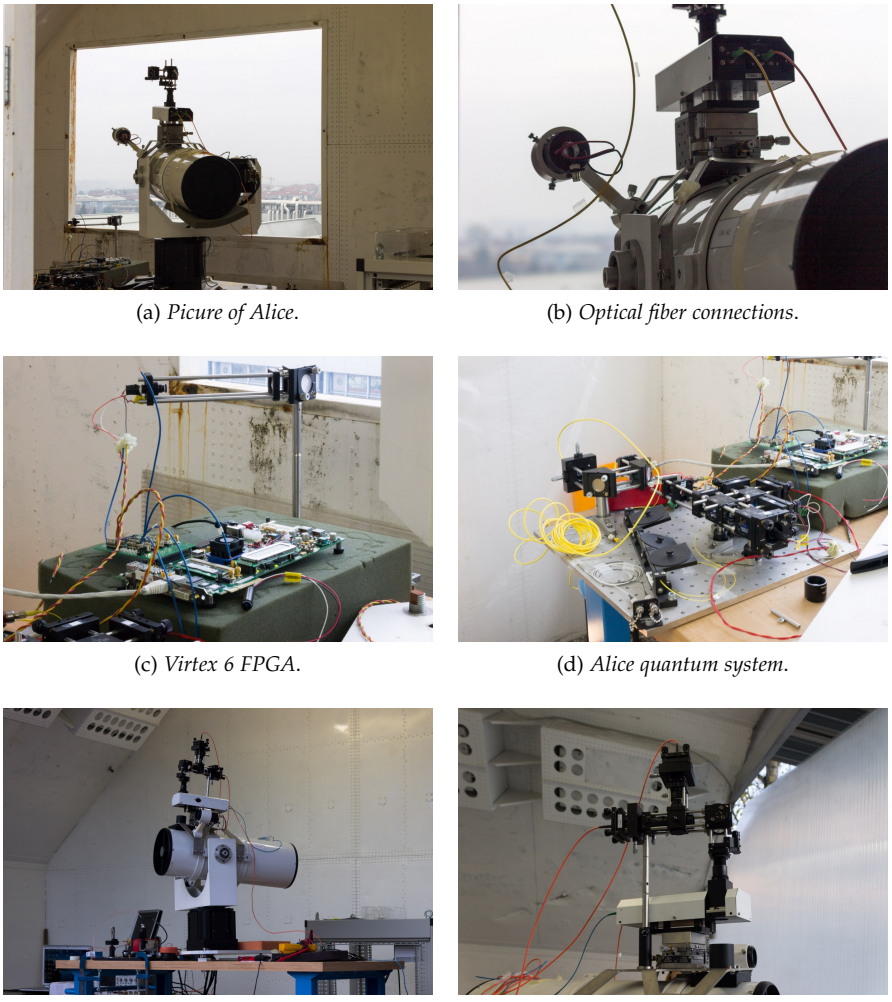
Figure 7.8: In this plot we reported the experimental QBER (blue dots) versus the measured SNR. The dotted red line represent the expected QBER depending on the attenuation factor.

to syncrhonize the two FPGA a 5 mW 808 nm infrared laser was used in a parallel contemporary channel. This fact is not a limitation because in the final system it can be easily integrated into the optical channel. During the experiment we have prefered to use a parallel channel due to a filter inside the optical transceiver. The quantum channel and the classical one (100 mW 1560 nm infrared laser) are combined together with a BS and then sent through the Newtonian telescope.

The corresponding receiver, employing a dichroic mirror in order to separate classical beam from quantum one. The receiving telescope is identical to the transmitter one and the structure is totally symmetric. From a classical point of view the infrared beam is collected by an optical fiber and then analyzed by an external photodiode. This permits the completely access to the classical pattern signal. From the other hand, a small receiver is mounted on the top of the telescope so allowing a better sensibility on the

quantum signal. The arriving photons are collected by a multimode optical fiber and then detect by SPAD. The detectors are linked to the FPGA, which through an Ethernet cable can pass the raw key to the transceiver, so as to allow Information Reconciliation (IR), PE and Privacy amplification (PA) operations. In order to decrease the dark counts, we filter background photons using an interferential filter before the SPAD aperture.

As reported we choose an experimental setup based on polarization encoding B92 protocol. As reported in Chapter 2 there exists a lot of QKD protocol based on different assumption and degree of freedom (e.g. phase distance between two wave packets). In this scenario the best feasible solution could be the alignment-free protocol proposed in [31]. In fact using the rotational invariant phase of single photons, it is possible to obtain a perfect alignment-free QKD system.



(a) *Picure of Alice.*

(b) *Optical fiber connections.*

(c) *Virtex 6 FPGA.*

(d) *Alice quantum system.*

(e) *Picture of the receiver.*

(f) *Bob quantum receiver.*

Figure 7.9: Picture of the OQL experiment made in collaboration with THALES (Torino).

7.5 SPACE ENVIRONMENT

Considering the possibility of a future quantum payload on satellites, we must take into account the space environment problem. This argument does not fall in the task of this thesis, but we would like to introduce some basic concepts useful for a completely description. It is known that the radiation flux is influenced by orbital altitude and inclination, see Figure 7.10. The most delicate instrument of a QKD are surely the detectors, both if you use SPAD both in the case of an APD detector [29]. Depending on the energy of the single particle and on the annual dose of radiation, the behavior of the detectors will change. For example experimental analysis of the LEO radiation environment suggests that uncooled Si APDs detectors, with thin shielding in a 400 km equatorial orbit, can operate for several years before dark counts saturate the quenching circuit.

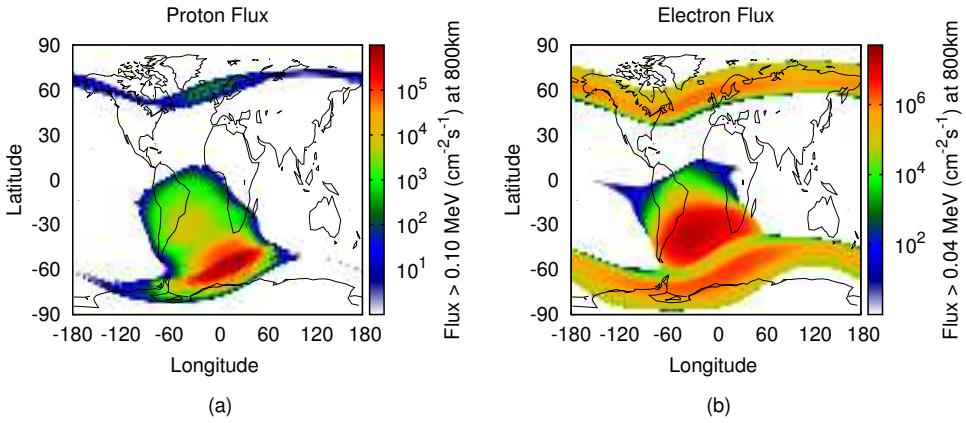


Figure 7.10: Radiation flux at 800 km altitude and 98 degree inclination: (a) Proton flux; (b) Electron flux.

ENVIRONMENT STRESS The space devices are subjected to a lot of stress: mechanical, thermal and electromagnetic damage will be possible. We report here a little analysis of these problems, trying to explain what are the main damages caused by space environment.

THERMAL Electronic devices used in space missions are usually enclosed in a controlled thermal environment inside the spacecraft interior. The internal temperature is determined by the external heat absorbed by the spacecraft and above all from the heat generated by the functioning electronic components. It is regulated by passive heat distribution and active heating elements. The increase of the temperature inside the satellite can be due to three kind of sources:

- incoming solar radiation (solar constant): $0 - 1367\ \mathrm{W/m^2}$;
- reflected solar energy (albedo): $0 - 0.32$ of the solar radiation; $0 - 450\ \mathrm{W/m^2}$ global annual mean;
- outgoing long-wave IR radiation emitted by the Earth and atmosphere: $100 - 270\ \mathrm{W/m^2}$.

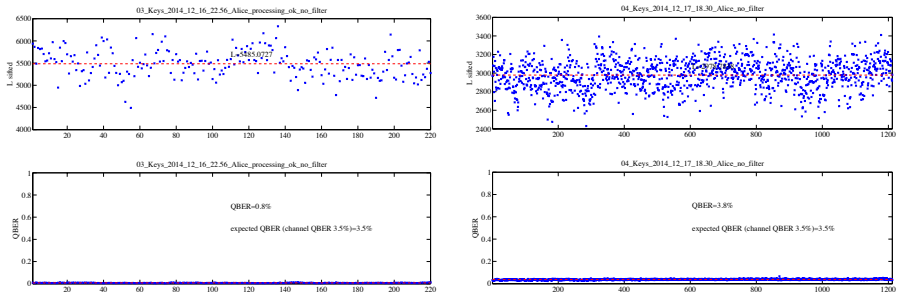
The reported values refer to an Earth orbiter.

VIBRATIONS Usually flight hardware is exposed to vibrations during launch and during the mission, in particular the launch vibrations originate from engine ignition and operations, atmospheric drag, and stage separations must be taken into account. Trajectory corrections using on-board engines cause vibrations while in orbit. The vibration environment can be subdivided in three different categories: acoustic vibrations, random vibrations and pyroshock. Acoustic noise represents the major source of vibrations.

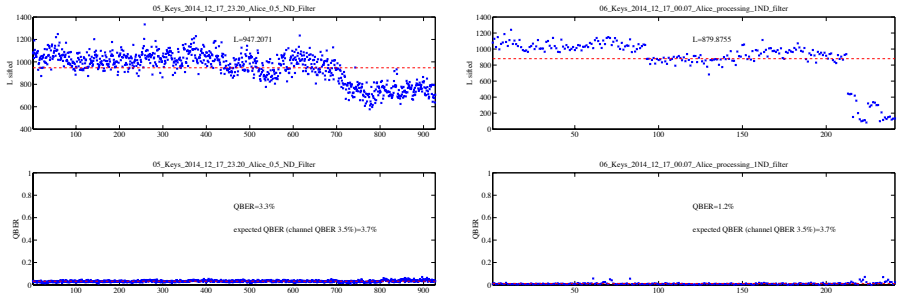
ELECTROMAGNETIC The electrostatic environment for parts and assemblies depends on the charging of a spacecraft, to which both the surrounding plasma environment and the spacecraft design contribute. Near the Earth, the plasma is dense and cold. Farther away, the density drops fast, however, the plasma energy increases out to geosynchronous orbit. The plasma environment is a dynamic one, determined by the interaction of the Earth magnetic field and the solar wind. Solar flares affect the plasma environment by heating and expanding the boundary of the neutral atmosphere, and by providing energetic particles, which increase the plasma density and temperature. The photo-effect under direct sunlight counteracts the charging by providing an outflow of low-energy electrons. This, however, may create potential differences between shaded and illuminated areas of a dielectric, which can cause electrostatic discharge. Satellites in LEO are exposed to cold dense ionospheric plasma.

7.6 CONCLUSION

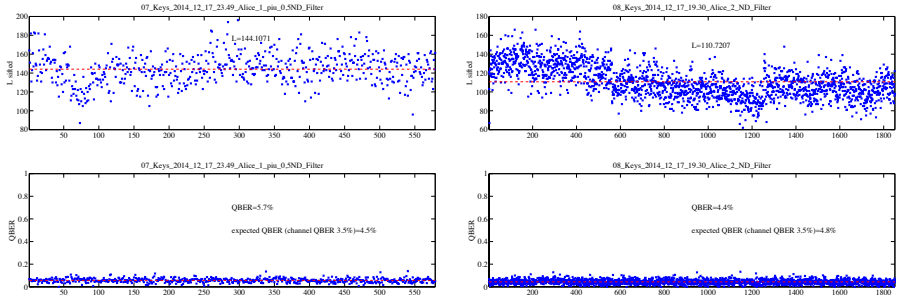
Once that space-to-ground quantum key distribution was considered feasible, as demonstrated in Chapter 5 and in Chapter 6, we consider a different scenario for the QC like the inter-satellite link between two or more moving terminals. In particular satellite like GPS or Glonass or future mission like Galileo are fundamental for the security point of view, and also a small tampering system could have disastrous consequences. In this perspective in order to increase the security of the GNSS satellite it was proposed a quantum system available on orbital spacecraft. We report an OQL experiment, in collaboration with TASI (Thalens Alenia Space Italia) where a space QKD terminal was implemented and tested in a free-space terrestrial link in order to demonstrate that a quantum application payload is available and possible for a GNSS constellation. It was proved that quantum system and optical classical payload could be entirely integrated in order to achieve secure key generation between to very distant satellites.



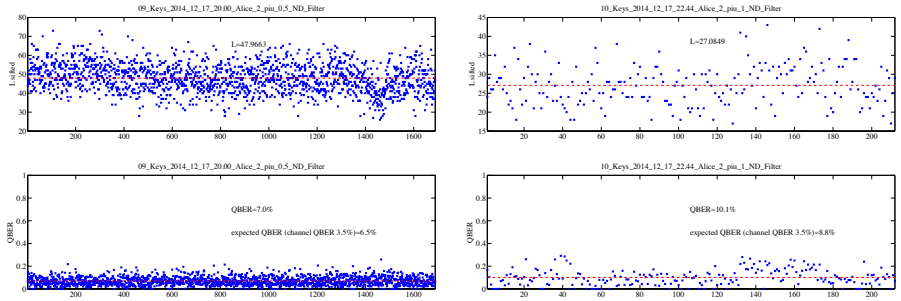
(a) *Without filter*. (b) *Without filter in different condition*.



(c) 0.5 *ND filter*. (d) 1 *ND filter*.



(e) 1.5 *ND filter*. (f) 2 *ND filter*.



(g) 2.5 *ND filter*. (h) 3 *ND filter*.

Figure 7.11: Plots of the obtained sifted bit L versus different attenuation scenarios. We report the rate achievable in different conditions of SNR. The dotted red line represents the average sifted bits and the average QBER in that environmental conditions. The data was acquired during several tests in different noise and weather conditions. A decreasing of the number of sifted bits during the same run, might be due to sudden change in the weather conditions. In particular during the observation nights the weather was foggy an cloudy.

8 RESULTS AND FUTURE WORK

In this chapter we resume the overall results obtained during this three years, explaining how these experiments pave the way for future Quantum communications and a Quantum satellites network.
In a global context, people doing Research have to look in the same direction, omitting general barriers or physical boundaries and work all together always seeking better results. With these words we look outside Europe, where there are a lot of projects about satellite QC and, in particular three of that deserve to be reported here. In Japan there exists a collaboration between JAA (Japan National Spatial) and University of Tokyo in order to demonstrate and improve actual quantum and classical optical communications. In particular during the month of May, Japan has launched the first satellite of their project, named SOCRATES that should orbit approximately for 2 years. SOCRATES is a LEO satellite equipped with a small optical payload (SOTA), able to send polarized weak coherent pulse between Space and an OGS; this future results should finally demonstrate the possibility to generate a single qubit into space and sending to the Earth. It is well known by the theory and demonstrated in a lot of experiments, that this kind of results should be possible, but a completely realization with an orbiting satellite has yet to be proven.
Instead in China there is a bigger project towards quantum Space called Chinese Quantum Science Satellite. The first satellite will be launched in the first months of 2016 and it will be equipped with a decoy state BB84 source, for finally demonstrating the possibility of satellite QKD. This satellite will orbit in a LEO distance and could be visible and trackable for a lot of OGS stations. In this perspective, collaborations with China project could be possible in order to create a small QKD network. Moreover this satellite should also have an entangled source, useful for experiments like Bell's violation and teleportation protocol. The plans of China are to create a network of satellites, both quantum and classical including an own Internationl Space Station (ISS), which will be launched before 2020 and where they can also test quantum experiments.

For what concerns American lands, Canadian universities like IQC has a project in collaboration with Canadian Space Agency (CSA) and other external companies, to realize a satellite for QC. In this case there are not available information about the future launch data. From their works and article we guess for a system in a downlink scenario, where the OGS should work as source and the satellite as receiver. They are studying from many years this solutions and they have proved, only by simulation, that in principle it could be possible, but obviously more lossy than the downlink solution.

In this context the work presented here shows how important the field of Quantum communications is, not only from theoretical physics point of view, but also with experimental implementation that could be very useful for the security of the people in the next years.

We would like to resume the main results of the four experiments, contextualizing into a possible field of application. As we known nowadays

telecommunications plays a crucial role in our daily lives. The possibility of exchanging secure information become more and more important in many areas, e.g. on-line purchases, emails and video chats. We use some fundamental laws of quantum physics to guarantee secure communications. Due to the natural imperfections of the devices and in the case of real QKD application, a theoretical analysis of the security isn't enough. We reported in Chapter 2 a finite key analysis of a real cryptographic system based on an asymmetric BB84 protocol, one of the most used in the polarization encoding scheme. This kind of analysis will offer a novel approach against the classical one, allowing an improvement of the final rate especially in a very bad scenario like satellite communications, where the attenuation of the channel is very high. We have experimentally demonstrated the feasibility of key distillation according to the finite-key analysis proposed and defined a less stringent definition of security, called pragmatic, that protects the protocol against intercept and resend attacks (the most probably in a real QKD system).

Once we have studied from a security point of view the QKD protocol implementation and realization, we took into exam the propagation of a quantum beam through the atmosphere, paying attention to some particular effects, like beam wondering, beam spreading and scintillations. We demonstrated in Chapter 2 how it is possible to establish secure key also in presence of noise and in the case of finite key regime. In order to increase the communication distance and to extend laboratory experiments in real life conditions, we performed a free-space QKD link in 2012 between La Palma and Tenerife islands in the Canary archipelago. It represent one of the most interesting scenario for a possible quantum link, because the proximity of Sahara desert and bad weather conditions make the environment very particular. From the astronomical point of view, the blanket of clouds that hide the scattering of city light, create a perfect conditions for space study and exploration; from the other side these clouds create a very turbulent channel once you look for an horizontal link, where a sender, positioned in the JKT telescope communicates with a receiver situated in OGS telescope. We explored atmosphere's effects, and we proved that polarized photons sent through 143 km of atmosphere have not be degraded. Moreover we introduced a new method of analysis in order to use atmospheric effects as a resource, so that increasing the SNR ratio. This method makes QC possible also in worst case conditions. Moreover we experimentally demonstrated that ARTS method is able to decrease the measured QBER allowing to extract secret key in extreme conditions, namely when the initial QBER is above the security threshold of 11%.

The most promising application of QKD is the generation of a provable unconditionally secure key at very distance location, which is not possible with classical cryptography. The use of satellites allows QC on a global world scale, an impossible task on ground with current optical fiber technology limited to 300 km. In order to achieve QKD through a Earth-Space channel, in the case of polarization encoding protocols, the degree of polarization of the transmitted radiation must be preserved. A possible way to verify this fundamental requirement is the study of the space channel using Laser Ranging system and a polarimeter. In a SLR system the reflection is done by optical components called CCRs, which ensure that the laser beam is retroreflected to the telescope direction. The behavior of polarization reflected by a CCRs is well known, in particular it has been widely proved that devices

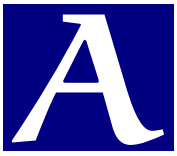
with a metal coated reflecting surface maintain the degree of polarization, while the ones without it cause a depolarizing effect on the incident beam. In fact data acquired at MLRO facility permitted us to verify the behaviour of two different type of satellite's corner cubes retroreflectors. In particular, it was observed that satellites with uncoated CCRs have a clear depolarization effect on a polarized laser pulse. On the other hand, the information provided by the channels of the polarimeter give good indications about the behaviour of metal-coated CCRs. In this experiment it was done a first demonstration of the feasibility of sending and receiving polarized classical photons from moving satellites. In this perspective we started from the results obtained in Chapter 5 to exploit QC using satellite corner cube retroreflectors as a quantum transmitter in orbit. A stable quantum link has been established between several low Earth orbit satellites and the MLRO of the Italian Space Agency in Matera, by transmitting different qubit states encoded in the photon polarization. The QBER has been kept steadily low for a total transmission time of 85 s. Indeed, we measured an average value of QQBER $= 4.5\%$, a level that is suitable for several QKD protocols and for the violation of Bell inequalities. Moreover, an important parameters like the mean photon number per pulse leaving the satellites was estimated to be of the order of one, as required in QKD. Better we proposed a new two-way protocol, in fact by exploiting modulated retroreflectors, which need a minimal payload on a satellite, our communication scheme could easily be turned into a fully operational satellite QKD system.

We improved the actual limit of single photon transmission, performing an experiment where Alice was positioned about 7000 km from Bob. Besides it was possible to demonstrate that our method works both for LEO and MEO satellite, allowing a good detection of the quantum signal over the noise counts. Unfortunately being Lageos an uncoated aluminum satellite, it was not possible to measure the QBER in the case of MEO satellite, but in a near future this kind of experiment will be done too.

Once that space-to-ground quantum key distribution was considered feasible, as demonstrated in Chapter 5 and in Chapter 6, we considered a different scenario for the QC like the intersatellite link between two or more moving terminals. In this chapter we focused on the extension of intersatellite communications into the quantum domain. The long distances involved and the fast relative motion are severe constraints, partially compensated by the absence of beam degradation due to the propagation in the atmosphere as well as the relatively low background noise level. In particular satellite like GPS or Glonass or future mission like Galileo are fundamental for the security point of view, and also a small tampering system could have disastrous consequences. In this perspective in order to increase the security of the GNSS satellite it was proposed a quantum system available on orbital spacecraft. We reported an OQL experiment, in collaboration with TASI (Thalens Alenia Space Italia) where a space QKD terminal was implemented and tested in a free-space terrestrial link in order to demonstrate that a quantum application payload is available and possible for a GNSS constellation. It was proven that quantum system and optical classical payload could be entirely integrated in order to achieve secure key generation between to very distant satellites.

The presented experiments could be represented as a perfect circle, starting with the choice of an achievable QKD protocol, moving in the direction of extending the actual limit of QC in different scenario. In this case we

increased the actual transmission of a quantum beam in a very turbulent link in order to look behind terrestrial link, implementing a QC system with moving terminal and fixing new limits in the quantum single photon propagation. Closing the circle with a very distant link point to point scenario, we demonstrated the feasibility of a completely optical payload for satellite. Our results pave the way to the implementation of a future Quantum worldwide network, extending the actual limit of QC and opening new scenarios for quantum satellite experiments and applications.



APPENDIX A

A.1 CLASSICAL POST-PROCESSING

After the parameter estimation phase, information reconciliation, error verification and privacy amplification are performed. Information reconciliation aims at correcting the discrepancies between $\mathbf{X}$ and $\mathbf{X}'$ that the channel may have introduced, thus allowing Bob to compute an estimate $\hat{\mathbf{X}}$ of $\mathbf{X}$. As a practical solution, we have chosen the Winnow scheme [23] which, by leveraging Hamming codes of different lengths over multiple iterations, allows an adaptive and lowly interactive error correction and represents a good trade-off between the high interactivity required by CASCADE and the low flexibility of LDPC code with limited key length. We fix an upper bound P_{fail} to the probability of a reconciliation failure and, under this constraint, we optimize the parameters of the Winnow scheme in order to minimize the expected (average) classical information leakage $\mathbb{E}[L_{\text{EC}}]$. First, given the average QBER on the $\mathbb{X}$ basis $Q_{\mathbb{X}}$, a threshold $Q_{\text{max}}^{\mathbb{X}} > Q_{\mathbb{X}}$ is fixed so that the empirical QBER $\hat{Q}_{\mathbb{X}}$ in the sifted key is higher than $Q_{\text{max}}^{\mathbb{X}}$ with probability less than $P_{\text{fail}}/2$. Then, the block sizes are chosen so that the output QBER is lower than $P_{\text{fail}}/(2n)$ whenever $\hat{Q}_{\mathbb{X}} < Q_{\text{max}}^{\mathbb{X}}$ and $\mathbb{E}[L_{\text{EC}}]$ is minimized, as detailed in [25]. Subsequently, an error verification mechanism such as the one proposed in [104] ensures that the protocol is ε_{cor}-correct, i.e., that $\mathbb{P}[\mathbf{X} \neq \hat{\mathbf{X}}] < \varepsilon_{\text{cor}}$, by comparing hashes of $(\lceil \log_2(P_{\text{fail}}/\varepsilon_{\text{cor}}) \rceil)$ bits. Namely, Alice chooses the hash function g randomly and uniformly from a class of universal$_2$ hash functions [27] (the class of Toeplitz matrices in our experimental setup) and computes her hash value $g_{\text{A}} = g(\mathbf{X})$. She then sends g_{A} and a compact representation of g to Bob, who computes $g_{\text{B}} = g(\hat{\mathbf{X}})$. The protocol aborts if the two hashes are different, i.e., if $g_{\text{A}} \neq g_{\text{B}}$. Finally, during the so-called privacy amplification, $\mathbf{X}$ and $\hat{\mathbf{X}}$ are compressed by means of a function which is, again, randomly and uniformly chosen from a class of universal$_2$ hash functions, in order to get the final secret keys $\mathbf{S}$ and $\hat{\mathbf{S}}$. The length ℓ of the final key and the corresponding amount of compression depend on the required level of secrecy, on the overall classical information leakage $L_{\text{EC}} + \lceil \log_2(P_{\text{fail}}/\varepsilon_{\text{cor}}) \rceil$, on the assumed attacker's model and on the estimate of the information leaked to the eavesdropper during the transmission over the quantum channel.

A.2 PROOF OF PRAGMATIC SECRECY

Proof of Theorem 1. Let t be the number of qubits observed and measured by Eve on the $\mathbb{X}$ basis among the n sifted bits. Then the Rényi entropy of order 2 for the sifted key, given all the information available to the eavesdropper, is lower-bounded by

$$R(\mathbf{X}|V) \geq n_{\text{EC}} - t, \tag{A.1}$$

being $R(\mathbf{X}|V) = -\sum_v p_V(v) \log_2 \left(\sum_{\mathbf{s}} p^2_{\mathbf{S}|V}(\mathbf{s}|v) \right)$.

Let us define the following pairs of complementary events, namely: let $A = \{\hat{Q}_{\mathbb{Z}} > Q_{\text{tol}}^{\mathbb{Z}}\}$ and $\bar{A} = \{\hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}\}$ be the aborting and non-aborting events, whereas $R = \{R(\mathbf{X}|V) \geq n_{\text{EC}} - a\}$ and $\bar{R} = \{R(\mathbf{X}|V) < n_{\text{EC}} - a\}$ define the events of acceptable and non-acceptable eavesdropping rate, respectively. Then,

$$H(\mathbf{S}|V) = \mathbb{E}[\log_2 \mathbb{P}(\mathbf{S}|V)|\bar{A}] = \tag{A.2}$$
$$= \mathbb{E}[\log_2 p(\mathbf{S}|V)|R,\bar{A}]\mathbb{P}[R|\bar{A}] + \mathbb{E}[\log_2 \mathbb{P}(\mathbf{S}|V)|\bar{R},\bar{A}]\mathbb{P}[\bar{R}|\bar{A}]\,. \tag{A.3}$$

The multiplication of $H(\mathbf{S}|V)$ by the probability of not aborting yields

$$\mathbb{P}[\bar{A}]H(\mathbf{S}|V) = \tag{A.4}$$
$$= \mathbb{E}[\log_2 p(\mathbf{S}|V)|R,\bar{A}]\mathbb{P}[R,\bar{A}] + \mathbb{E}[\log_2 \mathbb{P}(\mathbf{S}|V)|\bar{R},\bar{A}]\mathbb{P}[\bar{R},\bar{A}] \tag{A.5}$$
$$\leq \mathbb{E}[\log_2 p(\mathbf{S}|V)|R,\bar{A}] + \ell\mathbb{P}[\bar{R},\bar{A}]\,. \tag{A.6}$$

Finally, by applying corollary 4 in Reference [13] to a possibly aborting protocol that outputs a ℓ-bit key (i.e., $H(\mathbf{U}_{\mathbf{S}}) = \ell$), we have, for every a, ℓ,

$$\mathbb{P}[\hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}](\ell - H(\mathbf{S}|V)) \leq \tag{A.7}$$
$$\leq \frac{2^{-(n_{\text{EC}}-\ell-a)}}{\ln 2} + \ell\mathbb{P}[R(\mathbf{X}|V) < n_{\text{EC}} - a, \hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}]\,. \tag{A.8}$$

From (A.1), we can upper bound the probability on the right-hand side of (A.7) as

$$\mathbb{P}[R(\mathbf{X}|V) < n_{\text{EC}} - a, \hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}] \leq \mathbb{P}[t > a, \hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}] \tag{A.9}$$
$$= \mathbb{P}[t > a]\mathbb{P}[\hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}], \tag{A.10}$$

since the two events in the right-hand side brackets of equation (A.9) refer to disjoint qubit sets, namely those encoded in the $\mathbb{X}$ and $\mathbb{Z}$ basis, respectively, and are therefore independent. Furthermore, according to the selective individual attack model with attack rate q, t is a binomial random variable with parameters (n, q). Similarly, the number of measured errors on the $\mathbb{Z}$ basis, $k\hat{Q}_{\mathbb{Z}}$ is a binomial random variable with parameters $(k, Q_{\mathbb{Z}})$ and $Q_{\mathbb{Z}} = q/2$. Therefore, we can rewrite equation (A.10) as

$$\mathbb{P}[t > a]\mathbb{P}[\hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}] = (1 - F_{n,q}(a))(F_{k,q/2}(kQ_{\text{tol}}^{\mathbb{Z}})) = \tag{A.11}$$
$$= I_q(a+1, n-a)I_{1-q/2}(k(1-Q_{\text{tol}}^{\mathbb{Z}}), kQ_{\text{tol}}^{\mathbb{Z}} + 1), \tag{A.12}$$

with $F_{n,q}(\cdot)$ denoting the cumulative distribution function of a binomial random variable with parameters (n, q), and similarly for $F_{k,q/2}(\cdot)$. The last step is then assured by equation 6.6.4 in Reference [3].
Eventually, condition (2.30), together with definition (2.31) and given that $\mathbb{P}[\hat{Q}_{\mathbb{Z}} \leq Q_{\text{tol}}^{\mathbb{Z}}] = 1 - p_{\text{abort}}$, ensures that for any $q \in [0, 1]$ we get

$$\ell - H(\mathbf{S}|V) \leq \frac{\delta_{\text{sec}}}{1 - p_{\text{abort}}}, \qquad \forall\, a, \ell. \tag{A.13}$$

Relationship between equation (2.28) and (2.26). The Pinsker inequality (see section 11.6 in [30] and [116]) ensures that

$$\frac{1}{2}\|p_{\mathbf{S}V} - u_{\mathbf{S}}q_V\|_1 \leq \sqrt{\frac{\ln 2}{2}\mathbb{D}(p_{\mathbf{S}V}||u_{\mathbf{S}}q_V)} \tag{A.14}$$

where $u_{\mathbf{S}}$ is the uniform distribution on $\mathbf{S}$ and $\mathbb{D}(p||q)$ is the relative entropy between the p and q distributions. By minimizing each term with respect to q_V, we get

$$\begin{aligned} \min_{q_V} \frac{1}{2}\|p_{\mathbf{S}V} - u_{\mathbf{S}}q_V\|_1 &\leq \min_{q_V} \sqrt{\frac{\ln 2}{2}\mathbb{D}(p_{\mathbf{S}V}||u_{\mathbf{S}}q_V)} && \text{(A.15)} \\ &= \sqrt{\frac{\ln 2}{2}\mathbb{D}(p_{\mathbf{S}V}||u_{\mathbf{S}}p_V)} && \text{(A.16)} \\ &= \sqrt{\frac{\ln 2}{2}(H(\mathbf{U}_{\mathbf{S}}) - H(\mathbf{S}|V))}\,, && \text{(A.17)} \end{aligned}$$

where (A.16) is due to $\mathbb{D}(p_{\mathbf{S}V}||u_{\mathbf{S}}q_V) = \mathbb{D}(p_{\mathbf{S}V}||u_{\mathbf{S}}p_V) + \mathbb{D}(p_V||q_V) \leq \mathbb{D}(p_{\mathbf{S}V}||u_{\mathbf{S}}p_V)$. It is then straightforward to see that

$$\begin{aligned} H(\mathbf{U}_{\mathbf{S}}) - H(\mathbf{S}|V) \leq \frac{2}{\ln 2}\frac{\varepsilon_{\text{sec}}^2}{1-p_{\text{abort}}} \Rightarrow \\ \Rightarrow \min_{q_V} \frac{1}{2}\|p_{\mathbf{S}V} - u_{\mathbf{S}}q_V\|_1 \leq \frac{\varepsilon_{\text{sec}}}{(1-p_{\text{abort}})}. \end{aligned} \tag{A.18}$$

Relationship between equation (2.28) and (2.29). The uniformity condition trivially derives from the fact that $H(S|V) \leq H(S)$. Also, from basic information theory, we know that

$$I(\mathbf{S};V) = H(\mathbf{S}) - H(\mathbf{S}|V) \leq H(\mathbf{U}_{\mathbf{S}}) - H(\mathbf{S}|V), \tag{A.19}$$

since $\mathbf{S}$ has maximal entropy (i.e., $H(\mathbf{S}) = \ell$) if and only if it is uniformly distributed. Now, since condition (2.28) is verified for any IS attack strategy, and therefore for any outcome V of the eavesdropper measurement on the quantum system E, the security condition directly follows.

APPENDIX B

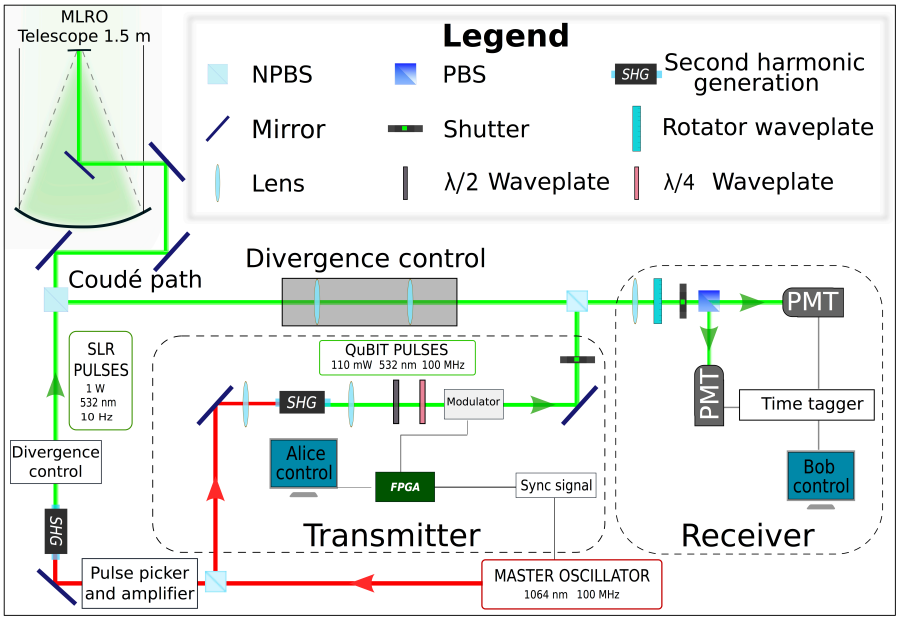


Figure B.1: Detail scheme of the experiment.

B.1 POLARIZATION COMPENSATION IN THE DOWNLINK

The polarization state generated on the optical table of the MLRO observatory is subjected to a unitary transformation due to the Coudé path of the telescope. Indeed, the Coudé path is composed of mirrors $M_1, \ldots, M_7$ as in B.2, with M_1 and M_2 the primary and secondary mirror of the telescope.

If the mirrors are coated to have π phase shift between s- and p- polarization (corresponding to a σ_z transformation), the transformation in the uplink channel is given by

$$U_{\text{up}} = \sigma_z \, R\left(\frac{\pi}{2} - \theta_{\text{el}}\right) \sigma_z \, R(\theta_{\text{az}}) \, \sigma_z \, R\left(\frac{\pi}{2}\right) ,$$

where θ_{az} and θ_{el} are the azimuth and elevation angles of the telescope and $R(\theta)$ is a rotation of the reference frame given by:

$$R(\theta) = e^{-i\theta\sigma_y} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} .$$

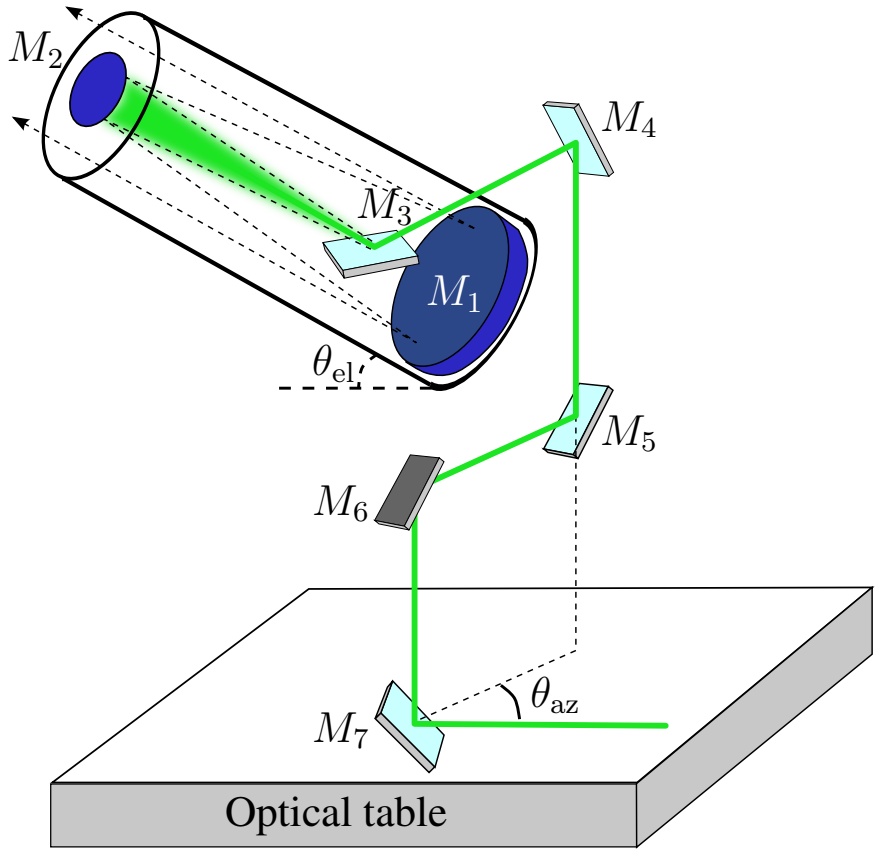


Figure B.2: Schematic scheme of the Coudé path.

With an input polarization $|\psi\rangle = \begin{pmatrix} \cos\alpha \\ e^{i\phi}\sin\alpha \end{pmatrix}$, the polarization at the output of the telescope is given by $|\psi'\rangle = U_{up}|\psi\rangle$. Since the CCRs induce a transformation of σ_z and the downlink channel can be written as

$$U_{down} = R\left(\frac{\pi}{2}\right)\sigma_z\, R(\theta_{az})\,\sigma_z\, R\left(\frac{\pi}{2}-\theta_{el}\right)\sigma_z\,,$$

the received polarization state is given by

$$|\psi_{rec}\rangle = U_{down}\,\sigma_z\,U_{up}|\psi\rangle\,.$$

By using the property $\sigma_z\,R(\theta) = R(-\theta)\,\sigma_z$, it is easy to demonstrate that

$$|\psi_{rec}\rangle = \sigma_z\,|\psi\rangle\,,$$

showing that the uplink rotation is compensated by the downlink transformation.
This compensation is at the base of our proposed two-way protocol. Indeed, if the CCRs is equipped with an active element like a Faraday Rotator at the entrance face, the transformation induced by the CCRs is given by $U_{CCR}(\phi) = R(-\phi)\sigma_z R(\phi)$ with $R(\phi) = e^{-i\phi\sigma_y}$. The overall transformation is then obtained as

$$|\psi_{rec}(\phi)\rangle = U_{down}\,U_{CCR}(\phi)\,U_{up}|\psi\rangle = R(2\phi)\sigma_z|\psi\rangle\,.$$

If the input state is horizontally polarized, the received state is thus rotated by an angle of 2ϕ in the laboratory reference frame. By modulating ϕ, the two-way QKD protocol can be realized.

B.2 THREE DECOY STATES PROTOCOL

As demonstrated in [106], it is possible to improve the key rate of the QKD protocol by using more decoy states. The secret key rate of the BB84 protocol, namely the ratio between secure and sent bits, is given by

$$r = Q_0 + Q_1[1 - h_2(e_1)] - Q_\mu f(E_\mu) h_2(E_\mu)\,, \tag{B.1}$$

where Q_μ is the total gain (the fraction of detected bits over the sent bits), Q_1 is the gain of the one-photon states, Q_0 the gain of the vacuum states, E_μ the total QBER, e_1 the upper bound of errors of the one-photon states, h_2 the binary entropy $h_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$. The term $f(E_\mu)$ represents the efficiency of the classical error correction protocol.

While the term Q_0, Q_1 and e_1 cannot be directly measured by using the attenuated source with mean photon number μ, the decoy state method allows to bound such quantities. By using infinite number of decoy states Q_0, Q_1 and e_1 can be perfectly estimated. For a lossy channel with error e_{ch} and overall transmittivity η, the expected parameter are $\widetilde{Q}_0 = Y_0$ (the background rate), $\widetilde{Q}_1 = Y_0 + 1 - e^{-\eta\mu}$ and $\widetilde{e}_1 = \frac{e_{\text{ch}}\eta + Y_0/2}{Y_0+\eta}$.

More simply, as shown in [67], by using a single decoy state with mean photon number ν_1 and the vacuum decoy it is possible to obtain the following bounds

$$\begin{aligned} &Q_0 = Y_0 \quad \text{(background rate)}\,,\\ &Q_1 \geq Q_1^L \equiv \frac{\mu^2 e^{-\mu}}{\mu\nu_1 - \nu_1^2}\left(Q_{\nu_1}e^{\nu_1} - Q_\mu e^{\mu}\frac{\nu_1^2}{\mu^2} - \frac{\mu^2-\nu_1^2}{\mu^2}Y_0\right)\,,\\ &e_1 \leq \frac{E_{\nu_1}Q_{\nu_1}e^{\nu_1} - Y_0/2}{Q_1^L e^{\mu}\frac{\nu_1}{\mu}}\,, \end{aligned} \tag{B.2}$$

with Q_{ν_1} and E_{ν_1} the measured gain and QBER of the decoy signal. A low value of ν_1 improves the bounds and for $\nu_1 \to 0$, the lower bound Q_1^L approaches to $\widetilde{Q}_1$. However, for any $\nu_1 < \mu$ a looser bound is obtained still allowing positive key rates for low losses.

Alternatively, a better bound on Q_1^L with $\nu \sim 1$ can be obtained by using more than one non-vacuum decoy state as demonstrated in [106]. In the case of three decoy states plus vacuum, the bound Q_1^L can be improved to

$$Q_1^L = \sum_{k=0}^{3}\frac{e^{\nu_k}Q_{\nu_k} - Y_0}{\nu_k}\prod_{j=0,j\neq k}^{4}\frac{\nu_j}{\nu_j - \nu_k}\,, \tag{B.3}$$

with $\nu_0 = \mu$.

The advantage can be appreciated by the simulation shown in Extended Data B.3, illustrating the key rate in function of the losses for the one decoy+vacuum and three decoy+vacuum case. We used the following parameters: dark rate $Y_0 = 2\cdot 10^{-8}$, channel error $e_{\text{ch}} = 0.01$, $f(E_\mu) = 1.2$ and $\mu = 1.3$. From the figure it is evident that three decoy states with mean photon number given by $\nu_1 = 0.9$, $\nu_2 = 0.95$ and $\nu_3 = 1$ well estimate the key

rate achievable with infinite number of decoys. Then pulses with mean photon number close to 1 are sufficient to implement QKD over long distances.

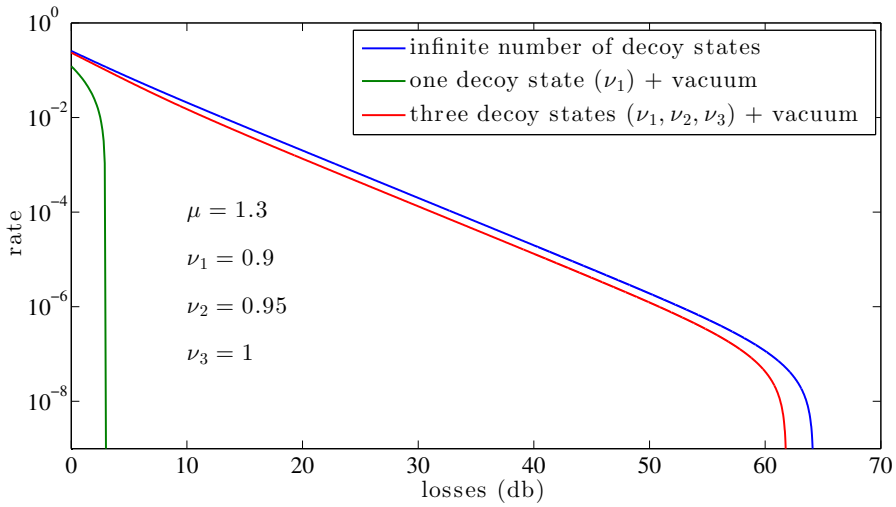


Figure B.3: Key rate in function of the losses for the one decoy+vacuum and three decoy+vacuum case.

BIBLIOGRAPHY

[1] Laser components. URL http://www.lasercomponents.com/de-en/lasers/laser-diodes/. (Cited on page 84.)

[2] International Laser Ranging Service. URL http://ilrs.gsfc.nasa.gov/network/stations/active/MATM_general.html. (Cited on pages 78 and 79.)

[3] M Abramowitz and I A Stegun. *eds*. Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Dover Publications, 1972. (Cited on page 126.)

[4] Silvestre Abruzzo, Sylvia Bratzik, Nadja K Bernardes, Hermann Kampermann, Peter Van Loock, and Dagmar Bruß. Quantum repeaters and quantum key distribution : analysis of secret key rates arXiv : 1208 . 2201v1 [quant-ph] 10 Aug 2012. (Cited on page 35.)

[5] Alberto Dall Arche. *Sviluppo di un polarimetro per l'analisi di un canale quantistico fra la terra e lo spazio.* PhD thesis, 2010. (Cited on page 85.)

[6] D.A. Arnold. Cross section of ILRS satellites, 2003. URL http://ilrs.gsfc.nasa.gov/docs/2003/CrossSectionReport.pdf. (Cited on page 96.)

[7] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W.R. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9(6):1541–1551, November 2003. ISSN 1077-260X. doi: 10.1109/JSTQE.2003.820918. URL http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=1263786. (Cited on pages 64 and 94.)

[8] Davide Bacco, Matteo Canale, Nicola Laurenti, Giuseppe Vallone, and Paolo Villoresi. Experimental QKD with finite-key security analysis for noisy channels. pages 1–17, 2012. (Cited on page 55.)

[9] Davide Bacco, Matteo Canale, Nicola Laurenti, Giuseppe Vallone, and Paolo Villoresi. Experimental quantum key distribution with finite-key analysis for noisy channels. *Nature Communications*, 4:1–8, 2013. doi: 10.1038/ncomms3363. URL http://dx.doi.org/10.1038/ncomms3363. (Cited on pages 35 and 93.)

[10] Joonwoo Bae and Antonio Acín. Key distillation from quantum channels using two-way communication protocols. *Physical Review A*, 75 (1):012334, January 2007. ISSN 1050-2947. doi: 10.1103/PhysRevA.75.012334. URL http://link.aps.org/doi/10.1103/PhysRevA.75.012334. (Cited on pages 50, 57, and 94.)

[11] M. Ben-Or. Security of BB84 QKD Protocol, 2002. URL |http://www.msri.Org/publications/ln/insri/2002/quantumintro/ben-or/2/. (Cited on page 28.)

[12] C. H. Bennett. Privacy in a Quantum World. *Science*, 284(5415): 747–748, April 1999. ISSN 00368075. doi: 10.1126/science.284.5415.747. URL http://www.sciencemag.org/content/284/5415/747.summary. (Cited on page 93.)

[13] C H Bennett, G Brassard, C Crepeau, and Generalized Privacy Amplification U. Maurer. IEEE Transactions on Information Theory, 1995. (Cited on page 126.)

[14] Charles H. Bennett. Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, vol. 68:3121–3124, 1992. (Cited on pages 29, 34, and 43.)

[15] Charles H. Bennett and Gilles Brassard. Quantum Cryptography: public key distribution and coin tossing. Bangalore, India, 1984. (Cited on pages 19, 24, 29, 33, 35, 42, and 94.)

[16] Eli Biham and Tal Mor. Security of Quantum Cryptography against Collective Attacks. *Physical Review Letters*, 78(11):2256–2259, March 1997. ISSN 0031-9007. doi: 10.1103/PhysRevLett.78.2256. URL http://link.aps.org/doi/10.1103/PhysRevLett.78.2256. (Cited on page 28.)

[17] C Bonato, A Tomaello, V Da Deppo, G Naletto, and P Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11 (4):045017, April 2009. ISSN 1367-2630. doi: 10.1088/1367-2630/11/4/045017. (Cited on pages 61, 62, 65, and 87.)

[18] Cristian Bonato, Markus Aspelmeyer, Thomas Jennewein, Claudio Pernechele, Paolo Villoresi, and Anton Zeilinger. Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link Abstract :. 14(21):10050–10059, 2006. (Cited on pages 61, 79, and 94.)

[19] J-p Bourgoin, B L Higgins, and B Helou. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New Journal of Physics*, 023006, 2012. doi: 10.1088/1367-2630/15/2/023006. (Cited on pages 50, 65, and 94.)

[20] Dagmar Bruß. Optimal Eavesdropping in Quantum Cryptography with Six States. *Physical Review Letters*, 81(14):3018–3021, October 1998. ISSN 0031-9007. doi: 10.1103/PhysRevLett.81.3018. URL http://link.aps.org/doi/10.1103/PhysRevLett.81.3018. (Cited on page 29.)

[21] Vasiliev Burmistrov, Parkhomenko, Shargorodsky. Reflector, Larets and Meteor-3M: what did we learn from tracking campaign results. Proc. of 14th Int. Workshop on Laser Ranging, San Fernando (ES), 2004. URL http://cddis.gsfc.nasa.gov/lw14/docs/papers/tar3a$\delimiter"026E30F$_vbm.pdf. (Cited on page 96.)

[22] W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons. Practical Free-Space Quantum Key Distribution over 1 km. *Physical Review Letters*, 81(15): 3283–3286, October 1998. ISSN 0031-9007. doi: 10.1103/PhysRevLett.81.3283. URL http://link.aps.org/doi/10.1103/PhysRevLett.81.3283. (Cited on page 50.)

[23] W. Buttler, S. Lamoreaux, J. Torgerson, G. Nickel, C. Donahue, and C. Peterson. Fast, efficient error reconciliation for quantum cryptography. *Physical Review A*, 67(5):052303, May 2003. ISSN 1050-2947. doi: 10.1103/PhysRevA.67.052303. URL http://link.aps.org/doi/10.1103/PhysRevA.67.052303. (Cited on page 125.)

[24] RYQ Cai and V Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11, 2009. (Cited on page 35.)

[25] M Canale, Davide 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. *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies - ISABEL*, 2011. (Cited on pages 37, 43, and 125.)

[26] Ivan Capraro, Andrea Tomaello, Alberto Dall Arche, Ruper Ursin, Giuseppe Vallone, and Paolo Villoresi. Impact of turbulence in long range quantum and classical communications. pages 1–5, 2012. (Cited on pages 50 and 54.)

[27] J L Carter and M N Wegman. Universal Classes of Hash Function. *Journal of Computer and System Sciences*, 18:143–154, 1979. (Cited on page 125.)

[28] Bob Coecke. The logic of entanglement, February 2004. URL http://arxiv.org/abs/quant-ph/0402014. (Cited on page 15.)

[29] S Cova, M Ghioni, a Lacaita, C Samori, and F Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Applied optics*, 35(12):1956–76, April 1996. ISSN 0003-6935. URL http://www.ncbi.nlm.nih.gov/pubmed/21085320. (Cited on page 118.)

[30] T M Cover and J A Thomas. Elements of Information Theory, 2nd edition, Willey-Interscience, 2006. (Cited on page 126.)

[31] Vincenzo D'Ambrosio, Eleonora Nagali, Stephen P. Walborn, Leandro Aolita, Sergei Slussarenko, Lorenzo Marrucci, and Fabio Sciarrino. Complete experimental toolbox for alignment-free quantum communication. *Nature Communications*, 3:961, July 2012. ISSN 2041-1723. doi: 10.1038/ncomms1951. URL http://www.nature.com/doifinder/10.1038/ncomms1951. (Cited on page 117.)

[32] John J Degnan. Millimeter Accuracy Satellite Laser Ranging ' A Review. *Geodynamics Series*, 1993. (Cited on pages 61, 66, 71, 96, 97, 98, and 104.)

[33] F. Dios, J.A. Rubio, and A. Rodrìguez. Scintillation and beam-wander analysis in an optical ground station-satellite uplink. *Appl. Opt. 43 (19), 3866–3873*, 2004. (Cited on pages 61 and 62.)

[34] David P. DiVincenzo and IBM. The Physical Implementation of Quantum Computation, February 2000. URL http://arxiv.org/abs/quant-ph/0002077. (Cited on pages 9 and 10.)

[35] Miloslav Dušek, Mika Jahma, and Norbert Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Physical Review A*, 62(2):022306, July 2000. ISSN 1050-2947. doi: 10.1103/PhysRevA.62.022306. URL http://link.aps.org/doi/10.1103/PhysRevA.62.022306. (Cited on page 34.)

[36] Miloslav Dušek, Norbert Lütkenhaus, and Martin Hendrych. Chapter 5 – Quantum cryptography. In *Progress in Optics*, volume 49, pages 381–454. 2006. ISBN 9780444527325. doi: 10.1016/S0079-6638(06)49005-3. URL http://www.sciencedirect.com/science/article/pii/S0079663806490053. (Cited on pages 34 and 54.)

[37] D Elser, T Bartley, B Heim, Ch Wittmann, D Sych, and G Leuchs. Feasibility of free space quantum key distribution with coherent polarization states. *New Journal of Physics*, 11(4):045014, April 2009. ISSN 1367-2630. doi: 10.1088/1367-2630/11/4/045014. URL http://stacks.iop.org/1367-2630/11/i=4/a=045014?key=crossref.5c7475e666045f944ed1de03e2ce399f. (Cited on page 50.)

[38] C Erven, B Heim, E Meyer-Scott, J P Bourgoin, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, December 2012. ISSN 1367-2630. doi: 10.1088/1367-2630/14/12/123018. URL http://stacks.iop.org/1367-2630/14/i=12/a=123018?key=crossref.089ae0f8e61943da6737ad19870b0a83. (Cited on pages 50, 51, and 57.)

[39] R.L. Fante. Electromagnetic beam propagation in turbulent media. *Proceedings of the IEEE*, 63(12):1669–1692, December 1975. ISSN 0018-9219. doi: 10.1109/PROC.1975.10035. URL http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=1451964. (Cited on page 109.)

[40] David L. Shumaker George J. Zissis,Joseph S. Accetta. The Infrared & Electro-Optical Systems Handbook. Sources of Radiation, Volume 2. 1993. URL http://www.researchgate.net/publication/235170852_The_Infrared__Electro-Optical_Systems_Handbook._Sources_of_Radiation_Volume_1. (Cited on page 50.)

[41] Francesca Gerlin, Nicola Laurenti, Giampiero Naletto, Giuseppe Vallone, Paolo Villoresi, Luciana Bonino, Sergio Mottini, and Zoran Sodnik. Design optimization for quantum communications in a GNSS intersatellite network. In *2013 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6. IEEE, June 2013. ISBN 978-1-4799-0486-0. doi: 10.1109/ICL-GNSS.2013.6577252. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6577252. (Cited on page 112.)

[42] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320, February 2006. ISSN 1050-2947. doi: 10.1103/PhysRevA.73.022320. URL http://link.aps.org/doi/10.1103/PhysRevA.73.022320. (Cited on page 99.)

[43] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, March 2002. ISSN 0034-6861. doi: 10.1103/RevModPhys.74.145. URL http://link.aps.org/doi/10.1103/RevModPhys.74.145. (Cited on page 29.)

[44] Daniel Greenberger, Klaus Hentschel, and Friedel Weinert, editors. *Compendium of Quantum Physics*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. ISBN 978-3-540-70622-9. doi: 10.1007/978-3-540-70626-7. URL http://www.springerlink.com/index/10.1007/978-3-540-70626-7. (Cited on page 93.)

[45] Hall A. Cirrus Cloud Model, In Atmospheric Transmittance/Radiance, 1983. (Cited on page 68.)

[46] Jun Hasegawa, Masahito Hayashi, Tohya Hiroshima, Akihiro Tanaka, and Akihisa Tomita. Experimental Decoy State Quantum Key Distribution with Unconditional Security Incorporating Finite Statistics. June 2007. URL http://www.researchgate.net/publication/1891255_Experimental_Decoy_State_Quantum_Key_Distribution_with_Unconditional_Security_Incorporating_Finite_Statistics. (Cited on page 35.)

[47] H. Hemmati. *Near-Earth Laser Communications* -. CRC Press Book, 2009. URL http://www.crcpress.com/product/isbn/9780824753818. (Cited on page 64.)

[48] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18):2044–2046, November 1987. ISSN 0031-9007. doi: 10.1103/PhysRevLett.59.2044. URL http://link.aps.org/doi/10.1103/PhysRevLett.59.2044. (Cited on page 15.)

[49] Ryszard Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009. ISSN 0034-6861. doi: 10.1103/RevModPhys.81.865. URL http://link.aps.org/doi/10.1103/RevModPhys.81.865. (Cited on page 15.)

[50] Richard Hughes and Jane Nordholt. Physics. Refining quantum cryptography. *Science (New York, N.Y.)*, 333(6049):1584–6, September 2011. ISSN 1095-9203. doi: 10.1126/science.1208527. URL http://www.sciencemag.org/content/333/6049/1584.full&link_type=GOOGLESCHOLAR. (Cited on page 93.)

[51] Richard J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer. Quantum cryptography. *Contemporary Physics*, 36(3):149–163, May 1995. ISSN 0010-7514. doi: 10.1080/00107519508222149. URL http://www.tandfonline.com/doi/abs/10.1080/00107519508222149. (Cited on page 23.)

[52] Richard J Hughes, Jane E Nordholt, Derek Derkacs, and Charles G Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, 4:43–43, July 2002. ISSN 1367-2630. doi: 10.1088/1367-2630/4/1/343. URL http://stacks.iop.org/1367-2630/4/i=1/a=343?key=crossref.d7b8b45f84c813d48668b496880b2be8. (Cited on page 50.)

[53] R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreuax, G.L. Morgan, J.E. Nordholt, and C.G. Peterson. Quantum cryptography for secure satellite communications. In *2000 IEEE Aerospace Conference. Proceedings (Cat. No.00TH8484)*, volume 1, pages 191–200. IEEE, February 2000. ISBN 0-7803-5846-5. doi: 10.1109/AERO.2000.879387. URL http://www.researchgate.net/publication/3869062_Quantum_cryptography_for_secure_satellite_communications. (Cited on page 112.)

[54] Todd E. Humphreys. Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 49(2):1073–1090, April 2013. ISSN 0018-9251. doi: 10.1109/TAES.2013.6494400. URL http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6494400. (Cited on page 112.)

[55] B Huttner, N Imoto, N Gisin, and T Mor. Quantum cryptography with coherent states. *Physical review. A*, 51(3):1863–1869, March 1995. ISSN 1050-2947. URL http://www.ncbi.nlm.nih.gov/pubmed/9911795. (Cited on page 37.)

[56] Won-Young Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Review Letters*, 91(5):057901, August 2003. ISSN 0031-9007. doi: 10.1103/PhysRevLett.91.057901. URL http://link.aps.org/doi/10.1103/PhysRevLett.91.057901. (Cited on page 34.)

[57] B. C. Jacobs and J. D. Franson. Quantum cryptography in free space. *Optics Letters*, 21(22):1854, November 1996. ISSN 0146-9592. doi: 10.1364/OL.21.001854. URL http://ol.osa.org/abstract.cfm?URI=ol-21-22-1854. (Cited on page 50.)

[58] R. Meyer K. Bohmer, M. Gregory, F. Heine, H. Kampfner, R. Lange, M. Lutzer. Laser communication terminals for the European Data Relay System. (Cited on page 111.)

[59] Ralph Kalibjian. Stokes polarization vector and Mueller matrix for a corner-cube reflector. *Optics Communications*, 240(1-3):39–68, October 2004. ISSN 00304018. doi: 10.1016/j.optcom.2004.06.045. URL http://www.sciencedirect.com/science/article/pii/S003040180400639X. (Cited on page 80.)

[60] Ralph Kalibjian. Polarization preserving corner cubes. *Optics & Laser Technology*, 44(1):239–246, February 2012. ISSN 00303992. doi: 10.1016/j.optlastec.2011.06.025. URL http://www.sciencedirect.com/science/article/pii/S003039921100185X. (Cited on page 80.)

[61] L. C. Andrews; R. L. Phillips; D. Wayne; T. Leclerc; P. Sauer; R. Crabbs; J. Kiriazes. Near-ground vertical profile of refractive-index fluctuations, 2009. URL http://spie.org/Publications/Proceedings/Paper/10.1117/12.820369. (Cited on page 46.)

[62] Masato Koashi. Complementarity, distillable secret key, and distillable entanglement. page 4, April 2007. URL http://arxiv.org/abs/0704.3661. (Cited on page 28.)

[63] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Physical review letters*, 98(14):140502, April 2007. ISSN 0031-9007. URL http://www.ncbi.nlm.nih.gov/pubmed/17501254. (Cited on pages 37 and 38.)

[64] Volodymyr Kuzkov, Sergii Kuzkov, Dmytro Volovyk, Zoran Sodnik, Vincenzo Caramia, and Sergii Pukha. Laser Ground System for Communication Experiments with ARTEMIS. In *International Conference on Space Optical Systems and Applications 2012 (ICSOS 2012)*, October 2012. URL http://www.researchgate.net/publication/236339926_Laser_Ground_System_for_Communication_Experiments_with_ARTEMIS. (Cited on page 111.)

[65] Ronald L. Phillips Larry C. Andrews. *Laser Beam Propagation through Random Media, Second Edition*. SPIE Publications, 2nd edition. (Cited on page 109.)

[66] H. Lo. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056, March 1999. ISSN 00368075. doi: 10.1126/science.283.5410.2050. URL http://www.sciencemag.org/content/283/5410/2050.abstract. (Cited on page 93.)

[67] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy State Quantum Key Distribution. *Physical Review Letters*, 94(23):230504, June 2005. ISSN 0031-9007. doi: 10.1103/PhysRevLett.94.230504. URL http://link.aps.org/doi/10.1103/PhysRevLett.94.230504. (Cited on pages 34, 96, and 131.)

[68] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas Cerf, Rosa Tualle-Brouri, Steven McLaughlin, and Philippe Grangier. Quantum key distribution over 25km with an all-fiber continuous-variable system. *Physical Review A*, 76(4):042305, October 2007. ISSN 1050-2947. doi: 10.1103/PhysRevA.76.042305. URL http://link.aps.org/doi/10.1103/PhysRevA.76.042305. (Cited on page 50.)

[69] Marco Lucamarini, Giovanni Di Giuseppe, and Kiyoshi Tamaki. Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states. *Physical Review A*, 80(3):032327, September 2009. ISSN 1050-2947. doi: 10.1103/PhysRevA.80.032327. URL http://link.aps.org/doi/10.1103/PhysRevA.80.032327. (Cited on page 34.)

[70] Thomas S. Lundgren. Kolmogorov two-thirds law by matched asymptotic expansion. *Physics of Fluids*, 14(2):638, February 2002. ISSN 10706631. doi: 10.1063/1.1429965. URL http://scitation.aip.org/content/aip/journal/pof2/14/2/10.1063/1.1429965. (Cited on page 47.)

[71] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304, April 2000. ISSN 1050-2947. doi: 10.1103/PhysRevA.61.052304. URL http://link.aps.org/doi/10.1103/PhysRevA.61.052304. (Cited on page 28.)

[72] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin. Time-bin entangled qubits for quantum communication created by femtosecond pulses. *Physical Review A*, 66(6):062308, December 2002. ISSN 1050-2947. doi: 10.1103/PhysRevA.66.062308. URL http://link.aps.org/doi/10.1103/PhysRevA.66.062308. (Cited on page 29.)

[73] Ueli Maurer. Secret key agreement by public discussion from common information. pages 733–742. Information Theory, IEEE Transactions on, 1993. (Cited on pages 24 and 50.)

[74] Ueli M. Maurer. IEEE Transactions on Information Theory, 1993. (Cited on page 51.)

[75] Mayers Dominic. *Advances in Cryptology CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, Berlin, Heidelberg, July 1996. ISBN 978-3-540-61512-5. doi: 10.1007/3-540-68697-5. (Cited on page 28.)

[76] Evan Meyer-scott, Zhizhong Yan, Allison Macdonald, Jean-philippe Bourgoin, and H Hannes. How to implement decoy-state quantum key distribution for a satellite uplink with 50 dB channel loss. *Phys. Rev. A*, pages 1–9, 2012. (Cited on page 112.)

[77] Atsushi Minato and Nobuo Sugimoto. Design of a Four-Element, Hollow-Cube Corner Retroreflector for Satellites by use of a Genetic Algorithm. *Applied Optics*, 37(3):438, January 1998. ISSN 0003-6935. doi: 10.1364/AO.37.000438. URL http://ao.osa.org/abstract.cfm?URI=ao-37-3-438. (Cited on page 80.)

[78] Giampiero Naletto, Vania Da Deppo, Maria Guglielmina Pelizzo, Roberto Ragazzoni, and Enrico Marchetti. Optical design of the Wide Angle Camera for the Rosetta Mission. *Applied Optics*, 41(7):1446, March 2002. ISSN 0003-6935. doi: 10.1364/AO.41.001446. URL http://ao.osa.org/abstract.cfm?URI=ao-41-7-1446. (Cited on page 83.)

[79] Baccichet Nicola. *Study of the transformation of polarization of a quantum channel in space*. PhD thesis, 2012. (Cited on page 85.)

[80] Dominic C. O'Brien, Grahame E. Faulkner, and David J. Edwards. Optical Properties of a Retroreflecting Sheet. *Applied Optics*, 38(19):4137, July 1999. ISSN 0003-6935. doi: 10.1364/AO.38.004137. URL http://ao.osa.org/abstract.cfm?URI=ao-38-19-4137. (Cited on page 80.)

[81] Jian-wei Pan, Dik Bouwmeester, and Harald Weinfurter. Experimental entanglement swapping: entangling photons that never interacted. *Phys. Rev. Lett*, 80, 1998. doi: 10.1103/PhysRevLett.80.3891. (Cited on page 15.)

[82] Panagiotis Papadimitratos and Aleksandar Jovanovic. Protection and fundamental vulnerability of GNSS. In *2008 IEEE International Workshop on Satellite and Space Communications*, pages 167–171. IEEE, October 2008. ISBN 978-1-4244-1947-0. doi: 10.1109/IWSSC.2008.4656777. URL http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=4656777. (Cited on page 112.)

[83] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11(7):075001, July 2009. ISSN 1367-2630. doi: 10.1088/1367-2630/11/7/075001. URL http://stacks.iop.org/1367-2630/11/i=7/a=075001. (Cited on page 50.)

[84] W Pfaff, B J Hensen, H Bernien, S B van Dam, M S Blok, T H Taminiau, M J Tiggelman, R N Schouten, M Markham, D J Twitchen, and R Hanson. Quantum information. Unconditional quantum teleportation between distant solid-state quantum bits. *Science (New York, N.Y.)*, 345(6196):532–5, August 2014. ISSN 1095-9203. doi: 10.1126/science.1253512. URL http://www.sciencemag.org/content/345/6196/532.abstract. (Cited on page 17.)

[85] Renato Renner. Security of Quantum Key Distribution, 2005. (Cited on page 28.)

[86] David Rideout, Thomas Jennewein, Giovanni Amelino-Camelia, Tommaso F Demarie, Brendon L Higgins, Achim Kempf, Adrian Kent, Raymond Laflamme, Xian Ma, Robert B Mann, Eduardo Martín-Martínez, Nicolas C Menicucci, John Moffat, Christoph Simon, Rafael Sorkin, Lee Smolin, and Daniel R Terno. Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities. *Classical and Quantum Gravity*, 29(22):224011, November 2012. ISSN 0264-9381. doi: 10.1088/0264-9381/29/22/224011. URL http://inspirehep.net/record/1119056?ln=it. (Cited on page 93.)

[87] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. ISSN 00010782. doi: 10.1145/359340.359342. URL http://dl.acm.org/citation.cfm?id=359340.359342. (Cited on page 21.)

[88] D Rosenberg, C G Peterson, J W Harrington, P R Rice, N Dallmann, K T Tyagi, K P McCabe, S Nam, B Baek, R H Hadfield, R J Hughes, and J E Nordholt. Practical long-distance quantum key distribution system using decoy levels. *New Journal of Physics*, 11(4):045009, April 2009. ISSN 1367-2630. doi: 10.1088/1367-2630/11/4/045009. URL http://iopscience.iop.org/1367-2630/11/4/045009/fulltext/. (Cited on page 35.)

[89] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: real implementation problems. June 2009. URL http://cds.cern.ch/record/1186194?ln=it. (Cited on page 28.)

[90] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*, 92(5):057901, February 2004. ISSN 0031-9007. doi: 10.1103/PhysRevLett.92.057901. URL http://link.aps.org/doi/10.1103/PhysRevLett.92.057901. (Cited on pages 29 and 34.)

[91] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*, 92(5):057901, February 2004. ISSN 0031-9007. doi: 10.1103/PhysRevLett.92.057901. URL http://link.aps.org/doi/10.1103/PhysRevLett.92.057901. (Cited on page 34.)

[92] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, September 2009. ISSN 0034-6861. doi: 10.1103/RevModPhys.81.1301. URL http://link.aps.org/doi/10.1103/RevModPhys.81.1301. (Cited on pages 26, 27, 29, 35, 37, 93, and 96.)

[93] Thomas Scheidl, Eric Wille, and Rupert Ursin. Quantum optics experiments to the International Space Station ISS: a proposal. pages 1–6, 2012. (Cited on page 94.)

[94] A. A. Semenov and W. Vogel. Quantum light in the turbulent atmosphere. *Physical Review A*, 80(2):021802, August 2009. ISSN 1050-2947. doi: 10.1103/PhysRevA.80.021802. URL http://link.aps.org/doi/10.1103/PhysRevA.80.021802. (Cited on page 51.)

[95] A A Semenov and W Vogel. Entanglement transfer through the turbulent atmosphere. 023835(2010):1–12, 2012. (Cited on page 51.)

[96] Alexander V Sergienko. *Quantum Communications and Cryptography*. 2006. (Cited on page 61.)

[97] George H. Seward. Measurement and characterization of angular reflectance for cube-corners and microspheres. *Optical Engineering*, 38(1):164, January 1999. ISSN 0091-3286. doi: 10.1117/1.602077. URL http://opticalengineering.spiedigitallibrary.org/article.aspx?articleid=1075625. (Cited on page 80.)

[98] C. E. Shannon. Communication Theory of Secrecy Systems*. *Bell System Technical Journal*, 28(4):656–715, October 1949. ISSN 00058580. doi: 10.1002/j.1538-7305.1949.tb00928.x. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6769090. (Cited on page 23.)

[99] Peter Shor and John Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2):441–444, July 2000. ISSN 0031-9007. doi: 10.1103/PhysRevLett.85.441. URL http://link.aps.org/doi/10.1103/PhysRevLett.85.441. (Cited on pages 28 and 31.)

[100] David Edmund Smith. *Contributions of Space Geodesy to Geodynamics: Technology*. American Geophysical Union, 1993.

ISBN 0875905269. URL http://books.google.com/books?id=502WQbmiIHEC&pgis=1. (Cited on page 79.)

[101] Toni Tolker-Nielsen and Gotthard Oppenhauser. High-Power Lasers and Applications. pages 1–15. International Society for Optics and Photonics, April 2002. doi: 10.1117/12.464105. URL http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=873352. (Cited on page 111.)

[102] Andrea Tomaello. Quantum communication channels between Earth and Space and Space to Earth. 2012. (Cited on page 85.)

[103] Andrea Tomaello, Cristian Bonato, Vania Da Deppo, Giampiero Naletto, and Paolo Villoresi. Link budget and background noise for satellite quantum key distribution. *Advances in Space Research*, 47(5):802–810, March 2011. ISSN 02731177. doi: 10.1016/j.asr.2010.11.009. URL http://linkinghub.elsevier.com/retrieve/pii/S0273117710007362. (Cited on page 94.)

[104] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3:634, January 2012. ISSN 2041-1723. doi: 10.1038/ncomms1631. URL http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3274703&tool=pmcentrez&rendertype=abstract. (Cited on pages 29, 31, 35, 37, 38, 44, 55, and 125.)

[105] Morio Toyoshima, Shiro Yamakawa, Toshihiko Yamawaki, Katsuyoshi Arai, Marcos Reyes, Angel Alonso, Zoran Sodnik, and Benoit Demelenne. Ground-to-satellite optical link tests between Japanese laser communications terminal and European geostationary satellite ARTEMIS. In G. S. Mecherle, Cynthia Y. Young, and John S. Strykewski, editors, *Free-Space Laser Communication Technologies*, pages 1–15. International Society for Optics and Photonics, June 2004. doi: 10.1117/12.530138. URL http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=1321976. (Cited on page 111.)

[106] Toyohiro Tsurumaru, Alexandre Soujaeff, and Shigeki Takeuchi. Exact minimum and maximum of yield with a finite number of decoy light intensities. *Physical Review A*, 77(2):022319, February 2008. ISSN 1050-2947. doi: 10.1103/PhysRevA.77.022319. URL http://link.aps.org/doi/10.1103/PhysRevA.77.022319. (Cited on pages 96 and 131.)

[107] R.K. Tyson. *Principles of adaptive optics*. Academic Press, 1998. (Cited on page 48.)

[108] R.K. Tyson. Adaptive optics engineering handbook., 2000. (Cited on page 48.)

[109] Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Tobias Schmitt-manderbach, Henning Weier, Martin Fu, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. 010504(January):1–4, 2007. doi: 10.1103/PhysRevLett.98.010504. (Cited on pages 35 and 50.)

[110] V.P. Vasilev and I.S. Gashkin. Improved ball-lens retroreflector satellite for operation in higher orbits. 2012. URL http://www.ipa.nw.ru/conference/wpltn2012/docs/25/1500$\delimiter"026E30F$sokolov.pdf. (Cited on page 96.)

[111] 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 Journal of Physics*, 10(3):033038, March 2008. ISSN 1367-2630. doi: 10.1088/1367-2630/10/3/033038. (Cited on pages 61, 79, and 94.)

[112] S. C. H. Wang and M. A. Plonus. Optical beam propagation for a partially coherent source in the turbulent atmosphere. *Journal of the Optical Society of America*, 69(9):1297, September 1979. ISSN 0030-3941. doi: 10.1364/JOSA.69.001297. URL http://www.opticsinfobase.org/abstract.cfm?URI=josa-69-9-1297. (Cited on page 46.)

[113] Shun Watanabe, Ryutaroh Matsumoto, Tomohiko Uyematsu, and Yasuhito Kawano. Key rate of quantum key distribution with hashed two-way classical communication. pages 1–21. (Cited on page 51.)

[114] Shun Watanabe, Ryutaroh Matsumoto, Tomohiko Uyematsu, and Yasuhito Kawano. Key rate of quantum key distribution with hashed two-way classical communication. *Physical Review A*, 76(3): 032312, September 2007. ISSN 1050-2947. doi: 10.1103/PhysRevA.76.032312. URL http://link.aps.org/doi/10.1103/PhysRevA.76.032312. (Cited on page 57.)

[115] Stephen Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1): 78–88, January 1983. ISSN 01635700. doi: 10.1145/1008908.1008920. URL http://dl.acm.org/citation.cfm?id=1008908.1008920. (Cited on page 19.)

[116] Mark M Wilde. *Quantum Information Theory*. Cambridge University Press, 2013. (Cited on page 126.)

[117] Juan Yin, Yuan Cao, Shu-bin Liu, Ge-sheng Pan, Tao Yang, Zhongping Zhang, Fu-min Yang, Yu-ao Chen, Cheng-zhi Peng, and Jian-wei Pan. Experimental Single-Photon Transmission from Satellite to Earth. 010504(2007):269–273, 2013. (Cited on page 94.)

[118] M. Żukowski, A. Zeilinger, M. Horne, and A. Ekert. "Event-ready-detectors" Bell experiment via entanglement swapping. *Physical Review Letters*, 71(26):4287–4290, December 1993. ISSN 0031-9007. doi: 10.1103/PhysRevLett.71.4287. URL http://link.aps.org/doi/10.1103/PhysRevLett.71.4287. (Cited on page 93.)

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography *"The Elements of Typographic Style"*. `classicthesis` is available for both LaTeX and LyX:

http://code.google.com/p/classicthesis/

The titlepage is inspired by the `suftesi` template included in the package called `frontespizio` developed by Enrico Gregorio.

Final Version as of February 2, 2015 (`classicthesis` version 4.1).