POLITECNICO DI TORINO

SCUOLA DI DOTTORATO
Dottorato in Ingegneria Elettronica e delle Comunicazioni
XXVI ciclo

Tesi di Dottorato

Soft Decoding Techniques for Quantum Key Distribution (QKD) and Weak Energy Optical Communication

Inam Bari

Tutore
prof. Marina Mondin

Coordinatore del corso di dottorato
prof. Ivo Montrosset

February 2014

This thesis is affectionately dedicated to my late father, *Akhunzada Ghulam Bari*, and my mother. The dreams they envisioned and the efforts they put in for realizing them, have always been an unwavering source of inspiration and determination for me.

Summary

This thesis deals with soft-information based decoding for optical and quantum communication application which uses low number of photon either at the transmitter for security reasons or at the receiver because of some extreme optical environment.In this thesis, both single photon and multi-photon transmission will be considered when characterizing the quantum communication system in the context of the proposed QKD protocol. When referring to multi-photon transmission, coherent states will be considered, generated using weak laser pulses (WLP) sources.

The main part of the thesis is focused on soft information based information reconciliation for Quantum Key Distribution (QKD). A novel composite channel model for QKD is identified, which includes a parallel of private quantum channel and a public classic channel. The information is transmitted on private quantum channel and redundancy on the public classical channel. The Log-Likelihood Ratios, - also called soft-metrics - derived from the two channels are jointly processed at the receiver, exploiting capacity achieving soft-metric based iteratively decoded block codes. The performance of the proposed mixed-soft-metric algorithms are studied via simulations as a function of the system parameters.

Other low photon number applications have also been considered, such as weak-laser pulses (WLP) communication.In both Quantum Key Distribution (QKD) and high-photon efficiency optical communications with direct detection, the transmission channel is typically modeled either as a Binary Symmetric Channel (BSC), or a Poisson Photon Channel (PPC) with binary input, and the sufficient statistic at the channel output is typically obtained with a simple hard decision on the received random variable. The availability of public side-channel information typical of QKD applications, or the multilevel characteristic of the Poissonian output of weak-energy optical links may however allow the use of soft metrics and of soft-metric-based iteratively decoded error correcting codes, which may be useful to counteract the channel errors typical of such low-energy channels.

In this thesis we will indeed show how soft-metric based metrics can be obtained in the considered scenarios, and how capacity achieving Forward Error Correcting (FEC) codes such as soft-metric based Low Density Parity Check (LDPC) codes and polar codes can be employed over QKD and Poisson cannels, exploring the limits of the achievable performance gains. We show that the classical channel capacity of the suggested BIMO model

is higher than the capacity of the BSC model, and that the use of the BIMO model allows to feed the channel decoder with soft information, in the form of Log-Likelihood Ratios (LLRs), achieving a significant reduction in Bit Error Rate (BER) and Frame Error Rate (FER) with respect to classical hard-metric-based schemes which should be used in conjunction with a BSC channel model. Furthermore, the possible application of soft-metrics to information reconciliation protocols is discussed, with the goal of designing QKD protocols able to take advantage of the available soft-information. In particular, the use of FEC codes for information reconciliation could lead to QKD protocols able to minimize the interaction between transmitter (Alice) and receiver (Bob), allowing for higher quantum bit-error-rates.

This thesis also offers a preliminary investigation on the use of FEC LDPC codes for information reconciliation when the underlying channel is a Q-ary DMC, for QKD applications based on higher photon flux levels with spatial entanglement of twin beams in PDC, and shows that acceptable error reconciliation efficiency values are obtained with reasonable complexity.

In general, the availability of the soft-metric allows for the use of advanced iterative soft-decoding techniques during the information reconciliation phase, significantly reducing the residual bit and frame error rates with subsequent impact on the achievable secret key rates which is, as said before, is one of the fundamental performance guideline in QKD. The proposed protocol, while having a negligible cost, can reduce the residual FER in QKD systems, largely reducing the interaction required between the two parties involved, increasing the key rate and protecting the secrecy of the information exchanged

Acknowledgments

First of all i would like to thank God almighty for giving me the strength and ability to perform this task.

It is with immense gratitude that I acknowledge the support and help of my supervisor Prof. Marina Mondin for showing her trust in me and for her constant commitment in teaching me as researcher and professional,all the while maintaining the most of humble and appreciative attitude, more than a tutor she has been like a mother to me. I owe my deepest gratitude to her husband prof.Fred Daneshgaran from California state university Los Angeles for his ideas, help and availability, and I consider it an honor to work with them.

We all have people in our lives who make success both possible and rewarding. My family steadfastly supported and encouraged me during the low and high times.My profound love and thanks to my parents and family members for their constant support and kindness at every stage of my life.

I would also like to thank prof. Marco Genovese, Stefano Olivares,Francesca Vatta and Telecom Italia for research collaboration during my PhD.

Deepest thanks and regards to my senior and colleague Maria Teresa Delgado for her help and assistance.

I would like to thank Higher Education Commission (HEC) Pakistan for providing me financial support during my PhD.

I can not complete this acknowledgement without thanking all my friends who have been a family for me in Italy.

Table of contents

List of figures

Chapter 1

Introduction

“Photonics is the optical equivalent of light. Photonic systems uses light, instead of electricity, to process, store and transmit energy. Photonics is a pervasive technology, which is capable of of significantly influencing communications and information systems worldwide”.[1]

1.1 Motivation

Communication is the Key of almost all sorts of human interests, businesses and concerns, that is why , since very long there has been a lot of work done in developing its technologies. The development and maturity in electronics and electromagnetic technology in the past century has led to the improvement in speed and coverage of communications. The high bandwidth demands for all sorts of communications and most importantly internet, grew by the end of twentieth century. Optical communications became the solution because it can use the large bandwidth availability and high speed of light.

Optical communication (OC) uses light to transmit information, which travels faster and provides larger bandwidth. Photons(i.e., light pulses) are very difficult to generate, measure and control, and hence has been used to transmit secret information. Optical communication can be achieved through fiber-optics as well as free-space technology. Over the internet today, a large number of photons per information bit are used to transport information. The optical communication technology needed to generate, measure and control the optical pulses with such large number of photons is quite mature, and has several commercial and military applications.

However, most long distance communication schemes used today employ relatively weak laser sources with small mean photon count at the receiver and non-photon number discriminating detectors with acceptable dark count rates and detector dead-times. Also for several diplomatic and military applications low number of photons in a single pulse must be measured in order to decode an information bit. These low number of photon applications are being developed and deployed. More specifically these low energy optical communication applications can be divided into[2]:

- Quantum communication.
- Stressed free-space optical communication.
- Low probability of intercept(LPI) optical communication.

Quantum communication take into account the transfer of quantum information between two locations, where the quantum nature of information is maintained. Today, it is vital to ensure the secrecy of information being transmitted, not only for military and diplomatic communication, but also in every day life. With the growth of computer networks for business transactions and confidentiality of information, there is an ever increasing need for encryption to insure the security of information being transmitted.
Cryptography is the science to encrypt and decrypt data by using some algorithms. Encryption is the process of encoding the original information (plaintext) in such a way that only the authorized party can read it, the unreadable data is called ciphertext . Hence, cryptography provides the advantage of making the information transfer over insecure networks confidential. The process of converting the ciphertext back to plaintext is called decryption.
Before transmission, an encryption algorithm and a secret key is used to encrypt the data. The authorized recipient uses the same key to decrypt the information. The security of this schemes is based on the distribution of the key to the legitimate recipients. Hence, the Key distribution is the vital problem.
Classical conventional key distribution techniques depends on complex mathematical approaches. and its security is based on unproven assumptions and depends on the technology available to an eavesdropper.
Quantum Key Distribution (QKD) is a technology to distribute, or rather generate, secure random keys between two communicating parties using optical fiber or free-space as a communication channel. The randomness and secrecy of the key is guaranteed by the laws of quantum physics. It exploits the fact, that measurement of the state of the quantum system cannot be done without perturbing it. QKD is combined with conventional key distribution techniques(dual key agreement) to produce as secure key as the strongest of the two original keys. Hence, contrary to its classical counterpart it provides unconditional security, independent to the technological progress.
Quantum Key Distribution has matured enough and is ready for commercialization. There has been a great interest in experimental QKD, with the longest distance achieved upto now of 148.7 km of Telecom fibers[3] and a transmission distance of the quantum bits of 144 km in free-space [4], [5]. QkD is also available commercially. Although a lot of research has been done on the security aspect of QKD there is still an enormous amount

of work that needs to be accomplished to create a truly secure and reliable system. With the commercial availability of quantum key distribution systems and hardware for secure data transmissions, it is extremely important that the details of quantum key distribution systems are explored and completely characterized.

Since the quantum bit error rate of a quantum channel used for QKD is high, as it uses the fairly lossy fibre optic or even more lossy free-space medium, error correction and detection protocols are very critical for its proper operation. Therefore, information reconciliation in QKD requires more attention. Error detection is also an important aspect in determining the presence or absence of an eavesdropper in the system. It is important to use good codes that has better error correction and detection capabilities. Now a days, LDPC and polar codes are believed to be capacity approaching and achieving respectively. There are two types of decoding techniques: 1) hard decoding and 2) soft decoding. In hard decoding the decoder takes fixed set of values(i.e, 0 and 1), while the input to a soft decoder may take a range of values in-between. So in soft decoding there is an extra amount of information that is associated to the reliability of the input information. The extra information gives a better estimates of the original data. So a soft decision decoding performs better than hard decoding in the presence of corrupted data [6].

1.2 Purpose

The focus of this research activity is to work on pragmatic information reconciliation applied to QKD schemes based on single photon or weak pulse laser (WPL) sources, so as to use feed-forward techniques which minimize the interaction between transmitter and receiver.

The core ideas of the thesis are employing Forward Error Correction (FEC) coding as opposed to two-way communication for information reconciliation in QKD schemes, exploiting all the available information for data processing at the receiver including information available from the quantum channel, since optimized use of this information can lead to significant performance improvement, and providing a security versus secret-key rate trade-off to the end-user within the context of QKD systems.

Moreover, as shown by accurate experimental studies, the communication channel used for quantum key exchange is not able to reach high levels of reliability (the Quantum Bit Error Rate -QBER may have a high value), both because of the inherent characteristics of the system, and of the presence of a possible attacker. In order to obtain acceptable residual error rates, it is necessary to use a parallel classical and public channel, characterized by high transmission rates and low error rates, on which to transmit only the redundancy bits of systematic channel codes with performance possibly close to the capacity limit.

Furthermore, since the more redundancy is added by the channel code, the more the corresponding information can be used to decipher the private message itself, it becomes necessary to design high-rate codes obtained by puncturing a low-rate mother code, possibly achieving a redundancy such that elements of the secret message cannot be uniquely determined from the redundancy itself, so for that purpose we designed high rate LDPC codes. Using high rate codes increases the security with trade-off to performance.

Other low photon number applications have also been considered, such as weak-laser pulses (WLP) communication. For that purpose, a low-complexity photon-counting receiver has been considered which may be employed in long-distance amplification-free classical optical communication schemes, and which is typically modeled as an equivalent Binary Symmetric Channel (BSC). We have developed a time varying Binary Input-Multiple Output (BIMO) channel model for this low-complexity photon-counting receiver, and analyzed its performance in presence of soft-metric based capacity approaching iteratively decoded error correcting codes, such as soft-metric based Low Density Parity Check (LDPC) codes and polar codes. We show that the classical channel capacity of the suggested BIMO model is higher than the capacity of the BSC model, and that the use of the BIMO model allows to feed the channel decoder with soft information, in the form of Log-Likelihood Ratios (LLRs), achieving a significant reduction in Bit Error Rate (BER) and Frame Error Rate (FER) with respect to classical hard-metric-based schemes which should be used in conjunction with a BSC channel model.

1.3 Outline

This thesis is organized as follows. The first chapter provides the motivation and purpose behind this thesis.

In the second chapter a brief background on the description of low number of photon communication applications have been given. The basis of classical cryptography are shortly reviewed, followed by a short introduction to quantum cryptography, the structure and functioning of a generic QKD protocol is discussed, using as a model one of the most famous protocol invented until now, the BB84 Protocol. In this Chapter particular attention is paid to the Information Reconciliation stage, highlighting the weakness of performing such an important task interactively between sender and receiver.

Third chapter introduces capacity achieving codes, such as Low Density Parity Check (LDPC) codes and polar codes, its structure and the advantages of working with capacity achieving codes in the context of practically any communication system, presenting a condensed overview of the belief propagation algorithm used by the LDPC decoders, channel polarization and successive cancellation decoding algorithms used by polar codes , which is the core of soft-information processing techniques.

In the fourth Chapter, a composite channel model for quantum key distribution is identified: formed by the parallel of the private (quantum) channel and a classic channel. A novel technique for forward error correction based information reconciliation is proposed, exploiting capacity achieving soft-metric based iteratively decoded block codes. The core ideas of this chapter are:

a employing FEC coding as opposed to two-way communication for information reconciliation, minimizing the interactions between transmitter and receiver;

b exploiting all the available information for data processing at the receiver including information available from the quantum channel;

c use of quantum communication schemes whereby photon counting receivers are used and the modeling of the BIMO Quantum-DMC channel.

Chapter 5 presents the potential improvements in key transmission rate in a Quantum Key Distribution (QKD) scheme whereby photon-counting detectors are used at the receiver. The classical capacity of such system is derived, showing the potential gains that photon counting detectors can provide in the context of a realistic cost-effective scheme from an implementation point of view.

Chapter 6 offers a preliminary investigation on the use of FEC LDPC codes for information reconciliation when the underlying channel is a Q-ary DMC, for QKD applications based on higher photon flux levels with spatial entanglement of twin beams in PDC, and shows that acceptable error reconciliation efficiency values obtained with reasonable complexity.

In the chapter 7 the performance results are presented. The performance obtained for weak energy optical communication simulating only the quantum channel and for the mixed-soft metric algorithms for QKD are studied via simulations as a function of the system parameters, in the presence of LDPC and Polar codes, in particular the achievable Bit Error Rates (BER) and Frame Error Rates (FER) are presented and confronted for different models of the quantum channel.

In the Last chapter a short conclusions of the thesis have been presented.

Chapter 2

Background

Optical communication is any type of communication in which light is used as a signal carrier, instead of electrical current. The merits of optical communication include high bandwidth, exceptionally low loss, great transmission range and no electromagnetic interference.

When we think about light we don't really think about what it is made of. For long, scientist tried to resolve if light was a wave or a particle. Eighteenth century's physicists strongly believed that light was made of basic units, but certain properties like refraction caused light to be reclassified as a wave. Thanks to Einstein and other renowned physicists who resolved the issue.

Photons are the rudimentary particle of light. Photons have a unique property in that they are both a particle and a wave. This is what allows photons unique properties like refraction and diffusion.

Because light is another form of energy it can be transferred or converted into other types. In the case of the photoelectric effect the energy of light photons is transferred through the photons bumping into the atoms of a giving material. This causes the atom that is hit to lose electrons and thus make electricity.

2.1 Weak energy optical communication

Over the internet today, a large number of photons per information bit are used to transport information. The optical communication technology needed to generate, measure and control the optical pulses with such large number of photons is quite mature, and has several commercial and military applications.

In binary optical communication, the logical information is encoded onto two different states of the radiation field. After the propagation, the receiver should perform a measurement, aimed at discriminating the two signals. Currently, most of the long-distance amplification-free optical classical communication schemes employ relatively weak laser sources with small mean photon count at the receiver. The same is true for quantum-enhanced secure cryptographic protocols. This low number of photon applications are being developed and deployed. More specifically these low energy optical communication applications can be divided into:

- Stressed free-space optical communication.
- Low probability of intercept (LPI) optical communication.
- Quantum communication.

The ideal technology for these limited number of photon application will be to use single photon detector, which can reliably detect the presence of optical pulses and convert its energy to electrical signals. There is an active research in the development of single photon detectors, and the development and deployment of optical communication systems using low number of photons rely on the enhancement of this technology[2].

2.1.1 Stressed free-space optical communication

As the name suggest the optical communication takes place under some extreme conditions. These stressed conditions affect the number of photons available at the receiver. The extreme conditions may be very large distance between the transmitter and the receiver or the stressed optical environment, such as, communication under water, in fog or smoke, where there are scattering loses and which effects the transmission of photons. In this scenario, a very large number of photons per pulse are used to encode the optical signal but, very low number of photons is available for detection at the receiver because of the nature of the link between the transmitter and the receiver.

For example, in satellite-earth optical communication the distance between transmitter and receiver is very large, this very large distance reduces the number of photons availability for reception. The sensitivity of the communication receiver becomes more important as the distance increases and the data rate that can be supported ultimately decreases. Photons counting detectors especially single photon detectors provides the improved sensitivity and stressed free-space optical communication application can take advantage of it.

2.1.2 Low probability of intercept (LPI) optical communication

In most communication scenarios, it is desirable to transmit the information secretly and securely i.e., military applications. In low probability of intercept (LPI) optical communication, the transmitter intentionally generates encoded optical pulses that contain a single or, at most, a few photons in order to minimize the probability that an eavesdropper will be able to detect the presence of the communication link.

2.1.3 Quantum communication

Quantum communication is the art of transferring quantum information between two locations. In Quantum communication the most important factor is to maintain the quantum nature of information being transmitted.

Photons are the only appropriate system for long distance quantum communication now a day. Other systems have also been studied deeply, such as atoms or ions, however currently and in the near future their adaptation for quantum communication applications is not feasible[7]. The loss of photons in the quantum channel is one of the drawback of photon-based applications, which limits the bridgeable distance for single photons to the order of 100 km with present silica fibers and detectors[8]. In principle, this problem can eventually be overcome by subdividing the larger distance to be bridged into smaller sections over which quantum entanglement[1] can be teleported[2]. The subsequent application of so called "entanglement swapping"[9] may result in transporting of entanglement over long distances. Quantum entanglement effects are used to create a binary communication system that works across infinite distances. Consequently, it is of strategic importance to develop the technology to send photons from one location to a distant one while preserving its truly quantum nature.

Quantum communication is a very broad field however; the most important sub-field is quantum cryptography which has a very well-known application called Quantum Key Distribution (QKD), which will be described later.

The subject of quantum communications brings together ideas from classical information theory, computer science, and quantum physics. Classical information theory and quantum mechanics fit together very well. In order to explain their relationship, an introduction to classical information theory is given, along with the principles of quantum mechanics. Before going in details of quantum cryptography and QKD a brief overview of classical cryptography along with some quantum mechanics will be presented in the next section.

[1] Quantum entanglement is a quantum mechanical phenomenon that transpires when groups of particles are produced or interacted in such a way that the quantum state of each particle must subsequently be described relative to the other, even though the individual objects may be spatially separated.

[2] Quantum teleportation is a process by which quantum information (e.g. the exact state of an atom or photon) can be transmitted (exactly, in principle) from one location to another, with the help of classical communication and previously shared quantum entanglement between the sending and receiving location. <http://en.wikipedia.org/wiki/Quantum_teleportation>

2.2 Classical Cryptography

2.2.1 Introduction

Secure communications and cryptography is as old as civilization itself. The Greek Spartans for instance would cipher their military messages and, for Chinese, just the act of writing the message constituted a secret message since almost no-one could read or write Chinese. When Julius Caesar sent messages to his generals, he didn't trust his messengers, so he replaced every alphabet with a shift of 3 (i.e., in his messages with a D, every B with an E, and so on) through the alphabet. The one who knew the shift by 3 rule could decipher his messages.

Today, secure communication is not only important for some military or diplomatic applications, but cryptography is also becoming vital in everyday life. With the growth of computer networks for business transactions and communication of confidential information there is an ever increasing need for encryption to ensure that the information exchanged is secure and cannot be acquired by third parties.

Cryptography is the study and operation of encoding and decoding secret messages to ensure secure communications. The main objective is to allow two participants, a sender and an intended recipient who share no information initially to be able to communicate in a form that is inscrutable to third parties. In addition, it is also important to authenticate the messages exchanged so that they may not be altered during the communication. Both of these aims can be fulfilled with provable security if the sender and the recipient are in possession of a shared, secret "key".

A key, which is a truly random sequence and deliver no useful information itself, is a part of information that controls the operation of a cryptographic algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

The sender and intended recipient should be able to agree and possess secret key material in such a way that third parties ("eavesdropper") cannot acquire, not even partially. Cryptography until the mid-1980 was founded on computational complexity of certain trap-door one-way functions that are easy to compute in one direction, but very difficult in the opposite direction. It is provably impossible to establish a secret key with conventional communications, so key distribution has relied on the conditional security of "difficult" mathematical problems in public key cryptography.

The search for unbreakable codes is one of the oldest themes of cryptographic research, but until the last century all proposed systems have ultimately been broken.

In 1917, Gilbert S.Vernam proposed an unbreakable cryptosystem, hence called the Vernam cipher or One-time Pad [10]. The One-time Pad is a special case of the substitution

cipher[3] , where each letter is advanced by a random number of positions in the alphabet. These random numbers then form the cryptographic key that must be shared between the sender and the recipient. Even though the Vernam cipher offers unconditional security against adversaries possessing unlimited computational power and technological abilities, it faces the problem of how to securely distribute the key. In 1949, Shannon proved that the one-time pad is information-theoretically secure, no matter how much computing power is available to the eavesdropper [11]. That is, if the key is truly random, never reused and kept secret, the one-time pad provides perfect secrecy (the only crypto-system with perfect secrecy).
Despite Shannon's proof of its security, the one-time pad has serious drawbacks in practice:

- it requires a perfectly random key;
- secure generation and exchange of the key must be at least as long as the message;

One time pads require extremely long keys and are therefore prohibitively expensive in most applications. These implementation difficulties have led to one-time pad systems being impractical and are so serious that they have prevented the one-time pad from being adopted as a widespread tool in information security.
There are two main branches of cryptography: secret (symmetric) key cryptography and public (asymmetric) key cryptography.

2.2.2 Secret-Key Cryptography

In secret key cryptography, a single common key is used for both encryption and decryption. As shown in Figure 2.1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver[12]. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. Secure key distribution is the main problem of secret-key cryptosystems. The security of communications is reduced to the security of secret-key distribution.

2.2.3 Public-Key Cryptography

A new surge of interest in cryptography was triggered by the upswing in electronic communications in the late 1970. It was essential to enable secure communication between

[3] The substitution cipher is a well-known classical cipher in which every plaintext character in all its occurrences in a message is replaced by a unique ciphertext character

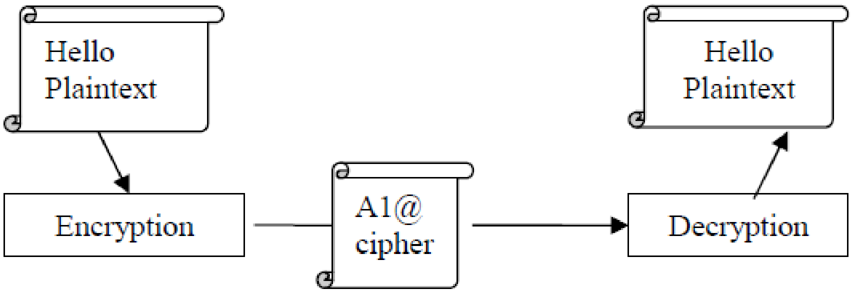


Figure 2.1: Secret Key Cryptography

users who have never met before and share no secret cryptographic key. But the question was how to distribute the key in a secure way. The solution was found by Whitfield Diffie and Martin E. Hellman, who invented public-key cryptography in 1976 [13]. The ease of use of public-key cryptography, in turn, stimulated the boom of electronic commerce during the 1990s.
Public-key cryptography requires a key pair: the public key and the private key. The recipient of a message generates two keys, reveals the public key through a trusted authority and keeps his private key in a secret place to ensure its private possession. In this algorithm anyone can encrypt a message using the public key, however, only the authentic recipient can decrypt the message using his/her private key. Figure 2.2 describes the Public Key Cryptography[12]

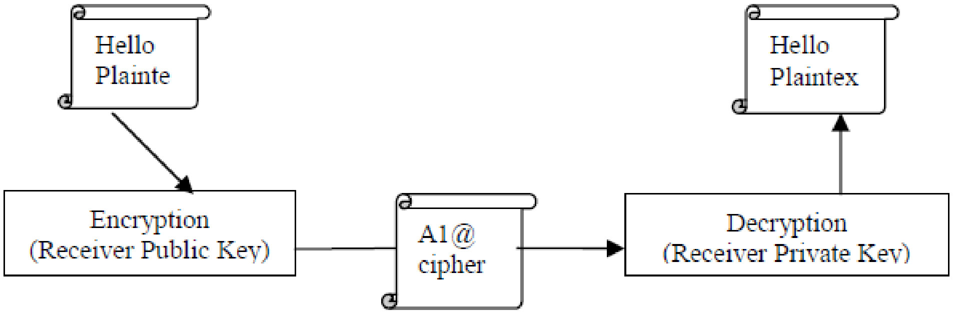


Figure 2.2: public Key Cryptography

Modern public key Cryptography until the mid-1980 was founded on computational complexity of certain trap-door one-way functions that are easy to compute in one direction, but very difficult in the opposite direction. It is, e.g., very easy to multiply two prime numbers, but to factor the product of two large primes is already a difficult task. Other public-key cryptosystems are based, e.g., on the difficulty of the discrete logarithm problem in Abelian groups on elliptic curves or other finite groups. To a large extent computational complexity is still the backbone of modern cryptography, hence, Public-key cryptography cannot provide unconditional security.

Today the most widely used public-key system is the RSA cryptosystem, invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman [14]. RSA exploits the difficulty of factoring large numbers, it uses a public key N which is the product of two large prime numbers (called "modulus"). Using this key, anyone can encrypt a message. However, in order to invert the algorithm it is necessary to know the prime factors of the modulus.

The possible construction of a quantum computer represents a menace to the security of public-key cryptography. The decryption using a quantum computer would take about the same time as the encryption, thereby making public-key cryptography worthless. Algorithms capable of doing so have already been developed[15] and first experiments with small-scale quantum computers successfully pave the way to more sophisticated devices [16]. For example, one way to crack RSA encryption is by factoring N, but with classical algorithms, factoring becomes increasingly time consuming as N grows large; more specifically, there is not any known classical algorithm that can factor N with a complexity $O((logN)k)$ for any k. By contrast, Short's algorithm can crack RSA in polynomial time.

2.3 Quantum Cryptography

2.3.1 Introduction

It has been said that the security of conventional cryptographic techniques relies on the assumption of limited advancement of mathematical algorithms and computational power in the foreseeable future, and also on limited financial resources available to a potential adversary. Computationally secure cryptosystems, no matter whether public- or secret-key, will always be at the mercy of mathematical and/or computational breakthroughs, which are difficult to predict and may even be hidden. In addition, steady progress in code-breaking allows the adversary to reach back in time and break older, earlier captured messages encrypted with weaker keys. As a consequence, periodic re-encryption or re-signing certain sensitive documents is necessary, along with the requirement to carefully sort information according to the used cryptosystem.

Another common problem of conventional cryptographic methods is the so-called side-channel cryptanalysis. Side channels are undesirable ways through which information related to the activity of the cryptographic device can leak out. The attacks based on side-channel information do not assault the mathematical structure of cryptosystems, but their particular implementations. It is possible to gain information for instance by measuring the amount of time needed to perform a certain operation, by measuring power consumption, heat or electromagnetic radiation.

Quantum mechanics offers a solution for the secure key distribution in cryptosystems. While the security of classical cryptographic methods can be undermined by advances in technology and mathematical algorithms, the quantum approach can provide unconditional security. In quantum mechanics the security is guaranteed by the Heisenberg uncertainty principle, which does not allow us to discriminate non-orthogonal states with certainty. Within the framework of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into any property of a classical object can be obtained without affecting the object itself. All classical signals can be monitored passively. In classical communications, one bit of information is encoded in billions of photons, electrons, atoms or other carriers. It is always possible to passively listen in, by splitting part of the signal and performing a measurement on it. Quantum cryptosystems eliminate this side channel by encoding each bit of information into an individual quantum object, such as a single photon. Single photons cannot be split, copied or amplified without introducing detectable disturbances.

It is important to notice that quantum mechanics does not prevent eavesdropping; it only allows one to detect the presence of a possible eavesdropper. Since only the cryptographic key is transmitted, no information leakage can take place when someone attempts to listen in. Eavesdropping causes discrepancies between measurements and when discrepancies are found, the key is simply discarded and the users may repeat the procedure to generate a new key.

2.3.2 Quantum Key Distribution (QKD)

In the early 1980s, Bennett and Brassard proposed a solution to the key distribution problem based on quantum physics[17]. They presented a protocol that allows users to establish an identical and purely random sequence of bits at two different locations, while revealing any eavesdropping with a very high probability. This idea, independently rediscovered by Ekert a few years later[18], was the beginning of quantum key distribution, which was to become the most promising element of quantum cryptography[4].

Quantum Key Distribution (QKD) is a technology to distribute, or rather generate, secure random keys between two communicating parties using optical fiber or free-space as a communication channel. It has been said that QKD has emerged in the last decades as one of the most important applications of quantum mechanics. Hence, in this paragraph the basic configuration and elements of such an important application will be introduced.

[4] For some authors, quantum cryptography and quantum key distribution are synonymous. For others, however, quantum cryptography also includes other applications of quantum mechanics related to cryptography, such as quantum secret sharing or every other possible tasks related to secrecy that are implemented with the help of quantum physics.

Alternative introductions to this subject are available in many sources, ranging from books [19],[20],[21],[22] to other review articles [23],[24],[25].

2.3.2.1 Generalities

The general setting of QKD is shown in Figure 2.3. The two authorized parties, wishing to share a secret message are traditionally called Alice and Bob. Alice, the sender, is the one who starts a key transmission, while Bob, the receiver, is the one who receives the quantum states and extracts the key sent by Alice. This is just a convention used in the field, but not a strict definition. The third important character is the eavesdropper, Eve, who is trying to intrude in the QKD and gain information about the key generated by Alice and Bob. Alice and Bob share a quantum secure channel, on which they send the quantum signals; and a classical public channel, on which they can send classical messages possibly back and forth. The classical channel needs to be authenticated; this means that Alice and Bob identify themselves, a third party can listen to the conversation but cannot participate in it. The quantum channel however, is open to any possible manipulation. The task of Alice and Bob is that of guaranteeing security against a possible eavesdropper that taps into the quantum channel and listens to the exchanges on the classical channel. In order to guarantee the security, either the authorized partners are able to create a secret key (a common list of secret bits known only to them) or they shall abort the protocol. Therefore, after the transmission of a sequence of symbols, Alice and Bob must estimate how much information about their set of bits has leaked out to Eve. In classical communications, such an estimate is obviously impossible, when Eve listens to the exchanges on the classical channel the communication goes on unmodified. This is where quantum physics comes into play: in a quantum channel, the leakage of information is directly related to the degradation of the communication quality.

Choice of photons (light)

In general, quantum information processing can be implemented with any quantum state of matter including energy state of ions, atoms, polarization states of light, electron spins, etc. Abstractly, this is also the case for QKD: one could imagine performing a QKD experiment with electrons, ions, and molecules; however, light is the only practical choice since it does not interact much with the environment leading to what is called de-coherence. Indeed, the task of key distribution makes sense only if Alice and Bob are separated by a macroscopic distance; if they are in the same room, there are much easier ways of generating a common secret key. Since, at any practical distance of interest, light propagates faster and with smaller de-coherence than matter, photons are the information carriers of choice. Various properties of photons can be employed to encode information for QKD, such as polarization, phase, quantum correlations of Einstein-Podolsky-Rosen

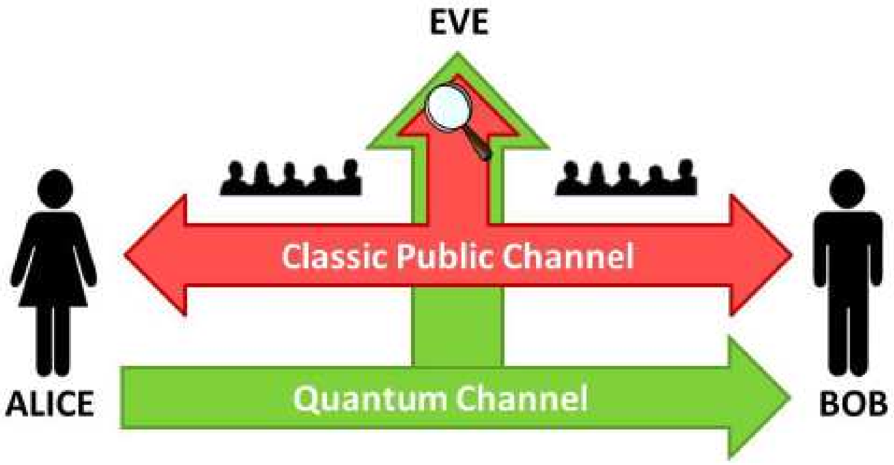


Figure 2.3: Quantum key distribution comprises a quantum channel and a public classical authenticated channel. As a universal convention in quantum cryptography, Alice sends quantum states to Bob through a quantum channel. Eve is suspected of eavesdropping on the line.

(EPR) pairs, and wavelength or quadrature components of squeezed states of light. It is also well known that light does not interact easily with matter.
The way losses affect QKD varies with the type of protocol and its implementation. Losses impose bounds on the secret key rate and on the achievable distance and may also leak information to the eavesdropper, according to the nature of the quantum signal (for coherent pulses this is certainly the case while for single photons it is not). Another difference is determined by the detection scheme. Implementations that use photon counters rely on post-selection. If a photon does not arrive, the detector does not click and the event is simply discarded. On the contrary, implementations that use homodyne detection always give a signal, therefore losses translate into additional noise. QKD is always implemented with light and there is no reason to believe that things will change in the future. As a consequence, the quantum channel is any medium that propagates light with acceptable losses, typically either an optical fiber or just free space, provided a line of sight path exists between Alice and Bob.

2.3.2.2 The BB84 Protocol

The first and probably most famous QKD protocol is the so-called BB84 protocol, which can help one to understand the basic QKD concepts. Suppose Alice holds a source of single photons. The spectral properties of the photons are sharply defined, so that the only degree of freedom left is the polarization[5]. Alice and Bob align their polarizers[6] and agree to use either the horizontal or vertical $(+)$ basis (rectilinear), or the complementary basis of linear polarizations, i.e., $+45/-45$ degrees $(\times)$ (diagonal). The transmitted bits are "prepared" at the transmitter (using the states of the selected basis) and "measured" at the receiver.

Specifically, the bits are encoded as follows:

$$|H\rangle \rightarrow 0_+ \ |{+45}\rangle \rightarrow 0_\times$$
$$|V\rangle \rightarrow 1_+ \ |{-45}\rangle \rightarrow 1_\times$$

where both bit values 0 and 1, are encoded in two possible ways in non-orthogonal states, since $|\pm 45\rangle = \sqrt{2}/2(|H\rangle \pm |V\rangle)$ It is important to notice that these four states satisfy the following relations:

$$\langle H \,|\, V\rangle = \langle -45 \,|\, +45\rangle = 0 \tag{2.1}$$

$$\langle H \,|\, H\rangle = \langle V \,|\, V\rangle = \langle +45 \,|\, +45\rangle = \langle -45 \,|\, -45\rangle = 1 \tag{2.2}$$

$$\langle H \,|\, \pm 45\rangle^2 = \langle V \,|\, \pm 45\rangle^2 = 1/2 \tag{2.3}$$

The theory of quantum-mechanics states that:

- Measurements performed in the basis identical to the basis of preparation of states will produce deterministic results (Equation 2.1 and Equation 2.2);
- Any measurements in the diagonal basis on photons prepared in the rectilinear basis will yield random outcomes with equal probabilities and vice-versa (Equation 2.3);

Once Alice and Bob have agreed on the coding, the BB84 protocol can be summarized by the following steps:

1. **Key Transmission**: Alice, the sender, generates a sequence of N random bits for transmission and chooses the encoding basis (rectilinear or diagonal) in a random and independent way for each bit. Physically this means that she transmits photons in the four polarization states shown in Figure 2.5 equally frequently. Bob, the receiver, randomly and independently of Alice, chooses his measurement basis, either rectilinear or diagonal. Statistically, Alice and Bob's bases match in 50% of the cases. At the end of this stage Alice and Bob will share what is called the raw key.

[5] Usually the way to encode the information being sent over the quantum channel is through the transmission of photons in some polarization states. The direction of the polarization encodes a classical bit.

[6] A polarizer is an optical filter that passes light of a specific polarization and blocks waves of other polarizations.

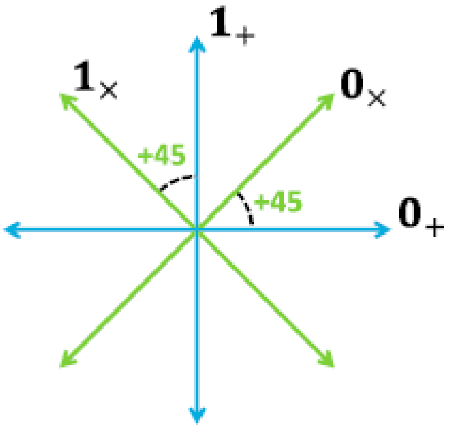


Figure 2.4: The four states of the BB84 Protocol.

2. **Basis Announcement**: Alice and Bob communicate over the classical channel and compare the basis used for each transmitted and detected photon. Whenever their bases coincide, Alice and Bob keep the bit whereupon it becomes part of the cryptographic key after reconciliation and privacy amplification. The bit is discarded when they chose different basis, when Bob's detector fails to register a photon due to the imperfect efficiency of detectors, or when the photon was lost somewhere along the way. Any potential eavesdropper, can only learn if Alice and Bob chose the same basis, but cannot determine whether Alice originally sent a "0" or "1". This step is called sifting. At the end, Alice and Bob have a string of bits of approximately $N/2$ bits, called the sifted key.

3. **Error Estimation**: Alice and Bob disclose part of their strings, a subset of the bits of size K, and estimate the error rate in the quantum channel. If Eve tries to eavesdrop on the quantum channel, she cannot passively monitor the transmissions. Instead she can intercept the photons sent by Alice, perform measurements on them and resend them. However, since Alice had chosen her encoding bases randomly Eve has to guess. Half the times Eve will guess the basis right and resend correctly polarized photons, while in the other 50% of the cases, she measures in the wrong basis, producing errors. When Alice and Bob reveal a random sample of the bits of their raw keys, they discover these errors. Alice and Bob use a predetermined "failure" error threshold (e_{max}) to decide whether or not an eavesdropper is present. In the literature, the most common failure error rate chosen is greater than or equal to 0.15 [50]. At 0.15 error rate, an eavesdropper could have intercepted over half of the bits transmitted. Both Alice and Bob compute the observed error-rate e and

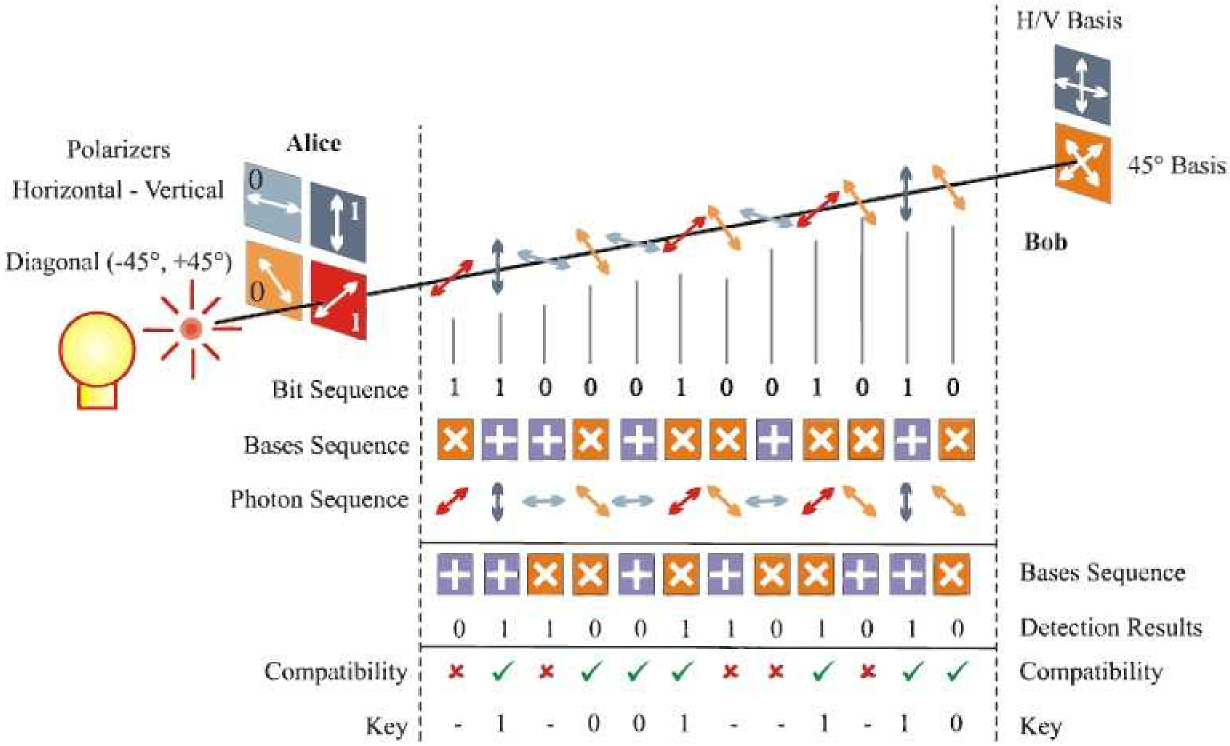

H/V Basis
45° Basis
Bob
Polarizers
Alice
Horizontal - Vertical
0
1
Diagonal (-45°, +45°)
0
1
Bit Sequence 1 1 0 0 0 1 0 0 1 0 1 0
Bases Sequence × + + × + × × + × × + ×
Photon Sequence
+ + × × + × + × × + + × Bases Sequence
0 1 1 0 0 1 1 0 1 0 1 0 Detection Results
Compatibility ✗ ✓ ✗ ✓ ✓ ✓ ✗ ✗ ✓ ✗ ✓ ✓ Compatibility
Key - 1 - 0 0 1 - - 1 - 1 0 Key

Figure 2.5: The BB84 Protocol.

accept the quantum transmission if $e < e_{max}$. In this case they remove the K bits announced from the raw key. Otherwise if $e > e_{max}$ Eve is suspected of tampering with the channel, and the cryptographic key is thrown away. Thus, no information leak occurs even in the case of eavesdropping. It should be mentioned that no physical apparatus is perfect and noiseless. Alice and Bob will always find discrepancies, even in the absence of Eve. As they cannot tell errors stemming from eavesdropping from the noise of the apparatus, they conservatively attribute all the errors in transmissions to Eve. The actual error rate stems from both noise in the channel and possibly, interference from an eavesdropper.

4. **Reconciliation and Privacy Amplification**: If there are errors however, Alice and Bob have to correct them and have to eliminate the information that could have been obtained by Eve. *Information reconciliation* is a form of error correction carried out on Alice and Bob's keys, in order to ensure both keys are identical. It is conducted over the public channel and as such it is vital to minimize the information sent about

> each key, since any such information is totally accessible by Eve. In the earlier versions of the complete protocol, Alice and Bob perform the error correction through an interactive reconciliation protocol called *Cascade*. This is a simple protocol that leaks an amount of information close to the theoretical bound of an almost ideal protocol, when the error probability is below 15%. *Cascade* was presented in [51] as an improvement of the procedure suggested in [52].*Cascade* operates in several rounds. During each round, Alice and Bob divide their raw keys into blocks, and disclose the parity of each block and compare them. If the parity bits do not match then a *binary search* is performed in order to find and correct the error. After all blocks have been compared, Alice and Bob both reorder their keys in the same random way, and a new round begins. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated recursively, which is the origin of the name cascade. At the end of multiple rounds, Alice and Bob have identical keys with high probability, however Eve has additional information about the key from the parity information exchanged.

Once the *Information reconciliation* has been performed, Alice and Bob share what is known as the reconciled key. *Privacy amplification* is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve has access to all the parity information). Privacy amplification uses Alice and Bob's key to produce a new, condensed key, in such a way that Eve's amount of information about the new key is negligible. This can be done using universal hashing functions, chosen randomly from a publicly known set. The size r of the secret key that Alice and Bob can distill depends on the kind, as well as the amount, of information available to Eve. It is important to notice that the final distilled key has a very short length when compared to the initial key size, as shown in Figure 2.6.

From the description of the BB84 protocol, it can be observed that, although the security of QKD relies on the laws of quantum mechanics, a considerable part of the protocol utilizes the classical communication channel and classical techniques exclusively. Once the raw key has been transmitted over the quantum channel, a secret key is distilled using classic post-processing techniques that require interaction. In the process, some information about the key is exchanged via the public channel in order to correct the errors and eliminate the possible information that Eve may have derived. Information reconciliation is a mechanism that allows for elimination of the discrepancies between two correlated variables. It is an essential component in every key agreement protocol where the key has to be transmitted through a noisy channel. Hence, it is important to explore other classical techniques in the context of QKD systems, to minimize the information exchanged over

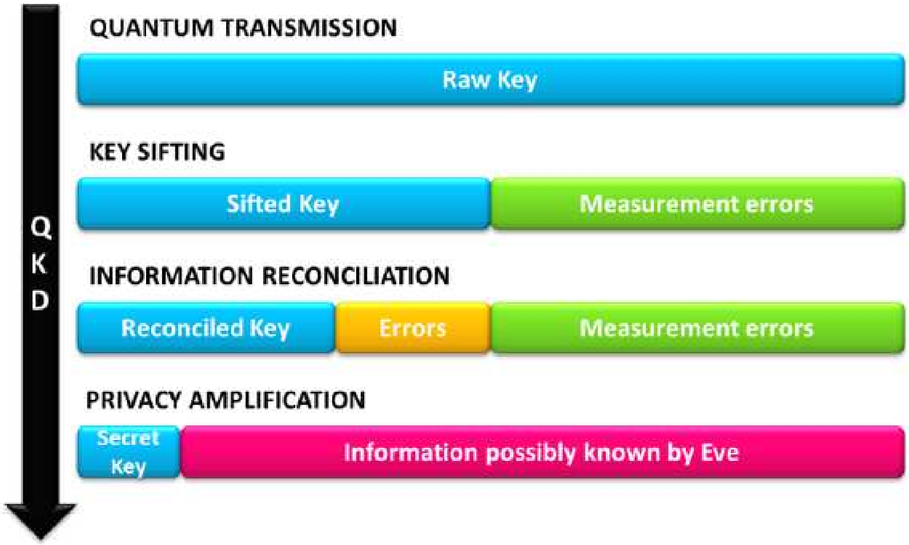


Figure 2.6: Distillation process and key length in BB84 Protocol.

the public channel so jeopardizing the provable security that quantum physics guarantees can be avoided.

Chapter 3

Capacity achieving Codes

A communication system is generally designed for the transmission of data reliably over a noisy channel. Channel encoding and decoding are very important in a communication system with a noisy channel. The channel encoder adds redundancy to the data for the reliable communication over a noisy channel. The channel decoder reproduces the data sent over the channel from the channel output. In this chapter we will describe some channel codes that are believed to be capacity approaching and capacity achieving for certain channels.

3.1 Preliminaries

3.1.1 Shannon's noisy channel coding theorem

In 1948, Claude E. Shannon published his seminal paper [26] on the mathematical theory of communication, which gave birth to information theory. In this paper, Shannon presented and formalized the concept of information, and substantiated the limits of maximum amount of reliable information transfer over unreliable channels. This theorem establishes that it is possible to communicate digital information almost error-free up to a computable maximum rate, over a communication channel with any given degree of noise.

The Shannon capacity of a communication channel with a certain level of noise is the theoretical maximum information transfer rate of the channel. Shannon proved that reliable transmission is possible for rates below the capacity, and is not possible for rates above capacity. The whim of capacity is defined purely in terms of information theory. As such it does not guarantee the existence of transmission schemes that achieve the capacity.

The theorem describes the maximum possible efficiency of error-correcting methods versus levels of noise, interference and data corruption.

The Shannon theorem states that given a noisy channel with channel capacity C and information transmitted at a rate R, then if $R < C$ there exist codes that allow the probability of error at the receiver to be made arbitrarily small.
On the contrary, if $R > C$, all codes will have a probability of error greater than a certain positive minimal level (that increases as the rate increases). So, information cannot be guaranteed to be transmitted reliably across a channel at rates beyond the channel capacity. The theorem does not address the rare situation in which rate and capacity are equal.
Shannon also introduced the concept of codes as (finite) sets of vectors over the input alphabet, which is to be transmitted. To achieve reliable communication, it is imperative to send input elements that are correlated. We assume that all the vectors have the same length, and call this length the block length of the code. If the number of vectors is $K = 2^k$ then every vector can be described with k-bits. If the length of the vectors is n, then in n times use of the channel k-bits have been transmitted. We say then that the code has a rate of $R_c = \frac{k}{n}$ bits per channel use.
Let suppose that a codeword is sent, and a vector over the output alphabet is received. If the channel is lossy and allows for error, then in general it cannot be said with absolute certainty which codeword was sent. However, the most likely codeword that was sent can be found, in the sense that the probability that this codeword was sent given the observed vector is maximized. To find such a codeword, we can simply list all the K codewords, and calculate the conditional probability for the individual codewords. We can then find the vector or vectors that yield the maximum probability and return one of them. This decoder is called the maximum likelihood decoder.
Shannon proved the existence of codes with rates arbitrarily close to capacity for which the probability of error of the maximum likelihood decoder goes to zero as the block length of the code goes to infinity.
Codes that approach the capacity of the channel are good from a communication point of view. However, along with achieving capacity, if these codes are to be used for communication, fast algorithms for encoding and decoding are needed. In the sections below, Low Density Parity Check codes (LDPC) and Polar codes that approach the capacity of the channel will be described.

3.1.2 Binary Discrete Memoryless Channel (B-DMC)

A channel is mathematically defined as a set of possible inputs to the channel X, a set of possible outputs to the channel Y, and a conditional probability distribution $P(y|x)$. The simplest class of channels is discrete memoryless channels (DMC).
In information theory symmetric B-DMCs are an important class of channels defined as: ***Definition***. A symmetric binary discrete memoryless channel (B-DMC) is a B-DMC $W\ :\ \{0,1\}\ \rightarrow\ Y$ with the additional property that there exists a permutation over the outputs of the channel $\pi\ :\ Y\ \rightarrow\ Y$ such that $\pi = \pi - 1$ and $P\left(y|0\right) = P\left(\pi\left(y\right)|1\right)$.
An important example of B-DMCs is binary symmetric channels (BSC).

3.1.2.1 Binary Symmetric Channel (BSC)

A BSC is a kind of communication channel with binary inputs and outputs respectively. A probability p is associated with BSC is called the crossover probability. This means, with a probability p, a bit sent through the BSC is flipped. And conversely with a probability $1 - p$ a bit sent through the BSC passes unchanged. The pictorial description is given in Figure 3.1

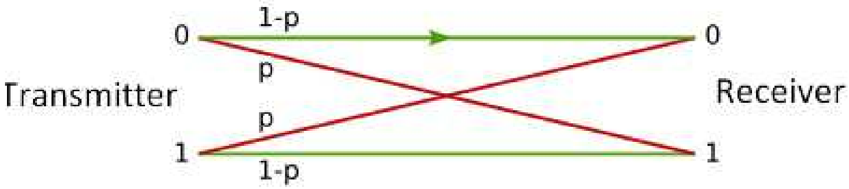


Figure 3.1: Binary Symmetric Channel with crossover probability p

3.1.2.2 Mutual Information and Bhattacharyya parameter

The two important parameters of symmetric B-DMC's are defined as:

- *Mutula Information:* The mutual information of a B-DMC with input alphabet $X = \{0,1\}$ is given as:

$$I\left(W\right) \triangleq \frac{1}{2} \sum_{y \in Y} \sum_{x \in X} W\left(y|x\right) log \frac{W\left(y|x\right)}{\frac{1}{2}W\left(y|0\right) + \frac{1}{2}W\left(y|1\right)} \tag{3.1}$$

  $I\left(W\right)$ is the measure of the rate of a channel. For a symmetric B-DMC reliable communication is possible at any rates up to I(W).

- *Bhattacharyya Parameter:* The Bhattacharyya parameter is defined as:

$$Z\left(W\right) \triangleq \sum_{y \in Y} \sqrt{W\left(y|0\right) W\left(y|1\right)} \tag{3.2}$$

  $Z(W)$ is an upper bound on the probability of maximum-likelihood (ML) decision error for uncoded transmission over W, Hence it is the measure of reliability if the channel.

3.2 Low Density Parity Check (LDPC) Codes

This section describes the characteristics of a class of capacity achieving block codes, the Low-Density Parity-Check (LDPC) codes. LDPC codes are a class of linear block codes whose name comes from the characteristic of their parity-check matrix which contains few ones in comparison to the number of zeros. Their main advantage is that they provide a performance which is very close to the capacity for a lot of different channels and there are linear time complexity decoding algorithms available for them. Furthermore, they are suited for implementations that make heavy use of parallelism. LDPC codes can be represented through a matrix as well as a graph.

3.2.1 Matrix representation

An (n,k) LDPC code is represented by a parity check matrix which consists of $m = n - k$ rows and n columns, where n is the codeword length, k the number of information bits and m the number of redundant bits. For example, the matrix defined in Equation 3.3 is a parity check matrix H with dimension $n \times k$ for a $(8,4)$ LDPC code.

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{3.3}$$

We can define two numbers describing the matrix H, w_r, that indicates the number of 1's in each row and w_c that indicates the number of 1's in each column. For a matrix to be called low-density the two conditions $w_c \ll n$ and $w_r \ll m$ must be satisfied. In order to achieve this, the parity check matrix should usually be very large (so the example matrix presented above is not really low-density).

3.2.2 Graphical representation

In a Tanner Graph representation of a (n,k) LDPC code, the n nodes related to the rows of the parity check matrix are denoted as Variable Nodes or Bit Nodes (V-nodes). On the other hand there are m nodes, called Check Nodes (C-nodes), that are related to the rows of the H matrix, i.e., the m parity check equations of the code. An edge on the Tanner Graph connects a V-node to a C-node only if the corresponding element is a "1" in the parity check matrix H. From the parity check matrix H of Equation 3.3, we have $n = 8$ V-nodes connected to $m = 4$ C-nodes. Figure 3.2 shows the Tanner graph representation of the parity check matrix of Equation 3.3. Notice that the bit nodes values connected to same check node must sum to zero. Similarly, a Tanner graph can also be constructed from the columns of H.

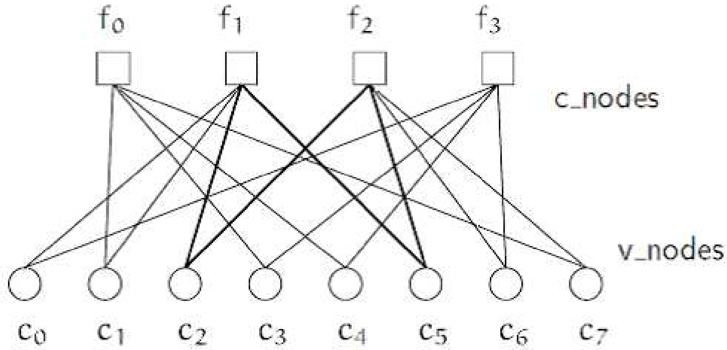


Figure 3.2: Tanner Graph representation of the LDPC code corresponding to the parity check

In a Tanner graph like the one in Figure 3.2 it is possible to identify close cycles. The marked path $c_2 \rightarrow f_1 \rightarrow c_5 \rightarrow f_2 \rightarrow c_2$ is an example of a short cycle. Those should usually be avoided since they are bad for decoding performance.

3.2.3 Encoding

In an (n,k) LDPC code, if the rank of the H matrix is r, then $n - r$ information bits can be transmitted per codeword. Accordingly the code rate is given by,

$$R_c = k/n = (n-m)/n \leq (n-r)/n \tag{3.4}$$

where the inequality holds when all m rows are linearly independent.

LDPC codes are encoded using the generator matrix G spanning a space which is the orthogonal complement of the space spanned by the parity-check matrix H, so that

$$GH^T = 0. \tag{3.5}$$

G and H can be derived from each other using Gaussian elimination. If the code is systematic, the matrix H can be expressed as,

$$H = \left[I_{n-k}|P\right] \tag{3.6}$$

where I is a $(n-k) \times (n-k)$ identity matrix and P is the $(n-k) \times k$ parity matrix. The generator-matrix G can be written in the systematic form as

$$H = \left[P^T|I_k\right] \tag{3.7}$$

where represents the $k \times (n-k)$ transposed parity matrix. If we consider a sequence of information bits x that contains k bits, the encoding process is achieved by simply multiplying this sequence by the generator matrix to get the codeword,

$$C = xG \tag{3.8}$$

3.2.4 Decoding

The iterative decoding algorithm used for LDPC codes is well known as the Sum Product Algorithm (SPA), Belief Propagation Algorithm (BPA) or Message Passing Algorithm (MPA). The term message passing refers to the fact that during each round messages in the form of probabilities (or beliefs) are passed from V-nodes to C-nodes and vice versa. An important aspect of iterative decoding is that message to be sent from the i^{th} V-node V_i to the j^{th} C-node C_j must not take into account the message sent in the previous iteration from C_j to V_i. The same rule holds for messages to be sent from C_j to V_i.

The Belief Propagation Algorithms (BPA) is an important class of message passing algorithm where the messages passed along the edges of a Tanner Graph are probabilities (or beliefs) [27]. More precisely, the message passed from the V-node V_i to the C-node C_j is the probability that V_i has a certain value, given its own noisy observed value, and all the values received in the previous iteration from its neighboring C-nodes (two nodes are said to be neighbors if they are connected to the same edge of Tanner graph) excluding C_j. Similarly, the message passed from C_j to V_i is the probability that V_i has a certain value given all the messages passed to C_j in the previous iteration from neighboring V-nodes other than V_i.

The aim of the belief propagation algorithm is to compute the A-Posteriori Probability (APP) that a given bit in the transmitted code-word $C = [c_0 c_1 ... c_{n-1}]$ equals 1, given the received sufficient statistic samples $Y = [y_0 y_1 ... y_{n-1}]$, i.e., the APP probability

$$p_i = P_r\left(c_i = 1|Y\right) \tag{3.9}$$

or the APP ratio (also called Likelihood Ratio (LR)),

$$l(c_i) = \frac{P_r(c_i = 0|Y))}{P_r(c_i = 1|Y)} \tag{3.10}$$

The LR can be iteratively computed exploiting the code's Tanner graph. In one half iteration, each V-node processes its input messages (probabilities or LLRs) and passes its resulting output messages to the neighboring C-nodes. In the other half iteration the C-node passes its messages to the V-nodes. After a pre-defined number of iterations, or after some stopping criteria have been met, the decoder computes the APP (A-Posteriori Probabilities), or LLR (Log Likelihood Ratios) from which decisions on the bits can be taken.

Let f_{ij}^k and g_{ji}^k be the messages from V_i to C_j and C_j to V_i in k^{th} iteration, respectively. The belief propagation algorithm in probability domain can be described as,

1. Initialization:

$$f_{ij}^0\left(0\right) = 1 - p_i \tag{3.11}$$

$$f_{ij}^0\left(1\right) = p_i \tag{3.12}$$

2. C-node update:

$$g_{ji}^k(0) = 1/2 + 1/2\mathit{\Pi}_{i\in f_{j/i}}\left(1 - 2f_{ij}^{(k-1)}(1)\right) \tag{3.13}$$

where $f_(j/i)$ is the set of all V-nodes connected to C_j excluding V_i, and,

$$g_{ji}^k(1) = 1 - g_{ji}^k(0) \tag{3.14}$$

3. V-node update:

$$f_{ij}^k(0) = 1 - A_{ij}f_{ij}^0\mathit{\Pi}_{j\in g_{i/j}}g_{ji}^k(0) \tag{3.15}$$

where $g_(i/j)$ is the set of all C-nodes connected to V_i excluding C_j, and,

$$f_{ij}^k(1) = A_{ij}f_{ij}^0(1)\mathit{\Pi}_{j\in g_{i/j}}g_{ji}^k(1) \tag{3.16}$$

where A_ij are constants, which satisfy

$$f_{ij}^k(0) + f_{ij}^k(1) = 1 \tag{3.17}$$

4. Soft Decision:

$$F_i^k(0) = A_i f_{ij}^0(0)\mathit{\Pi}_{j\in g_i}g_{ji}^k(0) \tag{3.18}$$

$$F_i^k(1) = A_i f_{ij}^0(1)\mathit{\Pi}_{j\in g_i}g_{ji}^k(1) \tag{3.19}$$

where g_i is the set of all C-nodes connected to V_i, and A_i is chosen to satisfy,

$$F_i^k(0) + F_i^k(1) = 1 \tag{3.20}$$

5. Hard Decision:

$$\tilde{c}\,(i) = \begin{cases} 1, & \text{if } F_i^k \gg 0 \\ 0, & \text{otherwise} \end{cases}$$

If $\tilde{c}H^T = 0$, or maximum number of iterations is reached, stop, else go back to step 2), where $\tilde{c}$ is the decoded codeword.

As it can be seen above, the decoding process involves the multiplication of probabilities, which have high computational complexity. With the increase in number of iterations a log domain manipulation is required to decrease the complexity, by converting multiplications to additions.
In log domain the algorithm can be described as follows, first we define:

$$L(c_i) = log\frac{P_r(c_i = 0|Y)}{P_r(c_i = 1|Y)} \tag{3.21}$$

$$L(f_{ij}) = log\frac{f_{ij}(0)}{f_{ij}(1)} \tag{3.22}$$

$$L(g_{ij}) = log\frac{g_{ij}(0)}{g_ij(1)} \tag{3.23}$$

$$L(F_i) = log\frac{F_i(0)}{F_i(1)} \tag{3.24}$$

1. Initialization:

$$L^0(f_{ij}) = L^0(c_i) \tag{3.25}$$

2. C-node update: From equation 3.13 and 3.14 we get

$$1 - 2g_{ji}(1) = \varPi_{i \in f_{j/i}} \left(1 - 2f_{ij}(1)\right) \tag{3.26}$$

Now since $tanh[\frac{1}{2}log(\frac{a}{b})] = 1 - 2b$ and using equation 3.22 and 3.23, 3.26 can be written as,

$$tanh\left[\frac{1}{2}L^k(g_{ij})\right] = \varPi_{i\,\in\, f_{j/i}} tanh\left[\frac{1}{2}L^{(k-1)}(f_{ij})\right] \tag{3.27}$$

Equation (3.27) still involves multiplication and a complex tanh(.) function that needs to be simplified. Let us represent $L(f_i)$ in its sign and magnitude form; in particular, let $\varTheta_{ij}$ represent the sign of $L(f_{ij})$, and δ_{ij} represent the magnitude of $L(f_{ij})$. Using these, equation 3.27 becomes,

$$tanh\left[\frac{1}{2}L^k(g_{ij})\right] = \mathit{\Pi}_{i\,\in\,f_{j/i}}\mathit{\Theta}_{ij}^{(k-1)}.\mathit{\Pi}_{i\in f_{j/i}}tanh\left[\frac{1}{2}\delta_{ij}^{(k-1)}\right] \tag{3.28}$$

Then,

$$L^k(g_{ij}) = \mathit{\Pi}_{i\in f_{j/i}}\mathit{\Theta}_{ij}^{(k-1)}.2tanh^{-1}.log^{-1}.log\left[\mathit{\Pi}_{i\in f_{j/i}}tanh\left[\frac{1}{2}\delta_{ij}^{(k-1)}\right]\right] \tag{3.29}$$

$$= \mathit{\Pi}_{i\in f_{j/i}}\mathit{\Theta}_{ij}^{(k-1)}.2tanh^{-1}.log^{-1}.\sum_{i\in f_{j/i}} log\left[tanh\left[\frac{1}{2}\delta_{ij}^{(k-1)}\right]\right] \tag{3.30}$$

Let γ be a map from the real numbers $[-\infty,\infty]$ to $F2 \times [0,\infty]$ defined by $\gamma(x) := (sgn(x) - log(tanh((|x|)/2)))$, whereby,

$$sgn\,(x) = \begin{cases} 1, & \text{if}\, x \geq 1 \\ 0, & \text{otherwise} \end{cases}$$

Equation (3.30) can be written as,

$$L^k(g_{ij}) = \gamma^{-1}\left(\sum_{i\in f_{j/i}}\gamma\left(\delta_{ij}^{(k-1)}\right)\right) \tag{3.31}$$

3. V-node update: Dividing equation 3.16 by 3.15 and taking log, we have,

$$L^k(f_{ij}) = L^0(c_i) + \sum_{j\in g_{i/j}} L^k(g_{ji}) \tag{3.32}$$

4. Soft Decision:

$$L(F_{ij}) = L^0(c_i) + \sum_{j\in g_i} L(g_{ji}) \tag{3.33}$$

5. Hard decision:

$$\tilde{c}\,(i) = \begin{cases} 1, & \text{if}\, L_i^k < 0 \\ 0, & \text{otherwise} \end{cases}$$

If $\tilde{c}H^T = 0$, or maximum number of iterations is reached, stop, else go back to step 2), where $\tilde{c}$ is the decoded codeword.

3.2.5 Density Evaluation (DE)

As stated previously, the asymptotic performance of LDPC codes, when the codeword length tends to infinity, has been studied using an analytical technique called density evolution (DE) or Gaussian approximation [27],[28],[29].
The density evolution computes the probability density function (PDF) of the messages defined by the message-passing algorithm on Tanner graphs at any iteration. From [31], "Asymptotically, the actual density of the messages passed is very close to the expected density. Tracking the expected density during the iterations thus gives a very good picture of the actual behavior of the algorithm[28]". Two assumptions are made for the calculation of density evolution [29],

- The independence condition assures that the messages passed on the Tanner graph are statistically independent;
- For infinite code length, the factor graph can be viewed as a cycle free graph.

In general, an LDPC code ensemble is specified by a degree profile (λ,ρ). Its corresponding generating functions are $\lambda(x) = \sum_{i=2}^{d_{vmax}} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{i=2}^{d_{cmax}} \rho_i x^{i-1}$ where $\lambda_i(\rho_i)$ is the fraction of edges with variable (check) node of degree i and d_{vmax} (d_{cmax}) is the maximal variable (check) node degree (number of edges connected to it), respectively.
Let ς_{c_k} denote the common density function of the messages g_{ji}^{k} sent from C-nodes to V-nodes at round k and let ς denote the density of the messages f_{ij}^{0}, i.e., the likelihood of the messages sent at iteration 0 of the algorithm. Then the update rule for the densities in equation 3.31 implies that the common density $\varsigma_{v_{k+1}}$ of the messages sent from V-nodes to C-nodes at round $k+1$ conditioned on the event that the degree of the node is d, equals $\varsigma * \varsigma_{c_k}^{(d-1)}$, where $(\varsigma * \varsigma_{c_k})(\tau) = \int (\varsigma(\sigma)\varsigma_{c_k}(\tau - \sigma))d_\tau$ is the convolution over some group G_0 of ς andς_{c_k} [29]. Using $\gamma(x)$ defined above, let $\Gamma(\gamma(x))$ be the density of $\gamma(x)$. Using equation 3.31 and the independence assumption, it can be shown that

$$\varsigma_{c_k} = \Gamma^{-1}(\rho(\Gamma(\varsigma_{v_k}))) \tag{3.34}$$

where Γ is the Laplace transform of the expected densities derived in[28],[29]. From this, the following recursion formula can be obtained for density evolution (DE):

$$\varsigma_{v_{k+1}} = \varsigma * \lambda(\Gamma^{-1}(\rho(\Gamma(\varsigma_{v_k})))) \tag{3.35}$$

The convolution can be efficiently computed using Fourier transform $\mathcal{F}$, so the DE can be expressed as

$$\varsigma_{v_{k+1}} = \Gamma\mathcal{F}^{-1}(\mathcal{F}(\varsigma)\lambda(\mathcal{F}(\varsigma_{c_k}))) \tag{3.36}$$

From density evolution together with Fourier transform techniques, asymptotic thresholds below which belief propagation decodes the code successfully, and above which belief propagation does not decode successfully, can be derived [27],[28],[29].
The asymptotic performance of LDPC is characterized by finding the maximum channel parameter (threshold σ^*) such that if $\sigma < \sigma^*$ then $\lim_{k\to\infty} P_e^k = 0$,and P_e^k is the expected fraction of incorrect messages at the k^{th} iteration.

3.3 Polar Codes

Polar codes were introduced by Arkan in [30]. Polar codes are linear block codes which provably achieve the capacity of symmetric B-DMC's.
Polar codes uses the concept of channel polarization described below. The idea of polar codes is to create from N independent copies of a B-DMC W through a linear transformation, another N different channels $\left\{W_N^{(i)} : 1 \leq i \leq N\right\}$, such that as N grows large these synthesized channels are polarized. i.e., their mutual information are close to either 0 or 1. It is shown that the fraction of indices i for which $I\left(W_N^{(i)}\right)$ is close to 1 is $I\left(W\right)$, and the fraction of indices i for which $I\left(W_N^{(i)}\right)$ is close to 0 is $1 - I\left(W\right)$ asymptotically. Hence some channel becomes good and some channels become worst. The encoding/decoding complexity of the codes is $O\left(NlogN\right)$.

3.3.1 Channel Polarization

Channel polarization is an operation which produces N channels $\left\{W_N^{(i)} : 1 \leq i \leq N\right\}$, from N independent copies of a B-DMC W such that the new channels are synthesized in the sense that their mutual information is either close to 0 (Bad, noisy channels) or close to 1 (good, noiseless channels). Channel polarization consists of two phases [30],[31],

1. ***Channel Combining:*** In channel combining phase, a recursive mechanism is applied to combine copies of a B-DMC in n steps to form a vector channel W_N, where $N = 2^n$. The channel combining can be described through the following transformation:

$$W_2\left(y_1,y_2|u_1,u_2\right) = W\left(y_1|u_1 \oplus u_2\right) W(y_2|u_2) \tag{3.37}$$

it can be seen from Equation 3.37 that a new vector channel of size 2 is created from combining two separate channels i.e., $W_2 : \{0,1\}^2 \rightarrow Y^2$. Since the linear transformation between (U_1,U_2) is a one-to-one mapping:

$$I\left(U_1,U_2;Y_1,Y_2\right) = I\left(X_1,X_2;Y_1,Y_2\right) = 2I\left(W\right) \tag{3.38}$$

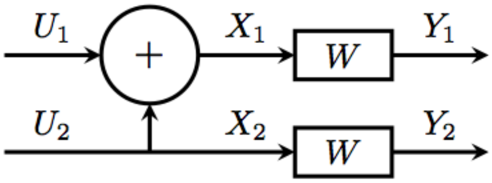


Figure 3.3: Channel Combining

For a general $N = 2^n$ channel combining can be done as:

$$W_N\left(Y^N|U^N\right) = W_{N/2}\left(Y^{N/2}|U_o^N \oplus U_e^N\right) W_{N/2}\left(Y_{N/2+1}^N|U_e^N\right) \tag{3.39}$$

where $W^N = \{W_1,W_2,...,W_N\}$, $U_o^N = \{u_1,u_3,...,u_N\}$, $U_e^N = \{u_2,u_4,...,u_N\}$.

2. ***Channel Splitting:*** In channel splitting, W_N is split back into N channels $W_N^{(i)} : \{0,1\} \rightarrow Y^N \times \{0,1\}^{i-1}, 1 \leq i \leq N$.
Equation 3.38 can be written using chain rule as:

$$I\left(U_1,U_2;Y_1,Y_2\right) = I\left(U_1;Y_1,Y_2\right) + I\left(U_2;Y_1,Y_2,U_1\right) \tag{3.40}$$

$I\left(U_1;Y_1,Y_2\right)$ is the mutual information of the channel between U_1 and Y_1,Y_2, with U_2 considered as noise. $I\left(U_2;Y_1,Y_2,U_1\right)$ is the mutual information of the channel between U_2 and Y_1,Y_2 given that U_1 is known [31]. Let the two splitted channel be denoted as W^- and W^+, their transition probabilities can be expressed as:

$$W^-\left(y_1,y_2|u_1\right) = \frac{1}{2}\sum_{u_2\in\{0,1\}} W\left(y_1|u_1 \oplus u_2\right) W\left(y_2|u_2\right) \tag{3.41}$$

$$W^+\left(y_1,y_2,u_1|u_2\right) = \frac{1}{2} W\left(y_1|u_1 \oplus u_2\right) W\left(y_2|u_2\right) \tag{3.42}$$

The two splitted channels have the following properties[30]:

(a)
$$I\left(W^+\right) + I\left(W^-\right) = 2I\left(W\right) \tag{3.43}$$

(b)
$$Z\left(W^-\right) \leq 2Z\left(W\right) - Z\left(W\right)^2 \tag{3.44}$$

(c)

$$Z\left(W^{+}\right) = Z\left(W\right)^{2} \tag{3.45}$$

$$I\left(W^{+}\right) + I\left(W^{-}\right) = 2I\left(W\right) \tag{3.46}$$

This way, the channel is splitted into the channel set $\{W^{+},W^{-}\}$. As U_2 is considered as noise, the W^{+} is set to be the error-free channel, while W^{-} is noisy.

For $N = 2^n$ the splitting can be done through:

$$W_N^i\left(y_1^N,u_1^{i-1}|u_i\right) \triangleq \sum_{u_{i+1}^N \to X^{N-1}} \frac{1}{2^{N-1}} W_N\left(y_1^N|u_1^N\right) \tag{3.47}$$

In this way the channel combined in the first phase ($W_N : U^N \to Y^N$), is splitted into the polarized channel set $W_N^i : 1 \leq i \leq N$ with the transition probability of Equation 3.47.
After splitting the channel W_N^i in the set has input U^i and output (y_1^N,u_1^{i-1}) with the form: $W_N^i : U \to Y^N \times X^{i-1}$

3.3.2 Encoding

Polar codes are linear codes, i.e., any linear combination of codewords is another codeword of the code. The polar transform is to apply the transform $G_2^{\otimes n}$, the n^{th} Kronecker power to the block of $N = 2^n$ bits U.

$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{3.48}$$

For code length $N = 2^n$, $n = 1,2,$, and information length K, the code rate is $R_c = K/N$.
A binary source block u_1^N which consists of K information bits and NK frozen bits[1] is mapped to a code block $x_1^N via$ via $x_1^N = u_1^N G_N$. The matrix $G_N = R_N G_2^{\otimes n}$, where G_2 is defined in Equation 3.48, and R_N is the bit-reversal permutation matrix. The binary channel x_N are then sent into channels which are obtained by N independent uses of W [30],[32].

[1] For the transmission of a K bits binary message block , the K most reliable polarized channels $W_N^{(i)}$ with indices $i \in I$ are picked out for carrying information bits; and transmit a fixed bit sequence called frozen bits over the others. The index set $I \in \{1,2,,N\}$ is called information set and $|I| = K$. And the complement set of I is called frozen set and is denoted by F.

3.3.3 Decoding

Arikan mentioned in [30] that, Polar codes can be decoded using successive cancellation (SC) decoding algorithm. Let $\tilde{u}_1^N$ denote the estimate of the information block u_1^N. After receiving the output y_1^n the bits $\tilde{u}_i$ are determined successively with $i = 1,2,...N$ as:

$$\tilde{u}_i = \begin{cases} L_i\left(y_1^N,\tilde{u}_1^{i-1}\right) & \text{if } i \in I \\ u_i & \text{if } i \in F \end{cases}$$

where

$$L_i\left(y_1^N,\tilde{u}_1^{i-1}\right) = \begin{cases} 0 & \text{if} \frac{W_N^{(i)}\left(y_1^N,\tilde{u}_1^{i-1}|0\right)}{W_N^{(i)}\left(y_1^N,\tilde{u}_1^{i-1}|0\right)} \geq 1 \\ 1 & \text{otherwise} \end{cases}$$

The block error rate (BLER) of this SC decoding is upper bounded by

$$P_S C\left(N,I\right) \leq \sum_{i \in I} P_e\left(W_N^{(i)}\right) \tag{3.49}$$

For more details and proofs about polar codes see [30].

Chapter 4

Soft-Metric based decision in QKD and Poisson photons channels

4.1 Overview and System Model

In chapter 2 an overview of weak energy optical communication and QKD systems has been given. Since the number of photons in all the optical communication scenarios discussed so far is quite low, either at the transmitter or at the receiver, because of the extreme conditions or the security constraints, the receiver needs to be very sensitive, and the information it collects needs to be carefully processed. Single photon detectors can provide the required sensitivity [2].

In binary optical communication, the logical information is encoded onto two different states of the radiation field. After the propagation, the receiver should perform a measurement, aimed at discriminating the two states. Currently, most of the long-distance amplification-free optical classical communication schemes employ relatively weak laser sources with small mean photon count at the receiver. The same is true for quantum-enhanced secure cryptographic protocols.

In fact, laser radiation, which is described by coherent states, preserves its fundamental properties also in presence of losses. On the other hand, operating in the regime of low number of detected photons gives rise to the problem of discriminating the signals by quantum-limited measurements [33, 34]. Indeed, the binary discrimination problem for coherent states has been thoroughly investigated, both for its fundamental interest and for practical purposes [35], [36], [37], [38], [39], [40].

It should be mentioned however that in order to exploit the phase properties of coherent states, one should implement phase sensitive receivers [41, 42] with nearly optimal performances also in presence of dissipation and noise [38], [43]. This is a challenging task, since it is generally difficult, and sometimes impossible, to have a suitable phase reference in order to implement this kind of detection scheme.

The simplest choice for a detection scheme involving radiation is given by direct measurements through energy detectors, namely detectors which only detect the presence or the absence of radiation (on/off detectors) with acceptable dark count rates and detector dead-times. A natural step forward in the evolution of such schemes would be to employ photon counting detectors at the receiver.
The first QKD protocols were based on interactive error correction schemes [50], [51], [52] (like the Cascade algorithm), specially because BB84-like schemes are based on a highly interactive process that requires many communication rounds. BB84-like protocols for error correction and information reconciliation in QKD systems are not very efficient in terms of throughput (distilled key per second) since a lot of information is discarded to ensure that the information Eve can possibly know is canceled from the final secret key.
More recently Forward Error Correction (FEC) schemes have been suggested [53], [53], [54], [55],[56], which can avoid re-transmission, increasing the system efficiency, and must be decoded by decoders exploiting the information available at the output of both the quantum and the public channel. In practice, the FEC block code must operate on an equivalent composite parallel channel formed by the quantum and the public channels, as shown in Figure 4.1, where the k information bits (the sifted key) are transmitted over the quantum private channel, while the $m = n - k$ redundancy bits are transmitted over the classical public channel. The eavesdropping on the secure channel in Figure 4.1 is shown as a dotted line, because if the system is properly designed and the channel QBER is periodically monitored, the presence of Eve can be detected, as previously described, and the information leaked to Eve can be made arbitrarily small, as if the eavesdropper did not exist. Given this hypothesis, we will from now on focus on the overall channel model linking Alice to Bob, neglecting the presence of Eve.

It is in this scenario that modern Forward Error Correction (FEC) schemes may offer an interesting solution. The idea is to make use of FECs inherent advantage of requiring a single channel use to reconcile the set of transmitted and received bits (”qubits” in the case of QKD).
Since extremely low residual Bit Error Rate (BER) must be achieved (theoretically, error free decoding is needed), capacity achieving codes with acceptable decoding complexities and with very long code-length n have been considered in the information reconciliation literature. LDPC codes constitute a possible interesting option. Furthermore, in order to minimize the quantity of information derived by Eve from the public channel, the code rate $R_c = k/n$ must be maximized, and it must be larger than 0.5. The description of the appropriate models for all the involved channels in Figure 4.1 (and in particular, the private and the public channels) will be given in the next sections.
In Quantum Key Distribution (QKD) and high-photon efficiency optical communications with direct detection, the transmission channel is typically modeled either as a Binary Symmetric Channel (BSC), or a Poisson Photon Channel (PPC) [55] with binary input, and the sufficient statistic at the channel output is typically obtained with a simple hard

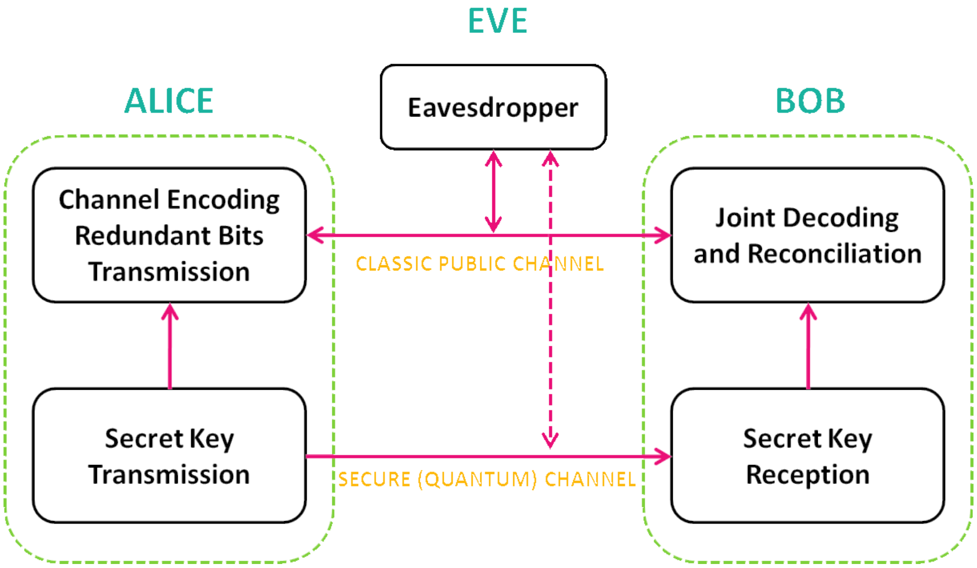


Figure 4.1: System model in a QKD system.

decision on the received random variable. The availability of public side-channel information typical of QKD applications, or the multilevel characteristic of the Poissonian output of weak-energy optical links may however allow the use of soft metrics and of soft-metric-based iteratively decoded error correcting codes, which may be useful to counteract the channel errors typical of such low-energy channels.
In this chapter we will show how soft-metric based metrics can be obtained in the considered scenarios [55], and how capacity achieving Forward Error Correcting (FEC) codes can be employed over QKD and Poisson cannels. Furthermore, the possible application of soft-metrics to information reconciliation protocols is discussed, with the goal of designing QKD protocols able to take advantage of the available soft-information. In particular, the use of FEC codes for information reconciliation could lead to QKD protocols able to minimize the interaction between transmitter (Alice) and receiver (Bob), allowing for higher quantum rates.

4.2 Information Reconciliation

The problem of information reconciliation in QKD schemes can be seen as the source coding problem with side information, as shown in Figure 4.2. Let X and Y be two of correlated variables belonging to Alice and Bob, and x and y their outcome strings, through information reconciliation it is possible to eliminate the discrepancies between x and y and agree on a string $S\left(x\right)$, with possibly $S\left(x\right)=x$.

Thus, as shown by Slepian and Wolf [57], the minimum information I that Alice

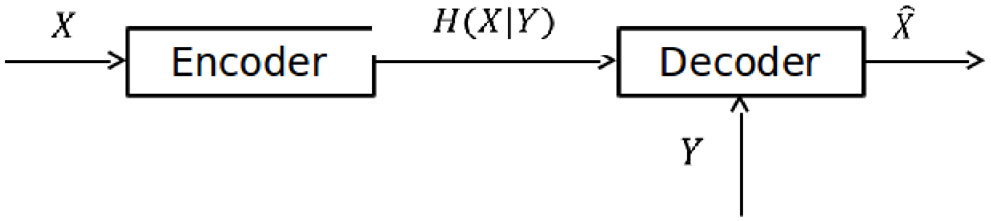


Figure 4.2: Source coding with side information.

would have to send to Bob in order to help him reconcile Y and X is $I_{opt} = H\left(X|Y\right)$. Taking into account that real reconciliation will not be optimal, a parameter $f > 1$ is used as a quality figure for the reconciliation efficiency:

$$I_{real} = fH\left(X|Y\right) > I_{opt}$$

4.3 Soft Metric Based QKD protocol

In any QKD scheme in general, Alice wants to transmit a plaintext message secretly to the receiver Bob. The secret key that will be later used for encryption is transmitted on a secure private (quantum) channel, which is secure because of the quantum mechanical properties. But the quantum channel may have a non-negligible bit error rate, that will be denoted as QBER, while comparatively the bit error rate on the public classical channel is typically very low, so that information reconciliation needs to be performed, typically using as media the more reliable (but not secure) public channel. After both Alice and Bob have knowledge of the secret key, Alice will encrypt the plaintext using the secret key according to the encryption rule of the system, and send the encrypted message to Bob, while Eve will not be able to recover the transmitted message, condition that Eve does not have the knowledge of the secret key.

As mentioned earlier, the problem of information reconciliation will be considered as if it were the source coding problem with side information. It is focused on effective FEC which exploits the “soft-metric” available at the exit of both the quantum and the public channel.

In Figure 4.3 the model for an equivalent systematic block-code in QKD system is presented. A composite channel is shown, which is formed by the parallel of the public and the quantum channels. The information and redundancy bits transmitted by these two communication channels constitute the codewords of an equivalent systematic block code. Alice divides the original information bit stream into blocks of finite length n_q which will be encoded in a redundant way into codewords of length n. The information bits (n_q bits per codeword) are transmitted over the quantum private channel, while the redundancy bits ($r = (n - n_q)$ bits per codeword) are transmitted over the classical public channel.

The code rate (or information rate) is equal to $R_c = n_q/n$ which is the proportion of the data-stream($nbits$) that is useful (non-redundant)[1].

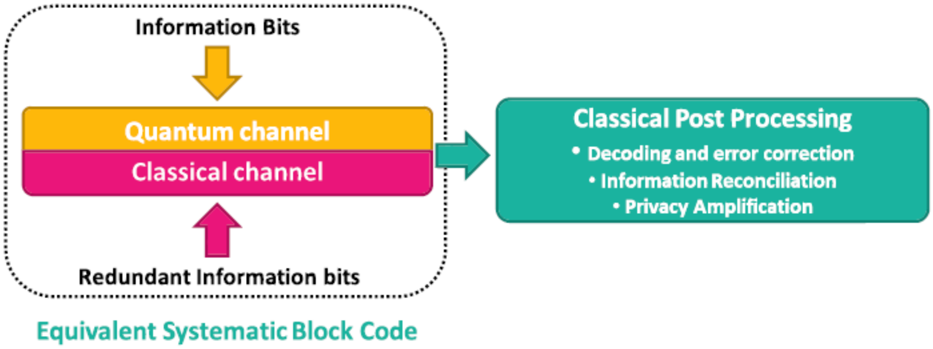

Information Bits
Quantum channel
Classical channel
Redundant Information bits
Equivalent Systematic Block Code
Classical Post Processing
• Decoding and error correction
• Information Reconciliation
• Privacy Amplification

Figure 4.3: Equivalent systematic block-code in QKD system.

The redundancy allows the receiver to detect and correct errors without re-transmission, using Forward Error Correction techniques. In this context, iterative belief propagation algorithms can be used to decode the codewords sent by Alice at the receiving stage, with a maximum likelihood decoding rule.
As previously mentioned, powerful capacity achieving or capacity approaching LDPC or polar codes with possibly long information blocks have been selected to make the quantum channel more reliable. This choice is motivated by the characteristics of LDPC and polar codes of being decodable in a time linearly proportional to their block length (when iterative belief propagation techniques are used), so that acceptable decoding complexities can be achieved also for large block lengths.

To minimize the quantity of information derived by Eve from the public channel the code rate must be maximized. In Figure 4.4 the rate code along with the number of available information and redundancy bits are highlighted, for a code with a rate equal to $n_q/(n_q+r) = n_q/n$. It is important to notice that at the input of the LDPC decoder, there will be n total available bits, i.e. n corresponding log-likelihood values.
The transmission rate on the QKD secret channel is generally very low since the technology is very complex, while the actual data rate on the public channel can be very high. It is therefore important to analyze the achievable overall QKD system rate. Furthermore, in practical cases, the quantum bit error rate on the secret channel is typically high when compared to the bit error rate of the public channel.

[1] That is, if for every n_q bits of useful information, the coder generates totally n bits of data, of which r are redundant

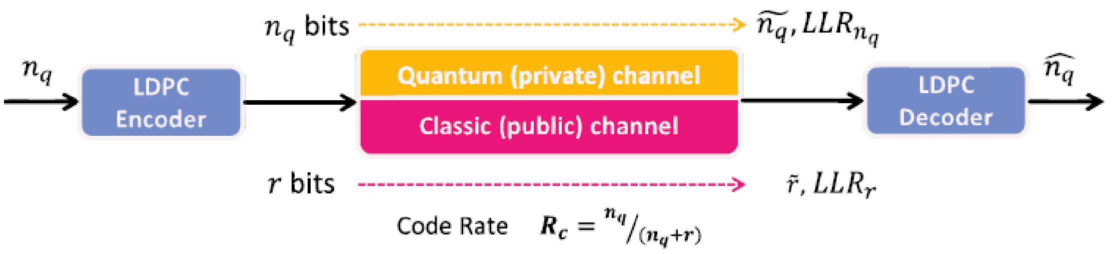


Figure 4.4: Composite Channel model, systematic FEC code with code rate $R_c = n_q/(n_q + r)$.

4.3.1 Code Rate and security

The public channel is authentic, Eve can listen to the public channel but can't do measurements on it. The information transmitted on the classic public channel is completely visible to the him. While on the other hand Eve can do measurements on the private quantum channel, but by doing so he will perturb the state of the quantum system, and that can lead to the detection of presence of Eve. In the security analysis it must be assumed that Eve has perfect knowledge of the code, and therefore of the r parity check equations used to generate the r parity bits ($(n - n_q)$ redundancy bits), that are assume to be received (eavesdropped) perfectly and without errors. The question then is how much information can Eve obtain about the n_q information bits from the knowledge of the r parity bits.
The r parity check equations represent a system of r linear equations in n_q variables over GF(2). This system in the case of LDPC codes is indeed quite sparse (i.e., few variables appear in each check equation). The space of solutions of such a system of equations represents the set of possible data sequences that Eve has access to. One of these solutions is in fact, the true data transmitted through the private quantum channel. The larger the size of the space of possible sequences, the more secure is the FEC code used against Eve. This assumes that Eve does not possess any additional information that may reduce the space of possible sequences. For instance, if the data transmitted by Alice is not independent identically distributed (i.i.d.) (i.e. binary with equal probabilities), Eve can easily focus on the most probable set of possible solutions of the linear equations. Note that the structural properties of the particular LDPC code used, ultimately determines the extent of the security of the system.
Let the data sequence transmitted over the private quantum channel be denoted by the n_q-component vector $\vec{X}$, and the parity checks transmitted over the classic public channel by the r-component vector $\vec{P}$. The amount of information provided about $\vec{X}$ by $\vec{P}$ is the mutual information $I\left(\vec{X},\vec{P}\right) = H\left(\vec{P}\right) H\left(\vec{P}|\vec{X}\right) = H\left(P\right) \leq r$, since $H\left(\vec{P}|\vec{X}\right) = 0$ (i.e., given $\vec{X}$, the amount of uncertainty remaining about $\vec{P}$ is zero). Remembering that

the quantum channel operates in conjunction with a classic public channel, together with the information bits the redundancy (parity check) bits generate an equivalent block code with rate:

$$R_c = \frac{n_q}{n_q + r} \tag{4.1}$$

So long as $n_q > 0$, a secret key can be distilled for a fixed code rate by increasing the block length. This puts a lower limit on the coding rate $\frac{1}{1 + r/n_q}$ of 0.5, which nonetheless is loose since the security of the scheme even at coding rate 0.5 or below ultimately depends on the particular FEC code being used.

4.4 System Characterization and Channel Models

In this section we present the system level models of the public and private channels in Figure 4.1.

4.4.1 Classical Communication System

A far as the public channel is concerned, it uses classical communication system with possibly strong coding so that the BER of the classic channel is very low. Typical Additive White Gaussian Noise (AWGN) channel model may be used, as shown in Figure 4.5, where n_k is a Gaussian random variable with variance σ^2 where for simplicity, a binary transmission scheme has been considered with the following association between the information bits b_k and the transmitted levels

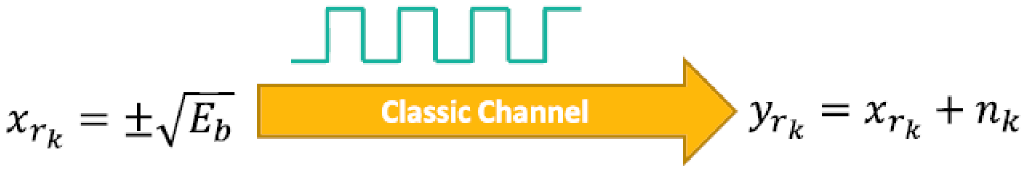


Figure 4.5: Classic AWGN model for the public channel.

The equivalent channel model shown in Figure 4.6 can be considered to represent a classic “public” channel in the QKD protocol being proposed.

In this model, when a bipolar transmission scheme is used such as PAM, BPSK or Gray coded QPSK, the k^{th} transmitted redundant bit is $b_k \in (0,1)$, the associated k^{th} transmitted symbol is $X_{r_k} \in (\sqrt{E_b}, +\sqrt{E_b})$, i.e. $X_{r_k} = \sqrt{E_b}(2b_k - 1)$, while $N_k \in N\,(0,\sigma^2)$ is a Gaussian random variable with zero mean and variance equals to $\sigma^2 = N_0/2 = E_b/2\eta_s$, where $\eta_s = E_b/N_0$ is the wireless link signal-to-noise ratio, and Y_{r_k} is

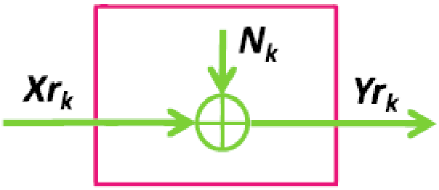


Figure 4.6: Classical Communication Channel.

the received sample obtained at the output of the public channel detector.
If soft decoding techniques are used in decoding the capacity achieving block codes, the channel output must be characterized with a likelihood ratio, i.e., the ratio between the likelihood (probability) of obtaining a given channel output conditioned on the possible transmitted bit. Often, the logarithm of this quantity defined as the Log Likelihood Ratio (LLR) is used. The LLR value for the public channel in Figure 4.5 is [58]:

$$\begin{aligned} LLR\left(Y_{r_k}\right) &= log\left[\frac{P\left(X_{r_k} = +\sqrt{E_b}|Y_{r_k}\right)}{P\left(X_{r_k} = -\sqrt{E_b}|Y_{r_k}\right)}\right] \\ &= log\left[\frac{P\left(Y_{r_k}|X_{r_k} = +\sqrt{E_b}\right)}{P\left(Y_{r_k}|X_{r_k} = -\sqrt{E_b}\right)}\right] \\ &= log\left[\frac{P\left(Y_{r_k}|b_k = 1\right)}{P\left(Y_{r_k}|b_k = 0\right)}\right] \end{aligned} \tag{4.2}$$

Equation 4.2 uses Bayes' Theorem[2]. Given the previous hypotheses, the expressions for the k^{th} trasmitted and received symbols respectively, can be written as:

$$X_{r_k} = \sqrt{E_b}(2b_k - 1) \tag{4.3}$$

$$Y_{r_k} = X_{r_k} + N_k = \sqrt{E_b}(2b_k - 1) + N_k \tag{4.4}$$

Y_{r_k} are the real signal samples being received, whose conditional probability density function is given by the Equation 4.5

$$f_y(Y_{r_k}|b_k) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{-(Y_{r_k} - \sqrt{E_b}(2b_k - 1))^2}{2\sigma^2}} \tag{4.5}$$

[2] Bayes' Theorem: $P(A|B) = \frac{P(B|A)P(A)}{P(B)}$

Finally, replacing the expressions presented in Equations 4.5 into Equation 4.2 the value of the LLR's metrics for the symbols received from the public channel can be expressed as:
This is the soft metric associated to the k^{th} redundant bit, associated to the sample Y_{r_k} at the output of the classic channel.

$$LLR\left(Y_{r_k}\right) = \frac{2Y_{r_k}\sqrt{E_b}}{\sigma^2} \tag{4.6}$$

4.4.2 Quantum Communication System

Many practical scenarios can be consider when modeling a quantum channel: the transmitted qubit can be associated to a single photon or a multi-photon, and different specific quantum states can be transmitted over the quantum channel (coherent state, entangled state, squeezed state, etc).
In this thesis, both single photon and multi-photon transmission will be considered when characterizing the quantum communication system in the context of the proposed QKD protocol. When referring to multi-photon transmission, coherent states will be considered, generated using weak laser pulses (WLP) sources.

4.4.2.1 Single-Photon Quantum Channel

When a single-photon is transmitted, the quantum channel can be modeled as a simple binary channel with error probability equal to the quantum bit error rate (QBER) Q, as shown in Figure 4.7.

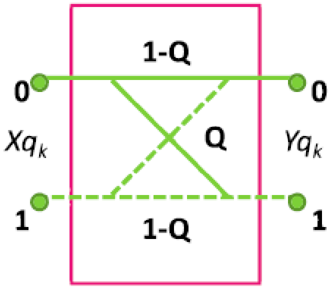


Figure 4.7: Equavelent QKD channel composed of clasical AWGN and Quantum BSC channel.

The expression for the Log-Likelihood metrics at the output of the quantum channel represented by the model of Figure4.7 used as input for the soft-metric decoder, is given by:

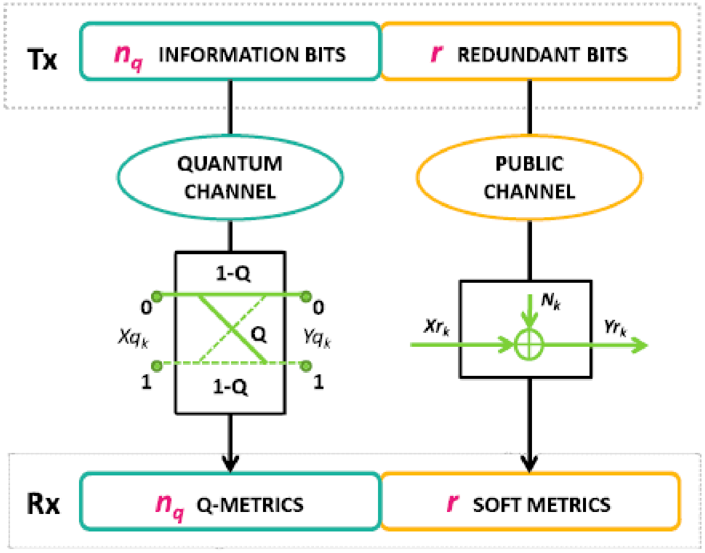
$$LLR(Y_{q_k}) = log\left[\frac{P(X_{q_k}=1|Y_{q_k})}{P(X_{q_k}=0|Y_{q_k})}\right] = log\left[\frac{P(Y_{q_k}|X_{q_k}=1)}{P(Y_{q_k}|X_{q_k}=0)}\right] \tag{4.7}$$

Denoting the k-th transmitted information bit as $X_{q_k} \in GF(2) = \{0,1\}$, and the received information bit as $Y_{q_k} \in GF(2) = \{0,1\}$ Equation 4.7 can be rewritten as follows:

$$LLR(Y_{q_k}) = log\left[\frac{P(Y_{q_k}=1|X_{q_k})}{P(Y_{q_k}=0|X_{q_k})}\right] = \begin{cases} log(\frac{1-Q}{Q}, & \text{if } X_{q_k}=1 \\ log(\frac{Q}{1-Q}, & \text{if } X_{q_k}=0 \end{cases} \tag{4.8}$$

It is also important to notice that the log-likelihoods (metrics) $LLR(Y_{q_k})$ can only assume two values, and will therefore be referred to as hard metrics or q-metrics,while the metrics from the public channel $LLR(Y_{r_k})$ can assume any real value, and are called soft metrics.

Since these metrics must be jointly used and compared in the LDPC decoder they need to be compatible and comparable. The equivalent QKD channel composed of classical AWGN and Quantum BSC channel that will provide us the available bits and metric for soft decoding can be shown in Figure 4.8.



$$R_c = \frac{n_q}{n_q + r}$$

Figure 4.8: Equavelent QKD channel composed of clasical AWGN and Quantum BSC channel.

4.4.2.2 Binary Input Multiple Output (BIMO) Quantum Channel

This section will describe the use of photon counting detectors which generate soft information at the output of a quantum channel as opposed to quantum binary symmetric channel which leads to hard decision decoding.
Figure 4.9 represents a sketch of the binary communication scheme based on polarization degree of freedom of a coherent state $|\alpha\rangle$. The information bit $k = \{0,1\}$ is encoded by applying the unitary transformation $U(\phi_k)$ to the polarization degree of freedom of a coherent state $|\alpha\rangle$, which is assumed to be initially in the polarization state $|+\rangle = \frac{|H\rangle+|V\rangle}{\sqrt{2}}$. This technique is based on the use of a Phase Beam Splitter (PBS) and two photon counters. The scheme allows one to map the discrete bit value "k" to an optical polarization quantum bit (or qubit), but at the detection stage can produce a discrete set of real numbers, which can also be expressed in the form of Log-Likelihood Ratios (LLR) which can be used for soft information processing. A possible experimental setup is shown in Figure 4.9, where the polarization degree of freedom ϕ_k of a coherent state is associated to the information bit "k" according to the following encoding rule:

Table 4.1: Encoding rule

k	$\longrightarrow$	ϕ_k
0	$\longrightarrow$	$\pi/4$
1	$\longrightarrow$	$3\pi/4$

So that there is a phase shift of $\pi/2$ of the qubit associated with $k = 0$ relative to the qubit associated with $k = 1$. The transformation $U(\phi_k) = exp(\frac{-\phi_k}{2}\sigma_3)$ is then applied, where σ_3 is the Pauli rotation matrix. This kind of transformation can be realized by means of a potassium dihydrogen phosphate (KDP) crystal driven by a high voltage generator and corresponds to change of the polarization from linear to elliptical.

At the detection stage a measurement of the phase shift of the qubit should be performed. This can be implemented as depicted in Figure 4.9 by using a Half-Wave Plate (HWP) placed in front of a Polarizing Beam Splitter (PBS) with two photon-counters providing the number of photons in the reflected and transmitted beams, denoted as n_0 and n_1 respectively. Let $n = n_0 + n_1$ denote the total number of detected photons. We assume this is also the total number of transmitted photons (in the hypothesis that no photon is lost), which is a Poisson distributed random variable with mean value $E[N] = N_c = |\alpha|^2$. Notice that, due to the weak energy of the transmitted optical signal, the value of N_c is typically small.
From the knowledge of the photon counts n_0 and n_1, the actual value of the phase shift can be obtained by using the Bayesian estimator [34]

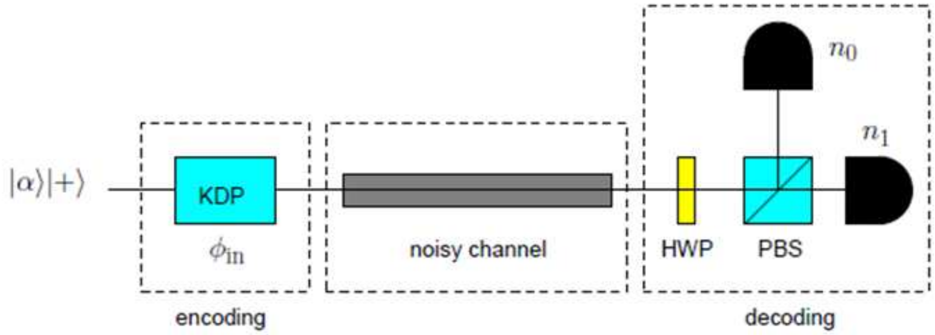


Figure 4.9: The considered low-complexity photon-counting scheme.

$$\phi_{est} = \int_0^\pi \phi p_B(\phi|n_0,n)\mathrm{d}\phi = E\left\{\phi|n_0,n\right\},$$

where,

$$\begin{aligned} p_B(\phi|n_0,n) &= \tfrac{p(k=0|\phi)^{n_0} p(k=1|\phi)^{n_1}}{N} \\ &= \tfrac{p(0|\phi)^{n_0} p(1|\phi)^{n-n_0}}{N} \end{aligned} \tag{4.9}$$

is the probability density function of the received phase shift given the fact that $n = n_0 + n_1$ photons have been received and n_0 photons have been counted at the "$k = 0$" output of the PBS. N is a normalization factor such that

$$\int_0^\pi p_B(\phi|n_0,n)\mathrm{d}\phi = 1,$$

This scenario generates the equivalent channel model with binary input (the random variable k), and multilevel output (the couple of random variables n_0,n_1) shown in Figure 4.10, which will be discussed in what follows.

Evaluation of the Log-Likelihood Ratios

In soft-decoding algorithms, Log-Likelihood-Ratios are typically required, which, for the channel model shown in Figure 4.10 can be defined as:

$$LLR(n_0,n_1) = log\left[\frac{p\left(k=1|\{n_0,n_1\}\right)}{p\left(k=0|\{n_0,n_1\}\right)}\right] \tag{4.10}$$

where,

$$p\left(k|\{n_0,n_1\}\right) = p\left(\phi_k|\{n_0,n_1\}\right) \quad k = 0,1 \tag{4.11}$$

is the probability that the transmitted bit was "k" given the measurement pair(n_0,n_1). Using Baye's theorem, Equation 4.10 can be rewritten as:

$$LLR(n_0,n_1) = log\left[\frac{p\left(\{n_0,n_1\}\left|k=1\right.\right)}{p\left(\{n_0,n_1\}|k=0\right)}\right] \tag{4.12}$$

Since coherent states are being used, the number of photons n_0 and n_1 measured at the two detectors are uncorrelated and, in particular, are distributed according to a Poisson statistic. Given ϕ_k, the average number $N_k^{(h)}$ of photons of type k detected at the detector "h" is given by the expression [33]:

$$N_k^{(h)} = N_c p(h|\phi_k) \;\; h,k = 0,1 \tag{4.13}$$

where $N_c = |\alpha|^2$ is the average number of photons of the input coherent state, and

$$\begin{aligned} p(0|\phi_k) &= \frac{1}{2}\left(1+\mathrm{e}^{-\Delta^2} cos\left(\phi_k\right)\right) \\ p(1|\phi_k) &= \frac{1}{2}\left(1-\mathrm{e}^{-\Delta^2} cos\left(\phi_k\right)\right) \end{aligned} \tag{4.14}$$

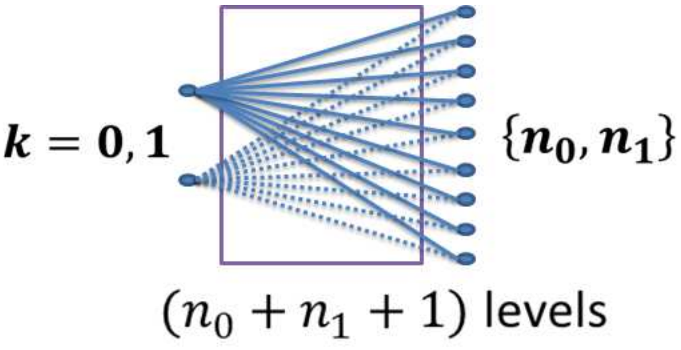


Figure 4.10: BIMO channel model of the considered system.

where, to make the analysis more general, it is assumed that during propagation, the qubit undergoes a phase diffusion process whose amplitude is characterized by the parameter $\varDelta$ (the feasibility of this scheme and its experimental demonstration have been

thoroughly investigated in [44]).
We have therefore:

$$p(n_0,n_1|k) = P(n_0,N_k^{(0)})P(n_1,N_k^{(1)}) \tag{4.15}$$

$$P(l,N) = \frac{e^{-N}N^l}{l!} \tag{4.16}$$

where, $P(l,N) = \frac{e^{-N}N^l}{l!}$ is the Poisson probability distribution. Then, substituting Equation 4.16 into Equation 4.12 the following expression for the LLR can be easily obtained:

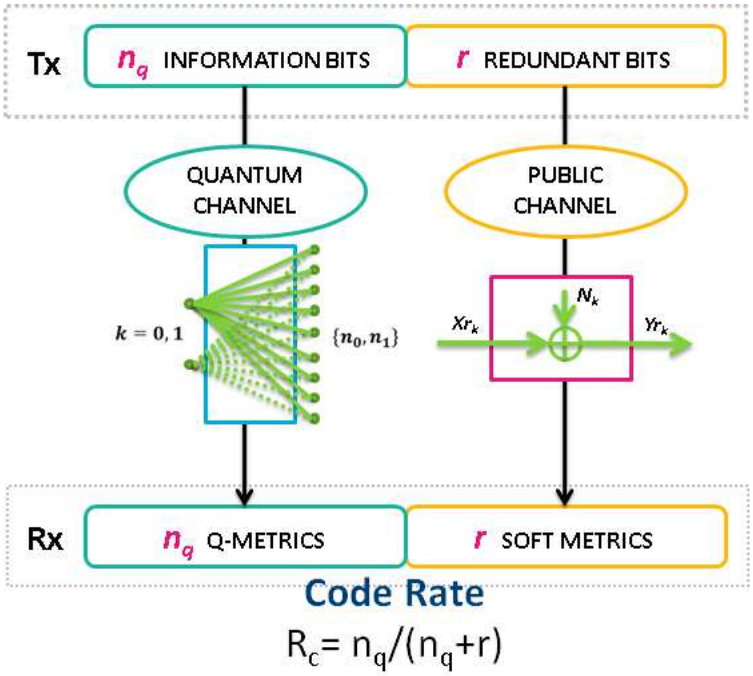


Figure 4.11: Equavelent QKD channel composed of classical AWGN and Quantum BIMO channel.

$$LLR(n_0,n_1) = (n_0 - n_1)log\left(\frac{p_{ii}}{p_{ij}}\right) \tag{4.17}$$

where,

$$p_{ii} = P(0|\phi_0) = P(1|\phi_1) = \frac{1}{2}\left(1 + e^{-\Delta^2}cos(\frac{\pi}{4})\right)$$
$$p_{ij} = P(1|\phi_0) = P(0|\phi_1) = \frac{1}{2}\left(1 - e^{-\Delta^2}cos(\frac{\pi}{4})\right) = 1 - p_{ii}$$

The system described up to this point can be modeled as a Discrete Memoryless Channel (DMC), and more precisely a Binary Input-Multiple Output (BIMO) channel, with binary input k and $n + 1 = n_0 + n_1 + 1$ outputs (n_0,n_1) (where n is a Poisson distributed random variable) as shown in Figure 4.10. The capacity of this channel is evaluated in the next chapter.
Finally, the equavelent QKD channel composed of classical AWGN and Quantum BIMO channel, which will give us the available bits and metric for soft decoding is shown in Figure 4.11.

Chapter 5

Capacity of Bayesian Inference Quantum Channel employing Photon counting detectors

In Chapter 4.4.2.2 the potential improvements in key transmission rate in a Quantum Key Distribution (QKD) scheme whereby photon-counting detectors (PCD) are used at the receiver were discussed. To take full advantage of such detectors, soft information is generated in the form of Log-Likelihood Ratios (LLRs).

In order to quantify the performance improvement may be achieved by such a detector, we will determine the capacity of the corresponding optical channel, and the achievable residual Bit Error Rate (BER) of practical communication schemes on such a channel. From a telecommunication point of view, the presence of a photon counting detector provides the possibility of generating at the receiver a soft-metric (as opposed to a hard metric which essentially indicates the presence or absence of a signal from an on/off detector) that may be used in iteratively decoded forward error correcting codes.

The receiver introduced in [33] is based on an optical setup for one-parameter qubit gate optimal estimation [34, 44], where the qubit is a polarization state of coherent states and the one-parameter gate corresponds to a polarization transformation. In the ideal case, orthogonal polarization states can be perfectly discriminated. However, in a realistic scenario and especially in free-space communication, non-dissipative noises affecting light polarization disturbs the orthogonality of the states at the receiver, thus requiring a suitable detection and strategy for discrimination. It is worth noting that coherent states preserve their fundamental properties when propagating in purely lossy channels, suffering only attenuation, thus only the noise affecting the polarization is the most detrimental.

In this chapter the limits of the achievable performance gains when using photon counting detectors are explored and compared to the case when such detectors are not available. To this end, the classical capacity of the Bayesian inference channel is found, clearly showing the potential gains that photon counting detectors can provide in the context of a realistic cost-effective scheme from an implementation point of view. While there are binary communication schemes that can achieve a higher capacity for a given mean photon count at the receiver compared to the scheme presented here (e.g., the Dolinar receiver [36]), most such schemes are complex and at times unrealistic from an implementation point of view.

5.1 Capacity Evaluation

The quantum channel in d-dimensions is often modeled as a completely positive trace preserving map Ψ. The most common channel model is the depolarizing channel which depends on one parameter λ mapping a mixed state in C^d into:

$$\rho \longrightarrow \lambda\rho + \frac{1-\lambda}{d} I$$

where I is the $d \times d$ identity matrix. For a general quantum channel, let ε denote the ensemble of input states, and M the measurement or a Positive Operator Valued Measure (POVM)$\{E_j\}$ at the channel output. The input state ensemble, channel and measurement together define a classical noisy channel with transition probabilities:

$$p_{nm} = T_r \left[\Psi(\rho_n)E_m\right]$$

Defining the probabilities over the input state, which we will denote as X, a natural definition of classical capacity of the quantum channel would be:

$$C_{shan}(\Psi) = \sup_{\varepsilon,M} \; I(X;Y)$$

where Y is the output state and $I(X;Y)$ is the Shannon mutual information. The complication in defining the capacity of the quantum channel in contrast with the classical channel arises in connection with the purely quantum-mechanical effects, which have no analogue in the classical domain, like for instance the entanglement. In particular, it is reasonable to assume (which is in fact shown to be true) that the capacity of parallel copies of a quantum channel with entangled inputs may be larger than the sum capacity of each channel treated separately. It turns out that for the most common channel model, namely the depolarizing channel, entanglement buys nothing.

The closest analogue of the binary communication scheme proposed here is the Binary Phase Shift Keying (BPSK) using coherent states. It is well known that for such a scheme the Dolinar receiver achieves nearly optimal results with capacity [41],citechap5d:

$$C_{BPSK-Dolinar} = 1 - H_2\left(0.5\left(1 - \sqrt{1 - e^{-4N_C}}\right)\right)$$

where, $H_2(.)$ is the binary Entropy function. This capacity is close to the ultimate capacity obtained using an as yet unknown optimal receiver:

$$C_{BPSK-Ultimate} = 1 - H_2\left(0.5\left(1 + e^{-2N_C}\right)\right)$$

The Dolinar receiver requires a complicated feedback system for its implementation, hence there is significant difference in the level of the complexity with respect to a photon counting receiver.

The discussion thus far has been general and focused on quantum channels as trace-preserving maps. However a much more humble pursuit in can be adopted and that is modeling an experimental setup using realistic off-the-shelf components, and specifically calculating the traditional Shannon capacity of the link viewed as a probabilistic transition mechanism that maps input bits into possibly multi-level outputs used for detection. In this sense, the channel is modeled as a Binary Input-Multilevel Output (BIMO) Discrete Memoryless Channel (DMC) as previously shown in Figure 4.10, and our goal is to contrast the capacity of a system employing photon counting detectors to that of the equivalent Binary Symmetric Channel (BSC) resulting from reducing the photon counts to presence or absence of signals (i.e., hard decoding).

As noted earlier, the sufficient statistic for detection with photon counting detectors is the count difference of detector 1 and 0 in Figure 4.9, i.e., $(n_1 - n_0)$. The outputs of the two counters are independently distributed Poisson random variables, i.e.

$$\begin{aligned} n_1 &\sim Poisson, \mu_1 = N_k^{(1)} \\ n_0 &\sim Poisson, \mu_0 = N_k^{(0)} \end{aligned}$$

where,

$$\begin{aligned} N_k^{(1)} &= N_c p(1|\phi_k) \\ N_k^{(0)} &= N_c p(0|\phi_k) \\ N_k^{(0)} + N_k^{(1)} &= N_c \end{aligned}$$

As a consequence, the difference $(n_1 - n_0)$ is Skellam distributed, and we have

$$P(n_1 - n_0 = m|\phi_k) =$$

$$e^{-\left(N_k^{(1)}+N_k^{(0)}\right)}\left(\frac{N_k^{(1)}}{N_k^{(0)}}\right)^{m/2} I_{|m|}\left(2\sqrt{N_k^{(1)}N_k^{(0)}}\right)$$

where, $k = 0$ or 1, and $I_{|m|}(.)$ is the modified Bessel function of the first kind and order $|m|$. Note that m itself is an integer that can be positive or negative. Plugging known values of the parameters, we get:

$$\frac{N_k^{(1)}}{N_k^{(0)}} = \frac{p(1|\phi_k)}{p(0|\phi_k)}$$

$$N_k^{(1)} N_k^{(0)} = N_c^2 p(1|\phi_k) p(0|\phi_k)$$

Specializing to the case ”0 is transmitted and is mapped to ϕ_0” we get:

$$P(n_1 - n_0 = m|\phi_0) =$$
$$e^{-N_c} \left(\frac{\sqrt{2} - e^{-\Delta^2}}{\sqrt{2} + e^{-\Delta^2}} \right)^{m/2} I_{|m|} \left(N_c \sqrt{1 - \frac{e^{-2\Delta^2}}{2}} \right)$$

similarly for the case “1 is transmitted and is mapped to ϕ_1” :

$$P(n_1 - n_0 = m|\phi_1) =$$
$$e^{-N_c} \left(\frac{\sqrt{2} + e^{-\Delta^2}}{\sqrt{2} - e^{-\Delta^2}} \right)^{m/2} I_{|m|} \left(N_c \sqrt{1 - \frac{e^{-2\Delta^2}}{2}} \right)$$

Let X be the random variable associated with the transmitted phase ϕ_k (or the transmitted bit “k”) and Y be the channel output (i.e. our sufficient statistic $(n_1 - n_0)$. Then, the formulas above give us the channel transition probabilities for the considered DMC. Using the classic definition of mutual information:

$$I(X;Y) = H(X) - H(X|Y)$$

and noting that the input is binary with $p(X = 0) = p(\phi_0) = p$, and $p(X = 1) = p(\phi_1) = 1 - p$, after some manipulation we have:

$$p(X = 0|Y = m) = \frac{p}{p(1 - \alpha_\Delta^m) + \alpha_\Delta^m}$$
$$p(X = 1|Y = m) = \frac{1 - p}{p(1 - \alpha_\Delta^m) + \alpha_\Delta^m}$$

where,

$$\alpha_{\Delta} = \frac{(\sqrt{2} + e^{-\Delta^2})}{(\sqrt{2} - e^{-\Delta^2})}$$

Finally, the conditional entropy based on two parameters, p and Δ can be written as:

$$\begin{aligned}
&H(X|Y) = \\
&- e^{-N_c} \sum_m p.(\alpha_{\Delta})^{-(m/2)} (B_m) log\,(p(X = 0|Y = m)) + \\
&- e^{-N_c} \sum_m (1 - p).(\alpha_{\Delta})^{(m/2)} (B_m) log\,(p(X = 1|Y = m)) \\
&where, \\
&B_m = I_{|m|} \left(N_c \sqrt{1 - \frac{e^{-2\Delta^2}}{2}} \right)
\end{aligned}$$

While the BIMO DMC is neither symmetric nor weakly symmetric, it is not difficult to show that the maximizing input probability distribution is uniform. Hence, $p = 0.5$ maximizes the mutual information leading to channel capacity. To compare the capacity of the link employing photon counting detector to that of a simple detector signaling the presence or absence of signal, it needs to be specified that how such a detector behaves. It is logical to assume that cross-over probability of the equivalent BSC (i.e. the raw Bit Error Rate, denoted in the following as QBER) associated with such a receiver can be obtained as:

$$\begin{aligned}
QBER &= \sum_{m=1}^{\inf} P(n_1 - n_0 = m|\phi_0) + \frac{1}{2} P(n_1 - n_0 = 0|\phi_0) \\
&= \sum_{m=1}^{\inf} P(n_1 - n_0 = -m|\phi_1) + \frac{1}{2} P(n_1 - n_0 = 0|\phi_1)
\end{aligned} \tag{5.1}$$

Notice that when $(n_1 - n_0) = 0$ (which for low values of N_c happens often), the detector chooses at random between $k = 0$ and $k = 1$.

Figure 5.1 depicts the capacity of our BIMO DMC and its comparison to the equivalent Binary Symmetric Channel (BSC) in case of hard decision decoding as a function of the mean photon count N_c in the case the phase diffusion parameter Δ is zero.

Figure 5.2 depicts the capacity of our BIMO DMC and its comparison to the equivalent BSC in case of hard decision decoding as a function of the phase diffusion parameter Δ

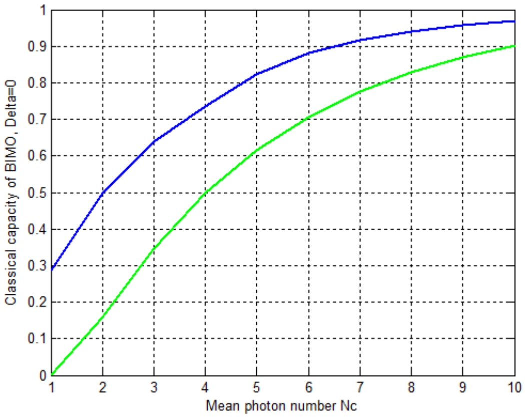


Figure 5.1: Classical capacity of BIMO DMC(solid curve) compared to the equivalent BSC with transition probability QBER, as a function of mean photon count N_c.

for three different values of the mean photon count N_c.
It can be observed that the BIMO DMC channel offers a capacity improvement over the equivalent BSC. This improvement could lead to a BER improvement when comparing the two channels in presence of an error correction code, as it will be shown in chapter 7.

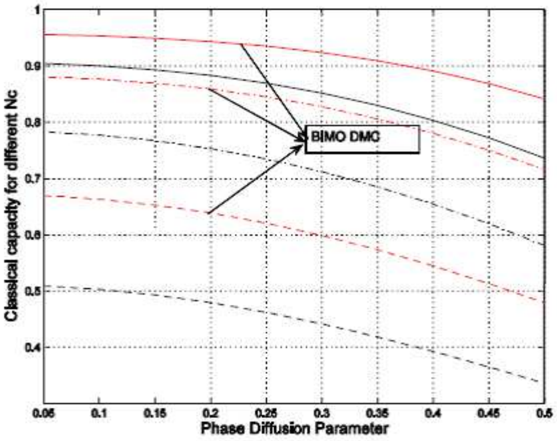


Figure 5.2: Classical capacity of BIMO DMC and equivalent BSC with transition probability QBER as a function of phase diffusion parameter Δ for three different values of N_c (solid line: $N_c = 9$, dash-dot line: $N_c = 6$, dash line: $N_c = 3$).

Chapter 6

LDPC Coding for QKD at Higher Photon Flux Levels Based on Spatial Entanglement of Twin beams in PDC

Twin beams generated by Parametric Down Conversion (PDC) exhibit quantum correlations that has been effectively used as a tool for many applications including calibration of single photon detectors. By now, detection of multi-mode spatial correlations is a mature field and in principle, only depends on the transmission and detection efficiency of the devices and the channel. In [60], [62], [63], the authors utilized their know-how on almost perfect selection of modes of pairwise correlated entangled beams and the optimization of the noise reduction to below the shot-noise level, for absolute calibration of Charge Coupled Device (CCD) cameras. The same basic principle is currently being considered by the same authors for possible use in Quantum Key Distribution (QKD) [[61], [59]]. The main advantage in such an approach would be the ability to work with much higher photon fluxes than that of a single photon regime that is theoretically required for discrete variable QKD applications (in practice, very weak laser pulses with mean photon count below one are used). The natural setup of quantization of CCD detection area and subsequent measurement of the correlation statistic needed to detect the presence of the eavesdropper Eve, leads to a QKD channel model that is a Discrete Memoryless Channel (DMC) with a number of inputs and outputs that can be more than two (i.e., the channel is a Multilevel DMC).

This chapter investigates the use of Low Density Parity Check (LDPC) codes for information reconciliation on the effective parallel channels associated with the multi-level DMC.

6.1 Introduction

Parametric Down Conversion (PDC) is an effective means of producing entangled photons. The state produced by spontaneous PDC exhibits perfect momentum phase matching for a plane wave pump field.
The state of a single bipartite transverse mode near degeneracy can be written as:

$$\left|\psi\left(\vec{q}\right)\right\rangle = \sum_{n} C_{\vec{q}}\left(n\right)\left|n\right\rangle_{i,\vec{q}}\left|n\right\rangle_{s,\vec{-q}} \tag{6.1}$$

where, i stands for the idler and s stands for the signal beam. The two modes in Equation 6.1 are entangled in the number of photons in each pair of modes $\pm\vec{q}$. Imaging the beams in the far field of a thin lens of focal length f in a $f-f$ arrangement as depicted in Figure 6.1, leads to an association of each mode to a unique position in the focal plane via the mapping:

$$\frac{2cf}{\omega_p}\vec{q} \rightarrow \vec{x}$$

Hence, a perfect correlation should be detected in the photon numbers $n_{i,\vec{x}}$ and $n_{s,-\vec{x}}$

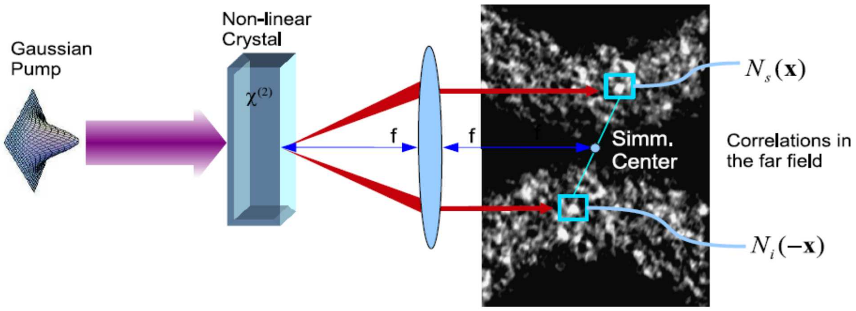


Figure 6.1: General block diagram of the experimental setup from [62].

where the center of symmetry relative to which the symmetric positions are identified is the pump detection plane interception point. In reality, the pump field is not a perfect plane wave, rather a Gaussian beam with spatial waist w_p inducing an uncertainty in the relative propagation direction of the twin photons on the order of the angular beam-width of the pump. This uncertainty is the coherence area of the process roughly corresponding to the transverse size of the mode in the far field and is given by:

$$A_{\omega h} \sim \left[\frac{2\pi cf}{\omega_p w_p}\right]^2$$

The number of spatial modes observed over a detection area that is usually taken to be much larger than the coherence area is given by $M_{spatial} = A_{det,j}/A_{coh}$, where $j = i$ or

s. Similarly, it is assumed that the detection time is much larger than the coherence time hence the number of temporal modes $M_t = T_{det}/T_{coh}$ is much larger than one. The total number of modes in the detection region is $M_{tot} = M_{spatial}M_t$. The different modes in a single region are independent and thus the statistics of the detected photons is multi-thermal with mean value $\langle N_j \rangle = M_{tot}\eta_j\mu$, where, $j = i$ or s, μ is the number of photons per mode, and η_j is the overall efficiency. The variance of the number of detected photons is given by:

$$\langle \delta^2 N_j \rangle = \langle N_j \rangle \left(1 + \frac{\langle N_j \rangle}{M_{tot}}\right) = \langle N_j \rangle (1 + \varepsilon) = M_{tot}\eta_j\mu\,(1 + \eta_j\mu) \tag{6.2}$$

where ε is the excess noise defined as fluctuations that exceed the Shot Noise Limit (SNL). The co-variance between the signal and idler photon numbers is given by:

$$\langle \delta N_i \delta N_s \rangle = M_{tot}\eta_j\eta_s\mu\,(1 + \mu) \tag{6.3}$$

The correlation statistic between signal and idler is measured in terms of the fluctuations of the difference $N_- = N_s - N_i$ normalized to the corresponding level of shot noise:

$$\sigma = \frac{\langle \delta^2 N_- \rangle}{\langle N_i + N_s \rangle} = 1 - \eta_+ + \frac{\eta_-^2}{4\eta_+^2}\left(\eta_+ + \frac{\langle N_s + N_i \rangle}{M_{tot}}\right) \tag{6.4}$$

where, $\eta_+ = (\eta_s + \eta_i)/2$ and $\eta_- = \eta_s - \eta_i$. If the losses are perfectly balanced, $\eta_s = \eta_i = \eta$ and we get $\sigma = 1 - \eta$ depending only on the quantum efficiency. In the ideal case of perfect efficiency, indeed, $\sigma \rightarrow 0$ while for classical states of light the degree of correlation is bounded by $\sigma \geq 1$ with the lower limit achieved by coherent beams leading to $\sigma = 1$. The basic requirement on the size of the detection area is that the number of speckles in the region far exceed the number on the perimeter. A pictorial representation of this is depicted in Figure 6.2. The core idea of using the spatial entanglement of twin beams for Quantum key Distribution (QKD) stems from the fact that the correlation statistic generated on two symmetric regions in the CCD focal plane must exhibit $\sigma < 1$. Eavesdropping by Eve will lead to increase in σ above one and is therefore detectable. Indeed, the extent of interference by Eve may be measured by how much σ has increased beyond its expected value. Depending on the extent of this interference, the parties can decide to either continue generating a random key or halt the process all together. Note that under ideal circumstances $\sigma \rightarrow 0$, while practically, it is always above zero but hopefully sufficiently below one to allow for secure communication to take place. This is pictorially depicted in Figure 6.3. In reality, one cannot assert that eavesdropping Eve will always lead to $\sigma > 1$. Even in the simplest situation, Eve can always reduce the level of eavesdropping for having $\sigma < 1$, but then again the information she acquires will be very small as well.

Eventually, disposing of ideal technologies, Eve can measure a certain number N of photons and reproduce it by a squeezed source in the photon number even post selected (e.g.,

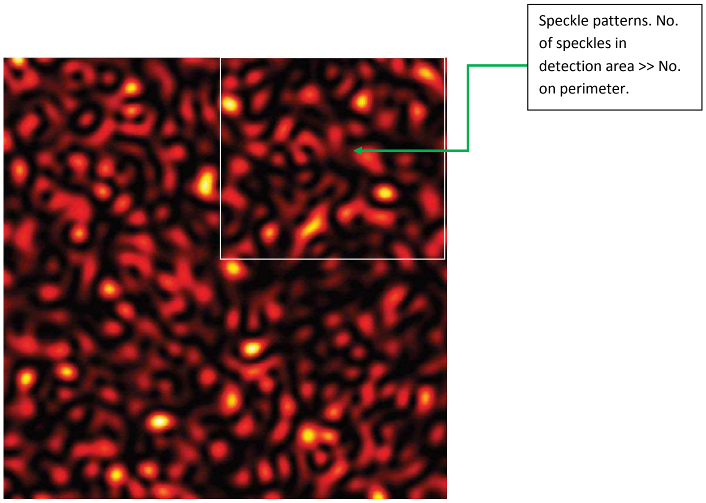


Figure 6.2: A detection region identified as a square on the upper right corner whereby the condition that the number of speckles in the region is much larger than that on the perimeter is satisfied.

a PDC sources), sending to Bob the signal only when she observes N Photons in the heralding channel. However, if one could detect quantum correlations in the near field and in the far field, this would correspond to having two conjugated bases. In this case, only entanglement should provide strict correlation at the same time in the two measurements, a situation that cannot be reproduced by Eve.
The process of generating a random key based on this core concept is as follows:

- Alice generates the twin beams via PDC and images one of the two beams on its CCD array and launches the second beam towards Bob;
- both Alice and Bob are assumed to have achieved timing synchronization so they know the start and end time of each firing of the laser pulses;
- the CCD detection area is partitioned into a number of smaller detection areas we call super-pixels, say four equal sized regions, satisfying our basic requirement that the detection area be much larger than the coherence area of the spatial modes;
- Alice and Bob make measurements on one reference quadrant (Alice and Bob's reference quadrants are at symmetric positions). Alice sends Bob her measurement results that Bob uses to estimate σ based on his a-priori knowledge of system level parameters and experimental setup uncertainties. Bob repeats the same process on a different set of measurement so that Alice can obtain a similar statistic. If the measured σ is acceptable by both parties, they continue with the protocol;

- assuming the measurements made on the reference quadrant in the previous step indicated that impact of eavesdropping by Eve is tolerable, Alice and Bob make measurements of the number of the detected photons in the other quadrants. A pair of quadrants, one at Alice and one at Bob, that are in symmetric regions of their CCDs focal plane represent a quantum channel between the two parties. In our example, three of the four quadrants would be used and constitute three parallel quantum channels that can be used to generate random keys;

- for each of the quantum channels described in the previous step, Alice and Bob make a measurement of the number of their detected photons and use binning and associate a unique label to their measurement. Ideally, for each quantum channel, Alice and Bob obtain an identical sequence of labels in their measurement that constitute a secret key. In practice, fluctuations in the number of measured photons lead to discrepancies and the label sequence at Alice and Bob don't match perfectly, hence requiring Information Reconciliation (IR) and privacy amplification to lead to distilled keys that can be used for cryptography.

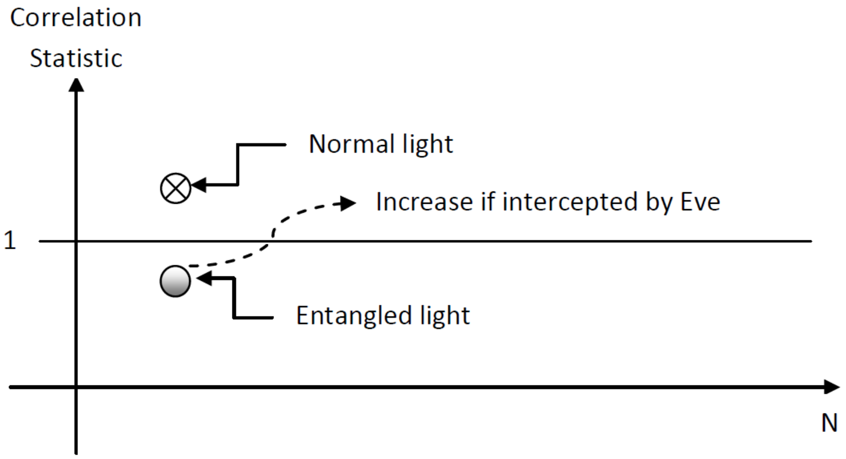


Figure 6.3: Pictorial representation of the impact of eavesdropping by Eve on the measured correlation statistic.

6.2 Development of the Channel Model

The aim of this section is to outline in detail the process for generating the binary or multilevel DMC channel model for each of the parallel quantum channels described in the previous section. To this end, we need a detailed knowledge of the photon statistics in each detection area. As stated previously, the number of modes in a given detection area is very large. The number of temporal modes is dependent on the duration of the laser pulse width and the coherence time and is reported to be 5000 in [62]. The number of spatial modes is dependent on the size of the detection area that carries a trade-off in terms of the degree of the determination of the Center of Symmetry (CS), requiring a small detection area, and visibility of the quantum correlation, requiring a large detection area. The determination of the center of symmetry can be done with high resolution using small pixels and then performing the experiment with larger pixels.

In the experimental setup presented in [62], the number of spatial modes is about 150. Given the large number of detected modes, the statistic of the number of detected photons in a given region is multi-thermal.For a single mode, the thermal distribution is geometric with Probability Mass Function (PMF) $P_1\left(n\right) = \left(1-\zeta\right)\zeta^n$, where, the parameter ζ is related to the mean of the geometric PMF λ via $\zeta = \frac{\lambda}{1+\lambda}$. The photons in different modes are independent and therefore the PMF of the total number of detected photons in N modes is the N-fold convolution of the geometric PMF and given by:

$$P_N\left(k\right) = \frac{\left(k+N-1\right)!}{k!\left(N-1\right)!}\left(1-\zeta\right)^N\zeta^k$$

The mean and variance of the photon number in this case is given by $E\left[X\right] = N\lambda$ and $\sigma_X^2 = N\lambda\left(1+\lambda\right)$.

In each detection region, at either Alice or Bob, the number of photons are counted and using a binning approach (i.e., multi-level quantization), the bin to which the number of detected photons belong is identified and the associated symbol is assigned as a component of a potential secret key. The Alice and Bob's measurements on the symmetric detection regions illuminated by the entangled twin beams may either result in identical bins, leading to identical symbols, or different bins leading to two different symbols. The derivation of the channel model requires computation of the probability that a certain number of photons is detected at Alice, and another number is detected at Bob. Once this joint probability is known, the computation of the transition probabilities associated with the resulting DMC modeling the behavior of a fictitious channel we may imagine exists between Alice and Bob and causes discrepancies between their detected symbols becomes straightforward.

The problem of determination of the number of detected photons at Alice and Bob is essentially a bipartite detection problem. Let $P\left(n\right)$ denote the probability of generation of n photon-pairs at the source and let $Bin\left(k|n,\zeta\right)$ denote the binomial PMF:

$$Bin\left(k|n,\zeta\right) = \frac{n!}{k!(n-k)!}\zeta^k(1-\zeta)^{n-k}$$

then the probability of detecting k photons at Alice and m photons at Bob is given by:

$$P\left(k,m\right) = \sum_{n=max(k,m)}^{\infty} P\left(n\right)Bin\left(k|n,\zeta_A\right)Bin\left(k|n,\zeta_B\right) \tag{6.5}$$

where, ζ_A and ζ_B are related to the mean of the geometric PMF for a single mode. Substituting $P_N(n)$ for $P()$ in above expression we get the desired PMF of detecting k photons at Alice and simultaneously m photons at Bob over our detection area.

6.3 Information Reconciliation

Alice and Bob need to be in possession of identical sequences of symbols before they can proceed with privacy amplification and generate secure keys for encryption. Information Reconciliation (IR) is the process of eliminating discrepancies that may exist in the sequences at Alice and Bob as much as possible. This is achieved, as seen in the previous chapters, using error correction coding. The process is not perfect in that there is always some residual symbol errors left leading to very low symbol and frame error rates. By selecting a very low frame error rate threshold, one can almost guarantee that the symbol sequences at Alice and Bob are identical with very high probability. Multitude of error correction techniques are available for information reconciliation. Broadly speaking, we can classify the available techniques into

I Forward Error Correction (FEC) techniques, and;

II interactive two-way coding schemes with feedback such as the CASCADE algorithm.

Fundamentally from an information theoretic point of view , there is no advantage to two-way interactive techniques (this is reinforced in light of the given symmetry of the problem formulation presented in the introduction section). Either Alice or Bob could initiate an information reconciliation protocol since their roles are perfectly interchangeable.
There are however some simple criteria one could apply in making the selection of a suitable technique:

- the code must be systematic since the data block is what Alice and Bob have direct access to, albeit, with possible discrepancies. As previously noted, there is no channel per-se between Alice and Bob. We may view the discrepancy between their symbol sequences as having been caused by a fictitious Q-ary DMC;

- any systematic FEC generates coded symbols that need to be communicated across a classic public channel. We assume the encoding operation is performed at Alice while decoding is performed at Bob;

- most modern decoding techniques rely on the use of soft-information processing and this is what we shall assume as well. We have however, two separate channels that lead to two different soft metrics that would need to be combined in decoding. The fictitious channel between Alice and Bob is modeled as a Q-ary DMC, the real channel over which the coded symbols propagate is a public channel we assume to be Gaussian.

Given the previous considerations, an LDPC FEC code has been selected for this applications, given its attractive performances and the availability of low-complexity soft-decoding algorithms, as discussed in the previous chapters. As an initial simplified model we will consider a Q-ary DMC channel model (initially with $Q = 4$) as shown in Figure 6.4, with input alphabet $X = \{x_k\}_{k=1}^{Q} = \{00,01,10,11\}$ and output alphabet $Y = \{y_k\}_{k=1}^{Q} = \{00,01,10,11\}$. We associate a binary labeling to the Q transmitted symbols, and denote as p_i the probability of having i bit errors in one transmitted Q-ary symbol ($i = 1,2$), with the added hypothesis (justified by preliminary tests) that the probability of having one bit error per symbol is independent on the position of the error within the symbol. With reference to Figure 6.4 notice that, in the hypothesis of independent equally likely transmitted bits, the equivalent bit error probability (i.e. the equivalent Quantum Bit Error Rate - $QBER$) is

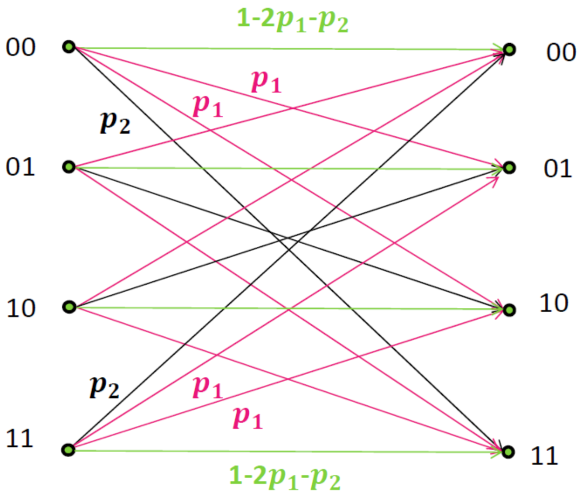


Figure 6.4: The considered Q-ary channel model ($Q = 4$).

$$QBER = P\left(biterror\right) = p_1 + p_2 \tag{6.6}$$

The Q-ary channel model in Figure 6.4 is used to transmit the k bits that compose the cryptographic key. After the transmission of the key, and once the presence of Eve has been excluded as described in Section 6.1, additional m redundancy bits are transmitted on a parallel ideal Binary Symmetric Channel (BSC), so that the k information bits together with the m redundancy bits represent a $n = k{+}m$ bits codeword of a rate $R_c = k/n$ code. Note that the above channel model is obtained from proper binning of the photon numbers at the transmitter and receiver (i.e., the intervals used to define the channel symbols at input and output can be adjusted to get the transition probabilities that adhere to the model above). At the receiver a soft metric LDPC decoder is employed, operating according to a belief propagation strategy, with input soft metrics from the Q-ary channel evaluated as:

$$LLR\left(y_k^i\right) = log\left(\frac{\sum_{x\in x(0)^i} P\left(y_k|x\right)}{\sum_{x\in x(1)^i} P\left(y_k|x\right)}\right) \tag{6.7}$$

where $LLR\left(y_k^i\right)$ is the Log Likelihood Ratio (LLR) of the i^{th} bit of the received symbol y_k and $x\left(\right)^i$ are the symbols of X whose i^{th} bit has weight w. Applying Equation 6.7 to our channel model we obtain

$$LLR\left(y_k^i\right) = \begin{cases} +log\left(\frac{1-p_1-p_2}{p_1+p_2}\right), & \text{if } y_k^i = 0 \\ -log\left(\frac{1-p_1-p_2}{p_1+p_2}\right), & \text{if } y_k^i = 1 \end{cases}$$

Chapter 7

Performance results

In this thesis we have considered optical communication scenarios where low number of photons are transmitted or detected. As described in the previous chapters these low photon number communication can include both QKD and weak energy optical communication.
Therefore, in this chapter, the novel protocol for information reconciliation in QKD, and error correction in the case of both QKD and weak energy optical communication are validated by means of intensive software simulations under well defined scenarios.

7.1 Simulations Setup

In order to exemplify the performances of capacity achieving iteratively soft decoded codes for the above mentioned applications, simulation results for the error rates achievable with LDPC code of various rates as a function of various system parameters, such as the quantum bit error rate $QBER$ and mean photon count N_c will be presented.

QKD: For QKD application we have used the composite channel, which comprises of a classical public channel and a private quantum channel as shown in Figure 7.1. The public channel will be modeled as an AWGN channel with a high signal-to-noise ratio (E_b/N_o)(since powerful coding is allowed on the public link and therefore possible errors on this channel may be considered extremely rare). For private channel we considered different secure quantum channels.
Furthermore, we assume that the information bits are transmitted on a private quantum channel modeled as in Figure 4.7, Figure 4.10 or Figure 6.4, while the additional redundancy bits are transmitted on a public channel, modelled as an Additive White Gaussian Noise (AWGN) channel, as shown in Figure 7.1. A block of n_q information bits plus the

corresponding r redundancy bits generate one codeword of a block FEC code with rate:

$$R_c = \frac{n_q}{n_q + r}$$

Weak Energy Optical Communication: For other low photon application we did the simulation only on the quantum channel of Figure 4.7 or Figure 4.10 because it does not need the parallel classical channel. In this case all the information and redundancy bits are transmitted on a single channel. For these applications we have conducted the simulation study using both LDPC and polar codes.
For the presentation of the simulation results, two figures will be used: the Bit Error Rate(BER)and the Frame Error Rate(FER). A single frame is equivalent to a decoded code block.

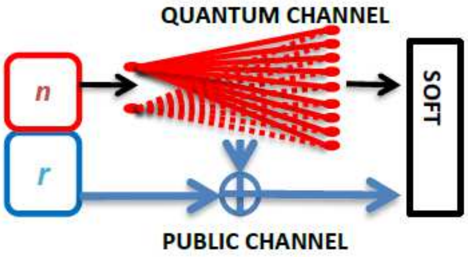


Figure 7.1: The composite channel (composed of the parallel secure and public channels) linking transmitter and receiver in QKD applications.

7.2 Performance Results for Weak Energy Optical Communication

In this section we will describe the performance results obtained through simulation of different quantum channel models using capacity achieving iteratively decoded channel codes, i.e., LDPC and polar codes. we used the channels as shown in Figure 4.7 and Figure 4.10. The LLR's which gives the soft information to the decoder for these channels were computed in channel chapter 4. The description of the codes used was given in chapter 3.

7.2.1 Performance with LDPC codes

First of all we would like to show the code gain that can be achieved by using error correcting codes as compared to the case when there is no coding, and the performance gain is clearly visible in Figure 7.2. Figure 7.3 depicts two sets of simulation results.

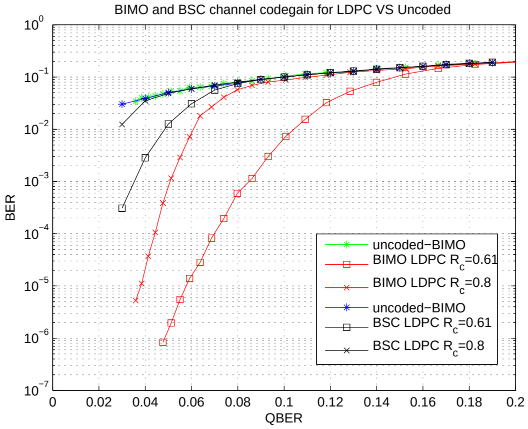


Figure 7.2: BER comparison for rate 0.61 LDPC(408,252) and rate 0.8 LDPC(1000,800) versus uncoded Quantum BSC and BIMO channels as a function of QBER

Each pair of curves is associated with a residual Bit Error Rate (BER) and Frame Error Rate (FER) curves. The LDPC code used for error correction is one with $n_q = 500$, $r = 500$ and code rate $R_c = 0.5$. The black pair (labeled "Q-BSC") is for quantum channel, modeled BSC with transition probability QBER. In this system, we assume the receiver does not to use the additional information derived from the knowledge of n_0 and n_1 , and we use as equivalent channel model, a simple Binary Symmetric Channel (BSC) with binary input X, binary output Y and cross-over probability QBER, (so that $P(Y = 0|X = 1) = P(Y = 1|X = 0) = QBER$), whose LLR values can be expressed as Equation 4.7. The red pair (curves labeled "Q-BIMO") is associated with the use of a quantum channel modeled as a BIMO DMC as shown in Figure 4.10 with equivalent un-coded bit error probability QBER and LLR metrics generated via photon counting according to Equation 4.17. Notice that for the "Q-BIMO" curves the QBER parameter is actually the cross-over probability of the equivalent BSC as defined in Equation 7.1 for the BIMO channel.

$$\begin{aligned} QBER &= \sum_{m=1}^{\inf} P(n_1 - n_0 = m|\phi_0) + \frac{1}{2}P(n_1 - n_0 = 0|\phi_0) \\ &= \sum_{m=1}^{\inf} P(n_1 - n_0 = -m|\phi_1) + \frac{1}{2}P(n_1 - n_0 = 0|\phi_1) \end{aligned} \tag{7.1}$$

As is evident from the results there is significant reduction in BER and FER. The Poisson channel with soft metric performs much better than BSC channel with no soft information. Figure 7.4 depicts three sets of simulation results. Each pair of curves is associated

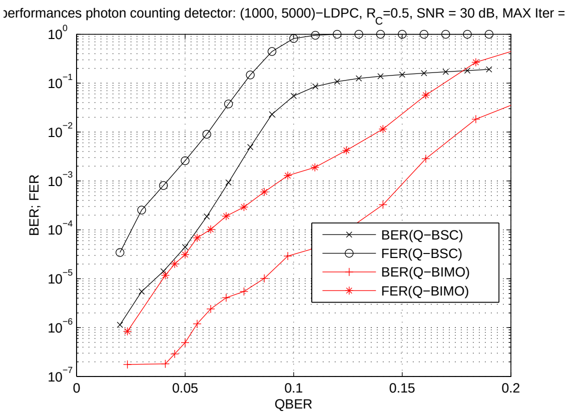


Figure 7.3: BER and FER performance of BSC and BIMO channels with LDPC code at rate 0.5.

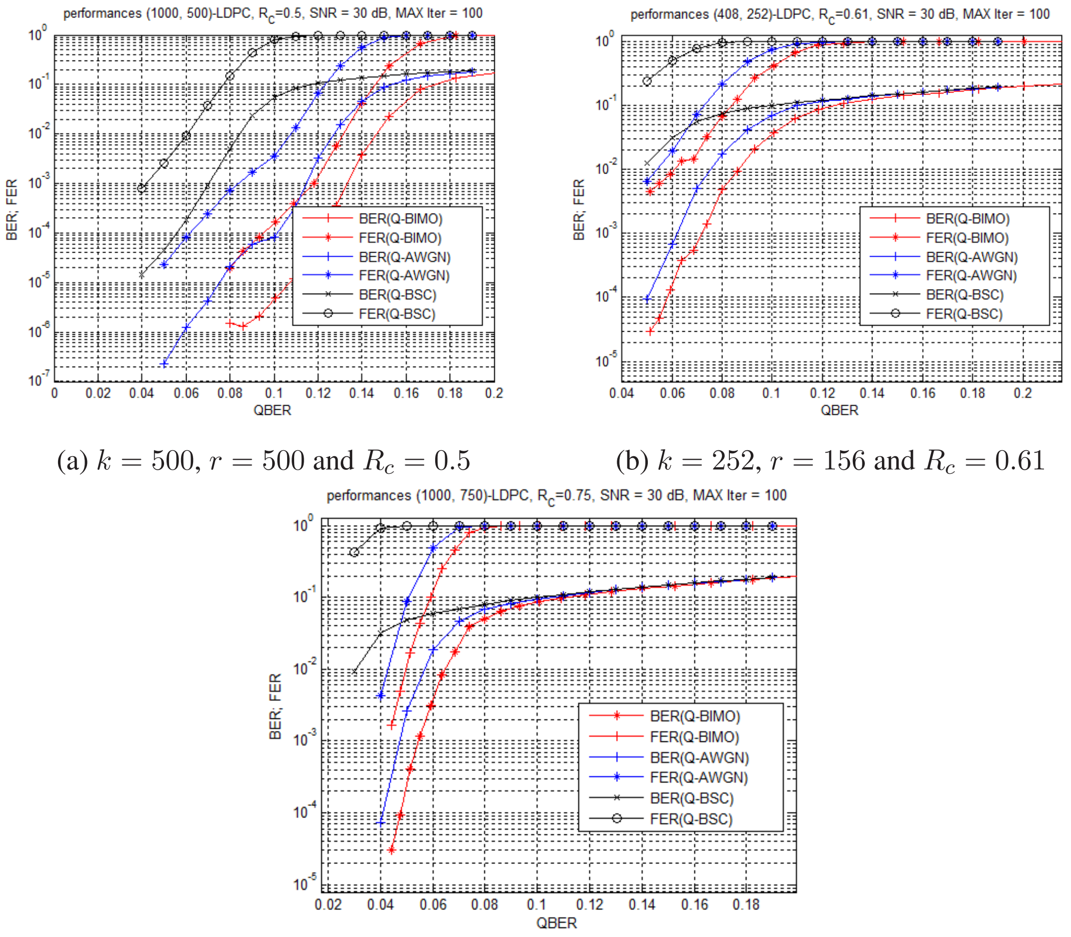
with residual Bit Error Rate (BER) and Frame Error Rate (FER) values after decoding. LDPC codes with the following parameters have been considered:

(a) $k = 500$, $r = 500$ and code rate $R_c = 0.5$,

(b) $k = 252$, $r = 156$ and code rate $R_c = 0.61$,

(c) $k = 750$, $r = 250$ and code rate $R_c = 0.75$.

Again here the black pair (labeled “Q-BSC”) is for the the quantum BSC channel and red pair (labeled “Q-BIMO”) is for BIMO DMC.
The blue curves represent the performance obtainable over a fictitious Additive White Gaussian Noise (AWGN) channel model with a Signal to Noise Ratio (SNR) that would yield the considered raw bit error probability QBER if a binary antipodal scheme were used for data transmission (curves labeled as “Q-AWGN”). As is evident from the results for the photon counting receiver, there is significant reduction in BER and FER values when using, the appropriate BIMO channel model and the associated LLR metrics derived in Equation 4.17 instead of the simpler BSC model (notice that the “Q-AWGN” curves have been only derived for reference, since with the small number of considered photons the AWGN channel model would not be appropriate).
The FER-BER performance show the improvement that can be achieved with the use of the BIMO channel model and the associated LLR metrics. For instance in Figure 7.4a at $QBER = 0.1$, there is more than three orders of magnitude improvement in BER and FER when comparing the proposed soft-metric processing versus the reference protocol whereby the quantum channel is a BSC. This is improvement in performance is the result of soft decoding instead of hard decoding, because the Q-BIMO channel model provide



(a) $k = 500$, $r = 500$ and $R_c = 0.5$

(b) $k = 252$, $r = 156$ and $R_c = 0.61$

(c) $k = 750$, $r = 250$ and $R_c = 0.75$

Figure 7.4: BER and FER simulation results for a LDPC code with a) $k = 500$,$r = 500$ and code rate $R_c = 0.5$, b) $k = 252$, $r = 156$ and code rate $R_c = 0.6$ 1and c) $k = 750$, $r = 250$ and code rate $R_c = 0.75$, obtained with different models of the quantum channel: BSC (Q-BSC curves), AWGN (Q-AWGN curves) and BIMO DMC (Q-BIMO curves)

the decoder with soft information, which is not available in the case of Q-BSC channel. Figure 7.4b and Figure 7.4c compare the FER-BER performance of the considered channel models and LLR values with LDPC codes with rates 0.61 and 0.75, respectively. It can be observed that a FER-BER improvement of up to several orders of magnitude can be obtained in these cases as well. It can also be observed that at higher code rate, the performances obtainable with the BIMO LLR soft-metrics gets closer to the performance of the classic AWGN channel metrics (although, as mentioned before, the AWGN model would not be applicable in the current case).

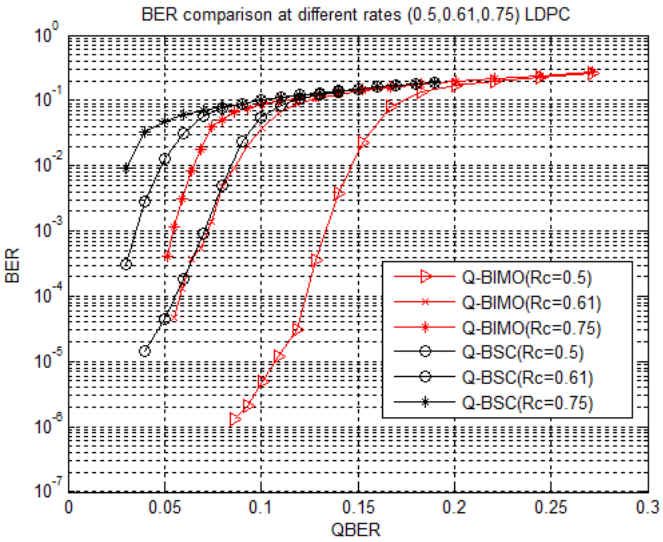


Figure 7.5: BER simulation results for a LDPC code with code rate $R_c = 0.5$,0.61 and 0.75 obtained with different models of the quantum channel: BSC (Q-BSC curves), and BIMO DMC (Q-BIMO curves)

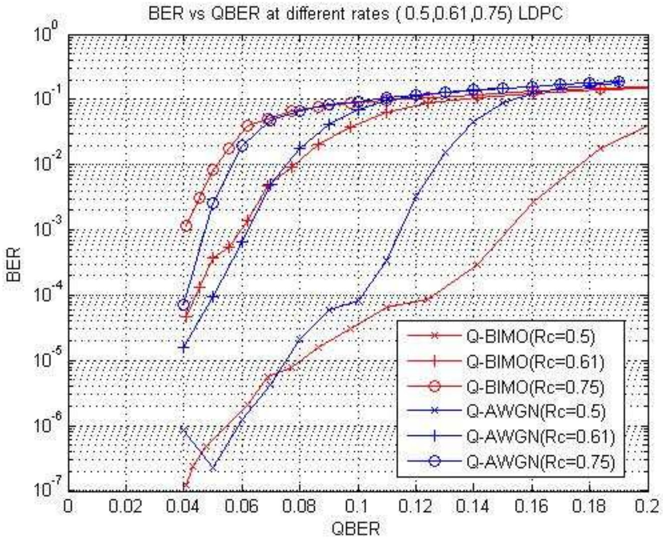


Figure 7.6: BER simulation results for a LDPC code with code rate $R_c = 0.5$,0.61 and 0.75 obtained with different models of the quantum channel:AWGN (Q-AWGN curves), and BIMO DMC (Q-BIMO curves)

Figure 7.5 compares the BER values obtained with the BSC and the BIMO channel models for different code rates, showing that as expected, for higher rates, a lower QBER

values is required before significant coding gains can be observed.
From Figure 7.6, we can observe that the BIMO channel can be approximated with an AWGN channel for high values of N_c, i.e. low values of QBER, while the AWGN model yields unreliable results with a low mean number of photons N_c, i.e. with high QBER. This effect is more evident with lower coding rates (as shown below, where the coding gain becomes apparent at low values of N_c).

7.2.2 Performance with Polar codes

We also did some performance analysis through the simulation of polar codes for various rates with block length $N = 1024$ for both BIMO and BSC channels. But here we will present the results obtained through simulating rate 0.7 polar code. And we will compare it to LDPC code with rate 0.75 and code length $N = 1000$.
Figure 7.7 shows the comparison of polar codes and LDPC codes for rate 0.7 using Q-BSC channel. We have plotted BER and block error rate (BLER) with respect to QBER. We can see that polar codes performs much better than LDPC on Q-BSC channel. Figure 7.8 shows the comparison of polar codes and LDPC codes for rate 0.7 using Q-BIMO channel. We have plotted BER and FER with respect to QBER. Here we can observe that LDPC codes performance is quite better than polar code. This may be because polar codes are channel specific codes and in the code construction process, we have design our polar codes for BSC channel and then we use Gausian Approximation (GA) technique for the construction of polar codes for BIMO channel using the same capacity as of BSC.

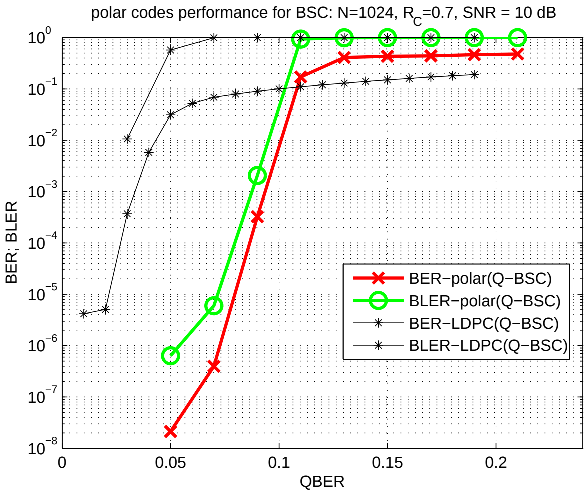


Figure 7.7: Polar codes vs LDPC for BSC at rate 0.7

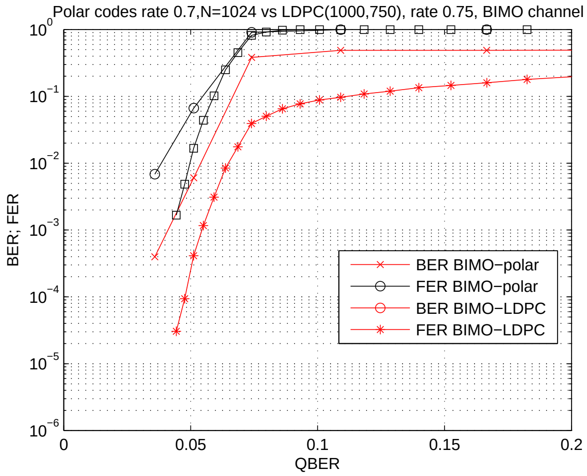


Figure 7.8: Polar codes vs LDPC for BIMO at rate 0.7

7.3 Performance Results for QKD

In this section we will describe the performance result obtained by using LDPC codes for the QKD protocol described in Section 4.The LDPC decoder uses belief propagation techniques, the values of the soft-metrics (LLRs) derived from the two sub-systems that form the composite communication channel, are calculated according to the schemes selected to model each one of them. The bit values and the LLRs values after the quantum and the classical transmission should be passed as an input to the decoder. The number of iterations for decoding can be selected as well as the minimum number of errors the user intends to correct. The parity matrix of the LDPC code used in the simulations is chosen from a set of suggested codes.

In Figure 7.9, the performance of two LDPC codes with rates 0.5 and 0.61 are shown and compared. we can see that by increasing the code rate BER performances becomes worst, that is because more information travels on the quantum channel which has high bit error rate. On the others side the security of QKD increases, since a lower fraction of bits are revealed on the classic public channel. This results leads us to the conclusion that we need to use higher rate codes in order to make the QKD protocol more secure. For this purpose we have done simulation with different high rate codes.

We did the performance analysis of soft metric based QKD protocol using higher rates codes i.e., LDPC code with rate 0.61 and 0.75 for the composite QKD channel, where for private channel we used three types of quantum channels: BSC,AWGN and BIMO, the results are depicted in Figure 7.10 and Figure 7.11.

It is clear from both of these figures that even in the case of QKD, the soft decoding because of the soft information that photon counting detectors provide, improves the performance. We can see that the BER and FER is much better for Q-BIMO curves (red)

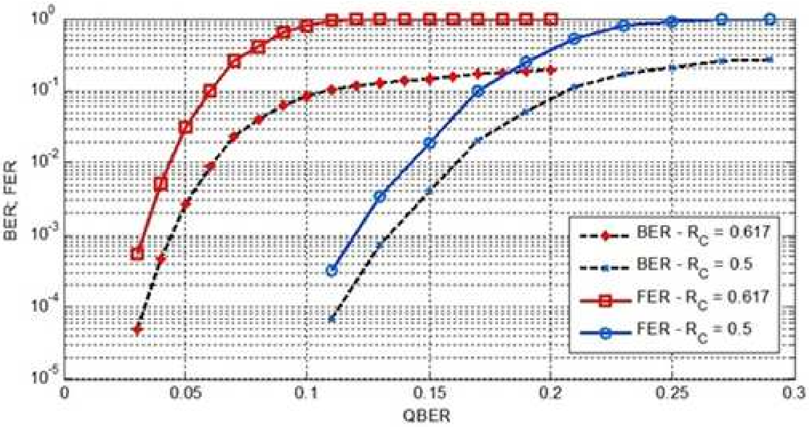


Figure 7.9: BER and FER performance of two LDPC codes with block length $n = 504$ and $R_c = 0.5$ and $n = 408$ and $R_c = 0.61$, respectively, as a function of the private channel QBER.

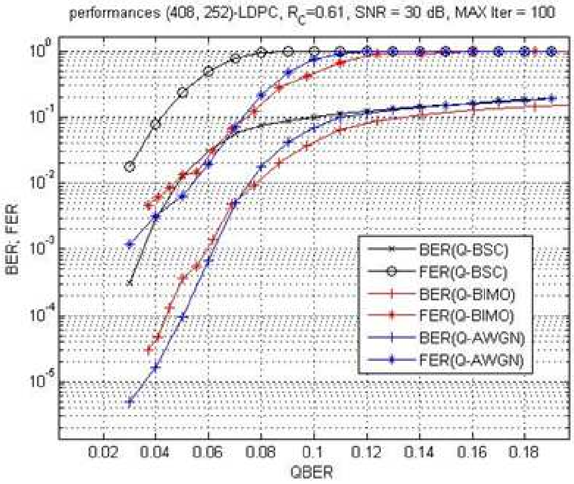


Figure 7.10: BER and FER performance of LDPC codes with block length $n = 408$ and $R_c = 0.61$, respectively, as a function of the private channel QBER, obtained with different models of the quantum channel: BSC (Q-BSC curves), AWGN (Q-AWGN curves) and BIMO DMC (Q-BIMO curves).

than Q-BSC curves (black).

Figure 7.12 shows the residual BER on the BIMO channel for different values of mean photon count N_c. The fact is that as N_c increases QBER decreases and vice versa. so, as the mean photon count increases the performance improves.

All of the above results were based on the use of 2 level quantum system (i.e., Qubits).

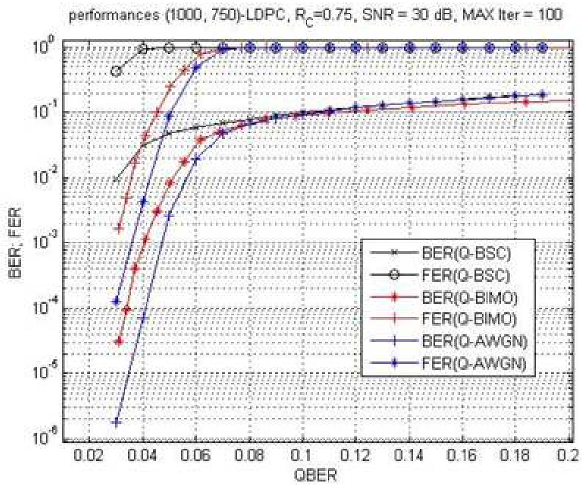


Figure 7.11: BER and FER performance of LDPC codes with block length $n = 1000$,$n_q = 750$and $R_c = 0.75$, respectively, as a function of the private channel QBER, obtained with different models of the quantum channel: BSC (Q-BSC curves), AWGN (Q-AWGN curves) and BIMO DMC (Q-BIMO curves

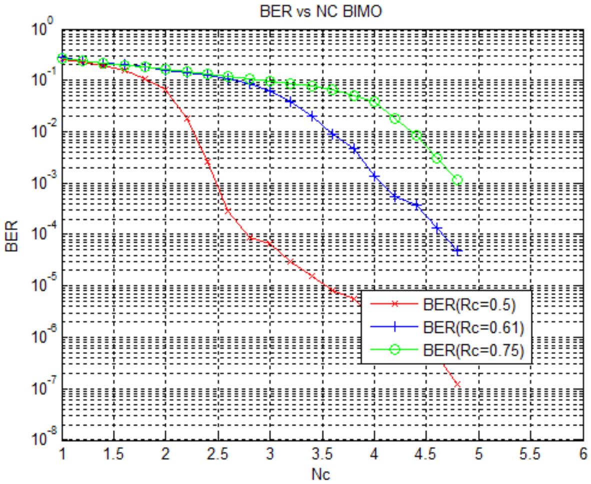


Figure 7.12: BER simulation results for a LDPC code with code rate Rc = 0.5,0.61 and 0.75 obtained with BIMO channel for different values of Nc

Multilevel quantum system (i.e., Qudits) were also considered and an example of 4 level system as shown in Section 6.3 Figure 6.4 was simulated.

A rate 0.8 (1000,800) LDPC code has been applied to perform IR on the scheme described in Section 6.3 selecting, for the same overall QBER, different values of p_1

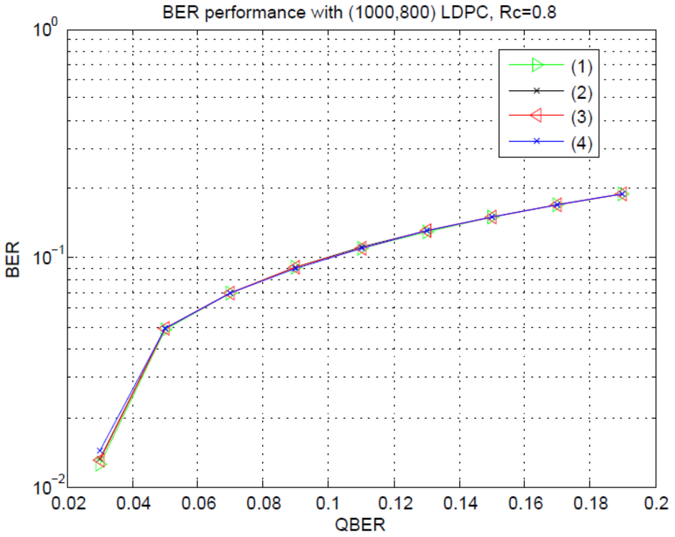


Figure 7.13: BER performances of a $(1000{,}800)$ binary LDPC over the Q-ary channel in Figure 6.4 for (2) $p_1 = (QBER)^2$, (3) $p_1 = (QBER)^2/2$ and (4) $p_1 = QBER/2$ as a function of QBER, compared with (1) a BSC with transition probability QBER. In (2), (3) and (4) $p_2 = QBER - p_1$.

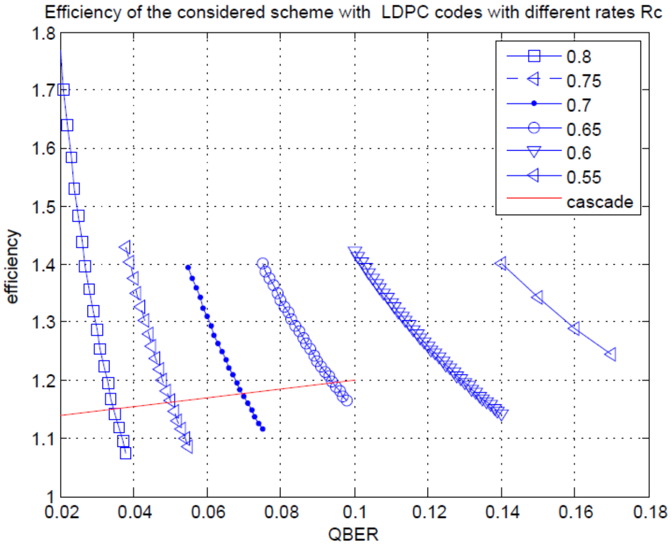


Figure 7.14: Efficiency with LDPC codes for different coding rates. The red continuous line is a graphical lower bound of the efficiency of the CASCADE IR algorithm.

and p_2 . The decoded Bit Error Rate (BER) performances shown in Figure 7.13 have been obtained by Montecarlo simulation, showing that the decoded BER depends on the overall QBER value and not on how the error probability is distributed on the first and second bit of the Q-ary channel. This proves, in practice, that with the considered binary FEC LDPC codes the use of a Q-ary channel is equivalent to $log_2(Q)$ successive uses of a BSC with the same value of QBER.
LDPC codes with different rates have then been simulated, obtaining the efficiency of the considered information reconciliation scheme. The efficiency, defined as [64]

$$\epsilon = \frac{1 - R_c}{H(X|Y)} = \frac{1 - R_c}{R_c H_2(QBER)} \tag{7.2}$$

is shown in Figure 7.14, where the considered codeword lengths n are always smaller or equal to 1000. It can be noticed that the proposed scheme allows to achieve efficiency values better than the CASCADE algorithm with reasonable complexities, proving the effectiveness of the proposed scheme.

Chapter 8

Conclusion

In this thesis we have considered the applications of Optical/Quantum communication where low number of photons are used. For these kind of applications the receiver sensitivity is very important in order to decode the information bit. single photon detectors technology is the underlying technology for these applications, which offers the required sensitivity. These application may include Quantum key distribution (QKD), quantum communication under extreme(stressed) environment and Low probability of intercept optical communication. For all these applications the use of photons(light) have been considered because of its underlying advantages.

In any Quantum Key Distribution system, Alice and Bob may use one of two types of reconciliation, in order to preserve the integrity and security of their keys. The first type is interactive reconciliation, which consists of two-way interaction between Alice and Bob over a public classical channel for the detection and correction of errors. The second type of interaction is one-way reconciliation in which a decision is made beforehand regarding how errors are detected and corrected. Considering the fact that, one-way protocols, by their nature, tend to reveal less information over the public channel than interactive protocols where possibly many messages are openly passed back and forth, in this work a novel information reconciliation and data sifting protocol has been proposed, which uses Forward Error Correction (FEC), minimizing the exchange of information related to the secret key that needs to be sent back and forth using the public channel. This protocol, is based on soft decoding of LDPC codes with mixed-metric inputs, where the information derived from a private quantum channel and a classic public channel are jointly used for decoding. The performance of the proposed methods has been studied by simulation, and the effects of the various system parameters have been considered.

The suggested algorithms can be applied to QKD schemes based both on Single Photon or WLP sources, with or without decoy states. The difference among the different schemes is the use of different channel metrics. However, independently from the scheme used, the protocol allows both parties involved in a quantum key distribution to identify a sifted secret key with minimum information exchange and reduced computational costs.

Specifically, in this thesis, the gains that can be achieved in the secret key rates of a QKD protocol and the performance improvement in other low photon communication scenarios, from the use of more advanced receivers employing photon counting detectors have been explored, motivated by the fact that the the presence of such detectors allows for the generation of soft-metrics at the receiver. Within the context of this system, a multi-level quantum channel BIMO Quantum-DMC has been identified and the evaluation of its theoretical capacity bound has been calculated.

The BIMO Quantum-DMC offered a capacity improvement over the equivalent BSC quantum channel (leading to a BER improvement when comparing the two channel in presence of an error correction code), translating in a significant reduction of the values of the BER and FER for several QBER values; meaning that a significant larger portion of the data after the stages of sifting and reconciliation may be kept There has been much interest in quantum key distribution.

Experimentally, quantum key distribution over 150 km of commercial Telecom fibers and over 144 km in atmosphere has been successfully performed. The crucial issues in quantum key distribution are the security and the key rate. All recent experiments are, in principle, insecure due to real-life imperfections. However with the use of methods like decoy states, it is possible to make most of those experiments by using essentially the same set-up. Since the security aspect seems to be improved by the use of such methods, it is becoming more and more important to obtain elevated key rates from QKD systems to keep up with the high rates of practically any telecommunication system, this way secure data transmission may be guarantee by using one time pad encryption algorithms.For this reason we have use high rate code and obtained the performance in terms of such codes.

This thesis also offers a preliminary investigation on the use of FEC LDPC codes for information reconciliation when the underlying channel is a Q-ary DMC, for QKD applications based on higher photon flux levels with spatial entanglement of twin beams in PDC, and shows that acceptable error reconciliation efficiency values are obtained with reasonable complexity.

Polar codes have been designed and used for error correction of both single photon communication(Quantum-BSC) and WLP communication(BIMO Quantum-DMC) channels with the use of soft decoding. And its performance have been reported.

In general, the availability of the soft-metric allows for the use of advanced iterative soft-decoding techniques during the information reconciliation phase, significantly reducing the residual bit and frame error rates with subsequent impact on the achievable secret key rates which is, as said before, is one of the fundamental performance guideline in QKD. The proposed protocol, while having a negligible cost, can reduce the residual FER in QKD systems, largely reducing the interaction required between the two parties involved, increasing the key rate and protecting the secrecy of the information exchanged

Bibliography

[1] "The rise of photonics", *Tech Trend Notes*, 1992;1(2):15-16.

[2] MIT Lincoln laboratory "Forecasting single-photon detector technology", *The Next wave*, vol.20 No.1. 2013

[3] P.A.Hiskett, D.Rosenberg, C.G.Peterson, R.J.Hughes, S.Nam, A.E.Lita, A.J.Miller and J.E.Nordholt, "Long-distance quantum key distribution in optical fibre", *New Journal of Physics* , 8 193 (2006).

[4] T. Schmitt-Manderbach, and et al, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km", *Physical Review Letters,* vol. 98, no. 1, pp. 1-4, 2007.

[5] R. Ursin, and et al "Entanglement-based quantum communication over 144 km", *Nature Physics,* vol. 3, no. 7, pp. 481-486, 2007.

[6] Proakis, John "Digital communications(4th edition)", *McGraw Hill,* pp. 457-460. ISBN 0-07-118183-0, 2001

[7] Markus Aspelmeyer, Thomas Jennewein, Anton Zeilinger, Martin Pfennigbauer and Walter Leeb "Long-Distance Quantum Communication with Entangled Photons using Satellites" *IEEE Journal of Selected Topics in Quantum Electronics, special issue on "Quantum Internet Technologies"* arXiv:quant-ph/0305105

[8] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Phys. Rev.A* vol. 65, p. 52310, 2002

[9] M.Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""Event-ready-detectors" Bell experiment via entanglement swapping," *Phys. Rev. Lett.* vol. 71, no. 26, pp.4287-4290, 1993.

[10] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers,* vol. XLV, no. 55, pp. 295-301, 1926.

[11] C. E. Shannon, "Communication theory of secrecy systems," *MD computing computers in medical practice,* vol. 28, no. 1, pp. 656-715, 1949.

[12] Ayushi, "A Symmetric Key Cryptographic Algorithm, " *International Journal of Computer Applications,* Vol. 1, No. 15, pp. 0975 - 8887, 2010.

[13] W. Diffie and M. Hellman, "New directions in cryptography, " *IEEE Transactions on Information Theory,* vol. 22, no. 6, pp. 644-654, 1976.

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21,no. 2, pp. 120-126, 1978.

[15] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science,* vol. 35, pp. 124-134, 1994.

[16] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance.," *Nature,* vol. 414, no. 6866, pp. 883-887, 2001.

[17] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* vol. 175, pp. 175-179. Bangalore, India, 1984.

[18] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information.* No. ISBN: 978-3-540-66778-0, Springer, 2000.

[19] H.-K. Lo, T. Spiller, and S. Popescu, *Introduction to Quantum Computation and Information,* vol. 399. World Scientific, 1998.

[20] N. Ilic, "The Ekert Protocol", *Quantum,* 1991.

[21] M. L. Bellac, "A Short Introduction to Quantum Information and Quantum Computation,", *Cambridge University Press,* vol. 60. 2006.

[22] V. Scarani, "Quantum Physics A First Encounter: Interference, Entanglement, and Reality.", *Oxford: Oxford Univ. Press,* 2006.

[23] M. Dusek, N. Lutkenhaus, and M. Hendrych, "Quantum cryptography,", *Progress in Optics,* vol. 18, no. 8, p. 51, 2006.

[24] H.-K. Lo and Y. Zhao, "Quantum cryptography,", *Encyclopedia of Complexity and Systems Science,* vol. 8, p. 7265, 2009.

[25] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography,", *Reviews of Modern Physics,* vol. 74, no. 1, pp. 145-195, 2002.

[26] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal,* vol. 27, pp. 379-423, 1948

[27] T. J. Richardson and R.L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform.Theory,* vol. 47, No.2, pp. 599-618, Feb. 2001

[28] A. Shokrollahi, "Design of capacity-approaching low density parity-check codes," *IEEE Trans. Inform.Theory,* vol. 47, No. 2, pp. 618-637, Feb. 2001

[29] S.-Y. Chung, T. J. Richardson, R.L. Urbanke, "Analysis of sum-product decoding of low-density," *IEEE Trans. Inform.Theory,* Vol 47, No. 2, pp. 637-657, Feb. 2001

[30] E. Arkan, "Channel Polarization: A Method for Construc ting Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Trans. Inf. Theory, vol. 55, no. 7, pp. 3051-3073, Jul. 2009.*

[31] S. H. Hassani, S. B. Korada, and R. Urbanke, "The Compound Capacity of Polar Codes," Proceedings of Allerton Conference on Communication, Control and Computing, Allerton, Sep. 2009.

[32] K. Chen, K. Niu, and J. R. Lin, “List successive cancellation decoding of polar codes,” *Electronics Letters, vol. 48, no. 9, pp. 500-501, 2012.*

[33] S. Olivares, M. G. A. Paris, M. Delgado, and M. Mondin, “Toward a soft output quantum channel via Bayesian estimation”, 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), *pp.1-2, Nov.7-10, 2010.*

[34] Teklu, B., Olivares S. and Paris, M. G. A., “Bayesian estimation of one-parameter qubit gates”, J. Phys. B: At. Mol. Opt. Phys. *42, (2009).*

[35] R. S. Kennedy, Research Laboratory of Electronics, MIT, Quarterly Progress Report No. 108, 1973, p. 219 (unpublished).

[36] S. J. Dolinar, Jr., “An Optimum Receiver for the Binary Coherent State Quantum Channel”, *MIT Research Laboratory of Electronics Quarterly Progress Report 111, Cambridge, Massachusetts,* pp. 115-120, October 15, 1973.

[37] M. Sasaki and O. Hirota, *Phys. Rev. A 54, 272 (1996).*

[38] S. Olivares et al., J. Opt. B: Quantum Semiclass. Opt. 6, 69 (2004).

[39] J. M. Geremia, *Phys. Rev. A 70, 062303 (2004).*

[40] M. Takeoka, M. Sasaki, P. van Loock, and N. Lutkenhaus, Phys. Rev. A 71, 022318 (2005).

[41] C.-W. Lau, V. A. Vilnrotter, S. Dolinar, J. M. Geremia, and H. Mabuchi, *IPN Progress Report 42-165, 1 (2006).*

[42] R. L. Cook, P. J. Martin, and J. M. Geremia, Nature, *466, 774 (2007).*

[43] C. Wittmann, U. L. Andersen, M. Takeoka, D. Sych, and G. Leuchs, Phys. Rev. A *81, 062338 (2010).*

[44] D. Brivio, S.Cialdi, S. Vezzoli, B. Teklu, M. G. Genoni, S. Olivares, and M. G. A. Paris, Phys. Rev. A 81, 012305 (2010).

[45] G. Zambra, A. Allevi, M. Bondani, A. Andreoni, and M. G. A. Paris, *Int. J. Quantum Inf.* 5, 305 (2007).

[46] A. Allevi, S. Olivares, and M. Bondani , *Opt. Express 20, 24850 (2012).*

[47] H.-K. Lo, and J. Preskill, CALT-68-2556 e-print arXiv:quant-ph/0504209v1 (2005).

[48] M. Curty, X. Ma, B. Qi, and T. Moroder, *Phys. Rev. A 81, 022310 (2010).*

[49] Mondin M., Delgado M., Mesiti F., Daneshgaran F., “Soft-processing for Information Reconciliation in QKD Applications,” International Journal of Quantum Information, vol. 9, pp. 155-164, 2011.

[50] A. Nakassis, “Expeditious reconciliation for practical quantum key distribution,”, *Proceedings of SPIE, vol. 5436, pp. 28-35, 2004.*

[51] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” Advances, vol. 765, pp. 410-423, 1994.

[52] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *Journal of Cryptology, vol. 5, no. 1, pp. 328, 1992.*

[53] J. Martinez-Mateo, D. Elkouss, V. Martin, “Blind Reconciliation”, Quantum Information and Computation, Rinton Press, 2003.

[54] D. Pearson, “High-speed QKD Reconciliation using Forward Error Correction”, *in 7th International Conference on Quantum Communication, Measurement and Computing, Vol. 734, pp. 299-302, 2004.*

[55] D. Elkouss, A. Leverrier, R. Allaume, and J. Boutros, “Efficient reconciliation protocol for discrete-variable quantum key distribution,” IEEE International Symposium on Information Theory, no. 1, pp. 1879-1883, 2009.

[56] M. Mondin, F. Daneshgaran, M. T. Delgado, F. Mesiti, “Soft-metric-based information reconciliation techniques for QKD”, *in SPIE Optics + Photonics 2010, San Diego, USA, Aug 1, 2010 to Aug 5, 2010.*

[57] D. Slepian and J. Wolf, “Noiseless coding of correlated information sources,” IEEE Transactions on Information Theory, vol. 19, no. 4, pp. 471-480, 1973.

[58] M. Mondin, F. Daneshgaran, M. Delgado, and F. Mesiti, “Novel Techniques for Information Reconciliation, Quantum Channel Probing and Link Design for Quantum Key Distribution”, *Proc. of PSATS10, Rome, Italy, February 4-6, 2010.*

[59] I. P. Degiovanni, M. Genovese, M.Gramegna, A. Avella, G. Brida, and P. Traina. Phys. Rev. A, *82:062309, 2010.*

[60] M. Genovese, Brida and I. Ruo Berchera. Nature Photonics, *4:227, 2010.*

[61] I. P. Degiovanni M. Genovese P. Traina G. Brida, A. Cavanna. Laser Physics Letters, *9:247, 2012.*

[62] M. Genovese M. L. Rastello I. Ruo-Berchera G. Brida, Ivo P. Degiovanni. Opt. Exp., *18:20572, 2010.*

[63] A. Gatti M.Genovese A.Meda I.Ruo-Berchera G.Brida, L. Caspani. Phys. Rev. Lett., *102:213602, 2009.*

[64] V. Martin J. Martinez-Mateo, D. Elkouss. Quantum Information and Computation, *12:0791-0812, 2012.*