UNIVERSITÀ POLITECNICA DELLE MARCHE

Dipartimento di Ingegneria dell'Informazione

Ph.D. Course in Information Engineering
Curriculum in Biomedical, Electronics and Telecommunications Engineering

Modern coding techniques for reliable and secure communications

Candidate:
Giacomo Ricciutelli

Supervisor:
Prof. Franco Chiaraluce

Co-supervisor:
Dr. Marco Baldi

A.A. 2016/2017

To my wife Lucia and daughter Martina
To my family and friends

Abstract

Nowadays, wireless communications are involved in many applications and the security and reliability targets are increasingly growing. Hence, based on modern coding schemes, in this thesis new solutions able to achieve more and more satisfactory performance are proposed. In particular, we adopt Low Density Parity Check (LDPC) codes and Polar Codes. Due to the versatility of LDPC codes, we use this codes family for both reliability and security scopes. A wire-tap channel is characterized by an eavesdropper that tries to decode the information sent among authorized receivers. In this scenario, by following the physical layer security approach, first we investigate the eavesdropper's equivocation rate achieved through practical LDPC schemes. Then, by generalizing this model with a broadcast channel with confidential messages, we design LDPC codes with unequal error protection capabilities that improve the privacy of data.

Instead, for reliability purposes, we use LDPC codes over a non-conventional satellite channel like the one affected by solar scintillation. In this context, the noise introduced by physical phenomena may lead to a low quality in the communication. Hence, by mitigating the performance degradation, in this thesis we propose coding schemes that improve the link reliability. Finally, we study communication systems based on the transmission of short blocks. In this case we use Polar codes since they are one of the most prominent codes family proposed for this scenario. However, in the short packet length regime Polar codes may have poor performance. To overcome this issue, a concatenation with a cyclic code was proposed in the literature. Concatenated Polar codes are competitive in this context and therefore they are recommended in the new generation of mobile systems (5G). Thus, we study the structure of these concatenated schemes from a distance spectrum point of view and propose some solutions able to further improve the reliability of communication.

Foreword

During my period at Dipartimento di Ingegneria dell'Informazione of Universitá Politecnica delle Marche as Ph.D. student, I had the pleasure to work with the research group leaded by Prof. Franco Chiaraluce and Dr. Marco Baldi.

In our work we have studied new approaches able to increase security and reliability in communication systems. Nowadays the need of confidential and reliable communications is increasingly required and our team dealt these issues by exploiting error correcting coding techniques, that play an important role in such contexts.

During these years I had the possibility to collaborate with very important international organizations as the German Aerospace Center (DLR). In particular, I spent three months at Institute of Communications and Navigation of the DLR center in Wessling, where part of this thesis was developed with the Information Transmission group leaded by Dr. Gianluigi Liva.

I had also the possibility to participate to two European Space Agency (ESA) research projects. The first one was entitled Reliable TT-C during supErior Solar conjUnctions (RESCUe) (ESA Contract NO. 4000112987/14/F/MOS). While the second one, that is still in progress, is entitled PROTotype of Off-line COrreLator for Arraying of large Aperture Antennas (PROTOCOL-A.3) (ESA Contract NO. AO/1−8456/15/D/AH).

The contents of this thesis have been partially included in the following publications.

- **G. Ricciutelli**, M. Baldi, F. Chiaraluce, G. Liva, "On the Error Probability of Short Concatenated Polar and Cyclic Codes with Interleaving", Proc. IEEE International Symposium on Information Theory (ISIT), pp. 1858-1862, Aachen, Germany, June 2017, DOI: 10.1109/ISIT.2017.8006851.

- M. Baldi, N. Maturo, **G. Ricciutelli**, F. Chiaraluce; "Security gap analysis of some LDPC coded transmission schemes over the flat and fast fading Gaussian wire-tap channels", EURASIP Journal on Wireless Communications and Networking 2015, vol. 2015, no. 1, pp. 232-244, Oct. 2015, DOI 10.1186/s13638-015-0463-6

- M. Baldi, **G. Ricciutelli**, N. Maturo and F. Chiaraluce, “Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel”, IEEE International Conference on Communications 2015 Workshop on Wireless Physical Layer Security (ICCWS 2015), pp. 435-440, London, UK, June 2015, DOI: 10.1109/ICCW.2015.7247218.

- **G. Ricciutelli**, M. Baldi, N. Maturo and F. Chiaraluce, “LDPC Coded Modulation Schemes with Largely Unequal Error Protection”, IEEE International Black Sea Conference on Communication and Networking (BlackSeaCom 2015), pp. 48-52, Constanta, Romania, May 2015, DOI: 10.1109/BlackSeaCom.2015.7185084, **Awarded as the best student paper of the Conference**.

- M. Baldi, N. Maturo, **G. Ricciutelli** and F. Chiaraluce, “Practical LDPC coded modulation schemes for the fading broadcast channel with confidential messages”, IEEE International Conference on Communications Workshop on Wireless Physical Layer Security (ICCW 2014), pp. 759-764, Sydney, Australia, June 2014, DOI: 10.1109/ICCW.2014.6881291.

- M. Baldi, N. Maturo, **G. Ricciutelli** and F. Chiaraluce, “LDPC coded transmissions over the Gaussian broadcast channel with confidential messages”, IEEE 21st International Conference on Telecommunications (ICT 2014), pp. 52-56, Lisbon, Portugal, May 2014, DOI: 10.1109/ICT.2014.6845079.

At the end of this thesis the full list of publications concerning also other research topics studied during my Ph.D. course is provided.

Contents

List of Figures

List of Tables

List of abbreviations

FP Fading Period.

AONT all-or-nothing transform.

AR4JA Accumulate, Repeat-by-4, and Jagged Accumulate.

AWEF average weight enumerating function.

AWGN Additive White Gaussian Noise.

BCC broadcast channel with confidential messages.

BCH Bose-Chaudhuri-Hocquenghem.

BEC binary erasure channel.

BEP block error probability.

BER bit error rate.

BI-DMS binary-input discrete memoryless symmetric.

BLER block error rate.

BPSK binary phase shift keying.

CC convolutional code.

CCSDS Consultative Committee for Space Data Systems.

CER codeword error rate.

CRC cyclic redundancy check.

CSI channel state information.

DE Density Evolution.

DPSK differential phase-shift keying.

DVB-S Digital Video Broadcasting - Satellite.

DVB-T Digital Video Broadcasting - Terrestrial.

ELRL Extremely (or “Ergodic”) low rate links.

ESA European Space Agency.

FER frame error rate.

FSK frequency-shift keying.

HRL High rate links.

IoT Internet of Things.

IOWEF input output weight enumerating function.

IRWEF input redundancy weight enumerating function.

LDPC low-density parity-check.

LLR log likelihood ratio.

LLR-SPA log-likelihood ratio sum product algorithm.

LRL Low rate links.

MDS maximum distance separable.

MIMO multiple-input multiple-output.

ML maximum likelihood.

MRL Medium rate links.

NASA National Aeronautics and Space Administration.

NMS normalized min-sum.

PC protection class.

PCTC parallel concatenated turbo code.

PEG Progressive Edge Growth.

PLS physical layer security.

PSK phase shift keying.

QAM quadrature amplitude modulation.

QSFC quasi-static fading channel.

RM Reed-Muller.

RS Reed-Solomon.

SC successive cancellation.

SEP Sun-Earth-Probe.

SNR signal-to-noise ratio.

STEREO Solar TErrestrial RElations Observatory.

TC telecommand.

TM telemetry.

UB union bound.

UEP unequal error protection.

WEF weight enumerating function.

Chapter 1

Introduction

Due to their versatility and ease of use, in the last few years wireless networks have become the system mainly used from people to have access to Internet or to share, store and send/receive data. Thus, the targets in terms of *reliability* and *security* of these networks are constantly growing. The former aspect concerns the possibility of improving the system performance in terms of quality of the link. While, the latter is referred to the capability of sending private information in a secure way. Therefore, in this thesis we aim to propose some solutions able to increase the reliability and security in wireless communications. Clearly, these issues are often overlapped, since in some cases a better error rate performance is needed to increase the security level.

We study these problems from the error correcting codes point of view. Since the '50s of the last century, when Shannon provided the bases of the information theory, coding schemes have been increasingly adopted to correct the errors occurred during the transmission. Thus, by adopting coding, the reliability of the communication improves. For this reason, one (or more) coding scheme is recommended in many services, e.g., satellite communications, Digital Video Broadcasting - Satellite (DVB-S), Digital Video Broadcasting - Terrestrial (DVB-T), mobile networks, Wi-Fi, etc... We consider *modern* code families, i.e., those that are the state of the art in the considered scenarios. The name *modern*, also reported in the title of the thesis, clearly suggests that the selected coding schemes are those most recently proposed. In some ways this is a correct observation, however the appellative *modern* indicates that the used codes are those currently adopted in the contexts of interest. In particular, we refer to polar and low-density parity-check (LDPC) codes. Due to the powerful performance of these codes, they are candidate to be used for future applications in the contexts here discussed. Also in this sense the name *modern* is justified.

Part of this work is focused on short packet transmission in a wireless network. This scenario is of interest for many wireless applications. For example, concatenated polar codes are recommended for the next generation of mobile systems (5G) for the medium/short packets length transmission [1]. In this case, a polar code concatenated with an outer cyclic redundancy check (CRC) code is considered. We study these schemes from a distance spectrum point of view. We provide bounds on the achievable error rate over a binary erasure channel (BEC). Moreover, we show as the introduction of an interleaver between the component codes can further improve the performance of these schemes at short block length. Obviously, our results are interesting for any short packets communication system, as for example Internet of Things (IoT), and not only limited to the 5G.

As mentioned, coding was proposed to correct most of the errors introduced by the transmission channel. We put under strain this capability of coding schemes, by considering a very noisy channel. In fact, we evaluate the performance achieved by error correcting codes in satellite communications whose channel is affected by solar scintillation. In this link the physical phenomena on the Sun corrupt the communication between the probe and the ground station. We show as LDPC codes improve the reliability of this system and we compare their performance with those of other classical coding schemes. We consider that the fading affects both amplitude and phase of the signal. The performance achieved with non conventional modulation, as frequency-shift keying (FSK), are also investigated.

In a wireless scenario, coding schemes can be also adopted to protect private data. Indeed, due to their broadcast nature and great amount of sensitive information sent over them, wireless networks are vulnerable to eavesdropping attacks. Traditionally, to avoid these problems, a cryptographic algorithm at the higher layers of the protocol stack is used. The security in the currently cryptographic primitives is mainly due to mathematical problems with hard numerical solutions (e.g., primitive roots, discrete logarithms, etc...). Moreover, in most cases, among the authorized users a pre-shared key is needed. Hence, some problems on the keys exchange may occur. Furthermore, due to the rapid evanescence of the technology, the cryptographic methods are exposed to risks of successful attacks, since the eavesdropper computing capabilities are continuously growing. This is, for example, the case of post-quantum scenarios, where the existing cryptographic solutions will be broken in a very short time. To overcome all these issues, a primary level of security can be already introduced at the physical layer. We refer to the so called physical layer security (PLS) approach. In this case, the secrecy of the information is achieved by exploiting the random nature of the physical channel. In fact, by using coding and signal processing, the physical characteristics of the wireless channel can be used to allow a successful decoding only for the authorized receiver. Hence, PLS is a breakthrough in communications security paradigms, since it allows to achieve secure transmissions without the need of any form of pre-shared secret (like cryptographic keys) within the group of legitimate users and it does not rely on the computational resources of the attacker. As channel models, we consider the wire-tap [2] and the broadcast channel with confidential messages (BCC) [3]. In the latter, to achieve the goals in terms of reliability and security, the data must be differently protected.

Thus, we design LDPC codes with unequal error protection (UEP) capabilities. Commonly, to assess the obtained security level, information theoretic metrics are used. Nevertheless, such metrics consider an asymptotic performance achieved by codes with infinite length. Obviously, this is not a realistic hypothesis in practical scenarios, as those considered in this work. Therefore, we use two metrics, namely, security gap and eavesdropper equivocation rate, that allow us to evaluate the security level achieved by finite length error correcting codes.

1.1 Outline of the thesis

The document is organized as follows.

Chapter 2
In Ch. 2 the rationale of this thesis and the basic notions on the considered error correcting codes are described. Moreover, in this chapter we introduce the grounds on the use of PLS techniques, by underlining as they can be adopted together with classical cryptographic primitives to improve the security of the communication.

Chapter 3
Chapter 3 contains the discussion on the considered channel models and security metrics. Hence, the wire-tap channel and the BCC model are introduced. Over the latter, to achieve a feasible system, different sensitivities to errors for the authorized and unauthorized receiver are needed. Thus, in this chapter we have also presented the concept of UEP of data, where the message is divided into protection classes (PCs). The security gap and the eavesdropper's equivocation rate are discussed as security metrics. Both of these metrics are adoptable when finite length codes are considered.

Chapter 4
In Ch. 4 the secrecy level achieved over a wire-tap channel by exploiting practical LDPC codes is investigated. In such case, the equivocation rate experienced by the eavesdropper is used as a metric. In particular, by focusing on the code design, we have provided a strategy for its optimization. Numerical results show as, through our method, the proposed finite length codes approach theoretical bounds.

Chapter 5
Chapter 5 contains a proposal to obtain security over a BCC. In this chapter, we show as LDPC codes with UEP capabilities are advisable to achieve security and reliability in this scenario. To underline this fact, we compare the performance achieved by LDPC codes with and without UEP. Then, we move to consider a fading BCC. In such case, an infeasible system condition

may occur. Thus, we study the outage probability and, in order to minimize its value, we propose the use of high order modulation schemes to send the less protected bits. In some cases, a large UEP of data is needed. Hence, in this chapter we also propose a strategy to achieve this goal. Moreover, an algorithm for the asymptotic performance evaluation of each PC, by considering high order modulation schemes and non-conventional bits labeling, has been provided.

Chapter 6

Concerning the reliability of a satellite link with solar scintillation, the performance achieved by error correction codes currently adopted in space missions over this kind of channel are compared. From this preliminary investigation, weaknesses of some classical coding schemes in very noisy conditions emerge. While, some coding techniques, as LDPC codes, have shown a greater reliability. In satellite systems, the phase synchronization is a critical issue. For such reason, we have also studied the performance achieved by adopting non-coherent modulation schemes, where the phase detection of the incoming signal is not a requirement. To the best of our knowledge, no previous works have addressed this scenario.

Chapter 7

Regarding concatenated polar codes for short packet communications, in this chapter a strategy for their theoretical characterization is provided. Moreover, by introducing an interleaver in the concatenated scheme, we have shown as, in some cases, this configuration overcomes the one already proposed in literature. Starting from the weight distributions of the outer and inner code, the average performance of the codes ensemble obtained by considering all possible interleavers is estimated. Furthermore, our results show as the outer code has an important role at short block lengths.

Chapter 8

Finally, Ch. 8 concludes the thesis.

1.2 Main contributions of the thesis

In the following list the main contributions of this thesis are reported.

Chapter 4

- The eavesdropper's equivocation rate achievable with practical LDPC codes is derived.
- Through a suitable optimization strategy, finite length LDPC codes that approach the capacity over the wire-tap channel are designed.

Chapter 5

- LDPC codes with and without UEP capabilities are compared.
- Gaussian and fading BCC channels are considered. In latter case the system outage probability is studied.
- To achieve a large UEP of data, a code optimization process and an asymptotic performance evaluation of the PCs are proposed.

Chapter 6

- A comparison among the results of several code families over a channel with amplitude and phase scintillation is provided.
- In the case without a correct phase estimation, the performance achieved with non-coherent modulations are derived.

Chapter 7

- Concatenated interleaved polar codes are proposed.
- Concatenated polar codes are studied from a distance spectrum point of view.
- The impact of the outer code on the performance of the concatenated scheme is investigated.

Chapter 2

Why error correcting codes for secure and reliable communications?

Wireless communications are involved in many of the current human activities (e.g., mobile, television, satellite and Wi-Fi communications), to send/receive, share and store data. In fact, wireless communications have become one of the most used transmission systems in the last decades. In this scenario the reliability and security of the communication are prominent aspects. In fact, if on one hand the charm of these systems is a communication without a wired link, on the other hand, this fact exposes such networks both to eavesdropper attacks and to a quality worsening of the link.

Traditionally, error correcting codes are used to improve the reliability of communications. In particular, block codes are one of the most important codes family, where a block of information bits is encoded into a codeword. At the beginning of coding theory, this codes family was mostly formed by algebraic codes, e.g., Reed-Solomon (RS) codes, Hamming codes, Reed-Muller (RM) codes, Bose-Chaudhuri-Hocquenghem (BCH) codes. Algebraic block codes are in general hard decoded. In this case, at the receiver side, the decision on the bit values (typically 1 or 0 if a binary code is considered as in this thesis) is taken through a "threshold" detector. After this decision stage, the decoder tries to recover the information sent. However, the error correction performance may be improved by using soft decision decoding, where the received bits sequence is compared with all possible codewords and the one which gives the minimum Euclidean distance is selected. This way, the extra information coming from the channel supplies an estimation on the bits reliability. From this observation, a lot of error correcting schemes have been proposed, we refer in particular to LDPC codes, parallel concatenated turbo codes (PCTCs) [4] and polar codes. These coding schemes, under certain conditions, are able to approach the channel capacity and therefore they are considered the state-of-the-art in coding theory. These codes are involved in many practical applications, as: satellite communications for telemetry (TM) and telecommand (TC) links, DVB-T, DVB-S and wireless and mobile communications. For all these reasons, we have considered LDPC and polar codes.

Beside the attitude of error correction, a coding scheme may be used also to improve the secrecy of data in a wireless communication. Usually the security of the information is guaranteed through some cryptographic primitives that work at the upper layers of the protocol stack. The security provided by these algorithms is mainly achieved by encrypting data through some mathematical problems whose solution has a non-polynomial complexity. However, through a quantum computer some cryptographic systems will be overcome in a polynomial time [5, 6]. This scenario may seem far away, indeed, some quantum computers already appeared in the market, from D-Wave Systems Inc. [7] or IBM [8]. Moreover, some researchers have recently shown as also WPA-2, the most widely adopted cryptography algorithm in Wi-Fi networks, can be cracked [9]. Thus, nowadays the secrecy of data in this scenario is a critical point. In such context, a different approach able to introduce a primary security level in the information sent is emerged. We refer to the PLS techniques that, prior to apply traditional cryptographic algorithm, can contribute to reduce the computational effort or even enhance the security level. Indeed, classical cryptographic primitives require a high computational cost that may affect the communication among wireless devices, where limited calculus resources are available.

2.1 Physical layer security (PLS) vs. classical cryptography

In order to introduce security in a wireless communication, commonly cryptographic techniques developed at the upper layer of the protocol stack are used. In general, these methods are divided in symmetric and asymmetric approaches. In the first one, a private key shared among the legitimate users is needed. Indeed, in this kind of solution the same key is used to encrypt and decrypt data, as schematically shown in Fig. 2.1.

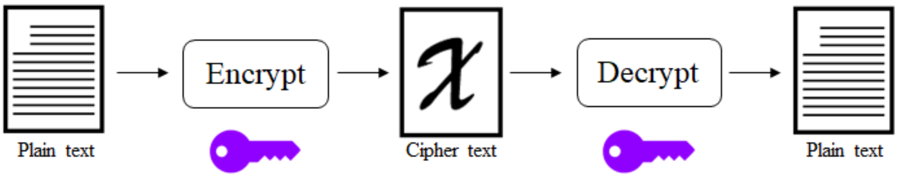


Figure 2.1: Symmetric cryptography.

The main advantage of symmetric algorithms is their easy implementation, however the way to share the private key is an important matter. In fact if the users do not have the private key, a secure channel for the key exchange is required. To overcome this issue, asymmetric algorithms may be adopted. In this case a couple of keys is used: the public and the private key. The first one is completely known by the users, while the latter is a personal key. Generally, the public (private) key is used to encrypt (decrypt) data. This way, the problem of the key exchange in symmetric solutions is avoided. The asymmetric algorithms can be used both to authenticate the transmitter (through the public key) and to protect the data, since only the owner of the appropriate private key may correctly recover the information. Well known asymmetric solutions are the RSA encryption algorithm or the McEliece cryptosystem. A pictorial representation of an asymmetric cipher system is reported in Fig. 2.2.

The aim of PLS paradigm is to minimize the amount of confidential information that can be attained by the eavesdroppers by indirectly manipulating their received signals. This goal is achieved without any pre-shared key or

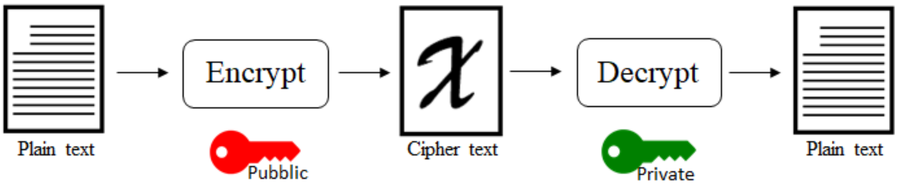


Figure 2.2: Asymmetric cryptography.

mathematical problem with a hard numerical solution, but only exploiting the randomness of the transmission channel. Traditionally, the channel noise is considered an impairment, instead PLS methods take advantage from it for improving the security of the communication. Through this approach, all receivers are perfectly aware of the encoding and transmission techniques, and the security is only due to the differences between the channels experienced by authorized and unauthorized users. Such a security level may suffice by itself or, more frequently, may constitute a basis for higher layer cryptographic protocols. As a result, the secrecy introduced by this kind of approach does not depend by the computational power of an adversary. PLS techniques are based on the information theory fundamentals where the existence of a channel coding able to ensure both security and robustness of the communication is proved. For this reason, we consider a PLS scenario and propose modern coding techniques to achieve security in the communication.

2.2 Modern coding techniques

In this section we introduce some basic concepts concerning the adopted coding schemes. The name *modern* indicates that the chosen coding schemes are currently recommended in the considered scenarios.

Definition 2.2.1 The binary linear block code $\mathcal{C}(n, k)$ is defined by a k-dimensional subspace of the n-dimensional vector space over the finite field $\mathbb{F}_2^n$.

We consider only binary codes, so the transmitted message is formed by 0's and 1's. The basic idea of error correcting codes is to add extra bits to the vector of information bits $\mathbf{u}$, in order to protect it from impairments introduced by the channel. The obtained message is the codeword $\mathbf{c}$. We call k and n the length of $\mathbf{u}$ and $\mathbf{c}$, respectively, and the ratio $R = \frac{k}{n}$ is called rate of $\mathcal{C}(n, k)$. Typically, $\mathbf{u}$ and $\mathbf{c}$ are row vectors.

This way, the introduced redundancy bits allow a greater distance among the codewords. Consequently, the received bits can be corrected, within certain limits, if corrupted during the transmission over the channel. A very simple example of coding technique, is the Single Parity Check (SPC) code. In this code a single extra bit is introduced to obtain $\mathbf{c}$, and its value depends on the bits in $\mathbf{u}$. A possible choice (not unique) is to fix the value of the extra bit in order to have an even number of 1's in $\mathbf{c}$. At the receiver side, a wrong $\mathbf{c}$, caused by the channel noise, can be easily detected by the inversion of the check bit. Even if the SPC code is able to detect errors in the arrived $\mathbf{c}$, it is not able to correct them, so it can be used only for error detection.

Since we aim to enhance the reliability and security of the communication, we are interested to introduce extra bits in order to correct $\mathbf{u}$. For this purpose, we use LDPC and polar codes. Clearly, LDPC and polar codes are much more sophisticated than the SPC code, however the basic idea is the same, i.e., to introduce some extra bits to correct the received data. In these codes the parity bits are more than one, so we call $r = n - k$ their number. In this case, each codeword must satisfy r parity check equations. Usually, the check equations are expressed in matrix form through the parity check matrix $\mathbf{H}$ with dimension $r \times n$. This matrix describes the code and can be used to encode/decode data.

Definition 2.2.2 A binary linear block code $\mathcal{C}(n, k)$ may be defined through its $r \times n$ parity check matrix $\mathbf{H}$ if and only if the following equation is satisfied

$$\mathbf{c} \cdot \mathbf{H}^{\top} = \mathbf{0}_r$$

where $^{\top}$ denotes transposition and $\mathbf{0}_r$ is a r-length vector of all-zero elements. Note as in the case of binary codes the elements of $\mathbf{H}$ are in $\mathbb{F}_2$.

Another way to obtain $\mathbf{c}$ from $\mathbf{u}$ is to use the generator matrix $\mathbf{G}$ of

$\mathcal{C}(n,k)$.

Definition 2.2.3 The $k \times n$ generator matrix $\mathbf{G}$ of a binary linear block code $\mathcal{C}(n,k)$ encodes $\mathbf{u}$ onto $\mathbf{c}$ through the equation

$$\mathbf{c} = \mathbf{u} \cdot \mathbf{G}.$$

Note as in the case of binary codes the elements of $\mathbf{G}$ are in $\mathbb{F}_2$. If $\mathbf{G}$ has a $k \times k$ identity sub-matrix, $\mathcal{C}(n,k)$ is a *systematic* code .

From Def. 2.2.1 follows that $\mathcal{C}(n,k)$ has 2^k codewords that are a subset of all possible 2^n binary vectors of length n. From this observation it derives that the main decoder task is to attribute the received data to the most likely sent $\mathbf{c}$. Since sometimes this process fails, the scope of the code design is to improve this skill of the decoder. The way to design $\mathbf{H}$ and $\mathbf{G}$ is a peculiarity of each code family. Clearly, the $\mathbf{H}$ and $\mathbf{G}$ matrices of $\mathcal{C}(n,k)$ can be derived one from the other. This process is well known in literature. The only relation that this couple of matrices must satisfy is $\mathbf{G} \cdot \mathbf{H}^\top = 0$. In this sense, $\mathbf{H}$ and $\mathbf{G}$ can be used indifferently to encode and decode data. With reference to the code families considered in this dissertation, $\mathbf{H}$ is used for LDPC codes, while $\mathbf{G}$ in polar coding.

Let $w_H(\cdot)$ be the Hamming weight of a vector. The $\mathbf{c}$ with the lowest $w_H(\mathbf{c})$ determines an important property of $\mathcal{C}(n,k)$, the so called *minimum distance* $d_{\min}$ of the code. In fact, by using a hard decision on the bit values, a code $\mathcal{C}(n,k)$ can always detect t errors if

$$t < d_{\min}$$

and correct e flipped bits if

$$e \leq \lfloor (d_{\min} - 1/2) \rfloor,$$

where $\lfloor x \rfloor$ is the largest integer at most equal to x. In scenarios where the quality or the reliability of the communication must be improved, the minimum distance of $\mathcal{C}(n,k)$ plays an important role, since it affects the performance of that code. The higher $d_{\min}$, the better performance. Thus, if our goal is to increase the number of errors corrected by the code, its design should aim to enhance the $d_{\min}$ value. Instead, in the case of (soft decision) maximum likelihood (ML) decoding, the performance of a code can be estimated through its distance spectrum via the union bound (UB), that is an upper bound on the block error probability of $\mathcal{C}(n, k)$. We use such bound in Ch. 7, where we also provide a more formal definition.

2.2.1 Low density parity check codes (LDPC)

LDPC codes were first proposed in 1962 by Gallager in his PhD thesis [10]. However, due to the available computational resources in those years, their great correction capabilities remained unused. The LDPC codes remain unknown until the last decade of the past century, when many researchers working on block codes rediscovered this code family. Through the activity of these researchers the incredible potential of LDPC codes was emerged, and the techniques used nowadays for their design allow to approach the Shannon's capacity. Currently, LDPC codes are recommended in many communication standards as: satellite communications, DVB-S2, DVB-T2, Wi-Fi 802.11, 10GBase-T Ethernet.

The main feature of LDPC codes, as suggested by the name, is the sparsity of their $\mathbf{H}$ matrix. Indeed, for this code family $\mathbf{H}$ has a small number of non-zero entries, this way a low complexity at the decoding side is ensured. Due to the need of a low density in $\mathbf{H}$, usually the design of an LDPC code starts from that matrix. If necessary, the corresponding $\mathbf{G}$ is subsequently derived. The main difference between LDPC codes and other block codes is their decoding algorithm. In fact, contrary to classical block codes, in this case an iterative decoding based an a graphical representation, called Tanner graph, is used. A Tanner graph $\mathcal{T}$ is a bipartite graph composed by two set of nodes: n variable nodes v and r check nodes c. Each variable node corresponds to one codeword bit (i.e., one node for each column of $\mathbf{H}$), while each check node is related to one parity-check equations in $\mathbf{H}$ (i.e., one node for each row). Noting by h_{ij} the (i, j)-th element of $\mathbf{H}$, an edge exists between the

j-th variable node and the i-th check node if and only if $h_{ij} = 1$. The number of edges connected to a node is called *degree* of that node and we define as E the total number of edges in $\mathcal{T}$. In Fig. 2.3 a pictorial example of a possible $\mathbf{H}$ and its Tanner graph is shown. The example is only illustrative, since the code is not LDPC.

$$\begin{array}{cc} & \begin{array}{ccccccc} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \end{array} \\ \mathbf{H} = & \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{array}{c} c_1 \\ c_2 \\ c_3 \\ c_4 \end{array} \end{array}$$

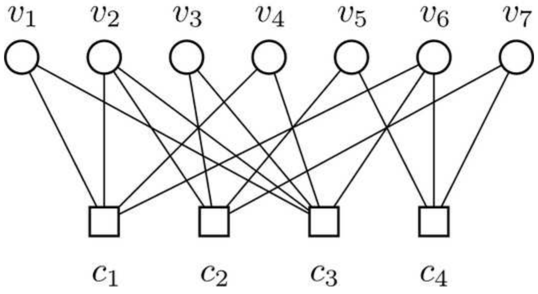


Figure 2.3: An example of a Tanner graph.

The following two polynomials are commonly used to denote the variable and check node degree distributions

$$\lambda(x) = \sum_{i=1}^{d_v} \lambda_i x^{i-1}, \tag{2.1}$$

$$\rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1} \tag{2.2}$$

where d_v and d_c are the maximum variable and check node degrees, respectively. In $\lambda(x)$ $(\rho(x))$, the coefficient λ_i (ρ_j) coincides with the fraction of edges connected to the variable (check) nodes having degree i (j). Therefore,

$\lambda(x)$ and $\rho(x)$ are defined from the so called edge perspective. By definition

$$\sum_i \lambda_i = 1$$

and

$$\sum_j \rho_j = 1.$$

The code rate can be expressed as

$$R = 1 - \frac{\sum_{i=2}^{d_v} \rho_i/i}{\sum_{j=2}^{d_c} \lambda_j/j}. \tag{2.3}$$

In some cases it is more useful to consider the node perspective of $\lambda(x)$ and $\rho(x)$. By denoting with $\tilde{\lambda}(x)$ the variable node degree distribution from the node perspective, the following formula allows to convert $\lambda(x)$ in $\tilde{\lambda}(x)$

$$\tilde{\lambda}_i = \frac{\lambda_i/i}{\sum_{k=2}^{d_v} \lambda_k/k}. \tag{2.4}$$

The same reasoning can be applied to the check nodes degree distributions, by denoting with $\tilde{\rho}(x)$ the check node degree distributions from the node perspectives, and replacing λ with ρ and d_v with d_c in (2.4).

Concerning the design of the check node degree distribution, we can adopt a concentrated distribution (i.e., with only two degrees, concentrated around the mean). This solution has the advantage of being very simple, while achieving good performance. This way, we obtain

$$\tilde{\rho}(x) = ax^{\lfloor c_m \rfloor} + bx^{\lceil c_m \rceil},$$

where $c_m = \frac{E}{r} = \frac{\sum_j \tilde{\lambda}_j \cdot j}{(1-R)}$. The values a and b are computed as

$$a = \lceil c_m \rceil - c_m, \qquad b = c_m - \lfloor c_m \rfloor.$$

If $\lambda(x)$ and $\rho(x)$ contain only one degree, the LDPC code is called *regular*, otherwise *irregular*. We consider only irregular LDPC codes, since they have better performance and more degrees of freedom during the design w.r.t.

regular ones. In fact, from previous considerations, we deduce that through $\lambda(x)$ and $\rho(x)$ (or equivalently $\tilde{\lambda}(x)$ and $\tilde{\rho}(x)$) an LDPC code is uniquely determined. Thus, we provide new solutions to improve the security level of the communication by acting on the degree distributions of the considered code. For example, as proposed in this thesis, irregular LDPC codes may by adopted to protect the message bits in a different manner. In this case an optimization of the degree distributions is required.

2.2.2 Polar codes

Polar codes, introduced by Stolte and Arikan [11, 12] in the first decade of 2000, have immediately attracted many researchers, since it is proved that they achieve the capacity in a binary-input discrete memoryless symmetric (BI-DMS) channel by using the (low complexity) successive cancellation (SC) decoding algorithm, in the limit of infinite block length. As for LDPC coding, also polar codes are well known in literature, therefore we introduce only the fundamental concepts used in this thesis. As their name suggests, the polar coding is based on a phenomenon called *channel polarization* [12]. Through this process, several virtual copies of the physical BI-DMS channel W are realized, we call with W^i the i-th copy of W. By denoting with $W : \mathcal{X} \to \mathcal{Y}$, where $\mathcal{X}$ and $\mathcal{Y}$ are the input and output alphabet, respectively, a generic BI-DMS channel, its transition probability is $W(y|x)$, where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. An important parameter of polar coding is the symmetric capacity $I(W)$, that is the highest rate at which reliable communication is possible over W. For a code length that goes to infinity, through the polarization process, the symmetric capacity of each channel copy $I(W^i)$ tends to 0 or 1. In this case, we have a strong separation among the $I(W^i)$ values, since their values can be only equal to 0 or 1. Vice versa, for short codes, $I(W^i)$ assumes also other values within the interval $[0, 1]$, this fact determines a performance deterioration. Thus, in order to achieve reliable communications, the k information bits must be sent in the most k reliable copies of W. To select this sub-set of channel copies, another important parameter in the polar coding is used, the so called Bhattacharyya parameter $Z(W)$ [12]

$$Z(W) \triangleq \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}. \tag{2.5}$$

This parameter is used to measure the reliability of each channel copy, since it is an upper bound on the probability of wrong decision under ML decoding when W is used only once to transmit 0 or 1. As $I(W)$, also $Z(W)$ assumes values in [0, 1]. In general, $I(W) \approx 1$ iif $Z(W) \approx 0$ and vice versa. So, the most reliable k copies of W correspond to the W^i with the lowest $Z(W)$ values. The process used to polarize the channel has an impact on the code design, since the virtual copies of W are realized with a successive recursions of a kernel. The one proposed by Arikan and used in this thesis is

$$\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

In such case, the $\mathbf{G}$ matrix is obtained by applying $\log_2 n-$times the Kronecker product to $\mathbf{G}_2$. At the end of this stage a $\mathbf{G}_{n\times n}$ matrix is obtained. Then, the $\mathbf{G}_{k\times n}$ matrix of the polar code is obtained by selecting the k rows with the lowest Bhattacharyya parameter values. This way, in $\mathbf{c}$ the k positions with the lowest Bhattacharyya parameter values are used to send information bits, while in the remaining r positions called *frozen* bits, a predetermined value is set.

During the past years a lot of systems based on polar coding have been proposed. For example, different kernels or channel models have been considered. We design polar codes over a BEC and use the definition of the Bhattacharyya parameter in (2.5) that is the one proposed in the original Arikan's paper [12].

As mentioned, polar codes achieve the capacity under the assumption of infinite block length. However, for short packet communications, polar codes under SC decoding tend to exhibit a poor performance. In [13] it was suggested that such a behavior might be due, on one hand, to an intrinsic weakness of polar codes and, on the other hand, to the sub-optimality of SC decoding w.r.t. ML decoding. Improved decoding algorithms were proposed in [13–15], while the structural properties of polar codes (e.g., their distance properties) were studied, among others, in [16–21]. The minimum distance properties of polar codes can be improved by resorting to concatenated schemes like the one in [13], where the concatenation of polar codes with an outer CRC code is considered. This solution, together with the use of the list decoding algorithm of [13], allows polar codes to become competitive in finite block length regime against other families of codes [22–26]. For this reason, recently the on-going 3GPP standardization group is considering the adoption of short polar codes with an outer CRC for the uplink control channel of the upcoming 5th generation mobile standard [1]. However, a theoretical characterization of the performance of concatenated CRC-polar codes is still an open problem. Furthermore, for a fixed code length, a concatenated scheme can be realized with several combinations of the component codes parameters (e.g., one may choose various CRC polynomials and polar codes designed for different target signal-to-noise ratios (SNRs)). For such reason we study concatenated polar codes from a distance spectrum point of view and propose some solutions to improve their performance.

2.3 Summary

In this chapter, we have explained the reasons for which error correcting codes can be used to achieve secure and reliable communication. Then, we have discussed the rationale of PLS approaches to improve the security of the data, or more realistically, to introduce a basic level of secrecy that can be exploited by cryptographic primitives. Finally, some basic elements of the used coding schemes have been exposed.

Chapter 3

Channel models and security metrics used in PLS

In this chapter we define the channel models and the security metrics considered in this work. Since a wireless communication with the presence of an eavesdropper is well represented by a wire-tap channel [2], in Sec. 3.1 we introduce this model. After that, in Sec. 3.3, the wire-tap channel is then generalized through a BCC [3]. We consider the case of only Additive White Gaussian Noise (AWGN) channel and quasi-static fading channel (QSFC), where a Rayleigh fading is included. Our focus is on finite block lengths, since we aim at evaluating the achievable security levels over continuous wire-tap channels when using a given practical coding scheme. The target to exploit practical coding schemes is of crucial importance to make PLS feasible in practice [27–29]. Moreover, short block codes are of current interest for the next mobile generation (i.e., 5G) and machine-to-machine communications [30]. Therefore, differently from most previous works, we do not aim at designing optimized coding schemes to achieve some asymptotic secrecy target like weak or strong secrecy [31, 32]. Instead, our target is to estimate the level of PLS which is achievable "for free" by using some given classical coding schemes. Thus, in this chapter we provide the metrics used to measure the achievement of these goals, namely, eavesdropper's equivocation rate and security gap. Finally, over the BCC model we introduce the concept of UEP of data. In such case, we discuss the conditions that lead to a feasible system.

3.1 Wire-tap channel

A PLS scenario may be modeled with a wire-tap channel [2], where a transmitter (Alice) sends some confidential information to a legitimate receiver (Bob), in the presence of an eavesdropper (Eve). The transmission technique used by Alice is perfectly known by both Bob and Eve. However, the channel between Alice and Bob is inherently different from the channel between Alice and Eve; hence, only based on this difference, there is the expectation that the information sent from Alice to Bob is not successfully retrieved by Eve.

We focus on continuous-output channel models, which are best suited to describe wireless transmissions. While in previous literature there are some valuable examples of coding schemes able to achieve secrecy over a discrete wire-tap channel [33–35], the extension to continuous channels has been faced only recently [36]. Even previous works considering well established cryptographic security metrics in this context only provide explicit schemes for the discrete channel case [37]. Obviously, a continuous channel can be converted into a discrete channel by using hard detection, but this cannot be forced for an adversary.

After the case of only an AWGN channel between Alice and the receivers, we consider the fading wire-tap channel shown in Fig. 3.1. Both Bob's and Eve's channels are subject to Rayleigh fading, with fading coefficients h_B and h_E, respectively, and affected by AWGN, whose samples are denoted by n_B and n_E. In the model we consider a QSFC, where h_B and h_E are two independent Rayleigh random variables known by Bob and Eve, respectively, hence we assume channel state information for the both receiver. The SNRs of the two channels are generally different, as well as the two vectors received by Bob and Eve, noted by $\mathbf{c}_B$ and $\mathbf{c}_E$, and the messages they get after decoding, noted by $\mathbf{u}_B$ and $\mathbf{u}_E$. More precisely, the real and imaginary parts of h_{B} and h_{E} are Gaussian random variables with mean 0 and variance 1/2; hence the squared modulus of h_{B} and h_{E} is chi-square distributed. The thermal noise

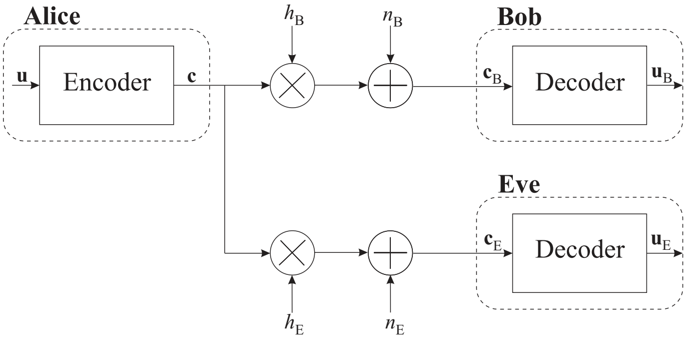


Figure 3.1: Fading wire-tap channel model.

is present also in this case. It follows that the SNR per bit (which has to be specialized for Bob and Eve, but we omit the subscripts B and E for the sake of simplicity), $\gamma = |h|^2 E_b/N_0$, is chi-square distributed as well, with probability density function

$$p_\Gamma(\gamma) = \frac{1}{\overline{\gamma}} e^{-\gamma/\overline{\gamma}}, \quad \gamma \geq 0, \tag{3.1}$$

where $\overline{\gamma} = E_b/N_0$ is the mean value.

3.2 Security metrics

The secrecy performance over wire-tap channels is classically measured using information-theoretic metrics, like the secrecy capacity, and in asymptotic conditions (e.g., infinite code length and random coding). However, we are interested to assess the performance, in terms of secrecy, achieved by using practical coding schemes. One of the most common metrics to assess the performance of finite length codes used for transmissions is the average bit error rate (BER) achieved by using some (possibly optimal) decoder. On the other hand, as a metric for PLS, we use a parameter which allows for a straightforward assessment and comparison of practical transmission schemes, based on the error rate achieved by Bob and Eve. This parameter is the so-called *security gap*, first introduced in [38]. It is defined as the quality ratio between Bob's and Eve's channels that is required to achieve a sufficient level of PLS, while ensuring that Bob reliably receives the transmitted information. This parameter will be further discussed in Sec. 3.2.1.

It must be said that other performance metrics exist, and are also often used for assessing transmissions over this kind of channels. One of them is the *eavesdropper's equivocation rate* on the secret message [29,39]. Nevertheless, a high error rate at Eve's is a necessary condition to achieve information-theoretic security, and therefore we impose such a constraint in our work. However, as shown in [40,41], in some cases this condition is not sufficient. Therefore, we integrate the analysis based on Eve's error rate with suitable information-theoretic metrics for assessing the achievable security levels. We introduce the eavesdropper equivocation rate as a metric in Sec. 3.2.2.

As the next sections will clarify, from the definitions of the chosen security metrics, i.e., security gap and eavesdropper equivocation rate, it follows that they will be adopted for different scopes. Since the first one is based on the error rate of codes, it is suitable where a comparison among their performance is of interest. Instead, the latter, due to its closeness with theoretic metrics, it is advisable when the performance of a finite length code is compared with asymptotic results. Hence, depending on the goal of the study, we adopt these two security metrics. In particular, the eavesdropper equivocation rate is used in Ch. 4, while the security gap in Ch. 5.

3.2.1 Security gap

Let us fix two suitable thresholds for Bob's and Eve's frame error rate (FER), named $P_f^{\mathrm{B}}\big|_{\mathrm{th}}$ and $P_f^{\mathrm{E}}\big|_{\mathrm{th}}$, respectively. In order to have reliability, we impose that Bob's mean FER is $\leq P_f^{\mathrm{B}}\big|_{\mathrm{th}}$; dually, in order to have security, we impose that Eve's mean FER is $\geq P_f^{\mathrm{E}}\big|_{\mathrm{th}}$. On the other hand, taking into account the error rate dependence on the SNR, the same conditions can be translated in terms of the channel quality by imposing $\overline{\gamma_{\mathrm{B}}} \geq \gamma_{\mathrm{B}}|_{\mathrm{th}}$ and $\overline{\gamma_{\mathrm{E}}} \leq \gamma_{\mathrm{E}}|_{\mathrm{th}}$, where $\gamma_{\mathrm{B}}|_{\mathrm{th}}$ and $\gamma_{\mathrm{E}}|_{\mathrm{th}}$ are the SNR values corresponding to $P_f^{\mathrm{B}}\big|_{\mathrm{th}}$ and $P_f^{\mathrm{E}}\big|_{\mathrm{th}}$, respectively, and $\overline{\gamma_{\mathrm{B}}}$ and $\overline{\gamma_{\mathrm{E}}}$ are the mean SNRs for Bob and Eve, respectively. To measure the difference from the Bob's and Eve's channel, we

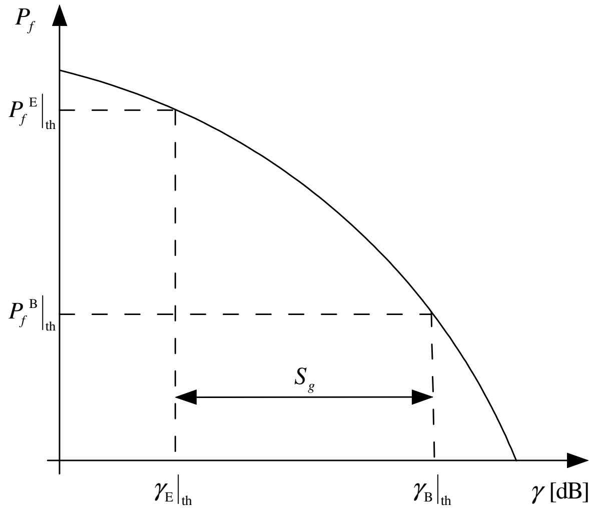


Figure 3.2: Pictorial representation of the security gap.

may use the security gap defined defined as

$$S_g = \frac{\gamma_{\mathrm{B}}\big|_{\mathrm{th}}}{\gamma_{\mathrm{E}}\big|_{\mathrm{th}}}. \tag{3.2}$$

As will be more clear in the following, the definition of the security gap depends on the considered scenario. In this sense, eq. (3.2) is only one of its possible statements. According to this definition, it is evident that S_g, that is always greater than 1, should be kept as close to 1 as possible, in such a way that the reliability and security targets are reached even with a small degradation of Eve's channel quality w.r.t. Bob's.

An example of S_g computation is shown in Fig. 3.2, where the SNR is expressed in dB (which justifies the difference in place of the ratio). Based on its definition, it is clear that the security gap depends on the steepness of the FER curve: the steeper the slope, the smaller the security gap.

It is also evident that S_g can be equally determined after having fixed the threshold values $P_b^{\mathrm{B}}\big|_{\mathrm{th}}$ and $P_b^{\mathrm{E}}\big|_{\mathrm{th}}$ on the BER instead of the FER. The value of S_g clearly depends on the decoder used by Bob and Eve, respectively.

3.2.2 Eavesdropper's equivocation rate

Let $\mathcal{M}$ the secret message sent by Alice over a Gaussian wire-tap channel. She encodes her message into the codeword $\mathbf{c}$, which uniquely depends on $\mathcal{M}$ and on some random message $\mathcal{R}$ generated by Alice for confusing Eve. We note that the use of a random part of the message is limited to Eve's equivocation rate discussion. If the secret message is k_s bits long and the random message is k_r bits long, the code rate is $R = (k_s + k_r)/n = k/n$. The secret message rate, instead, is $R_s = k_s/n$. The noisy codewords received by Bob and Eve are denoted by $\mathbf{y}$ and $\mathbf{z}$, respectively. In order to achieve successful transmission of $\mathcal{M}$ over this channel, both the following targets must be fulfilled

i. $\mathcal{M}$ must be reliably decoded by Bob, i.e., with a sufficiently small error rate (*reliability target*),

ii. the information about $\mathcal{M}$ gathered by Eve must be sufficiently small (*security target*).

Concerning the reliability target, in ideal conditions (i.e., infinite code length and random coding) the channel capacity can be used as the ultimate code rate limit. In the finite length regime, instead, a practical code must be designed to allow Bob to achieve a sufficiently low error rate in decoding the secret message. Concerning the security target, some classical information theoretic secrecy metrics are only useful in the asymptotic regime. In fact, denoting by $\mathrm{I}(a; b)$ the mutual information between a and b, we have [42]

- Strong secrecy when the total amount of information leaked about $\mathcal{M}$ through observing $\mathbf{z}$ goes to zero as n goes to infinity, i.e., $\lim_{n\to\infty} \mathrm{I}(\mathcal{M}; \mathbf{z}) = 0$.

- Weak secrecy when the rate of information leaked about $\mathcal{M}$ through observing $\mathbf{z}$ goes to zero as n goes to infinity, i.e., $\lim_{n\to\infty} \mathrm{I}(\mathcal{M}; \mathbf{z})/n = 0$.

So, these metrics are not useful in order to assess the performance in finite length conditions.

However, another metric can be exploited, which was already used in Wyner's original work [2]. According to [2], transmission is accomplished in perfect secrecy when the wire-tapper equivocation rate on the secret message, $R_e = \frac{1}{n}\mathrm{H}(\mathcal{M}|\mathbf{z})$, with $\mathrm{H}(\cdot)$ denoting the entropy function, equals the entropy of the data source. We consider independent and identically distributed secret messages, therefore the source entropy rate is equal to R_s. So, perfect secrecy is achieved when the equivocation rate R_e equals the secret message rate R_s, i.e.,

$$\widetilde{R_e} = R_e/R_s = 1. \tag{3.3}$$

$\widetilde{R_e}$ is called fractional equivocation rate.

Actually, the ultimate limit achievable by the equivocation rate is the secrecy capacity $C_s = C_B - C_E$, where C_B and C_E are Bob's and Eve's channel capacities, respectively. For a binary-input channel with AWGN and SNR γ, the capacity is given by the following expression

$$C(\gamma) = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(y-\sqrt{\gamma})^2}{2}} \log_2\left(1 + e^{-2y\sqrt{\gamma}}\right) dy. \tag{3.4}$$

Then, the target is to maximize R_e in such a way as to approach the secrecy capacity. On the other hand, when considering finite length codes, it is expected that $C_s < R_s$ and another valuable issue is the evaluation of the gap between the secret message rate and the secrecy capacity.

Concerning the computation of the equivocation rate, it can be shown that [43]

$$R_e = \frac{1}{n}\left[\mathrm{H}(\mathbf{c}) - \mathrm{I}(\mathbf{c};\mathbf{z}) + \mathrm{H}(\mathcal{M}|\mathbf{z},\mathbf{c}) - \mathrm{H}(\mathbf{c}|\mathcal{M},\mathbf{z})\right]. \tag{3.5}$$

From (3.5) it results that this formulation of Eve's equivocation rate requires to compute the quantity $\mathrm{H}(\mathbf{c}|\mathcal{M},\mathbf{z})$, that is, the entropy of $\mathbf{c}$ conditioned to receiving $\mathbf{z}$ and knowing the secret message $\mathcal{M}$. Eve obviously does not know the secret message, therefore we suppose the existence of another (fictitious) receiver in the same position as Eve's, knowing the secret message $\mathcal{M}$. We denote such a receiver as Frank: he receives the same vector $\mathbf{z}$ as Eve but, differently from Eve, he has perfect knowledge of the secret message $\mathcal{M}$.

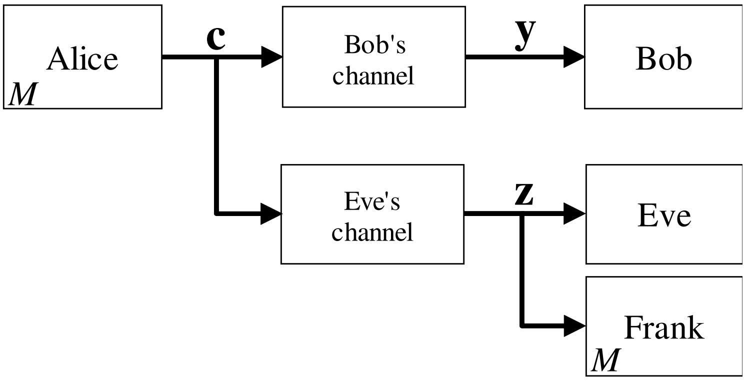


Figure 3.3: Wire-tap channel model with fictitious receiver.

Then, he tries to decode $\mathbf{z}$ for recovering the random message $\mathcal{R}$, which is the only source of uncertainty for Frank in order to reconstruct $\mathbf{c}$. The resulting wire-tap channel model is schematically depicted in Fig. 3.3. The letter M inside Alice's and Frank's boxes points out that the message is known to both Alice and Frank.

Let us suppose that, in these conditions, Frank experiences a decoding error probability (or codeword error rate (CER)) equal to θ. By Fano inequality we have $\mathrm{H}(\mathbf{c}|\mathcal{M}, \mathbf{z}) \leq 1 + k_r \cdot \theta$. We also have $\mathrm{H}(\mathbf{c}) = k$ and $\mathrm{H}(\mathcal{M}|\mathbf{z}, \mathbf{c}) \leq \mathrm{H}(\mathcal{M}|\mathbf{c}) = 0$. Concerning Eve's channel mutual information $\mathrm{I}(\mathbf{c}; \mathbf{z})$, we could obtain a tight upper bound on it as proposed in [44], by taking into account the code length and the target error rate. Note that the proposed finite length analysis is not a second-order coding rate analysis as in [44]. However, by using the classical bound $\mathrm{I}(\mathbf{c}; \mathbf{z}) \leq nC_E$, we obtain a limit value which is independent of Eve's error rate. Such a value cannot be overcome even if Eve's error rate changes, therefore it represents a conservative choice for our purposes. Based on these considerations, we can find a lower bound on Eve's equivocation rate about the secret message as [43]

$$R_e \geq \frac{1}{n}\left[k - nC_E - k_r\theta - 1\right] = R - C_E - (R - R_s)\theta - \frac{1}{n} = R_e^*. \quad (3.6)$$

By looking at (3.6), it is evident that this metric is well suited to assess the secrecy performance of practical, finite length codes. In fact, the code length is taken into account, and the error rate experienced by Frank can be estimated for practical codes through numerical simulations. Its value obviously depends on Frank's SNR, which is the same as Eve's, and therefore, according to (3.4), it determines C_E. It follows that, for a fixed code length and rate, the equivocation rate can be maximized by optimizing the choice of the pair (θ, C_E).

3.3 Broadcast channel with confidential messages (BCC)

In this thesis we also consider a particular case of a wire-tap channel that well describes the common wireless scenarios, the BCC [3]. This channel model is a well-known transmission scheme for communications achieving security at the physical layer, which generalizes Wyner's wire-tap channel. Since its introduction, a lot of work has been done to study the BCC from the information theory standpoint, mostly aimed at computing the secrecy capacity regions for this channel and its several variants (see [45–47] and the references therein). More recently, the secrecy capacity regions have been studied also for the BCC with multiple-input multiple-output (MIMO) [48–50] and cooperative communications [51].

For the classical wire-tap channel, the use of several practical families of codes has already been investigated: this is the case of lattice codes [52], polar codes [53] and LDPC codes [54]. Instead, for the BCC, despite the large amount of theoretical work, there is still a lack of practical systems able to achieve some specific security and reliability targets. The use of coding is recognized as an important tool also in such a context, but most studies consider the abstraction of random coding [55], which indeed is difficult to translate into a practical coding scheme. Only in [56–58] the authors propose the use of practical polar codes over this special channel. Other, and even more widespread families of codes, like LDPC codes, have never been considered in such a context.

We focus on the Gaussian BCC and study some practical LDPC coded transmission schemes for achieving reliability and security over this channel. For this purpose, we follow some recent literature and use the error rate as a metric [29, 54, 59–61]. We define suitable reliability and security targets for the Gaussian BCC in terms of the error rate, and use the concept of *security gap*, defined in Section 3.2.1.

3.3.1 Unequal error protection (UEP)

In practical BCC scenarios, different sensitivities to errors are often required. In this case, a possible solution to achieve different levels of protection against the noise is to use coding and modulation schemes with UEP. In this scenario we refer to the *public* and *secret* part of the sent message, since it includes these two kind of information. Hence, in our model, each transmitted message of n bits contains a block of $k_s \leq k$ information bits which are secret, while the remaining $k_p = k - k_s$ information bits form a block of public information. It follows that the secret and public information rates are $R_s = \frac{k_s}{n}$ and $R_p = \frac{k_p}{n}$, respectively, and $R = R_s + R_p$.

In this work, $P_s(\gamma)$ ($P_p(\gamma)$) denotes the block error rate (BLER) for the secret (public) information block, i.e., the probability that, within a received frame of n bits, one or more of the k_s (k_p) secret (public) information bits are in error after decoding. In order to use the S_g as a metric of the security level in a BCC, in the following we give its definition applied to this scenario. Let us fix two small threshold values, δ and η, and define the security and reliability targets in terms of the decoding error probability as follows

$$P_p(\gamma^{(B)}) \leq \delta, \tag{3.7a}$$

$$P_p(\gamma^{(E)}) \leq \delta, \tag{3.7b}$$

$$P_s(\gamma^{(B)}) \leq \delta, \tag{3.7c}$$

$$P_s(\gamma^{(E)}) \geq 1 - \eta. \tag{3.7d}$$

Let us suppose that the public information blocks are more protected against noise than the secret information blocks. This scenario is exemplified in Fig. 3.4, where we suppose that the public information blocks experience a lower BLER than the secret information blocks. Conditions (3.7) can then be translated in terms of Bob's and Eve's SNRs, i.e., $\gamma^{(B)}$ and $\gamma^{(E)}$, respectively. More precisely, by looking at the figure, we have that conditions (3.7a) and (3.7c) become

$$\gamma^{(B)} \geq \max\{\beta_p, \beta_s\} = \beta_s, \tag{3.8}$$

whereas conditions (3.7b) and (3.7d) become

$$\beta_p \leq \gamma^{(E)} \leq \alpha_s. \tag{3.9}$$

It follows from (3.9) that, for the system to be feasible, we must actually ensure that the public message is more protected against noise than the secret one (this typically implies $R_p < R_s$). In fact, if the opposite occurs, since $1 - \eta > \delta$, we have $\alpha_s < \beta_p$, and condition (3.9) cannot be met. From the theoretical standpoint, the system is feasible even when $\alpha_s = \beta_p$. This obviously is a limit condition, while from the practical standpoint it is useful that $\alpha_s > \beta_p$, such that the system remains feasible even when $\gamma^{(E)}$ has some fluctuations.

When the system is feasible, i.e., the public message is more protected against noise than the secret one, and $\alpha_s \geq \beta_p$, we can compare different coding techniques by using the security gap S_g, defined as the ratio between Bob's minimum SNR and Eve's maximum SNR

$$S_g = \frac{\beta_s}{\alpha_s}. \tag{3.10}$$

We observe that in this case the definition of security gap is different from that in (3.2), since it has been explicated by considering a BCC. Based on the above considerations, the design target is to find codes which make the system feasible. In fact, differently from the wire-tap channel model, in this case there is no guarantee that the system is feasible even when Eve has a degraded channel w.r.t. Bob. Then, a meaningful objective is to find codes able to achieve small security gaps.

However, we also propose a different approach, in which the target is to

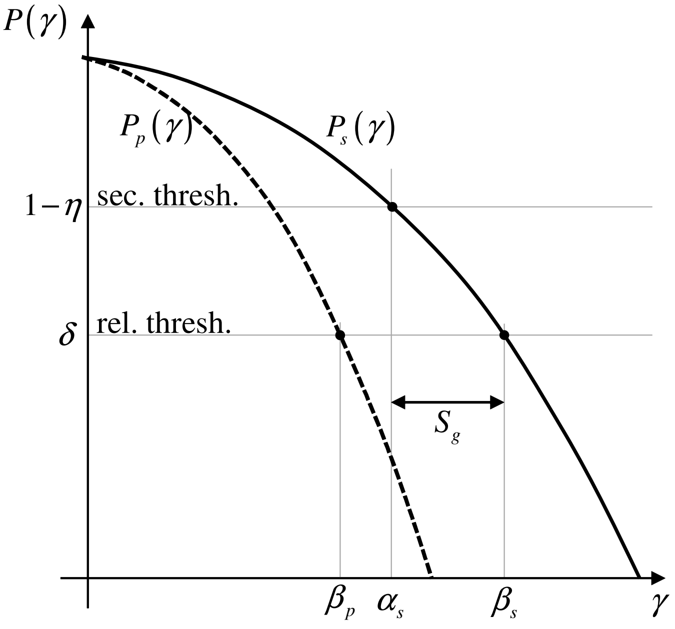


Figure 3.4: Expected block error rate curves for the public and secret messages as functions of the SNR.

improve as much as possible the error correcting performance over the most protected bits. Clearly this strategy leads to a performance degradation of the less protected bits.

3.4 Summary

In this chapter we have introduced the channel models and the metrics used to assess the security in a PLS scenario. We have discussed the wire-tap channel and BCC model and over the latter we have introduced the concept of UEP. Moreover, we have formally introduced the two considered security metrics, that are: the security gap and the Eve's equivocation rate. We have also discussed some important conditions under which the system is feasible and secure. Throughout the chapter, we have more times underlined that we are interested to measure the security achieved by practical coding schemes. Keeping this observation in mind, in the following some examples that use the introduced security metrics will be proposed.

Chapter 4

LDPC codes for the wire-tap channel

Coding for the Gaussian wire-tap channel is a well-established research topic, but there are some partially unsolved and challenging problems. One of these issues is to study the secrecy performance in the finite block length regime. Thus, our scope is to design practical LDPC codes optimized for this channel model, by assessing their performance in terms of secrecy rate.

To evaluate how far our codes are from optimality, which is achieved in asymptotic conditions, we use the eavesdropper equivocation rate defined in Sec. 3.2.2. This permits us to explore the capacity-equivocation regions of these codes in the finite length regime. We also propose a twofold code optimization tool which allows to design optimal codes in terms of the considered metrics. Similar twofold code optimizations have been proposed for the relay channel [62–64], but no solution has been presented for the wire-tap channel, at our best knowledge. We show that our approach allows to achieve great flexibility in the choice of the system parameters, as well as higher security levels w.r.t. previous solutions based on punctured LDPC codes [43].

4.1 Code design

The most common LDPC code decoding algorithm, which is an instance of the well-known belief propagation principle, is based on the exchange of soft messages about each received bit between the nodes of its Tanner graph. Therefore, the performance of an LDPC code depends on the connections among the nodes of its Tanner graph. Indeed, a variable node with a greater number of connected edges has more parity-check equations which verify its associated bit. On the other hand, check nodes with low degrees correspond to parity-check equations with less unknowns. The optimization of the code performance under message passing decoding consists in finding the best tradeoff between these two effects, and this usually requires irregular degree distributions. The well-known Density Evolution (DE) algorithm, proposed in [65], aims at optimizing the pair of degree distributions $(\lambda(x), \rho(x))$ in (2.1) and (2.2) based on the statistics of the decoder messages. However, by referring to the channel model depicted in Fig. 3.3 and differently from classical transmission problems, in our setting the same code (chosen by Alice) is used by three receivers: Bob, Eve and Frank, and the code optimization should take this into account.

Let us consider the notation and wire-tap channel model introduced in Sec. 3.2.2. When systematic encoder is used, the transmitted codeword is $\mathbf{c} = [\mathcal{M}|\mathcal{R}|\mathcal{P}]$, where $\mathcal{M}$ is the k_s bits secret message, $\mathcal{R}$ is the k_r bits random message and $\mathcal{P}$ is the r bits redundancy vector added by the encoder. Obviously, systematic encoding shall be avoided in security applications, especially if source coding is not optimal. In fact, in such a case, Eve could look at the systematic part of the received codeword and gather some information about the secret message parts which are less affected by errors. In practical systems, systematic encoding can be easily avoided by scrambling the information bits prior to encoding [61]. Having this clearly in mind, for our code design and analysis purposes it is convenient to keep the assumption of systematic encoding. Under this hypothesis, the code $\mathbf{H}$ matrix can be divided into three blocks as shown in Fig. 4.1, corresponding to the three parts of $\mathbf{c}$. Bob must use the whole matrix to decode for both the secret and random

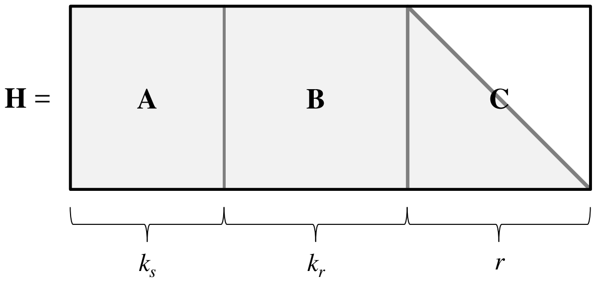


Figure 4.1: Parity-check matrix of the considered codes.

messages (since he does not know in advance any of them), although in the end he is interested only in $\mathcal{M}$. Eve is in the same condition, although she receives the signal through a different channel. Frank, instead, has perfect knowledge of $\mathcal{M}$, and only needs to decode for $\mathcal{R}$. Therefore, he can precompute $\mathbf{A} \cdot \mathcal{M}^\top = \mathbf{s}$. Then, he can use $\mathbf{s}$ as a syndrome vector and focus on the reduced parity-check system

$$[\mathbf{B}|\mathbf{C}] \cdot [\mathcal{R}|\mathcal{P}]^\top = \mathbf{H}' \cdot \mathbf{c}'^\top = \mathbf{s}.$$

Obviously, decoding for a vector having an all-zero syndrome or a different syndrome is equivalent, due to the code linearity. Hence, Frank performs decoding through the LDPC code defined by $\mathbf{H}'$, having rate $R_F = k_r/(k_r + r)$. The code rate for Bob instead coincides with the overall code rate, i.e., $R_B = k/n$. It follows that $R_F = \frac{R_B - R_s}{1 - R_s}$. In the setting we consider, it is important that both Bob's and Frank's codes are optimized. In fact, an optimized code for Bob allows to approach the channel capacity, which is the ultimate limit for the reliability target. An optimized code for Frank instead serves to achieve the desired η with the smallest possible SNR. Since Frank's SNR is the same as Eve's, this reduces Eve's channel capacity C_E.

4.2 Code optimization

We propose an optimization strategy for Bob's and Frank's codes based on the DE algorithm, which is commonly used to optimize a single code, with some modifications in order to consider the joint optimization target.

In Section 4.2.1 we briefly recall the steps of the single code optimization and then in Section 4.2.2 we describe our strategy for the joint code optimization. As in [65], we use the DE algorithm with Gaussian approximation of the decoder messages.

4.2.1 Single optimization

The DE algorithm is well-known in the literature; therefore, for the sake of brevity, we report here only the main equations of [65], as they are used in the proposed joint code optimization.

Given $\rho(x)$, R and d_v, the optimization of $\lambda(x)$ of a single code is possible by applying the following constraints:

C_1 - Rate constraint

$$\sum_{i=2}^{d_v} \frac{\lambda_i}{i} = \frac{1}{1-R} \sum_{i=2}^{d_c} \frac{\rho_i}{i}.$$

C_2 - Proportion distribution constraint

$$\sum_{i=2}^{d_v} \lambda_i = 1.$$

C_3 - Convergence constraint (from [65, Eq. (16)])

$$r > h(s,r), \quad \forall r \in (0, \phi(s)) \tag{4.1}$$

where $s = \frac{2}{\sigma^2}$, σ^2 being the noise variance, and $\phi(\cdot)$ will be defined in (4.3). For $0 < s < \infty$ and $0 < r \leq 1$, we define $h(s,r)$ in (4.1) as follows

$$h(s,r) = \sum_{i=2}^{d_v} \lambda_i h_i(s,r)$$

where

$$h_i(s,r) = \phi\left(s + (i-1)\sum_{j=2}^{d_c}\rho_j\phi^{-1}\left(1-(1-r)^{j-1}\right)\right). \tag{4.2}$$

In (4.1) and (4.2),

$$\phi(x) = \begin{cases} 1 - \frac{1}{\sqrt{4\pi x}}\int_{-\infty}^{+\infty}\tanh\frac{u}{2}e^{-\frac{(u-x)^2}{4x}}du, & \text{if } x > 0 \\ 1, & \text{if } x = 0. \end{cases} \tag{4.3}$$

Condition (4.1) is equivalent to impose that $r_l(s) \to 0$ for $l \to \infty$ [65], with $r_l = h(s, r_{l-1})$ and $r_0 = \phi(s)$.

C_4 - Stability condition

$$\lambda_2 < \frac{e^{\frac{1}{2\sigma^2}}}{\sum_{j=2}^{d_c}\rho_j(j-1)}. \tag{4.4}$$

In the single code optimization, the code threshold s^* is defined as the minimum s for which the constraints $[C_1 - C_4]$ are satisfied. From the definition of s, it is evident that s^* corresponds to the maximum noise variance σ^2 for which the constraints are verified.

4.2.2 Joint optimization

In order to perform the joint optimization of Bob's and Frank's codes, we must impose that Frank's code is somehow *contained* in Bob's code (in other terms, that Frank's parity-check matrix is a sub-matrix of Bob's parity-check matrix). Therefore, in addition to the constraints in Section 4.2.1, we need another condition. To obtain this further constraint, through (2.4) we introduce the polynomial $\tilde{\lambda}(x)$ which corresponds to the node perspective of $\lambda(x)$.

Since Bob's parity-check matrix contains Frank's parity-check matrix, the number of variable nodes in Bob's Tanner graph having some fixed degree must be greater than or equal to that of variable nodes in Frank's Tanner graph having the same degree. Hence, we must take into account the following further constraint [66]

C_5 - Joint optimization constraint

$$\tilde{\lambda}_{B,i} \geq \tilde{\lambda}_{F,i}, \quad \forall i \in \left[2, 3, 4, \ldots, d_v^{(F)}\right],$$

where $\tilde{\lambda}_B(x)$ and $\tilde{\lambda}_F(x)$ are Bob's and Frank's variable node degree distributions from the node perspective, respectively, and $d_v^{(F)}$ is Frank's maximum variable node degree. C_5 adds to $[C_1 - C_4]$ and the optimum $\lambda_B(x)$ must satisfy all these constraints.

In the joint optimization algorithm, we define the convergence threshold as the maximum of $\zeta = \sigma_B^2 + \sigma_F^2$, denoted by ζ^*, for which the constraints $[C_1 - C_5]$ are satisfied. In the expression of ζ, σ_B^2 and σ_F^2 are Bob's and Frank's noise variances, respectively. It should be noted that this procedure differs from optimizing the two codes separately. In fact, in principle, we could first optimize Frank's code, and then try to optimize Bob's code by taking account the degree distributions obtained for Frank and the constraint C_5. This, however, could impose too strong constraints on Bob's code degree distribution, thus preventing to find a good solution for him, too. In fact, some solutions may exist for which neither Bob's nor Frank's degree distributions are individually optimal, but their joint performance is optimal.

As in [65], in order to design the check node degree distribution, we adopt a concentrated distribution (i.e., with only two degrees, concentrated around the mean).

4.3 Numerical results

In order to provide some practical examples, we use the procedure described in Section 4.2.2 to design several codes with $d_v^{(B)} = d_v^{(F)} = 50$. We consider code rates $R = R_B = 0.35, 0.5, 0.75$ and several values of $R_s < R_B$. The degree distributions obtained through the joint optimization procedure are reported in Tab. 4.1.

Table 4.1: Degrees distribution pairs obtained with the technique described in Section 4.2.2 for several values of R_s and R_B.

R_s	0.33		0.4		0.45		0.5		0.6		0.7		0.725	
R_B	0.35		0.5		0.5		0.75		0.75		0.75		0.75	
i	$\lambda_{F,i}$	$\lambda_{B,i}$	$\lambda_{F,i}$	$\lambda_{B,i}$	$\lambda_{F,i}$	$\lambda_{B,i}$	$\lambda_{F,i}$	$\lambda_{B,i}$	$\lambda_{F,i}$	$\lambda_{B,i}$	$\lambda_{F,i}$	$\lambda_{B,i}$	$\lambda_{F,i}$	$\lambda_{B,i}$
2	0.6677	0.1858	0.4208	0.2259	0.6181	0.2070	0.2187	0.1588	0.2066	0.1382	0.4257	0.1712	0.6181	0.1300
3	0.2279	0.2291	0.1656	0.1701	0.2117	0.2123	0.1826	0.1851	0.1436	0.1549	0.1763	0.1787	0.2117	0.2128
4	-	-	0.1192	0.1195	-	-	-	-	0.0280	0.0278	0.1014	0.1029	-	-
5	-	-	-	-	0.1445	0.1471	0.0497	0.0449	0.0123	0.0112	-	-	0.1445	0.1786
6	0.0267	0.0252	-	-	0.0246	0.0254	0.0365	0.0378	0.0248	0.0267	-	-	0.0246	0.0354
7	0.0767	0.0751	-	-	-	-	0.0309	0.0317	0.0999	0.1054	-	-	-	-
8	-	-	0.0057	0.0061	-	-	0.1662	0.1683	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	0.0539	0.0574	0.1321	0.1410	-	-
10	-	-	0.2877	0.2907	-	-	-	-	0.0413	0.0409	0.1635	0.1639	-	-
11	-	0.0249	-	-	-	-	-	-	0.0144	0.0175	-	-	-	-
12	-	0.1792	-	-	-	-	-	-	0.0126	0.0119	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0359
14	-	-	-	-	-	0.0184	-	-	-	-	-	-	-	0.0625
15	-	-	-	-	-	0.2779	-	-	-	-	-	-	-	0.1561
19	-	-	-	-	-	-	-	-	0.0637	0.0713	-	-	-	-
20	-	-	-	-	-	-	0.0154	0.0124	0.0050	0.0190	-	-	-	0.0031
21	-	-	-	0.0096	-	-	0.0747	0.0954	-	-	-	-	-	0.0103
22	-	-	-	-	-	-	0.0666	0.0659	-	-	-	-	-	0.0014
23	-	-	-	-	-	0.1109	0.0568	0.0549	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-	-	-	-	0.0307	-	-
25	-	-	-	0.0697	-	-	0.1007	0.1016	-	-	-	0.2106	-	-
26	-	-	-	0.1074	-	-	-	-	-	-	-	-	-	-
32	-	-	-	-	-	-	-	-	-	-	-	-	-	0.1727
34	-	0.0203	-	-	-	-	-	-	-	-	-	-	-	-
36	-	0.0844	-	-	-	-	-	-	-	-	-	-	-	-
38	-	0.0716	-	-	-	-	-	-	-	-	-	-	-	-
39	-	0.0652	-	-	-	-	-	-	0.2929	0.2946	-	-	-	-
40	-	0.0382	-	-	-	-	-	-	-	-	-	-	-	-
50	0.0010	0.0010	0.0010	0.0010	0.0011	0.0010	0.0012	0.0432	0.0010	0.0232	0.0010	0.0010	0.0011	0.0012

Concerning the choice of the degrees of x allowed in the two polynomials, the only constraints we impose are that they must not overcome the maximum values $d_v^{(B)}$ and $d_v^{(F)}$, and that the number of nodes of degree 2 must be such that the stability condition (4.4) is met by both codes.

To provide some examples of finite length codes, we consider LDPC codes with length $n_1 = 10000$ and $n_2 = 50000$; Frank's code length is then obtained from these values by considering the submatrix $\mathbf{H}'$. Once having defined the degree distributions, the parity-check matrices are designed through the Progressive Edge Growth (PEG) algorithm [67]. The numerical results are obtained by considering, for all coding schemes, binary phase shift keying (BPSK) modulation over the AWGN channel. When considering finite length codes, through numerical simulations we are able to determine the values of the SNR per bit (E_b/N_0) that ensure a given CER. These values are reported in Tab. 4.2, for both Bob and Frank, assuming CER $= 10^{-2}$ and several values of R_s. In the table, the values of $\left.\frac{E_b}{N_0}\right|_{th}$ identify the codes convergence thresholds obtained through DE. These values represent the ultimate performance bounds achievable in asymptotic conditions (i.e., infinite code length). The values of $\left.\frac{E_b}{N_0}\right|_{n_1}$ and $\left.\frac{E_b}{N_0}\right|_{n_2}$ instead represent the SNR working points, estimated through simulations, for the practical codes with lengths n_1 and n_2, respectively. We observe from Tab. 4.2 that, for Bob's code, the finite length performance approaches the asymptotic threshold as the code rate increases. Indeed, for $R_B = 0.75$ and code length equal to n_1 and n_2, the gap between the asymptotic threshold and the finite length codes performance is about 0.4 dB and 0.2 dB, respectively.

As a security metric we use the lower bound R_e^* on the equivocation rate, computed according to (3.6) and the values in Tab. 4.2. The secrecy capacity C_s, that represents the ultimate limit achievable by the equivocation rate, is also computed for the cases of interest, and used as a benchmark. We compute C_s under the hypothesis of ideal coding, i.e., that Bob's and Frank's code rates coincide with the respective channel capacities. Since Frank's and Eve's channels coincide, it follows that $C_s = R_B - R_F = R_s \frac{1-R_B}{1-R_s}$. In order to assess if practical codes can approach the perfect secrecy condition (3.3), we then compute the fractional lower bound on the equivocation rate $\widetilde{R_e^*} = R_e^*/R_s$

Table 4.2: SNR working points of the considered coding schemes for several values of R_s and R_B; the values of $\frac{E_b}{N_0}$ are in dB.

R_s	R_B	$\left.\frac{E_b}{N_0}\right\|_{th}^{B}$	$\left.\frac{E_b}{N_0}\right\|_{th}^{F}$	$\left.\frac{E_b}{N_0}\right\|_{n_1}^{B}$	$\left.\frac{E_b}{N_0}\right\|_{n_1}^{F}$	$\left.\frac{E_b}{N_0}\right\|_{n_2}^{B}$	$\left.\frac{E_b}{N_0}\right\|_{n_2}^{F}$
0.33	0.35	-0.14	-1.52	1.10	3.82	0.72	3.18
0.4	0.5	0.41	-0.52	1.00	0.76	0.78	0.44
0.45	0.5	0.42	-0.69	1.12	1.22	0.82	0.98
0.5	0.75	1.73	0.38	2.14	1.17	1.94	0.84
0.6	0.75	1.72	-0.14	2.12	0.98	1.97	0.63
0.7	0.75	1.75	-0.52	2.13	0.91	1.92	0.60
0.725	0.75	1.75	-0.69	2.18	2.11	1.96	1.59

both in asymptotic conditions and in the finite code length regime, and compare its values with the fractional secrecy capacity $\widetilde{C_s} = C_s/R_s = \frac{1-R_B}{1-R_s}$. The values so obtained are reported in Fig. 4.2, for the same values of R_s considered in Tabs. 4.1 and 4.2. As an example, for the considered code parameters and $R_s = 0.725$, we find that in asymptotic conditions the designed codes approach the secrecy capacity and the perfect secrecy condition. Notably, even using relatively short codes, with 10000-bit codewords, the fractional equivocation rate is close to 0.8. For the sake of comparison, we consider some results reported in [43] for the scheme based on punctured LDPC codes. The corresponding points are marked with an asterisk in Fig. 4.2. Those results consider codes with length $n = 10^6$, at which the performance of LDPC codes usually approaches the DE threshold. However, the asymptotic performance achieved by the degree distributions found through the proposed approach exhibits some gain at the same secret message rates. Furthermore, for $R_s = 0.43$, even our schemes with $n = 10000$ and $n = 50000$ outperform that proposed in [43] with $n = 10^6$.

From Fig. 4.2 it results that the best performance in terms of Eve's equivocation rate is achieved when the secret message rate approaches the code rate. This could seem counterintuitive, since suggests to use few random bits to confuse the eavesdropper. However, in this condition R_F is small and Frank is able to reach the desired performance at low SNR. The latter coincides with Eve's channel SNR, therefore Eve's equivocation rate is large.

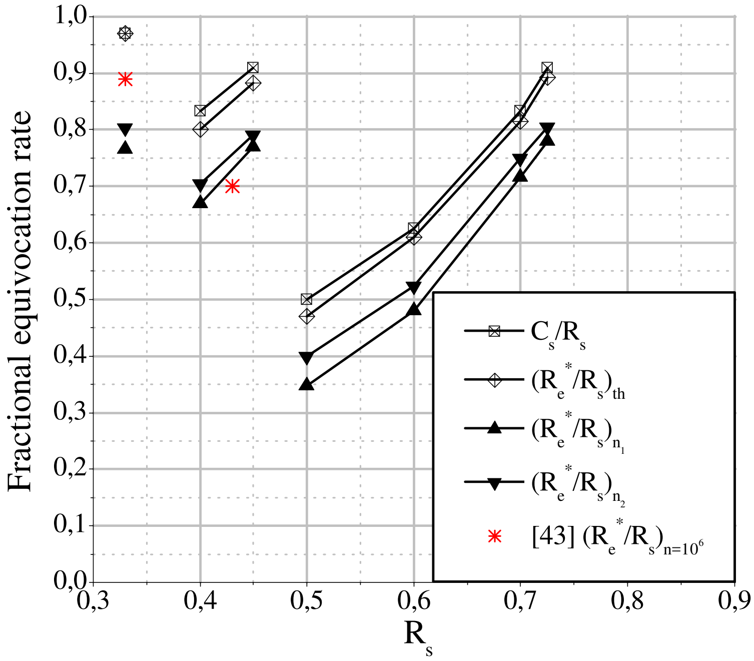


Figure 4.2: Comparison between $\frac{C_s}{R_s}$, $\frac{R_e^*}{R_s}$ calculated through the asymptotic threshold values, $\frac{R_e^*}{R_s}$ for code length n_1, and $\frac{R_e^*}{R_s}$ for code length n_2, as a function of R_s.

On the other hand, imposing that Eve's channel has a too low SNR is not realistic, therefore some randomness shall always be used in order to relax the constraints on Eve's channel quality.

4.4 Summary

In this chapter, by using suitable reliability and security metrics, we have computed performance bounds in the asymptotic regime and assessed the achievable performance under the hypothesis of finite codeword lengths. To achieve this aim we have considered the case of a wire-tap channel with a fictitious receiver. In this scenario, we have proposed a strategy that, based on the well known DE algorithm, allow us to obtain a twofold optimization of the code. Through the concept of fractional equivocation rate, the performance obtained with our solution and those presented in previous works have been compared. Results show that our codes are able to approach the ultimate performance limits even with relatively small block lengths.

Chapter 5

LDPC codes for the BCC

In this chapter we consider the case of a BCC and show as LDPC codes with UEP capabilities are preferable in this context to satisfy the feasibility conditions in (3.7). As explained in Sec. 3.3.1, to achieve a feasible system different error rates are needed for the public and secret part of the message. For this reason, we use irregular LDPC codes, since they have an inherent UEP property. In fact, by considering the code Tanner graph, the variable nodes with the higher degrees in $\lambda(x)$ have greater number of connected check nodes, i.e., the corresponding codeword bit is involved in a larger number of parity check equations. Thus, a different protection level can be achieved by mapping the highest degrees of $\lambda(x)$ over the most protected bits, while the other degrees are associated to the less protected bits. Since one of the main aims of this chapter is to compare the performance achieved through finite length codes, we resort to the concept of security gap defined in Sec. 3.3.1 to accomplish this goal.

5.1 UEP LDPC vs. no UEP LDPC codes

In this section we assess LDPC codes with and without UEP capabilities. This way, we can observe as codes with this property are useful in a BCC. To achieve our aim, first we consider two separate codes for the public and secret part of the massage, then we compare their results with those obtained with a single UEP LDPC.

In order to increase the difference between the two levels of protection against noise for the public and secret messages, we can resort to message concatenation [61] and all-or-nothing transforms (AONTs) [68]. Let us suppose that L secret messages, each with length k_s, are concatenated and then transformed through an AONT. The transformed string is then transmitted in L fragments, which replace the original messages. Only if all of them are correctly received, the AONT can be inverted and the L secret messages successfully obtained; otherwise, none of them can be even partially recovered. Through concatenation, the error probability on each secret message becomes

$$P_s^{(L)}(\gamma) = 1 - [1 - P_s(\gamma)]^L \geq P_s(\gamma).$$

Hence, for a given $\gamma^{(E)} = \bar{\gamma}^{(E)}$, if $P_s(\bar{\gamma}^{(E)})$ does not meet the security condition, we can resort to message concatenation and AONTs, and find a suitable value of L such that $P_s^{(L)}(\bar{\gamma}^{(E)})$ overcomes the security threshold.

Obviously, when we introduce message concatenation and AONTs, we must replace $P_s(\gamma)$ with $P_s^{(L)}(\gamma)$ also for Bob. Hence, the use of these tools is paid in terms of the SNR working point for Bob, which increases w.r.t. the case without concatenation. In addition, increasing L increases the latency for receiving the secret message. Concerning the implementation of an AONT, several examples can be found in the literature. For the purposes of this study, we observe that scrambling the information bits through a linear (and dense) map can achieve features similar to those of an AONT, thanks to the randomness of the errors induced by the channel [61].

We note that AONTs can also be used, at higher layers, to achieve some desired level of computational security. In fact, the condition (3.7d) only guarantees that Eve's decoder has a high error probability on the secret blocks. However, this does not exclude that some secret blocks may be correctly decoded by Eve. Furthermore, even when Eve's decoder is in error, some bits within the block may be correct. Therefore, as often occurs in PLS and as described in Sec. 2.1, this setting represents a substrate which must be exploited by higher layer protocols to achieve some desired level of computational security.

5.1.1 Using two different LDPC codes

Let us suppose to use two different LDPC codes to encode the public and the secret information blocks. For the sake of simplicity, our choice is to split the transmitted frame into two codewords of length $n/2$. One of these two codewords is obtained from an LDPC code $LDPC_p$, having rate R_p, and carries the k_p public information bits. The other codeword belongs to an LDPC code $LDPC_s$, with rate R_s and corresponds to the k_s secret information bits. Since the two codes have the same length, provided that they are well designed, it must be $R_p < R_s$ to achieve a higher level of protection against noise for the public information block, to meet the conditions (3.7).

Example 5.1.1 Let us consider $n = 2048$ and two LDPC codes with the following parameters:

- LDPC$_p$: length 1024, rate $R_p = 0.2$.
- LDPC$_s$: length 1024, rate $R_s = 0.8$.

Their variable and check node degree distributions have been optimized through the tools available in [69]. Concerning the choice of the node degrees, for the variable nodes we have used the same degrees we will consider in Example 5.1.2, while for the check nodes we have considered a concentrated distribution, as introduced in Sec. 2.2.1.

The resulting variable and check node degree distributions are, respectively,

$$\begin{aligned}\lambda(x) &= 0.1765x^{19} + 0.2392x^{18} + 0.0638x^{17} + 0.0988x^{16} \\ &\quad + 0.0117x^{15} + 0.1976x^{2} + 0.2124x, \\ \rho(x) &= 0.1607x^{6} + 0.8393x^{5},\end{aligned}$$

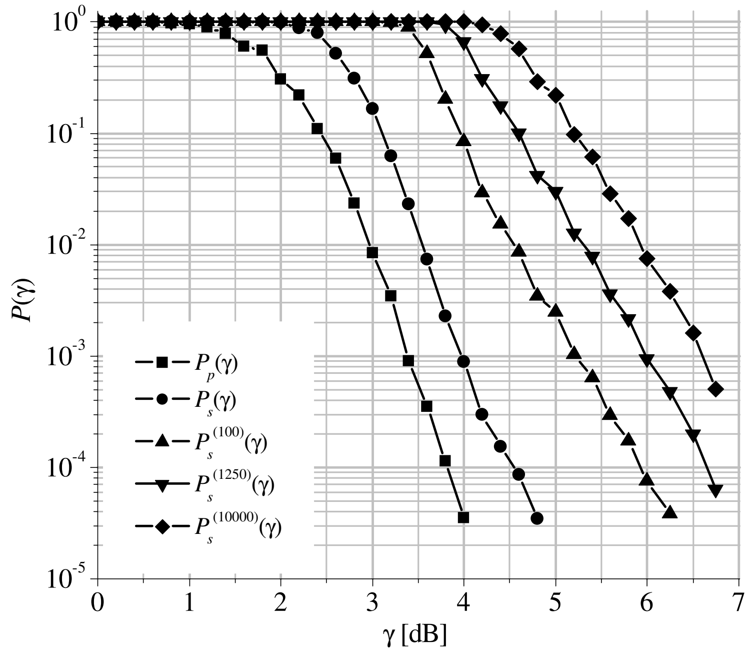


Figure 5.1: Error rate curves for two different LDPC codes with length $n = 1024$ and rates $R_p = 0.2, R_s = 0.8$, with and without concatenation of the secret messages (indicated in the superscript of $P_s(\gamma)$).

for the first code, and

$$\lambda(x) = 0.8815x^2 + 0.1185x,$$
$$\rho(x) = 0.1708x^{14} + 0.8292x^{13},$$

for the second code. These degree distributions have been used to design the parity-check matrices of the two codes LDPC$_p$ and LDPC$_s$ through the *zigzag-random* construction [67,70]. The performance of these codes, assessed through numerical simulations, and using the log-likelihood ratio sum product algorithm (LLR-SPA) [71] with 100 maximum iterations for decoding, is reported in Fig. 5.1, also considering some examples of concatenation of the secret message ($L = 100, 1250, 10000$).

5.1.2 Using a single UEP LDPC code

Let us suppose to use a single UEP LDPC code with length n. Most of the existing works on UEP LDPC codes aim at designing codes with three PCs:

- PC1 contains $k_1 < k$ information bits which are those most protected against noise.
- PC2 contains $k_2 = k - k_1$ information bits which are less protected against noise than those in PC1.
- PC3 contains the whole redundancy part ($r = n - k$ bits).

Codes of this kind are suitable for the considered scenario. In fact, given an UEP LDPC code with the three PCs outlined above, we can map the public message bits into PC1 (i.e., $k_p = k_1$) and the secret message bits into PC2 (i.e., $k_s = k_2$).

To design LDPC codes with good UEP properties, several approaches have been proposed in the literature [70, 72, 73]. All these methods aim at optimizing the node degree distributions in such a way that the variable node degrees are spanned in a wide range, and good convergence thresholds are achieved under iterative decoding. Then the variable nodes with the highest degrees are mapped into the bits of PC1, whereas the others form PC2 and PC3 (depending on their association with information or redundancy bits).

Once the variable node degree distribution $\lambda(x)$ has been designed, the number of bits in PC1 can be easily obtained by converting $\lambda(x)$ from the edge perspective to the node perspective with (2.4), and then computing the fraction of variable nodes with the highest degrees, that are those in PC1. As discussed in Sec. 2.2.1 we adopt a concentrated distribution for the check node degrees, as already done for the case of two different LDPC codes in Sec. 5.1.1.

Example 5.1.2 Let us consider the following UEP LDPC variable node degree distribution taken from [73, Tab. 3], with some minor modifications

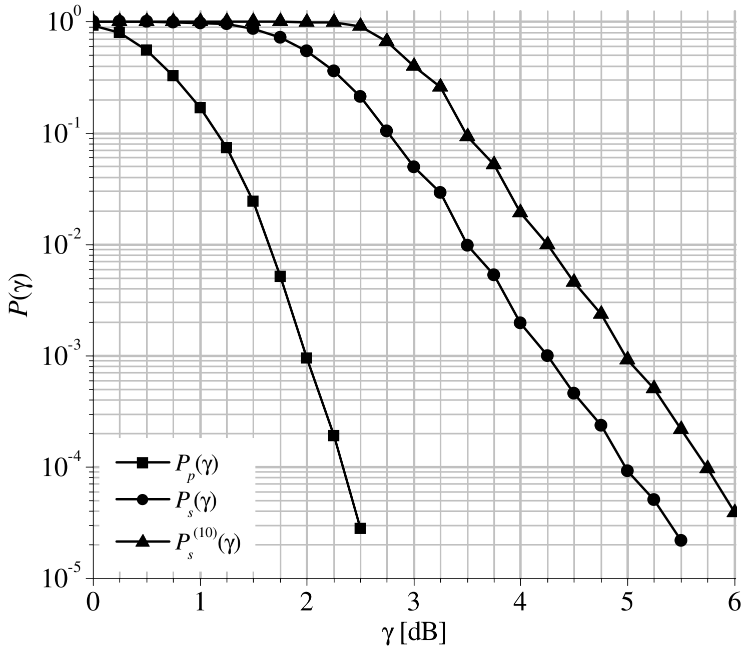


Figure 5.2: Error rate curves for an UEP LDPC code with length $n = 1024$ and PC1 and PC2 with proportions $20\% - 80\%$, with and without concatenation of secret messages (indicated in the superscript of $P_s(\gamma)$).

to adapt the proportion between PC1 and PC2 in such a way that it coincides with the one used in Example 5.1.1

$$\begin{aligned}\lambda(x) = {} & 0.0025x^{19} + 0.0009x^{18} + 0.0031x^{17} + 0.0630x^{16} \\ & + 0.3893x^{15} + 0.2985x^2 + 0.2427x.\end{aligned}$$

The corresponding node perspective distribution is

$$\begin{aligned}\tilde{\lambda}(x) = {} & 0.0005x^{20} + 0.0002x^{19} + 0.0007x^{18} + 0.0151x^{17} \\ & + 0.0835x^{16} + 0.4054x^3 + 0.4946x^2.\end{aligned}$$

The nodes in PC1 are those with degree ≥ 16, while those with degree ≤ 3 are in PC2 or PC3 depending on their association to information bits or redundancy bits. This way, we find that PC1 and PC2 contain, respectively,

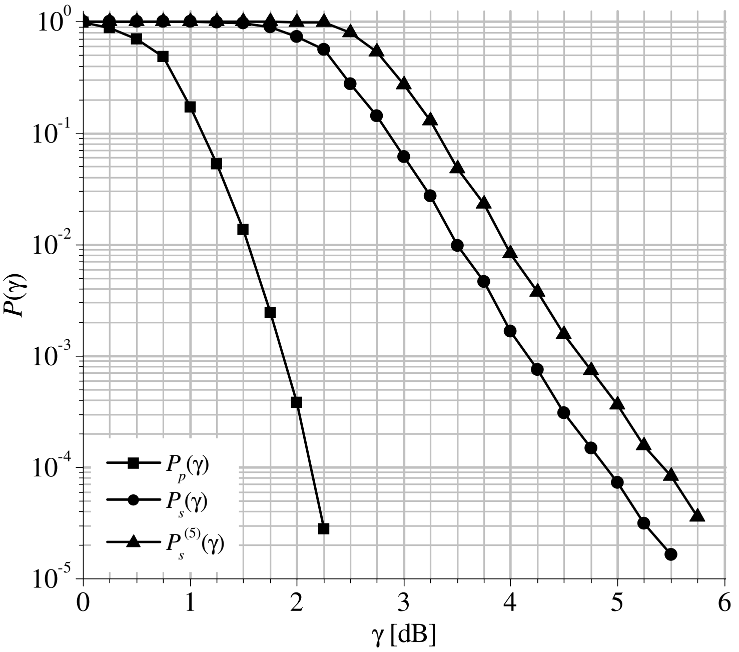


Figure 5.3: Error rate curves for an UEP LDPC code with length $n = 2048$ and PC1 and PC2 with proportions $20\% - 80\%$, with and without concatenation of secret messages (indicated in the superscript of $P_s(\gamma)$).

20% and 80% of the information bits. By using this distribution for the variable nodes and a concentrated degree distribution for the check nodes, we have designed three UEP LDPC codes with $n = 1024, 2048$ and 4096. As above, their parity-check matrices have been obtained through the zigzag random construction. The performance obtained by these codes under LLR-SPA decoding with 100 maximum iterations is reported in Figs. 5.2-5.4. Some examples of the use of concatenation of secret messages are also shown in Figs. 5.2 and 5.3.

5.1.3 Performance assessment

We fix two values for the reliability and security thresholds in (3.7), namely, $\delta = 10^{-4}$ and $\eta = 0.1$. Actually, one could think that a decoding error probability equal to 0.9 for Eve does not represent a condition of sufficient security. However, we remind that this setting only provides a sub-

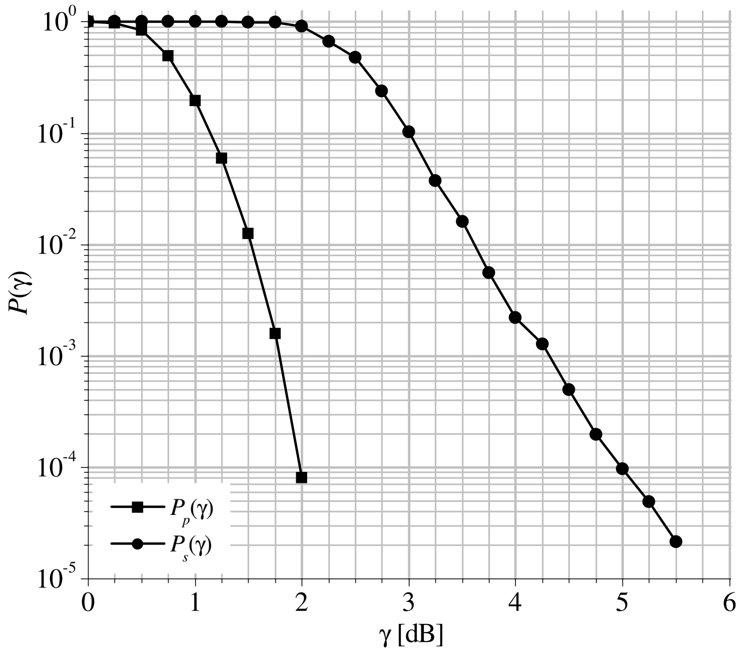


Figure 5.4: Error rate curves for an UEP LDPC code with length $n = 4096$ and PC1 and PC2 with proportions $20\% - 80\%$.

strate over which any desired level of computational security can be achieved through higher layer techniques, as described in Section 2.1. Furthermore, our purpose is just to compare the considered coding schemes, not to define any absolute security level. For each coding scheme, we choose the smallest value of L concatenated secret messages such that the system is feasible, i.e., $\alpha_s \geq \beta_p$ in (3.9). Finally, we compute the values of β_s and the security gap S_g, according to (3.10).

The results obtained by considering the coding schemes in Examples 5.1.1 and 5.1.2 are reported in Tab. 5.1 [74]. From these examples, we observe that using UEP LDPC codes is actually effective for implementing practical transmission schemes over the BCC, since the system feasibility is achieved even with a small number of concatenated messages, and the security gap values are in the order of $3 - 3.3$ dB. Increasing the block length improves performance: apart from a small reduction in the security gap, longer codes require a smaller SNR for Bob and less concatenation. In fact, while an UEP

Table 5.1: Performance assessment of the coding schemes in Examples 5.1.1 and 5.1.2 ($\beta_p, \alpha_s, \beta_s$ and S_g are in dB) .

Scheme	n	L	β_p	α_s	β_s	S_g
UEP	1024	10	2.34	2.46	5.74	3.28
non-UEP	2048	1250	3.81	3.83	6.65	2.82
UEP	2048	5	2.13	2.37	5.43	3.06
UEP	4096	1	1.99	2.01	4.98	2.97

LDPC code with $n = 1024$ requires $L = 10$ and $\beta_s = 5.74$ dB, by increasing n to 4096 we reduce β_s to less than 5 dB (thus reducing Bob's SNR), and we no longer need the concatenation of secret messages for the system to be feasible. Instead, using two different codes is not a good choice, as we observe by comparing the second and the third rows of Tab. 5.1. In fact, for $n = 2048$, the two non-UEP LDPC codes considered in Example 5.1.1 achieve some small reduction in the security gap, but they require a very high level of concatenation ($L = 1250$) for the system to be feasible. This increases the minimum SNR for Bob by more than 1 dB, and also has detrimental effects on the system latency.

5.2 Fading BCC

In the previous section, we have supposed a Gaussian channel between Alice and the receivers. In order to investigate the performance achieved by UEP LDPC codes in a more realistic scenario, in the following we consider a BCC also affected by fading. In particular, we aim at designing suitable coding and modulation schemes to achieve a feasible communication in a QSFC. A pictorial example of the considered channel model is reported in Fig. 3.1.

The SNRs on the two channels, noted by $\gamma^{(B)}$ and $\gamma^{(E)}$, result from the combination of the AWGN contribution and the Rayleigh fading contribution. The average SNRs are equal to $\bar{\gamma}^{(B)}$ and $\bar{\gamma}^{(E)}$ for Bob and Eve, respectively. According to the Rayleigh fading model and (3.1), the probability density functions of $\gamma^{(B)}$ and $\gamma^{(E)}$ are

$$p_{\gamma^{(B)}}(x) = \frac{1}{\bar{\gamma}^{(B)}} e^{-x/\bar{\gamma}^{(B)}}, \qquad x \geq 0 \tag{5.1a}$$

$$p_{\gamma^{(E)}}(x) = \frac{1}{\bar{\gamma}^{(E)}} e^{-x/\bar{\gamma}^{(E)}}, \qquad x \geq 0 \tag{5.1b}$$

We suppose to have average channel state information (CSI), that is, Alice knows the values of $\bar{\gamma}^{(B)}$ and $\bar{\gamma}^{(E)}$. Several works in the literature assume to have perfect CSI, that is, Alice knows exactly the values of $\gamma^{(B)}$ and $\gamma^{(E)}$ for each transmitted codeword. We prefer to make the assumption of having only average CSI, since it is more realistic for a practical system like the one we want to address.

5.2.1 System feasibility and outage

Let us suppose that we use a coding and modulation scheme which offers a higher level of protection against noise to the public information part w.r.t. the secret information part. Typical error rate curves for this case are reported in Fig. 3.4. As explained in Sec. 3.3.1, when some fluctuations on the Eve's channel may occur, the condition in which she has a degraded channel w.r.t. Bob does not suffice to make the system feasible as it occurs for the wire-tap channel model.

Therefore, provided that the system is feasible, in the following we assess and compare different coding and modulation schemes by computing the security gap S_g.

Bob's outage

When Bob receives a transmitted codeword, he must be able to meet the reliability conditions (3.7a) and (3.7c). From (3.8) we have that both these conditions are met when $\gamma^{(B)} \geq \beta_s$, hence an outage event occurs when $\gamma^{(B)} < \beta_s$. We denote by ξ the probability of such an event, and from (5.1a) we have

$$\xi = P\left\{0 \leq \gamma^{(B)} < \beta_s\right\} = \int_0^{\beta_s} p_{\gamma^{(B)}}(x)dx = 1 - \exp\left(-\frac{\beta_s}{\bar{\gamma}^{(B)}}\right).$$

We suppose to have average CSI on both channels, hence the transmission power can be chosen such that the probability of outage is not greater than some fixed value $\xi_{\max}$, that is

$$\bar{\gamma}^{(B)} \geq \bar{\gamma}_{\min}^{(B)} = -\frac{\beta_s}{\ln\left(1 - \xi_{\max}\right)}. \tag{5.2}$$

Eve's outage

When Eve receives a transmitted codeword, two outage events can occur:

- The reliability condition (3.7b) on the public information is not met. We define ω_r the probability of this event.
- The security condition (3.7d) on the secret information is not met. We define ω_s the probability of this event.

Based on (5.1b), we have

$$\omega_r = P\left\{0 \leq \gamma^{(E)} < \beta_p\right\} = \int_0^{\beta_p} p_{\gamma^{(E)}}(x)dx = 1 - \exp\left(-\frac{\beta_p}{\bar{\gamma}^{(E)}}\right)$$

and

$$\omega_s = P\left\{\gamma^{(E)} > \alpha_s\right\} = \int_{\alpha_s}^{\infty} p_{\gamma^{(E)}}(x)dx = \exp\left(-\frac{\alpha_s}{\bar{\gamma}^{(E)}}\right).$$

Since the two outage events are incompatible, the overall outage probability for Eve is

$$\omega = \omega_r + \omega_s = 1 - \exp\left(-\frac{\beta_p}{\bar{\gamma}^{(E)}}\right) + \exp\left(-\frac{\alpha_s}{\bar{\gamma}^{(E)}}\right). \tag{5.3}$$

As we suppose to have average CSI on both channels, we can assume that $\bar{\gamma}^{(E)}$ is chosen in such a way that ω equals its minimum, $\omega_{\min}$. This optimal value of $\bar{\gamma}^{(E)}$, named $\bar{\gamma}^{(E)}_{\mathrm{opt}}$, can be easily found by computing the derivative of ω w.r.t. $\bar{\gamma}^{(E)}$, that is,

$$\frac{d\omega}{d\bar{\gamma}^{(E)}} = \frac{\alpha_s \exp\left(-\frac{\alpha_s}{\bar{\gamma}^{(E)}}\right) - \beta_p \exp\left(-\frac{\beta_p}{\bar{\gamma}^{(E)}}\right)}{(\bar{\gamma}^{(E)})^2}.$$

Then, $\bar{\gamma}^{(E)}_{\mathrm{opt}}$ is obtained by setting $\frac{d\omega}{d\bar{\gamma}^{(E)}} = 0$. This way, we have

$$\bar{\gamma}^{(E)}_{\mathrm{opt}} = \frac{\beta_p - \alpha_s}{\ln\left(\frac{\beta_p}{\alpha_s}\right)}.$$

Therefore, by taking Bob's and Eve's outage probabilities (i.e., $\xi_{\max}$ and $\omega_{\min}$) into account, we can compute the security gap as

$$S_g = \frac{\bar{\gamma}^{(B)}_{\min}}{\bar{\gamma}^{(E)}_{\mathrm{opt}}}.$$

5.2.2 Numerical results

As in Sec. 5.1.2, also in this case we consider an UEP LDPC code with three PCs and the same variable node degree distributions in Example 5.1.2. Moreover, our code has $n = 4096$ and overall rate $R = 1/2$ and its parity check matrix is constructed through the *zigzag-random* approach. Since we use UEP LDPC codes to map the first two PCs to the public and the secret information bits, in the case of fading channel, it is advisable to ensure that a high level of separation exists between these two classes, in such a way that possible fluctuations of the error rate on one of them do not affect the error rate on the other. For this purpose, we design the parity-check matrix in such a way as to keep the number of parity-check equations which are common between the first two PCs as small as possible, while still achieving good performance. To achieve this aim, the bits in the PC1 are always transmitted by using BPSK modulation, while for the bits in the PC2 several quadrature amplitude modulation (QAM) formats have also been tested. For the latter, we have adopted the labeling known as Yarg [75], which has been suitably designed for physical layer security contexts. Concerning QAM transmissions,

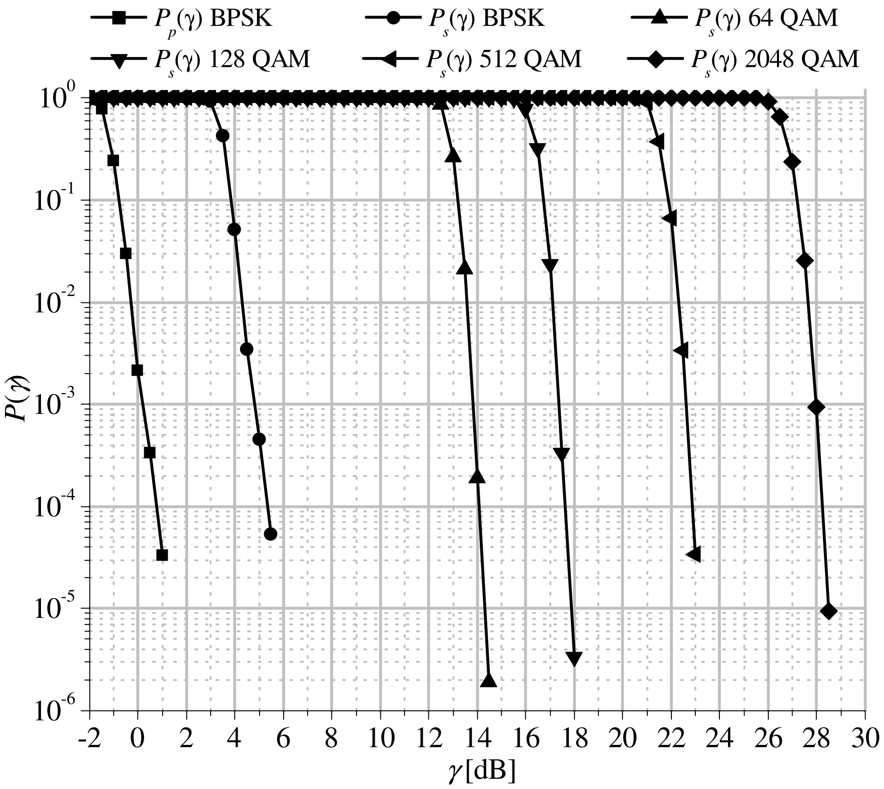


Figure 5.5: Error rate curves for an UEP LDPC code with length 4096 and PC1 and PC2 with proportions 20% – 80%. The bits in the PC1 are always BPSK modulated, while the performance of several QAM schemes with Yarg labeling on the bits in the PC2 is reported.

they have been implemented through a pragmatic approach, by mapping groups of bits into QAM symbols, and then using a classical symbol-to-bit soft metric conversion before LDPC decoding.

The performance of our code has been assessed by simulating transmission over a Gaussian channel with SNR per bit equal to γ, and by performing decoding through the LLR-SPA. The results obtained, in terms of $P_p(\gamma)$ and $P_s(\gamma)$, is reported in Fig. 5.5.

Also in this case we fix $\delta = 10^{-4}$ and $\eta = 0.1$ in (3.7). Based on these choices, from Fig. 5.5 we obtain $\beta_p = 0.75$ dB, while α_s and β_s vary according to the modulation scheme used for the secret information bits. The values taken by α_s and β_s for the considered modulation schemes are reported in

Table 5.2: Performance of the considered coding and modulation schemes (all values are in dB, except the outage probability)

Scheme	α_s	$\omega_{\min}$ ($\xi_{\max}$)	$\bar{\gamma}^{(E)}_{\text{opt}}$	β_s	$\bar{\gamma}^{(B)}_{\min}$	S_g
BPSK	2.95	0.81	1.90	5.35	3.14	1.24
64 QAM	12.25	0.24	7.70	14.12	19.73	12.03
128 QAM	15.78	0.13	10.25	17.67	26.23	15.98
512 QAM	20.64	0.05	13.99	22.94	35.84	21.85
2048 QAM	25.27	0.02	17.73	28.49	45.44	27.71

Tab. 5.2 [76].

Starting from the values of α_s and β_s, we can compute Eve's overall outage probability ω (5.3), as a function of Eve's average SNR per bit, $\bar{\gamma}^{(E)}$. The values of ω, so obtained, are reported in Fig. 5.6 for the considered secret information modulation formats. Then, the value of $\omega_{\min}$ is easily obtained, as well as the value of $\bar{\gamma}^{(E)}_{\text{opt}}$ for which $\omega = \omega_{\min}$. These values are also reported in Tab. 5.2. Concerning Bob, we have fixed a maximum outage probability $\xi_{\max} = \omega_{\min}$, and computed the corresponding minimum value of his average SNR per bit, $\bar{\gamma}^{(B)}_{\min}$, according to (5.2). The values of $\bar{\gamma}^{(B)}_{\min}$, so obtained, are also reported in Tab. 5.2.

Based on these results, we observe that, when both the public and the secret information bits are modulated with BPSK, the outage probability for Eve is always very large (more than 0.8). Therefore, although the system is theoretically feasible, in practice the fading nature of the channel rarely allows to achieve a successful transmission. The situation improves by adopting higher modulation orders for the private information bits, which also increases the values of α_s. This way, the outage probability for Eve is progressively reduced. When we adopt a QAM scheme with 2048 symbols, Eve's outage probability can be reduced down to 0.02. Under the hypothesis that Bob's outage probability is the same as Eve's outage probability (or less), we observe that there is a tradeoff between the outage probability and the security gap. In fact, if we are able to tolerate a high probability of outage, the system requires small security gaps (in the order of 10 dBs or even

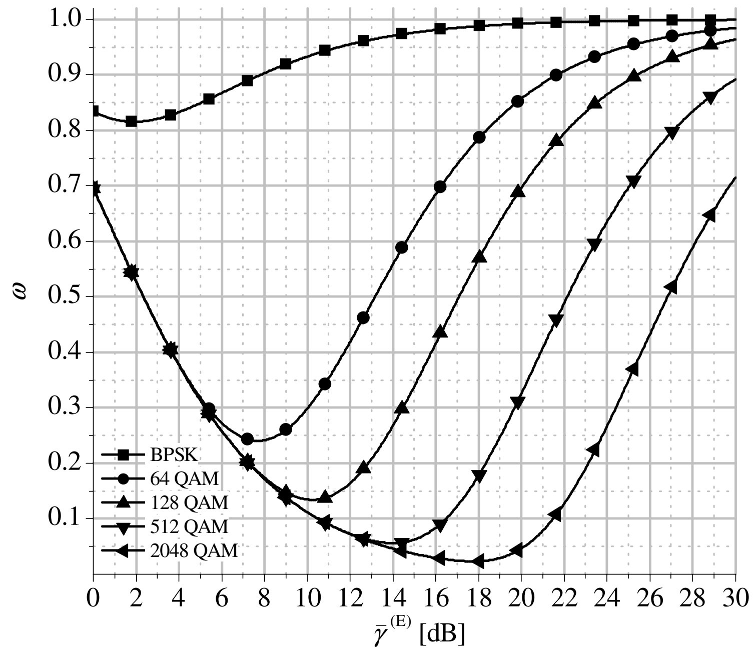


Figure 5.6: Eve's outage probability ω as a function of Eve's average SNR per bit $\bar{\gamma}^{(E)}$ for an UEP LDPC coded transmission with BPSK-modulated public information bits and several QAM formats with Yarg labeling on the secret information bits.

less). Instead, if we aim at small outage probabilities, we need large security gaps (in the order of 20 or 30 dBs).

5.3 Coding and modulation schemes with larger UEP

As it is clear from the discussion above, often in practical communication systems, to satisfy the reliable conditions in (3.7), a wide separation between the error rate performance of the public and secret part of the message is required. For example, it is usually important that the header of each received packet is reliably received to allow correct synchronization and decoding, while some rare errors in the payload may be tolerated (e.g., in multimedia transmissions). As we have shown previously, a solution to achieve different levels of protection against the noise is to use coding and modulation schemes with UEP. In this case, contrary to the approach in Sec.5.1 and also other works in literature [70,72,73,77], our goal is not optimize the overall (average) performance of the code. Clearly, this is an important target, but it may result in a limited separation between the performance experienced over different PCs.

Thus, in this section we propose a different approach, aimed at improving the error correcting performance over the most protected bits without the constraint of achieving good performance also on the least protected ones. For this purpose, we have developed an asymptotic analysis tool which allows to estimate the performance over each PC. We also consider high order modulation schemes which allow to increase the spectral efficiency at some cost in performance, and therefore may be of interest for the least protected bits. A solution to study the asymptotic performance of UEP LDPC codes with high order modulation schemes is proposed in [78], but considering the overall check node degree distribution. Instead, we have proposed a method to study the asymptotic performance over each protection class separately. As in Sec. 4.2, our solution is based on the well known DE algorithm [65, 79] that, given the node degree distributions of an LDPC code, allows to predict the performance of a code in asymptotic terms (i.e., under the hypothesis of infinite code length and absence of closed loops in the Tanner graph).

As in the previous sections, we divide the codeword bits into three PCs. As shown in [70], the UEP capabilities can be increased by reducing the number of edges shared by nodes belonging to different PCs. We also show how to compute the maximum number of check nodes which is possible to reserve to the bits belonging to PC1. Since the highest degrees of $\lambda(x)$ ensure a greater protection against the noise, the corresponding nodes are assigned to PC1, whereas the others form the remaining protection classes. We put the highest weight columns of $\mathbf{H}$ in the leftmost positions, which therefore correspond to the k_1 codeword bits belonging to PC1. The subsequent k_2 codeword bits belong to PC2, and the last r bits belong to PC3. For each protection class PCi, $i = 1, 2, 3$, we consider the corresponding sub-matrix $\mathbf{H}^{(\mathbf{i})}$ of $\mathbf{H}$ and compute $\lambda^{(i)}(x)$ and $\rho^{(i)}(x)$. Differently from [70], we normalize

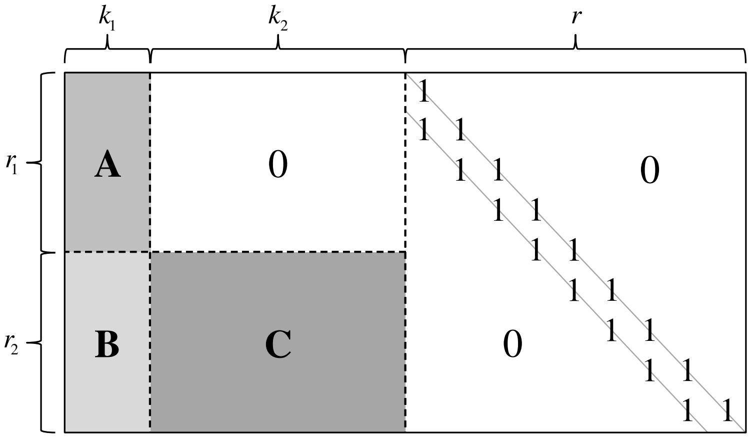


Figure 5.7: General form of the parity-check matrix of the designed UEP LDPC codes.

all the degree distribution polynomials, such that their coefficients sum to one.

5.3.1 Design of the UEP LDPC parity-check matrix

We aim at controlling the level of interconnection between any two protection classes by controlling the connections between the variable nodes of each protection class and the check nodes. In order to improve the performance over PC1, we must design $\mathbf{H}$ in such a way as to maximize the number of check nodes connected to its variable nodes, and not to those in PC2. For this purpose, we impose that some check nodes are connected only to variable nodes in PC1 and PC3. Since encoding is systematic, these check nodes represent parity-check equations which only involve information bits in PC1 and redundancy bits; therefore, we can say that the corresponding parity-check equations are *reserved* to PC1. We denote the number of these check nodes as $r_1 \leq r$, and their fraction as $\mu = r_1/r$.

A pictorial example of this approach is illustrated in Fig. 5.7, where the zigzag-random construction of $\mathbf{H}$ is considered. According to this construction, the rightmost square block of $\mathbf{H}$ has the "staircase" form shown in Fig. 5.7. Then, we divide the leftmost block into four sub-blocks, three of which (denoted by A, B and C) may contain non-zero elements, while the fourth, denoted by 0, is an all-zero block. As we see from the figure, the bits in PC1 may take part in all the parity-check equations (since the blocks A and B contain both zeros and ones), while the bits in PC2 may only take part in the last $r_2 = r - r_1$ parity-check equations (since only the block C contains both zeros and ones). If one wishes to achieve maximum separation between PC1 and PC2, r_1 has to be maximized (under some constraint imposed by the degree distributions, as described next). Instead, classical approaches [70, 72, 73, 77] exploit the whole matrix to optimize the overall performance, and therefore fix $\mu = r_1 = 0$. Obviously, increasing r_1 is paid in terms of some loss in performance over PC2, but this is counterbalanced by significant improvements in performance over PC1, as we will show next. This also increases the performance gap between the first two protection classes. For a code defined through the polynomials $\lambda(x)$ and $\rho(x)$, an upper bound on the value of r_1 can be easily computed as

$$r_1 \leq r - k_2 \frac{\sum_{i=1}^{d_{v_2}} \lambda_i^{(2)} \cdot i}{\sum_{j=1}^{d_c} \rho_j \cdot j}, \tag{5.4}$$

where d_{v_2} is the maximum variable node degree in PC2 and d_c is the maximum overall check node degree. This follows from the consideration that any check node connected to a variable node in PC2 cannot be reserved to PC1.

In order to compare our results with those reported in previous works, we start from the optimized variable node degree distribution provided in [73], with some minor modifications needed to comply with the size of the protection classes we consider. As in the previous sections, in our code PC1 contains 20% of the information bits, PC2 contains the remaining 80% of the information bits and PC3 contains all the redundancy bits. The overall code rate R is equal to 1/2. The nonzero coefficients of the normalized $\lambda^{(i)}(x)$ from which we start are reported in Tab. 5.3, for $i = 1, 2, 3$. From [73], we also assume, as starting point to be used in (5.4), $\rho(x) = 0.0437x^7 + 0.9563x^8$. We consider two values of code length: $n_1 = 4096$ and $n_2 = 16384$.

For these parameters, we obtain through (5.4) that the maximum value of μ is about 0.7. We then consider three different values of μ, namely: 0.3, 0.5

Table 5.3: Normalized variable node degree distributions within the three protection classes

$\lambda^{(1)}(x)$	$\lambda^{(2)}(x)$	$\lambda^{(3)}(x)$
$\lambda_{16}^{(1)} = 0.8485$ $\lambda_{17}^{(1)} = 0.1373$ $\lambda_{18}^{(1)} = 0.0067$ $\lambda_{19}^{(1)} = 0.0020$ $\lambda_{20}^{(1)} = 0.0055$	$\lambda_{3}^{(2)} = 1$	$\lambda_{2}^{(3)} = 0.9854$ $\lambda_{3}^{(3)} = 0.0146$

and 0.7, in addition to $\mu = 0$, which represents the classical approach [73]. The choice of μ obviously affects only the rows of $\mathbf{H}$. We report $\tilde{\rho}^{(i)}(x)$, $i = 1, 2, 3$, in Tab. 5.4, for the values of μ we consider. A first set of simulation results, considering the AWGN channel with BPSK, is reported in Fig. 5.8 in terms of the BER as a function of the SNR per bit (E_b/N_0). We observe that the classical approach ($\mu = 0$) achieves good performance over PC2, which always dominates the overall average performance. Through the proposed method ($\mu > 0$), the performance gap between PC1 and PC2 increases. In fact, by increasing μ, the error rate performance over PC1 improves, while that over PC2 worsens.

5.3.2 Asymptotic performance

The asymptotic performance of LDPC code ensembles over the AWGN channel with sum-product decoding can be estimated through the DE technique, by using a Gaussian approximation for the message densities [65]. The messages exchanged and iteratively updated during sum-product decoding are the log likelihood ratio (LLR) values of the received bits. However, while in classical density evolution the received bits are undifferentiated, we need to take into account their separation into PCs, and to consider the node degree distributions within each class. For this purpose, we start from the

Table 5.4: Normalized check node degree distributions from the node perspective within the three protection classes for some choices of μ

μ	$\tilde{\rho}^{(1)}(x)$	$\tilde{\rho}^{(2)}(x)$	$\tilde{\rho}^{(3)}(x)$
0	$\tilde{\rho}_0^{(1)} = 0.0298$	$\tilde{\rho}_0^{(2)} = 0.0757$	$\tilde{\rho}_1^{(3)} = 0.0005$
	$\tilde{\rho}_1^{(1)} = 0.1133$	$\tilde{\rho}_1^{(2)} = 0.1953$	$\tilde{\rho}_2^{(3)} = 0.9995$
	$\tilde{\rho}_2^{(1)} = 0.2026$	$\tilde{\rho}_2^{(2)} = 0.2734$	
	$\tilde{\rho}_3^{(1)} = 0.2427$	$\tilde{\rho}_3^{(2)} = 0.2451$	
	$\tilde{\rho}_4^{(1)} = 0.1968$	$\tilde{\rho}_4^{(2)} = 0.1455$	
	$\tilde{\rho}_5^{(1)} = 0.1274$	$\tilde{\rho}_5^{(2)} = 0.0508$	
	$\tilde{\rho}_6^{(1)} = 0.0557$	$\tilde{\rho}_6^{(2)} = 0.0132$	
	$\tilde{\rho}_7^{(1)} = 0.0317$	$\tilde{\rho}_7^{(2)} = 0.0010$	
0.3	$\tilde{\rho}_0^{(1)} = 0.0308$	$\tilde{\rho}_0^{(2)} = 0.3228$	$\tilde{\rho}_1^{(3)} = 0.0005$
	$\tilde{\rho}_1^{(1)} = 0.1108$	$\tilde{\rho}_1^{(2)} = 0.0508$	$\tilde{\rho}_2^{(3)} = 0.9995$
	$\tilde{\rho}_2^{(1)} = 0.2139$	$\tilde{\rho}_2^{(2)} = 0.1216$	
	$\tilde{\rho}_3^{(1)} = 0.2319$	$\tilde{\rho}_3^{(2)} = 0.1558$	
	$\tilde{\rho}_4^{(1)} = 0.1938$	$\tilde{\rho}_4^{(2)} = 0.1724$	
	$\tilde{\rho}_5^{(1)} = 0.1245$	$\tilde{\rho}_5^{(2)} = 0.1226$	
	$\tilde{\rho}_6^{(1)} = 0.0611$	$\tilde{\rho}_6^{(2)} = 0.0435$	
	$\tilde{\rho}_7^{(1)} = 0.0332$	$\tilde{\rho}_7^{(2)} = 0.0105$	
0.5	$\tilde{\rho}_0^{(1)} = 0.1362$	$\tilde{\rho}_0^{(2)} = 0.5039$	$\tilde{\rho}_1^{(3)} = 0.0005$
	$\tilde{\rho}_1^{(1)} = 0.0967$	$\tilde{\rho}_1^{(2)} = 0.0171$	$\tilde{\rho}_2^{(3)} = 0.9995$
	$\tilde{\rho}_2^{(1)} = 0.1479$	$\tilde{\rho}_2^{(2)} = 0.0381$	
	$\tilde{\rho}_3^{(1)} = 0.1704$	$\tilde{\rho}_3^{(2)} = 0.0645$	
	$\tilde{\rho}_4^{(1)} = 0.1587$	$\tilde{\rho}_4^{(2)} = 0.0845$	
	$\tilde{\rho}_5^{(1)} = 0.1260$	$\tilde{\rho}_5^{(2)} = 0.0967$	
	$\tilde{\rho}_6^{(1)} = 0.0859$	$\tilde{\rho}_6^{(2)} = 0.0757$	
	$\tilde{\rho}_7^{(1)} = 0.0782$	$\tilde{\rho}_7^{(2)} = 0.1195$	
0.7	$\tilde{\rho}_0^{(1)} = 0.5669$	$\tilde{\rho}_0^{(2)} = 0.6997$	$\tilde{\rho}_1^{(3)} = 0.0005$
	$\tilde{\rho}_1^{(1)} = 0.0508$	$\tilde{\rho}_1^{(2)} = 0.0010$	$\tilde{\rho}_2^{(3)} = 0.9995$
	$\tilde{\rho}_2^{(1)} = 0.0093$	$\tilde{\rho}_2^{(2)} = 0.0088$	
	$\tilde{\rho}_7^{(1)} = 0.0493$	$\tilde{\rho}_3^{(2)} = 0.0161$	
	$\tilde{\rho}_8^{(1)} = 0.3237$	$\tilde{\rho}_4^{(2)} = 0.0361$	
		$\tilde{\rho}_5^{(2)} = 0.0415$	
		$\tilde{\rho}_6^{(2)} = 0.1968$	

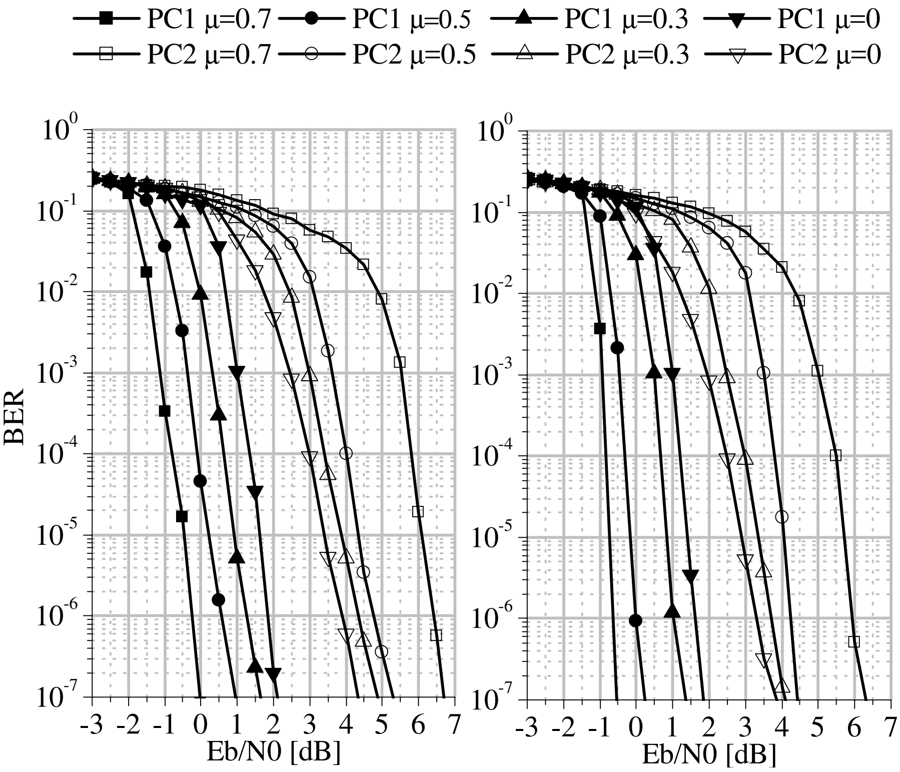


Figure 5.8: Bit error rate performance of UEP LDPC codes with $\mu = 0.3, 0.5, 0.7$, BPSK modulation over the AWGN channel and length (a) $n = 4096$ bits, (b) $n = 16384$ bits. The case with $\mu = 0$, corresponding to the classical approach, is also considered as a benchmark.

overall average mutual information m_l at the decoding iteration l, that is,

$$m_l \quad = \quad \sum_{j=2}^{d_c} \rho_j \;\cdot\; \phi^{-1}\left(1 - \left[1 - \sum_{i=2}^{d_v} \lambda_i \phi\left(m_I + (i-1)\cdot m_{l-1}\right)\right]^{j-1}\right), \quad (5.5)$$

where $\phi(x) = 1 - \frac{1}{\sqrt{4\pi x}} \int_{-\infty}^{+\infty} \tanh\left(\frac{u}{2}\right) e^{-\frac{(u-x)^2}{4x}} du$ and m_I is the mean of the initial LLRs (computed on the symbols received from the channel). For an AWGN with zero mean and variance σ^2, m_I is equal to $\frac{2}{\sigma^2}$. Equation (5.5) can be specialized for each protection class by replacing the polynomials $\lambda(x)$ and $\rho(x)$ with the polynomials $\lambda'^{(i)}(x)$ and $\rho^{(i)}(x)$, as explained in the following. The convergence threshold is then defined as the minimum SNR (i.e., maximum value of σ) at which $m_l \to 1$ for $l \to \infty$. Therefore, it can be found by recursively computing (5.5), starting with $m_0 = 0$.

High order modulation schemes

An interesting option for the least protected bits is to use high order modulation schemes, which further deteriorate the error rate on that part of the bitstream, but allow to increase the spectral efficiency and to reach high speeds. This also increases the gap between the first two protection classes, which is useful, for example, in transmissions over the BCC [74, 76]. A method to model the asymptotic performance with high order modulations is to consider a BPSK-equivalent noise variance σ_e^2, which depends on the modulation scheme [78]. Let us consider an M-ary rectangular QAM with $M = 2^p$. The probability of a symbol error is $P_M = 1 - (1 - P_{\sqrt{M}})^2$, where

$$P_{\sqrt{M}} = 2\left(1 - \frac{1}{\sqrt{M}}\right) \cdot Q\left(\sqrt{\frac{3}{M-1}\frac{E_{ave}}{N_0}}\right),$$

$\frac{E_{ave}}{N_0}$ is the average SNR per symbol and $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} \exp(-t^2/2)dt$. The probability of a bit error in M-ary modulations depends on the adopted labeling, and is often expressed in average terms. For example, by using the Gray labeling which, under the assumption of large SNR, implies that a symbol error results in only one bit error, the average bit error rate can be estimated as $P_b \approx P_M/\log_2 M$. Despite P_b is the overall average bit error rate, the bits corresponding to each symbol may have a different error probability based on their position, as shown in [78] for the case of an 8-PSK modulation. Similarly, for 16-QAM with Gray labeling, we can obtain the probability of error of each of the four bits (d_0, d_1, d_2, d_3) associated to each symbol as

$$\begin{cases} P_{b,d_0} &= 0.1458 P_M \\ P_{b,d_1} &= 0.3542 P_M \\ P_{b,d_2} &= 0.1458 P_M \\ P_{b,d_3} &= 0.3542 P_M \end{cases},$$

under the hypothesis of large SNR. This assumption could be removed by resorting to an exact formulation (as in [80]), but this is not necessary for the scope of this paper.

In some contexts, it may be useful to adopt labelings different from the classical Gray. An interesting case is that of anti-Gray [81] or Yarg labelings [75], which are also used in PLS [74, 76]. Both these labelings ensure that adjacent symbols have at most one bit in common. If we use one of these labelings for the bits in PC2, we further increase the performance gap between the first two protection classes [74, 76]. As an example, if we consider a 16-QAM with Yarg labeling as in [75, Fig. 8], the error probabilities for the four bits $[d_0, \ldots, d_3]$ corresponding to each symbol are

$$\begin{cases} P_{b,d_0} &= 0.8542 P_M \\ P_{b,d_1} &= 0.6458 P_M \\ P_{b,d_2} &= 0.8542 P_M \\ P_{b,d_3} &= P_M \end{cases}.$$

For any modulation and labeling, we can use the values of $[P_{b,d_0}, \ldots, P_{b,d_{p-1}}]$ to compute the average bit error probability P_b. The value of σ_e^2, which can be used to compute m_I in (5.5), is simply obtained from P_b as [78]

$$\sigma_e^2 = \frac{1}{\left[Q^{-1}\left(2P_b\right)\right]^2}.$$

Convergence threshold of the protection classes

We aim at finding a convergence threshold for each protection class, in such a way as to study separately their asymptotic performance. The rate $R^{(i)}$, $i = 1, 2, 3$, which corresponds to each protection class can be easily computed as

$$R^{(i)} = 1 - \frac{\int_0^1 \rho^{(i)}(x)dx}{\int_0^1 \lambda^{(i)}(x)dx}. \tag{5.6}$$

In other terms, $R^{(i)}$ is the rate of the code defined by the sub-matrix $\mathbf{H^{(i)}}$, $i = 1, 2, 3$. By using the degree distributions $\lambda^{(i)}(x)$ and $\rho^{(i)}(x)$, however, the values of $R^{(i)}$ computed through (5.6) are misleading. For example, when the overall code rate is $R = 1/2$, as in the cases we consider, the sub-matrices $\mathbf{H^{(1)}}$ and $\mathbf{H^{(2)}}$ have more rows than columns. Therefore, the corresponding values of $R^{(1)}$ and $R^{(2)}$ would be negative (that, obviously, has no sense), and the actual rates of the codes defined by $\mathbf{H^{(1)}}$ and $\mathbf{H^{(2)}}$ (based on the number of their independent rows) would be 1 or almost 1. To overcome this problem, we replace $\lambda^{(i)}(x)$ with a new polynomial $\lambda'^{(i)}(x)$, obtained by scaling the degrees appearing in $\lambda^{(i)}(x)$ in such a way that each pair $(\lambda'^{(i)}(x), \rho^{(i)}(x))$, used in (2.3), gives a rate equal to the overall code rate R, i.e., $R^{(i)} = R, i = 1, 2, 3$. In order to compute the degrees of $\lambda'^{(i)}(x)$ which yield $R^{(i)} = R$, the degrees of $\lambda^{(i)}(x), i = 1, 2, 3$, must be multiplied by the real coefficient

$$\psi_i = \frac{\sum_{j=1}^{d_c^{(i)}} \rho_j^{(i)} \cdot j}{\sum_{l=1}^{d_v^{(i)}} \lambda_l^{(i)} \cdot l} \cdot (1 - R), \tag{5.7}$$

where $d_c^{(i)}$ and $d_v^{(i)}$ are, respectively, the maximum check and variable node degrees within the protection class PCi.

For the code parameters we consider the variable and check node degree distributions shown in Tabs. 5.3 and 5.4, through (5.7) we obtain $\psi_1 = 0.1025$, $\psi_2 = 0.1997$ and $\psi_3 = 0.5$. The degrees of the nonzero coefficients of the scaled polynomial $\lambda'^{(i)}(x)$ are computed by multiplying the degrees of the nonzero coefficients of $\lambda^{(i)}(x)$ by ψ_i, and then approximating the result to the nearest integer.

The asymptotic performance of each protection class can be assessed by using the pair $(\lambda'^{(i)}(x), \rho^{(i)}(x))$. In summary, these degree distributions have the same check node degrees resulting from the sub-matrices $\mathbf{H^{(i)}}$, but the variable node degrees are scaled by a factor equal to ψ_i, obtained from (5.7). According to this approach, and by using the method described for high order modulations, we can compute a convergence threshold for each protection class through the recursive use of (5.5). The results (considering 1000 decoding iterations) are reported in Tab. 5.5.

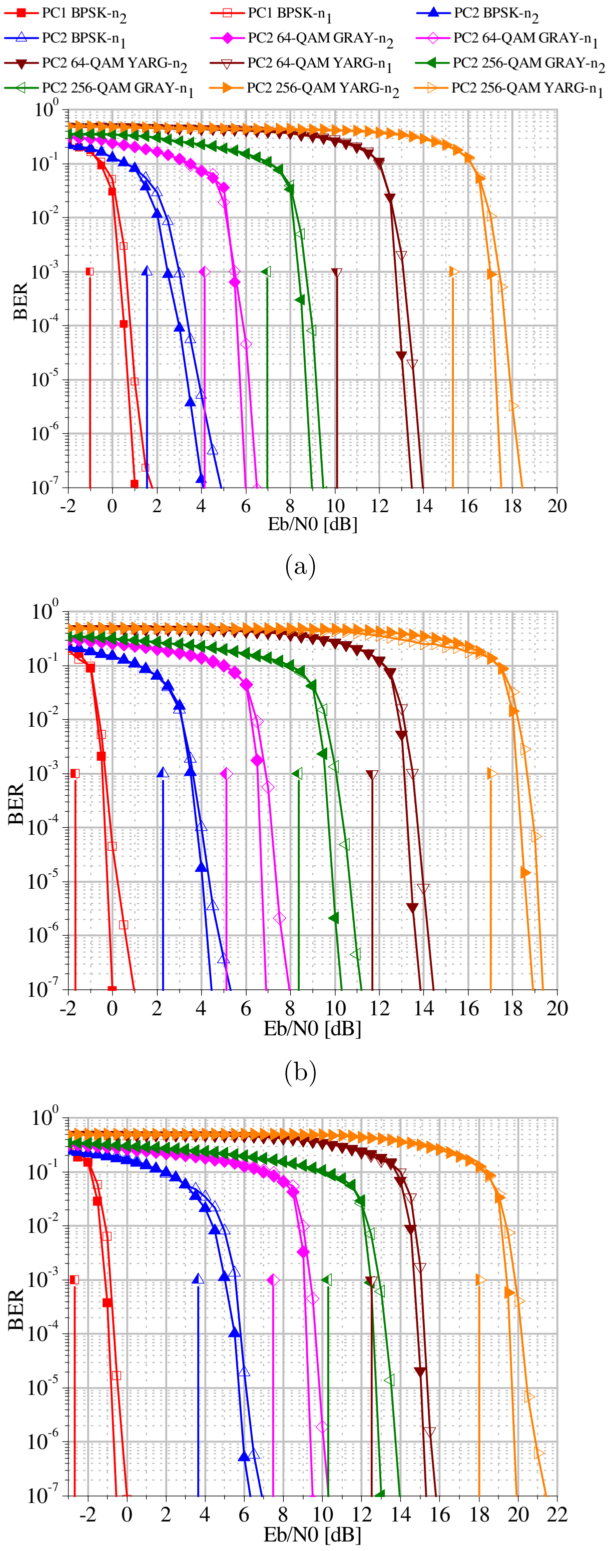
Table 5.5: Decoding threshold (E_b/N_0 [dB]) per protection class for some UEP LDPC coded modulation schemes and values of μ

Scheme	$\mu = 0$	$\mu = 0.3$	$\mu = 0.5$	$\mu = 0.7$
PC1 BPSK	0.214	−1.010	−1.697	−2.681
PC2 BPSK	1.015	1.537	2.270	3.641
PC2 64-QAM GRAY	2.491	4.128	5.1170	7.471
PC2 64-QAM YARG	6.682	10.110	11.678	12.521
PC2 256-QAM GRAY	5.357	6.956	8.372	10.298
PC2 256-QAM YARG	11.174	15.326	17.022	18.010

5.3.3 Finite length codes performance

Let us consider several UEP LDPC codes with $R = 1/2$, two values of code length ($n_1 = 4096$, $n_2 = 16384$) and three PCs, according to the degree distributions reported in Tabs. 5.3 and 5.4. The BER performance achieved by these codes over each PC has been assessed by simulating transmission over the AWGN channel. Decoding is performed through the LLR-SPA. The bits in PC1 are always transmitted by using BPSK modulation to ensure maximum protection, while for the bits in PC2 we consider several modulation schemes, that is, BPSK, 64-QAM with Gray and Yarg labelings and 256-QAM with Gray and Yarg labelings. Concerning PC3, we always use the BPSK modulation, since this allows to achieve the best performance over the bits in PC1.

The performance attained over PC1 and PC2 is illustrated in Fig. 5.9 for $\mu = 0.3, 0.5$ and 0.7 [82]. The convergence thresholds obtained in the asymptotic regime, reported in Tab. 5.5, are also plotted as a reference. We observe that there is a good agreement between the performance observed in the asymptotic regime and in the finite length regime. We also observe that, even with high order modulations and different labelings, an increase in the value of μ yields a better performance over PC1, paid in terms of a performance loss over PC2. The results of this assessment also confirm that the performance of the longer codes is closer to the asymptotic limits, as expected.



(a)

(b)

(c)

Figure 5.9: Bit error rate performance of the designed UEP LDPC codes with (a) $\mu = 0.3$, (b) $\mu = 0.5$, (c) $\mu = 0.7$ and lengths $n_1 = 4096$ bits and $n_2 = 16384$ bits. Each vertical segment represents the asymptotic threshold corresponding to the curves with the same marker shape.

5.4 Summary

In this chapter, we have proposed some strategies to achieve reliable and secure communication over a BCC. To achieve our aims, the authorized and unauthorized receivers have to experience different error rates. For this reason, we use LDPC codes with UEP capabilities and we have shown as they should be preferable in this context. In addition to the Gaussian BCC, we have also introduced the case of a fading channel. This way, we have considered a more realistic scenario and we have studied the outage probability for which the feasibility conditions are not met. In this case, we have shown that a wide performance gap between the public and secret part of the massage is needed. To achieve this goal, we use high order modulation and Yarg labeling to send the private bits. To further increase this performance gap, a strategy to obtain a largely UEP was proposed. This result is achieved by reserving some parity check equations to the most protected bits during the code design. Moreover, by considering high order modulation schemes and non conventional bits labeling, an analytical tool to assess separately the asymptotic performance of each PC is provided. All the proposed strategies have been confirmed by numerical simulations.

Chapter 6

Coding schemes for reliable satellite communications

Phase and amplitude scintillation due to solar wind and solar corona has always been an important issue in the design and operation of deep space tracking systems. In particular, the communication link between the Earth and a space probe may be exposed to turbulence phenomena during superior solar conjunctions, when the Sun lies between the Earth and the probe. As the turbulent field in the solar corona moves away from the sun at a large speed (200-1000 km/s), the receiver sees a time varying amplitude in addition to a time varying phase. These phenomena are called *amplitude* and *phase scintillation* and the reliability analysis of the radio link must take into account their statistics. When a radio link enters in the strong scintillation regime the received amplitude may drop to very small values and fading may compromise the quality of the transmission. In such a scenario, a very important role is played by error correcting codes. At the cost of some redundancy and increased complexity, they permit to reduce the SNR required for achieving prefixed error rate performances. For both TM and TC links, the channel coding and synchronization standards recommended by the Consultative Committee for Space Data Systems (CCSDS) include a wide set of possibilities, ranging from conventional BCH codes and RS codes, to convolutional codes (typically concatenated with RS codes) and PCTCs and LDPC codes. Actually, some of these schemes, like PCTCs and LDPC codes, have been proven able to achieve performance close to the theoretical ultimate limits over the AWGN channel, so they are considered the state-of-the-art in this context.

In this chapter we provide a thorough analysis of the performance of these codes over a channel with solar scintillation, by taking into account that the fading affects both amplitude and phase of the signal. Furthermore, in the case of phase error where the use of non-coherent modulation schemes is mandatory, results obtained with the FSK are shown.

To the best of our knowledge, few works have previously addressed such a scenario [83], [84]. However, in these papers only amplitude scintillation is considered. Thus, the results collected in this chapter cover a wide range of several, more realistic, operating scenarios.

6.1 Impact of solar scintillation

Solar scintillation might cause a BER degradation and eventually residual carrier unlock. Accordingly, the amount of scintillation is due to charged particles of the solar corona and depends on the solar elongation (i.e., minimum distance of the signal ray path from the sun), solar cycle and sub-solar latitude of the signal path. A pictorial example that describes the solar conjunction geometry is shown in Fig. 6.1.

Several statistical models describe the effects of a scattering medium on radio communications. For solar scintillation, each coronal inhomogeneity can be modeled as a scattering center for the impinging electromagnetic wave. At the receiver the electric fields of the scattered waves add up, producing a time-varying interference pattern that may lead to fading. Considering the receiver far away from the scattering medium, it is reasonable to assume that the received electric field is the sum of a large number of statistically independent waves scattered from different regions within the medium. Application of the central limit theorem leads to a complex-valued received signal with independent Gaussian real and imaginary parts. Assuming the real and imaginary random components have the same variance we may thus model the

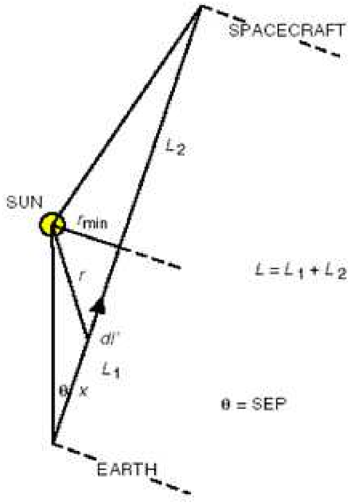


Figure 6.1: Solar conjunction geometry.

scintillation channel as a multipath fading channel with a Rice distribution.

The Rician statistics depends on the carrier frequency as well as the geometry of the Sun, Earth and Probe i.e., the Sun-Earth-Probe (SEP) angle shown in Fig. 6.1. Usually, the Rician fading distribution is specified in terms of the scintillation index, noted by m, which is the ratio of the standard deviation of the received signal power to its mean.

Let us consider first the uncoded system. After propagating through a Rician fading channel, the received signal at on-board receiver input can be written as

$$r(t) = \sqrt{2P}V \sin\left[\omega_c t + \phi_c + \phi_R + D(t)\right] + n(t) \tag{6.1}$$

where P is the total received signal power; V is the Rician-distributed fading amplitude due to scintillation; ω_c and ϕ_c are the carrier radian frequency and phase respectively; ϕ_R is the phase scintillation associated with Rician fading; $D(t)$ is the BPSK-modulated subcarrier and $n(t)$ is the AWGN noise. Considering narrowband modulation (i.e., symbol rate $<$ 4 ksps), the multipath fading channel can be considered as frequency-nonselective and a slow-fading model can be adopted, according to coherence time $(\Delta t)_c$ reported, for example, in Tab. 6.1.

Table 6.1: Examples of coherence time in different frequency transmission intervals.

	S-Band	X-Band	Ka-Band
$(\Delta t)_c$	13.9 ms	7.25 ms	3.72 ms

The probability density function $p_V(\nu)$ of the Rician variable V is given by eq. (6.2)

$$p_V(\nu) = \frac{\nu}{\sigma^2}\exp\left(-\frac{\nu^2+a^2}{2\sigma^2}\right)I_0\left(\frac{\nu a}{\sigma^2}\right), \qquad \nu \geq 0 \tag{6.2}$$

where a^2 is the noncentrality parameter and σ^2 is the variance of each Gaussian random variable related to the Rice random variable. Assuming that the amplitude scintillation causes no loss in the long term average received signal power, we can write

$$E\left[V^2\right] = 1 = \mathrm{var}\left[V\right] + E\left[V\right]^2 = 2\sigma^2 + a^2. \tag{6.3}$$

The parameter a^2 and σ^2 are related to the scintillation index as shown below

$$a^2 = \sqrt{(1-m^2)} \tag{6.4}$$

$$\sigma^2 = \frac{1-\sqrt{1-m^2}}{2}. \tag{6.5}$$

In Tab. 6.2 we summarize the Rician statistics due to scintillation according to the operative scintillation index values m.

Focusing on the residual carrier recovery loop we can expand (6.1) as

$$\begin{aligned} r(t) = \sqrt{2P}\left[V\cos(\phi_R)\sin(\omega_C t+\phi_C) + V\sin(\phi_R)\cos(\omega_C t+\phi_C)\right] + \\ + n(t) = \sqrt{2P}\left[X\sin(\omega_C t+\phi_C) + Y\cos(\omega_C t+\phi_C)\right] + n(t) \end{aligned} \tag{6.6}$$

where

Table 6.2: Relation between the scintillation index (m) and the Rician statistics

m	a	σ^2
0.1	0.997	0.002
0.2	0.990	0.010
0.3	0.977	0.023
0.4	0.957	0.042
0.5	0.931	0.067
0.6	0.894	0.1
0.7	0.845	0.143
0.8	0.775	0.2
0.9	0.660	0.282
0.99	0.375	0.429

$$X = V\cos(\phi_R),$$

$$X = V\sin(\phi_R).$$

From (6.6), it results that X and Y are independent Gaussian random variables with the same variance σ^2 and mean values equal to

$$E\left[X\right] = a = \sqrt[4]{1-m^2},$$

$$E\left[Y\right] = 0.$$

We can now analytically derive the BER function, considering a BPSK modulation and assuming that the subcarrier tracking and bit synchronizer are perfect. To have this condition we need a loop bandwidth (B_l) at least 5 times larger than the Doppler spread of the scintillation channel i.e. $B_l \geq 5/\left(\Delta t\right)_c$. Under this condition we have [85]

$$P_b = \int_0^\infty \int_{-\pi}^{\pi} \mathrm{Q}\left(\sqrt{2\frac{E_b}{N_0}\nu^2\cos^2(\phi)}\right) p_V(\nu)p_\phi(\phi \mid \nu)\, d\nu\, d\phi$$

As for most carrier synchronization loops, we may consider a Tikhonov distribution for the steady-state probability density function (PDF) of the modulo-2π phase error

$$p_\phi(\phi \mid \nu) = \frac{1}{2\pi I_0\left(\rho\nu^2\right)} e^{\rho\nu^2\cos(\phi)} \tag{6.7}$$

where ρ is the carrier PLL signal-to-noise ratio. Therefore the BER as a function of the scintillation index m and E_b/N_0 can be computed as reported below

$$\begin{aligned} P_b\left(\frac{E_b}{N_0}\right) = \int_0^\infty \int_{-\pi}^{\pi} \mathrm{Q}\left(\sqrt{2\frac{E_b}{N_0}\nu^2\cos^2(\phi)}\right) \frac{\nu}{\sigma_m^2} \exp\left(-\frac{\nu^2 + a_m^2}{2\sigma_m^2}\right) \\ I_0\left(\frac{\nu a_m}{\sigma_m^2}\right) \frac{1}{2\pi I_0(\rho\nu^2)} \exp\left[\rho\nu^2\cos(\phi)\right]\, d\nu\, d\phi \end{aligned} \tag{6.8}$$

where subscript m means that a and σ are computed using (6.4) and (6.5), respectively. In (6.8) $\mathrm{Q}(x)$ is the Q-function, defined as

$$\mathrm{Q}(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}}\, dt.$$

Now let us write the instantaneous fading SNR as

$$\gamma = \frac{E_b}{N_0}\nu^2$$

and the average SNR per bit as

$$\overline{\gamma} = \frac{E_b}{N_0} E\left[\nu^2\right]. \tag{6.9}$$

According to (6.3), we can rewrite (6.9) as

$$\overline{\gamma} = \frac{E_b}{N_0}.$$

So, an approximate solution to (6.8) can be written for large loop SNR (ρ) as

$$P_e\left(\frac{E_b}{N_0}, m\right) \simeq \mathrm{Q}_1(a_m, b_m) - \frac{1}{2}\left(1 + \sqrt{\frac{p_m}{1+p_m}}\right)\exp\left(-\frac{a_m^2 + b_m^2}{2}\right) I_0\left(a_m b_m\right) +$$
$$+ \frac{1+k_m}{2\left[\frac{\rho}{\frac{E_b}{N_0}}\right]\sqrt{\frac{E_b}{N_0}^2 + (1+k_m)\frac{E_b}{N_0}}} \exp\left(-k_m \frac{2\frac{E_b}{N_0} + 1 + k_m}{2\left(\frac{E_b}{N_0} + 1 + k_m\right)}\right) I_0\left[\frac{k_m\left(1+k_m\right)}{2\left(\frac{E_b}{N_0} + 1 + k_m\right)}\right]$$

where Q_1, the first order Marcum Q-function, a_m, b_m, p_m and k_m are defined as hereafter

$$\mathrm{Q}_1(a, b) = \int_b^\infty x \exp\left[-\frac{x^2 + a^2}{2}\right] I_0(ax)\, dx$$

$$a_m = \sqrt{k_m\left[\frac{1+2p_m}{2(1+p_m)} - \sqrt{\frac{p_m}{1+p_m}}\right]}$$

$$b_m = \sqrt{k_m\left[\frac{1+2p_m}{2(1+p_m)} + \sqrt{\frac{p_m}{1+p_m}}\right]}$$

$$p_m = \frac{E_b/N_0}{1+k_m}$$

$$k_m = \frac{\sqrt{1-m^2}}{1-\sqrt{1-m^2}}$$

The PLL SNR, ρ, can be written in term of the modulation index θ as

$$\rho = \frac{C}{N_0 B_l} J_0(\theta)^2 = \frac{E_b}{N_0} \frac{1}{2J_1(\theta)^2} \frac{R_b}{B_l} J_0(\theta)^2. \tag{6.10}$$

In (6.10) R_b/B_l represents the ratio between bit rate (R_b) and loop bandwidth (B_l).

For bit rates less than 1 kHz (i.e. 7.8125 bps, the lowest bit rates in deep scenario), fast fading can be assumed since the phase error process varies during a bit interval. In such a case (6.8) can be approximated by replacing the bit SNR degradation with its mean over the Tikhonov PDF and reducing the double integral to a single one, so obtaining

$$P_b\left(\frac{E_b}{N_0}, m\right) = \int_0^\infty \mathrm{Q}\left(\sqrt{2\frac{E_b}{N_0}\nu^2 E\left[\cos^2(\phi)\right]}\right) \frac{\nu}{\sigma_m^2} \exp\left(-\frac{\nu^2 + a_m^2}{2\sigma_m^2}\right) d\nu \tag{6.11}$$

where

$$E\left[\cos^2(\theta)\right] = \frac{I_1'(\rho\nu^2)}{I_0(\rho\nu^2)}$$

However the BER degradation in (6.11) due to scintillation effects is not relevant since at low bit rates the bit SNR is significantly large and non ideal carrier tracking is negligible.

It is important to stress, however, that (6.7) and (6.10) take into account the impact of the thermal noise only. So, they are able to model the effect of synchronization errors only in the particular case of a receiver bandwidth large enough to filter out completely the impact of plasma on the phase. Moreover, as the bandwidth of the Costas loop for the subcarrier demodulation is typically smaller than the PLL one, the phase jitter introduced by the subcarrier recovery process can be neglected in the model.

6.1.1 Operation Scenarios

Depending on the value of the symbol rate w.r.t. the (reciprocal of) the coherence time $(\Delta t)_c$, we can define the following different operation scenarios:

- Extremely (or "Ergodic") low rate links (ELRL): Where the statistical averages over the encoded bit fairly represent the average over all time.
- Low rate links (LRL): when the channel varies during the transmission of a bit.
- Medium rate links (MRL): when the channel does not vary during the transmission of an encoded symbol, but varies during the transmission of a codeword.
- High rate links (HRL): when the channel does not vary during the transmission of a codeword.

The ELRL scenario can be applied only when the channel varies many times (e..g., $>$ 100 times) during the transmission of an encoded symbol. Clearly, it is a rather unpractical situation (the value of $(\Delta t)_c$ should be extremely small); so, despite the fact this scenario can be investigated in analytical terms, it is not considered of interest and will not be examined in the following.

A semi-analytical approach can be used also for the HRL scenario. The starting point is constituted by the performance over the AWGN channel. More precisely, setting E_b/N_0, we can define a function $g(\alpha)$ which expresses the CER experienced over the AWGN channel (baseline probability) by using the considered error correcting code, determined analytically or, more frequently, through numerical simulations. Obviously we can consider both the BER and the CER. However, in the presence of an error correcting code the latter is usually more important than the former. For this reason, we refer to the CER curves instead of the BER curves.

The advantage of the first and the last cases is that the performance over channels with scintillation can be extrapolated from the performance estimated over the channel with AWGN only. Contrary to the ELRL and the HRL scenarios, no theoretical treatment is available for the LRL and the MRL scenarios to quantify the impact of the amplitude scintillation and the phase error. So, for these cases, the simulation program incorporates the generation of Rice and Tikhonov samples and uses them, in the decoding algorithm, according to the assumed operation conditions.

Then, by assuming applicability of the Tikhonov distribution (in the sense specified above and with the limitations) the following expression can be applied

$$\begin{array}{l}\int\limits_{0}^{\sqrt{\frac{\bar{\alpha}}{\alpha}}}\int\limits_{-\pi}^{\pi} g\left(v^2\alpha\cos^2\phi\right)p_V\left(v\right)p_\Phi\left(\phi|v\right)dvd\phi \leq \mathrm{CER}\left(\alpha\right) \leq \\ \int\limits_{0}^{\sqrt{\frac{\bar{\alpha}}{\alpha}}}\int\limits_{-\pi}^{\pi} g\left(v^2\alpha\cos^2\phi\right)p_V\left(v\right)p_\Phi\left(\phi|v\right)dvd\phi\ + \\ \int\limits_{\sqrt{\frac{\bar{\alpha}}{\alpha}}}^{\infty}\int\limits_{-\pi}^{\pi} g\left(v^2\bar{\alpha}\cos^2\phi\right)p_V\left(v\right)p_\Phi\left(\phi|v\right)dvd\phi\end{array} \tag{6.12}$$

where $\bar{\alpha}$ represents the maximum value of α for which $g(\alpha)$ is known. Equation (6.12) provides a lower bound and an upper bound to the value of the CER for any E_b/N_0. In many cases the value of $\bar{\alpha}$ is high and the CER can be approximated as follows

$$\mathrm{CER}\left(\alpha\right) \approx \int\limits_{0}^{\sqrt{\frac{\bar{\alpha}}{\alpha}}}\int\limits_{-\pi}^{\pi} g\left(v^2\alpha\cos^2\phi\right)p_V\left(v\right)p_\Phi\left(\phi|v\right)dvd\phi.$$

On the contrary, when the value of $\bar{\alpha}$ is not sufficiently high, the gap between the lower and the upper bounds may be large. In such a case, in principle, it is necessary to plot them both, but it is impossible to establish how much the actual curve is far from the limits. For this reason, it is better to draw the curves up to the maximum value of E_b/N_0 for which the lower bound and the upper bound are indistinguishable.

The HRL scenario may be of interest (depending on the value of $(\Delta t)_c$) for TM links, as the values of the data rate R_b are rather large; however, its applicability also depends on the codeword length that, for TM codes, may be very large as well. On the other hand, the HRL scenario is rather unlikely for TC links where, despite the fact that the codeword length is small, the codeword duration is generally long (because of the long bit duration). Of

Table 6.3: Supported TM coding schemes for BepiColombo

Scheme	R	Max. sym. rate (sps)	Min. sym rate (sps)
RS(255, 223)+CC(7, 1/2), I = 5	223/510	699050	21.33
PCTC(17848, 8920)	1/2	1398101.3333	21.33
PCTC(35696, 8920)	1/4	1398101.3333	42.6667

Table 6.4: Supported TM coding schemes for Solar orbiter

Scheme	R	Max. sym. rate (sps)	Min. sym. rate (sps)
PCTC(17848, 8920)	1/2	$2 \cdot 10^6$	21.33
PCTC(35696, 8920)	1/4	$3.33 \cdot 10^6$	42.6667

course, this depends also on the fading duration, which is a function of the scintillation index.

6.1.2 Typical operation conditions

In a first series of evaluations, we have considered the error correcting codes adopted in flying or next-to-flight European Space Agency (ESA) missions. More precisely, for better evidence, BepiColombo and Solar Orbiter missions have been taken as a reference, and also used in the subsequent numerical examples. For TC, both they use a BCH(63, 56) code, with symbol rates from 4 ksps down to 7.8125 sps. For TM, the supported coding schemes are reported in Tab. 6.3 for BepiColombo and in Tab. 6.4 for Solar Orbiter, together with the maximum and minimum symbol rate.

RS(255, 223) + CC(7, 1/2), $I = 5$ denotes a RS code with length $N = 255$ symbols and dimension $K = 223$ symbols (each symbol consisting of 8 bits) concatenated with a convolutional code (CC) with rate 1/2 and constraint length 7, and with a row-by-column interleaver having interleaving depth I = 5 in the middle. For simplicity, in the following this scheme will be denoted as RSCC. The code rates indicated in Tabs. 6.3 and 6.4 for the PCTCs are nominal, in the sense these codes require some extra bits for termination, whose impact on R, however, is quite marginal. These codes are described in

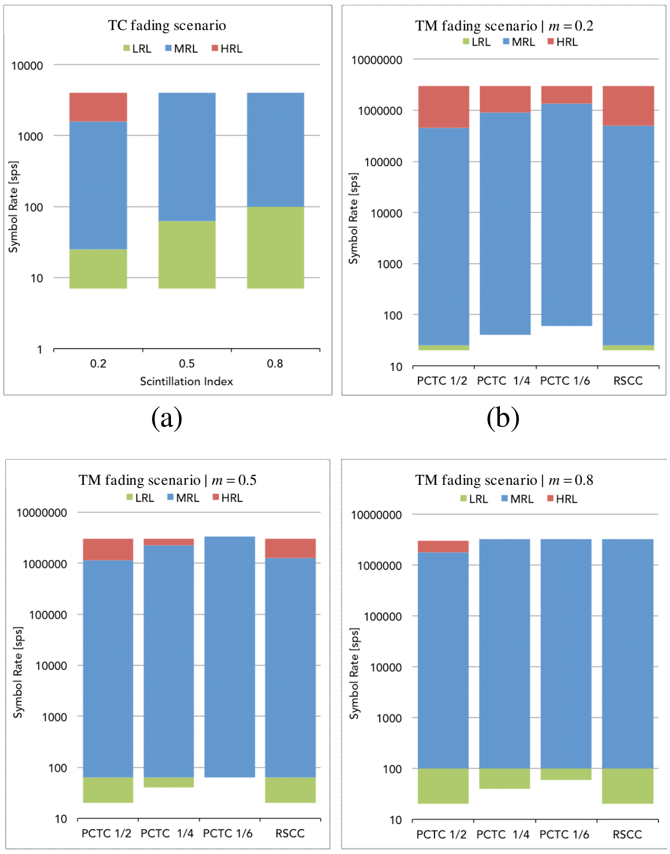
Table 6.5: Coherence time as a function of the scintillation index

m	$(\Delta t)_c$ [ms]
0.2	40
0.5	16
0.8	10

detail in [86] and [87].

As underlined in Sec. 6.1.1, the considered operating scenario depends on the value of $(\Delta t)_c$, whose inverse is defined as the Doppler spread. The moving irregularities in the solar plasma produce replicas of the signal, each one affected by its proper Doppler shift. The recombination of these replicas on the ground produces a Doppler spread, which is a function of the scintillation index, and consequently of the SEP angle. According with these considerations, it is evident that the coherence time depends on the value of the scintillation index. Some typical values of $(\Delta t)_c$, for different m, extracted from X band data of the mentioned (and other) missions are reported in Tab. 6.5. Using the values in Tab. 6.5, it is possible to determine, for any value of the scintillation index, the operation scenarios, LRL, MRL and HRL, where the codes work as a function of m (and, therefore, of the SEP). These are summarized in Fig. 6.2. For completeness, also the case of the PCTC(53544, 8920), that is, with nominal $R = 1/6$ has been added. Indeed, this code is also included in the CCSDS recommendation [87] and used, for example, in the ExoMars mission.

From this figure, we see that the region of major interest (in the sense it occurs more frequently) for TC and TM codes, is the MRL one. Thus, for the sake of brevity, in the following we consider only this operation scenario.



(a) (b)

(c) (d)

Figure 6.2: Regions LRL, MRL and HRL for the coherence times reported in Tab. 6.5: (a) BCH code in TC; (b) codes in TM with $m = 0.2$; (c) codes in TM with $m = 0.5$; (d) codes in TM with $m = 0.8$.

6.2 Numerical results

In this section we show some examples of the results obtained with different code families over a channel with solar scintillation. First in Sec. 6.2.1 we consider the case in which the fading affects only the amplitude of the signal. Then, in Sec. 6.2.2 we add the phase scintillation. To measure the amplitude and phase fading we define a parameter called Fading Period (FP) that represents the number of bits during which the fading sample is constant.

6.2.1 Only amplitude scintillation

One possible approach to compare the performance of different codes, is to fix the *FP* value. However, when codes with different code rate are considered and the source emits a fixed number of bits/s of information, this choice corresponds to simulate the performance over scenarios with different $(\Delta t)_c$ (one for each code rate). Wishing to realize a comparison for the same value of $(\Delta t)_c$, the fading period must be adapted, as a function of the code rate. As an example, if the fading period is $FP = 150$ encoded symbols for the code with rate $R = 1/2$, it must be changed into $FP = 172$ encoded symbols for the code with rate $1/2 \cdot 223/255$ (that is the case of the RS(255, 223) code + CC(7, 1/2)), into $FP = 300$ encoded symbols for the code with rate 1/4 (that is the case of the PCTC(35696, 8920)), and into $FP = 450$ encoded symbols for the code with rate 1/6 (that is the case of the PCTC(53544, 8920)).

A comparison between the CER performances of these codes is shown in Fig. 6.3 for $m = 0.5$ and in Fig. 6.4 for $m = 0.9$. The PCTCs are decoded by using the BCJR algorithm [88]. For a better figures readability, we omit the performance of the considered codes over the AWGN channel, since they are well known and reported in [87].

The assumption of equal coherence time implies that the adoption of the PCTCs with lower code rate is no longer preferable as in the only AWGN channel [87]. The performance of the PCTC(53544, 8920) and the PCTC(35696, 8920) becomes, in fact, worse than that of the PCTC(17848, 8920), at least in the error rate region of major interest. This can be explained by considering that, despite the fact that channel conditions may remain unfavorable for the same fraction of time, in case of codes with lower rates fading affects a larger number of consecutive encoded symbols that, evidently, the decoder is not able to compensate. So, the conclusion is that the adoption of the PCTCs with low rate (i.e., longer codes, for fixed $k = 8920$ bits) should be discouraged, in the presence of amplitude scintillation, when m is large (e.g., $m = 0.5$ and $m = 0.9$).

These results are in line with those obtained in other space missions

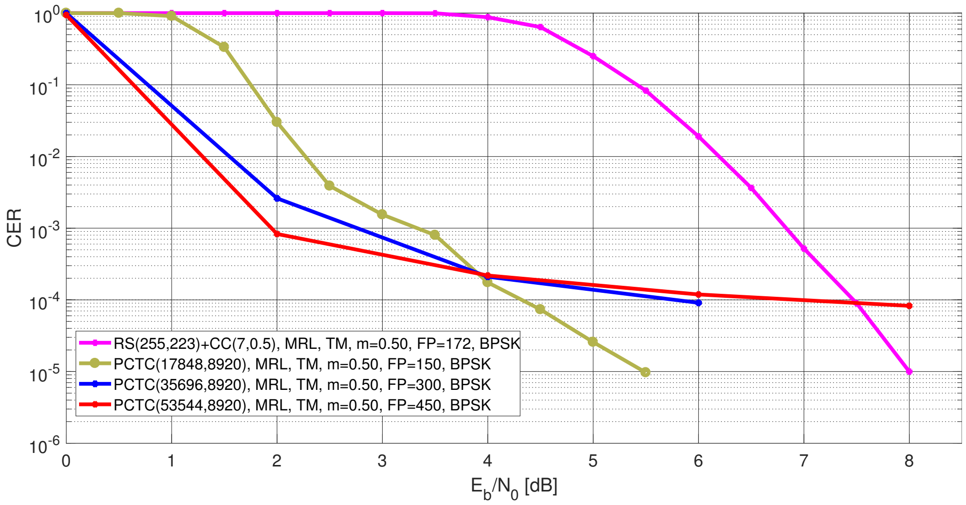


Figure 6.3: CER performance comparison between TM codes currently in use in the MRL scenario with the same coherence time. Amplitude scintillation only; $m = 0.5$. $FP = 150$ encoded symbols for the PCTC(17848, 8920); the other values of FP are properly scaled accordingly.

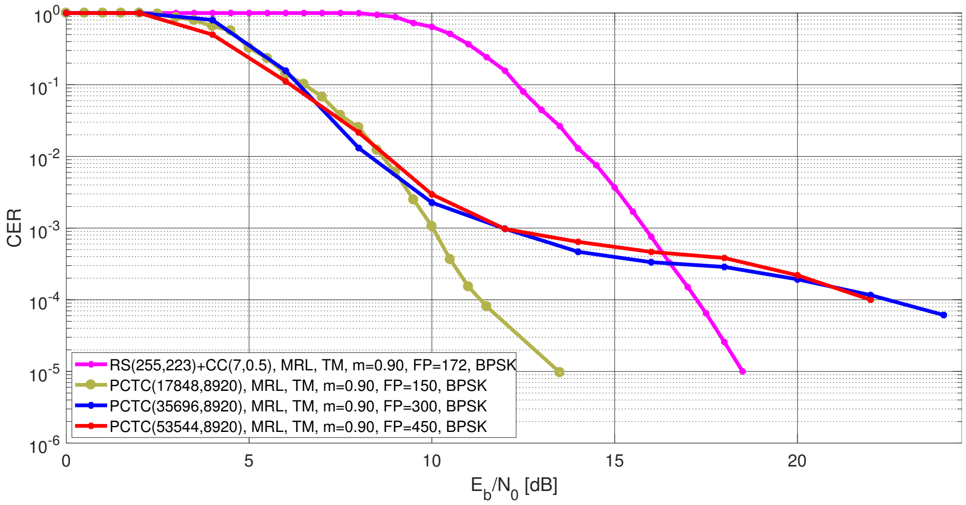


Figure 6.4: CER performance comparison between TM codes currently in use in the MRL scenario with the same coherence time. Amplitude scintillation only; $m = 0.9$. $FP = 150$ encoded symbols for the PCTC(17848, 8920); the other values of FP are properly scaled accordingly.

(e.g., the Solar TErrestrial RElations Observatory (STEREO) mission of the National Aeronautics and Space Administration (NASA)) and confirm the vulnerability, in the case of slow fading, of the low rate PCTCs codes proposed by the CCSDS in [87]. From this observation, the Coding and Synchronization working group of the CCSDS has decided to open a conjuncted ESA/NASA action that aims to improve the performance of these codes or even propose new coding schemes for low rate transmissions.

Another interesting comparison is with the Accumulate, Repeat-by-4, and Jagged Accumulate (AR4JA) standard LDPC codes [87]. A first comparison is shown in Fig. 6.5 to Fig. 6.7 for the case of $FP = 150$ encoded symbols. As usual, different values of m are considered. All the LDPC codes are decoded by using the normalized min-sum (NMS) algorithm [89]. All codes are characterized by $R = 1/2$ (apart from the small deviation of the PCTC(17848, 8920), which is due to the termination bits); so the comparison is fair and the assumption of the same value of FP ensures the coherence time is also the same for all simulations. From the figures, we see that, except for high error rates, the LDPC(32768, 16384) code is able to outperform the PCTC(17848, 8920) for any value of the scintillation index. The LDPC(8192, 4096) code is worse than the PCTC(17848, 8920) for $m = 0.2$ but its performance becomes better than that of the PCTC(17848, 8920) for $m = 0.5$ and $m = 0.9$. The LDPC(2048, 1024) code, instead, is always beaten by the PCTC(17848, 8920) but this was somehow expected because of its significantly smaller length.

The comparison is repeated in Fig. 6.8 to Fig. 6.10 by assuming $FP = 3500$ encoded symbols. This fading period exceeds the codeword length of the LDPC(2048, 1024) code, that therefore has been not considered in this case. From these figures, we see that the LDPC(32768, 16384) code outperforms the PCTC(17848, 8920) for any considered value of the scintillation index. Differently from the examples with $FP = 150$ encoded symbols, the LDPC(8192, 4096) code has better performance than that of the PCTC(17848, 8920) only for $m = 0.9$. Moreover, for high values of the scintillation index the performance of the PCTC(17848, 8920) and LDPC(8192, 4096) are very close.

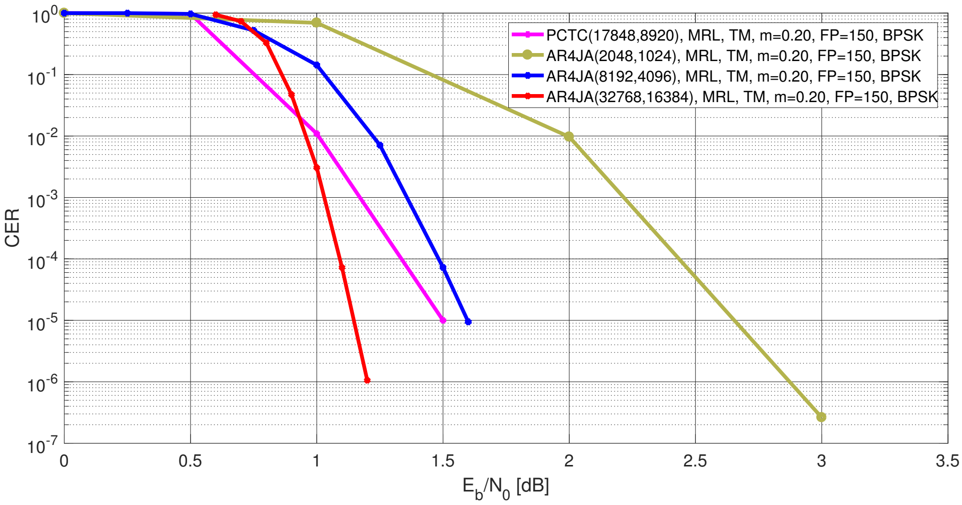


Figure 6.5: CER performance comparison between the PCTC(17848, 8920) and different standard codes with $R = 1/2$; MRL scenario with $FP = 150$ encoded symbols and $m = 0.2$; amplitude scintillation only.

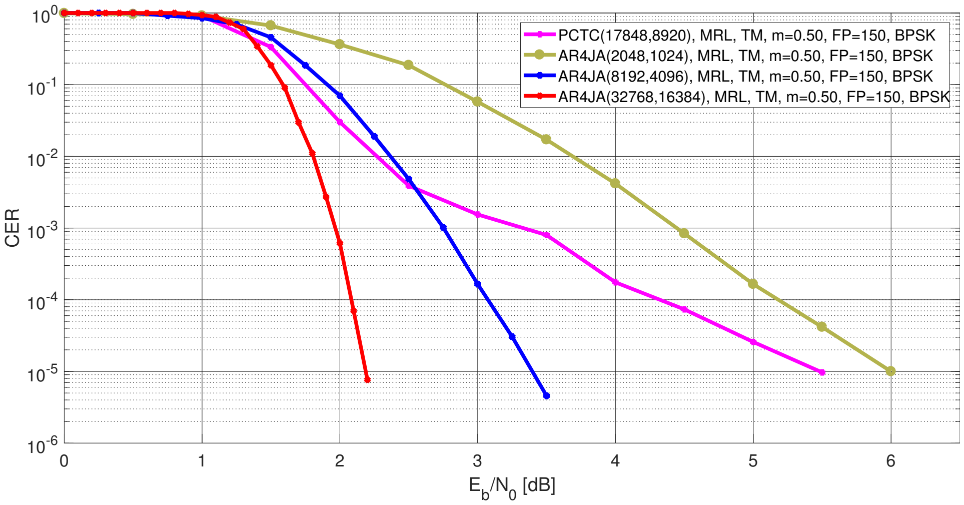


Figure 6.6: CER performance comparison between the PCTC(17848, 8920) and different standard codes with $R = 1/2$; MRL scenario with $FP = 150$ encoded symbols and $m = 0.5$; amplitude scintillation only.

6.2.2 Amplitude and phase scintillation

In this section, we report some examples of performance evaluation by including in the simulation the effect of the Tikhonov distribution, for the

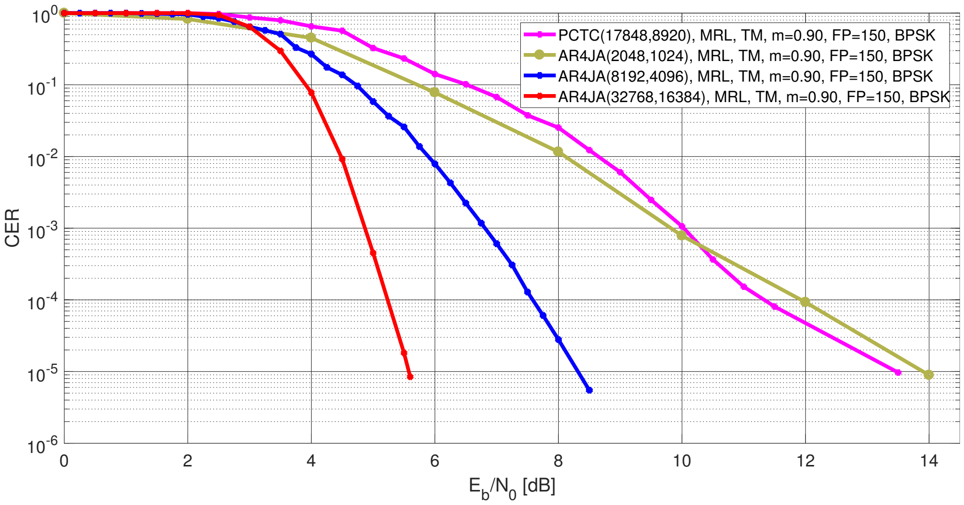


Figure 6.7: CER performance comparison between the PCTC(17848, 8920) and different standard codes with $R = 1/2$; MRL scenario with $FP = 150$ encoded symbols and $m = 0.9$; amplitude scintillation only.

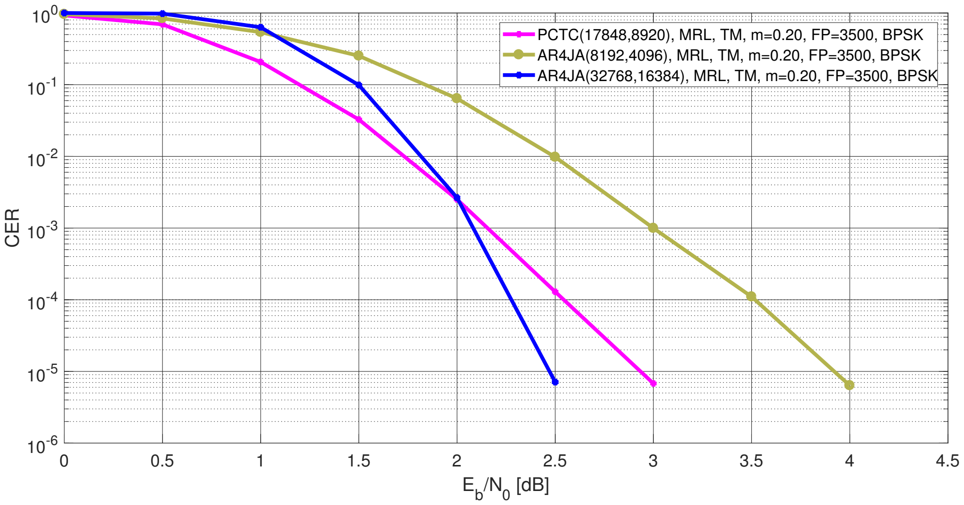


Figure 6.8: CER performance comparison between the PCTC(17848, 8920) and different standard codes with $R = 1/2$; MRL scenario with $FP = 3500$ encoded symbols and $m = 0.2$; amplitude scintillation only.

phase, in addition to the Rice distribution, for the amplitude. The use of the Tikhonov distribution to model synchronization errors is appropriate (in the sense it provides reliable results) under suitable conditions, also related to the system parameters, especially the extent of the loop bandwidth. So, the

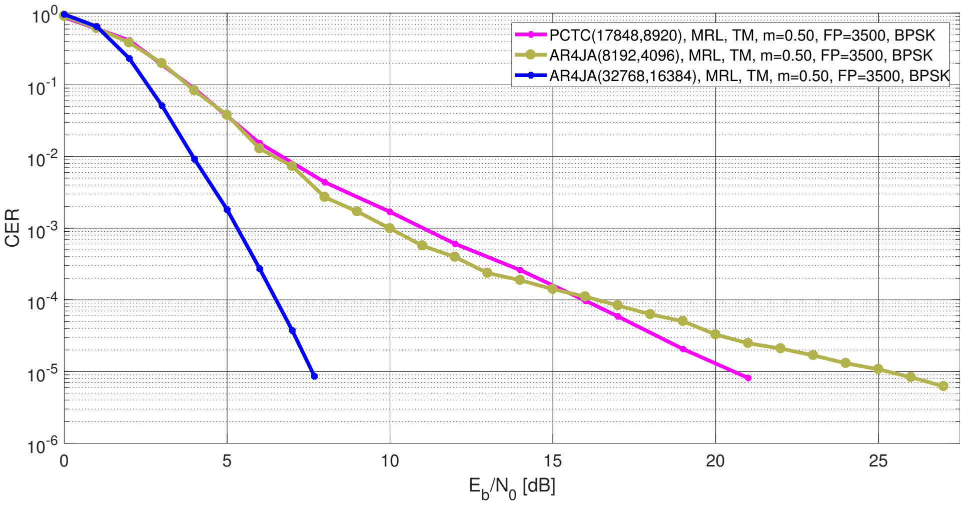


Figure 6.9: CER performance comparison between the PCTC(17848, 8920) and different standard codes with $R = 1/2$; MRL scenario with $FP = 3500$ encoded symbols and $m = 0.5$; amplitude scintillation only.

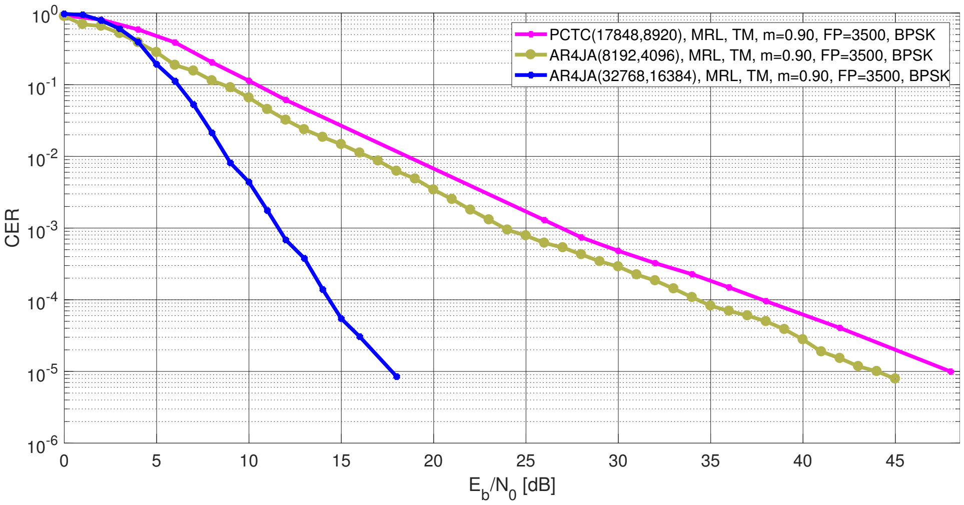


Figure 6.10: CER performance comparison between the PCTC(17848, 8920) and different standard codes with $R = 1/2$; MRL scenario with $FP = 3500$ encoded symbols and $m = 0.9$; amplitude scintillation only.

results obtained by using this model are valid only when the loop bandwidth is sufficiently large to follow the phase due to plasma in the phase locked loop (PLL). By removing this constraint on the loop bandwidth, the more general case has been addressed within the RESCUe project (mentioned at the beginning of this thesis) through an end-to-end simulator. Nevertheless, our task (where this work has provided a contribution), has been focused on the baseband simulations, which do not consider higher order issues as the modeling of the synchronization loop.

Due to large length of TM codes that affects the simulation time, we limit to consider the MRL scenario and TC codes. In this context, after a wide discussion within the CCSDS, there is now a general and consolidated consensus about the adoption of two short LDPC codes, namely the LDPC(128, 64) code and the LDPC(512, 256) code, as valuable alternatives to the current standard BCH code in [86]. The new short LDPC codes are described in detail in [90]. Since, these short LDPC schemes have better performance than the BCH code, in the following we consider only these coding schemes. Moreover, although PCTCs are not recommended for the TC link, an evaluation of their performance is of interest also in this context. This way, as the purpose of this part is basically to compare the performance of the PCTCs against the LDPC codes, we limit to study the behavior of these codes. For the LDPC(128, 64) code we suppose adoption of the hybrid decoding algorithm [91–93], since it provides the best performance. The simulator assumes, as an example, a modulation index 0.9 rad-pk.

Figures 6.11, 6.12 and 6.13 show the CER performance comparison between the considered codes, by assuming $FP = 8$ encoded symbols, $R_b/B_l = 1.5$, and different values of m. For $m \geq 0.5$ the slope of the CER curve for the LDPC(512, 256) code becomes significantly more favorable than that of the PCTC(512, 256), to the point that the former overcomes the latter, at $\text{CER} \leq 7 \cdot 10^{-5}$ for $m = 0.9$.

The analysis is repeated from Fig. 6.14 to Fig. 6.16, by assuming $FP = 32$ encoded symbols and maintaining unchanged the other parameters. In presence of a longer fading, the performance of the LDPC(512, 256) code becomes rapidly preferable to that of the PCTC(512, 256). The LDPC code offers a small extra-gain even for $m = 0.2$. For $m = 0.9$, the extra-gain is about 2.1 dB at $\text{CER} = 10^{-3}$, while it reaches the significant value of 5.5 dB at $\text{CER} = 10^{-5}$.

In essence, we can say that the LDPC codes (the longer one, in partic-

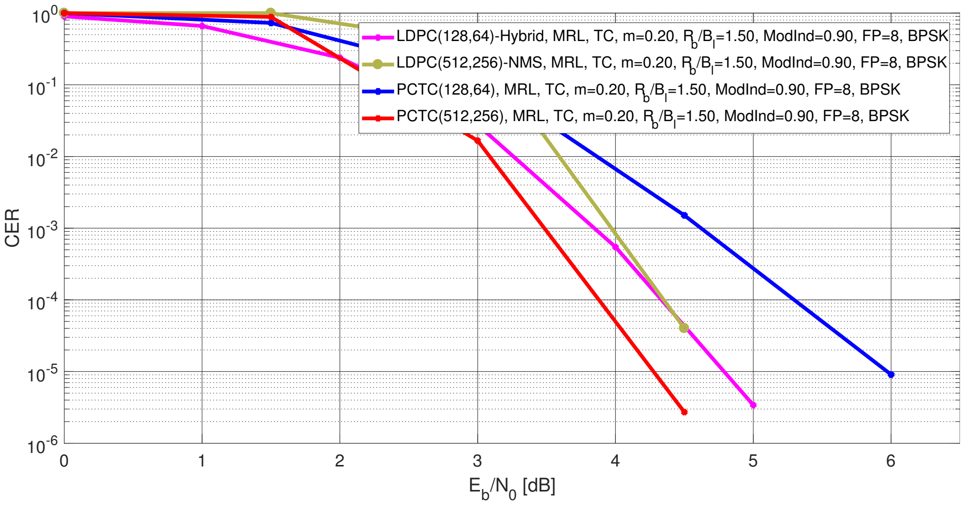


Figure 6.11: CER performance comparison between LDPC codes and PCTCs in the MRL scenario with $FP = 8$ encoded symbols, by assuming $m = 0.2$, in the presence of amplitude scintillation and synchronization error (Tikhonov model).

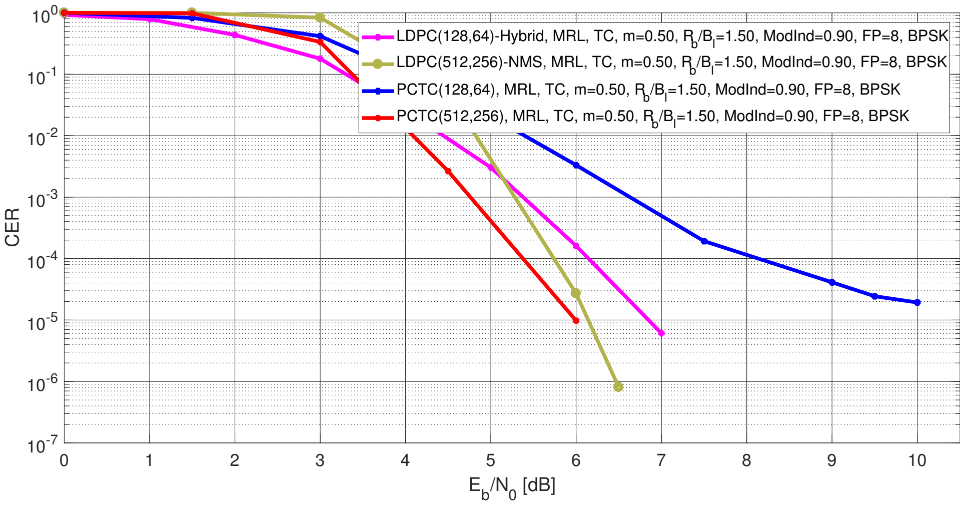


Figure 6.12: CER performance comparison between LDPC codes and PCTCs in the MRL scenario with $FP = 8$ encoded symbols, by assuming $m = 0.5$, in the presence of amplitude scintillation and synchronization error (Tikhonov model).

ular) may become preferable to the PCTCs for, relatively, large values of the coherence time and high scintillation index (more and more as lower and

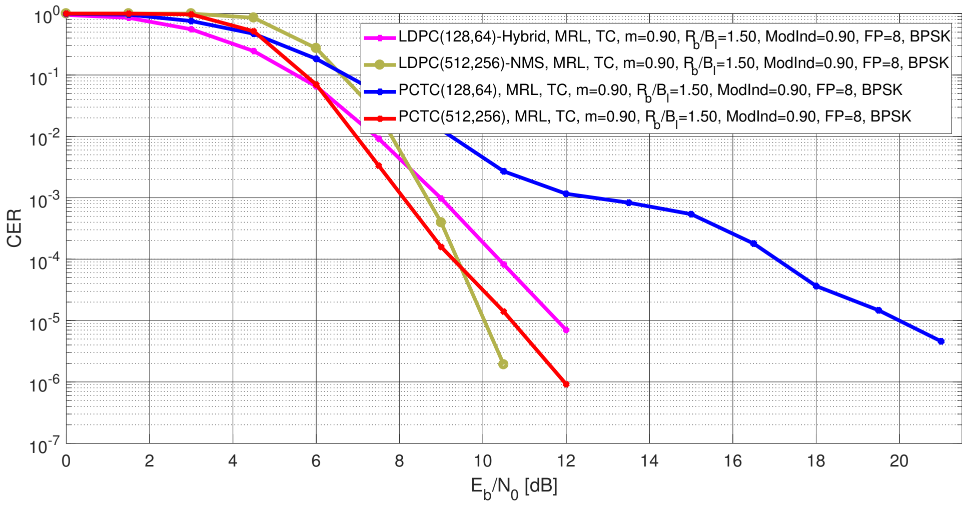


Figure 6.13: CER performance comparison between LDPC codes and PCTCs in the MRL scenario with $FP = 8$ encoded symbols, by assuming $m = 0.9$, in the presence of amplitude scintillation and synchronization error (Tikhonov model).

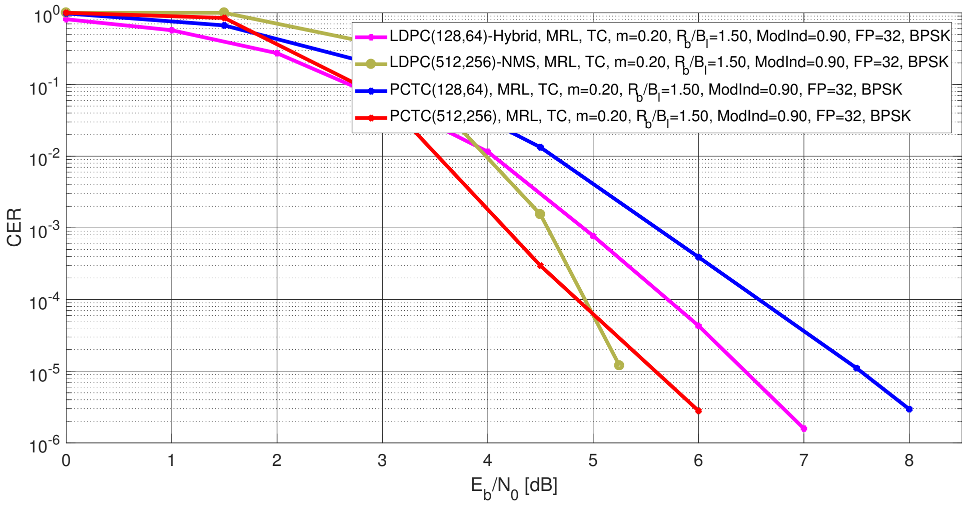


Figure 6.14: CER performance comparison between LDPC codes and PCTCs in the MRL scenario with $FP = 8$ encoded symbols, by assuming $m = 0.2$, in the presence of amplitude scintillation and synchronization error (Tikhonov model).

lower values of the CER are considered). The relevant point is that such a phenomenon, already evident in the presence of amplitude scintillation only,

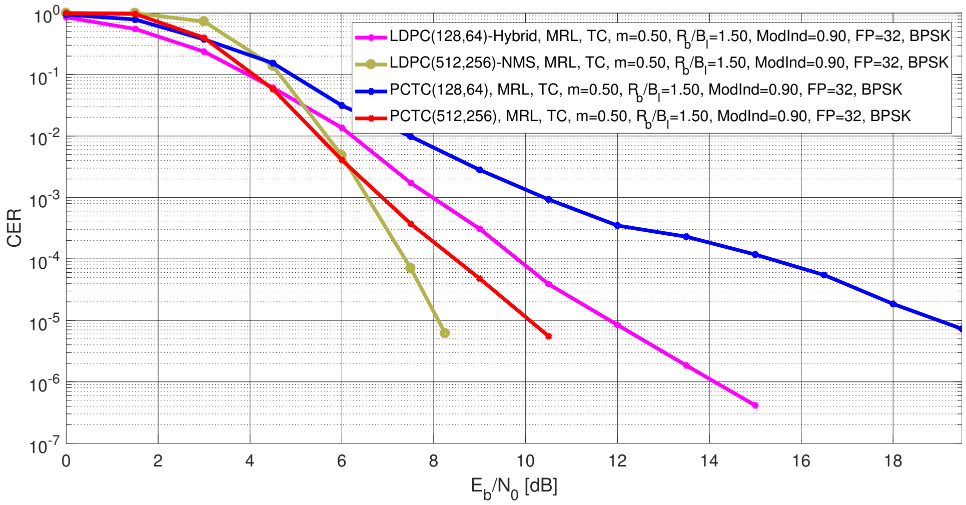


Figure 6.15: CER performance comparison between LDPC codes and PCTCs in the MRL scenario with $FP = 8$ encoded symbols, by assuming $m = 0.5$, in the presence of amplitude scintillation and synchronization error (Tikhonov model).

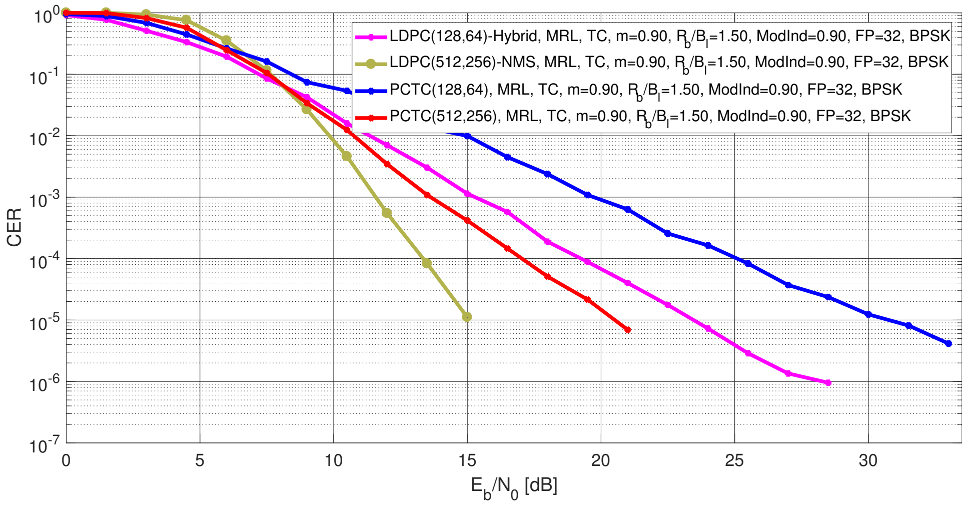


Figure 6.16: CER performance comparison between LDPC codes and PCTCs in the MRL scenario with $FP = 8$ encoded symbols, by assuming $m = 0.9$, in the presence of amplitude scintillation and synchronization error (Tikhonov model).

is accentuated by the presence of the synchronization error, at least when modeled through the Tikhonov distribution. Then, though limited by the applicability of the model, these results are interesting to address the choice of the codes in view of facing the most severe operation conditions.

6.3 Performance with non-coherent modulation schemes

In scenarios in which the BPSK is unusable, as the one where the synchronization error is considered, modulation schemes based on non–coherent communications, as the FSK, must be adopted. Let us consider first the case of binary formats. The fact to use non-coherent detection yields an additional loss w.r.t. the BPSK. In absence of coding, the amount of this loss over the AWGN channel is well known: in the order of 4 dB in the case of 2-FSK. Contrary to phase shift keying (PSK), FSK modulation allows to improve the error rate performance by increasing the cardinality of the constellation, that is, assuming $M > 2$ orthogonal waveform. So, a gain of about 3 dB are reached by the uncoded system, over the AWGN channel, for the error rates of interest, when passing from $M = 2$ to $M = 4$. Even more, the error rate performance of uncoded 8-FSK with non-coherent demodulation becomes better than that of uncoded BPSK. An introductory example is shown in Fig. 6.17, where the performances over the AWGN channel have been compared for the considered modulation schemes without coding. In this case, since we compare uncoded transmissions the use of the BER as a metric is more appropriate. The price to pay when non–coherent modulation schemes are adopted is in terms of enlarged bandwidth occupation, that in fact increases according to the classical law $M/\log_2 M$.

In this work, the performance achieved with differential modulation schemes, as the differential phase-shift keying (DPSK) (only binary format), has been evaluated, too. In such case, we have verified as these modulation schemes are not preferable to the FSK one. Moreover, the latter has an easier implementation than differential formats. Thus, for the sake of brevity, results obtained with the DPSK modulation are omitted.

As in the present work, coherently with the RESCUe project, the band-

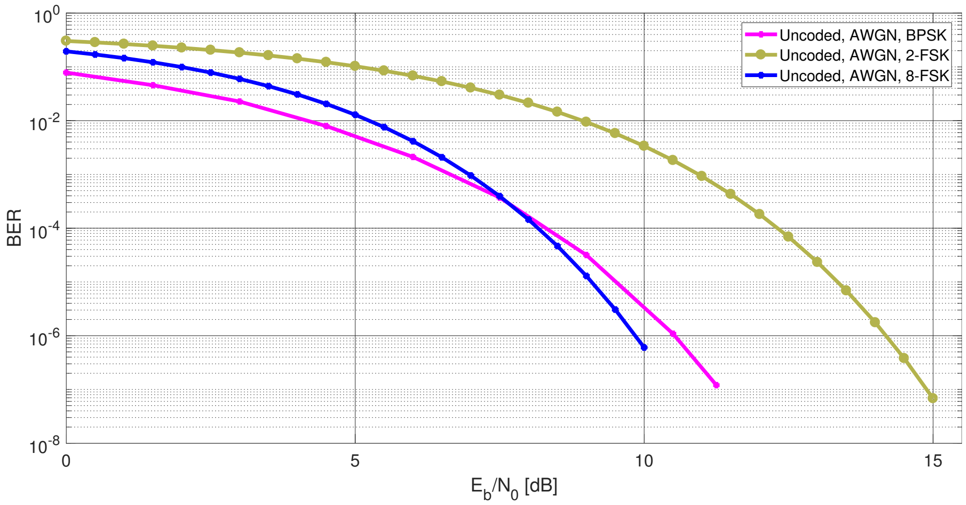


Figure 6.17: Comparison between the BER performance achievable by using uncoded transmission over the AWGN channel with coherent (BPSK) and non-coherent (FSK) demodulation.

width has not been set as a constraint, we are justified to propose the adoption of $M-$FSK. A good candidate in this sense, for the reasons explained above, seems to be 8-FSK. Hence, in the following of this section we present some preliminary evaluation of the performance of coded 8-FSK modulated systems, focusing attention, for explicative purposes, on the TC LDPC(128, 64) code used over the MRL scenario in the presence of amplitude scintillation only. Moreover, BPSK will be considered for the sake of comparison.

An example of performance evaluation of the 8-FSK modulation format, in the presence of amplitude scintillation (only) is reported in Fig. 6.18, for the case with $m = 0.5$, different decoding algorithms, in comparison with that of the BPSK and the FSK. The fading period has been set equal to FP = 8 symbols for the binary format and FP = 3 symbols for the 8-FSK one. This way, taking into account that the duration of an 8-FSK symbol is three times that of a binary symbol, the two schemes operate, approximately, under the same value of the coherence time. Its value would be exactly the same by assuming FP = 2.67 encoded symbols for 8-FSK. Our choice, FP = 3 symbols, permits us to operate with integer numbers (while the performance difference w.r.t. the exact value is quite negligible). The figure confirms that

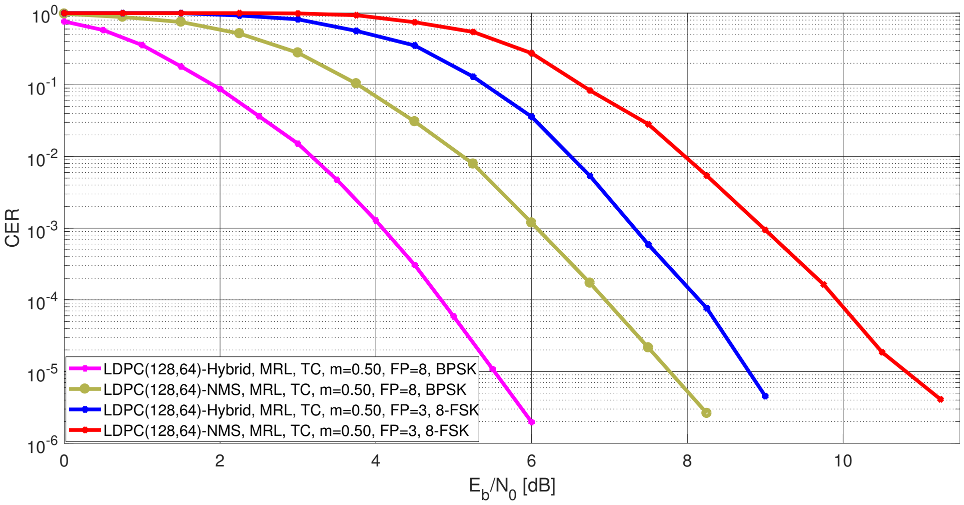


Figure 6.18: CER performance comparison for the LDPC(128, 64) code by using BPSK and 8-FSK modulation schemes in the presence of amplitude scintillation, for the MRL scenario with $m = 0.50$ and approximately equal coherence time.

the performance of 8-FSK, for both the decoding algorithms adopted, is worse than that of the BPSK. Despite its not favorable error rate performance, the advantage of 8-FSK is in its simplicity (no phase recovery is required), although this is paid with a three time larger bandwidth, that however, as already stressed, can be tolerated for the considered application. The analysis is repeated in Fig. 6.19 for the case of $m = 0.9$, leaving unchanged the other parameters and the decoding options. In comparison with Fig. 6.18, in this more critical scenario the gap between BPSK and 8-FSK is slightly emphasized. On the other hand, the efficiency of the hybrid algorithm, against the NMS algorithm, is increased as well, and this justifies the intersection between the curve of 8-FSK with hybrid decoding and the curve of BPSK with NMS decoding.

A similar analysis has been developed by assuming a larger value of FP, namely, $FP = 32$ symbols for BPSK and, in order to have approximately the same coherence time, $FP = 11$ symbols for 8-FSK. Figures 6.20 and 6.21 refer to the case with $m = 0.5$ and $m = 0.9$, respectively. W.r.t. the results in Figs. 6.18 and 6.19 obtained with a smaller value of FP we observe that

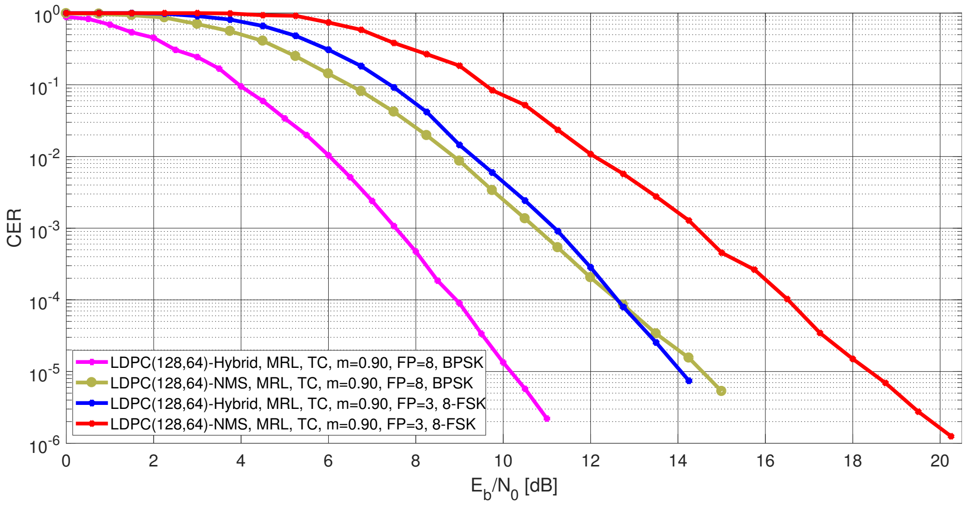


Figure 6.19: CER performance comparison for the LDPC(128, 64) code by using BPSK and 8-FSK modulation schemes in the presence of amplitude scintillation, for the MRL scenario with $m = 0.90$ and approximately equal coherence time.

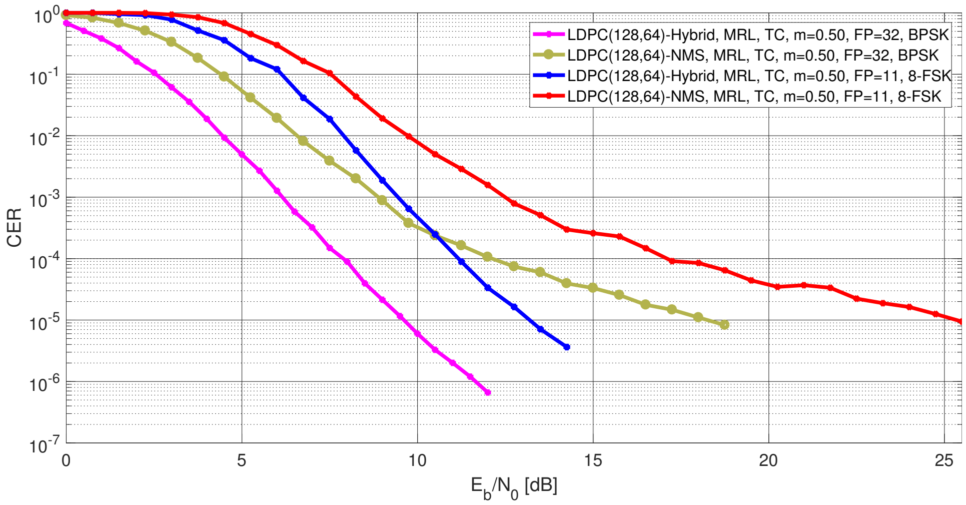


Figure 6.20: CER performance comparison for the LDPC(128, 64) code by using BPSK and 8-FSK modulation schemes in the presence of amplitude scintillation, for the MRL scenario with $m = 0.50$ and approximately equal coherence time.

the gap between BPSK and 8-FSK is larger.

Wishing to draw some conclusions from the results presented in this sec-

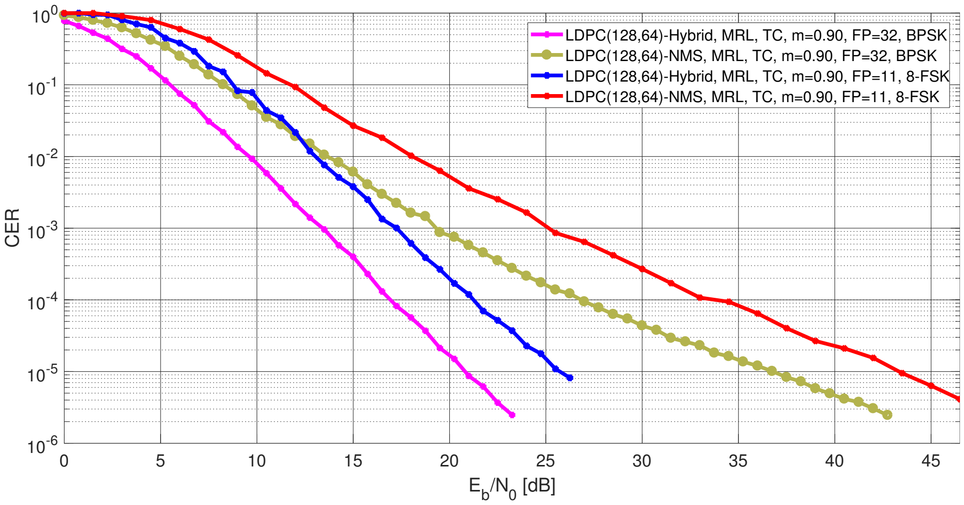


Figure 6.21: CER performance comparison for the LDPC(128, 64) code by using BPSK and 8-FSK modulation schemes in the presence of amplitude scintillation, for the MRL scenario with $m = 0.90$ and approximately equal coherence time.

tion, we can say that 8-FSK largely outperforms binary FSK but the minor efficiency in exploiting the applied error correcting scheme prevents this format to overcome BPSK, too.

This is due to the fact that consolidated decoding algorithms are optimized for coherent modulations and do not work equally well in the non-coherent case. On the other hand, to develop decoding algorithms which are more suited for non-coherent schemes (FSK in particular) is an open (not simple) issue and, to the best of our knowledge, no proved strong method is available in the literature. For the sake of brevity we omit the results concerning the 16-FSK, that have been derived as well during the study. Moreover, guessing that a further increase in the value of M (that is, above $M = 16$) can fill the gap w.r.t. BPSK is unrealistic as, even for the uncoded case over the AWGN channel, the improvement obtained passing from $M = 2^k$ to $M = 2^{k+1}$ becomes smaller and smaller for increasing M. Actually, we have verified that the increase in the value of M may be particularly effective in the case of large scintillation indexes (e.g., $m = 0.9$) but we must also consider that for these values the gap to fill, w.r.t. BPSK, is also larger. The error rate performance of coded M-FSK should become closer to that of BPSK when including phase scintillation that the Tikhonov distribution is not able to model properly. Even more important, the inclusion of phase scintillation might prevent the adoption of the BPSK format [94].

6.4 Summary

In this chapter we have compared standard and non standards coding schemes over a channel with solar scintillation. We have considered the presence of amplitude scintillation, without and with phase scintillation. After having discussed the probability density functions used to model these phenomena, we have provided several numerical results. As expected, the E_b/N_0 value required to achieve a target CER, increases according to the scintillation index and fading period values. In the case of synchronization error, the use of non-coherent modulations, as the FSK, is mandatory. In such scenario, under the hypothesis of loop bandwidth sufficiently large in the PLL, the Tikhonov distribution may be adopted to model the phase error. Performance obtained with M-FSK modulation schemes over a channel with only amplitude scintillation are shown. To the best of our knowledge, these results are not available in literature. By introducing the phase scintillation, that the baseband analysis is able to model only under certain conditions, the error rate performance of coded M-FSK should become closer to that of BPSK. As a counterpart, these modulation formats imply a bandwidth expansion factor M/log_2M which becomes higher and higher for increasing M.

Chapter 7

Concatenated polar codes for short packet communications

In this chapter, we propose error correcting codes able to improve the reliability in short packets communications. We adopt concatenated polar-cyclic codes, since they have been included in the recommendation of the next 5G system for short block regime [1]. To achieve our aims, we have proposed a theoretical analysis of these coding schemes able to estimate their performance under ML decoding. This analysis is carried out by deriving the average weight enumerating functions (AWEFs) of the concatenated schemes by following the well-known uniform interleaver approach [95]. In the analysis, the knowledge of the input output weight enumerating function (IOWEF) and the weight enumerating function (WEF) of the inner polar and outer cyclic code is required, respectively. However, the polar code IOWEF calculation through analytical methods is still an unsolved problem. Hence, we restrict our attention to short, high-rate polar codes for which the problem can be solved through a pragmatic approach. More precisely, we consider the dual code of the selected polar code and then we find its IOWEF by listing the codewords. Subsequently, by using the generalized MacWilliams identity [96], we obtain the IOWEF of the original polar code. The WEF of the outer cyclic code, instead, is computed by following the method presented in [97].

By adopting the uniform interleaver approach, we subsume the existence of an interleaver between the inner and the outer code, and attain the average performance of an ensemble composed by the codes obtained by selecting all possible interleavers. Our analysis shows that the performance of the concatenated scheme with and without interleaver (as proposed in [13]) may differ substantially. Similarly, by considering both CRC and BCH outer codes, we show that the choice of the outer code plays an important role in the short block length regime.

7.1 Distance spectrum analysis

We denote as N and K the outer cyclic code length and dimension, respectively, while n and k identify the same parameters for the inner polar code. Therefore, the code rates of the outer and inner code are $R_O = \frac{K}{N}$ and $R_I = \frac{k}{n}$, respectively. The two codes can be serially concatenated on condition that $N = k$, thus the overall code rate of the concatenated code is $R = \frac{K}{n}$.

Given a binary linear code $\mathcal{C}(n,k)$, its WEF is defined as [96]

$$A_{\mathcal{C}}(X) = \sum_{i=0}^{N} A_i X^i$$

where A_i is the number of codewords $\mathbf{c}$ with $w_H(\mathbf{c}) = i$. We focus on systematic polar codes (the reason of this choice will be discussed later); so, the first k bits of a codeword $\mathbf{c}$ coincide with the information vector $\mathbf{u}$, yielding $\mathbf{c} = (\mathbf{u}|\mathbf{p})$ with $\mathbf{p}$ being the parity vector. The IOWEF of a code $\mathcal{C}(n,k)$ is

$$A_{\mathcal{C}}^{\text{IO}}(X,Y) = \sum_{i=0}^{k} \sum_{\omega=0}^{n} A_{i,\omega}^{\text{IO}} X^i Y^{\omega}$$

where $A_{i,\omega}^{\text{IO}}$ is the multiplicity of codewords $\mathbf{c}$ with $w_H(\mathbf{u}) = i$ and $w_H(\mathbf{c}) = \omega$. The enumeration of the codeword weights entails a large complexity even for small code dimensions. In order to overcome this problem and obtain the IOWEF of the considered polar codes, we focus on short, high-rate polar codes and we exploit the generalized MacWilliams identity [96]. This approach was followed also for cyclic codes, for example, in [97] to compute the WEF of several CRCs. Denote by $\mathcal{C}^\perp$ the dual code of $\mathcal{C}$. Given the dual code WEF $A_{\mathcal{C}^\perp}(X)$, we can express the original code WEF $A_{\mathcal{C}}(X)$ as [96]

$$A_{\mathcal{C}}(X) = \frac{(1+X)^n}{|\mathcal{C}^\perp|} A_{\mathcal{C}^\perp}\left(\frac{1-X}{1+X}\right) \tag{7.1}$$

where $\left|\mathcal{C}^\perp\right|$ is the cardinality of the dual code. When the IOWEF is of interest, a significant reduction of the computational cost can be achieved by considering systematic codes. For such reason, in this work we have used only systematic inner polar codes. In the case of a systematic code $\mathcal{C}(n,k)$, it is convenient to derive the IOWEF from the input redundancy weight enumerating function (IRWEF) $A^{\mathrm{IR}}_{\mathcal{C}}(x,X,y,Y)$ defined as

$$A^{\mathrm{IR}}_{\mathcal{C}}(x,X,y,Y) = \sum_{i=0}^{k}\sum_{p=0}^{r} A^{\mathrm{IR}}_{i,p} x^{k-i} X^i y^{r-p} Y^p$$

where $A^{\mathrm{IR}}_{i,p}$ is the multiplicity of codewords $\mathbf{c}$ with $w_H(\mathbf{u}) = i$ and $w_H(\mathbf{p}) = p$, with $w_H(\mathbf{c}) = i + p$ and $n = k + r$. Hence, starting from the IRWEF of the dual code $A^{\mathrm{IR}}_{\mathcal{C}^\perp}(x,X,y,Y)$, we have [98, 99]

$$A^{\mathrm{IR}}_{\mathcal{C}}(x,X,y,Y) = \frac{1}{|\mathcal{C}^\perp|} A^{\mathrm{IR}}_{\mathcal{C}^\perp}(x+X, x-X, y+Y, y-Y).$$

Then, the IOWEF is obtained as

$$A^{\mathrm{IO}}_{\mathcal{C}}(X,Y) = A^{\mathrm{IR}}_{\mathcal{C}}(1, XY, 1, Y). \tag{7.2}$$

7.2 Union bound of the average block error probability of the concatenated scheme

Given an ensemble of binary linear codes $\mathscr{C}(n,k)$, the average block error probability (BEP) P_B of a random code $\mathcal{C} \in \mathscr{C}(n,k)$ under ML decoding over a BEC with erasure probability ϵ can be upper bounded as [100]

$$\begin{aligned}\mathbb{E}\left[P_B\left(\mathcal{C},\epsilon\right)\right] &\leq P_B^{(s)}(n,k,\epsilon)\\ &+\sum_{e=1}^{k}\binom{n}{e}\epsilon^e(1-\epsilon)^{n-e}\min\left\{1,\sum_{\omega=1}^{e}\binom{e}{\omega}\frac{\bar{A}_\omega}{\binom{n}{\omega}}\right\}\end{aligned} \tag{7.3}$$

where $\bar{A}_\omega = \mathbb{E}\left[A_\omega\left(\mathcal{C}\right)\right]$ is the average multiplicity of codewords of code $\mathcal{C}$ with $w_H(\mathbf{c}) = \omega$ and $P_B^{(s)}$ represents the BEP of an ideal maximum distance separable (MDS) code, with parameters n and k. The UB in (7.3) is applicable to every code ensemble whose average WEF is known.

When dealing with concatenated codes, it is commonplace to consider a general setting including an interleaver between the inner and the outer codes. The concatenated code ensemble is hence given by the codes obtained by selecting all possible interleavers. The special case without any interleaver can then be modeled as an identity interleaver. From [95], the AWEF of a concatenation formed by an inner polar code and an outer cyclic code can be obtained from the cyclic code WEF and the polar code IOWEF as

$$\bar{A}_\omega = \sum_{i=0}^{N}\frac{A_i^{\text{out}}\cdot A_{i,\omega}^{\text{IO,in}}}{\binom{N}{i}} \tag{7.4}$$

where A_i^{out} is the weight enumerator of the outer code and $A_{i,\omega}^{\text{IO,in}}$ is the input-output weight enumerator of the inner code (we remind that the average multiplicities resulting from (7.4) are, in general, real numbers).

The ensemble $\mathscr{C}(n,k)$ contains the codes generated by all possible interleavers. Thus, also bad codes (i.e., characterized by bad error rate performance) belong to the ensemble. It is clear that the bad codes adversely affect the average weight enumerator obtained through (7.4) causing a too pessimistic estimate of the error probability obtained through (7.3), w.r.t. that achieved by properly designed codes. A simple way to overcome this issue is to divide $\mathscr{C}(n,k)$ into the bad and good code subsets, and then derive the average weight enumerator only of good codes through the expurgated ensemble [10]. In fact, for a given integer $d^\star \geq 0$ and an arbitrary $\theta \in (0,1)$

we have

$$\Pr\{d_{\min} \leq d^{\star}\} \leq \sum_{\omega=0}^{d^{\star}} A_{\omega} - 1 \leq \theta$$

where $d_{\min}$ is the minimum distance of a code randomly chosen in the ensemble. A fraction of at least $1-\theta$ codes belonging to the original $\mathscr{C}(n,k)$ possess $d_{\min} > d^{\star}$. We refer to the subset of codes with $d_{\min} > d^{\star}$ as the expurgated ensemble. Therefore, the average weight enumerator of the expurgated ensemble can be upper bounded as [10, Sec. 2.2]

$$\bar{A}_{\omega}^{\text{exp}} \leq \frac{1}{1-\theta}\bar{A}_{\omega} \tag{7.5}$$

for $\omega > d^{\star}$, whereas $\bar{A}_{\omega}^{\text{exp}} = 0$ for $1 \leq \omega \leq d^{\star}$. Hence, through (7.3) and (7.5) the average performance of the expurgated ensemble is derived. In this thesis we have assumed $\theta = 0.5$.

Studying the dual codes and exploiting MacWilliams identities allow considerable reductions in complexity of exhaustive analyses as long as the original code rate is sufficiently large. This will be the case for the component codes considered next, which are characterized by $R_O, R_I > \frac{1}{2}$. Therefore, in our case (7.1) and (7.2) can effectively be exploited to calculate A_i^{out} and $A_{i,\omega}^{\text{IO,in}}$ in (7.4).

7.3 Code examples

In this section we consider several examples of polar-cyclic concatenated codes and assess their performance through the approach described in the previous sections. Our focus is on short, high rate component codes, which allow to perform exhaustive analysis of their duals in a reasonable time. Our results are obtained considering a BEC with erasure probability ϵ. As known, in the polar code design a fixed value of the error transition probability is considered. As usual in literature, in each of the following examples the polar code is designed by using $\epsilon = 0.3$. All performance curves provided next are obtained through (7.3). We consider codes with $n = 64$ bits and a CRC or a (shortened) BCH outer code, with N according to the polar code dimension.

In particular, we use a CRC-8 and a CRC-16 with the following generator polynomials [97]

- CRC-8: $g(x) = x^8 + x^2 + x + 1$;
- CRC-16-CCITT: $g(x) = x^{16} + x^{12} + x^5 + 1$.

We also consider two BCH codes that have the same redundancy as the CRC-8 and CRC-16 codes. Thus, for the same rate, a performance comparison of the results achieved by using a CRC or a BCH outer code is feasible and fair. For the case without interleaver considered in [13], the generator matrix $\mathbf{G}$ of the concatenated code can be obtained from the cyclic and polar code generator matrices $\mathbf{G}_C$ and $\mathbf{G}_P$, respectively, as

$$\mathbf{G} = \mathbf{G}_C \cdot \mathbf{G}_P.$$

When we instead consider the more general case with an interleaver between the inner and outer codes, we have

$$\mathbf{G} = \mathbf{G}_C \cdot \mathbf{\Pi} \cdot \mathbf{G}_P \tag{7.6}$$

where $\mathbf{\Pi}$ is an $N \times N$ permutation matrix representing the interleaver. Considering all codes in $\mathscr{C}(n,k)$, (7.4) leads to their AWEF and hence to the average performance in terms of UB, according to the uniform interleaver approach. In order to have an idea of the gap between this average performance and those of single codes in the ensemble, in each of the following figures we include the performance of codes randomly picked in $\mathscr{C}(n,k)$. Without changing the outer and inner code, this can be easily done by introducing a random interleaver between the outer code and the polar code in the concatenated scheme. Hence, in this case, the matrix $\mathbf{\Pi}$ in (7.6) is a random permutation matrix. For readability reasons, in addition to the solution without interleaver, in each of the following examples, we have considered only 25 random interleavers. Indeed, the conclusions we draw have

Table 7.1: Number of concatenated codes with random interleaver for a given minimum distance value

Concatenated scheme	$d_{\min} = 4$	$d_{\min} = 6$	$d_{\min} = 8$
Polar$(64, 48)$ + CRC-8	22	3	-
Polar$(64, 48)$ + BCH$(48, 40)$	23	2	-
Polar$(64, 48)$ + CRC-16	1	8	16
Polar$(64, 48)$ + BCH$(48, 32)$	-	-	25
Polar$(64, 56)$ + CRC-16	11	14	-

been verified with a much larger set of interleavers. The UB on the BEP is also provided for the expurgated ensemble whenever it differs from the one given by the AWEF. The UB of the considered polar code alone is also included as a reference. Clearly, the comparison between the performance of the polar code and those of the concatenated schemes is not completely fair at least because of the different code rates; however, it is useful to highlight the performance gain achieved through concatenation.

Figures 7.1 and 7.2 show the UB of the concatenated scheme, with and without random interleaver, formed by a polar code with $R_I = 0.75$ and an outer code with $R_O = 0.83$ (i.e., $R = 0.625$) in terms of BEP. In Fig. 7.1 and Fig. 7.2 a CRC-8 and a $(48, 40)$ shortened BCH outer code is considered, respectively, the latter obtained by shortening the $(255, 247)$ BCH code. In both the examples, the result obtained through the AWEF corresponds to an average behavior, while as expected some interleaver configurations achieve a smaller BEP. This trend is due to the different minimum distance of the codes. The results in Figs. 7.1 and 7.2 are very similar, showing that, for this particular case, there is no substantial difference in performance arising from the different type of outer code. This conclusion is also supported by the results in Tab. 7.1 [101], where the number of concatenated schemes with random interleavers corresponding to minimum distance value is reported. From these figures we can observe the performance gain introduced by the concatenated scheme w.r.t. the $(64, 48)$ polar code used alone, that has $d_{\min} = 4$. In both the examples the AWEF and the concatenated code without interleaver have $d_{\min} = 4$ and $d_{\min} = 6$, respectively.

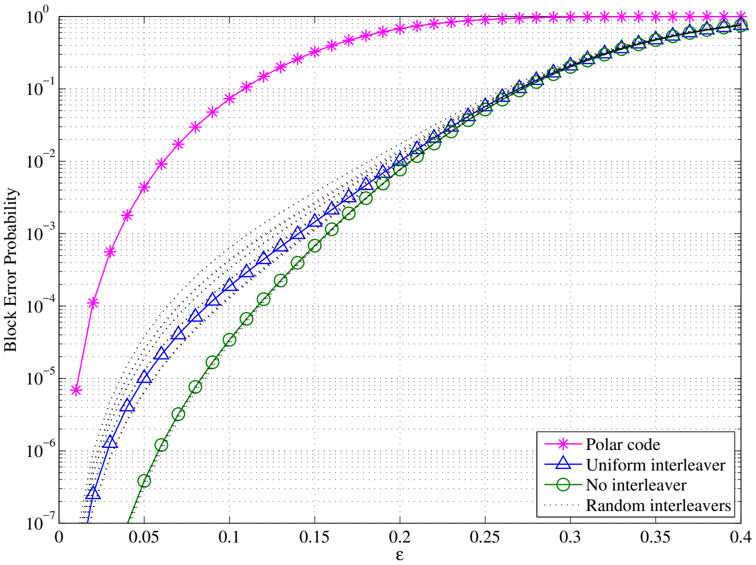


Figure 7.1: Estimated performance of concatenated codes with and without interleaver composed by a $(64, 48)$ polar code and a CRC-8 code over the BEC under ML decoding. Performance of the $(64, 48)$ polar code alone is also reported.

In Fig. 7.3 and Fig. 7.4 the UB of the concatenated codes, with and without interleaver, composed by a polar code with $R_I = 0.75$ and an outer code with $R_O = 0.66$ (i.e., $R = 0.5$) in terms of BEP is plotted. In Figs. 7.3 and 7.4 a CRC-16 and a $(48, 32)$ BCH outer code are considered, respectively, the latter obtained by shortening the $(255, 239)$ BCH code. Differently from the previous figures, the UB obtained with the expurgated AWEF is now available. As in Figs. 7.1 and 7.2, the curve obtained through the AWEF well describes the ensemble average performance, while we see that the curve corresponding to the expurgated AWEF belongs to the group of best codes. Also in these cases, the performance gap between the $(64, 48)$ polar code alone and the concatenated codes is remarkable. In both the examples the AWEF has $d_{\min} = 6$, while the expurgated AWEF and the concatenated scheme without interleaver have $d_{\min} = 8$. However, from Fig. 7.4, we can observe that, contrary to Fig. 7.3, all curves of concatenated codes are very close. In fact, for the case in Fig. 7.4 only the AWEF results in $d_{\min} = 6$ but with a codewords multiplicity equal to 0.0336. Instead, the realizations of

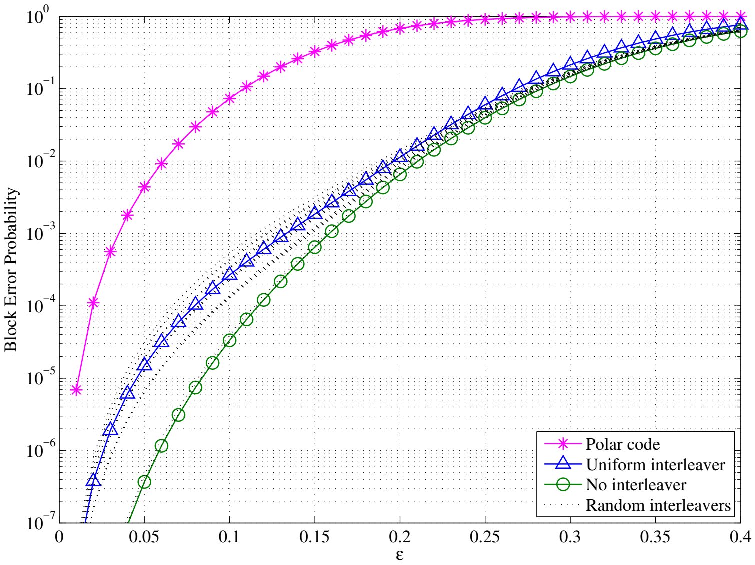


Figure 7.2: Estimated performance of concatenated codes with and without interleaver composed by a $(64, 48)$ polar code and a $(48, 40)$ shortened BCH code over the BEC under ML decoding. Performance of the $(64, 48)$ polar code alone is also reported.

concatenated codes have $d_{\min} = 8$, as shown in Tab. 7.1. Therefore, differently from the CRC, in this case the use of a BCH code is able to increase the minimum distance of the concatenated code (also for the solution without interleaver); thus, for this specific case, the BCH code should be preferred to the CRC code.

In all the previous figures the curve of the concatenated scheme without interleaver proposed in [13] falls within the group of best performing codes. This might lead to the conclusion that this configuration always produces a good result; in reality this trend is not preserved for any choice of the code parameters. An example of this type is shown in Fig. 7.5, where a polar code with $R_I = 0.875$ and a CRC-16 code (i.e., $R_O = 0.71$ and $R = 0.625$) are considered. From the figure we observe that, in this case, the introduction of a random interleaver can improve the scheme without interleaving. Also for this example, Tab. 7.1 summarizes the number of concatenated schemes with interleaver for each value of the code minimum distance. In this case the polar code has $d_{\min} = 2$, while both the AWEF and the concatenated

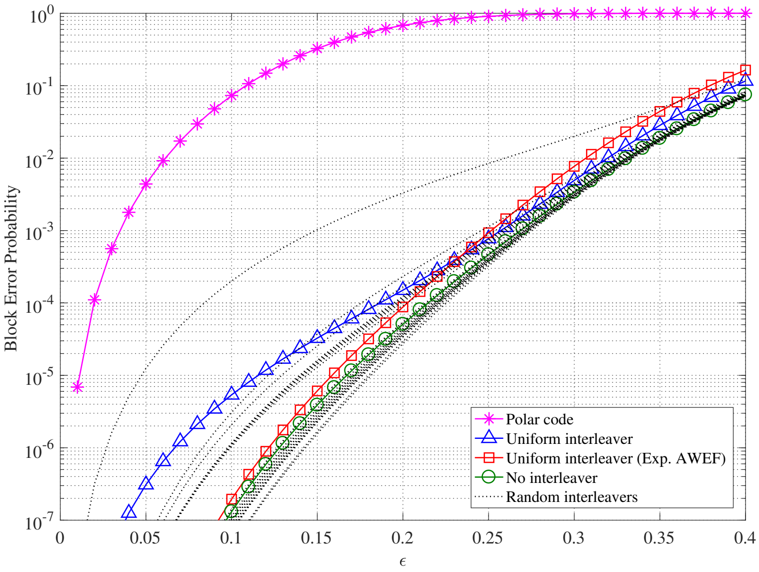


Figure 7.3: Estimated performance of concatenated codes with and without interleaver composed by a $(64, 48)$ polar code and a CRC-16 code over the BEC under ML decoding. Performance of the $(64, 48)$ polar code alone is also reported.

scheme without interleaver have $d_{\min} = 4$. We have found a similar result also by using the CRC-8 code in place of the CRC-16 but it is omitted here for the sake of brevity. So, these counter examples (others can be found) clearly demonstrate that the use of a selected interleaver may be beneficial from the error rate viewpoint.

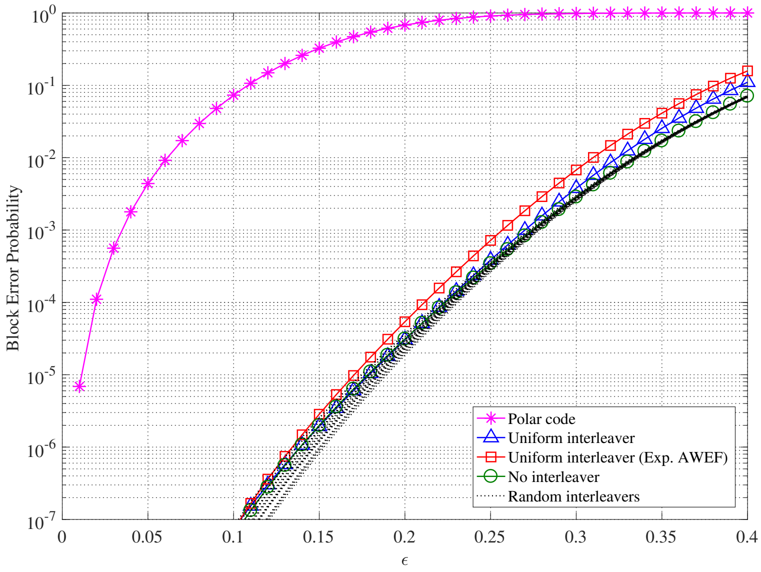


Figure 7.4: Estimated performance of concatenated codes with and without interleaver composed by a $(64, 48)$ polar code and a $(48, 32)$ shortened BCH code over the BEC under ML decoding. Performance of the $(64, 48)$ polar code alone is also reported.

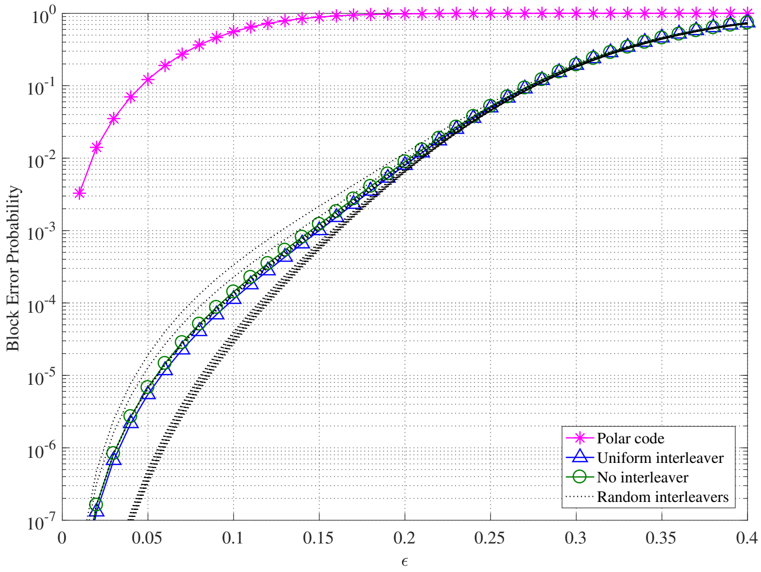


Figure 7.5: Estimated performance of concatenated codes with and without interleaver composed by a $(64, 56)$ polar code and a CRC-16 code over the BEC under ML decoding. Performance of the $(64, 56)$ polar code alone is also reported.

7.4 Summary

In this chapter, the analysis of the performance of the concatenation of a short polar code with an outer binary linear block code has been addressed from a distance spectrum viewpoint. By introducing an interleaver at the input of the polar encoder, we have shown that remarkable differences on the block error probability at low erasure probabilities can be observed for various permutations. The variations are due to the change in the overall concatenated code minimum distance (and minimum distance multiplicity) induced by the choice of the interleaver. Bounds on the achievable error rates under maximum likelihood decoding are obtained by applying the union bound to the (expurgated) average weight enumerators. Our results point out the need of careful optimization of the outer code, at least in the short block length regime, to attain low error floors.

Chapter 8

Conclusions

In this thesis we have proposed error correcting codes for secure and reliable wireless communications. In particular, we have considered two coding schemes that are the state-of-the-art in this context, namely, LDPC and polar codes.

By following a PLS approach, over the wire-tap channel then generalized through the BCC model, we have proposed finite length LDPC codes suitable to introduce security in the communication, by assessing their performance through the eavesdropper equivocation rate. In such context, based on the DE algorithm, we have proposed an optimization strategy for designing LDPC codes that approach the ultimate asymptotic limits. After having introduced the unequal error protection and the protection class concepts, through the security gap we have compared the performance achieved by several finite length coding schemes. In particular, we have proved as UEP LDPC codes are advisable in the scenarios where different sensitivities to the error are needed to achieve a feasible system. By considering a fading BCC, we have derived the expression of the outage probability, then we have shown as high order modulation schemes used on the less protected bits may minimize its value. In some cases, a wide separation between the most and less protected bits is needed. In such cases a larger UEP of the data is required. Thus, we have proposed a strategy to further improve the performance of the most protected bits, to the detriment of those of the other protection classes. Moreover, an algorithm for the asymptotic performance estimation of each protection class with high order modulation schemes and non-conventional bits labeling has been provided.

Concerning reliable communications, we have shown as LDPC codes are competitive also in very noisy channels, like the one affected by solar scintillation. In such case, we have compared the performance of coding schemes recommended by the CCSDS for TC and TM links. From this activity, weaknesses of the low rate PCTCs in presence of very compromised channels have emerged, while the considered LDPC codes have shown a greater reliability. Both amplitude and phase scintillation have been considered. Furthermore, we have shown as non-coherent modulation schemes (e.g., FSK) may be used when the synchronization error occurs.

Finally, error correcting codes for improving the reliability of short packets communications have been proposed. In this case, we have considered concatenated polar-cyclic codes, since they will be probably included in the next standard of mobile communication (5G). However, our results are interesting for any system with short packets transmission, like IoT or machine-to-machine communication. We have studied concatenated polar codes from a distance spectrum point of view. By introducing an interleaver between the component codes, we have shown as this configuration may achieve better performance w.r.t. that without interleaver previously studied in literature. We have proposed a method that, follows the well-known uniform interleaver approach, permits to estimate the average performance of the codes ensemble in terms of block error probability. With reference to the BEC, by plotting bounds on the achievable error rate of concatenated polar codes under ML decoding, we have shown as the outer code plays an important role in short block length regime.

Bibliography

[1] Huawei, “Evaluation of TBCC and polar codes for small block lengths”, Tech. Rep., 3GPP TSG RAN WG1 N.85, 2016.

[2] A. D. Wyner, “The wire-tap channel”, *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszar and J. Korner, “Broadcast channels with confidential messages”, *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near shannon limit error-correcting coding and decoding: Turbo-codes”, in *Proc. IEEE Int. Conf. on Commun. Workshop (ICC) 1993*, May 1993, vol. 2, pp. 1064–1070.

[5] L. K. Grover, “A fast quantum mechanical algorithm for database search”, in *Proc. 28th Annual ACM Symp. on the Theory of Computing*, 1996, pp. 212–219.

[6] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[7] “D-Wave Systems Inc. website”, *https://www.dwavesys.com/d-wave-two-system*.

[8] “IBM website”, *https://www.research.ibm.com/ibm-q/learn/what-is-ibm-q/*.

[9] M. Vanhoef and F. Piessens, “Key reinstallation attacks: forcing nonce reuse in WPA2”, in *ACM Conf. on Computer and Commun. Security (CCS) 2017*, Nov. 2017.

[10] R. G. Gallager, *Low-Density Parity-Ceck Codes*, PhD thesis, Dept. Elect. Eng., MIT, Cambridge, MA, USA, Jul. 1963.

[11] N. Stolte, *Rekursive Codes mit der Plotkin-Konstruktion und ihre Decodierung*, PhD thesis, TU Darmstadt, 2002.

[12] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels”, *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[13] I. Tal and A. Vardy, “List decoding of polar codes”, *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.

[14] E. Arikan, H. Kim, G. Markarian, Ü. Özgür, and E. Poyraz, “Performance of short polar codes under ML decoding”, in *Proc. ICT-Mobile Summit Conf.*, Santander, Spain, 2009.

[15] P. Trifonov, “Efficient design and decoding of polar codes”, *IEEE Trans. on Commun.*, vol. 60, no. 11, pp. 3221–3227, Nov. 2012.

[16] S. B. Korada, *Polar codes for channel and source coding*, PhD thesis, Ecole Polytechnique Fédérale de Lausanne, Switzerland, 2009.

[17] J. Guo, A. G. i. Fábregas, and J. Sayir, “Fixed-threshold polar codes”, in *Proc. IEEE Int. Symp. Inf. Theory (ISIT) 2013*, Istanbul, Turkey, Jul. 2013, pp. 947–951.

[18] M. Valipour and S. Yousefi, “On probabilistic weight distribution of polar codes”, *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2120–2123, Nov. 2013.

[19] Z. Liu, K. Chen, K. Niu, and Z. He, “Distance spectrum analysis of polar codes”, in *Proc. IEEE Wireless Commun. and Networking Conf. (WCNC) 2014*, Istanbul, Turkey, Apr. 2014, pp. 490–495.

[20] B. Li, H. Shen, and D. Tse, “A RM-polar codes”, *CoRR*, 2014.

[21] M. Bardet, V. Dragoi, A. Otmani, and J. P. Tillich, “Algebraic properties of polar codes from a new polynomial formalism”, in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT) 2016*, Barcelona, Spain, Jul. 2016, pp. 230–234.

[22] B. Li, H. Shen, and D. Tse, “An adaptive successive cancellation list decoder for polar codes with cyclic redundancy check”, *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 2044–2047, Dec. 2012.

[23] K. Niu and K. Chen, “CRC-aided decoding of polar codes”, *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1668–1671, Oct. 2012.

[24] A. Bhatia, V. Taranalli, P. H. Siegel, S. Dahandeh, A. R. Krishnan, P. Lee, Dahua Qin, M. Sharma, and T. Yeo, “Polar codes for magnetic recording channels”, in *Proc. IEEE Inf. Theory Workshop (ITW) 2015*, Jerusalem, Israel, Apr. 2015, pp. 1–5.

[25] D. Wu, Y. Li, X. Guo, and Y. Sun, “Ordered statistic decoding for short polar codes”, *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1064–1067, Jun. 2016.

[26] G. Liva, L. Gaudio, T. Ninacs, and T. Jerkovits, “Code design for short blocks: A survey”, *CoRR*, 2016.

[27] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, “Coding for secrecy”, *IEEE Signal Processing Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[28] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, “Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes”, *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1765–1779, Nov. 2014.

[29] C. W. Wong, Tan F. Wong, and John M. Shea, “Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel”, *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 551–564, Sep. 2011.

[30] G. Durisi, T. Koch, and P. Popovski, “Towards massive, ultra-reliable, and low-latency wireless communication with short packets”, *Proc. IEEE*, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[31] I. Csiszár, “Almost independence and secrecy capacity”, *Probl. of Inform. Transmission*, vol. 32, no. 1, pp. 40–47, Jan.–Mar. 1996.

[32] M. Bloch and J. Laneman, “Strong secrecy from channel resolvability”, *IEEE Trans. Inform. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[33] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes”, *IEEE Trans. Inform. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[34] O. Ozan Koyluoglu and Hesham El Gamal, “Polar coding for secure transmission and key agreement”, *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1472–1483, Oct. 2012.

[35] M. Hayashi and R. Matsumoto, “Construction of wiretap codes from ordinary channels codes”, in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT) 2010*, Austin, TX, Jun. 2010, pp. 2538–2542.

[36] H. Tyagi and A. Vardy, “Explicit capacity-achieving coding scheme for the Gaussian wiretap channel”, in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT) 2014*, Honolulu, HI, Jun. 2014, pp. 956–960.

[37] M. Bellare, S. Tessaro, and A. Vardy, “Semantic security for the wiretap channel”, in *Advances in Cryptology - CRYPTO 2012*, R. Savafi-Naini and R Canetti, Eds. 2012, vol. 7417 of *LNCS*, pp. 294–311, Springer Berlin Heidelberg.

[38] D. Klinc, Jeongseok Ha, S.W. McLaughlin, J. Barros, and Byung-Jae Kwak, “LDPC codes for the Gaussian wiretap channel”, in *Proc. IEEE Inf. Theory Workshop (ITW) 2009*, Taormina, Italy, Oct. 2009, pp. 95–99.

[39] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel", in *Proc. IEEE Int. Conf. on Commun. (ICC) 2015 - Workshop on Wireless Physical Layer Security*, London, UK, Jun. 2015.

[40] A. Wickramasooriya, I. Land, and R. Subramanian, "Comparison of equivocation rate of finite-length codes for the wiretap channel", in *Proc. 9th Int. ITG Conf. on Systems, Commun. and Coding (SCC) 2013*, Munich, Germany, Jan. 2013.

[41] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy", *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[42] M. Bloch and J. Barros, *Physical-Layer Security*, Cambridge University Press, 2011.

[43] C. W. Wong, T. F. Wong, and J. M. Shea, "LDPC code design for the BPSK-constrained gaussian wiretap channel", in *IEEE GLOBECOM Workshops (GC Wkshps) 2011*, Dec. 2011, pp. 898–902.

[44] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime", *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[45] M. van Dijk, "On a special class of broadcast channels with confidential messages", *IEEE Trans. Inform. Theory*, vol. 43, no. 2, pp. 712–714, Mar. 1997.

[46] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages", *IEEE Trans. Inform. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.

[47] Y. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages", *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[48] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages", *IEEE Trans. on Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[49] Ruoheng L., T. Liu, H. V. Poor, and S. Shamai (Shitz), "New results on multiple-input multiple-output broadcast channels with confidential messages", *IEEE Trans. on Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[50] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel", *IEEE Trans. on Inf. Theory*, vol. 59, no. 5, pp. 2673–2682, May 2013.

[51] R. F. Wyrembelski and H. Boche, "Physical layer integration of private, common, and confidential messages in bidirectional relay networks", *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3170–3179, Sep. 2012.

[52] J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design", in *Proc. Int. Symp. on Inf. Theory and Its Applications (ISITA) 2010*, Taichung, Taiwan, Oct. 2010, pp. 174–178.

[53] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes", in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT) 2010*, Austin, TX, Jun. 2010, pp. 913–917.

[54] D. Klinc, Jeongseok Ha, S.W. McLaughlin, J. Barros, and Byung-Jae Kwak, "LDPC codes for the Gaussian wiretap channel", *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[55] S. Watanabe and Y. Oohama, "Broadcast channels with confidential messages by randomness constrained stochastic encoder", in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT 2012)*, Cambridge, MA, Jul. 2012, pp. 61–65.

[56] M. Andersson, R. F. Schaefer, T. J. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and

confidential messages", *IEEE Journal on Selected Areas in Commun.*, vol. 31, no. 9, pp. 1901–1908, Sep. 2013.

[57] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages", in *IEEE Inf. Theory Workshop (ITW) 2015*, Apr. 2015, pp. 1–5.

[58] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy", *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.

[59] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security", in *Proc. IEEE Inf. Theory Workshop (ITW) 2010*, Dublin, Ireland, Aug. 2010.

[60] M. Baldi, M. Bianchi, and F. Chiaraluce, "Increasing physical layer security through scrambled codes and ARQ", in *Proc. IEEE Int. Conf. on Commun. (ICC) 2011*, Kyoto, Japan, Jun. 2011.

[61] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis", *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[62] A. Chakrabarti, A. D. Baynast, A. Sabharwal, and B. Aazhang, "Low density parity check codes for the relay channel", *IEEE Journal on Selected Areas in Commun.*, vol. 25, no. 2, pp. 280–291, Feb. 2007.

[63] J. Wang, S. Che, Y. Li, and J. Wang, "Optimal design of the joint network LDPC codes for half-duplex cooperative multi-access relay channel", in *5th Int. Conf. on Intelligent Networking and Collaborative Systems 2013*, Xi'an, China, Sep. 2013, pp. 622–625.

[64] R. Khattak and S. Sandberg, "Jointly optimized rate-compatible UEP-LDPC codes for half-duplex co-operative relay networks", *EURASIP*

Journal on Wireless Commun. and Networking, vol. 2014, no. 1, pp. 22, Feb. 2014.

[65] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation", *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 657–670, Feb. 2001.

[66] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel", in *Proc. IEEE Int. Conf. on Commun. Workshop (ICC) 2015*, London, UK, Jun. 2015, pp. 435–440.

[67] X. Y. Hu, E. Eleftheriou, and D. M. Arnold, "Progressive edge-growth Tanner graphs", in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM) 2001*, San Antonio, Texas, Nov. 2001, pp. 995–1001.

[68] V. Boyko, "On the security properties of OAEP as an all-or-nothing transform", in *Advances in Cryptology – CRYPTO 1999*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 503–518. Springer, 1999.

[69] University of Newcastle Signal Processing Microelectronics research center, "LDPC codes project", `http://sigpromu.org/ldpc/`, 2013.

[70] N. von Deetzen and S. Sandberg, "On the UEP capabilities of several LDPC construction algorithms", *IEEE Trans. Commun.*, vol. 58, no. 11, pp. 3041–3046, Nov. 2010.

[71] X.Y. Hu, E. Eleftheriou, D.M. Arnold, and A. Dholakia, "Efficient implementations of the sum-product algorithm for decoding LDPC codes", in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM) 2001*, San Antonio, Texas, USA, Nov. 2001, vol. 2, pp. 1036–1036E.

[72] H.V.B. Neto, W. Henkel, and V.C. da Rocha, "Multi-edge type unequal error protecting low-density parity-check codes", in *Proc. IEEE Inf. Theory Workshop (ITW) 2011*, Paraty, Brazil, Oct. 2011, pp. 335–339.

[73] D. Poulliat, C.and Declercq and I. Fijalkow, “Enhancement of unequal error protection properties of LDPC codes”, *EURASIP Journal on Wireless Commun. and Networking*, vol. 2007, 2007, Article ID 92659.

[74] M. Baldi, N. Maturo, G. Ricciutelli, and F. Chiaraluce, “LDPC coded transmissions over the Gaussian broadcast channel with confidential messages”, in *Proc. 21st IEEE Int. Conf. on Telecommun. (ICT) 2014*, Lisbon, Portugal, May 2014, pp. 52–56.

[75] B.-J. Kwak, N.-O. Song, B. Park, D. Klinc, and S.W. McLaughlin, “Physical layer security with Yarg code”, in *Proc. First Int. Conf. on Emerging Network Intelligence*, Sliema, Malta, Oct. 2009, pp. 43–48.

[76] M. Baldi, N. Maturo, G. Ricciutelli, and F. Chiaraluce, “Practical LDPC coded modulation schemes for the fading broadcast channel with confidential messages”, in *Proc. IEEE Int. Conf. on Commun. Workshop (ICC) 2014*, Sydney, Australia, Jun. 2014, pp. 759–764.

[77] N. Rahnavard and F. Fekri, “New results on unequal error protection using LDPC codes”, *IEEE Commun. Lett.*, vol. 10, no. 1, pp. 43–45, January 2006.

[78] N. von Deetzen and S. Sandberg, “Design of unequal error protection LDPC codes for higher order constellations”, in *Proc. IEEE Int. Conf. on Commun. (ICC) 2007*, Glasgow, UK, Jun. 2007, pp. 926–931.

[79] 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.

[80] Dongweon Yoon, Kyongkuk Cho, and J. Lee, “Bit error probability of M-ary quadrature amplitude modulation”, in *Proc. 52nd Vehicular Technology Conf. 2000 (VTC) 2000*, Boston, MA, Sep. 2000, vol. 5, pp. 2422–2427.

[81] A. Boronka and J. Speidel, “A low complexity MIMO system based on BLAST and iterative anti-Gray-demapping”, in *Proc. IEEE 14th*

Int. Symp. on Personal, Indoor and Mobile Radio Commun. (PIMRC) 2003, Beijing, China, Sep. 2003, pp. 1400–1404.

[82] G. Ricciutelli, M. Baldi, N. Maturo, and F. Chiaraluce, “LDPC coded modulation schemes with largely unequal error protection”, in *Proc. IEEE Int. Black Sea Conf. on Commun. and Networking (BlackSeaCom) 2015*, Costanta, Romania, May 2015, pp. 48–52.

[83] M. Lanucara, “Computation of the telecommunications link degradation due to amplitude scintillation”, Tech. Rep., ESA/ESOC OPS-GS/02126/ML, Issue 2 Rev. 0, 10/10/2013, 2013.

[84] J. Lu Q. Li, L. Yin, “Performance study of a deep space communication system with low-density parity-check coding under solar scintillation”, *Int. Journal of Commun.*, vol. 6, no. 1, pp. 1–9, 2012.

[85] M.Simon and M.S. Alouini, *Digital Communication over Fading Channels*, Wiley, 2005.

[86] *TC Synchronization and Channel Coding–Summary of Concept and Rationale.*, CCSDS 230.1-G-2, Nov. 2012.

[87] *TM Synchronization and Channel Coding — Summary of Concept and Rationale*, CCSDS 130.1-G-2, Nov. 2012.

[88] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, “Optimal decoding of linear codes for minimizing symbol error rate”, *IEEE Trans. on Inf. Theory*, vol. 20, no. 2, pp. 284–287, Mar. 1974.

[89] J. Zhang, M. Fossorier, D. Gu, and J. Zhang, “Improved min-sum decoding of LDPC codes using 2-dimensional normalization”, in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM) 2005*, St. Louis, MO, USA, Nov. 2005, vol. 3, pp. 1187–1192.

[90] *Short Block Length LDPC Codes for TC Synchronization and Channel Coding*, CCSDS 231.1-O-1, Apr. 2015.

[91] M. Baldi, F. Chiaraluce, N. Maturo, G. Liva, and E. Paolini, "A Hybrid Decoding Scheme for Short Non-Binary LDPC Codes", *IEEE Commun. Lett.*, vol. 18, no. 12, pp. 2093–2096, Dec. 2014.

[92] M. Baldi, F. Chiaraluce, R. Garello, N. Maturo, I. Aguilar Sanchez, and S. Cioni, "Analysis and performance evaluation of new coding options for space telecommand links - Part I: AWGN channels", *Int. Journal of Satellite Commun. and Networking*, vol. 33, no. 6, pp. 509–525, 2015.

[93] M. Baldi, F. Chiaraluce, R. Garello, N. Maturo, I. Aguilar Sanchez, and S. Cioni, "Analysis and performance evaluation of new coding options for space telecommand links – Part II: jamming channels", *Int. Journal of Satellite Commun. and Networking*, vol. 33, no. 6, pp. 527–542, 2015.

[94] ESA/ESOC, "Reliable TT-C during supErior Solar conjunctions (RESCUe) – Final report", Tech. Rep., Issue 1, Rev. 1, Jun. 2017.

[95] S. Benedetto and G. Montorsi, "Unveiling turbo codes: some results on parallel concatenated coding schemes", *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 409–428, Mar. 1996.

[96] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I and II*, North-Holland Publishing Co., 1977.

[97] J. K. Wolf and R. D. Blakeney, "An exact evaluation of the probability of undetected error for certain shortened binary CRC codes", in *Proc. 21st IEEE Military Commun. Conf.*, San Diego, CA, USA, Oct. 1988, vol. 1, pp. 287–292.

[98] C. Weiss, C. Bettstetter, and S. Riedel, "Code construction and decoding of parallel concatenated tail-biting codes", *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 366–386, Jan. 2001.

[99] F. Chiaraluce and R. Garello, "Extended Hamming product codes analytical performance evaluation for low error rate applications", *IEEE Trans. on Wireless Commun.*, vol. 3, no. 6, pp. 2353–2361, Nov. 2004.

[100] G. Liva, E. Paolini, and M. Chiani, “Bounds on the error probability of block codes over the q-ary erasure channel”, *IEEE Trans. on Commun.*, vol. 61, no. 6, pp. 2156–2165, Jun. 2013.

[101] G. Ricciutelli, M. Baldi, F. Chiaraluce, and G. Liva, “On the error probability of short concatenated polar and cyclic codes with interleaving”, in *Proc. IEEE Int. Symp. Inf. Theory (ISIT) 2017*, Aachen, Germany, Jun. 2017, pp. 1858–1862.

Acknowledgments

I am sincerely grateful to my supervisor Prof. Franco Chiaraluce, for his precious guidance during my Ph.D. course. Thanks to his enthusiasm and patience, I had the opportunity to grow under every point of view. With his advice, these years were a very pleasant period.

The second thanks goes to Dr. Marco Baldi for his friendship and prompt assistance across my Ph.D. course.

Another thanks goes to Dr. Gianluigi Liva and to all people that I had the pleasure to meet at the DLR center in Wessling. Their friendly support has made my period in Munich a very enjoy-full experience.

I would also like to thank my friend abroad Nicola Maturo, his invaluable assistance and his friendship are one of the most beautiful surprises of these years.

A thanks goes to all my fellows at the Department of Information Engineering, in particular to Paolo Santini, Massimo Battaglioni, Linda Senigagliesi, Laura Montanini and Manola Ricciuti for their optimism and their support.

I would finally like to thank my family, to my parents and friends for their encouragement throughout these years. I am very grateful to them.

Complete Publications List

Journal Papers:

- M. Baldi, N. Maturo, **G. Ricciutelli**, F. Chiaraluce; "Security gap analysis of some LDPC coded transmission schemes over the flat and fast fading Gaussian wire-tap channels", EURASIP Journal on Wireless Communications and Networking 2015, vol. 2015, no. 1, pp. 232-244, Oct. 2015, DOI 10.1186/s13638-015-0463-6.

- M. Baldi, N. Maturo, **G. Ricciutelli**, F. Chiaraluce; "Measuring the performance of coded transmissions over the wire-tap channel with fast fading"; *under review on IEEE Transactions on Wireless Communications.*

- **G. Ricciutelli**, T. Jerkovits, M. Baldi, F. Chiaraluce, G. Liva; "Analysis of the Block Error Probability of Concatenated Polar Code Ensembles"; *in preparation.*

- **G. Ricciutelli**, M. Baldi, F. Chiaraluce;, G. Liva "A semi-analytical approach for the design of optimal interleavers in short concatenated polar and cyclic codes"; *in preparation.*

- S. Finocchiaro, A. Ardito, F. Barbaglio, M. Baldi, F. Chiaraluce, N. Maturo, **G. Ricciutelli**, L. Simone, R. Abelló, J. De Vicente, M. Mercolino, "On the performance of standard and non standard error correcting codes for space communications in the presence of solar scintillation."; *in preparation.*

Conference Proceedings:

- **G. Ricciutelli**, M. Baldi, F. Chiaraluce and G. Liva, “On the Error Probability of Short Concatenated Polar and Cyclic Codes with Interleaving”, Proc. IEEE International Symposium on Information Theory (ISIT) 2017, pp. 1858-1862, Aachen, Germany, June 2017, DOI: 10.1109/ISIT.2017.8006851.

- S. Finocchiaro, A. Ardito, F. Barbaglio, M. Baldi, F. Chiaraluce, N. Maturo, **G. Ricciutelli**, L. Simone, R. Abelló, J. De Vicente, M. Mercolino, “Improving deep space telecommunications during solar superior conjunctions”, IEEE Aerospace Conference 2017, pp. 1-13, Yellowstone conference center, Big Sky, Montana, Mar. 2017, DOI: 10.1109/AERO.2017.7943738.

- M. Baldi, F. Chiaraluce, N. Maturo, **G. Ricciutelli**, R. Abelló, J. De Vicente, S. Marti, A. Ardito, F. Barbaglio, S. Finocchiaro, "Coding for space telemetry and telecommand transmissions in presence of solar scintillation", ESA International Workshop on Tracking, Telemetry and Command Systems for Space Applications (TTC) 2016, ISBN 978-1-4673-9731-5, pp. 1-8, Noordwijk, Netherlands, September 2016.

- M. Baldi, N. Maturo, **G. Ricciutelli** and F. Chiaraluce, "On the Error Detection Capability of Combined LDPC and CRC Codes for Space Telecommand Transmissions", IEEE Symposium on Computers and Communications (ISCC) 2016, pp. 1058-1065, Messina, Italy, June 2016, DOI: 10.1109/ISCC.2016.7543876.

- M. Baldi, **G. Ricciutelli**, N. Maturo and F. Chiaraluce, “Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel”, IEEE International Conference on Communications 2015 Workshop on Wireless Physical Layer Security (ICC) 2015, pp. 435-440, London, UK, June 2015, DOI: 10.1109/ICCW.2015.7247218.

- **G. Ricciutelli**, M. Baldi, N. Maturo and F. Chiaraluce, “LDPC Coded Modulation Schemes with Largely Unequal Error Protection”, IEEE

International Black Sea Conference on Communication and Networking (BlackSeaCom) 2015, pp. 48-52, Constanta, Romania, May 2015, DOI: 10.1109/BlackSeaCom.2015.7185084, **Awarded as the best student paper of the Conference**.

- M. Baldi, N. Maturo, **G. Ricciutelli** and F. Chiaraluce, “Practical LDPC coded modulation schemes for the fading broadcast channel with confidential messages”, IEEE International Conference on Communications Workshop on Wireless Physical Layer Security (ICC) 2014, pp. 759-764, Sydney, Australia, June 2014, DOI: 10.1109/ICCW.2014.6881291.

- M. Baldi, N. Maturo, **G. Ricciutelli** and F. Chiaraluce, “LDPC coded transmissions over the Gaussian broadcast channel with confidential messages”, IEEE 21st International Conference on Telecommunications (ICT) 2014, pp. 52-56, Lisbon, Portugal, May 2014, DOI: 10.1109/ICT.2014.6845079.