Chapter 4
Performance Analysis of Transmission over AWGN Wiretap Channels with Practical Codes

Marco Baldi, Franco Chiaraluce, Nicola Maturo and Stefano Tomasin

Abstract The wiretap coding problem has been addressed since a long time from an information theoretic standpoint. This has permitted to find the ultimate achievable limits under the hypothesis of random coding, which however is far from practice. Some families of practical codes have also been already considered in this scenario, but their achievable secrecy has mostly been assessed in asymptotic conditions (i.e., under the hypothesis of infinite codeword length) and using discrete channel models. In this chapter, we analyze the performance of practical codes over the Gaussian wiretap channel by using suitable metrics which take into account the codeword length and even the specific code structure. This way, we are able to assess the performance of real codes in the finite code length regime, and compare it with the ultimate achievable limits. We focus on low-density parity-check codes as they are among the most viable candidates for the use in this setting.

4.1 Introduction

The wiretap channel model [25] is the first and main reference model for physical layer secure transmissions, and it is well known that perfect secrecy can be achieved over the wiretap channel under the hypothesis of ideal random coding [14, 25].

M. Baldi (✉) · F. Chiaraluce · N. Maturo
Università Politecnica delle Marche, Ancona, Italy
e-mail: m.baldi@univpm.it

F. Chiaraluce
e-mail: f.chiaraluce@univpm.it

N. Maturo
e-mail: n.maturo@univpm.it

S. Tomasin
University of Padua, Padua, Italy
e-mail: tomasin@dei.unipd.it

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_4

However, apart from the theoretical model, the need to implement real transmissions with practical codes may force them to be far from perfect secrecy, and such a risk needs to be quantified.

4.1.1 Previous Works

Some families of practical codes, like low-density parity-check (LDPC) codes and polar codes, have been shown to be able to achieve the wiretap channel secrecy capacity in the asymptotic regime (i.e., with infinite codeword length) [13, 17, 22]. However, despite this provides a very important new insight into the design of practical codes for the wiretap channel, it is not easy to predict how far from the secrecy capacity the secret throughput will be when the codeword length is reduced to some (finite) practical value. Moreover, many previous works consider discrete channel models (like the binary erasure channel (BEC) or the binary symmetric channel (BSC) models) for both the main and wiretapper's channels. However, the most interesting applications of physical layer security techniques are recognized to be in wireless communications, therefore a continuous channel model (like the additive white Gaussian noise (AWGN) channel model, with or without fading) is best suited for describing the physical layer. On the other hand, it is not realistic to suppose that an eavesdropper of a wireless link is forced to discard the soft information coming from the channel, and to use hard detection.

More in detail, an interesting family of two edge type LDPC codes has been proposed in [1, 18, 19] for the use in wiretap coding schemes exploiting Wyner's coset encoding technique. These codes are shown to achieve weak secrecy in asymptotic conditions (i.e., at infinite code lengths) over wiretap channels modeled as BECs. In addition, in [19] some results for finite length codes are provided, but still only over BECs. The weak secrecy criterion used in these works requires that the mutual information between the secret message and the eavesdropper's observation goes to zero rate-wise, rather than in absolute terms, as needed by the strong secrecy criterion. More recently, the same setting of a wiretapper BEC and a coset encoding technique has been considered in the proposal of a scheme able to achieve strong secrecy rather than weak secrecy [21], by exploiting large-girth LDPC codes. However, this result only holds in the asymptotic regime, i.e., for infinite length codes. Another scheme which has been proven to achieve perfect secrecy is based on polar codes [9]. However, also in this case such a target is achieved for discrete channels and infinite length codes, while no result is provided for finite length codes. Indeed, all evidence up to now suggests that perfect secrecy (interpreted as zero information leakage about the secret message in absolute terms, rather than rate-wise) may not be achievable by using short length codes, or in general finite length codes.

Another recent trend which is important to mention concerns some attempts to study the problems of physical layer security and wiretap coding in more general terms, and also exploring their links with computational security and cryptography. The work [7] studies the general problem of finding efficiently invertible extractors, which involves wiretap protocols. However, also in this case, the focus is on asymptotic security notions used to search for asymptotic optimal wiretap protocols over discrete, memoryless, and symmetric channels. In [5], the security notions classically used for transmissions over the wiretap channel are reviewed, and their links with the more robust notion of semantic security used in cryptography are explored. The authors also propose a new coding scheme characterized by polynomial-time decoding and achieving the secrecy capacity for the case of BSCs. Such a scheme can be extended to other discrete memoryless channels, but continuous channels (like the AWGN channel) are not taken into account. One of the very few works on coding for Gaussian wiretap channels is [16], where the authors address the problem of practical code design and propose a secure nested code structure. The authors derive the achievable rate-equivocation region based on the threshold behavior of good code sequences, that is, by considering the performance of code ensembles in the asymptotic regime, without taking into account finite length codes.

4.1.2 Error Rate Used as a Secrecy Metric

The bit error rate (BER) and codeword error rate (CER) are very common metrics for assessing the transmission reliability in practical terms, since they are quite easy to estimate for any fixed coding and modulation scheme, even through numerical simulations. An approach to use these metrics also for security has been proposed in [12], where the condition of being subjected to a BER close to 0.5 was imposed to the eavesdropper in order to achieve security. Then, the differential evolution technique was used to design optimized LDPC codes with the aim of achieving the desired BER performance for both the authorized receiver and the eavesdropper. The quality ratio between their two channels, defined as the *security gap*, was also used as a metric, which should be kept as small as possible. A similar approach has been followed in [2].

When used for assessing reliability, the error rate-based metrics can be easily related to other, information theoretic metrics, like the conditional entropy (for which we can exploit Fano's inequality). The same is instead not straightforward when we aim at measuring security. A bridge between information theoretic and error rate-based security metrics can be found in [24], where the authors propose a secret key sharing scheme for the wiretap channel. The same approach, based on the eavesdropper's equivocation rate on the secret message, has also been used to study coded transmissions over the Gaussian wiretap channel [23] and parallel channels [3], in the finite code length regime. The work [23] considers punctured LDPC codes, while in [3] the focus is on more classical coding schemes (like Bose-Chaudhuri-Hocquenghem (BCH) codes).

4.1.3 Our Contribution

In this chapter, we address the problem of measuring the reliability and secrecy performance from an information theoretic standpoint in the finite codeword length regime. For this purpose, as in the mentioned previous works, we exploit the link between the equivocation rate and the error rate in order to explore the capacity-equivocation regions of the codes we consider. Using the equivocation rate as a security metric also allows us to compare the performance achieved in the finite codeword length regime with that achievable in the asymptotic regime. We also focus on LDPC codes as a prominent solution for wiretap coding, but, differently from [23], we consider non-punctured LDPC coded transmissions, which are more common in practice with respect to punctured transmissions. We aim at finding good codes both in terms of reliability and security through a very simple code optimization approach. With respect to existing literature, the main contributions of this chapter are as follows.

- We consider continuous wiretap channels (no restriction on the use of soft information by Eve) and finite length codes.
- We take into account the specific code structure (no code ensembles).
- We relate the wiretapper's equivocation rate to the error rate, thus providing an information theoretic secrecy metric which is, at the same time, relevant to the specific code and comparable with the ultimate achievable limits.

The organization of the chapter is as follows. In Sect. 4.2, we define the channel model and the metrics we use throughout the chapter. In Sect. 4.3, we use these metrics to assess the ultimate performance achievable in asymptotic conditions. In Sect. 4.4, we show how the same metrics can be applied to the finite codeword length regime, and in Sect. 4.5 we draw some conclusions.

4.2 Channel Model and Metrics

In the Gaussian wiretap channel model, Alice transmits a k_s-bit secret message M by encoding it into an n-bit codeword X, through a binary linear block code $\mathscr{C}$. The choice of the transmitted codeword X not only depends on the secret message bits, but also on k_r random bits which are used to implement a form of nested coding [10]. The code $\mathscr{C}$ has information length $k = k_s + k_r$ and codeword length n. Its rate is $R_c = k/n$. The secret message rate is $R_s = k_s/n$. Both the authorized receiver (Bob) and an eavesdropper (Eve) receive Alice transmission, and they have full knowledge of the code $\mathscr{C}$. Bob's and Eve's channels are impaired with AWGN, and their received vectors are noted by Y and Z, respectively. In order to achieve successful transmission of M, we must achieve the following targets:

1. *reliability target*: the secret message M must be reliably decoded by Bob (i.e., with a sufficiently small error rate),
2. *security target*: Eve must be unable to gather any (or almost any) information about M.

From both the security and reliability standpoints, we aim at finding suitable metrics to be used for measuring performance in the finite code length regime, and comparing it with that achievable in asymptotic conditions.

4.2.1 Reliability Metrics

Concerning the reliability target, the following metrics can be used:

- In asymptotic conditions (infinite length codes), without any constraints on the choice of the code, the ultimate performance limit is represented by the channel capacity, which coincides with the highest code rate that can be used to achieve error-free transmission. We consider a continuous binary-input channel with AWGN and signal-to-noise ratio (SNR) per bit $\frac{E_b}{N_0}$, having capacity:

$$C\left(\frac{E_b}{N_0}\right) = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{e}^{-\frac{\left(y-\sqrt{E_b/N_0}\right)^2}{2}} \log_2\left(1 + \mathrm{e}^{-2y\sqrt{E_b/N_0}}\right) dy. \quad (4.1)$$

- In asymptotic conditions (infinite length codes), but with the constraint to use LDPC coded transmissions, the density evolution technique [8, 20] can be used to compute a decoding threshold, in terms of SNR, above which transmission can occur without errors.
- In the finite code length regime, the performance of practical LDPC codes can be assessed through Montecarlo simulations, and the SNR needed to achieve a sufficiently low decoding error probability can be estimated.

4.2.2 Security Metrics

Concerning the security target, the concepts of *strong secrecy* and *weak secrecy* are classically used for wiretap coding schemes [6, 15]. The definitions of strong and weak secrecy are in the asymptotic regime. In fact, we say that we have strong secrecy when the amount of information leaked about M through observing Z vanishes as n goes to infinity, i.e., $\lim_{n\to\infty} \mathrm{I}(M; Z) = 0$, where $\mathrm{I}(x; y)$ denotes the mutual information between x and y. Similarly, we have weak secrecy when the rate of information leaked about M through observing Z vanishes as n goes to infinity, i.e., $\lim_{n\to\infty} \mathrm{I}(M; Z)/n = 0$. Despite this, we can use notions similar to strong and weak secrecy also in the finite code length regime. In fact, both of them are based on the information leakage about the secret message, measured in terms of the mutual information between the secret message and the wiretapper's observation. The difference is that for weak secrecy the information leakage is measured rate-wise, while for strong secrecy it is measured in absolute terms. Therefore, we could measure these quantities in the finite code length regime as well.[1] Another, similar way of measuring the information leakage about the secret message is by using the wiretapper's equivocation on the secret message, as done in Wyner's original work [25]. According to [25], perfect secrecy is achieved when the wiretapper's equivocation rate on the secret message equals the entropy of the data source. In this case, we use again a rate-wise measure of the information leakage, which is weaker than the notion of strong secrecy. However, as outlined in Sect. 4.1, all evidence up to now suggests that strong secrecy may not be achievable with finite length codes. Based on these premises, in the following we use the wiretapper's equivocation rate as a secrecy measure. We make this choice since it allows to relate the secrecy metrics with the error rate, as we will show next, which is an important feature to take into account the specific code structure in the performance assessment.

By denoting as $\mathrm{H}(\cdot)$ the entropy function, the wiretapper's equivocation rate is simply defined as $R_e = \frac{1}{n}\mathrm{H}(M|Z)$. Since we suppose to deal with independent and identically distributed secret messages, the source entropy rate is equal to R_s, and perfect secrecy is achieved when the equivocation rate R_e equals the secret message rate R_s:

$$\widetilde{R_e} = R_e/R_s = 1. \tag{4.2}$$

We denote $\widetilde{R_e}$ as the *fractional equivocation rate*. Obviously, the ultimate limit achievable by the equivocation rate is represented by the secrecy capacity $C_s = [C_B - C_E]^+$, where C_B and C_E are Bob's and Eve's channel capacities, respectively. It is well known that the wiretapper's equivocation rate on the secret message can also be expressed as [6, 15]:

$$R_e = \frac{1}{n}\left[\mathrm{H}(X) - \mathrm{I}(X;Z) + \mathrm{H}(M|Z,X) - \mathrm{H}(X|M,Z)\right], \tag{4.3}$$

where $\mathrm{H}(X|M,Z)$ is the entropy of X conditioned on receiving Z and knowing the secret message M.

4.2.3 Fictitious Receiver

In order to estimate $\mathrm{H}(X|M,Z)$, we can suppose the existence of a fictitious receiver which is in the same position as Eve's, but, differently from Eve, he knows the secret message M. We name this other subject Frank, and include it in our communication

[1] Obviously, in the finite length regime Bob's error probability cannot be vanishing. Therefore, in order to apply these metrics in such a regime, the reliability target must be converted into requiring that Bob achieves some sufficiently small error probability.

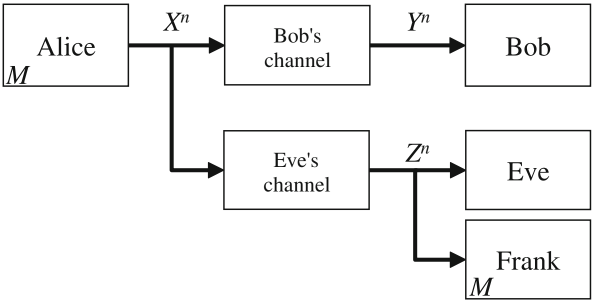

Fig. 4.1 Wiretap channel model with fictitious receiver

model, which is depicted in Fig. 4.1. The letter M inside Alice's and Frank's boxes points out that the message M is known to both Alice and Frank. Frank receives from the channel the same vector Z received by Eve and then tries to perform decoding for recovering the k_r random bits, which represent the only source of uncertainty for him in order to retrieve X.

In (4.3), we have $\mathrm{I}(X; Z) \leq nC_E$, $\mathrm{H}(X) = k$ and $\mathrm{H}(M|Z, X) \leq \mathrm{H}(M|X) = 0$. Concerning the term $\mathrm{H}(X|M, Z)$, by Fano inequality we have $\mathrm{H}(X|M, Z) \leq 1 + k_r\eta$, where η is the decoding error probability (or CER) experienced by Frank. Based on these considerations, we can find a lower bound on the wiretapper's equivocation rate on the secret message as [23]:

$$\begin{aligned} R_e &\geq \frac{1}{n}\left[k - nC_E - k_r\eta - 1\right] = \\ &= R_c - C_E - (R_c - R_s)\eta - \frac{1}{n} = R_e^*. \end{aligned} \tag{4.4}$$

This way, we find a secrecy metric which takes into account the code length, and therefore it is suitable to assess performance also in the finite code length regime, which is of interest for practical codes. Furthermore, this metric depends on Frank's CER, which can be easily estimated, for practical codes, through numerical simulations. Looking at (4.4), one could think that an optimal solution is to impose that Eve and Frank have a very low SNR. In this case, we have $\eta \approx 1$ and $C_E \approx 0$. Under these hypotheses, and by considering sufficiently long codes to make the term $\frac{1}{n}$ negligible, we would have $R_e^* \approx R_s$. Unfortunately, this apparently optimal solution is not viable for the following reasons:

- Fixing a small value of η as Frank's performance target is beneficial for security. In fact, if Frank's error rate on the sole random bits is small, this means that Eve's equivocation will be concentrated on the secret message bits, which is what we want to achieve.
- Allowing a not-too-degraded channel for the eavesdropper is also beneficial, since this means that security can be guaranteed even when Eve is not far from Bob. This is an important aspect which is also caught by the analysis based on the security gap.

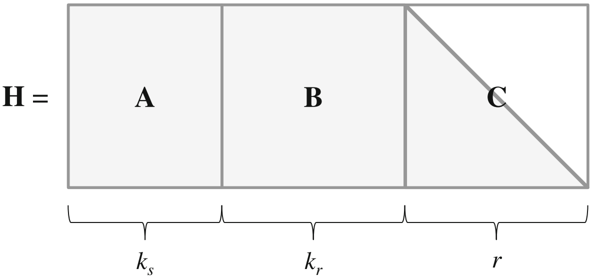

Fig. 4.2 Parity-check matrix of the considered codes

Based on these considerations, we want to achieve a value of R_e^* as high as possible, without renouncing to impose a small value of η. This requires to optimize Frank's performance as well, in such a way that he is able to achieve good decoding performance (i.e., small η) with small SNR, which means having a small capacity C_E of (Frank's and) Eve's channel.

Let us consider LDPC coding and let us suppose (without loss of generality) that encoding is systematic. Let the transmitted codeword be $\mathbf{c} = [M|R|P]$, where M is the k_s-bit secret message, R is the k_r-bit random message and P is the r-bit redundancy vector added by the encoder. In real world secure transmissions, systematic encoding shall be avoided, especially if source coding is not perfect (as always occurs in practice). For this purpose, the use of an information bit scrambler is advisable [2]. Nevertheless, in our analysis, which is aimed at estimating the performance achievable, the hypothesis of systematic coding can be maintained, since it helps simplifying the analysis. Under this hypothesis, we can describe the code $\mathscr{C}$ through a lower triangular parity-check matrix $\mathbf{H}$. More precisely, we can divide the matrix $\mathbf{H}$ into three blocks as shown in Fig. 4.2. These three blocks, named $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ in the figure, have size $r \times k_s$, $r \times k_r$ and $r \times r$ bits, respectively. $\mathbf{C}$ is a lower triangular matrix, which is a sufficient condition to perform systematic encoding.

Bob, who does not know in advance either the secret or the random message, must use the whole matrix $\mathbf{H}$ to perform decoding. Eve is in the same condition, although she receives the signal through a different channel. Frank, instead, can take advantage of the perfect knowledge of M, and only needs to recover the random message R. Therefore, he can precompute $\mathbf{A} \cdot M^T = \mathbf{s}$, were ^{T} denotes transposition. Then, he can use the following reduced parity-check system to look for the vector $[R|P]$ having syndrome $\mathbf{s}$:

$$[\mathbf{B}|\mathbf{C}] \cdot [R|P]^T = \mathbf{H}' \cdot \mathbf{c}'^T = \mathbf{s}. \tag{4.5}$$

Obviously, decoding for a vector having an all-zero syndrome (as usual) or a different syndrome is equivalent, due to the code linearity. Hence, Frank can perform decoding through the reduced LDPC code defined by $\mathbf{H}' = [\mathbf{B}|\mathbf{C}]$, which has rate $R_F = k_r/(k_r + r)$. The code rate for Bob and Eve instead coincides with the overall code rate, i.e., $R_c = k/n$. Through simple arithmetic, we find

$$R_F = \frac{R_c - R_s}{1 - R_s}. \tag{4.6}$$

From (4.6) we have $\frac{R_F}{R_c} = \frac{1-\frac{R_s}{R_c}}{1-R_s}$ and, since $R_c < 1$, we have $\frac{R_F}{R_c} < 1$. Therefore, Frank's advantage of knowing the secret message M translates into his ability to work with a lower code rate with respect to Bob and Eve, i.e., with an increased error correction capability.

4.3 Asymptotic Performance

A first important benchmark is represented by the performance achievable in optimal conditions, which represents the ultimate bound we will aim at approaching when working with practical, finite length codes.

4.3.1 Ideal Codes

Let us first consider the hypothesis of working with optimal codes, i.e., codes able to reach the channel capacity. Under this hypothesis, R_c coincides with Bob's channel capacity C_B, while R_F coincides with Frank's channel capacity C_F. Moreover, since Eve and Frank experience the same channel, Eve's channel capacity is $C_E = C_F = R_F$. Therefore, the secrecy capacity can be written as $C_s = R_c - R_F$. Then, replacing R_F with the r.h.s. of (4.6), we obtain the following expression for the fractional secrecy capacity, which provides the ultimate bound on $\widetilde{R_e}$:

$$\widetilde{C_s} = \frac{C_s}{R_s} = \frac{1 - R_c}{1 - R_s}. \tag{4.7}$$

We have chosen some values of the code rate R_c of the type $1/x$ or $x/(x+1)$, with x integer, ranging between $1/5$ and $4/5$. For all of them, we have computed $\widetilde{C_s}$ as a function of R_s, and the results are reported in Fig. 4.3. From the figure we observe that $\widetilde{C_s}$ is a monotonically increasing function of R_s, as expected from (4.7), and it reaches 1 when the secret message rate reaches its maximum, i.e., $R_s = R_c$. Apparently, this brings us to the conclusion that we should fix $R_s = R_c$ in order to maximize $\widetilde{C_s}$ and achieve optimal performance from the secrecy standpoint. This would mean to renounce transmitting randomness to confuse the eavesdropper. However, moving on the curves of Fig. 4.3 (i.e., fixing R_c) means also varying the SNR of Eve: in particular, from (4.6) we can obtain the value of R_F associated with a couple R_s and R_c. Since we are considering rates coincident with capacities, the value of R_F corresponds to a capacity of the Eve's channel and therefore to a specific SNR value,

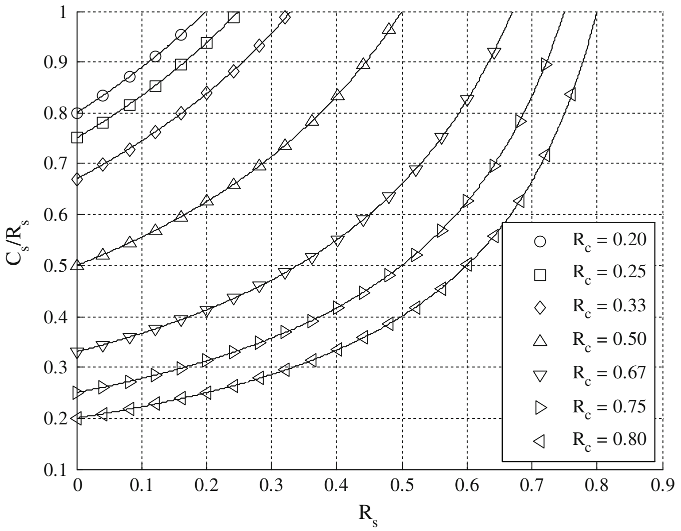

Fig. 4.3 $\widetilde{C_s}$ versus secret message rate (R_s) for some values of the code rate (R_c), under the hypothesis of ideal (capacity achieving) coding

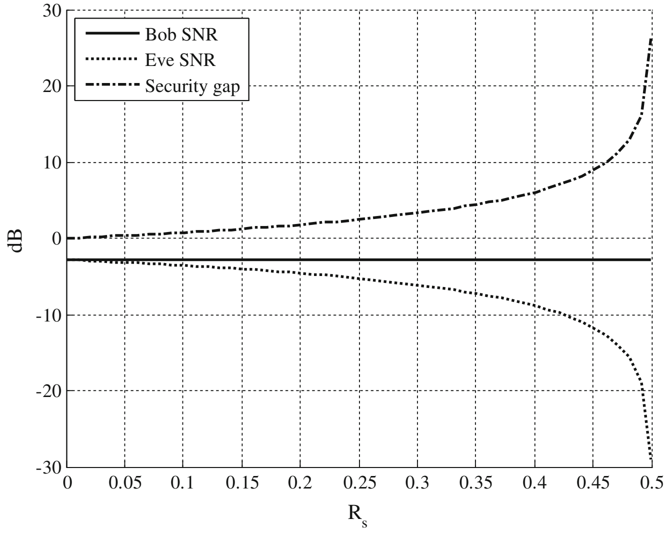

Fig. 4.4 Bob's and Eve's channels SNR and their ratio (security gap) versus secret message rate (R_s) for $R_c = 0.5$, under the hypothesis of ideal (capacity achieving) coding

through the binary input additive white Gaussian noise (BIAWGN) channel capacity (4.1). As $R_s \rightarrow R_c$ we have that Eve's SNR tends to zero (as R_F tends to zero, too). This trend is shown in Fig. 4.4, where we fix $R_c = 0.5$ and plot the Bob's and Eve's channels SNR under the hypothesis of ideal coding, for varying R_s. In the figure we also report the value of the security gap. As expected, while the SNR of Bob's channel is fixed (as the code rate), when R_s approaches R_c the SNR of Eve's channel converges to zero and the security gap diverges. Therefore, in order to have non-zero Eve's SNR and a finite security gap we must consider $R_s < R_c$, and this requires the use of randomness. However, the choice of a value of R_s not too small compared to R_c is obliged in order to achieve high values of $\widetilde{C_s}$.

4.3.2 Infinite Length LDPC Codes

Another valuable assessment in the asymptotic regime can be done by taking into account the specific LDPC code structure. In fact, any LDPC code can be represented through a Tanner graph, that is a bipartite graph having two groups of nodes, variable and check nodes, corresponding to the codeword bits and the parity-check equations, respectively. An edge exists between the jth variable node and the ith check node if and only if the (i, j)th element of $\mathbf{H}$ is 1. The number of edges connected to a node is called the degree of that node. The code Tanner graph can hence be described through the following two polynomials, which define the variable and check node degree distributions:

$$\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}, \qquad \rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1}. \tag{4.8}$$

In (4.8), d_v and d_c are the maximum variable and check node degrees, respectively, and the coefficient λ_i $\left(\rho_j\right)$ is the fraction of edges connected to the variable (check) nodes with degree i (j). For this reason, we say that these two polynomials describe the degree distributions from the edge perspective. Alternatively, $\lambda(x)$ can be converted into the polynomial $\nu(x) = \sum_{i=1}^{d_v} \nu_i x^i$, which describes the same distribution from the node perspective. The coefficients ν_i and λ_i are related as follows:

$$\begin{aligned} \nu_i &= \frac{\lambda_i/i}{\sum_{j=1}^{d_v} \lambda_j/j}, \\ \lambda_i &= \frac{\nu_i \cdot i}{\sum_{j=1}^{d_v} \nu_j \cdot j}. \end{aligned} \tag{4.9}$$

The same procedure can be applied to the polynomial $\rho(x)$ to obtain another polynomial, $c(x)$, which represents the same distribution from the node perspective. The code rate can be computed starting from $\lambda(x)$ and $\rho(x)$ as:

$$R_c = 1 - \frac{\sum_{i=2}^{d_v} \rho_i/i}{\sum_{j=2}^{d_c} \lambda_j/j}. \tag{4.10}$$

Efficient, low complexity LDPC code decoding algorithms are based on the belief propagation principle, which exploits an iterated exchange between the nodes of the code Tanner graph of soft messages concerning the reliability of each received bit. Therefore, the Tanner graph node degree distributions determine the performance of an LDPC code under belief propagation decoding. The density evolution technique [20] allows to estimate the performance achievable in the asymptotic regime (i.e., under the hypothesis of infinite length codes with Tanner graphs free of closed loops), under belief propagation decoding, by an LDPC code described through its degree distribution pair $(\lambda(x), \rho(x))$. In short, the method consists of computing the statistics of the decoder messages and their evolution during the iterations of the decoding algorithm, in such a way as to estimate the probability that decoding converges to an error-free codeword. Using a Gaussian approximation for the probability distributions of the decoder messages has been shown as a good solution to reduce the computational complexity without losing accuracy [8]. Through density evolution, a channel quality threshold can be found, above which the code is expected to converge to error-free estimations in asymptotic conditions. When we deal with AWGN channels, as in our case, such threshold is expressed in terms of an SNR value. Density evolution can also be used to optimize the code degree distributions, that is, to find degree distribution pairs able to achieve minimum values of the channel threshold.

Differently from classical transmission problems, in the considered setting we have a code chosen by Alice which is used by three receivers: Bob, Eve and Frank. In particular, Bob and Eve use the same code, defined by $\mathbf{H}$, while Frank uses the code defined by $\mathbf{H}'$, according to (4.5). Since we want both Bob and Frank to achieve good performance, we need to optimize both $\mathbf{H}$ and $\mathbf{H}'$. These two codes have different rate, and the second parity-check matrix is somehow contained in the first one. This is quite a new and challenging code optimization problem, which can be faced through a density evolution-based joint optimization of the two codes, as done in [4]. In this chapter, instead, for the sake of simplicity we follow a greedy approach, that is, we first optimize the smallest code, defined by $\mathbf{H}'$, and then, having fixed its degree distributions, we optimize the largest code, defined by $\mathbf{H}$, in an incremental way. In the next section we provide an example of optimization and compare the asymptotic performance with that achievable in the finite code length regime.

4.4 Finite Length Performance

Based on the analysis developed in the previous sections, we can estimate the reliability and security performance achievable by some finite length LDPC codes, and compare it with that achievable in asymptotic conditions.

For this purpose, we first choose the code rate R_c and the secret message rate R_s. Given their values, we need to find an optimized degree distribution pair for both Bob's and Frank's codes. This must be done by taking into account that Frank's code parity-check matrix is contained in Bob's code parity-check matrix, according to Fig. 4.2. Then, the value n of Bob's code length is fixed, and Frank's code length follows as $n' = (1 - R_s)n$. Given the two codes length and rate, as well as their optimized degree distributions, we can design their parity-check matrices through the Progressive Edge Growth (PEG) algorithm [11].

The performance achieved by these two codes can then be assessed through numerical simulations. In particular, we can fix two target values for Bob's and Frank's CER (ζ and η, respectively), and estimate the limit SNR, in terms of $\frac{E_b}{N_0}$, which is needed on the two channels in order to achieve the target CERs.

Let us consider, as an example, the following choice of the code parameters:

- $R_c = 0.5$
- $R_s = 0.4$
- $R_F = 0.16667$
- $n = 10{,}000$ or $n = 50{,}000$

In order to find good distribution pairs for both Bob and Frank, we use the greedy approach described in the previous section, with some heuristics in order to ensure that both distributions have good asymptotic thresholds but are also practically feasible through the PEG algorithm (in the sense that it succeeds in allocating all the edges without introducing short closed loops in the associated Tanner graphs). For the latter purpose, we also aim at keeping the average variable node degree in Frank's distribution below 4, since we have verified that this allows to achieve practical codes with better performance than by using higher average degrees. This way, for Frank's code we have obtained the following degree distributions (from the node perspective):

$$\begin{cases} \nu(x) = 0.1268x^6 + 0.186x^3 + 0.6872x^2, \\ c(x) = 0.2382x^4 + 0.7682x^3, \end{cases} \tag{4.11}$$

which correspond to a density evolution threshold equal to $\frac{E_b}{N_0} = -0.32\,\text{dB}$. Bob's degree distribution has been obtained starting from Frank's distribution and adding only degree-3 variable nodes, which has resulted to be a simple and efficient solution. This way, for Bob we obtain the following degree distributions (from the node perspective):

$$\begin{cases} \nu(x) = 0.07608x^6 + 0.5116x^3 + 0.41232x^2, \\ c(x) = 0.63184x^6 + 0.36816x^5, \end{cases} \tag{4.12}$$

corresponding to a density evolution threshold equal to $\frac{E_b}{N_0} = 1.1\,\text{dB}$.

Starting from these distributions, and using the PEG algorithm, we design Frank's and Bob's code parity-check matrices with ($n = 10{,}000, n' = 6{,}000$) and ($n = 50{,}000, n' = 30{,}000$). Through Montecarlo simulations of transmission over the AWGN channel with binary phase shift keying (BPSK), we estimate the value of $\frac{E_b}{N_0}$ which is needed to reach $\zeta = \eta = 10^{-2}$ when these codes are used. These $\frac{E_b}{N_0}$ values allow us to assess the performance in terms of reliability and security both in asymptotic and in finite code length conditions.

Table 4.1 Performance ($\frac{E_b}{N_0}$ in dB and $\widetilde{C_s}$ or $\widetilde{R_e^*}$ in bit/s/Hz) achieved in ideal, asymptotic and finite length conditions by Frank and Bob in the considered setting ($R_c = 0.5$, $R_s = 0.4$, $R_F = 0.16667$, $\zeta = \eta = 10^{-2}$)

Condition	Frank's $\frac{E_b}{N_0}$	Bob's $\frac{E_b}{N_0}$	$\widetilde{C_s}$ or $\widetilde{R_e^*}$
Ideal	−1.07	0.19	$\widetilde{C_s} = 0.83$
$n \to \infty$	−0.32	0.85	$\widetilde{R_e^*} = 0.77$
$n = 50{,}000$	0.4	1.05	$\widetilde{R_e^*} = 0.69$
$n = 10{,}000$	0.8	1.3	$\widetilde{R_e^*} = 0.65$

The results obtained are reported in Table 4.1, where we provide the estimated $\frac{E_b}{N_0}$ values for Bob and Frank. The corresponding values of SNR per codeword bit can be simply obtained by multiplying them by R_c and R_F, respectively. We remind that the SNR per codeword bit of Frank's and Eve's channels is the same by definition. In the table we first consider the ideal condition, that is, when both Frank's and Bob's codes are ideal and achieve capacity. For this case, besides the $\frac{E_b}{N_0}$ values, we provide the value of $\widetilde{C_s}$, computed according to (4.7). The other rows of the table instead consider LDPC codes: first in asymptotic conditions (based on density evolution), and then in the finite code length regime. For these cases, besides the $\frac{E_b}{N_0}$ values, we provide the value of $\widetilde{R_e^*} = R_e^*/R_s$, where R_e^* is computed according to (4.4).

From these results we observe that the considered code parameters do not allow to achieve perfect secrecy, as expected, since all the values in the last column of the table are below one. On the other hand, under the hypothesis of infinite length LDPC codes, a fractional equivocation rate ≥ 0.77 is reached, which is not far from the fractional secrecy capacity limit (0.83) corresponding to the case of ideal coding. Using finite length LDPC codes yields some further losses, as expected. However, if we use codes with length $n = 50{,}000$ bits, for the considered parameters we achieve a fractional equivocation rate ≥ 0.69, which means that about 70 % or more of the secret message bits are actually secret from an information theoretic standpoint. This is a useful measure, which tells us that we have a *practical coding loss* of about 30 % on the uncertainty (and hence the security level) of each transmitted message.

4.5 Conclusion

We have addressed the problem of assessing the reliability and security performance of practical coded transmissions over the AWGN wiretap channel. Differently from most previous analyses, which work in the asymptotic (i.e., infinite code length) regime, we have focused on the finite code length regime, and also taken into account the specific code structure. For this purpose, we have resorted to an information theoretic measure of secrecy which advocates Wyner's definition of perfect secrecy, and is also applicable in the finite code length regime.

This has permitted us to estimate the performance achievable by practical, finite length LDPC coded transmissions and to compare it with the ultimate limits achievable in ideal and asymptotic conditions. This tool has permitted us to show that practical coded transmissions incur in a practical coding loss which prevents them from achieving the ultimate performance limits.

Acknowledgments This work was supported in part by the MIUR project "ESCAPADE" (Grant RBFR105NLC) under the "FIRB—Futuro in Ricerca 2010" funding program.

References

1. Andersson M, Rathi V, Thobaben R, Kliewer J, Skoglund M (2010) Equivocation of Eve using two edge type LDPC codes for the binary erasure wiretap channel. In: Proceedings of the 44th Asilomar conference on signals, systems and computers, Pacific Grove, California, pp 2045–2049
2. Baldi M, Bianchi M, Chiaraluce F (2012) Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: a security gap analysis. IEEE Trans Inf Forensics Secur 7(3):883–894
3. Baldi M, Chiaraluce F, Laurenti N, Tomasin S, Renna F (2014) Secrecy transmission on parallel channels: theoretical limits and performance of practical codes. IEEE Trans Inf Forensics Secur 9(11):1765–1779
4. Baldi M, Ricciutelli G, Maturo N, Chiaraluce F (2015) Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel. In: Proceedings of IEEE ICC 2015—workshop on wireless physical layer security, London, United Kingdom, pp 446–451
5. Bellare M, Tessaro S, Vardy A (2012) Semantic security for the wiretap channel. In: Safavi-Naini R, Canetti R (eds) Advances in cryptology—CRYPTO 2012, vol 7417, Lecture Notes in Computer Science, Springer, Berlin, pp 294–311
6. Bloch M, Barros J (2011) Physical-layer security: from information theory to security engineering, 1st edn. Cambridge University Press, Cambridge
7. Cheraghchi M, Didier F, Shokrollahi A (2012) Invertible extractors and wiretap protocols. IEEE Trans Inf Theory 58(2):1254–1274
8. Chung SY, Richardson TJ, Urbanke RL (2001) Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation. IEEE Trans Inf Theory 47(2):657–670
9. Şaşoğlu E, Vardy A (2013) A new polar coding scheme for strong security on wiretap channels. In: Proceedings of IEEE international symposium on information theory, Istanbul, Turkey, pp 1117–1121
10. Harrison WK, Almeida J, Bloch MR, McLaughlin SW, Barros J (2013) Coding for secrecy. IEEE Signal Process Mag 30(5):41–50
11. Hu XY, Eleftheriou E, Arnold DM (2001) Progressiveedge-growth Tanner graphs. In: Proceedings of IEEE global telecommunication conference (GLOBECOM'01), San Antonio, Texas, pp 995–1001
12. Klinc D, Ha J, McLaughlin S, Barros J, Kwak BJ (2011) LDPC codes for the Gaussian wiretap channel. IEEE Trans Inf Forensics Secur 6(3):532–540
13. Koyluoglu OO, El Gamal H (2010) Polar coding for secure transmission and key agreement. In: Proceedings of IEEE international symposium on personal, indoor, and mobile radio communications (PIMRC 2010), Istanbul, Turkey, pp 2698–2073
14. Leung-Yan-Cheong S, Hellman M (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456

15. Liang Y, Poor HV, Shamai (Shitz) S (2008) Information theoretic security. Found Trends Commun Inf Theory **5**(4–5):355–580
16. Liu R, Liang Y, Poor HV, Spasojević P (2007) Secure nested codes for type II wiretap channels. In: Proceedings of IEEE information theory workshop, Lake Tahoe, California, pp 337–342
17. Mahdavifar H, Vardy A (2010) Achieving the secrecy capacity of wiretap channels using polar codes. In: Proceedings of IEEE international symposium on information theory, Austin, Texas, pp 913–917
18. Rathi V, Andersson M, Thobaben R, Kliewer J, Skoglund M (2009) Two edge type LDPC codes for the wiretap channel. In: Proceedings of 43rd Asilomar conference on signals, systems and computers, Pacific Grove, California, pp 834–838
19. Rathi V, Urbanke R, Andersson M, Skoglund M (2011) Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel. In: Proceedings of IEEE international symposium on information theory, St. Petersburg, Russia, pp 2393–2397
20. Richardson TJ, Urbanke RL (2001) The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans Inf Theory 47(2):599–618
21. Subramanian A, Thangaraj A, Bloch M, McLaughlin SW (2011) Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes. IEEE Trans Inf Forensics Secur 6(3):585–594
22. Thangaraj A, Dihidar S, Calderbank A, McLaughlin S, Merolla JM (2007) Applications of LDPC codes to the wiretap channel. IEEE Trans Inf Theory 53(8):2933–2945
23. Wong CW, Wong TF, Shea JM (2011) LDPC code design for the BPSK-constrained Gaussian wiretap channel. In: Proceedings of IEEE global telecommunication conference (GLOBECOM'11), Houston, Texas, pp 898–902
24. Wong CW, Wong TF, Shea JM (2011) Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel. IEEE Trans Inf Forensics Secur 6(3):551–564
25. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387