Contents

Chapter 1

Application cases of secrecy coding in communication nodes and terminals

François Delaveau, Christiane Kameni Ngassa, Cong Ling, Ling Liu, Adrian Kotelba, Renaud Molière, Jani Suomalainen, Sandrine Boumard, Nir Shapira

1.1 Introduction

The objective of this chapter is to study practical coding techniques to provide security to wireless systems. First, the chapter will briefly introduce theoretical results relevant to LDPC codes, polar codes and lattice coding for the wiretap channel. Then, it will propose practical secrecy coding schemes able to provide a reliable and confidential wireless communication link between Alice and Bob. Finally, these practical wiretap codes are implemented in WiFi and LTE testbeds and their confidentiality performance is evaluated using the Bit Error Rate (BER) as it is a simple and practical the metric for secrecy. The reader is referred to [1] for a throughout survey on recent advances related to the design of wiretap codes for information-theoretic metrics such as strong secrecy and semantic secrecy.

In the first part of this chapter, we use a nested lattice structure to design secrecy codes for Gaussian wiretap channels. We design two lattice codes with rates almost equal to the capacities of the legitimate channel (between Alice and Bob) and the wiretapper's channel (between Alice and Eve), respectively. The lattice code for the wiretapper's channel encodes random bits, and the code for the legitimate channel only makes use of the coset leader to send the message.

Furthermore, we will show that:

- a similar structure can also be extended to the MIMO channel and fading channel scenarios;
- a simplified wiretap code can be practically implemented in real radio communication standards (such as Wifi, Long Term Evolution - LTE), under state of the art radio devices and processing units, that achieve significant secrecy rate in most of radio-environments.

In section 1.2, we introduce the wiretap coding scheme for discrete channels, based on the famous Low Density Parity Check (LDPC) codes [2] and the recently proposed polar codes [3]. Then, we extend the coset wiretap coding scheme for discrete

channels to continuous Gaussian channels, by constructing polar lattices. As a result, we show that the proposed scheme is able to achieve strong secrecy and the secrecy capacity. In the meantime, an explicit lattice shaping scheme based on discrete lattice Gaussian distribution is also presented. This shaping scheme is compatible with the wiretap coding structure thanks to the versatility of polar codes, meaning that a convenient implementation is possible, as shown in following sections. Finally we study in detail the wiretap coding design for the MIMO channels and fading channels, based on a similar structure of nesting lattice codes.

In section 1.3, we introduce a practical simplified implementation of such wiretap codes, under a radio configuration that provides a slight radio advantage to Bob (a few decibels only), thanks to artificial noise and beam forming under to MIMO transmission. Our simplified secrecy scheme consists of:

- Artificial Noise and Beam Forming from Channel State Information measured on the legitimate link,
- error correction with an inner codes identical to Forward Error Correction (FEC) codes used in wireless standards,
- secrecy with an outer code involving nested polar or Reed Muller codes.

An explicit design of the scheme is given for WiFi-like signals and LTE-like signals. Performance is first analyzed with simulations under an Additive Gaussian Noise Channel, then illustrated for real field WiFi links (with real field propagation and real radio devices) and for simulated LTE link scenarios (involving real field propagation records but idealized transmitter and receiver models). Practical considerations about radio network engineering are given, and relevant radio parameters are highlighted.

Section 1.4 concludes the chapter and points out the potential of these techniques for radio standards regarding privacy of subscribers and confidentiality of data stream, and suggests tracks for their practical implementation.

1.2 Theoretical aspects of secrecy coding

1.2.1 Wiretap coding for discrete wiretap channels

In this section, we discuss the use of some practical binary codes such as LDPC codes and polar codes to construct efficient secrecy codes for discrete wiretap channels.

The vast majority of work on physical player security is based on non-constructive random-coding arguments to establish the theoretical results. Such results demonstrate the existence of codes that achieve the secrecy capacity, but do not provide any practical method to design these codes. Moreover, the design of wiretap codes is further impaired by the absence of a simple metric, such as the bit error rate, which could numerically evaluated to assess their secrecy performance [4].

In recent years, progress has been made on the construction of practical codes for physical player security, to some extent. The design methodology can be traced back to Wyner's original work on coset coding [5] which suggests that several codewords should represent the same message and that the choice of which codeword to transmit should be random to confuse the eavesdropper. In what follows, we will show how

the original concept of the coset coding could be implemented with binary codes to achieve strong secrecy.

1.2.1.1 LDPC codes for discrete wiretap channels

LDPC codes are famous for their capacity-approaching performance on many communication channels. However, wiretap codes built from LDPC codes only had limited success.

When the legitimate channel is noiseless and the wiretapper's channel is the Binary Erasure Channel (BEC), LDPC codes for the BEC were presented in [6, 7]. Especially in [7], the authors generalized the link between capacity-approaching codes and weak secrecy capacity. The use of capacity-achieving codes for the wiretapper's channel is a sufficient condition for weak secrecy [8]. This view point provided a clear construction method for coding schemes for secure communication across arbitrary wiretap channels. Then, they used this idea to construct the first secrecy capacity-achieving LDPC codes for a wiretap channel with a noiseless legitimate channel and a BEC under Message Passing decoding (MP), however in terms of weak secrecy. Later, [4] proved that the same construction can be used to guarantee strong secrecy at lower rates. A similar construction based on two-edge-type LDPC codes was proposed in [9] for the BEC wiretap channel.

The coset coding scheme using LDPC codes for the BEC wiretap channel model can be interpreted as follows. Prior to transmission, Alice and Bob publicly agree on a $(n, n(1-R))$ binary LDPC code $\mathscr{C}$, where n is the block length of $\mathscr{C}$ and R is the secrecy rate. For each possible value m of the nR bits secret message M, a coset of $\mathscr{C}$ given by $\mathscr{C}(m) = \{x^n \in \{0,1\}^n : x^n H^T = m\}$ is associated, where H is the parity check matrix of $\mathscr{C}$. To convey the message M to Bob, Alice picks a codeword in $\mathscr{C}(m)$ randomly and transmits it. Bob can obtain the secret message by calculating $X^n H^T$. Suppose that code $\mathscr{C}(m)$ has a generator matrix $G = [a_1, a_2, ..., a_n]$, where a_i denotes the ith column of G. Consider that Eve observes u unerased symbols from X^n, with the unerased positions given by $\{i : z_i \neq ?\} = \{i_1, i_2, ..., i_u\}$. Message m is secured by $\mathscr{C}$ in the sense that the probability $\Pr\{M = m | Z = z\} = 1/2^{nR}$ if and only if the matrix $G_u = [a_{i_1}, a_{i_2}, ..., a_{i_u}]$ has rank u. This is due to the fact that if G_u has rank u, the code $\mathscr{C}$ has all 2^u possible u-tuples in the u unerased positions. Therefore, by linearity, each coset of $\mathscr{C}$ would have all 2^u possible u-tuples in the same positions as well, which means that Eve has no idea which coset Alice has chosen. To guarantee that such G_u is with high probability to be full rank, we need to use the threshold property of LDPC codes, namely, for a LDPC code $\mathscr{C}^\perp$ with parity check matrix $H(\mathscr{C}^\perp)$ and Belief Propagation (BP) decoding threshold ε^{BP} on BEC, a submatrix formed by selecting columns of $H(\mathscr{C}^\perp)$ independently with probability ε would have full column rank with high probability for sufficiently large n if $\varepsilon < \varepsilon^{BP}$. If $\mathscr{C}^\perp$ is the dual code of $\mathscr{C}$, $H(\mathscr{C}^\perp)$ is equal to the generator matrix G of $\mathscr{C}$, and selecting the columns of $H(\mathscr{C}^\perp)$ with probability ε can be viewed as obtaining G_u from G through a BEC with erasure probability $1-\varepsilon$. Consequently, the problem of designing a secrecy achieving LDPC code over a binary erasure wiretap

channel with erasure probability ε can be converted to the problem of constructing a dual LDPC code over a BEC with erasure probability $1-\varepsilon$.

Let $P_e^{(n)}(\varepsilon)$ denote the probability of block error probability of a LDPC code $\mathscr{C}$ with block length n over BEC(ε). For a parity check matrix H of $\mathscr{C}$, $1-P_e^{(n)}(\varepsilon)$ is a lower bound on the probability that the erased columns of H form a full rank submatrix, which means that generator matrix $G_u(\mathscr{C}^\perp)$ resulted by a BEC($1-\varepsilon$) has full rank with probability larger than $1-P_e^{(n)}(\varepsilon)$. If $\mathscr{C}^\perp$ is used in the coset coding scheme, the conditional entropy $H(M|Z^n)$ can be bounded as

$$\begin{aligned} H(M|Z^n) &\geq H(M|Z^n, rank(G_u(\mathscr{C}^\perp))) && (1.1)\\ &\geq H(M|Z^n, G_u(\mathscr{C}^\perp))\text{is full rank})\cdot \Pr\{G_u(\mathscr{C}^\perp))\text{is full rank}\} && (1.2)\\ &\geq H(M)(1-P_e^{(n)}(\varepsilon)). && (1.3)\end{aligned}$$

Then we have

$$I(M;Z^n) = H(M) - H(M|Z^n) \leq H(M)P_e^{(n)}(\varepsilon) \leq nRP_e^{(n)}(\varepsilon). \quad (1.4)$$

Therefore, if code $\mathscr{C}$ has a BP threshold ε^{BP} such that $P_e^{(n)}(\varepsilon) = O(\frac{1}{n^\alpha})$ ($\alpha > 1$), for $\varepsilon < \varepsilon^{BP}$, then the dual code of $\mathscr{C}$ used in the coset coding scheme provides strong secrecy over a binary erasure wiretap channel with erasure probability $\varepsilon > 1-P_e^{(n)}(\varepsilon)$. Note that weak secrecy is provided if $\alpha > 0$. The design rate R of $\mathscr{C}$ should satisfy $R < 1-\varepsilon^{BP}$, while the secrecy capacity ε of the wiretap channel is larger than $1-\varepsilon^{BP}$. To achieve the secrecy capacity, $1-\varepsilon^{BP}$ is required to be very close to the code rate R. It is known that LDPC codes achieve capacity over a BEC under the BP decoding [10]. However, the parameter α can only be proved to be positive for the rate arbitrarily close to $1-\varepsilon^{BP}$ [6]. To satisfy the strong secrecy requirement $\alpha > 1$, the design rate should be slightly away from $1-\varepsilon^{BP}$.

Unfortunately, for other Binary Memoryless Symmetric Channels (BMSCs) except BECs, general LDPC codes do not have the capacity achieving property, which means that the coset coding scheme using general LDPC codes cannot achieve the secrecy capacity when the wiretapper's channel is not a BEC. In this case, spatially coupled low density parity check (SC-LDPC) codes [11], which have been proved to be able to achieve the capacity of general BMSCs, provide us a promising approach. In [12], a coset coding scheme based on regular two edge type SC-LDPC codes is proposed over a BEC wiretap channel, where the main channel is also a BEC. It is shown that the whole rate equivocation region of such BEC wiretap channel can be achieved by using this scheme under weak secrecy condition. Since SC-LDPC codes are universally capacity achieving, it is also conjectured that this construction is optimal for the class of wiretap channel where the main channel and wiretapper's channel are BMSCs and the wiretapper's channel is physically degraded with respect to the main channel.

In addition, LDPC codes has also been proposed for Gaussian wiretap channel in [13] but with a different criterion. The proposed coding scheme is asymptotically effective in the sense that it yields a Bit Error Rate (BER) very close to 0.5 for an

eavesdropper with Signal to Noise Ratio (SNR) lower than a certain threshold, even if the eavesdropper has the ability to use a Maximum A-Posteriori (MAP) decoder. However, this approach does not provide information theoretic strong secrecy.

1.2.1.2 Polar codes for discrete wiretap channels

Polar codes [3] are the first explicit codes which can be proved to achieve the channel capacity of BMSCs with low encoding and decoding complexity. As the block length increases, the capacities of bit-channels polarize to either to 0 or 1. It is shown that as the block length goes to infinity, the proportion of the bit-channels with 1 capacity is equal to the channel capacity. Therefore polar codes can achieve the channel capacity by just transmitting information bits through these perfect bit-channels.

In addition, polar coding also seems to offer a more powerful approach to design wiretap codes. Recently there has been a lot of interest in the design of wiretap codes based on polar codes. For example, [14],[15] and [16] use polar codes to build encryption schemes for the wiretap setting with BMSCs. However, these schemes only provide weak security. In [17], it is shown that, with a minor modification of the original design, polar codes achieve strong secrecy (and also semantic security). However, they could not guarantee reliability of the main channel when it is noisy. In [18], a multi-block polar coding scheme was proposed to solve this reliability problem under the condition that the number of block is sufficiently large. In addition, a similar multi-block coding scheme was discussed in [19]. Their polar coding scheme also achieves the secrecy capacity under strong secrecy condition and guarantees reliably for the legitimate receiver. However, the work in [19] only proved the existence of this coding scheme, and thus it might be computationally hard to find the explicit structure. Finally, recent works proposing the use of polar codes for the general non-degraded wiretap channel have being performed in [20] and [21].

However, in the remaining of this subsection, we concentrate on how polar codes can achieve the secrecy capacity of the binary wiretap channel [17, 18]. Define the sets of very reliable and very unreliable indices for a binary channel Q and for $0 < \beta < 0.5$ as:

$$\mathscr{G}(Q) = \{i \in [N] : Z(Q_N^{(i)}) \leq 2^{-N^\beta}\}, \text{(Reliability-good indices)} \tag{1.5}$$

$$\mathscr{N}(Q) = \{i \in [N] : I(Q_N^{(i)}) \leq 2^{-N^\beta}\}, \text{(Information-bad indices)}, \tag{1.6}$$

where $Z(Q_N^{(i)})$ and $I(Q_N^{(i)})$ represent the Bhattacharyya parameter and mutual information of the polarized bit-channel $Q_N^{(i)}$ [3]. Let V and W denote the main channel and the wiretapper's channel, respectively. The indices in set $\mathscr{G}(V)$ and set $\mathscr{N}(W)$ are the reliable and the secure indices, respectively. Then, the whole index set $[N]$ can be partitioned into the following four sets:

$$\mathscr{A} = \mathscr{G}(V) \cap \mathscr{N}(W) \tag{1.7}$$

$$\mathscr{B} = \mathscr{G}(V) \cap \mathscr{N}(W)^c \tag{1.8}$$

$$\mathscr{C} = \mathscr{G}(V)^c \cap \mathscr{N}(W) \tag{1.9}$$

$$\mathscr{D} = \mathscr{G}(V)^c \cap \mathscr{N}(W)^c. \tag{1.10}$$

Unlike the standard polar coding, the bit-channels are now partitioned into three parts: the set $\mathscr{A}$ that carries the confidential message bits M, the set $\mathscr{B} \cup \mathscr{D}$ that carries random bits R, and the set $\mathscr{C}$ that carries frozen bits F which are known to both Bob and Eve prior to transmission.

According to [17], this assignment introduces a new channel which is also symmetric. The mutual information of this channel can be upper-bounded by the sum of the mutual information of bit-channels in $\mathscr{N}(W)$. The threshold of the mutual information on each bit-channel within $\mathscr{N}(W)$ is 2^{-N^β}. Then, the mutual information between the message and the signal Eve received $I(M;Z^N)$ can be upper-bounded by $N2^{-N^\beta}$. Therefore the strong secrecy is achieved since $\lim_{N\to\infty} I(M;Z^N) = 0$. Furthermore, in case of degraded wiretap channels, the achievable secrecy rate is equal to the secrecy capacity. This is due to the facts of polarization theory [3].

This polar coding scheme is also capable of satisfying the reliability condition. According to the construction of polar codes [3], the block error probability at Bob's end is upper-bounded by the sum of the Bhattacharyya parameters of those bit-channels that are not frozen. Let $V_N^{(i)}$ denote the ith bit-channel of the main channel V , the decoding error probability P_e^{SC} under the successive cancellation (SC) decoding is upper-bounded as

$$P_e^{SC} \leq \sum_{i\in\mathscr{G}(V)\cup\mathscr{D}} Z(V_N^{(i)}) = \sum_{i\in\mathscr{G}(V)} Z(V_N^{(i)}) + \sum_{i\in\mathscr{D}} Z(V_N^{(i)}). \tag{1.11}$$

The last equation is due to the fact that set $\mathscr{G}(V)$ and set $\mathscr{D}$ are disjoint. By the definition of $\mathscr{G}(V)$, the term $\sum_{i\in\mathscr{G}(V)} Z(V_N^{(i)})$ is bounded by $N2^{-N^\beta}$, which vanishes when N is sufficiently large. However, the bound on the term $\sum_{i\in\mathscr{D}} Z(V_N^{(i)})$ is difficult to derive. To overcome this problem, a modified scheme dividing the message M into several blocks was proposed [18]. For a specific block, $\mathscr{D}$ is still assigned with random bits but transmitted in advance in the set $\mathscr{A}$ of the previous block. By embedding $\mathscr{D}$ in $\mathscr{A}$, we induce some rate loss, but obtain an arbitrarily small error probability. Since the size of $\mathscr{D}$ is very small compared with the block length N, the rate loss is negligible and finally the new scheme realizes reliability and strong security simultaneously.

We note that the information-bad set $\mathscr{N}(Q)$ can also be defined by

$$\mathscr{N}(Q) \quad = \quad \{i \in [N] : Z(Q_N^{(i)}) \geq 1 - 2^{-N^\beta}\}, \tag{1.12}$$

which is according to the Bhattacharyya parameter.

1.2.2 Wiretap coding for Gaussian wiretap channels

In this section, we address how to construct polar lattices to achieve the secrecy capacity of Gaussian wiretap channels. We will mainly focus on how to obtain the AWGN-good lattice Λ_b and secrecy-good lattice Λ_e for the mod-Λ_s Gaussian wiretap channels. The result also holds for the polar lattices when the input distribution

is uniform for the genuine Gaussian wiretap channels (GWC). The setting without power constraint is similar to the Poltyrev setting in the Gaussian point-to-point channel. Then, we introduce an explicit lattice shaping scheme for Λ_b and Λ_e simultaneously and remove the mod-Λ_s front-end. As a result, we develop an explicit wiretap coding scheme based on polar lattices which can be proved to achieve the secrecy capacity of the GWC with no requirement on SNR.

1.2.2.1 Construction of polar lattices codes

From the previous section, we see that polar codes have great potential in solving the wiretap coding problem. The polar coding scheme proposed in [17], combined with the block Markov coding technique [18], was proved to achieve the strong secrecy capacity when W and V are both BMSCs, and W is degraded with respect to V. For continuous channels such as the GWC, there also has been notable progress in lattice wiretap coding. On the theoretical aspect, the existence of lattice codes achieving the secrecy capacity to within 1/2-nat under the strong secrecy as well as semantic security criterion was demonstrated in [22]. On the practical aspect, wiretap lattice codes were proposed in [23] and [24] to maximize the eavesdropper's decoding error probability.

A lattice is a discrete subgroup of $\mathbb{R}^n$ which can be described by $\Lambda = \{\lambda = Bx : x \in \mathbb{Z}^n\}$, where B is the n-by-n lattice generator matrix and we always assume that it has full rank in this section.

For a vector $x \in \mathbb{R}^n$, the nearest-neighbor quantizer associated with Λ is $Q_\Lambda(x) = \arg\min_{\lambda\in\Lambda} \|\lambda - x\|$. We define the modulo lattice operation by $x \bmod \Lambda \triangleq x - Q_\Lambda(x)$. The Voronoi region of Λ, defined by $\mathscr{V}(\Lambda) = \{x : Q_\Lambda(x) = 0\}$, specifies the nearest-neighbor decoding region. The Voronoi cell is one example of fundamental region of the lattice. A measurable set $\mathscr{R}(\Lambda) \subset \mathbb{R}^n$ is a fundamental region of the lattice Λ if $\cup_{\lambda\in\Lambda}(\mathscr{R}(\Lambda)+\lambda) = \mathbb{R}^n$ and if $(\mathscr{R}(\Lambda)+\lambda)\cap(\mathscr{R}(\Lambda)+\lambda')$ has measure 0 for any $\lambda \neq \lambda'$ in Λ. The volume of a fundamental region is equal to that of the Voronoi region $\mathscr{V}(\Lambda)$, which is given by $\mathrm{vol}(\Lambda) = |\det(B)|$.

A sublattice $\Lambda' \subset \Lambda$ induces a partition (denoted by Λ/Λ') of Λ into equivalence classes modulo Λ'. The order of the partition is denoted by $|\Lambda/\Lambda'|$, which is equal to the number of cosets. If $|\Lambda/\Lambda'| = 2$, we call this a binary partition. Let $\Lambda/\Lambda_1/\cdots/\Lambda_{r-1}/\Lambda'$ for $r \geq 1$ be an n-dimensional lattice partition chain. For each partition $\Lambda_{\ell-1}/\Lambda_\ell$ ($1 \leq \ell \leq r$ with convention $\Lambda_0 = \Lambda$ and $\Lambda_r = \Lambda'$) a code C_ℓ over $\Lambda_{\ell-1}/\Lambda_\ell$ selects a sequence of representatives a_ℓ for the cosets of Λ_ℓ. Consequently, if each partition is binary, the code C_ℓ is a binary code.

1.2.2.2 Polar lattices for Gaussian wiretap channels

The idea of wiretap lattice coding over the mod-Λ_s GWC [22] can be explained as follows. Let Λ_b and Λ_e be the AWGN-good lattice and secrecy-good lattice designed for Bob and Eve accordingly. Let $\Lambda_s \subset \Lambda_e \subset \Lambda_b$ be a nested chain of N-dimensional lattices in $\mathbb{R}^N$, where Λ_s is the shaping lattice. Note that the shaping lattice Λ_s here is employed primarily for the convenience of designing the secrecy-good lattice and secondarily for satisfying the power constraint. Consider a one-to-one mapping:

$\mathscr{M} \to \Lambda_b/\Lambda_e$ which associates each message $m \in \mathscr{M}$ to a coset $\tilde{\lambda}_m \in \Lambda_b/\Lambda_e$. Alice selects a lattice point $\lambda \in \Lambda_e \cap \mathscr{V}(\Lambda_s)$ uniformly at random and transmits $X^{[N]} = \lambda + \lambda_m$, where λ_m is the coset representative of $\tilde{\lambda}_m$ in $\mathscr{V}(\Lambda_e)$. This scheme has been proved to achieve both reliability and semantic security in [22] by random lattice codes. We will make it explicit by constructing polar lattice codes.

Polar lattices are constructed by "Construction D" [25, p.232] using a set of nested polar codes $C_1 \subseteq C_2 \cdots \subseteq C_r$ [26]. Suppose C_ℓ has block length N and the number of information bits k_ℓ for $1 \le \ell \le r$. Choose a basis $\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_N$ from the polar generator matrix G_N such that $\mathbf{g}_1, \cdots \mathbf{g}_{k_\ell}$ span C_ℓ. When the dimension $n = 1$, the lattice L admits the form [26]

$$L = \left\{ \sum_{\ell=1}^{r} 2^{\ell-1} \sum_{i=1}^{k_\ell} u_\ell^i \mathbf{g}_i + 2^r \mathbb{Z}^N \mid u_\ell^i \in \{0,1\} \right\}, \tag{1.13}$$

where the addition is carried out in $\mathbb{R}^N$. The fundamental volume of a lattice obtained from this construction is given by

$$\mathrm{vol}(L) = 2^{-NR_C} \cdot \mathrm{vol}(\Lambda_r)^N,$$

where $R_C = \sum_{\ell=1}^{r} R_\ell = \frac{1}{N}\sum_{\ell=1}^{r} k_\ell$ denotes the sum rate of component codes. In this section, we limit ourselves to the binary lattice partition chain and binary polar codes for simplicity.

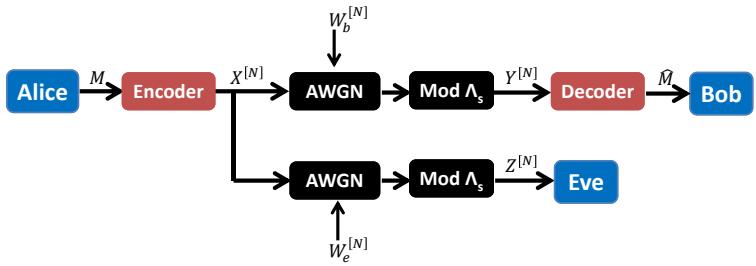

Figure 1.1: The mod-Λ_s Gaussian wiretap channel.

Now we consider the construction of secrecy-good polar lattices over the mod-Λ_s GWC shown in Figure 1.1. The difference between the mod-Λ_s GWC and the genuine GWC is the mod-Λ_s operation on the received signal of Bob and Eve. With some abuse of notation, the outputs $Y^{[N]}$ and $Z^{[N]}$ at Bob and Eve's ends respectively become

$$\begin{cases} Y^{[N]} = [X^{[N]} + W_b^{[N]}] \bmod \Lambda_s, \\ Z^{[N]} = [X^{[N]} + W_e^{[N]}] \bmod \Lambda_s. \end{cases}$$

Let Λ_b and Λ_e be constructed from a binary partition chain $\Lambda/\Lambda_1/\cdots/\Lambda_{r-1}/\Lambda_r$, and assume $\Lambda_s \subset \Lambda_r^N$ such that $\Lambda_s \subset \Lambda_r^N \subset \Lambda_e \subset \Lambda_b$[1]. Also, denote by $X_{1:r}^{[N]}$ the bits

[1]This is always possible with sufficient power, since the power constraint is not our primary concern. We will deal with it using lattice Gaussian distribution later.

encoding Λ^N/Λ_r^N, which include all information bits for message M as a subset. We have that $[X^{[N]} + W_e^{[N]}] \bmod \Lambda_r^N$ is a sufficient statistic for $X_{1:r}^{[N]}$ [26].

In our context, we identify Λ with Λ_r^N and Λ' with Λ_s, respectively. Since the bits encoding Λ_r^N/Λ_s are uniformly distributed, the mod-Λ_r^N operation is information-lossless in the sense that

$$I(X_{1:r}^{[N]}; Z^{[N]}) = I(X_{1:r}^{[N]}; [X^{[N]} + W_e^{[N]}] \bmod \Lambda_r^N).$$

As far as mutual information $I(X_{1:r}^{[N]}; Z^{[N]})$ is concerned, we can use the mod-Λ_r^N operator instead of the mod-Λ_s operator here. Under this condition, similarly to the multilevel lattice structure introduced in [26], the mod-Λ_s channel can be decomposed into a series of BMSCs according to the partition chain $\Lambda/\Lambda_1/\cdots/\Lambda_{r-1}/\Lambda_r$. Therefore, the already mentioned polar coding technique for BMSC channels can be employed. Moreover, the channel resulted from the lattice partition chain can be proved to be equivalent to that based on the chain rule of mutual information. Following this channel equivalence, we can construct an AWGN-good lattice Λ_b and a secrecy-good lattice Λ_e, using the wiretap coding technique (1.5) at each partition level. Finally, the polar wiretap coding for each partition level guarantees reliable and secure communication and the nested polar codes form a AWGN-good polar lattice for Bob and a secrecy-good polar lattice for Eve, respectively.

We then apply Gaussian shaping on the AWGN-good and secrecy-good polar lattices. The idea of lattice Gaussian shaping was proposed in [27] and then implemented in [28] to construct capacity-achieving polar lattices. For wiretap coding, the discrete Gaussian distribution can also be utilized to satisfy the power constraint. In simple terms, after obtaining the AWGN-good lattice Λ_b and the secrecy-good lattice Λ_e, Alice still maps each message m to a coset $\tilde{\lambda}_m \in \Lambda_b/\Lambda_e$ as mentioned previously. However, instead of the mod-Λ_s operation, Alice samples the encoded signal X^N from a lattice Gaussian distribution $D_{\Lambda_e+\lambda_m,\sigma_s}$, where λ_m is the coset representative of $\tilde{\lambda}_m$ and σ_s^2 is arbitrarily close to the signal power. Please see [28] and [22] for more details of the implementation of lattice Gaussian shaping.

1.2.3 Wiretap coding for MIMO and Fading Channels

In this section, we consider MIMO (Multiple Input Multiple Output) wiretap channels, where Alice is communicating with Bob in the presence of Eve, and communication is done via MIMO channels. We suppose that Alice's strategy is to use a code book which has a lattice structure, which then allows her to perform coset encoding. We analyse Eve's probability of correctly decoding the message Alice meant to Bob, and from minimizing this probability, we derive a code design criterion for MIMO lattice wiretap codes. The case of block fading channels is treated similarly, and fast fading channels are derived as a particular case.

Similarly to the Gaussian wiretap coding case mentioned in the preceding section, we consider the case where Alice transmits lattice codes using coset encoding, which requires two nested lattices $\Lambda_e \subset \Lambda_b$. Alice encodes her data in the coset representatives of Λ_b/Λ_e. Both Bob and Eve try to decode using coset decoding. For Gaussian

channels, it was shown in [29] that a wiretap coding strategy is to design Λ_b for Bob (since Alice knows Bob's channel, she can ensure he will decode with high probability), while Λ_e is chosen to maximize Eve's confusion, characterized by a lattice invariant called secrecy gain, under the assumption that Eve's noise is worse than the one experienced by Bob. We can generalize this approach to MIMO channels (and in fact block and fast fading channels as particular cases). We compute Eve's probability of making a correct decoding decision, and deduce how the lattice Λ_e should be designed to minimize this probability. A MIMO wiretap channel will then consist of two nested lattices $\Lambda_e \subset \Lambda_b$ where Λ_b is designed to ensure Bob's reliability, while Λ_e is a subset of Λ_b chosen to increase Eve's confusion.

When the channel between Alice and Bob, resp. Eve, is a quasi-static MIMO channel with n_t transmitting antennas at Alice's end, n_b resp. n_e receiving antennas at Bob's, resp. Eve's end, and a coherence time T, that is:

$$Y = H_b X + V_b, \tag{1.14}$$

$$Z = H_e X + V_e, \tag{1.15}$$

where the transmitted signal X is a $n \times T$ matrix, the two channel matrices are of dimension $n_b \times n_t$ for H_b and $n_e \times n_t$ for H_e, and V_b, V_e are $n_b \times T$, resp. $n_e \times T$ matrices denoting the Gaussian noise at Bob, respectively Eve's side, both with coefficients zero mean, and respective variance σ_b^2 and σ_e^2. The fading coefficients are complex Gaussian i.i.d. random variables, and in particular H_e has covariance matrix $\sum_e = \sigma_{H_e}^2 I_{n_e}$. As for the Gaussian case, we assume that Alice transmits a lattice code, via coset encoding, and that the two receivers are performing coset decoding of the lattice, thus $n_b, n_e \geq n_t$. Indeed, if the number of antennas at the receiver is smaller than that of the transmitter, the lattice structure is lost at the receiver. This case will not be treated. Finally, we denote by $\gamma_e = \sigma_{H_e}^2/\sigma_e^2$ Eve's SNR. We do not make assumption on knowing Eve's channel or on Eve's SNR, since we will compute bounds which are general, though their tightness will depend on Eve's SNR.

In order to focus on the lattice structure of the transmitted signal, we vectorize the received signal and obtain

$$\mathrm{vec}(Y) = \mathrm{vec}(H_b X) + \mathrm{vec}(V_b) = \begin{bmatrix} H_b & & \\ & \ddots & \\ & & H_b \end{bmatrix} (X) + (V_b) \tag{1.16}$$

$$\mathrm{vec}(Z) = \mathrm{vec}(H_e X) + \mathrm{vec}(V_e) = \begin{bmatrix} H_e & & \\ & \ddots & \\ & & H_e \end{bmatrix} (X) + (V_e). \tag{1.17}$$

We now interpret the $n \times T$ codeword X as coming from a lattice. This is typically the case if X is a space-time code coming from a division algebra [30], or more generally if X is a linear dispersion code as introduced in [31] where Tn_t symbols QAM are linearly encoded via a family of Tn_t dispersion matrices. We write $\mathrm{vec}(H_e X) = M_b u$, where $u \in \mathbb{Z}[i]^{Tn_t}$ and M_b denotes the $Tn_t \times Tn_t$ generator matrix of the $\mathbb{Z}[i]$-lattice Λ_b intended to Bob. Thus, in what follows, by a lattice point

$x \in \Lambda_b$, we mean that $x = \mathrm{vec}(X) = M_b u$, and similarly for a lattice point $x \in \Lambda_e$, we have $x = \mathrm{vec}(X) = M_e u$.

We now focus on Eve's channel, since we know from [32] how to design a good linear dispersion space-time code, and the lattice Λ_b is chosen so as to correspond to this space-time code. We also know that Eve's probability of correctly decoding is upper-bounded by

$$P_{c,e,H_e} \leq \frac{\mathrm{vol}(\Lambda_{b,H_e})}{(2\pi\sigma_e^2)^{n_t T}} \sum_{\mathbf{r}\in\Lambda_{e,H_e}} e^{-\|\mathbf{r}\|^2/2\sigma_e^2} \tag{1.18}$$

$$= \frac{\mathrm{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{n_t T}} \det(H_e H_e^*)^T \sum_{\mathbf{x}\in\Lambda_e} e^{-\|H_e X\|_F^2/2\sigma^2}, \tag{1.19}$$

where $\|H_e X\|_F^2 = \mathbf{Tr}(H_e X X^* H_e^*)$ is the Frobenius norm.

Using the equation of error probability, we derive Eve's average probability of correct decision:

$$\overline{P_{c,e}} = \mathbb{E}_{H_e}[P_{c,e,H_e}] \tag{1.20}$$

$$\leq \frac{\mathrm{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{n_t T}(2\pi\sigma_{H_e}^2)^{n_e n_t}} \cdot \tag{1.21}$$

$$\sum_{\mathbf{x}\in\Lambda_e} \int_{\mathbb{C}^{n_e\times n_t}} \det(H_e H_e^*)^T e^{-\mathbf{Tr}(H_e^* H_e \left[\frac{1}{2\sigma_{H_e}^2}\mathbf{I}n_t + \frac{1}{2\sigma_e^2} XX^*\right])} dH_e. \tag{1.22}$$

According to the analysis in [33], we finally obtain an upper bound on the average probability of correct decoding for Eve as

$$\overline{P_{c,e}} \leq C_{MIMO} \gamma_e^{T n_t} \sum_{\mathbf{x}\in\Lambda_e} \det(\mathbf{I}_{n_t} + \gamma_e XX^*)^{-n_e - T}, \tag{1.23}$$

where we set $C_{MIMO} = \frac{\mathrm{vol}(\Lambda_b)\Gamma_{n_t}(n_e+T)}{\pi^{n_t T}\Gamma_{n_t}(n_e)}$.

In order to design a good lattice code for the MIMO wiretap channel, we use the so-called "rank-criterion" of [32]. This means that, if $X \neq 0$ and $T \geq n_t$, we have $\mathrm{rank}(X) = n_t$. If we assume now γ_e is high compared to the minimum distance of Λ_e, we get

$$\overline{P_{c,e}} \leq C_{MIMO}\left[\gamma_e^{T n_t} + \frac{1}{\gamma_e^{n_e n_t}} \sum_{\mathbf{x}\in\Lambda_e\setminus\{0\}} \det(XX^*)^{-n_e - T}\right]. \tag{1.24}$$

We thus conclude that to minimize Eve's average probability of correct decoding, the design criterion is to minimize $\sum_{\mathbf{x}\in\Lambda_e\setminus\{0\}} \det(XX^*)^{-n_e-T}$.

For block and fast fading channels, we cannot use the final result for MIMO channels immediately, since the integral over all positive definite Hermitian matrices does not hold anymore. However, we can start from the generic equation and use a polar coordinates change. Then, following a similar fashion, we obtain an upper bound of

the average probability of correct decision for Eve

$$\overline{P_{c,e}} \leq C_{BF}\gamma_e^{nT} \sum_{\mathbf{x}\in\Lambda_e} \Pi_{i=1}^{n} \left[1+\gamma_e \|x_i\|^2\right]^{-1-T}, \tag{1.25}$$

where $C_{BF} = \frac{(T!)^n \mathrm{vol}(\Lambda_b)}{\pi^{nT}}$ and similarly to the MIMO case, $\gamma_e = \frac{\sigma_{He}^2}{\sigma_e^2}$. Then the design criterion for block and fast fading channels is to minimize $\sum_{\mathbf{x}\in\Lambda_e\setminus\{0\}} \Pi_{i=1}^{n} \left[\gamma_e \|x_i\|^2\right]^{-1-T}$.

1.3 Integration of secrecy coding techniques into existing Radio Access Technologies

1.3.1 Radio advantage establishment – Case of MIMO transmission

In MIMO Radio Access Technologies (RATs), the Radio Advantage is achieved by combining Beam Forming of data towards the legitimate receiver with the emission of interfering signals (Artificial Noise) elsewhere (Figure 1.2). The Artificial Noise power is controlled and the user signal is steered to optimize the decoding capability for legitimate receivers while decreasing it for eavesdroppers.

1.3.1.1 Artificial Noise and Beam Forming processing

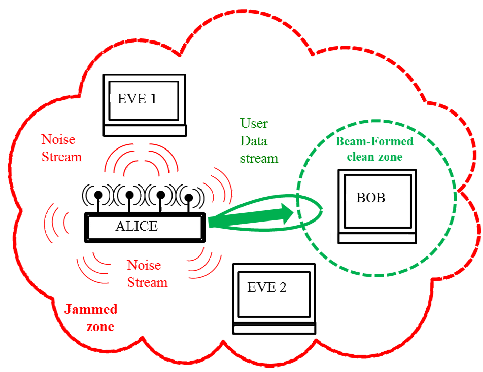

Figure 1.2: Scheme of transmission with AN-BF protections .

Most promising Artificial Noise (AN) and Beam Forming (BF) schemes studied in the literature proceed as follows [34]:

- Estimation of the legitimate Channel Frequency Response (CFR) or Channel Impulse Response (CIR), from Alice to Bob, and extraction of orthogonal directions of the legitimate CFR or CIR.
- Transmission of noise streams on orthogonal directions to the legitimate channel. As Eve cannot estimate the legitimate channel matrix, she is thus forced into low Signal to Interference + Noise Ratio (SINR) regime and is unable to decode.

- Beam Forming (BF) of the Alice-Bob data stream for Bob to maximize the legitimate link budget. Bob extracts Alice's channel and suppresses orthogonal noisy channel directions thanks to BF. In ideal cases, the interference at Bob's side completely vanishes and the SINR at Bob's side becomes equal to a Signal to Noise Ratio ($\mathrm{SINR}_{\mathrm{Bob}} = \mathrm{SNR}_{\mathrm{Bob}}$).

When AN and BF techniques are established, a better SINR is provided to Bob than to Eve in any case and the maximal $\mathrm{SINR}_{\mathrm{Eve}}$ at Eve's side is controlled by Alice. The relevant Radio Advantage ($\mathrm{RA} = \mathrm{SINR}_{\mathrm{Bob}} - \mathrm{SINR}_{\mathrm{Eve}}$) is thus guaranteed and it can be further exploited by the legitimate link to compute secrecy codes 1.3.2.

1.3.1.2 AN and BF for initiating Secrecy Coding schemes

The goal of Secrecy Codes is to ensure reliable communication for the legitimate link and to avoid any information leakage elsewhere. Secrecy Codes conceal the information sent by Alice up to a secrecy capacity. In general case, the secrecy capacity is always larger than or equal the difference of channel capacities at Bob and Eve's side; in simplest cases such as AWGN channel, it is directly driven by the Radio Advantage. Without a positive Radio Advantage, secrecy capacity is null. Moreover, in real environment with time and space varying channel, shadowing and fading, the Radio Advantage should be controlled to guarantees a minimum secrecy capacity, so that Alice and Bob can properly choose and control the secrecy coding parameters.

1.3.1.3 Power of the jamming signal – case of colocated transmit antennas

Several access methods have been developed across the years in the different standards: Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) or Orthogonal Frequency Division Multiplex Access (OFDMA). Regardless of the access method, one has to consider the limit of the decoding sensitivity which is required in the standard in term of received Signal to Interference + Noise Ratio (noted SINR in decibel). In linear value, this SINR is noted $\rho_{\mathrm{SINR}} = S_{\mathrm{Rx}}/(J_{\mathrm{Rx}} + N_{\mathrm{Rx}})$, where S_{Rx} is the received user signal power, N_{Rx} the receiving noise power, and J_{Rx} the received interference power.

- Without interference, SINR reduces to a Signal to Noise Ratio (SNR), meaning $\rho_{\mathrm{SINR}} = \rho_{\mathrm{SNR}} = S_{\mathrm{Rx}}/N_{\mathrm{Rx}}$.
- When receiving noise is negligible SINR reduces to a Signal to Interference Ratio (SIR), meaning $\rho_{\mathrm{SINR}} = \rho_{\mathrm{SIR}} = S_{\mathrm{Rx}}/J_{\mathrm{Rx}}$.
- In any case, $\mathrm{SINR} \leq \mathrm{SIR}$ and $\rho_{\mathrm{SINR}} \leq \rho_{\mathrm{SIR}}$, $\mathrm{SINR} \leq \mathrm{SNR}$ and $\rho_{\mathrm{SINR}} \leq \rho_{\mathrm{SNR}}$.

When the sources of Artificial Noise and user data stream are strictly co-located (i.e. same transmitting antenna elements), Alice has to adjust her jamming signal $J_{\mathrm{Tx,Alice}}$, to the user transmit signal $S_{\mathrm{Tx,Alice}}$ to a minimum value of $\rho_{\mathrm{SIR,Rx,Eve}}$, called ρ_{min} that makes decoding impossible for Eve even in optimal reception condition (e.g. whatever her receiving noise is). For any RAT, a relevant sufficient condition is

$\rho_{\text{SIR,Tx,Alice}} = S_{\text{Tx,Alice}}/J_{\text{Tx,Alice}} \leq \rho_{\min}$ leading to $J_{\text{Tx,Alice}} \geq S_{\text{Tx,Alice}}/\rho_{\min}$.

In the case of FDMA TDMA or OFDMA RATs, such a co-located jamming signal at each orthogonal direction with power roughly equal to the user signal ($\rho_{\text{SIR,Tx,Alice}} \approx 1$) is enough to limit most eavesdropping risks. More generally, a jamming signal 6 dB above the data stream should avoid any eavesdropping risk of FDMA TDMA or OFDMA link. Extremal $\rho_{\min}$ should thus verify $\rho_{\min} \geq 0.25$ (-6 dB).

In the case of Pseudo Noise (PN) or CDMA schemes such as UMTS, the situation is more complex because the lowest data rate signals have spreading factors of 256 (24 dB), Thus practical value of $\rho_{\min}$ is around -18 dB. Nevertheless, the power control and the global received noise at Eve's side highly depend on the network engineering practices regarding signaling and data communication streams under the carrier of the serving and neighbor cells. As a consequence, a practical $\rho_{\text{SIR,Tx,Alice}}$ value of 12 dB for a co-located jamming signal achieves a significant advantage in most of 3G network engineering and traffic scenarios.

1.3.1.4 Impact of the locations of antennas that transmit user and jamming signals

When the sources of artificial noise and user data stream are not strictly co-located (i.e. different antennas or different antenna elements, such as in many scenarios of cooperative jamming), the efficiency of AN-BF is highly dependent on the spatial correlation at Bob's side, and on the source separation capabilities at Eve's side [35].

Indeed, the channel estimation performed by Bob over dedicated frames sent by Alice may not match perfectly for artificial noise issued from different locations of antenna.

Moreover several questions relevant to Eve's capabilities regarding source separation remain open. Even with a very small distance between transmitting antennas (lower than a quarter of wave length), several laboratory experiments mentioned in [36] and performed in [35] showed that an accurate location of Eve's multiple antennas combined with analog mitigation techniques and digital power inversion may achieve practical discrimination of the user data stream and mitigation of the artificial noise with significant performance.

Nevertheless, even if discrimination of Alice's streams can be performed at Eve's side, real fied signal recorded and processed in [36] show that recovering of the legitimate channel by Eve is almost impossible when propagation is dispersive.

As a conclusion, we should consider that the most resilient AN-BF schemes would use co-located and even same antenna elements for artificial noise and user data stream.

1.3.2 Description of the practical Secrecy Coding scheme

Our goal is to design a low-complexity and practical secrecy coding scheme for current and next-generation Radio Access Technologies.

Since polar codes provide strong security for discrete channels [17], a first idea is to concatenate them to a capacity approaching code. The capacity approaching code

should be the inner code so that the channel between the polar encoder and the polar decoder can be viewed as a Binary Symmetric Channel (BSC). Thus, we propose a scheme which is initially composed of a LDPC code as inner code and of a polar code as outer code 1.3a. The inner code can also be any FEC codes employed currently for practical wireless communications such as Turbo codes or Binary Convolutional Codes (BCC). The design of the inner code is therefore straightforward as we only follow the requirements defined in standards. In this work we consider particularly LDPC codes defined in the 802.11 standard (WiFi).

1.3.2.1 Construction of the outer code using polar codes

We first consider two nested polar codes of length $N = 2^n$ as the outer code. The rate of the first polar code is the target rate for Eve, denoted R_E, and the rate of the second polar code is the target rate for Bob, denoted, R_B. Since we suppose that legitimate users have a Radio Advantage over Eve, $R_E < R_B$ (meaning that the wiretap channel is degraded). Therefore Eve can perfectly decode $N.R_E$ bits and Bob $N.R_B$ bits. In order to confuse Eve and to ensure 0.5 error probability at her side, we send random bits over $N.R_E$ perfect bit-channels.

The design strategy of the outer code is then the following.

- Bhattacharyya parameters are computed for Bob target's error probability at the output of the inner decoder
- Bit-channels are sorted in ascending order of their Bhattacharyya parameters
- Random bits are sent over the first $N.R_E$ bit-channels.
- Information bits are sent over the following $N(R_B - R_E)$ bit-channels.
- Frozen bits (i.e. zeros) are sent over the remaining bit-channels.

1.3.2.2 Construction of the outer code using Reed-Muller codes

We propose to use Reed-Muller (RM) codes as an alternative to polar codes in the design of the outer code [37]. The constructions of Reed-Muller codes and polar codes are similar. The main difference is the selection criteria of bit-channels. Indeed, for polar codes, the selection criteria is the Bhattacharrya parameter whereas this selection criteria is the Hamming weight of rows of the generator matrix for the Reed-Muller codes. Consequently, at same length, the Reed-Muller code usually has a larger minimum distance and better performance than the corresponding polar code .

The design strategy for the outer Reed-Muller code is then modified as follows.

- Hamming weights of generator matrix's rows are computed
- Bit-channels are sorted in ascending order of their Hamming weight
- Random bits are sent over the $N.R_E$ first bit-channels.
- Information bits are sent over the $N(R_B - R_E)$ following bit-channels
- Frozen bits (i.e. zeros) are sent over the remaining bit-channels.

1.3.2.3 Decoding algorithm for polar and Reed-Muller codes

When Arikan introduced polar codes, he also proposed a low-complexity decoding algorithm named the successive cancellation decoding algorithm [3]. However, the

Table 1.1: Designed Secrecy Codes

Secrecy Code	SC 1	SC 2	SC 3	SC 4
Inner Code	LDPC code of length 1296 and rate $5/6$ defined in the 802.11 standard			
Outer code	Polar code	Polar code	Reed-Muller code	Reed-Muller code
Eve's target rate	0.05	0.13	0.05	0.05
Bob's target rate	0.55	0.52	0.5	0.4
(R, F, I)	$(51,512,461)$	$(133,399,492)$	$(56,430,538)$	$(56,330,638)$
Secrecy coding rate	0.4	0.3	0.33	0.25

successive cancellation decoder has limited performance at moderate block length. In [38], Tal and Vardy proposed an improved version of the SC decoder referred to as successive cancellation list decoder. We use the LLR-based successive cancellation list decoding algorithm presented in [39] (with list size of 8).

1.3.2.4 Practical metrics for secrecy

The security provided by each secrecy code is evaluated by computing the Bit Error Rate (BER). Secrecy is considered to be achieved when BER $= 0.5$.

1.3.2.5 Practical designed secrecy codes

We use the LDPC code of length 1296 and rate $5/6$ defined in the 802.11n/ac standard as the inner code. The outer code is either a polar code of length $2^{10} = 1024$ or a Reed-Muller code of the same length. For simulation purpose, four outer codes were designed using polar and Reed-Muller codes of different rates. The parameters of these four secrecy codes are presented in Table 1.1. Note that R, I and F denote respectively the number of random bits, information bits and frozen bits.

1.3.3 Performance analysis of designed Secrecy Codes

Figure 1.3a presents the architecture of the proposed secrecy codes.

Simulations were carried out with Matlab and messages were sent over an AWGN channel using a QPSK modulation.

Taking into account characteristics of WiFi encoders, Figure 1.3b shows the performance of the designed secrecy codes.

- The black curve represents the Bit Error Rate (BER) at the output of the LDPC decoder.
- Red curves represent the BER at the output of secrecy polar decoders.
- Blue curves represent the BER at the output of secrecy Reed-Muller decoders.

The Belief Propagation algorithm is used for LDPC decoders and the successive cancellation list decoding algorithm is used for polar and Reed-Muller decoders.

The results show that:

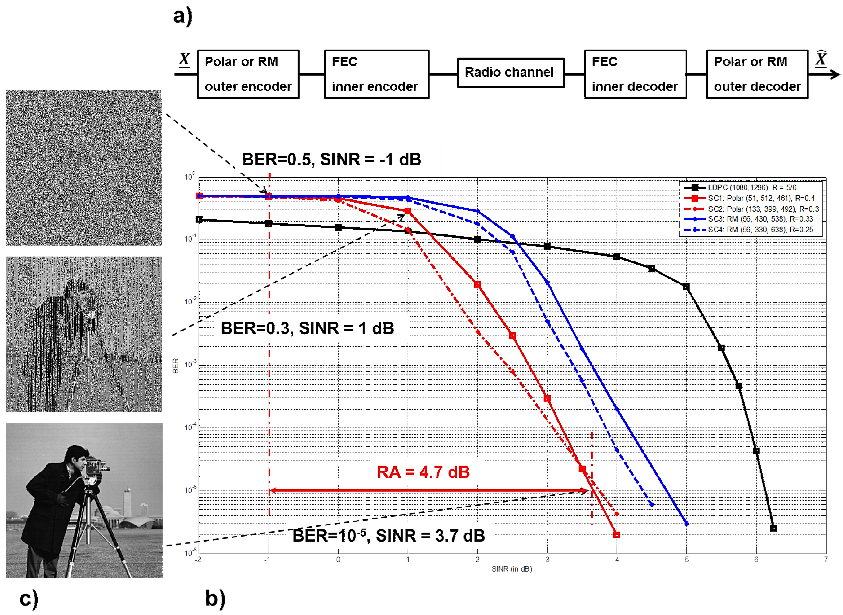

Figure 1.3: Structure and simulated performance of practical secrecy codes.

- Polar-based secrecy codes have better reliability performance than RM-based secrecy codes of similar rates.
- When SINR ≤ -1 dB, the BER at the output of the four secrecy codes is equal to 0.5. Meaning that, all secrecy codes guarantee no information leakage if Eve's SINR is less than -1 dB.
- When SINR ≤ 0 dB, the BER at the output of secrecy codes SC3 and SC4 is equal to 0.5 while the BER at the output of secrecy codes SC1 and SC3 is above 0.45. Meaning that if Eve's SINR is less than 0 dB, SC3 and SC4 guarantee no information leakage while only a limited amount of information (less than 5%) is leaked for SC1 and SC2.
- For a target error probability of 10^{-5} for Bob, the required Radio Advantage to ensure no information leakage is limited to 4.4 dB to 4.7 dB.

These simulation results demonstrate that Eve cannot retrieve any transmitted information when a slight Radio Advantage (< 5 dB) is provided to legitimate users. The secrecy is achieved with a limited increase in coding and decoding complexity.

Figure 1.3 illustrates the performance of the secrecy coding scheme by simulating the transmission of the cameraman image over an AWGN channel using the polar-based secrecy codes of rate 0.4 (SC1), for different values of the SINR.

Figure 1.3c shows that:

- when the SINR ≤ -1 dB no clue on the transmitted image can be deduced from the received image. The BER at the output of the secrecy code is equal to 0.5.
- When SINR $= 1$ dB, BER $= 0.3$ and Eve manages to successfully decode enough information on the transmitted image. Although 0.3 is a high value for a BER, too much information is leaked. Consequently, Eve's BER should be as close as possible of 0.5 to guarantee no information leakage.
- When SINR ≥ 3.7 dB, BER $= 10^{-5}$ and Bob can perfectly decode the transmitted information.

1.3.4 Simulation results on LTE signals

1.3.4.1 Configuration of simulations

The simulations described below are relevant to LTE cellular based links at frequency 2.6 GHz in the downlink transmission direction mode referred as Transmission Mode 7 (TM7) which support Beam Forming.

For performance assessment of the proposed secrecy-coding scheme, we use MATLAB-based LTE link-level simulators [40] developed by Technical University of Vienna. The simulators implement standard-compliant LTE downlink and LTE uplink transceivers with their main features, i.e., basic channel models, modulation and coding, multiple-antenna transmission and reception, channel estimation, and scheduling. For reliable performance assessment, the channels seen by Bob and Eve need to show a distance-dependent correlation, which WINNER II model cannot model. For that reason, the QuaDRiGa channel model [41], which can produce correlation between Alice-Bob, Alice-Eve, and Bob-Eve channels, is used. The configuration of the simulation and its main parameters are synthesized figure 1.4a.

- The LTE carrier frequency is 2.6 GHz and the channel bandwidth is 10 MHz. Alice transmits data to Bob using QPSK modulation with coding rate $602/1024$, which corresponds to channel quality indicator (CQI) value of 6. Bob's SNR is assumed to be 10 dB.
- We consider an outdoor urban micro-cell radio environment with line-of-sight component, so called B1 [42], with LOS component (delay spread: 36 ns, shadow fading: 3 dB) and NLOS component (delay spread: 76 ns, shadow fading: 4 dB). Alice uses a 4-element circular antenna array circular antennas array, Bob and Eve are single antenna each and they use the same processing for CM estimation (least-squares method). Similarly, in the uplink direction, Alice and Eve use least-squares method to estimate, respectively, Bob-Alice and Bob-Eve channels.
- Distance between Alice and Bob is 15 m and the distance between Bob and Eve is 11.5 m, which corresponds to 100 wavelengths at carrier frequency of 2.6 GHz, Eve being located at one of four possible locations denoted by P1, P2, P3, and P4 lying on the circle of radius 11.5 m (100 wavelength) centered at Bob's position

1.3.4.2 Simulation of transmitting and processing of the secret en-coded LTE signals

Assuming Time-Division-Duplexing (TDD) transmission mode, the BF coefficients are determined from the Channel Matrix (CM) estimated by the eNodeB Alice from the uplink transmission of reference signals by intended User Equipment (UE) Bob. A single BF coefficient is used per resource block. The AN signal is generated such that it lies in the null space of the Alice-to-Bob CM and it is added to all symbols. Following the discussion in Section 1.3.1.3, the AN signal lies 6 dB above information-bearing signal to reduce any eavesdropping risk.

Besides, in LTE systems, turbo codes are used for forward-error correction. Thus, following the architecture of figure 1.3a, the secrecy-coding scheme is implemented by concatenating an outer Reed-Muller code with the inner standard-compliant turbo code. We use $(56, 330, 638)$ Reed-Muller based secrecy code defined in table 1.1 as the secrecy code.

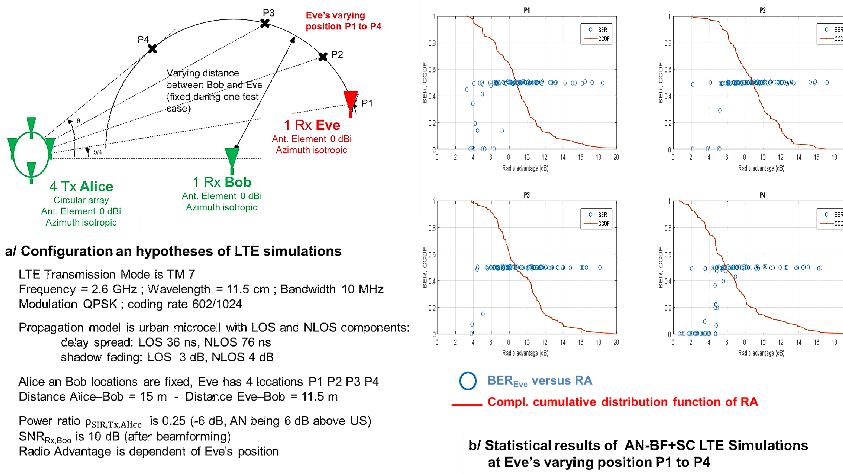

Figure 1.4: Configuration, parameters and results of LTE simulations.

1.3.4.3 Results of simulations under LTE carrier Transmission mode TM7- Discussion

At each Eve's location, we take 100 independent snapshots of channel model, and for each of them, we simulate the transmission of 20 LTE sub-frames . The observed figures-of-merit include Eve's and Bob's bit-error rate as well as established radio advantage of Bob over Eve. In Figure 1.4b we plot of the empirical complementary cumulative distribution function (ccdf) of Bob's radio advantage over Eve as well as Eve's bit error rate as a function of the radio advantage.

These results first demonstrate that radio advantage of 5 6 dB is sufficient to preclude Eve from reliably decoding the transmitted signal.

Nevertheless, the location of Eve with respect to Alice and Bob significantly affects the radio advantage. For example, if Eve is closer to Alice than Bob (P4), her signal is obviously stronger than Bob's signal and the probability of achieving a sufficient RA is significantly reduced. For example, when Eve is in position P2 or P3, the probability of achieving at least 5 dB of radio advantage is above 90%, when Eve is in position P4 the respective probability drops to 60% only.

Furthermore, establishing and maintaining sufficient radio advantage is a challenging engineering task in fading channels, because fading can affect the CM measurement and the BF establishment: while channel state is changing, any channel estimation errors reduce the effectiveness of the AN-BF processing.

Thus the AN-BF and secrecy coding scheme should be designed for the worst-case scenario and applied for high mean SNR regimes where channel estimation errors are smaller, whatever is the fading into the transmission. It can thus be expected that non-line-of-sight long range radio propagation should be more difficult to handle in LTE networks than short range propagation because the AN and the BF values are fixed for the whole resource block (performance suffers when channel changes occur during the block). Nevertheless, in any case, the power control can contribute to the AN-BF + SC scheme by ensuring that the $\mathrm{SINR}_{\mathrm{Rx,Bob}}$ at Bob's side is sufficiently large over the block to allow successful CM estimation, efficient BF establishment at Alice's side and reliable decoding at Bob's side, while AN still prevents Eve's decoding attempts.

Finally, the simulation results above demonstrate that the secrecy schemes of figure 1.3 should well apply to real world radio-cellular networks (significant performances with limited RA value). Besides, to achieve significant performances in most difficult NLOS propagation conditions, these results also show that the network engineering (SINR threshold of the legitimate link, power control, etc.) has to be adapted in the same time of the tuning of the AN-BF + SC scheme.

1.3.5 Experimental results on WiFi signals

1.3.5.1 Configuration of experiments

The experiments described below are relevant to 802.11ac WiFi links at frequency 5.2 GHz, with standard modulation coding schemes at transmitter Alice and at receivers Bob and Eve. The geometry is indoor and Line of Sight (LOS).

The access point Alice is implemented on a 4-antenna dedicated chipset (CL 2400), developed by the Company Celeno Communications. Through the IPERF test application (commonly used to generate TCP and USP traffic), Alice transmits a pre-defined bit pattern as User Signal (US) to facilitated Bit Error Rate (BER) Evaluation. In addition, Alice adds Artificial Noise (AN) to the data part of the user signal bit pattern and Beam Forms it towards Bob.

Bob is implemented by using a single-antenna Smartphone device (XIAOMI's MI5). Eve is implemented by using a 3-antennas MacBook Pro, working in sniffer mode with the Wireshark application. The Wireshark application outputs Packet

Error Rates and stores Rx signals frames. The BER at Eve side is then computed offline (using a Matlab script) by comparing the stored received packets to the known transmitted pattern.

The overall geometry and locations of Alice Bob and Eve are represented into figure 1.5a.

The overall hardware and software components hosting the AN-BF application are represented figure 1.5b (CL 2400 wifi chipsets and host board). The AN-BF processing is based on a Spatial Multiplexing (SM) transmit matrix which is computed from an Single Value Decomposition (SVD) of the Channel Matrix (CM) issued from channel sounding exchanges. Note that when antennas are calibrated at Alice and Bob's side, AN-BF can be based on channel reciprocity assumption, without any added information exchanged over the air.

During computations, Alice has to restrict Rx or Tx operations and match numerous technological constraints. Thus, several compressions, acceleration and parametrization capabilities are added to support AN-BF:

- QR decomposition and size reduction of the matrix involved in the computations,
- adjustment of the number of noise spatial streams (NAN=3 among 4) and user spatial stream (NSS=1 among 4),
- adjustment of the power ratios $\rho_{\text{SIR,Tx,Alice}}$ between the data and the noise streams,
- uniform distribution of independent noise samples over all transmitting antennas,
- gain scaling of the entire signal to ensure that the total Tx power matches the required digital back-off level and avoids saturation of the Digital to Analog Converter, etc.

The WiFi transmitting and receiving radio parameters are recalled figure 1.5c

Figure 1.5d provides the values of the power ratios $\rho_{\text{SIR,Tx,Alice}}$ and the relevant values of Packet Error Rates (PER at Bob's Side) that lead to the experimental results shown in the following paragraphs.

1.3.5.2 Transmission and processing of the secret encoded Wifi signals

To experiment the decoding of secret codes by Eve and Bob, a fixed frame is still sent by Alice over repeated transmissions (by using the same IPERF application as above). These frame is now off-line pre-computed from the initial bit pattern and one of the secret encoder described in paragraph 1.3.3. The parameters of the secrecy code used in the experiments results below is the polar-based secrecy code (R,I,F) = $(102, 409, 513)$.

Note that the code-word length of 1024 bits perfectly matches the Wifi Frame length. While the new secret encoded bit pattern now replaces the initial one, the decoding at Bob's and Eve's side is done offline from signal frames records by using a Matlab script.

The whole procedure allows to estimate the efficiency of Secrecy Coding through

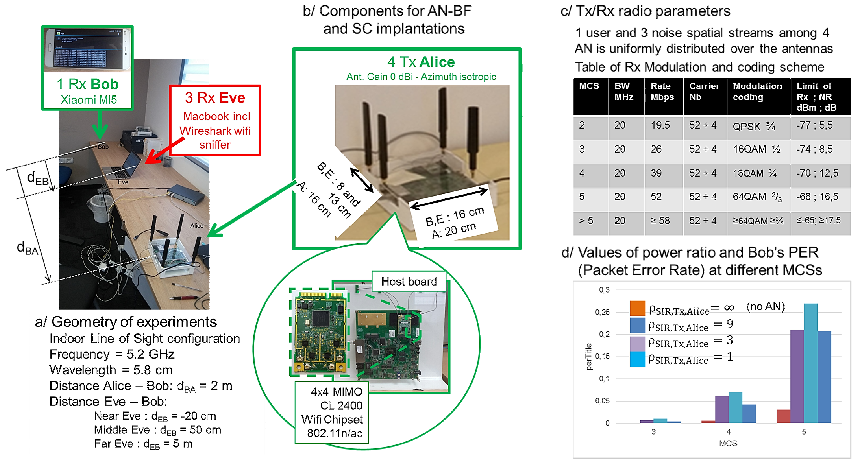

Figure 1.5: configuration of the AN-BF and SC experiments in Indoor Line Of Sight (LOS) environment.

BER estimates at Eve's side. Moreover, comparison of Eve's BER when using first the native the WiFi FEC scheme (either LDPC or BCC) and then the concatenated secret coding scheme described in paragraph 1.3.3, allow to analyze first the basic protection of the Radio Advantage provided by AN-BF alone and the security enhancement due to the secrecy coding scheme itself.

Recall that Eve has 3 Rx antennas and is supposed to have the complete information about the secret code. Moreover, she can test any Modulation and Coding Scheme in her attempts to recover parts of the legitimate user information, MCS2 being the best for Eve regarding the resilience of her decoding when facing Artificial Noise.

1.3.5.3 Experimental results in Line of Sight geometry (LOS) – Discussion

Figure 1.6 shows the results of the AN-BF scheme and of the combined AN-BF + SC scheme on recorded WiFi frames. Two (low and middle) values of the power ratio $\rho_{\text{SIR,Tx,Alice}}$ are taken into account ($\rho_{\text{SIR,Tx,Alice}} = 3$ in figure 1.6a while the AN power is 25 percent of the total power and $\rho_{\text{SIR,Tx,Alice}} = 1$ in figure 1.6b while the AN power is 50 percent of the total power).

In any cases, Bob uses the MCS4 decoder with $\text{PER}_{\text{Bob}} \approx 0$, $\text{BER}_{Bob} \leq 0.1$, $\text{SINR}_{\text{Rx,Bob}} \geq 12.5$ dB while Eve attempts to decode the signal frames by using the MCS2 decoder (that advantages her by decreasing the radio Advantage of Bob Eve gets about 4 dB more compared to the MCS4). The Radio Advantage indications in figure 1.6 are given with respect of one received antenna at Eve's side.

When comparing the result of figure 1.6 to analyses of paragraph 1.3.3, remembering the particular propagation properties of indoor LOS configurations and con-

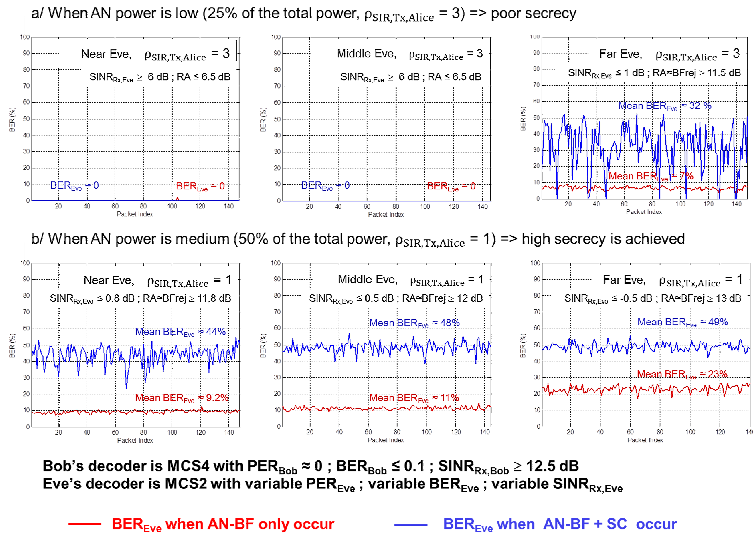

Figure 1.6: experimental results of secrecy code schemes in LOS environment - Comparison between AN-BF alone and AN-BF + SC for several values of $\rho_{SIR,Tx,Alice}$.

sidering the low and medium values of power ratio $\rho_{\text{SIR,Tx,Alice}}$, we can note the following trends:

- At far Eve's locations, even in LOS geometry when the power ratio $\rho_{\text{SIR,Tx,Alice}}$ remains low, the radio advantage is very significant. This very favorable situation for security occurs mainly thanks to the Beam Forming (BF) that achieves significant BF rejection performances (12 dB and more in the experiments reported in figure 1.6).
- We can be confident that similar trends would occur in any NLOS environments, whatever is Eve's location, because the BF rejection should be enhanced thanks to the positive effects of propagation reflectors in the neighborhood of Alice and Bob.
- When coming back to LOS configuration and considering now Eve locations closer to Bob. One has to interpret the decreasing performances of the AN-BF + SC scheme in the following sense. First, a main lobe is most often the result of LOS propagation impact to BF processing. Second, this main lobe can be intercepted by Eve. In addition, the 3 Rx of Eve in our experimental configuration can provide some array discrimination and processing gain on the data user signal. Finally the effect of BF at Alice side can be partially mitigated by Eve close to Bob. To counter this, the power ratio $\rho_{\text{SIR,Tx,Alice}}$ should be decreased down to value $\rho_{\text{SIR,Tx,Alice}} = 1/4$ (that correspond to an AN power that is 6 dB over the user signal power as mentioned in 1.3.1.3), and the antenna aperture at Alice's side should be enlarged to decrease the main lobe size and improve the rejection performances of BF.

Finally, the experimental results above are evidence that the proposed secrecy schemes well applies to real world WLAN chipsets and propagationwith limited AN power in most of practical NLOS and LOS configurations. It is also evident that even when very adverse conditions occur (LOS configurations, Eve very close to Bob or very close to Alice), secrecy efficiency should be achieved through a suitable tuning of the radio parameters (increasing of the AN noise, enlarging of the Alice antenna array).

1.3.6 Tuning of the Radio Advantage for OFDM/QPSK wave forms such as Wifi and LTE signals considerations on radio engineering

Analysis and experimental results show that the Bit Error Rate at the output of the polar decoder is 0.5 up to a given *attacker threshold* of the SINR ($\mathrm{SINR}_{\mathrm{Rx,Eve}}$), depending on the modulation and concatenated coding scheme, that ensures no information leakage.

When the $\mathrm{SINR}_{\mathrm{Rx,Bob}}$ increases, the bit error rate at the output of the polar decoder vanishes. When $\mathrm{SINR}_{\mathrm{Rx,Bob}}$ is high enough (greater than a user threshold $\mathrm{SINR}_{\mathrm{user,min}}$) the bit error rate at the output of the polar decoder approaches zero.

In all the presented simulation and tests, only a few dB of Radio Advantage (typically 3 dB to 5 dB) is required to provide both reliability and secrecy to legitimate users. These reasonable values ensure the compatibility of Secrecy Code schemes with exiting AN-BF schemes and other means for providing the Radio Advantage (such as directive antennas for transmission, Full Duplex communications technologies)

For these Secrecy Coding schemes, the typical value of $\mathrm{SINR} = -1$ dB (0.8) in linear should be considered as the maximum $\mathrm{SINR}_{\mathrm{Rx,Eve}}$ tolerated at Eve's receiver as demonstrated in paragraph 1.3.3.

Therefore the corresponding $\rho_{\min}$ should be equal to 0.8 to be used at Alice's transmitters in order to tune the Artificial Noise power from the value of the user data stream power with a ratio $(J_{\mathrm{Tx}}/S_{\mathrm{Tx}}) \geq 1/\rho_{\min}$.

Then, the tuning of the power of the user (signaling or data) stream and of the Beam Forming performance is set in order to achieve reliable communication for Bob. When considering the mean channel propagation losses (noted l_{AB} in linear values, L_{AB} in dB), the beam forming rejection (noted $\mathrm{bf}_{\mathrm{rej}}$ in linear value, $\mathrm{BF}_{\mathrm{rej}}$ in dB), the receiving noise at Bob's side (noted N_{Rx} in linear values), and the SNR threshold of Bob's receiver (noted $\rho_{\mathrm{Thres,Rx}}$ in linear value),

- the global signal to noise + interference ratio at Bob side's is given by $\rho_{\mathrm{SINR,Rx,Bob}} = [S_{\mathrm{Tx}}/l_{\mathrm{AB}}]/[(J_{Tx}/l_{\mathrm{AB}}/\mathrm{bf}_{\mathrm{rej}}) + N_{\mathrm{Rx}}]$,
- and the global signal to noise ratio by $\rho_{\mathrm{SNR,Rx,Bob}} = [S_{\mathrm{Tx}}/l_{\mathrm{AB}}]/[N_{\mathrm{Rx}}]$.

In practice, one has to:

- define two margin values η_1 and η_2 such that $1 < \eta_2 < \eta_1$ to tune of the radio engineering;

- tune the user stream power S_{Tx} to achieve enough receiving power such that $\rho_{\mathrm{SNR,Rx,Bob}} \geq \rho_{\mathrm{Thres,Rx}}.\eta_1$,
- turn the BF rejection $\mathrm{bf}_{\mathrm{rej}}$ such that $\rho_{\mathrm{SINR,Rx,Bob}} \geq \rho_{\mathrm{Thres,Rx}}.\eta_2$.

As a summary, it appears that two main radio parameters are necessary to implant the secrecy coding schemes:

- A "minimum $\mathrm{SINR}_{\mathrm{user,min}}$" for the legitimate link, which is relevant to the performance of the modulation and coding schemes for Bob (when taking into account some margin, typical values are a few dBs, 3 to 5 dB in the secret codes considered above). Achieving SINR values greater than $\mathrm{SINR}_{\mathrm{user,min}}$ for ongoing legitimate radio-communications involves some network engineering activities: management of the network topology (real field path losses, transmit power, energy budget link, and control of the Beam Forming performance $\mathrm{BF}_{\mathrm{rej}}$ in the established AN scheme (input by Channel State Information). Note that all these parameters are involved in the equalization processing and in the Quality of Service Management.
- A "SINR Security gap" $\mathrm{SINR}_{\mathrm{SG}}$ that represents the lower bound of the Radio Advantage to be provided to the legitimate link by increasing the interference J_{Tx} emitted by Alice. $\mathrm{BF}_{\mathrm{rej}}$ being controlled by Alice and Bob, $\mathrm{SINR}_{\mathrm{SG}}$ drives the tuning of the Artificial Noise power to ensure the Radio Advantage independently of Eve's location.

In general case, Alice and Bob have thus to manage parameters S_{Tx}, J_{Tx} and $\mathrm{bf}_{\mathrm{rej}}$ so that $\mathrm{SINR}_{\mathrm{user,min}}$ and input $\mathrm{SINR}_{\mathrm{SG}}$ values are between 3 to 5 dB depending on the applied secrecy coding scheme. Nevertheless, the exact radio advantage remains dependent on Eve's Receiver capabilities.

In simplified optimal case where jamming signal transmission is co-located with user signal transmission (Eve has no spatial rejection capabilities whatever is her receiver performance), and receiving noise at Bob is negligible (thus $\mathrm{SINR}_{\mathrm{Rx,Bob}} \approx \mathrm{SIR}_{\mathrm{Rx,Bob}} = \mathrm{SIR}_{\mathrm{Tx,Alice}} + \mathrm{BF}_{\mathrm{rej}}$ while we have in any case $\mathrm{SINR}_{\mathrm{Rx,Eve}} \leq \mathrm{SIR}_{\mathrm{Rx,Eve}} = \mathrm{SIR}_{\mathrm{Tx,Alice}}$), Alice and Bob get facilitated radio management of the link with parameters $\mathrm{SIR}_{\mathrm{Tx,Alice}}$ and $\mathrm{BF}_{\mathrm{rej}}$ such that $\mathrm{SIR}_{\mathrm{Tx,Alice}} + \mathrm{BF}_{\mathrm{rej}} \geq \mathrm{SINR}_{\mathrm{user,min}}$ and $\mathrm{SIR}_{\mathrm{Tx,Alice}} \leq \mathrm{SNR}_{\mathrm{user,min}} - \mathrm{SINR}_{\mathrm{SG}}$.

Hence, the Radio Advantage verifies $\mathrm{RA} \geq \mathrm{BF}_{\mathrm{rej}}$ (non-equality occurs when Eve's receiver noise is significant, what increasing the advantage of Bob), and a simplified requirement for $\mathrm{BF}_{\mathrm{rej}}$ is achieved by considering
$\mathrm{BF}_{\mathrm{rej}} \geq \max\{\mathrm{SINR}_{\mathrm{SG}}, \mathrm{SINR}_{\mathrm{user,min}} - \mathrm{SIR}_{\mathrm{Tx,Alice}}\}$.

1.4 Conclusion: security upgrades provided to future Radio Access Technologies

As described above, any secrecy coding schemes applies under the assumption that a prior radio advantage is provided. For achieving this radio advantage, several tacks are followed into the *PHYLAWS* project [29]:

- Use of AN-BF schemes into MIMO architectures, as described above;

- Use of directive antennas, and Use of directive array of antennas (with beamforming technologies);
- Use of Full Duplex radio technologies as described in [43];
- Secure pairing and interrogation technologies such as in system for Identification Friend or Foe. A particular key-free application of such a technology is developed and studied into [34] for public Radio Access Technologies. It is based on low power self-interfered signals (named Tag Signals -TS) and on Interrogation and Acknowledgment Sequences (IAS) supported by these Tag Signals. Very early in the radio access, IAS achieves the security pairing of Alice's and Bob's devices, then provides dual sense TS with a controlled radio advantage. Then secret codes can be applied to these TSs in order to achieved subscriber identity authentication and further negotiation of the communications services without any disclosure risk of subscriber private data on the physical layer.

As soon a slight Radio Advantage is achieved, the results provided above prove that the proposed secrecy coding schemes are efficient.

- The provided secrecy rate is significant (as shown table 1.1 and figure 1.3), even if they remain sub-optimal when compared to theoretical results in ideal case without any constraint on code length and complexity.
- Realistic constraints apply to code length and computation operations that make the technique fully compatible with existing wireless standards.
- The simulation of LTE links (paragraph 1.3.4) and the experimental WiFi results in real field (paragraph 1.3.5) give the feasibility proof of the technique and show that it can be readily implemented in existing wireless MIMO or MISO communication systems that propose Beam Forming services (such as in WLAN 802.11ac, LTE and for emerging 5G standards that would involve massive MIMO technologies):
  - the AN-BF scheme being activated, only minor modifications of the software architecture of the nodes and terminals are required for the implementation of the secrecy coding scheme
  - all modifications are only located at the coding stage and remain transparent for upper protocol layers.

Besides, AN and BF Schemes, we can be confident that same kind of simplified implantation architecture of secret codes schemes should apply to most of "Radio Advantage technologies":

- MIMO and massive MIMO architectures (evolution of existing standard towards usages for Internet of Things, for public safety applications; new WLAN standards and new radio-cellular standards)
- Directive antenna patterns, and especially
  - Microwave links and satellite links in C band (4 to 8 GHz) and in upper bands

  - Many of automatic radio-command of planes and of un-manned aircraft transport vehicles in C band that should be deployed in the future Airborne Traffic Control (ATC) standards and systems [44].
- Full Duplex technologies, when they will be mature and deployed in radio networks [43].

Finally, secrecy coding appears to be an accessible technology to implant in radio-communications systems once a radio advantage is established. SC can apply at numerous stages of the radio protocol :

- First, to enhance the weakly secure transmission of signaling and access messages (use of clear text) that exist in public radio cellular networks and in wireless access networks of nowadays .
- Then, to limit the disclosure risk of subscriber and network parameters that are relevant to identification, authentication and ciphering procedures.
- Finally, to complete the protection of on-going communication by adding a security protection at the physical layer in addition to the traditional cipher schemes of the user data stream.

1.5 Bibliography

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

[2] R. Gallager, "Low density parity check codes," Ph.D. dissertation, MIT Press, Cambridge, 1963.

[3] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, 1st ed. New York, NY, USA: Cambridge University Press, 2011.

[5] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] A. T. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy for erasure wiretap channels," in *Information Theory Workshop (ITW), 2010 IEEE*, Dublin, Ireland, Aug. 2010, pp. 1–5.

[7] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[8] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth ldpc codes," *IEEE*

Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 585–594, Sept. 2011.

[9] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1048–1064, Feb. 2013.

[10] T. Richardson and R. Urbanke, *Modern Coding Theory*. New York, NY, USA: Cambridge University Press, 2008.

[11] S. Kudekar, T. Richardson, and R. L. Urbanke, "Spatially coupled ensembles universally achieve capacity under belief propagation," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 7761–7813, Dec. 2013.

[12] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, St. Petersburg, Russia, July 2011, pp. 2393–2397.

[13] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B. J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, Sept. 2011.

[14] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, no. 8, pp. 752–754, Aug. 2010.

[15] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Information Theory Workshop (ITW), 2010 IEEE*, Dublin, Ireland, Aug. 2010, pp. 1–5.

[16] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, Oct. 2012.

[17] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[18] E. Şaşoğlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, Istanbul, Turkey, July 2013, pp. 1117–1121.

[19] D. Sutter, J. M. Renes, and R. Renner, "Efficient one-way secret-key agreement and private channel coding via polarization," April 2013. [Online]. Available: https://arxiv.org/abs/1304.3658

[20] T. Gulchu and A. Barg, "Achieving secrecy capacity of the general wiretap channel and broadcast channel with a confidential component," Nov 2016. [Online]. Available: https://arxiv.org/abs/1410.3422

[21] Y.-P. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 2, pp. 278–291, Feb. 2016.

[22] C. Ling, L. Luzzi, J. C. Belfiore, and D. Stehl, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[23] F. Oggier, P. Sol, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," Mar. 2011. [Online]. Available: http://arxiv.org/abs/1103.4086

[24] A. M. Ernvall-Hytönen and C. Hollanti, "On the eavesdropper's correct decision in Gaussian and fading wiretap channels using lattice codes," in *Information Theory Workshop (ITW), 2011 IEEE*, Paraty, Brazil, Oct. 2011, pp. 210–214.

[25] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*. New York: Springer, 1993.

[26] G. D. Forney Jr., M. Trott, and S.-Y. Chung, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 820–850, May 2000.

[27] C. Ling and J. Belfiore, "Achieving AWGN channel capacity with lattice Gaussian coding," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 5918–5929, Oct. 2014.

[28] Y. Yan, L. Liu, C. Ling, and X. Wu, "Construction of capacity-achieving lattice codes: Polar lattices," Nov. 2014. [Online]. Available: http://arxiv.org/abs/1411.0187

[29] J. C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *Information Theory and its Applications (ISITA), 2010 International Symposium on*, Oct. 2010, pp. 174–178.

[30] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.

[31] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Transactions on Information Theory*, vol. 48, no. 7, pp. 1804–1824, July 2002.

[32] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 744–765, March 1998.

[33] N. R. Goodman, "Statistical analysis based on a certain multivariate complex Gaussian distribution (an introduction)," *Ann. Math. Statist.*, vol. 34, no. 1, pp. 152–177, 03 1963. [Online]. Available: http://dx.doi.org/10.1214/aoms/1177704250

[34] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation," *PHYCOM: Physical Communication*, vol. 4, no. 4, pp. 313–321, 2011.

[35] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Security and Privacy (SP), 2013 IEEE Symposium on*, May 2013, pp. 160–173.

[36] "PHYLAWS," http://www.Phylaws-ict.org.

[37] E. Arikan, "A performance comparison of polar codes and reed-muller codes," *IEEE Communications Letters*, vol. 12, no. 6, pp. 447–449, June 2008.

[38] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2213–2226, May 2015.

[39] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "Llr-based successive cancellation list decoding of polar codes," *IEEE Transactions on Signal Processing*, vol. 63, no. 19, pp. 5165–5179, Oct 2015.

[40] C. Mehlfuehrer, J. C. Ikuno, M. Simko, S. S, M. Wrulich, and M. Rupp, "The vienna lte simulators - enabling reproducibility in wireless communications research," *EURASIP Journal on Advances in Signal Processing*, vol. 21, 2011.

[41] S. Jaeckel, L. Raschkowski, K. Brner, , and L. Thiele, "Quadriga: A 3-d multicell channel model with time evolution for enabling virtual field trials," *IEEE Trans. Antennas Propag*, vol. 62, pp. 3242–3256, 2014.

[42] "Winner II channel models," https://www.ist-winner.org/WINNER2-Deliverables/D1.1.2v1.1.pdf.

[43] A. V. V. Z. Zhang, K. Long and L. Hanzo, "Full-Duplex wireless communications: Challenges, solutions and future research directions," Proceedings of the IEEE, to appear.

[44] "SESAR," http://www.sesarju.eu/.