# Orthogonal Signalling in the Gaussian Wiretap Channel in the Wideband Regime

K. Zhang , M. R. D. Rodrigues
Instituto de Telecomunicações
Universidade do Porto, Portugal
{kezhang,mrodrigues}@dcc.fc.up.pt

M. Z. Ahmed, M. Tomlinson
University of Plymouth
United Kingdom
{M.Ahmed,M.Tomlinson}@plymouth.ac.uk

F. Cercas
Instituto de Telecomunicações
ISCTE-IUL, Portugal
francisco.cercas@iscte.pt

***Abstract*—We consider communication between a legitimate transmitter and a legitimate receiver in the presence of an eavesdropper in the conventional Gaussian wiretap channel setting. Based on Wyner's coding scheme, we show that a code construction using orthogonal codewords can achieve the secrecy capacity of the Gaussian wiretap channel in the wideband regime. This is illustrated through analysis of the error probability between the legitimate parties and the eavesdropper equivocation rate, as well as various simulation results.**

## I. Introduction

The wiretap channel, which was introduced by Wyner [1], is a basic physical–layer model that captures the essence of communication security. In this model, a transmitter wishes to send confidential information to a legitimate receiver in the presence of an eavesdropper. Wyner characterized the rate-equivocation region of the degraded wiretap channel as well as its secrecy capacity.

A number of attempts have been made in designing coding schemes for secure communication over wiretap channels. For example, Liu *et al.* [2] propose the use of secure nested coding schemes for secure communication over a type II Gaussian wiretap channel, based on cosets of a good code sequence or cosets of the dual of a good code sequence. Belfiore and Oggier [3] propose a wiretap lattice code in additive white Gaussian noise channel. Other coding schemes for wiretap channels exploit low-density parity-check (LDPC) codes [4] or polar codes [5], [6].

This paper focus on secure communication over degraded Gaussian wiretap channels in the wideband regime, which has been studied in detail in [7] In particular, by capitalizing on Wyner's code construction, the objective is to show that an orthogonal coding scheme is able to achieve the secrecy capacity of the Gaussian wiretap channel in the wideband regime.

## II. The Gaussian Wiretap Channel

We consider the conventional Gaussian wiretap channel, where two legitimate parties, Alice and Bob, communicate in the presence of an eavesdropper, Eve, given by:

$$Y_M(i) = X(i) + N_M(i), \qquad i = 1, \ldots, n \tag{1}$$

$$Y_E(i) = X(i) + N_E(i), \qquad i = 1, \ldots, n \tag{2}$$

where $Y_M(i)$ and $Y_E(i)$ correspond to the main channel and the eavesdropper channel outputs at time $i$, respectively, $X(i)$ corresponds to the channel input at time $i$, and $N_M(i)$ and $N_E(i)$ are independent and identically distributed (i.i.d.) Gaussian random processes with mean zero and variance $N_M = N_{M0} \cdot B = N$ and $N_E = N_{E0} \cdot B = \frac{1}{\alpha} \cdot N$, respectively, where $N_{M0} = N_0$ and $N_{E0} = \frac{1}{\alpha} \cdot N_0$ are one-sided noise power spectral densities and $B$ is the effective bandwidth of the channel. In particular, we assume that $0 \leq \alpha \leq 1$.

We denote for simplicity the set of channel inputs (the transmit codeword) by $\mathbf{X} = [X(1)\ X(2)\ \cdots\ X(n)]$, the set of channel outputs (the receive codewords) by $\mathbf{Y} = [Y(1)\ Y(2)\ \cdots\ Y(n)]$, and the set of noise values by $\mathbf{N} = [N(1)\ N(2)\ \cdots\ N(n)]$.[1] We also assume the average power constraint:

$$\frac{1}{n} \sum_{i=1}^{n} |X(i)|^2 \leq \mathsf{P} \tag{3}$$

The legitimate transmitter, Alice, wishes to convey a (uniformly distributed) message $W \in \{1, 2, \ldots, 2^{nR}\}$ to the legitimate receiver, Bob, where $R$ corresponds to the information rate in bits per channel use. The legitimate transmitter-receiver pair use an $(2^{nR}, n)$ code (assumed to be known also to the eavesdropper), a stochastic encoding function that maps the message $W$ into a transmit codeword $\mathbf{X} = [X(1)\ X(2)\ \cdots\ X(n)]$, and a decoding function that maps the receive codeword $\mathbf{Y}_M = [Y_M(1)\ Y_M(2)\ \cdots\ Y_M(n)]$ into the message estimate $\hat{W}$. The average (message) error probability of the $(2^{nR}, n)$ code is

$$P_e = \frac{1}{2^{nR}} \sum_{W} \Pr(\hat{W} \neq W | W) \tag{4}$$

Define the eavesdropper equivocation rate as follows:

$$R_e = \frac{1}{n} \cdot \mathsf{H}(W | \mathbf{Y}_E) \tag{5}$$

where $\mathsf{H}(\cdot|\cdot)$ denotes conditional entropy. Then, the information rate-equivocation rate pair $(R', R'_e)$ is achievable if for all $\epsilon > 0$ there exists a sequence of $(2^{nR}, n)$ codes such that $R \geq R' - \epsilon$, $R_e \geq R'_e - \epsilon$, and $P_e \leq \epsilon$. The perfect secrecy

[1] We use subscripts to indicate whether the vector $\mathbf{Y}$ and the vector $\mathbf{N}$ refer to the main or the eavesdropper channel.

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

rate $R_s$ is achievable if for all $\epsilon > 0$ there exists a sequence of $(2^{nR}, n)$ codes such that $R \geq R_s - \epsilon$, $R_e \geq R_s - \epsilon$, and $P_e \leq \epsilon$. The secrecy capacity $C_s$ of the Gaussian wiretap channel, which corresponds to the supremum of achievable perfect secrecy rate, is given by:

$$C_s = \sup_{p_X(x):\ \mathbb{E}\{|X|^2\} \leq \mathsf{P}} \mathsf{I}(X; Y_M) - \mathsf{I}(X; Y_E) \tag{6}$$

where $p_X(x)$ denotes the probability distribution of the random variable $X$ and $\mathsf{I}(X;Y)$ denotes the mutual information between the input random variable $X$ and the output random variable $Y$ of the Gaussian channels.

The secrecy capacity, which in the degraded Gaussian wiretap channel is achieved by circularly symmetric complex Gaussian inputs, admits the closed form expression [8]:

$$C_s = [C_M - C_E]^+ = \left[\log_2\left(1 + \frac{\mathsf{P}}{N}\right) - \log_2\left(1 + \alpha \cdot \frac{\mathsf{P}}{N}\right)\right]^+ \tag{7}$$

where $[x]^+ = \max(0, x)$, $C_M = \log_2(1 + \mathsf{P}/N)$ is the capacity of the main channel and $C_E = \log_2(1 + \alpha \cdot \mathsf{P}/N)$ is the capacity of the eavesdropper channel.

### A. Wyner's Coding Scheme

It is particularly enlightening to review briefly the structure of the secrecy capacity achieving coding scheme put forth in [1]. The scheme achieves the reliability and security objectives by incorporating redundancy as well as randomness. In particular, the coding scheme, and the encoding and decoding procedure operate as follows:

- *Codebook*: The codebook $\mathcal{C}$ is composed of a number of equal size sub-codebooks $\mathcal{C}_1, \ldots, \mathcal{C}_{N_g}$. The number of sub-codebooks is $N_g = 2^{nC_s} = 2^{n(C_M - C_E)}$. The total number of codewords in the codebook is $N_c = 2^{nC_M}$ and the total number of codewords in each sub-codebook is $N_{c/g} = 2^{nC_E}$.
- *Encoding*: The transmitter maps the message $W$ into a randomly chosen codeword from sub-codebook $\mathcal{C}_W$. This codeword is transmitted over the channel.
- *Decoding*: The legitimate receiver can successfully decode over the codebook $\mathcal{C}$, but the eavesdropper receiver can not. This ensures reliability and perfect secrecy.

Wyner's coding construction, which revolves around the notion of stochastic encoding, suggests a basic structure to design secrecy capacity achieving codes for reliable and secure communication over the wiretap channel.

## III. The Gaussian Wiretap Channel in the Wideband Regime

### A. Tradeoff $C_s$ vs. $\xi_b/N_0$ in the Wideband Regime

We adopt the tradeoff between the secrecy capacity $C_s$ and the ratio between the energy per bit to the one-sided noise spectral density $\xi_b/N_0$, which mirrors the tradeoff between bandwidth and power, to characterize the secrecy capacity of the Gaussian wiretap channel. Such a characterization is particularly important in the wideband regime, in order to capture the interplay between the notions of power, bandwidth and rate [9]. In view of the fact that $\mathsf{P} = RB\xi_b$, the secrecy capacity in (7) is also given by:

$$C_s = \log_2\left(1 + \frac{\xi_b}{N_0} \cdot R\right) - \log_2\left(1 + \alpha \cdot \frac{\xi_b}{N_0} \cdot R\right) \tag{8}$$

for $0 \leq \alpha \leq 1$, so that, by assuming that the communication rate is equal to the highest possible secrecy rate, i.e., $R = C_s$, one obtains immediately the tradeoff $C_s$ *vs.* $\xi_b/N_0$ as follows:

$$\frac{\xi_b}{N_0} = \frac{2^{\ C_s} - 1}{C_s} \cdot \frac{1}{\left(1 - \alpha \cdot 2^{\ C_s}\right)} \tag{9}$$

Figure 1 shows the tradeoff between $C_s$ and $\xi_b/N_0$ for various values of $\alpha \in [0,1]$. The figure portrays well the price of secrecy in the sense that the energy required to achieve a certain secrecy capacity is higher for a wiretap channel ($\alpha > 0$) than for the standard Gaussian channel ($\alpha = 0$). In particular, the higher the value of $\alpha$ the higher the value of $\xi_b/N_0$ required to achieve a target $C_s$.

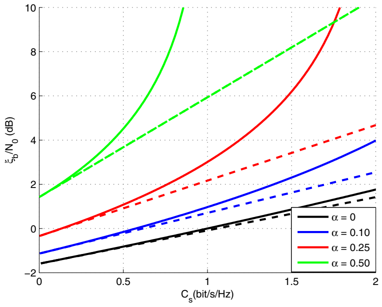

Figure 1. Tradeoff between $C_s$ and $\xi_b/N_0$ for various values of $\alpha$. Solid lines represent the true curve. Dashed lines represent the affine expansion.

Of particular relevance is also the characterization of the tradeoff between $C_s$ and $\xi_b/N_0$ in the wideband regime, where $R \to 0$. The appropriate characterization expands the secrecy capacity as follows [7], [9]:

$$C_s = \mathcal{S}_0 \cdot \left(\frac{\frac{\xi_b}{N_0}\big|_{\mathsf{dB}}}{3\ \mathsf{dB}} - \frac{\frac{\xi_b}{N_0}_{\min}\big|_{\mathsf{dB}}}{3\ \mathsf{dB}}\right) + \mathsf{o}\left(\frac{\xi_b}{N_0}\bigg|_{\mathsf{dB}} - \frac{\xi_b}{N_0}_{\min}\bigg|_{\mathsf{dB}}\right) \tag{10}$$

where $\frac{\xi_b}{N_0}\big|_{\mathsf{dB}}$ is the (transmitted) energy per information bit $\frac{\xi_b}{N_0}$ in dB, $\frac{\xi_b}{N_0}_{\min}\big|_{\mathsf{dB}}$ is the minimum (transmitted) energy per information bit $\frac{\xi_b}{N_0}_{\min}$ required for reliable and secure communication in dB and $\mathcal{S}_0$ is the slope therein in bit/s/Hz/(3 dB).

The two fundamental wideband performance measures, $\frac{\xi_b}{N_0}_{\min}$ and $\mathcal{S}_0$, can be obtained directly from (9), as follows:

$$\frac{\xi_b}{N_0}_{\min} = \lim_{C_s \to 0} \frac{2^{\ C_s} - 1}{C_s} \cdot \frac{1}{(1 - 2^{\ C_s} \cdot \alpha)} = \frac{\ln 2}{1 - \alpha} \tag{11}$$

$$\mathcal{S}_0 = \lim_{C_s \to 0} \frac{1}{\frac{\mathsf{d}}{\mathsf{d}C_s} 10 \log_{10} \frac{\xi_b}{N_0}(C_s)} \cdot 10 \log_{10} 2 = 2 \cdot \frac{1 - \alpha}{1 + \alpha} \tag{12}$$

Note that when $\alpha = 1$ then $\frac{\xi_b}{N_0}_{\text{min}} = +\infty$ and $\mathcal{S}_0 = 0$, so that, as expected, secure communication is not possible; on the other hand, when $\alpha = 0$ the quantities $\frac{\xi_b}{N_0}_{\text{min}}$ and $\mathcal{S}_0$ reduce to the corresponding wideband measures of the standard Gaussian channel. The affine expansions are also depicted in Figure 1, which provides a reasonable approximation in the wideband regime. We use the affine expansions as a means to study secrecy capacity achieving coding schemes in the wideband regime.

Sections IV and V demonstrate through analysis and simulation that orthogonal codes achieve the secrecy capacity in the wideband regime, by showing that as $\frac{\xi_b}{N_0}\big|_{\text{dB}} \to \frac{\xi_b}{N_0}_{\text{min}}\big|_{\text{dB}}$ then it is possible to communicate at a rate $R = C_s$ (with $C_s \to 0$) with $P_e \to 0$ and $R_e \to R$. It will be instructive though to re-examine beforehand the structure of Wyner's coding scheme in the wideband regime.

### B. *Wyner's Coding Scheme in the Wideband Regime*

We are interested in communication in the wideband regime at a rate $R = C_s$ with $\frac{\xi_b}{N_0}\big|_{\text{dB}} \to \frac{\xi_b}{N_0}_{\text{min}}\big|_{\text{dB}}$. Let us write:

$$\frac{\xi_b}{N_0}\bigg|_{\text{dB}} = \frac{\xi_b}{N_0}_{\text{min}}\bigg|_{\text{dB}} + \Delta|_{\text{dB}} \tag{13}$$

Therefore, as $\Delta\big|_{\text{dB}} \to 0$ the secrecy capacity in (10) can be written as follows:

$$C_s = \mathcal{S}_0 \cdot \frac{\Delta|_{\text{dB}}}{3\text{ dB}} + \mathsf{o}\left(\Delta|_{\text{dB}}\right) \tag{14}$$

As $\Delta\big|_{\text{dB}} \to 0$ the capacities of the main and wiretap channel also admit the expansions:

$$C_M = \frac{1}{\ln 2} \cdot \mathcal{S}_0 \cdot \frac{\Delta|_{\text{dB}}}{3\text{ dB}} \cdot \frac{\xi_b}{N_0}_{\text{min}} + \mathsf{o}\left(\Delta\big|_{\text{dB}}\right) \tag{15}$$

$$C_E = \frac{\alpha}{\ln 2} \cdot \mathcal{S}_0 \cdot \frac{\Delta|_{\text{dB}}}{3\text{ dB}} \cdot \frac{\xi_b}{N_0}_{\text{min}} + \mathsf{o}\left(\Delta\big|_{\text{dB}}\right) \tag{16}$$

The structure of Wyner's coding scheme as $\frac{\xi_b}{N_0}\big|_{\text{dB}} \to \frac{\xi_b}{N_0}_{\text{min}}\big|_{\text{dB}}$ follows from the expansions in (14), (15) and (16). In particular, the total number of sub-codebooks as $\Delta\big|_{\text{dB}} \to 0$ is given by:

$$N_g = 2^{nC_s} = 2^{n\cdot\mathcal{S}_0\cdot\frac{\Delta|_{\text{dB}}}{3\text{ dB}}+\mathsf{o}(\Delta|_{\text{dB}})} \approx 2^{n\cdot\mathcal{S}_0\cdot\frac{\Delta|_{\text{dB}}}{3\text{ dB}}} \tag{17}$$

The total number of codewords in the codebook and the total number of codewords per sub-codebook as $\Delta\big|_{\text{dB}} \to 0$ are given by:

$$N_c = 2^{nC_M} = 2^{n\cdot\frac{1}{\ln 2}\cdot\mathcal{S}_0\cdot\frac{\Delta|_{\text{dB}}}{3\text{ dB}}\cdot\frac{\xi_b}{N_0}_{\text{min}}+\mathsf{o}(\Delta|_{\text{dB}})} \approx N_g^{\frac{1}{1-\alpha}} \tag{18}$$

$$N_{c/g} = 2^{nC_E} = 2^{n\cdot\frac{\alpha}{\ln 2}\cdot\mathcal{S}_0\cdot\frac{\Delta|_{\text{dB}}}{3\text{ dB}}\cdot\frac{\xi_b}{N_0}_{\text{min}}+\mathsf{o}(\Delta|_{\text{dB}})} \approx N_g^{\frac{\alpha}{1-\alpha}} \tag{19}$$

The relations in (14), (18) and (19) are the basis of the construction of the orthogonal coding scheme for reliable and secure communications in the wideband regime as $\frac{\xi_b}{N_0}\big|_{\text{dB}} \to \frac{\xi_b}{N_0}_{\text{min}}\big|_{\text{dB}}$.

## IV. Orthogonal Codes for Secure Communication in the Wideband Regime

### A. *Code Construction*

We use $n$ orthogonal codewords with length $n$ and with average power $\mathsf{P}$ to construct the coding scheme:

$$\begin{aligned}
\mathbf{X}_1 &= \left[\sqrt{n\mathsf{P}}\ 0\ \cdots\ 0\ 0\right] \\
\mathbf{X}_2 &= \left[0\ \sqrt{n\mathsf{P}}\ 0\ \cdots\ 0\right] \\
&\ \ \vdots \\
\mathbf{X}_n &= \left[0\ 0\ \cdots\ 0\ \sqrt{n\mathsf{P}}\right]
\end{aligned}$$

Based on Wyner's code construction, we divide the set of codewords – the codebook $\mathcal{C}$ – into several equal size sub-sets of codewords – the sub-codebooks $\mathcal{C}_1, \mathcal{C}_2 \ldots, \mathcal{C}_{N_g}$. Sub-codebook $\mathcal{C}_1$ consists of orthogonal codewords $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_{N_{c/g}}$; sub-codebook $\mathcal{C}_2$ consists of orthogonal codewords $\mathbf{X}_{N_{c/g}+1}, \mathbf{X}_{N_{c/g}+2}, \ldots, \mathbf{X}_{2\cdot N_{c/g}}$; etc. Message $W = 1$ is mapped with equal probability to any of the codewords in sub-codebook $\mathcal{C}_1$; message $W = 2$ is mapped with equal probability to any of the codewords in sub-codebook $\mathcal{C}_2$; etc.

In the wideband regime as $\frac{\xi_b}{N_0}\big|_{\text{dB}} \to \frac{\xi_b}{N_0}_{\text{min}}\big|_{\text{dB}}$, the total number of codewords in the codebook, the total number of codewords per sub-codebook, and the number of sub-codebooks, obey the relations put forth in (14), (18) and (19). It is also important to note that due to the orthogonality constraint the total number of codewords is equal to the length of the codewords, i.e., $N_c = n$.

It is also possible to show that communication in the wideband regime at a rate $R = C_s$ with $\frac{\xi_b}{N_0}\big|_{\text{dB}} \to \frac{\xi_b}{N_0}_{\text{min}}\big|_{\text{dB}}$, in view of (14), (18) and (19), requires orthogonal codewords with length $n$ such that:

$$\frac{1}{n} \cdot \log_2 n \approx \frac{1}{1-\alpha} \cdot \mathcal{S}_0 \cdot \frac{\Delta|_{\text{dB}}}{3\text{ dB}} \tag{20}$$

This implies, as expected, that as $\frac{\xi_b}{N_0}\big|_{\text{dB}} \to \frac{\xi_b}{N_0}_{\text{min}}\big|_{\text{dB}}$ then $n \to \infty$.

### B. *Error Probability Analysis*

We analyze the error probability between the legitimate transmitter and the legitimate receiver, by assuming that the receiver is equipped with the optimal detector for a set of orthogonal codewords. The optimal detector selects the codeword that leads to the largest cross-correlation between the receive codeword and each of the possible transmit codewords, i.e.,

$$\hat{\mathbf{X}} = \arg \max_{\mathbf{X} \in \{\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_n\}} C(\mathbf{X}, \mathbf{Y}_M) \tag{21}$$

where

$$C(\mathbf{X}, \mathbf{Y}_M) = \sum_{i=1}^{n} \mathsf{Re}\left\{\mathbf{Y}_M(i)\mathbf{X}(i)\right\} \tag{22}$$

Due to the nature of the encoding and decoding process, where at the transmitter the original message $W$ is mapped randomly to a codeword within sub-codebook $\mathcal{C}_W$ and at the receiver a codeword estimate within sub-codebook $\mathcal{C}_{\hat{W}}$ is mapped into the message $\hat{W}$, an error occurs when the sub-codebook of the codeword estimate differs from the sub-codebook of the original codeword. The error probability between the original message at the legitimate transmitter and the estimate of the message at the legitimate receiver can then be expressed as follows:

$$P_e = \Pr\left(e\right) = \frac{1}{n}\sum_{i=1}^{n}\Pr\left(e|\mathbf{X}=\mathbf{X}_i\right) \tag{23}$$

where $e$ is the error, and the conditional error probabilities, which are equal due to symmetry considerations, can be expressed as follows:

$$\Pr(e|\mathbf{X}=\mathbf{X}_1)=\Pr\left(\hat{\mathbf{X}}\neq\mathbf{X}_1\wedge\cdots\wedge\hat{\mathbf{X}}\neq\mathbf{X}_{N_{c/g}}|\mathbf{X}=\mathbf{X}_1\right) \tag{24}$$

Let us now note that:

$$\Pr\left(\hat{\mathbf{X}}\neq\mathbf{X}_1\wedge\cdots\wedge\hat{\mathbf{X}}\neq\mathbf{X}_{N_{c/g}}|\mathbf{X}=\mathbf{X}_1\right) \tag{25}$$

$$= 1-\Pr\left(\hat{\mathbf{X}}=\mathbf{X}_1\vee\cdots\vee\hat{\mathbf{X}}=\mathbf{X}_{N_{c/g}}|\mathbf{X}=\mathbf{X}_1\right) \tag{26}$$

$$\leq 1-\Pr\left(\hat{\mathbf{X}}=\mathbf{X}_j|\mathbf{X}=\mathbf{X}_1\right) \tag{27}$$

for any $j=1,\ldots,N_{c/g}$. Consequently, the error probability can be upper bounded as follows:

$$P_e \leq 1-\Pr\left(\hat{\mathbf{X}}=\mathbf{X}_j|\mathbf{X}=\mathbf{X}_1\right) \tag{28}$$

for any $j=1,\ldots,N_{c/g}$.

The probability in (28) can be further upper bounded by using the techniques in [10], which leads to the upper bound to the probability of error given by:

$$P_e \leq \begin{cases} 2e^{-k_1\left(\frac{n\mathsf{P}}{\log_2 n}\cdot\frac{1}{N}-2\ln 2\right)/2}, & \ln n \leq \frac{n\mathsf{P}}{4N} \\ 2e^{-k_1\left(\sqrt{\frac{n\mathsf{P}}{\log_2 n}\cdot\frac{1}{N}}-\sqrt{\ln 2}\right)^2}, & \frac{n\mathsf{P}}{4N} \leq \ln n \leq \frac{n\mathsf{P}}{N} \end{cases} \tag{29}$$

where $k_1=\log_2 n$. Note that the first upper bound is loose for large values of $n$, whereas the second upper bound is tight for large values of $n$.

It follows immediately that as $n\rightarrow\infty$ then $P_e\rightarrow 0$ provided that:

$$\frac{n\mathsf{P}}{\log_2 n}\cdot\frac{1}{N} > \ln 2 \tag{30}$$

or, using the fact that $\mathsf{P}=RB\xi_b$, $N=N_0B$ and the relations in (18) and (19), provided that:

$$\frac{\xi_b}{N_0} > \frac{\ln 2}{1-\alpha} = \frac{\xi_b}{N_{0\,\mathrm{min}}} \tag{31}$$

### *C. Equivocation Analysis*

We analyze the eavesdropper equivocation to determine its uncertainty about the message. Let us determine a lower bound to the eavesdropper equivocation as follows:

$$\begin{aligned}\mathsf{H}\left(W|\mathbf{Y}_E\right) &= \mathsf{H}\left(W,\mathbf{Y}_E\right)-\mathsf{H}\left(\mathbf{Y}_E\right)\\ &= \mathsf{H}\left(W,\mathbf{X},\mathbf{Y}_E\right)-\mathsf{H}\left(\mathbf{X}|W,\mathbf{Y}_E\right)-\mathsf{H}\left(\mathbf{Y}_E\right)\\ &= \mathsf{H}\left(\mathbf{X}\right)+\mathsf{H}\left(\mathbf{Y}_E|\mathbf{X}\right)+\mathsf{H}\left(W|\mathbf{X},\mathbf{Y}_E\right)\\ &\quad -\mathsf{H}\left(\mathbf{X}|W,\mathbf{Y}_E\right)-\mathsf{H}\left(\mathbf{Y}_E\right)\\ &\geq \mathsf{H}\left(\mathbf{X}\right)-\mathsf{H}\left(\mathbf{X}|\mathbf{Y}_M\right)-\mathsf{H}\left(\mathbf{Y}_E\right)+\mathsf{H}\left(\mathbf{Y}_E|\mathbf{X}\right)\\ &\quad -\mathsf{H}\left(\mathbf{X}|W,\mathbf{Y}_E\right)\\ &= \mathsf{I}\left(\mathbf{X};\mathbf{Y}_M\right)-\mathsf{I}\left(\mathbf{X};\mathbf{Y}_E\right)-\mathsf{H}\left(\mathbf{X}|W,\mathbf{Y}_E\right)\end{aligned} \tag{32}$$

Now, it is possible to show that in the wideband regime the mutual information between the input and output of the main channel and the mutual information between the input and the output of the eavesdropper channel for the orthogonal code construction tend to:

$$\mathsf{I}\left(\mathbf{X};\mathbf{Y}_M\right) \approx \log_2 N_g\cdot\frac{\xi_b}{N_0}\cdot\frac{1}{\ln 2} \tag{33}$$

$$\mathsf{I}\left(\mathbf{X};\mathbf{Y}_E\right) \approx \log_2 N_g\cdot\frac{\xi_b}{N_0}\cdot\frac{1}{\ln 2}\cdot\alpha \tag{34}$$

so that the difference tends to:

$$\mathsf{I}\left(\mathbf{X};\mathbf{Y}_M\right)-\mathsf{I}\left(\mathbf{X};\mathbf{Y}_E\right)\approx\log_2 N_g\cdot\frac{\xi_b}{N_0}\cdot\frac{1}{\ln 2}\cdot(1-\alpha) \tag{35}$$

It is also possible to show, by using Fano's inequality, that:

$$\mathsf{H}\left(\mathbf{X}|W,\mathbf{Y}_E\right) \leq 1+\Pr\left(\hat{\mathbf{X}}\neq\mathbf{X}|W\right)\cdot\log_2 N_{c/g} \tag{36}$$

where $\Pr\left(\hat{\mathbf{X}}\neq\mathbf{X}|W\right)$ represents the probability that the codeword estimate is different from the original codeword at the eavesdropper given the message. Consequently, one immediately infers from (35) and (36) that in the wideband regime as $\frac{\xi_b}{N_0}\big|_{\mathrm{dB}}\rightarrow\frac{\xi_b}{N_{0\,\mathrm{min}}}\big|_{\mathrm{dB}}$, which also implies $n\rightarrow\infty$ via (20), the eavesdropper equivocation rate obeys:

$$\frac{1}{n}\cdot\mathsf{H}\left(W|\mathbf{Y}_E\right) \geq \frac{1}{n}\cdot\log_2 N_g-\epsilon = C_s-\epsilon \tag{37}$$

where $\epsilon$ is negligible.

To conclude, we observe that in the wideband regime as $\frac{\xi_b}{N_0}\big|_{\mathrm{dB}}\rightarrow\frac{\xi_b}{N_{0\,\mathrm{min}}}\big|_{\mathrm{dB}}$ the orthogonal code construction defined by (18), (19) and (20) guarantees communication at a rate $R=C_s$ (with $C_s\rightarrow 0$) with perfect reliability and security.

## V. Simulation Results

We provide various simulation results to illustrate the performance of the orthogonal code construction in the Gaussian wiretap channel. Figure 2 plots the (codeword) error probability between the legitimate transmitter and the legitimate receiver *vs.* $\xi_b/N_0$ for various values of $N_g$ with $\alpha=\frac{N_{M_0}}{N_{E_0}}=0.08$. We observe that the higher the value of $N_g$ (and hence $n$) the lower the value of $\xi_b/N_0$ required to achieve a target (message) error probability. In particular, in accordance with the analysis, one would obtain that $P_e\rightarrow 0$ as $N_g\rightarrow\infty$ (and hence $n\rightarrow\infty$) provided that $\frac{\xi_b}{N_0}\geq\frac{\xi_b}{N_{0\,\mathrm{min}}}=\frac{\ln 2}{1-\alpha}=-1.23$ dB. Figure 3 plots the eavesdropper equivocation lower bound using (32) and (36) *vs.* $\xi_b/N_0$ for various values of $N_g$ with $\alpha=\frac{N_{M_0}}{N_{E_0}}=0.08$. In particular, one observes that the eavesdropper equivocation tends to the message entropy in a vicinity of $\frac{\xi_b}{N_0} = \frac{\xi_b}{N_0}_{\text{min}}$ for large values of $N_g$ (and hence $n$) This is further emphasized in Figure 4, which depicts the gap (denoted by $\gamma$) between the message entropy and the eavesdropper equivocation lower bound, normalized to the message entropy.

These simulation results suggest that the orthogonal code construction achieve the secrecy capacity of the Gaussian wiretap channel in the wideband regime as $\frac{\xi_b}{N_0} \to \frac{\xi_b}{N_0}_{\text{min}}$. The price, of course, is reliable and secure communications at a vanishing information rate.

Finally, Table I depicts the tradeoff between rate, reliability and security for $P_e = 10^{-2}$ and $P_e = 10^{-3}$. As expected, as the information rate tends to zero the higher the reliability (i.e. the lower the $\xi_b/N_0$ necessary to attain a target error probability) and the higher the security (i.e. the lower the equivocation upper bound). We also observe that for a certain target information rate the higher the reliability level the lower the security level.

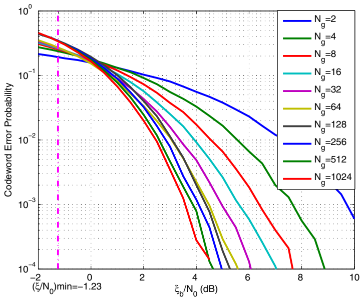

Figure 2. Codeword error probability between the legitimate parties for $\alpha = 0.08$.

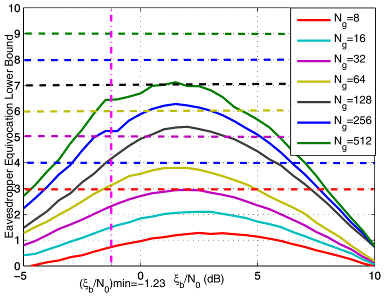

Figure 3. Eavesdropper equivocation lower bound for $\alpha = 0.08$. Solid lines correspond to the equivocation lower bound. Dashed lines correspond to the message entropy.

## VI. Conclusions

We have considered communication in the Gaussian wiretap channel in the wideband regime. In particular, it has been shown by analysis and suggested by simulation that the use of orthogonal codes, which follow a construction *akin* to Wyner's code construction, can achieve the secrecy capacity of the Gaussian wiretap channel in the asymptotic wideband regime, which entails communication at a vanishing rate. The results can also be used to infer the error probability between the legitimate parties or bound the information rate leaked to the eavesdropper due to the use of the orthogonal coding construction in non-asymptotic regimes.

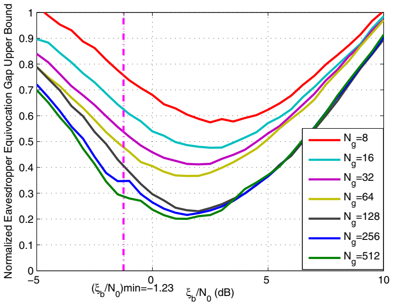

Figure 4. Normalized eavesdropper equivocation gap upper bound $\gamma$ for $\alpha = 0.08$. $\gamma$ is obtained by using the equivocation lower bound in $\frac{\mathsf{H}(W)-\mathsf{H}(W|\mathbf{Y}_E)}{\mathsf{H}(W)}$.

Table I
Tradeoff between rate, reliability and security

| $N_g$ | 8 | 16 | 32 | 64 | 128 | 256 | 512 |
|---:|---:|---:|---:|---:|---:|---:|---:|
| R | 0.375 | 0.250 | 0.156 | 0.094 | 0.055 | 0.031 | 0.018 |
| $\xi_b/N_0$ (dB)@$P_e = 10^{-2}$ | 4.4 | 3.8 | 3.5 | 3.1 | 2.9 | 2.8 | 2.6 |
| $\xi_b/N_0$ (dB)@$P_e = 10^{-3}$ | 6.2 | 5.6 | 4.9 | 4.6 | 4.3 | 4.2 | 4 |
| $\gamma$@$P_e = 10^{-2}$ | 0.6 | 0.51 | 0.45 | 0.4 | 0.25 | 0.24 | 0.22 |
| $\gamma$ @$P_e = 10^{-3}$ | 0.7 | 0.6 | 0.53 | 0.48 | 0.32 | 0.31 | 0.3 |

## VII. Acknowledgment

This work has been supported by Fundação para a Ciêñcia e a Tecnologia through the research project PTDC/EEA-TEL/100854/2008. The authors also would like to acknowledge the FCT PhD fellowship.

## References

[1] A. D. Wyner, The wire-tap channel, *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1367, 1975.

[2] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, Secure nested codes for type II wiretap channels, in *Proc. 2007 IEEE Information Theory Workshop*, Tahoe City, CA, pp. 337-342, Sep. 2007.

[3] J. C. Belfiore and F. Oggier, Secrecy gain: a wiretap lattice code design, *IEEE Information Theory and its Applications*, Taichung, pp. 174-178, Oct.2010.

[4] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin and J-M. Merolla, Application of LDPC codes to the wiretap channel, *IEEE Trans. Inform. Theory*, vol.53, pp.2933-2945, Aug.2007.

[5] H. Mahdavifar and A. Vardy, Achieving the secrecy capacity of wiretap channels using polar codes, in *Proc. 2010 IEEE International Symposium on Information Theory*, Austin, TX, pp. 913-917, Jun.2010.

[6] E. Hof, S. Shamai, Secrecy-achieving polar-coding, *IEEE Information Theory Workshop*, Dublin, Aug.2010 .

[7] M. C. Gursoy, Secure communication in the low-SNR regime: A Characterization of the energy-secrecy tradeoff, *IEEE International Symposium on Information Theory*, Seoul, Korea, pp.2291-2295, Jun.2009.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, The Gaussian wire-tap channel, *IEEE Trans. Inf. Theory*, vol. 24, no.4, pp.451-456, Jul.1978.

[9] S. Verdú, Spectral Efficiency in the Wideband Regime, *IEEE Trans. Inf. Theory*, vol. 48, no.6, pp.1319-1343, Jun.2002.

[10] John G. Proakis, *Digital communications*, Third Edition,1995.