

An Error Probability Approach to MIMO Wiretap Channels

Jean-Claude Belfiore and Frédérique Oggier

Abstract

We consider MIMO (Multiple Input Multiple Output) wiretap channels, where a legitimate transmitter Alice is communicating with a legitimate receiver Bob in the presence of an eavesdropper Eve, and communication is done via MIMO channels. We suppose that Alice's strategy is to use a codebook which has a lattice structure, which then allows her to perform coset encoding. We analyze 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. The Alamouti code is carefully studied as an illustration of the analysis provided.

Index Terms

Code design criterion, Epstein zeta function, Error probability, Fading channels, MIMO channels, Wiretap channels.

I. INTRODUCTION

Wiretap channels were introduced by Wyner [21] in the seventies as broadcast channels, where a legitimate transmitter Alice communicates with a legitimate receiver Bob through a noisy communication channel in the presence of an eavesdropper Eve. They have attracted a regain of interest recently, in particular in the context of physical layer security. We consider MIMO (Multiple Input Multiple Output) wiretap channels, for which the secrecy capacity, that is

Jean-Claude Belfiore is with Telecom ParisTech, CNRS, UMR 5141, France. Frédérique Oggier is with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Email:belfiore@telecom-paristech.fr, frederique@ntu.edu.sg. Part of this work appeared as an invited paper in ICC 2011 [3].

the maximum amount of information that Alice can transmit confidentially to Bob, is known [10], [14], [12]. We consider an alternative approach, which consists of studying the probability that Eve correctly decodes the message meant to Bob, as initiated in [2], [15] for Gaussian channels. An early work by Hero [9] proposed a non-information theoretical approach to secrecy in MIMO channels, where a code design was proposed, based on the assumption that Eve is doing a non-coherent decoding. In [20], the model of wiretap channel is further used to study secret sharing over fast fading MIMO channels.

We consider the case where Alice transmits lattice codes using coset encoding, which requires two nested lattices $\Lambda_e \subset \Lambda_b$, and Alice encodes her data in the coset representatives of Λ_b/Λ_e . Both Bob and Eve try to decode using coset decoding. It was shown in [2] for Gaussian channels 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. The contribution of this work is to 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. More precisely, we prove that to minimize Eve's average probability of correct decoding, a code design is

$$\min_{\Lambda_e} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \frac{1}{\det(\mathbf{X} \mathbf{X}^*)^{n_e + T}}$$

where n_e is Eve's number of antennas, T is the coherence time of the MIMO channel, and \mathbf{x} is the vectorized codeword X . As a corollary, we derive a design criterion for a block fading channels where all numbers of antennas are the same, namely

$$\min_{\Lambda_e} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \frac{1}{(\prod_{i=1}^n \|\mathbf{x}_i\|^2)^{1+T}}$$

which in turn gives a criterion for a fast fading channel:

$$\min_{\Lambda_e} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \frac{1}{(\prod_{i=1}^n |x_i|^2)^2}.$$

This paper is organized as follows: in Section II, we recall how Eve's probability of correct decision is derived for Gaussian channels, and extend the computation to include the case where low dimensional lattice codes are used. Section III is the chore part of this paper, which contains Eve's probability of correctly decoding the confidential message when her channel from Alice is a MIMO channel. We consequently treat the case of block and fast fading channels in Section IV. The relevance of our approach is illustrated in Section V where the Alamouti code is studied following the newly introduced techniques.

II. GAUSSIAN CHANNELS

We first consider a Gaussian wiretap channel, modeled by

$$\begin{aligned}\mathbf{y} &= \mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathbf{x} + \mathbf{v}_e\end{aligned}\tag{1}$$

over n complex channel uses, where $\mathbf{x} \in \mathbb{C}^n$ is the transmitted signal, $\mathbf{v}_b \in \mathbb{C}^n$ and $\mathbf{v}_e \in \mathbb{C}^n$ denote the Gaussian noise at Bob, respectively Eve's side, both with coefficients which are zero mean, and have respective variance σ_b^2 and σ_e^2 , where σ_e is assumed larger than σ_b . We assume that Alice knows Bob's channel σ_b , and uses $\mathbb{Z}[i]$ -lattice codes, namely $\mathbf{x} \in \Lambda$, where Λ is an m -dimensional complex lattice¹, which can be described by its generator matrix M [5]:

$$\Lambda = \{\mathbf{x} = M\mathbf{u} \mid \mathbf{u} \in \mathbb{Z}[i]^m\},$$

and the columns of M form a linearly independent set of vectors in \mathbb{C}^n (so that $m \leq n$) which form a basis of the lattice.

Alice performs coset encoding [21]: she chooses a lattice Λ_b that she partitions into a union of disjoint cosets $\Lambda_e + \mathbf{c}$, with Λ_e a sublattice of Λ_b and \mathbf{c} an n -dimensional vector which encodes her data. Alice then randomly chooses a random vector $\mathbf{r} \in \Lambda_e$ so that the transmitted lattice point $\mathbf{x} \in \Lambda_b$ is finally

$$\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_e + \mathbf{c}.\tag{2}$$

Why coset encoding is actually beneficial for wiretap lattice codes is illustrated in [15].

¹Note that in the theoretical computer science literature, the dimension of a lattice is defined as the number of rows of M , whereas the rank of a lattice is defined as the number of columns of M .

Recall from [2]² that when $m = n$, the probability P_c of correct decision when doing coset decoding is

$$\begin{aligned} P_c &= \frac{1}{(2\pi\sigma^2)^n} \sum_{\mathbf{t} \in \Lambda_e} \int_{\mathcal{V}(\mathbf{x}+\mathbf{t})} e^{-\|\mathbf{y}-\mathbf{x}\|^2/2\sigma^2} d\mathbf{y} \\ &= \frac{1}{(2\pi\sigma^2)^n} \sum_{\mathbf{t} \in \Lambda_e} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma^2} d\mathbf{y} \end{aligned}$$

where $\mathcal{V}(\Lambda_b)$ denotes the Voronoi region of Λ_b and $\mathbf{u} = \mathbf{y} - \mathbf{x} - \mathbf{t}$. Equality holds because infinite lattice constellations are considered (this gives an upper bound on finite lattice constellations). Since Bob's received vector \mathbf{y} is most likely to lie in the Voronoi region around the transmitted point, the terms corresponding to $\mathbf{t} \neq 0$ are negligible, which yields the well known bound on the probability $P_{c,b}$ of Bob's correct decision:

$$P_{c,b} \leq \frac{1}{(2\pi\sigma_b^2)^n} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}\|^2/2\sigma_b^2} d\mathbf{u}.$$

Regarding the probability $P_{c,e}$ of Eve's correct decision in doing coset decoding, note that

$$\frac{1}{(2\pi\sigma_e^2)^n} \sum_{\mathbf{t} \in \Lambda_e} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2} d\mathbf{y} = \frac{1}{(2\pi\sigma_e^2)^n} \int_{\mathcal{V}(\Lambda_b)} \sum_{\mathbf{t} \in \Lambda_e} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2} d\mathbf{y}$$

and since $\sum_{\mathbf{t} \in \Lambda_e} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_e^2}$ reaches its maximum when $\mathbf{u} \in \Lambda_e$ (see Remark 2 in [11]), we find that

$$P_{c,e} \leq \frac{1}{(2\pi\sigma^2)^n} \sum_{\mathbf{t} \in \Lambda_e} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{t}\|^2/2\sigma^2} d\mathbf{y} = \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^n} \sum_{\mathbf{t} \in \Lambda_e} e^{-\|\mathbf{t}\|^2/2\sigma_e^2},$$

where $\text{vol}(\Lambda_b)$ is defined to be $\sqrt{\det(MM^*)}$. We need to discuss the case where $m < n$ before proceeding. The notation we will use refers to Bob's channel, though the same holds for Eve's.

The decoding rule for a Gaussian channel (1) when $m < n$ is similarly to the case $m = n$ given by

$$\min_{\mathbf{x}} \|\mathbf{y} - \mathbf{x}\|^2,$$

where $\mathbf{y} = \mathbf{x}' + \mathbf{v}_b$ is the noisy message at the receiver when \mathbf{x}' is sent, except that now, $\mathbf{x}' = M\mathbf{u}'$ and $\mathbf{x} = M\mathbf{u}$ where M is an $n \times m$ complex matrix. By performing a QR decomposition of M , we get

$$M = QR = Q \begin{bmatrix} R' \\ \mathbf{0} \end{bmatrix}$$

²A real channel was considered in [2], the extension to the complex case discussed here is immediate.

with R' an upper triangular $m \times m$ matrix, and Q a unitary $n \times n$ matrix, whose Hermitian transpose is denoted by Q^* . Thus

$$\min_{\mathbf{x}} \|\mathbf{y} - \mathbf{x}\|^2 = \min_{\mathbf{u}} \|Q^*(M\mathbf{u}' + \mathbf{v}_b) - Q^*M\mathbf{u}\|^2 = \min_{\mathbf{u}} \|(R\mathbf{u}' + Q^*\mathbf{v}_b) - R\mathbf{u}\|^2$$

that is

$$\min_{\mathbf{u} \in \mathbb{Z}[i]^m} \left\| \begin{bmatrix} R'\mathbf{u}' \\ \mathbf{0} \end{bmatrix} + \mathbf{v}'_b - \begin{bmatrix} R'\mathbf{u} \\ \mathbf{0} \end{bmatrix} \right\|^2$$

where \mathbf{v}'_b is a new noise vector with the same noise statistics as \mathbf{v}_b since Q^* is unitary. It is now clear from the above minimization that

$$\arg \min_{\mathbf{u}} \|\mathbf{y} - M\mathbf{u}\|^2 = \arg \min_{\mathbf{u}} \|R'\mathbf{u}' + \mathbf{v}''_b - R'\mathbf{u}\|^2$$

where \mathbf{v}''_b is the noise vector \mathbf{v}'_b where the last $n-m$ rows have been ignored ($R'\mathbf{u}' + \mathbf{v}''$ is a vector containing the first m elements of $Q^*\mathbf{y}$), and thus the problem of decoding an m -dimensional lattice in an n -dimensional space can be reduced to perform the decoding in an m -dimensional space, showing that what matters is the dimension of the lattice, and not the one of the ambient space. Consequently, we have

$$P_{c,b} = \frac{1}{(2\pi\sigma_b^2)^m} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}\|^2/2\sigma_b^2} d\mathbf{u}, \quad (3)$$

$$P_{c,e} \leq \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^m} \sum_{\mathbf{r} \in \Lambda_e} e^{-\|\mathbf{r}\|^2/2\sigma_e^2}, \quad (4)$$

when Alice sends an m -dimensional lattice (living in an n -dimensional space) to Bob. We are now ready to analyze the MIMO case.

III. THE MIMO CASE

We now consider the case 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:

$$\begin{aligned} Y &= H_b X + V_b \\ Z &= H_e X + V_e, \end{aligned} \quad (5)$$

where the transmitted signal X is a $n_t \times T$ 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 $\Sigma_e = \sigma_{H_e}^2 \mathbf{I}_{n_e}$. As for the Gaussian case (as described in Section II), 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. That $n_e \geq n_t$ might be assumed without loss of generality, since in this case Eve is in a more advantageous situation than if she had less antennas. 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 (5) and obtain

$$\begin{aligned} \text{vec}(Y) &= \text{vec}(H_b X) + \text{vec}(V_b) \\ &= \begin{pmatrix} H_b & & \\ & \ddots & \\ & & H_b \end{pmatrix} \text{vec}(X) + \text{vec}(V_b) \end{aligned} \quad (6)$$

$$\begin{aligned} \text{vec}(Z) &= \text{vec}(H_e X) + \text{vec}(V_e) \\ &= \begin{pmatrix} H_e & & \\ & \ddots & \\ & & H_e \end{pmatrix} \text{vec}(X) + \text{vec}(V_e). \end{aligned} \quad (7)$$

We now interpret the $n_t \times T$ codeword X as coming from a lattice. This is typically the case if X is a space-time code coming from a division algebra [17], or more generally if X is a linear dispersion code as introduced in [8] where Tn_t symbols QAM are linearly encoded via a family of Tn_t dispersion matrices. We write

$$\text{vec}(X) = M_b \mathbf{u}$$

where $\mathbf{u} \in \mathbb{Z}[i]^{Tn_t}$ 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 $\mathbf{x} \in \Lambda_b$, we mean that

$$\mathbf{x} = \text{vec}(X) = M_b \mathbf{u},$$

and similarly for a lattice point $\mathbf{x} \in \Lambda_e$, we have

$$\mathbf{x} = \text{vec}(X) = M_e \mathbf{u}.$$

By setting

$$M_{b,H_b} = \text{diag}(H_b, \dots, H_b) M_b,$$

$$M_{b,H_e} = \text{diag}(H_e, \dots, H_e) M_b$$

we can rewrite (6) and (7) as

$$\begin{aligned} \text{vec}(Y) &= M_{b,H_b} \mathbf{u} + \text{vec}(V_b) \\ \text{vec}(Z) &= M_{b,H_e} \mathbf{u} + \text{vec}(V_e), \end{aligned} \tag{8}$$

where M_{b,H_b} , resp. M_{b,H_e} can be interpreted as the lattice generators of the lattices Λ_{b,H_b} , resp. Λ_{b,H_e} , representing the transmitted lattice seen through the respective receivers' channel, with by definition volume³

$$\begin{aligned} \text{vol}(\Lambda_{b,H_b}) &= |\det(M_{b,H_b} M_{b,H_b}^*)| = |\det(H_b H_b^*)|^T \text{vol}(\Lambda_b) \\ \text{vol}(\Lambda_{b,H_e}) &= |\det(M_{b,H_e} M_{b,H_e}^*)| = |\det(H_e H_e^*)|^T \text{vol}(\Lambda_b). \end{aligned} \tag{9}$$

Similarly, the lattices Λ_{e,H_b} , resp. Λ_{e,H_e} describe the lattices intended to Eve, seen through Bob's, resp. Eve's channel, with respective generator matrix $M_{e,H_b} = \text{diag}(H_b, \dots, H_b) M_e$ and $M_{e,H_e} = \text{diag}(H_e, \dots, H_e) M_e$.

Note that for $\mathbf{r} \in \Lambda_{e,H_e}$, we have

$$\|\mathbf{r}\|^2 = \|\text{diag}(H_e, \dots, H_e) M_e \mathbf{u}\|^2 = \|\text{diag}(H_e, \dots, H_e) \mathbf{x}\|^2 = \|H_e X\|_F^2 \tag{10}$$

where $\|H_e X\|_F^2 = \text{Tr}(H_e X X^* H_e^*)$ is the Frobenius norm, and $\mathbf{x} = \text{vec}(X) \in \Lambda_e$.

For a given realization of the channel matrices H_e and H_b , the channel (8) can be seen as the Gaussian wiretap channel

$$\begin{aligned} \mathbf{y} &= M_{b,H_b} \mathbf{u} + \mathbf{v}_b \\ \mathbf{z} &= M_{b,H_e} \mathbf{u} + \mathbf{v}_e, \end{aligned} \tag{11}$$

where $\mathbf{y} = \text{vec}(Y)$, $\mathbf{z} = \text{vec}(Z)$, $\mathbf{v}_b = \text{vec}(V_b)$, $\mathbf{v}_e = \text{vec}(V_e)$. We now focus on Eve's channel, since we know from [19] how to design a good linear dispersion space-time code, and the

³Note that if Λ has generator matrix M , we define its volume to be $|\det(MM^*)|^{1/2}$ if Λ is real and $\det(MM^*)$ if Λ is complex.

lattice Λ_b is chosen so as to correspond to this space-time code. We know from (4) that Eve's probability of correctly decoding is

$$P_{c,e,H_e} \leq \frac{\text{vol}(\Lambda_{b,H_e})}{(2\pi\sigma_e^2)^{n_t T}} \sum_{\mathbf{r} \in \Lambda_{e,H_e}} e^{-\|\mathbf{r}\|^2/2\sigma_e^2} \quad (12)$$

$$= \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{n_t T}} \det(H_e H_e^*)^T \sum_{\mathbf{x} \in \Lambda_e} e^{-\|H_e \mathbf{x}\|_F^2/2\sigma_e^2} \quad (13)$$

where last equality follows from (9) and (10), with $\mathbf{x} = \text{vec}(X) \in \Lambda_e$. Note that as mentioned at the end of Section II, the exponent of $2\pi\sigma_e^2$ depends on the dimension of the transmitted lattice, which is here $n_t T$.

Using Equation (13), we derive Eve's average probability of correct decision:

$$\begin{aligned} \bar{P}_{c,e} &= \mathbb{E}_{H_e} [P_{c,e,H_e}] \\ &\leq \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{T n_t}} \sum_{\mathbf{x} \in \Lambda_e} \int_{\mathbb{C}^{n_e \times n_t}} \det(H_e H_e^*)^T e^{-\|H_e \mathbf{x}\|_F^2/2\sigma_e^2} \frac{e^{-\frac{1}{2}\text{Tr}(H_e^* \Sigma_e^{-1} H_e)}}{(2\pi)^{n_e n_t} \det(\Sigma_e)^{n_t}} dH_e \\ &= \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{T n_t} (2\pi)^{n_e n_t} \det(\Sigma_e)^{n_t}} \\ &\quad \sum_{\mathbf{x} \in \Lambda_e} \int_{\mathbb{C}^{n_e \times n_t}} \det(H_e H_e^*)^T e^{\frac{-1}{2\sigma_e^2} \text{Tr}(H_e X X^* H_e^*)} e^{-\frac{1}{2} \text{Tr}(H_e^* \Sigma_e^{-1} H_e)} dH_e \\ &= \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{T n_t} (2\pi\sigma_{H_e}^2)^{n_e n_t}} \\ &\quad \sum_{\mathbf{x} \in \Lambda_e} \int_{\mathbb{C}^{n_e \times n_t}} \det(H_e H_e^*)^T e^{-\text{Tr}\left(H_e^* H_e \left[\frac{1}{2\sigma_{H_e}^2} \mathbf{I}_{n_t} + \frac{1}{2\sigma_e^2} X X^*\right]\right)} dH_e. \end{aligned} \quad (14)$$

By setting $W = H_e^* H_e$, we note that the above integral can be rewritten as

$$\int_{W \in \mathcal{D}_W} \left\{ \int_{H_e^* H_e = W} \det(H_e H_e^*)^T e^{-\text{Tr}\left(H_e^* H_e \left[\frac{1}{2\sigma_{H_e}^2} \mathbf{I}_{n_t} + \frac{1}{2\sigma_e^2} X X^*\right]\right)} dH_e \right\} dW, \quad (15)$$

where \mathcal{D}_W is the set of all $n_t \times n_t$ positive definite Hermitian matrices⁴. We have, since we assumed $n_t \leq n_e$, from Theorem 2.1 in [13] (see also [18]), that

$$\begin{aligned} &\int_{H_e^* H_e = W} \det(H_e H_e^*)^T e^{-\text{Tr}\left(H_e^* H_e \left[\frac{1}{2\sigma_{H_e}^2} \mathbf{I}_{n_t} + \frac{1}{2\sigma_e^2} X X^*\right]\right)} dH_e \\ &= \frac{\pi^{n_e n_t}}{\Gamma_{n_t}(n_e)} (\det W)^{n_e - n_t + T} e^{-\text{Tr}\left(W \left[\frac{1}{2\sigma_{H_e}^2} \mathbf{I}_{n_t} + \frac{1}{2\sigma_e^2} X X^*\right]\right)} \end{aligned}$$

⁴Note that W is definite with probability one since H_e has full rank with probability one.

where $\Gamma_{n_t}(n_e)$ is the multivariate gamma function which can be developed as

$$\Gamma_{n_t}(n_e) = \pi^{n_t(n_t-1)/2} \prod_{k=1}^{n_t} \Gamma(n_e - k + 1).$$

Now, Equation (14) becomes

$$\begin{aligned} \bar{P}_{c,e} &\leq \frac{\text{vol}(\Lambda_b) \pi^{n_e n_t}}{\Gamma_{n_t}(n_e) (2\pi\sigma_e^2)^{n_t T} (2\pi\sigma_{H_e}^2)^{n_e n_t}} \sum_{\mathbf{x} \in \Lambda_e} \int_{W \in \mathcal{D}_W} \det(W)^{n_e - n_t + T} e^{-\text{Tr}\left(W \left[\frac{1}{2\sigma_{H_e}^2} \mathbf{I}_{n_t} + \frac{1}{2\sigma_e^2} X X^* \right]\right)} dW \\ &= \frac{\text{vol}(\Lambda_b) \pi^{n_e n_t} \Gamma_{n_t}(n_e + T)}{\Gamma_{n_t}(n_e) (2\pi\sigma_e^2)^{n_t T} (2\pi\sigma_{H_e}^2)^{n_e n_t}} \sum_{\mathbf{x} \in \Lambda_e} \det\left(\frac{1}{2\sigma_{H_e}^2} \mathbf{I}_{n_t} + \frac{1}{2\sigma_e^2} X X^*\right)^{-n_e - T} \end{aligned} \quad (16)$$

where the last equality comes from [6]

$$\int_{\mathcal{D}_W} (\det W)^k \exp\{-\text{Tr}(\Sigma^{-1} W)\} dW = \pi^{\frac{1}{2}p(p-1)} \Gamma(p+k) \cdots \Gamma(1+k) (\det \Sigma)^{p+k}$$

where \mathcal{D}_W is here the set of all $p \times p$ positive definite Hermitian matrices.

We finally obtain that an upper bound on the average probability of correct decoding for Eve is

$$\boxed{\bar{P}_{c,e} \leq C_{\text{MIMO}} \gamma_e^{T n_t} \sum_{\mathbf{x} \in \Lambda_e} \det(\mathbf{I}_{n_t} + \gamma_e X X^*)^{-n_e - T}} \quad (17)$$

where we set $\gamma_e = \frac{\sigma_{H_e}^2}{\sigma_e^2}$ for Eve's SNR, and

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

In order to design a good lattice code for the MIMO wiretap channel, we try to derive a code design criterion from Equation (17):

$$\bar{P}_{c,e} \leq C_{\text{MIMO}} \gamma_e^{T n_t} \left[1 + \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \det(\mathbf{I}_{n_t} + \gamma_e X X^*)^{-n_e - T} \right].$$

We can suppose that the space-time code used to transmit data to Bob is designed according to the so-called ‘‘rank criterion’’ of [19]. This means that, if $X \neq 0$ and $T \geq n_t$ then, $\text{rank}(X) = n_t$. If we assume now that Eve's SNR γ_e is high compared to the minimum distance of Λ_e , or actually design Λ_e that way assuming Alice knows Eve's channel, we get

$$\bar{P}_{c,e} \leq C_{\text{MIMO}} \left[\gamma_e^{T n_t} + \frac{1}{\gamma_e^{n_e n_t}} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \det(X X^*)^{-n_e - T} \right]. \quad (18)$$

We thus conclude that to minimize Eve's average probability of correct decoding, the design criterion is now

$$\min_{\Lambda_e} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \frac{1}{\det(\mathbf{X} \mathbf{X}^*)^{n_e+T}}. \quad (19)$$

Remark 1: We discuss the meaning of the bound in (18). The higher γ_e , the higher should be Eve's probability of correct decoding. The expression in (18) is decreasing as a function of γ_e around the origin, a regime which we do not consider (as we just derived the expression assuming γ_e big enough), and is then indeed increasing elsewhere as expected. The minimum value of this upper bound (computed by taking its derivative) is achieved for

$$\gamma_{e,\min} = \left(\frac{n_e}{T} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \det(\mathbf{X} \mathbf{X}^*)^{-n_e-T} \right)^{\frac{1}{n_t(n_e+T)}}.$$

Remark 2: It is important to notice that the upper bound was computed using an infinite lattice Λ_e . In some rare cases, as for an example in the case of the Alamouti code discussed later on, the bound happens to be finite even though the lattice is not. In general, it is not, in which case the bound refers not to the infinite lattice Λ_e , but instead a finite subset carved from Λ_e via a shaping region. The same holds for the bounds derived below for block and fast fading channels.

IV. BLOCK AND FAST FADING CHANNELS

As a corollary of the analysis done for the MIMO case, we consider the particular fading channels where H_b, H_e are diagonal matrices. In this case, setting $n_t = n_b = n_e = n$, the channel (5) can be rewritten as

$$\begin{aligned} Y &= \text{diag}(\mathbf{h}_b)X + V_b \\ Z &= \text{diag}(\mathbf{h}_e)X + V_e, \end{aligned} \quad (20)$$

which corresponds to a block fading channel with n transmit antennas emitting one after the other, coherence time T and

$$\text{diag}(\mathbf{h}_b) = \begin{pmatrix} h_{b,1} & & \\ & \ddots & \\ & & h_{b,n} \end{pmatrix}, \quad \text{diag}(\mathbf{h}_e) = \begin{pmatrix} h_{e,1} & & \\ & \ddots & \\ & & h_{e,n} \end{pmatrix}. \quad (21)$$

However, we cannot use the final result for MIMO channels immediately, since the integral over all positive definite Hermitian matrices does not hold anymore. Moreover, the general expression of (15) does not hold either since it assumes that H_e (here $\text{diag}(\mathbf{h}_e)$) is i.i.d distributed. We thus start from the generic equation (13), which gives, using a polar coordinates change, and the change of variables $u_{e,i} = \rho_{e,i}^2$

$$\begin{aligned}
\bar{P}_{c,e} &\leq \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{nT}(2\pi\sigma_{\mathbf{h}_e}^2)^n} \sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^n \int_{\mathbb{C}} |h_{e,i}|^{2T} e^{-|h_{e,i}|^2 \left[\frac{1}{2\sigma_{\mathbf{h}_e}^2} + \frac{1}{2\sigma_e^2} \|\mathbf{x}_i\|^2 \right]} dh_{e,i} \\
&= \frac{(2\pi)^n \text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{nT}(2\pi\sigma_{\mathbf{h}_e}^2)^n} \sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^n \int_0^\infty \rho_{e,i}^{2T+1} e^{-\rho_{e,i}^2 \left[\frac{1}{2\sigma_{\mathbf{h}_e}^2} + \frac{1}{2\sigma_e^2} \|\mathbf{x}_i\|^2 \right]} d\rho_{e,i} \\
&= \frac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{nT}(2\sigma_{\mathbf{h}_e}^2)^n} \sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^n \int_0^\infty u_{e,i}^T e^{-u_{e,i} \left[\frac{1}{2\sigma_{\mathbf{h}_e}^2} + \frac{1}{2\sigma_e^2} \|\mathbf{x}_i\|^2 \right]} du_{e,i} \\
&= \frac{\Gamma(1+T)^n \text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{nT}(2\sigma_{\mathbf{h}_e}^2)^n} \sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^n \left[\frac{1}{2\sigma_{\mathbf{h}_e}^2} + \frac{1}{2\sigma_e^2} \|\mathbf{x}_i\|^2 \right]^{-1-T}.
\end{aligned}$$

We finally obtain an upper bound of the average probability of correct decision for Eve for the wiretap block fading channel, given by

$$\boxed{\bar{P}_{c,e} \leq C_{\text{BF}} \gamma_e^{nT} \sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^n [1 + \gamma_e \|\mathbf{x}_i\|^2]^{-1-T}} \quad (22)$$

where

$$C_{\text{BF}} = \frac{(T!)^n \text{vol}(\Lambda_b)}{\pi^{nT}}$$

and similarly to the MIMO case, $\gamma_e = \frac{\sigma_{\mathbf{h}_e}^2}{\sigma_e^2}$.

In order to design a good lattice code for the block fading wiretap channel, we now try to derive a code design criterion from (22):

$$\bar{P}_{c,e} \leq C_{\text{BF}} \gamma_e^{Tn} \left[1 + \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \prod_{i=1}^n [1 + \gamma_e \|\mathbf{x}_i\|^2]^{-1-T} \right].$$

We can suppose that the code used to transmit data to Bob is designed according to the minimum product distance criterion. This means that, if $\mathbf{x} \neq 0$, then, $\mathbf{x}_i \neq 0$ for any i . If we assume this time that Eve's SNR γ_e is high compared to the minimum distance of Λ_e , or actually design Λ_e that way assuming Alice knows Eve's channel, we get

$$\bar{P}_{c,e} \leq C_{\text{BF}} \left[\gamma_e^{Tn} + \frac{1}{\gamma_e^n} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \prod_{i=1}^n (\|\mathbf{x}_i\|^2)^{-1-T} \right].$$

This expression is decreasing as a function of γ_e around the origin, a regime which we do not consider (as we again just derived the expression assuming γ_e big enough), and is then indeed increasing as expected. The minimum value of this upper bound is achieved for

$$\gamma_{e,\min} = \left(\frac{\sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \prod_{i=1}^n (||\mathbf{x}_i||^2)^{-1-T}}{T} \right)^{\frac{1}{n(1+T)}}.$$

We thus conclude that to minimize Eve's average probability of correct decoding, the design criterion is now

$$\min_{\Lambda_e} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \frac{1}{(\prod_{i=1}^n ||\mathbf{x}_i||^2)^{1+T}}.$$

When furthermore $T = 1$ (and X is thus a $n \times 1$ vector \mathbf{x}) in (20), we get a fast fading channel:

$$\begin{aligned} \mathbf{y} &= \text{diag}(\mathbf{h}_b)\mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \text{diag}(\mathbf{h}_e)\mathbf{x} + \mathbf{v}_e, \end{aligned}$$

where all vectors are n -dimensional complex vectors corresponding to n usages of the channel, and

$$\text{diag}(\mathbf{h}_b) = \begin{pmatrix} h_{b,1} & & \\ & \ddots & \\ & & h_{b,n} \end{pmatrix}, \quad \text{diag}(\mathbf{h}_e) = \begin{pmatrix} h_{e,1} & & \\ & \ddots & \\ & & h_{e,n} \end{pmatrix}$$

as before (see (21)). We can thus immediately apply the result (22) to deduce that

$$\bar{P}_{c,e} \leq C_{\text{FF}} \gamma_e^n \sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^n [1 + \gamma_e |x_i|^2]^{-2} \quad (23)$$

where

$$C_{\text{FF}} = \frac{\text{vol}(\Lambda_b)}{\pi^n}$$

and still again, $\gamma_e = \frac{\sigma_{\mathbf{h}_e}^2}{\sigma_e^2}$. The design criterion follows accordingly

$$\min_{\Lambda_e} \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \frac{1}{(\prod_{i=1}^n |x_i|^2)^2}.$$

We thus recover the expressions presented in [3], though here in the complex case, which explains the difference in the exponent ⁵.

⁵Please note an erratum in [3], since the sum derived there is over all lattice points, while of course, the zero vector should be removed from the sum.

V. A MIMO EXAMPLE: THE ALAMOUTI CODE

In this section, we illustrate the code design criterion derived above using the Alamouti code [1] with QAM constellation, $n_t = 2$, $n_e \geq 2$ and $T = 2$. Note that the Alamouti code does not form a $\mathbb{Z}[i]$ -lattice, but a \mathbb{Z} -lattice. We choose the Alamouti code nevertheless since this is the best understood and the simplest MIMO code available in the literature. It is not difficult to check that our analysis, and thus the resulting code design, holds for real lattices as well. An Alamouti codeword is then of the form

$$X = \begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix}, \quad x_1, x_2 \in \mathbb{Z}[i],$$

so that

$$\det(X X^*) = (|x_1|^2 + |x_2|^2)^2 = \|\mathbf{x}\|^4,$$

where

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{Z}[i]^2 = \Lambda_e.$$

The design criterion (19) requires to study

$$\sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \det(X X^*)^{-n_e - T} = \sum_{\mathbf{x} \in \Lambda_e \setminus \{0\}} \frac{1}{\|\mathbf{x}\|^{2(2(n_e + T))}} = \zeta_{\Lambda_e}(2(n_e + 2)), \quad (24)$$

where we recognize the Epstein zeta function of a scaled lattice $\mu\Lambda$ ($\mu > 0$), defined by

$$\zeta_{\mu\Lambda}(s) = \sum_{\mathbf{x} \in \Lambda \setminus \{0\}} \frac{1}{\mu^{2s}} \frac{1}{\|\mathbf{x}\|^{2s}} = \frac{1}{\mu^{2s}} \zeta_{\Lambda}(s). \quad (25)$$

Since $\mathbf{x} \in \mathbb{Z}[i]^2 \simeq \mathbb{Z}^4$, we will consider as possible lattices Λ_e either \mathbb{Z}^4 itself, with Epstein zeta function (see Proposition 3 in Appendix)

$$\zeta_{\mathbb{Z}^4}(s) = 8(1 - 4^{1-s}) \zeta(s) \zeta(s-1) \quad (26)$$

or D_4 , in which case the vector \mathbf{x} above is coded, and belongs to D_4 ⁶ instead of \mathbb{Z}^4 , which in turn involved the Epstein zeta function of D_4 (see Proposition 4 also in Appendix)

$$\zeta_{D_4}(s) = 3 \cdot 4^{2-s} (2^{s-1} - 1) \zeta(s) \zeta(s-1). \quad (27)$$

⁶The complex construction $D_4 = (1+i)\mathbb{Z}[i]^2 + (2, 1, 2)$ may be used, for instance, where $(2, 1, 2)$ is the repetition code of length 2.

In both cases, $\zeta(s) = \sum_{n>0} \frac{1}{n^s}$ is the Riemann zeta function.

In order to compare the Epstein zeta function of the two lattices \mathbb{Z}^4 and D_4 , we rescale D_4 so that its fundamental volume is equal to the fundamental volume of \mathbb{Z}^4 , that is 1. Since $\text{vol}(D_4) = 2$, the scaling factor is $\mu = \frac{1}{\sqrt[4]{2}}$. Combining (27) and (25), we obtain

$$\begin{aligned}\zeta_{\frac{1}{\sqrt[4]{2}}D_4}(s) &= \left(\sqrt[4]{2}\right)^{2s} 3 \cdot 4^{2-s} (2^{s-1} - 1) \zeta(s) \zeta(s-1) \\ &= 3 \cdot 2^{4-3\frac{s}{2}} \cdot (2^{s-1} - 1) \zeta(s) \zeta(s-1)\end{aligned}\quad (28)$$

where $s = 2n_e + 4$, which we have to compare with

$$\zeta_{\mathbb{Z}^4}(s) = 8 (1 - 4^{1-s}) \zeta(s) \zeta(s-1).$$

We eventually define the gain ς_{D_4} obtained by using D_4 instead of \mathbb{Z}^4 (the uncoded case) as

$$\begin{aligned}\varsigma_{D_4} &= \frac{\zeta_{\mathbb{Z}^4}(s)}{\zeta_{\mu D_4}(s)} \Big|_{s=2n_e+4} \\ &= \frac{-2^3 4^{1-s} (1 - 4^{s-1})}{3 \cdot 2^{4-3\frac{s}{2}} \cdot (2^{s-1} - 1)} \\ &= \frac{1}{3 \cdot 2^{\frac{s}{2}-1}} (2^{s-1} + 1) \Big|_{s=2n_e+4} \\ &= \frac{2^{2n_e+3} + 1}{3 \cdot 2^{n_e+1}} \cong \frac{4}{3} 2^{n_e}.\end{aligned}$$

We illustrate the obtained results on Figure 1 by plotting the upper bound (18) on Eve's probability $\bar{P}_{c,e}$ of correct decision, divided by the constant C_{MIMO} , when the Alamouti code is used with as coarse lattice Λ_e either \mathbb{Z}^4 or D_4 .

Notice that when γ_e is small, this upper bound becomes of course very loose as it is a decreasing function in γ_e , while we expect on the contrary $\bar{P}_{c,e}(\gamma_e)$ to be an increasing function. This motivates the following discussion the tightness of the upper bound (18).

We go back to the tighter upper bound (17) on $\bar{P}_{c,e}$:

$$\begin{aligned}\bar{P}_{c,e} &\leq C_{\text{MIMO}} \gamma_e^{Tn_t} \sum_{\mathbf{x} \in \Lambda_e} \det(\mathbf{I}_{n_t} + \gamma_e X X^*)^{-n_e-T} \\ &= C_{\text{MIMO}} \gamma_e^{-n_e n_t} \underbrace{\sum_{\mathbf{x} \in \Lambda_e} \det\left(\frac{1}{\gamma_e} \mathbf{I}_{n_t} + X X^*\right)^{-n_e-T}}_{\varphi_{\Lambda_e}(\gamma_e)}.\end{aligned}\quad (29)$$

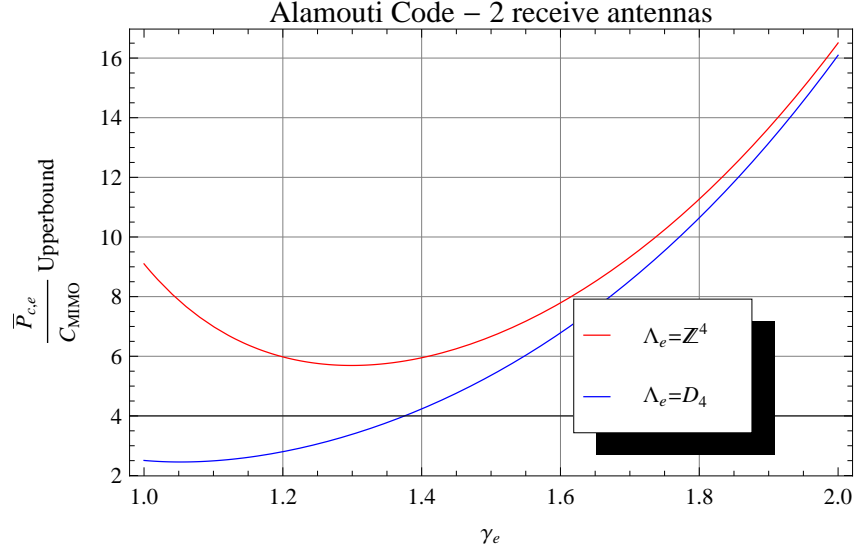


Fig. 1. An upper bound on $\frac{\bar{P}_{c,e}}{C_{\text{MIMO}}}$: the Alamouti code with $n_e = 2$.

When X is a codeword from the Alamouti code, with $T = n_t = 2$, then

$$\det \left(\frac{1}{\gamma_e} \mathbf{I}_{n_t} + X X^* \right) = \left(\frac{1}{\gamma_e} + \|\mathbf{x}\|^2 \right)^2,$$

so that

$$\varphi_{\Lambda_e}(\gamma_e) \triangleq \gamma_e^{-n_e n_t} \sum_{\mathbf{x} \in \Lambda_e} \det \left(\frac{1}{\gamma_e} \mathbf{I}_{n_t} + X X^* \right)^{-n_e - T} \quad (30)$$

$$= \gamma_e^{-2n_e} \sum_{\mathbf{x} \in \Lambda_e} \frac{1}{\left(\frac{1}{\gamma_e} + \|\mathbf{x}\|^2 \right)^{2(n_e+2)}} \quad (31)$$

$$= \gamma_e^4 + \gamma_e^{-2n_e} \sum_{\mathbf{x} \in \Lambda_e \setminus \{\mathbf{0}\}} \frac{1}{\left(\frac{1}{\gamma_e} + \|\mathbf{x}\|^2 \right)^{2(n_e+2)}}. \quad (32)$$

We are thus interested in the calculation of

$$\zeta_{\Lambda_e}(s, a) \triangleq \sum_{\mathbf{x} \in \Lambda_e} \frac{1}{(a + \|\mathbf{x}\|^2)^s} = \frac{1}{a^s} + \sum_{\mathbf{x} \in \Lambda_e \setminus \{\mathbf{0}\}} \frac{1}{(a + \|\mathbf{x}\|^2)^s}, \quad a = \frac{1}{\gamma_e}, \quad s = 2(n_e + 2),$$

which will be done via the Mellin transform

$$\mathcal{M}(f)(s) = \int_0^{+\infty} f(t) t^{s-1} dt,$$

thanks to which we obtain the following:

Lemma 1: If $a < \|\mathbf{x}\|^2$, we have that

$$\frac{1}{(a + \|\mathbf{x}\|^2)^s} = \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(\frac{1}{\|\mathbf{x}\|^2} \right)^{s+k}.$$

Proof: The Mellin transform of $e^{-(a+\|\mathbf{x}\|^2)t}$, for some positive $a \in \mathbb{R}$, is

$$\begin{aligned} \mathcal{M}\left(e^{-(a+\|\mathbf{x}\|^2)t}\right)(s) &= \int_0^{+\infty} e^{-(a+\|\mathbf{x}\|^2)t} t^s \frac{dt}{t} \\ &= \frac{1}{(a + \|\mathbf{x}\|^2)^s} \int_0^{+\infty} e^{-u} u^s \frac{du}{u} \\ &= \Gamma(s) \frac{1}{(a + \|\mathbf{x}\|^2)^s}, \end{aligned} \tag{33}$$

which we can alternatively write as

$$\begin{aligned} \mathcal{M}(e^{-(a+\|\mathbf{x}\|^2)t})(s) &= \mathcal{M}(e^{-at} e^{-\|\mathbf{x}\|^2 t})(s) \\ &= \int_0^{+\infty} \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} t^{k+s} e^{-\|\mathbf{x}\|^2 t} \frac{dt}{t} \\ &= \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \Gamma(s+k) \left(\frac{1}{\|\mathbf{x}\|^2} \right)^{s+k}. \end{aligned} \tag{34}$$

Now (34) involves a dangerous exchange of an integral with an infinite sum. For it to be allowed, we need to check that

$$\left(\sum_{k=0}^n \int_0^\infty \frac{|(-1)^k| a^k}{k!} t^{k+s} e^{-\|\mathbf{x}\|^2 t} \frac{dt}{t} \right)_{n \in \mathbb{N}}$$

converges for every t in the integration range, which is the same as showing that

$$\left(\sum_{k=0}^n \frac{|(-1)^k| a^k}{k!} \Gamma(s+k) \left(\frac{1}{\|\mathbf{x}\|^2} \right)^{s+k} \right)_{n \in \mathbb{N}}$$

converges for every t in the integration range. Since we only have strictly positive terms, comparing the n th term with the $(n+1)$ th term yields, recalling that since $s = 2(n_2 + 2)$, $\Gamma(s+n) = (s+n-1)!$:

$$\frac{a}{n+1} \frac{s+n}{\|\mathbf{x}\|^2}$$

whose limit needs to be strictly smaller than 1, that is

$$\lim_{n \rightarrow \infty} \frac{a}{n+1} \frac{s+n}{\|\mathbf{x}\|^2} = \frac{a}{\|\mathbf{x}\|^2} < 1, \tag{35}$$

showing that the above computation is valid when $a < \|\mathbf{x}\|^2$. We then have, comparing (33) and (34), that

$$\frac{1}{(a + \|\mathbf{x}\|^2)^s} = \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(\frac{1}{\|\mathbf{x}\|^2} \right)^{s+k}.$$

■

We are now ready to prove the following result for \mathbb{Z}^4 . The equivalent result for D_4 follows, and the consequences of both computations for the bound on the error probability can be found below in Corollary 1.

Proposition 1: Suppose $0 < a < q$. For the lattice \mathbb{Z}^4 , we have

$$\zeta_{\mathbb{Z}^4}(s, a) = \sum_{\mathbf{x} \in \mathbb{Z}^4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} = \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(-8 \cdot 4^{1-s-k} - \sum_{j=2}^{q-1} \frac{r_4(j)}{j^{s+k}} \right),$$

where $r_4(j)$ denotes the number of vectors of norm j in \mathbb{Z}^4 . In particular if $0 < a < 2$, we have

$$\zeta_{\mathbb{Z}^4}(s, a) = \sum_{\mathbf{x} \in \mathbb{Z}^4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} = \frac{1}{a^s} + \frac{8}{(1+a)^s} - 8 \cdot 4^{1-s} \left(1 - \frac{a}{4} \right)^s,$$

and

$$\zeta_{\mathbb{Z}^4}(s, a) \leq \sum_{j=0}^3 \frac{r_4(j)}{(a+j)^s} - 8 \cdot 4^{1-s} \left(1 - \frac{a}{4} \right)^s - \frac{1}{4^s} \sum_{j=2}^3 r_4(j) \left(1 - \frac{a}{4} \right)^s$$

if $0 < a < 4$.

Proof: Since \mathbb{Z}^4 is an integer lattice with vectors of norm 1, we have $\|\mathbf{x}\|^2 \geq 1$ if $\mathbf{x} \neq 0$, that is we need $a < 1$ to use the above lemma. Alternatively, if we consider lattice points whose norm is at least q , we can use $a < q$, which gives

$$\begin{aligned} \sum_{\mathbf{x} \in \Lambda_e} \frac{1}{(a + \|\mathbf{x}\|^2)^s} &= \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} + \sum_{\mathbf{x} \in \Lambda_e, \|\mathbf{x}\|^2 \geq q} \frac{1}{(a + \|\mathbf{x}\|^2)^s} \\ &= \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} + \sum_{\mathbf{x} \in \Lambda_e, \|\mathbf{x}\|^2 \geq q} \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(\frac{1}{\|\mathbf{x}\|^2} \right)^{s+k} \\ &= \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \sum_{\mathbf{x} \in \Lambda_e, \|\mathbf{x}\|^2 \geq q} \frac{1}{\|\mathbf{x}\|^{2(s+k)}} \\ &= \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(\zeta_{\Lambda_e}(s+k) - \sum_{j=1}^{q-1} \frac{r_4(j)}{j^{s+k}} \right) \end{aligned}$$

where $\zeta_{\Lambda_e}(s)$ is the Epstein zeta function of Λ defined in (25), and $r_4(j)$ counts the number of vectors of norm j in \mathbb{Z}^4 . We were allowed to exchange both infinite sums since $\zeta_{\Lambda_e}(s+k)$ converges, and thus so does $\zeta_{\Lambda_e}(s+k) - \sum_{j=1}^{q-1} \frac{r_4(j)}{j^{s+k}}$, for every $k \geq 0$, and

$$\sum_{k=0}^{+\infty} \frac{|(-1)^k| a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(\zeta_{\Lambda_e}(s+k) - \sum_{j=1}^{q-1} \frac{r_4(j)}{j^{s+k}} \right) \quad (36)$$

converges as well, which follows from

$$\frac{a(s+n) \left(\zeta_{\Lambda_e}(s+n+1) - \sum_{j=1}^{q-1} \frac{r_4(j)}{j^{s+n+1}} \right)}{(n+1) \left(\zeta_{\Lambda_e}(s+n) - \sum_{j=1}^{q-1} \frac{r_4(j)}{j^{s+n}} \right)} \leq \frac{a(s+n)}{q(n+1)} \rightarrow \frac{a}{q} < 1$$

when n grows, noting that

$$\zeta_{\Lambda_e}(s+n+1) - \sum_{j=1}^{q-1} \frac{r_4(j)}{j^{s+n+1}} = \sum_{\mathbf{x} \in \Lambda_e, \|\mathbf{x}\|^2 \geq q} \frac{1}{\|\mathbf{x}\|^{2(s+n)} \|\mathbf{x}\|^2} \leq \frac{1}{q} \sum_{\mathbf{x} \in \Lambda_e, \|\mathbf{x}\|^2 \geq q} \frac{1}{\|\mathbf{x}\|^{2(s+n)}}.$$

The Epstein zeta function of the lattice \mathbb{Z}^4 is given (see Proposition 3) by

$$\zeta_{\mathbb{Z}^4}(s) = 8(1 - 4^{1-s})\zeta(s)\zeta(s-1)$$

and since $s = 2(n_e + 2) \geq 8$ when $n_2 \geq 2$, $\zeta(s+k)\zeta(s-1+k)$ can be approximated by the smallest value of k and s , namely $\zeta(8)\zeta(7)$, where $\zeta(7) \simeq 1.00835$. Thus

$$\zeta_{\mathbb{Z}^4}(s+k) = 8(1 - 4^{1-s-k})\zeta(s+k)\zeta(s+k-1) \simeq 8(1 - 4^{1-s-k}),$$

and, using that $r_4(1) = 8$ (there are 8 vectors of norm 1, the 4 unit vectors and the same vectors with a minus sign)

$$\begin{aligned} \sum_{\mathbf{x} \in \mathbb{Z}^4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} &= \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(8(1 - 4^{1-s-k}) - \sum_{j=1}^{q-1} \frac{r_4(j)}{j^{s+k}} \right) \\ &= \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(-8 \cdot 4^{1-s-k} - \sum_{j=2}^{q-1} \frac{r_4(j)}{j^{s+k}} \right). \end{aligned}$$

In particular if $q = 2$, we get that

$$\begin{aligned} \sum_{\mathbf{x} \in \mathbb{Z}^4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} &= \frac{1}{a^s} + \frac{8}{(1+a)^s} - 8 \cdot 4^{1-s} \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{4^k} \frac{\Gamma(s+k)}{k! \Gamma(s)} \\ &= \frac{1}{a^s} + \frac{8}{(1+a)^s} - 8 \cdot 4^{1-s} \sum_{k=0}^{+\infty} \left(\frac{-a}{4} \right)^k \binom{s+k-1}{k} \\ &= \frac{1}{a^s} + \frac{8}{(1+a)^s} - 8 \cdot 4^{1-s} \sum_{k=0}^{+\infty} \left(\frac{-a}{4} \right)^k \binom{s-1}{k}, \end{aligned}$$

recalling the definition of Gamma functions for positive integers. In summary, recognizing the generalized binomial coefficients, we get

$$\sum_{\mathbf{x} \in \mathbb{Z}^4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} = \frac{1}{a^s} + \frac{8}{(1+a)^s} - 8 \cdot 4^{1-s} \left(1 - \frac{a}{4}\right)^s.$$

If instead $q = 4$, we note first (this first inequality holds for any q but not what will follow) that

$$\sum_{j=2}^{q-1} \frac{r_4(j)}{j^{s+k}} \geq \frac{1}{q^{s+k}} \sum_{j=2}^{q-1} r_4(j),$$

so that

$$\begin{aligned} & \sum_{\mathbf{x} \in \mathbb{Z}^4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} \\ & \leq \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} - 8 \cdot 4^{1-s} \sum_{k=0}^{+\infty} \frac{(-1)^k a^k \Gamma(s+k)}{4^k k! \Gamma(s)} - \frac{1}{q^s} \sum_{j=2}^{q-1} r_4(j) \sum_{k=0}^{+\infty} \frac{(-1)^k a^k \Gamma(s+k)}{q^k k! \Gamma(s)} \\ & = \sum_{j=0}^{q-1} \frac{r_4(j)}{(a+j)^s} - 8 \cdot 4^{1-s} \left(1 - \frac{a}{4}\right)^s - \frac{1}{q^s} \sum_{j=2}^{q-1} r_4(j) \left(1 - \frac{a}{q}\right)^s. \end{aligned}$$

The condition $q = 4$ ensures the convergence of the second series. ■

Proposition 2: Suppose $0 < a < q$. For the lattice D_4 , we have

$$\zeta_{D_4}(s, a) = \sum_{\mathbf{x} \in D_4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} = \sum_{j=0}^{q-1} \frac{r_{D_4}(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k \Gamma(s+k)}{k! \Gamma(s)} \left(-3 \cdot 4^{2-s-k} - \sum_{j=3}^{q-1} \frac{r_{D_4}(j)}{j^{s+k}} \right),$$

where $r_{D_4}(j)$ denotes the number of vectors of length j in D_4 . In particular, if $0 < a < 2$, we have

$$\zeta_{D_4}(s, a) = \frac{1}{a^s} - 3 \cdot 4^{2-s} \left(1 - \frac{a}{4}\right)^s,$$

and

$$\zeta_{D_4}(s, a) = \frac{1}{a^s} + \frac{24}{(a+2)^s} - 3 \cdot 4^{2-s} \left(1 - \frac{a}{4}\right)^s$$

for $0 < a < 4$.

Proof: The following computed above for \mathbb{Z}^4 holds similarly for D_4

$$\sum_{\mathbf{x} \in D_4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} = \sum_{j=0}^{q-1} \frac{r_{D_4}(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k \Gamma(s+k)}{k! \Gamma(s)} \left(\zeta_{\Lambda_e}(s+k) - \sum_{j=1}^{q-1} \frac{r_{D_4}(j)}{j^{s+k}} \right)$$

where we use the notation $r_{D_4}(j)$ to denote the number of vectors of length j in D_4 . Note that D_4 has no vector of norm 1, and 24 of norm 2.

From Proposition 4, the Epstein zeta function of D_4 is

$$\zeta_{D_4}(s+k) = 3 \cdot 4^{2-s-k} (2^{s+k-1} - 1) \zeta(s+k) \zeta(s+k-1),$$

and as before for \mathbb{Z}^4

$$\zeta_{D_4}(s+k) \simeq 3 \cdot 4^{2-s-k} (2^{s+k-1} - 1),$$

so that

$$\begin{aligned} \sum_{\mathbf{x} \in D_4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} &= \sum_{j=0}^{q-1} \frac{r_{D_4}(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(3 \cdot 4^{2-s-k} (2^{s+k-1} - 1) - \sum_{j=1}^{q-1} \frac{r_{D_4}(j)}{j^{s+k}} \right) \\ &= \sum_{j=0}^{q-1} \frac{r_{D_4}(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} \left(-3 \cdot 4^{2-s-k} - \sum_{j=3}^{q-1} \frac{r_{D_4}(j)}{j^{s+k}} \right). \end{aligned}$$

If $q = 2$, we can simplify the above expression to get

$$\begin{aligned} \sum_{\mathbf{x} \in D_4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} &= \frac{1}{a^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} (-3 \cdot 4^{2-s-k}) \\ &= \frac{1}{a^s} - 3 \cdot 4^{2-s} \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{4^k} \frac{\Gamma(s+k)}{k! \Gamma(s)} \\ &= \frac{1}{a^s} - 3 \cdot 4^{2-s} \left(1 - \frac{a}{4} \right)^s, \end{aligned}$$

while if $q = 4$, recalling that D_4 has no vector of length 3

$$\begin{aligned} \sum_{\mathbf{x} \in D_4} \frac{1}{(a + \|\mathbf{x}\|^2)^s} &= \sum_{j=0}^3 \frac{r_{D_4}(j)}{(a+j)^s} + \sum_{k=0}^{+\infty} \frac{(-1)^k a^k}{k!} \frac{\Gamma(s+k)}{\Gamma(s)} (-3 \cdot 4^{2-s-k}) \\ &= \frac{1}{a^s} + \frac{24}{(a+2)^s} - 3 \cdot 4^{2-s} \left(1 - \frac{a}{4} \right)^s. \end{aligned}$$

■

The implications of the above computations for the error probability are summarized below for $\gamma_e > 1/2$. Similar expressions can be obtained for $\gamma_e > 1/4$ (or smaller values of γ_e).

Corollary 1: Suppose $\gamma_e > 1/2$. We have when using $\Lambda_e = \mathbb{Z}^4$ that

$$\bar{P}_{c,e} \leq C_{\text{MIMO}} \gamma_e^{-2n_e} \left(\gamma_e^{2(n_e+2)} + \frac{8}{(1 + 1/\gamma_e)^{2(n_e+2)}} - 8 \cdot 4^{1-2(n_e+2)} \left(1 - \frac{1}{4\gamma_e} \right)^{2(n_e+2)} \right)$$

while with $\Lambda_e = D_4$

$$\bar{P}_{c,e} \leq C_{\text{MIMO}} \gamma_e^{-2n_e} \left(\gamma_e^{2(n_e+2)} - 3 \cdot 4^{2-2(n_e+2)} \left(1 - \frac{1}{4\gamma_e} \right)^{2(n_e+2)} \right).$$

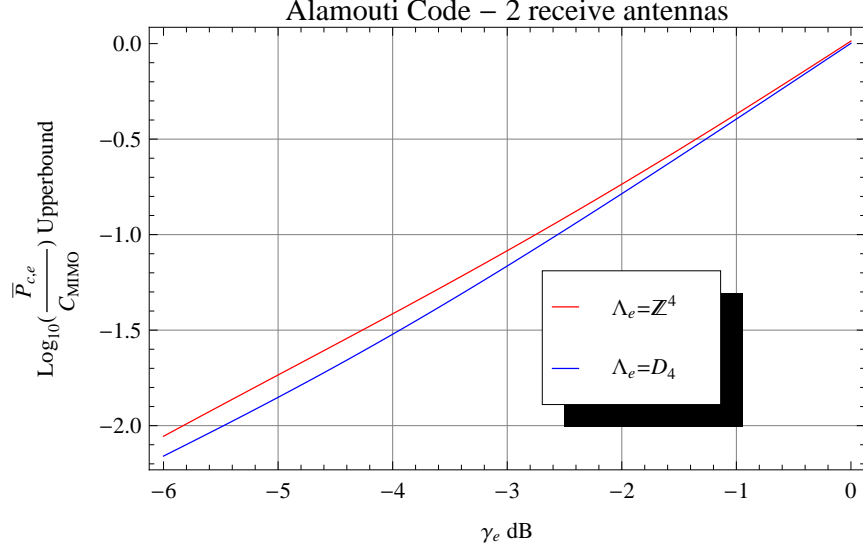


Fig. 2. A tighter upper bound on $\frac{\bar{P}_{c,e}}{C_{\text{MIMO}}}$: the Alamouti code with $n_e = 2$.

See Figure 2 for an illustration of the new bounds.

To conclude, we compare the loose upperbounds with the tight ones in Figure 3, and our bounds on the probability of correct decision for the eavesdropper with simulations in Figure 4. The coarse lattice Λ_e is \mathbb{Z}^4 (resp. D_4) while the fine lattice Λ_b is $1/2\mathbb{Z}^4$ (resp. $1/2D_4$) giving rise to a secret spectral efficiency equal to 1 bit per real dimension. For simulations, we used the linear ML decoder of the original Alamouti paper [1]. Decoding of D_4 has been done using the Wagner decoder of the binary parity check (4,3) code.

VI. CONCLUSION

We considered a MIMO wiretap channel, where Alice uses lattice codes via coset encoding to communicate with Bob in the presence of an eavesdropper Eve. We showed, by analyzing Eve's probability of correctly decoding the message meant to Bob, that this probability can be minimized by designing the lattice codes according to a suitable design criterion. The cases of block and fast fading channels are treated similarly. We also illustrate how our analysis applies to the Alamouti code, making explicit an interesting connection to Epstein zeta functions. Current and future work involve a more systematic design of such lattice wiretap codes.

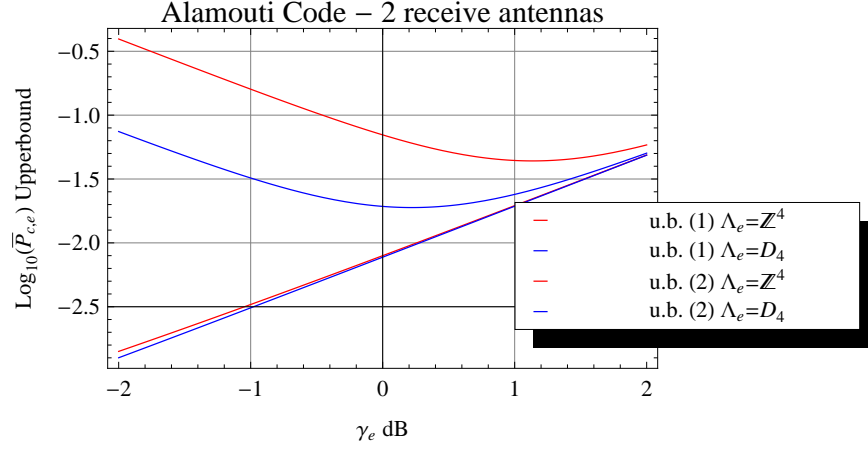


Fig. 3. Loose upper bounds versus tight upper bounds: the Alamouti code with $n_e = 2$.

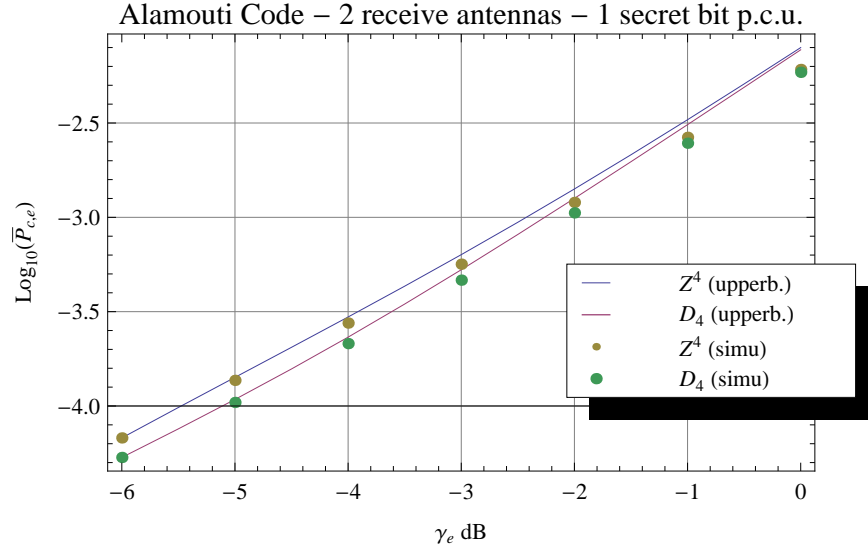


Fig. 4. Upper bounds versus simulations: the Alamouti code with $n_e = 2$.

ACKNOWLEDGMENTS

Part of this work was done while J.-C. Belfiore was visiting Nanyang Technological University, Singapore. The work of F. Oggier is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07. The authors would like to thank Patrick Solé for his help regarding Epstein zeta functions.

APPENDIX

In this appendix, we compute the Epstein zeta functions of \mathbb{Z}^4 and D_4 .

Recall that the Epstein zeta function of a lattice Λ is defined by

$$\zeta_\Lambda(s) \triangleq \sum_{\mathbf{x} \in \Lambda \setminus \{0\}} \frac{1}{\|\mathbf{x}\|^{2s}} = \sum_{n>0} \frac{r_\Lambda(n)}{n^s} \quad (37)$$

where $r_\Lambda(n)$ is the number of vectors of Λ with a squared Euclidean norm equal to n . Note that $r_\Lambda(n)$ similarly appears in the theta series of Λ :

$$\Theta_\Lambda(q) = 1 + \sum_{\mathbf{x} \in \Lambda \setminus \{0\}} q^{\|\mathbf{x}\|^2} = 1 + \sum_{n>0} r_\Lambda(n) q^n.$$

Proposition 3: The Epstein zeta function of \mathbb{Z}_4 is

$$\zeta_{\mathbb{Z}^4}(s) = 8 (1 - 4^{1-s}) \zeta(s) \zeta(s-1).$$

Proof: We have

$$\zeta_{\mathbb{Z}^4}(s) = \sum_{n>0} \frac{r_4(n)}{n^s}$$

where $r_N(n)$ is the number of solutions to the Diophantine equation $k_1^2 + k_2^2 + \dots + k_N^2 = n$ (counting permutations and signs). We now use a result of [16, Paragraph 91], better exposed in [4],

$$r_4(n) = 8\sigma(n) - 32\sigma\left(\frac{n}{4}\right)$$

where $\sigma(n) = \sum_{d|n} d$ and it is understood that $\sigma(m) = 0$ if m is not a positive integer. In particular, this implies that

$$\sum_{n>0} \frac{\sigma(n/4)}{n^s} = \sum_{m>0} \frac{\sigma(m)}{(4m)^s}.$$

We thus obtain

$$\begin{aligned} \zeta_{\mathbb{Z}^4}(s) &= 8 \sum_{n>0} \frac{\sigma(n)}{n^s} - \frac{32}{4^s} \sum_{n>0} \frac{\sigma(n)}{n^s} \\ &= 8 (1 - 4^{1-s}) \sum_{n>0} \frac{\sigma(n)}{n^s} \\ &= 8 (1 - 4^{1-s}) \zeta(s) \zeta(s-1) \end{aligned} \quad (38)$$

where the last equality comes from [7, Chapter XVII] and $\zeta(s) = \sum_{n>0} \frac{1}{n^s}$ is the Riemann zeta function. ■

Proposition 4: The Epstein zeta function of D_4 is

$$\zeta_{D_4}(s) = 3 \cdot 4^{2-s} (2^{s-1} - 1) \zeta(s) \zeta(s-1).$$

Proof: The lattice D_4 is the 4-dimensional checkerboard lattice i.e., the set of all 4 dimensional integer valued vectors whose components have an even sum. Its theta series is well-known [5] and is equal to

$$\Theta_{D_4}(q) = \frac{1}{2} (\vartheta_3^4(q) + \vartheta_4^4(q))$$

where

$$\begin{aligned} \vartheta_3(q)^4 &= \left(\sum_{k \in \mathbb{Z}} q^{k^2} \right)^4 \\ &= 1 + \sum_{n > 0} r_4(n) q^n \end{aligned}$$

is the theta series of \mathbb{Z}^4 , whereas

$$\begin{aligned} \vartheta_4(q)^4 &= \left(\sum_{k \in \mathbb{Z}} (-1)^k q^{k^2} \right)^4 \\ &= \sum_{k_1 \in \mathbb{Z}} (-1)^{k_1} q^{k_1^2} \sum_{k_2 \in \mathbb{Z}} (-1)^{k_2} q^{k_2^2} \sum_{k_3 \in \mathbb{Z}} (-1)^{k_3} q^{k_3^2} \sum_{k_4 \in \mathbb{Z}} (-1)^{k_4} q^{k_4^2} \\ &= \sum_{k_1, k_2, k_3, k_4 \in \mathbb{Z}} (-1)^{k_1 + k_2 + k_3 + k_4} q^{k_1^2 + k_2^2 + k_3^2 + k_4^2} \\ &= 1 + \sum_{n > 0} (-1)^n r_4(n) q^n \end{aligned}$$

since $k_1 + k_2 + k_3 + k_4 \equiv k_1^2 + k_2^2 + k_3^2 + k_4^2 \pmod{2}$. Thus the theta series of D_4 can be rewritten as

$$\begin{aligned} \Theta_{D_4}(q) &= \frac{1}{2} \left(1 + \sum_{n > 0} r_4(n) q^n + 1 + \sum_{n > 0} (-1)^n r_4(n) q^n \right) \\ &= 1 + \frac{1}{2} \sum_{n > 0} (r_4(n) q^n + (-1)^n r_4(n) q^n), \end{aligned}$$

showing that the Epstein zeta function of D_4 is

$$\begin{aligned} \zeta_{D_4}(s) &= \frac{1}{2} \sum_{n > 0} \frac{r_4(n) + (-1)^n r_4(n)}{n^s} \\ &= \frac{1}{2} \zeta_{\mathbb{Z}^4} + \frac{1}{2} \sum_{n > 0} \frac{(-1)^n r_4(n)}{n^s}. \end{aligned}$$

Using again as in the above proof that

$$r_4(n) = 8\sigma(n) - 32\sigma\left(\frac{n}{4}\right),$$

we get

$$\begin{aligned} \frac{1}{2} \sum_{n>0} (-1)^n \frac{r_4(n)}{n^s} &= 4 \left(\sum_{n>0} (-1)^n \frac{\sigma(n)}{n^s} - 4 \sum_{m>0} \frac{\sigma(m)}{(4m)^s} \right) \\ &= 4 \left(\sum_{n>0} (-1)^n \frac{\sigma(n)}{n^s} - 4^{1-s} \zeta(s) \zeta(s-1) \right) \end{aligned}$$

since [7, Chapter XVII]

$$\sum_{n>0} \frac{\sigma(n)}{n^s} = \zeta(s) \zeta(s-1).$$

We are left to compute

$$\begin{aligned} \sum_{n>0} (-1)^n \frac{\sigma(n)}{n^s} &= - \sum_{n \text{ odd}} \frac{\sigma(n)}{n^s} + \sum_{n \text{ even}} \frac{\sigma(n)}{n^s} \\ &= - \sum_{n \text{ odd}} \frac{\sigma(n)}{n^s} + \sum_{v>0} \frac{\sigma(2^v)}{2^{vs}} \sum_{n \text{ odd}} \frac{\sigma(n)}{n^s} \\ &= \sum_{n \text{ odd}} \frac{\sigma(n)}{n^s} \left(-1 + \sum_{v>0} \frac{2^{v+1} - 1}{2^{vs}} \right) \\ &= \sum_{n \text{ odd}} \frac{\sigma(n)}{n^s} \left(-1 + \frac{2^{2-s}}{1 - 2^{1-s}} - \frac{2^{-s}}{1 - 2^{-s}} \right) \end{aligned}$$

where the second equality follows from the multiplicativity of σ . Since similarly

$$\sum_{n>0} \frac{\sigma(n)}{n^s} = \sum_{n \text{ odd}} \frac{\sigma(n)}{n^s} \left(1 + \frac{2^{2-s}}{1 - 2^{1-s}} - \frac{2^{-s}}{1 - 2^{-s}} \right),$$

a comparison of both expressions yields

$$\begin{aligned} \sum_{n>0} (-1)^n \frac{\sigma(n)}{n^s} &= \sum_{n>0} \frac{\sigma(n)}{n^s} \left(\frac{-1 + \frac{2^{2-s}}{1-2^{1-s}} - \frac{2^{-s}}{1-2^{-s}}}{1 + \frac{2^{2-s}}{1-2^{1-s}} - \frac{2^{-s}}{1-2^{-s}}} \right) \\ &= \zeta(s) \zeta(s-1) \left(\frac{\frac{2^{2-s}}{1-2^{1-s}} - \frac{1}{1-2^{-s}}}{\frac{2^{2-s}}{1-2^{1-s}} + \frac{1-2^{1-s}}{1-2^{-s}}} \right) \\ &= \zeta(s) \zeta(s-1) \left(\frac{2^{2-s}(1-2^{-s}) - (1-2^{1-s})}{2^{2-s}(1-2^{-s}) + (1-2^{1-s})^2} \right) \\ &= \zeta(s) \zeta(s-1) (2^{2-s} - 2^{2-2s} + 2^{1-s} - 1), \end{aligned}$$

and we obtain that

$$\begin{aligned} \frac{1}{2} \sum_{n>0} (-1)^n \frac{r_4(n)}{n^s} &= 4 (2^{2-s} - 2^{2-2s} + 2^{1-s} - 1 - 4^{1-s}) \zeta(s) \zeta(s-1) \\ &= 4 (2 \cdot 2^{1-s} - 2 \cdot 2^{2-2s} + 2^{1-s} - 1) \zeta(s) \zeta(s-1). \end{aligned}$$

We finally obtain the expression of the Epstein zeta function of D_4 :

$$\begin{aligned} \zeta_{D_4}(s) &= \frac{1}{2} \zeta_{\mathbb{Z}^4} + \frac{1}{2} \sum_{n>0} \frac{(-1)^n r_4(n)}{n^s} \\ &= 4 (1 - 4^{1-s}) \zeta(s) \zeta(s-1) + 4 (3 \cdot 2^{1-s} - 2 \cdot 2^{2-2s} - 1) \zeta(s) \zeta(s-1) \\ &= 4 (-3 \cdot 2^{2-2s} + 3 \cdot 2^{1-s}) \zeta(s) \zeta(s-1) \\ &= 3 \cdot 4^{2-s} (2^{s-1} - 1) \zeta(s) \zeta(s-1). \end{aligned}$$

■

REFERENCES

- [1] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communication," *IEEE Journal on Selected Areas in Communication*, Vol 16, No, 8, October 1998
- [2] J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design," ISITA 2010, 2010. [Online]. Available: <http://arXiv:1004.4075v2> [cs.IT]
- [3] J.-C. Belfiore and F. Oggier, "Lattice Code Design for the Rayleigh Fading Wiretap Channel", IEEE International Conference on Communications (ICC) 2011, Japan.
- [4] J. M. Borwein and K. S. Choi, "On Dirichlet Series for Sums of Squares," *The Ramanujan Journal*, 7, 95–127, 2003.
- [5] J.H. Conway, N.J.A. Sloane, "Sphere packings, Lattices and Groups," Third edition, *Springer-Verlag*, New York, 1998.
- [6] N.R. Goodman, "Statistical Analysis Based on a Certain Multivariate Complex Gaussian Distribution (an Introduction)", *Ann. Math. Statist.*, Volume 34, Number 1 (1963), 152-177.
- [7] G. H. Hardy and E. M. Wright, "An Introduction to the Theory of numbers," Oxford, 1979.
- [8] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. on Inform. Theory*, vol. 48, no. 7, pp. 1804-1824.
- [9] A. O. Hero, "Secure Space-Time Communication," *IEEE Trans. on Info Theory*, Vol. 49, No. 12, pp. 1-16, Dec. 2003.
- [10] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas-II: The MIMOME Wiretap Channel," *IEEE Trans. Inf. Theory*, Vol. 56, No. 11, pp. 5515-5532, Nov. 2010
- [11] C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehlé, "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel", preprint, available at <http://arxiv.org/abs/1210.6673>.
- [12] T. Liu, Shlomo Shamai (Shitz), "A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel," *IEEE Trans. on Information Theory*, vol. 55, no. 6, pp. 2547-2553, June 2009.

- [13] D. K. Nagar and A. K. Gupta, "Expectations of Functions of Complex Wishart Matrix," *Acta Appl. Math.* (2011) 113: pp. 265 - 288
- [14] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel", *IEEE Trans. Inf. Theory*, vol. 57, no 8, August 2011.
- [15] F. Oggier, P. Solé and J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis," preprint, available on arXiv arXiv:1103.4086v1 [cs.IT].
- [16] H. Rademacher, "Topics in Analytic Number Theory," Springer-Verlag, 1973.
- [17] B.A. Sethuraman, B. Sundar Rajan and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Transactions on Information Theory*, vol. 49, no. 10, Oct. 2003,
- [18] M. S. Srivastava, "On the Complex Wishart Distribution", *Ann. Math. Statist.*, Volume 36, Number 1 (1965), 313-315.
- [19] V. Tarokh, N. Seshadri and A. R. Calderbank, "Space-Time codes for high data rate wireless communication: Performance analysis and code construction," *IEEE Trans. on Inform. Theory*, vol. 44 (2), Mar. 1998, pp. 744 - 765.
- [20] Tan F. Wong, M. Bloch, J. M. Shea, "Secret Sharing over Fast-Fading MIMO Wiretap Channels", *EURASIP Journal on Wireless Communications and Networking*, Volume 2009 (2009), Article ID 506973.
- [21] A.D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, October 1975.