# Analysis on Wiretap Lattice Codes and Probability Bounds from Dedekind Zeta Functions

Camilla Hollanti, *Member, IEEE*
cajoho@utu.fi
Department of Mathematics
FI-20014 University of Turku
Finland

Emanuele Viterbo, *Fellow, IEEE*
emanuele.viterbo@monash.edu
Department of Electrical and Comp. Syst. Eng.
Monash University
Victoria 3800, Australia

***Abstract*—When employing lattice codes based on algebraic number fields in wiretap channel coding, certain norm sums pop up in the expression of the probability of correct decision for Eve the Eavesdropper. These norm sums closely resemble the Dedekind zeta function. The aim in this paper is to derive bounds for Eve's probability of correct decision in Rayleigh fading channels by using zeta functions and provide some numerical analysis on the behavior of the norm sums. It is then pointed out that, not surprisingly, similar sums occur in *e.g.* the expression of the pairwise error probability (PEP), when using similar number field lattice codes. Hence, same tools can be – and have been – used to derive bounds for the PEP and diversity-multiplexing gain tradeoff (DMT) as well.**

## I. Introduction

Gaussian and fading wiretap channels have been considered at least in [1], [2], [3], [4]. In [5] the authors propose to use number field lattice (NFL) codes, which will be the basis for our study and constructions. This paper can be seen as a continuation of [6], where preliminary analysis on NFL codes in fast fading channels was carried out based on various explicit four-dimensional NFL code constructions, as well as of [7], [8], where zeta functions were first used for deriving diversity-multiplaxing gain tradeoff (DMT) and PEP bounds.

First, following [6], we attempt to increase the understanding of the performance of wiretap lattice codes through a numerical analysis on the probability of Eve the Eavesdropper's correct decision in fast and block fading channels. To this end, we analyze some explicit lattice code constructions based on algebraic number fields $K$ and the canonical embedding of their rings of integers $\mathcal{O}_K$ or an ideal $\mathcal{I} \subseteq \mathcal{O}_K$, as suggested in [5], and then compute the truncated *inverse norm power sum* factors in Eve's probability expression. The study concentrates on the special case of totally real number field extensions to guarantee full diversity [9], with explicit example codes arising from both orthogonal and skewed lattices that are subsets in $\mathbb{R}^n$. Some of the results indicate a performance-secrecy-complexity tradeoff: relaxing on the legitimate user's performance can, in some cases, significantly increase the security of transmission. The confusion experienced by the eavesdropper may be further increased by using skewed lattices, but at the cost of increased complexity.

Second, we derive bounds for the probability expressions related to the wiretap channel and for the pairwise error probability by using Dedekind zeta functions.

## II. Preliminaries

Let us first recall the notion of a lattice as they will play a key role throughout the paper. For our purposes, a *lattice* $\Lambda$ is a discrete abelian subgroup of a real vector space,

$$\Lambda = \mathbb{Z}\beta_1 \oplus \mathbb{Z}\beta_2 \cdots \oplus \mathbb{Z}\beta_s \subset \mathbb{R}^n,$$

where the elements $\beta_1, \ldots, \beta_s \in \mathbb{R}^n$ are linearly independent, *i.e.*, form a lattice basis, and $s \leq n$ is called the *rank* of the lattice. Here, we only consider full ($s = n$) totally real lattices arising from algebraic number fields (see Def. 2.3 below).

The *Gram matrix* of a full totally real lattice is defined as

$$G(\Lambda) = MM^T,$$

where

$$M = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}_{n \times n}$$

is the *generator matrix* of the lattice. The determinant of the Gram matrix is also called *lattice determinant*. The *volume* of the fundamental parallelotope of the lattice is

$$\mathrm{Vol}(\Lambda) = \sqrt{\det(G(\Lambda))} = |\det(M)|.$$

*Definition 2.1:* The *minimum product distance* of a lattice $\Lambda$ is

$$d_{p,min}(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} \prod_{i=1}^{n} |x_i|,$$

where $\mathbf{x} = (x_1, \ldots, x_n) \in \Lambda$.

*Remark 2.1:* In order to fairly compare different lattices, we first normalize them to a unit volume and then compute the normalized minimum product distance as described in the next definition.

*Definition 2.2:* The *normalized minimum product distance* of an $n$-dimensional lattice $\Lambda$ is

$$Nd_{p,min}(\Lambda) = d_{p,min}(\rho\Lambda) = \rho^n d_{p,min}(\Lambda),$$

where $\rho \in \mathbb{R}$ is chosen so that $\mathrm{Vol}(\rho\Lambda) = 1$.

*Definition 2.3:* Let $K/\mathbb{Q}$ be a totally real number field extension of degree $n$ and $\sigma_1, \ldots, \sigma_n$ its embeddings to $\mathbb{R}$. Let $\mathcal{O}_K$ denote the ring of integers in $K$. The *canonical embedding* $\psi : K \hookrightarrow \mathbb{R}$ defines a lattice $\Lambda = \psi(\mathcal{O}_K)$ in $\mathbb{R}^n$:

$$\psi(x) = (\sigma_1(x), \ldots, \sigma_n(x)) \in \psi(\mathcal{O}_K) \subset \mathbb{R}^n,$$

where $x \in \mathcal{O}_K$. We further have that

$$d_{p,min}(\psi(\mathcal{O}_K)) = \min_{0 \neq x \in \mathcal{O}_K} |N_{K/\mathbb{Q}}(x)| = 1.$$

The generator matrix of the algebraic lattice is

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\omega_1) & \cdots & \sigma_n(\omega_n) \end{pmatrix},$$

where $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}$-basis of $K$.

*Definition 2.4:* With the above notation, we define the *twisted canonical embedding* by

$$\psi_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \ldots, \sqrt{\sigma_n(\alpha)}\sigma_n(x)) \in \mathbb{R}^n,$$

where $\alpha \in K$ is a totally positive element, *i.e.*, $\sigma_i(\alpha) > 0 \, \forall i$ (see [9, Sec. 6] for more details). The corresponding *twisted lattice* $\Lambda_\alpha$ is generated by the matrix

$$M_\alpha = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(\omega_1) & \cdots & \sqrt{\sigma_1(\alpha)}\sigma_1(\omega_n) \\ \vdots & & \vdots \\ \sqrt{\sigma_n(\alpha)}\sigma_n(\omega_1) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(\omega_n) \end{pmatrix}.$$

The volume of the twisted lattice is

$$\mathrm{Vol}(\Lambda_\alpha) = \sqrt{N_{K/\mathbb{Q}}(\alpha)}\mathrm{Vol}(\Lambda),$$

and the minimum product distance

$$d_{p,min}(\Lambda_\alpha) = \sqrt{N_{K/\mathbb{Q}}(\alpha)},$$

where $\Lambda = \psi(\mathcal{O}_K)$ is the original nontwisted lattice.

We can form a $2n$-dimensional lattice from two $n$-dimensional lattices $\Lambda_1$ and $\Lambda_2$ by tensoring. Let $\alpha_1 \in K_1$ and $\alpha_2 \in K_2$ be the possible totally positive twisting elements, respectively. The volume of the tensored lattice is

$$\mathrm{Vol}(\Lambda_{\alpha_1} \otimes \Lambda_{\alpha_2}) = N_{K_1/\mathbb{Q}}(\alpha_1) N_{K_2/\mathbb{Q}}(\alpha_2) \mathrm{Vol}(\Lambda_1)^2 \mathrm{Vol}(\Lambda_2)^2.$$

Let us then denote by $(r_1, r_2)$ the *signature* of $K$, *i.e.*,

$$[K : \mathbb{Q}] = n = r_1 + 2r_2,$$

where $r_1$ is the number of real embeddings $K \hookrightarrow \mathbb{R}$ and $r_2$ is the number of conjugate pairs or imaginary embeddings $K \hookrightarrow \mathbb{C}$. The group $\mathcal{O}_K^\times$ of units of $\mathcal{O}_K$ is described by the following well-known theorem, repeated here for the ease of reading.

*Theorem 2.1:* ([10, Dirichlet Unit Theorem 1.9]) Let $K$ be a number field and let $(r_1, r_2)$ be the signature of $K$. There are units $\epsilon_1, \ldots, \epsilon_{r_1+r_2+1} \in \mathcal{O}_K^\times$ such that

$$\begin{aligned} \mathcal{O}_K^\times &\cong \mathcal{W}_K \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_{r_1+r_2-1} \rangle \\ &\cong \mathcal{W}_K \times \mathbb{Z}^{r_1+r_2-1}, \end{aligned}$$

where $\mathcal{W}_K$ is the group of roots of units in $K$. The $\epsilon_j$ are called a *fundamental system of units* for $K$.

The fundamental units are used for defining the *regulator* of $K$. Let $\{\epsilon_1, \ldots, \epsilon_r\}$ be a fundamental system of units for $K$, where $r = r_1 + r_2 - 1$. Consider a matrix

$$A = (\log |\sigma_j(\epsilon_i)|_j)$$

for $1 \leq i \leq r$ and $1 \leq j \leq r_1 + r_2$, and where we have used the notation

$$|x|_j = \begin{cases} |x| & \text{if } 1 \leq j \leq r_1, \\ |x|^2 & \text{if } r_1 \leq j \leq r_1 + r_2. \end{cases}$$

Here $|x|$ is the usual absolute value of on $\mathbb{C}$, and $\sigma_1, \ldots, \sigma_{r_1}$ are all the real embeddings, while $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ are a set of representatives of the imaginary embeddings.

*Definition 2.5:* The *regulator* $R_K$ is the absolute value of the determinant of any $r \times r$ minor of $A$. It is independent of the choice of the fundamental system of units.

The regulator is a positive real number that in essence tells us how dense the units are. The smaller the regulator, the denser the units. Regulators can be easily computed by the Sage computer software [11].

Let us conclude this section by defining the Dedekind zeta function.

*Definition 2.6:* The *Dedekind zeta function* (cf. [10, p. 37]) of a field $K$ is defined as

$$\zeta_K(s) = \sum_{\mathcal{I} \subseteq \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathcal{I})^s}, \tag{1}$$

where $\mathcal{I}$ runs through the nonzero integral ideals of $\mathcal{O}_K$. The sum converges for $\Re(s) > 1$. Since $N_{K/\mathbb{Q}}(\mathcal{O}_K) = 1$, we always have

$$\zeta_K(s) > 1.$$

From now on, we assume $2 \leq s \in \mathbb{Z}$ since these are the interesting values for the applications under study in this paper.

The Dedekind zeta function can be written as a *Dirichlet series*

$$\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

where $a_n = 0$ for those $n$ that do not appear as a norm of an integral ideal.

Also the zeta functions as well as the Dirichlet coefficients $a_n$ can be computed by Sage [11].

*Remark 2.2:* When we derive probability bounds for lattice codes with the aid of zeta functions, we need to use the same normalization for the zeta function as used for the lattice code. Otherwise the comparison of the two norm sums under observation (see (1) and (4)) will be meaningless. Keeping this in mind, let us define the scaled zeta function for later use.

*Definition 2.7:* The *normalized Dedekind zeta function* is denoted and defined as

$$N\zeta_K(s) = \frac{1}{\rho^{ns} N_{K/\mathbb{Q}}(\alpha)^{s/2}} \sum_{\mathcal{I} \subseteq \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathcal{I})^s},$$

where $\rho \in \mathbb{R}$ is a real scaling factor such that $\mathrm{Vol}(\rho\Lambda_\alpha) = 1$.

This normalized zeta function will then be comparable to the norm sum (4) related to the lattice $\rho\Lambda_\alpha$ of volume 1. Also the normalized zeta functions corresponding to different lattices can be meaningfully compared to each other.

## III. Coset coding

In a wiretap channel, Alice is transmitting confidential data to the intended receiver Bob over a fading channel, while an eavesdropper Eve tries to intercept the data received over another fading channel. The security is based on the assumption that Bob's SNR is sufficiently large compared to Eve's SNR. In addition, a coset coding strategy [12] is employed in order to confuse Eve. In coset coding, random bits are transmitted in addition to the data bits as follows.

Let us denote the lattice intended to Bob by $\Lambda_b$, and by $\Lambda_e \subset \Lambda_b$ a sublattice embedding the random bits. Now the transmitted codeword $\mathbf{x}$ is picked from a certain coset $\Lambda_e + \mathbf{c}$ belonging to the disjoint union

$$\Lambda_b = \cup_{j=1}^{2^k} \Lambda_e + \mathbf{c_j}$$

embedding $k$ bits:

$$\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_e + \mathbf{c},$$

where $\mathbf{r}$ embeds the random bits, and $\mathbf{c}$ contains the data bits.

We assume the fading is Rayleigh distributed and that both Bob and Eve have perfect channel state information (CSI). We do not repeat the channel model nor the probability calculations here, but refer to [5] for more details.

## IV. On the size of Eve's inverse norm power sum in a fast Rayleigh fading wiretap channel

Let us now look at the fast fading wiretap channel and analyze the behavior of the probability of Eve's correct decision in some example cases[1]. This will give us a preliminary understanding as to what are the key properties affecting the secrecy gained by lattice coding.

### A. The probability expression and the inverse norm power sum

We start by recalling the expression $P_{c,e}$ for the probability of a correct decision for Eve, when observing a lattice $\Lambda_e$. For the fast fading case [5, Sec. III-A],

$$P_{c,e} \simeq \left(\frac{1}{4\gamma_e^2}\right)^{n/2} \mathrm{Vol}(\Lambda_b) \sum_{0\neq\mathbf{x}\in\Lambda_e} \prod_{i=1}^{n} \frac{1}{|x_i|^3}, \qquad (2)$$

where $\gamma_e$ is the average SNR for Eve assumed sufficiently large so that Eve can perfectly decode $\Lambda_e$. This is a reasonable assumption, as Eve is assumed to have perfect CSI. Here $\Lambda_b$ denotes the lattice intended to Bob, and $\Lambda_e \subset \Lambda_b$. It can be concluded from (2) that the smaller the sum

$$\sum_{0\neq\mathbf{x}\in\Lambda_e} \prod_{i=1}^{n} \frac{1}{|x_i|^3},$$

the more confusion Eve is experiencing.

[1]Part of this section has been submitted to ITW 2011 [6].

As a construction method, the authors of [5] propose to use the canonical embedding of the ring of integers $\mathcal{O}_K$ (or a suitable proper ideal $\mathcal{I} \subset \mathcal{O}_K$) of a totally real number field $K$ over $\mathbb{Q}$. The field $K$ is chosen totally real to achieve full diversity. More precisely, if $x \in \mathcal{O}_K$, the transmitted lattice vector in the fast fading case would be

$$\mathbf{x} = \psi(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)) \in \Lambda_e \subset \mathbb{R}^n, \qquad (3)$$

where $\psi$ denotes the canonical embedding (cf. Def. 2.3) and $\sigma_i$ are the (now all real) embeddings of $K$ into $\mathbb{R}$. The corresponding probability of Eve's correct decision (2) yields the following *inverse norm power sum* to be minimized [5, Sec. III-B]:

$$S_M = \sum_{0\neq x\in\mathcal{O}_K} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}, \qquad (4)$$

where $M$ denotes the generator matrix of the lattice $\Lambda_e$.

*Remark 4.1:* The above sum $S_M$ may not converge, since infinitely many elements can have the same norm. This happens *e.g.* when the unit group is infinite, which is the case for all field extensions other than the trivial one and imaginary quadratic fields. In practice, however, we always consider finite signaling alphabets, so the sum becomes truncated and converges.

### B. Example constructions and analysis on the sum $S_M$

In this section, we describe five alternative constructions for the fast fading channel built from different number fields and their ideals. Optimal and nearly optimal unitary lattice generator matrices in terms of the minimum product distance (cf. Def. 2.2) are provided in [13]. We will first analyze the ones with degree $n = 4$, denoted here by $\Lambda_1$ and $\Lambda_2$, with the respective unitary (*i.e.*, $MM^T = I_4$) generator matrices $M_1$ ([13, optimal, $M_1 = \mathrm{krus\_4}$ ]) and $M_2$ ([13, suboptimal, $M_2 = \mathrm{mixed\_2x2}$]). The first construction corresponds to the canonical embedding of $\mathcal{O}_{\mathbb{Q}(\delta)}$, where $\delta^4 - \delta^3 - 3\delta^2 + \delta + 1 = 0$. The second construction is based on the Kronecker product of the lattice generator matrices corresponding to the canonical embeddings of the rotated $\mathbb{Z}^2$ lattices $\alpha_1\mathbb{Z}[\sqrt{2}]$ and $\alpha_2\mathbb{Z}[\theta]$, where $\theta = \frac{1+\sqrt{5}}{2}$, $\alpha_1 = \frac{1}{2\sqrt{2}+4}$ and $\alpha_2 = 3 - \theta$. Both lattices are rotated versions of $\mathbb{Z}^4$ with full diversity and good minimum product distances,

$$Nd_{p,min}(\Lambda_1) = \frac{1}{\sqrt{5^2 \cdot 29}} \approx 0.037139...$$

and

$$Nd_{p,min}(\Lambda_1) = \frac{1}{40} \approx 0.025.$$

See [9, Sec. 7] for a fully worked out example.

We use finite constellations $\mathcal{S}_m$ constructed by taking a square box with a zero mean within the lattice, *i.e.*,

$$\mathbf{x} \in \mathcal{S}_m = \left\{ \sum_{i=1}^{n} z_i x_i \;\middle|\; z_i \in \mathbb{Z}, |z_i| \leq m \right\} \subset \Lambda_e.$$

This will then give us a natural energy limit $P_{lim} = P_{max} = ||\sum_{i=1}^{n} m x_i||_E^2$ as well. Note that for nonorthogonal lattices,

we may want to have

$$P_{lim} < \max\left\{ ||\sum_{i=1}^{n} z_i x_i||_E^2 \;\middle|\; |z_i| \leq m \right\}$$

in order to achieve a spherical constellation.

Let us now compare these two (finite) orthogonal constructions by computing truncated sums

$$S_M(P_{lim}) = \sum_{0 \neq \mathbf{x} \in \Lambda_e, ||\mathbf{x}||_E^2 \leq P_{lim}} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3} \qquad (5)$$

for a given power limit $P_{lim}$. We may emphasize the finite constellation $\mathcal{S}_m$ in use by writing $S_M(P_{lim}, m)$, especially for a skewed lattice. In the above sum, $\mathbf{x} = (x_1, \ldots, x_n) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x))$, where $x \in \mathcal{O}_K$ or $x \in \mathcal{I} \subset \mathcal{O}_K$. For a fair comparison, the lattices are normalized to unit energy, *i.e.*, to have $\mathrm{Vol}(\Lambda_e) = 1$. The volumes of the corresponding superlattices $\Lambda_b$ of Bob will then scale accordingly.

TABLE I
VALUES OF $S_M(P_{lim})$ FOR ORTHOGONAL LATTICES ($n = 4$) WITH $P_{lim} = P_{max}$ AND WITH A CODEBOOK SIZE $|\mathcal{C}_{ort}| = (2m+1)^4$.

| $m$ | $P_{max}$ | $P_{ave}$ | $S_{M_1}(P_{lim})$ | $S_{M_2}(P_{lim})$ |
|---|---|---|---|---|
| 1 | 4 | 2.67 | $9.12264 \cdot 10^7$ | $2.83706 \cdot 10^6$ |
| 2 | 16 | 8.00 | $2.24565 \cdot 10^{10}$ | $6.46037 \cdot 10^6$ |
| **3** | **36** | **16.00** | $\mathbf{2.49382 \cdot 10^{11}}$ | $\mathbf{1.16395 \cdot 10^7}$ |
| 4 | 64 | 26.67 | $2.49829 \cdot 10^{11}$ | $1.52838 \cdot 10^7$ |
| 5 | 100 | 40.00 | $2.49851 \cdot 10^{11}$ | $1.99487 \cdot 10^7$ |
| 6 | 144 | 56.00 | $2.50437 \cdot 10^{11}$ | $2.38188 \cdot 10^7$ |
| 7 | 196 | 74.67 | $2.61395 \cdot 10^{11}$ | $2.69652 \cdot 10^7$ |
| 8 | 256 | 96.00 | $2.61736 \cdot 10^{11}$ | $3.00791 \cdot 10^7$ |
| 9 | 324 | 120.00 | $2.61739 \cdot 10^{11}$ | $3.42272 \cdot 10^7$ |
| 10 | 400 | 146.67 | $2.71764 \cdot 10^{11}$ | $3.68287 \cdot 10^7$ |

In Table I we have listed the inverse norm power sums for fixed constellations $\mathcal{S}_n$, that is, the codebook will be of size $|\mathcal{C}_{ort}| = (2m+1)^4$. The maximum energies $P_{max}$ used by the constellations are also provided ($P_{lim} = P_{max}$).

From Table I we can make the following important conclusion. In terms of the pairwise error probability (PEP) for Bob as the intended legitimate receiver, the optimal lattice is known to provide asymptotically the best performance. However, non-asymptotically and from the secrecy point of view the suboptimal lattice may provide significantly improved secrecy by causing more confusion to the eavesdropper Eve. This is due to a secondary code design criterion related to the distribution of the norms (usually showing its PEP effect at the low SNR regime), which obviously plays an important role also in the wiretap scenario (cf. (4)).

Next, we extend our analysis by computing the inverse norm power sums for a skewed lattice, denoted by $\Lambda_3$, corresponding to the maximal real subfield

$$\mathbb{Q}(\tau = \zeta_{15} + \zeta_{15}^{-1})$$

of the 15th cyclotomic field. Here $\tau$ satisfies

$$\tau^4 - \tau^3 - 4\tau^2 + 4\tau + 1 = 0.$$

The generator matrix is denoted by $M_3$. The minimum product distance of this lattice is

$$Nd_{p,min}(\Lambda_3) = \frac{1}{\sqrt{1125}} \approx 0.02981...$$

putting it in between the lattices $\Lambda_1$ and $\Lambda_2$ in terms of $Nd_{p,min}(\Lambda)$. From Table II, we can conclude that skewed lattices may significantly increase the secrecy compared to orthogonal lattices. One has to notice, however, that this bares the price of increased complexity as we need to carve spherical codebooks by using a bigger alphabet in order to get the possible benefits. More precisely, we only choose the codewords in the set $\{\mathbf{x} \in \Lambda_e \cap \mathcal{S}_m \,|\, ||x||_E^2 \leq P_{lim}\}$. Hence, in order to achieve the same size of a codebook that we would have without an additional energy limit, we may need to increase $m$ (see *e.g.* the boldface lines in Table II). The bigger the $m$, the closer we get to a spherical constellation with a given energy limit. In other words, in the table below, the values $m$ are smaller for the orthogonal lattices than those used for the skewed lattice. The true maximum energies consumed by the spherical constellation are also provided in Table II.

TABLE II
VALUES OF $S_M(P_{lim}, m)$ FOR A SKEWED LATTICE ($n = 4$) WITH BOUNDED ENERGY.

| $m$ | $P_{lim}$ | $P_{max}$ | $P_{ave}$ | $\lvert\mathcal{C}_{sph}\rvert$ | $\lvert\mathcal{C}_{ort}\rvert$ | $S_{M_3}(P_{lim}, m)$ |
|---|---|---|---|---|---|---|
| 8 | 4 | 3.63 | 2.66 | 79 | 81 | $1.89195 \cdot 10^6$ |
| 5 | 16 | 15.71 | 9.18 | 555 | 625 | $4.24298 \cdot 10^6$ |
| 6 | 16 | 15.71 | 9.56 | 715 | 625 | $4.77423 \cdot 10^6$ |
| **7** | **36** | **35.57** | **20.33** | **2405** | **2401** | $\mathbf{7.13024 \cdot 10^6}$ |
| **12** | **36** | **24.00** | **15.24** | **2401** | **2401** | $\mathbf{2.29374 \cdot 10^6}$ |
| 9 | 64 | 63.89 | 35.67 | 6929 | 6561 | $9.93903 \cdot 10^6$ |
| 10 | 100 | 99.97 | 55.72 | 13663 | 14641 | $1.20680 \cdot 10^7$ |
| 11 | 100 | 99.97 | 55.57 | 16053 | 14641 | $1.29038 \cdot 10^7$ |
| 14 | 196 | 195.98 | 106.63 | 50975 | 50625 | $1.29038 \cdot 10^7$ |
| 18 | 324 | 323.93 | 175.95 | 137273 | 130321 | $2.18703 \cdot 10^7$ |
| 20 | 400 | 399.90 | 217.31 | 208411 | 194481 | $2.40716 \cdot 10^7$ |

Note that we have normalized the lattices to a unit volume (corresponding to a unit minimum energy in the orthogonal case), whereas to compare the full probability expressions (2) we should normalize the SNR term rather with respect to a unit average energy. For comparison purposes, this makes no difference for orthogonal lattices as the average energies are directly determined by the signaling alphabet and not affected by the generator matrices, so the scaling factors will coincide. However, in the case of skewed lattices the situation is different, and the average energy has an input coming from the generator matrix in addition to the alphabet. This may loosen our conclusion related to skewed lattices to some extend. We studied this effect in the case of maximum energy/energy limit 36 (see the boldfaced lines in Table I and Table II). We can see that the skewed lattice can achieve even better energy distribution than the orthogonal ones, when $m$ is chosen sufficiently large. Unfortunately, the bigger the $m$, the higher the complexity. Further analysis will be carried out in the forthcoming journal version [14] of this paper.

Finally, we compare two orthogonal 6-dimensional lattices generated by $M_4$ ([13, optimal, $M_4$ = mixed_2x3]) and $M_5$ ([13, suboptimal, $M_5$ = cyclo_6]). The corresponding

minimum product distances are

$$Nd_{p,min}(\Lambda_4) = \frac{1}{\sqrt{5^3 \cdot 7^4}} \approx 0.001825...$$

and

$$Nd_{p,min}(\Lambda_5) = \frac{1}{13^{5/2}} \approx 0.001641....$$

From Table III we can see that in this case, the optimal lattice also provides smaller sums up to $m = 3$. For $m = 4$, it is again the suboptimal lattice who attains the smallest value. Higher values of $m$ will be again studied in the forthcoming journal version [14] of this paper.

TABLE III
VALUES OF $S_M(P_{lim})$ FOR ORTHOGONAL LATTICES ($n = 6,\ P_{lim} = P_{max}$) WITH A CODEBOOK SIZE $|\mathcal{C}_{ort}| = (2m+1)^6$.

| $m$ | $P_{max}$ | $P_{ave}$ | $S_{M_4}(P_{lim})$ | $S_{M_5}(P_{lim})$ |
|---|---|---|---|---|
| 1 | 6 | 4 | $6.90525 \cdot 10^{10}$ | $8.95995 \cdot 10^{10}$ |
| 2 | 24 | 12 | $3.09812 \cdot 10^{11}$ | $3.88309 \cdot 10^{11}$ |
| 3 | 54 | 24 | $6.89391 \cdot 10^{11}$ | $8.77134 \cdot 10^{11}$ |
| 4 | 96 | 40 | $\mathbf{1.45141 \cdot 10^{12}}$ | $\mathbf{1.38502 \cdot 10^{12}}$ |

## V. On the size of Eve's inverse norm power sum in a block Rayleigh fading wiretap channel

For the block fading case [5, Sec. IV-A], the probability of Eve's correct decision becomes

$$P_{c,e} \simeq \left(\frac{\Gamma(L/2+1)}{(2\pi)^{L/2}\gamma_e}\right)^n \mathrm{Vol}(\Lambda_b) \sum_{0 \neq \mathbf{x} \in \Lambda_e} \prod_{i=1}^{n} \frac{1}{||x_i||_E^{L+2}}, \quad (6)$$

where $L$ is the coherence time. This time, the authors propose to use $L$ independent columns coming from the canonical embedding of a field $K$ in order to transmit a vectorized form of the matrix $X$:

$$X = (\mathbf{x}_1^T \ \cdots \ \mathbf{x}_L^T)_{n \times L}, \quad (7)$$

*i.e.*, $\mathbf{x}_i = (\sigma_1(x_i), \cdots, \sigma_n(x_i)) \in \mathbb{R}^n$ are as in (3). Applying (6) here, we should minimize the sum [5, Sec. IV-B]

$$\sum_{0 \neq \mathbf{x} \in \Lambda_e} \frac{1}{N_{K/\mathbb{Q}}\left(||\mathbf{y}||_E^2\right)^{L/2+1}}, \quad (8)$$

where the transmitted vector $\mathbf{x} = \mathrm{vec}(X) \in \Lambda_e \subset \mathbb{R}^{nL}$ is the vectorized matrix $X$ and $\mathbf{y}$ is the first row of $X$. See [5, Sec. IV] for more details.

We denote by

$$BS_M(P_{lim}) = \sum_{0 \neq \mathbf{x} \in \Lambda_e, ||\mathbf{x}||_E^2 \leq P_{lim}} \frac{1}{N_{K/\mathbb{Q}}\left(||\mathbf{y}||_E^2\right)^{L/2+1}}$$

the truncated version of the block sum.

In Table IV, we have listed the values of $BS_M(P_{lim})$ for two 4-dimensional lattices with $n = L = 2$. The corresponding lattice generator matrices are formed by using optimal/suboptimal $2 \times 2$ generator matrices as diagonal blocks in the $4 \times 4$ generator matrices $M_6$ and $M_7$. See ([13, optimal, cyclo_2, ideal_2]) for more details. According to Table IV, the optimal lattice provides smaller values for the block sum as well.

TABLE IV
VALUES OF $BS_M(P_{lim})$ FOR ORTHOGONAL LATTICES ($n = L = 2,\ P_{lim} = P_{max}$) WITH A CODEBOOK SIZE $|\mathcal{C}_{ort}| = (2m+1)^4$.

| $m$ | $P_{max}$ | $P_{ave}$ | $BS_{M_1}(P_{lim})$ | $BS_{M_2}(P_{lim})$ |
|---|---|---|---|---|
| 1 | 4 | 2.67 | 454.44 | 602.69 |
| 2 | 16 | 8.00 | 696.25 | 1175.07 |
| 3 | 36 | 16.00 | 933.47 | 1228.67 |
| 4 | 64 | 26.67 | 938.06 | 1235.60 |
| 5 | 100 | 40.00 | 1173.47 | 1801.27 |
| 6 | 144 | 56.00 | 1176.64 | 1802.55 |
| 7 | 196 | 74.67 | 1178.26 | 1854.47 |
| 8 | 256 | 96.00 | 1413.41 | 1855.67 |
| 9 | 324 | 120.00 | 1413.81 | 1856.81 |
| 10 | 400 | 146.67 | 1416.71 | 1862.50 |

## VI. Bounds for the eavesdropper's probability of correct decision

In this section, we will derive lower and upper bounds for the inverse norm power sum in the probability expression for the fast fading channel by using the Dedekind zeta functions (cf. Def. 2.6).

For $x \in \mathcal{O}_K$, we trivially have that $S_M > 1$ as $1 \in \mathcal{O}_K$. Albeit straightforward, the following result gives us a nontrivial lower bound $\neq 1$ for the sum $S_M$. Note that in the proposition below, we do not require $K$ to be totally real. See Remark 6.1 following the proof for explanation.

*Proposition 6.1:* (Lower Bound) Assume that $\mathcal{O}_K$ is a principal ideal domain (PID) and $\Lambda_e$ is as above with $x \in \mathcal{O}_K$. Prior to normalization of the lattice, the Dedekind zeta function $\zeta_K(s)$ evaluated at $s = 3$ provides us with a lower bound for $S_M$, *i.e.*,

$$S_M > \zeta_K(3) > 1.$$

More interestingly, if $P_{lim}$ is sufficiently large, the same holds for the truncated sums,

$$S_M(P_{lim}, N) > \zeta_K(3, N) > 1,$$

where $N$ denotes the maximum norm included in the sum; $|N_{K/\mathbb{Q}}(x)| \leq N$ and $N_{K/\mathbb{Q}}(\mathcal{I}) \leq N$.

*Proof:* Note that $N_{K/\mathbb{Q}}(\mathcal{I}) = [\mathcal{O}_K : \mathcal{I}] \in \mathbb{Z}_+$, and that in the zeta function the summation only goes through the (integral) ideals of $\mathcal{O}_K$, whereas in $S_M$ we sum over all the algebraic integers of $K$.

Let us denote by

$$S_M = \sum_{n \geq 1} \frac{b_n}{n^3} \quad \text{and} \quad \zeta_K(3) = \sum_{n \geq 1} \frac{a_n}{n^3}$$

the Dirichlet series [10, p. 31] of $S_M$ and $\zeta_K(3)$. Denote further by

$$A = \{n \,|\, a_n \neq 0\} \subseteq \mathbb{Z}_+$$

the set of values $n$ that appear as norms in $\zeta_K(3)$, and by

$$B = \{n \mid b_n \neq 0\} \subseteq \mathbb{Z}_+$$

the set of values that appear as norms in $S_M$. As $K$ is a PID, we know that $N_{K/\mathbb{Q}}(\mathcal{I}) = \min_{0\neq x\in\mathcal{I}} |N_{K/\mathbb{Q}}(x)|$, and that $N_{K/\mathbb{Q}}(\mathcal{I}) = N_{K/\mathbb{Q}}((\alpha)) = N_{K/\mathbb{Q}}(\alpha)$, where $\alpha$ is the generator of $\mathcal{I}$. Hence, we have that

$$A = B.$$

Further, we easily see that $b_n \geq a_n$. Namely, if $n$ appears as a norm for distinct ideals $\mathcal{I}_i = (\alpha_i)$, $i = 1, \ldots, a_n$, it then appears as a norm at least for the (distinct) elements $\alpha_i \in \mathcal{O}_K$. In addition, we may have an element $\alpha \in \mathcal{O}_K$, $\alpha \neq \alpha_i\, \forall i$ with the same norm $n$. On the other hand, if $n$ appears as a norm for distinct elements $\alpha_i \in \mathcal{O}_K$, $i = 1, \ldots, b_n$, it cannot appear as a norm for an ideal for more than $a_n = b_n$ times, since $\mathcal{O}_K$ is a PID. This proves the claimed lower bound for the infinite sums.

The truncated sums generally need not satisfy the same inequation, where we truncate by setting $n \leq N$, $N \in \mathbb{Z}$ with the same $N$ for both sums. Due to the finiteness of the constellation and hence the maximum power in use, we might be missing some terms in $S_M$ that do satisfy the norm boundary. This can be overcome by increasing the energy limit (and the constellation size) as required. Hence, with $m$ and $P_{lim}$ sufficiently large, we get the same inequality for the truncated sums. ∎

*Remark 6.1:* According to Dirichlet's Unit Theorem (cf. Prop. 2.1) the rank of the group of units in $\mathcal{O}_K$ is $r = r_1 + r_2 - 1$, where $(r_1, r_2)$ is the signature of $K$, that is, $n = r_1 + 2r_2$. Therefore the infinite sum $S_M$ does not converge for totally real number fields $\supsetneq \mathbb{Q}$ ($r_1 > 1$), as they have an infinite unit group (cf. Remark 4.1). Hence, in this application case where $K$ is totally real, we always need to consider truncated sums to make any sense to the above bound. This is totally fine, as in practice the constellations are finite anyway.

*Remark 6.2:* Dedekind zeta functions have also been used in [7] for studying the DMT of the multiple-access channel (MAC). Interesting subsequent work has been carried out in [8].

Next, let us denote by

$$S_M(P_{lim}, N) = \sum_{n\leq N} \frac{b'_n}{n^3},$$

the truncated sum, where $b'_n \neq 0$ for those $n$ that appear as a norm for $x \in \mathcal{O}_K$, $||x||_E^2 \leq P_{lim}$. An upper bound for the truncated sum is achieved from the truncated Dedekind zeta function $\zeta_K(s, N)$ evaluated at $s = 3$.

*Proposition 6.2:* (Upper Bound) Let $\mathcal{O}_K$ be a PID. Then we have that

$$S_M(P_{lim}, N) \leq \max\{b'_n \,|\, n \leq N\} \cdot \zeta_K(3, N).$$

*Proof:* First, note that if $a_n = 0$, then $b_n = 0$ and hence $b'_n = 0$ since $\mathcal{O}_K$ is a PID. Now a simple computation gives us

$$\begin{aligned} S_M(P_{lim}, N) &= \sum_{n\leq N, 0\neq\mathbf{x}\in\Lambda_e, ||\mathbf{x}||^2\leq P_{lim}} \frac{b'_n}{n^3} \\ &\leq \max\{b'_n \,|\, n \leq N\} \sum_{b'_n\neq 0, n\leq N, 0\neq\mathbf{x}\in\Lambda_e, ||\mathbf{x}||^2\leq P_{lim}} \frac{1}{n^3} \\ &\leq \max\{b'_n \,|\, n \leq N\} \cdot \zeta_K(3, N). \end{aligned}$$

In the second step, the summation is only taken over the values of $n$ for which $b'_n \neq 0$, *i.e.*, $n$ appears as a norm for some element $x$. Hence, for all the terms $1/n^3$ included in the sum $a_n \neq 0$. In addition to this, the truncated zeta sum may contain other terms (for which $b_n \neq 0$ but $b'_n = 0$ due to the energy limit) so we indeed get an upper bound. ∎

Finally, let $\mathbf{x} = (\sigma_1(x), \ldots, \sigma_n(x))$, $x \in \mathcal{O}_K$, and assume that we have set the energy limit to

$$||\mathbf{x}||_E^2 \leq P_{lim} = R^2.$$

Then we can show (see [7] for the proof) the following:

*Proposition 6.3:* Assume $K$ is a PID. Then there exists a constant $T$ independent of $R$ such that

$$S_M(P_{lim} = R^2) \leq T \log(R)^{n-1}.$$

*Remark 6.3:* We anticipate that the above bounds are not very tight. The next step is to derive tighter bounds arising from geometric analysis. The results will be reported in a forthcoming paper.

## VII. An upper bound for the pairwise error probability

Similar analysis can be used to get bounds for the pairwise error probability for the fast fading channel when employing the same number field code as in (3). Let us use the following Dirichlet series notation for the PEP (see *e.g.* [9]),

$$P_e = C(SNR) \sum_{0\neq x\in\mathcal{O}_K} \frac{1}{|N_{K/\mathbb{Q}}(x)|^2} = C(SNR) \sum_{n\geq 1} \frac{c_n}{n^2},$$

where $C(SNR)$ is a constant depending on the SNR. We shortly denote

$$S_{M,PEP} = \sum_{n\leq N, ||x||_E^2\leq P_{lim}} \frac{c'_n}{n^2}.$$

Again, let us assume that $\mathcal{O}_K$ is a PID, *i.e.*, $a_n = 0 \Leftrightarrow c'_n = 0$. Adopting the same notation as in the wiretap case, we get the following bounds. The proof is analogous to the wiretap case.

*Proposition 7.1:* When $K$ is a PID, we have that

$$S_{M,PEP}(P_{lim}, N) \leq \max\{c'_n \,|\, n \leq N\} \cdot \zeta_K(2, N)$$

and, provided that the constellation size and hence $P_{lim}$ are sufficiently large,

$$S_{M,PEP}(P_{lim}, N) > \zeta_K(2, N).$$

*Example 7.1:* Finally, we compute the regulators and the zeta functions for the 4-dimensional example fields.

For the optimal orthogonal lattice,

$$R_{\mathbb{Q}(\delta)} = 0.825068847934757,$$

$$\zeta_{\mathbb{Q}(\delta)}(3) = 1.00228959689242,$$

$$\zeta_{\mathbb{Q}(\delta)}(2) = 1.03693298807624.$$

For the suboptimal orthogonal lattice,

$$R_{\mathbb{Q}(\sqrt{2},\sqrt{5})} = 1.54250590983349,$$

$$\zeta_{\mathbb{Q}(\sqrt{2},\sqrt{5})}(3) = 1.01897545804910,$$

$$\zeta_{\mathbb{Q}(\sqrt{2},\sqrt{5})}(2) = 1.10699528520823.$$

For the skewed lattice,

$$R_{\mathbb{Q}(\tau)} = 1.16545519432417,$$

$$\zeta_{\mathbb{Q}(\tau)}(3) = 1.01004731094107,$$

$$\zeta_{\mathbb{Q}(\tau)}(2) = 1.07289917862490.$$

The normalized zeta functions in the wiretap case (the PEP case is analogous, cf. Def. 2.7) are, respectively,

$$N\zeta_{\mathbb{Q}(\delta)}(3) = \frac{1}{\rho^{12} N_{K/\mathbb{Q}}(\alpha)^{3/2}} \cdot 1.00228959689242 \overset{\rho=\frac{1}{\sqrt[8]{5^2\cdot 29}}, N(\alpha)=1}{=} 19565.9\,,$$

$$N\zeta_{\mathbb{Q}(\sqrt{2},\sqrt{5})}(3) = \frac{1}{\rho^{12} N_{K/\mathbb{Q}}(\alpha)^{3/2}} \cdot 1.01897545804910 \overset{\rho=\frac{1}{\sqrt{5}}, N(\alpha)=\frac{1}{8}}{=} 360262\,,$$

$$N\zeta_{\mathbb{Q}(\tau)}(3) = \frac{1}{\rho^{12} N_{K/\mathbb{Q}}(\alpha)^{3/2}} \cdot 1.01004731094107 \overset{\rho=\frac{1}{\sqrt[8]{1125}}, N(\alpha)=1}{=} 38112.8\,.$$

A nice feature of this example is that the normalized zeta functions are ordered with respect to the minimum product distances. There is however no guarantee at this point that this would hold more generally.

## VIII. Conclusions and future work

We studied the inverse norm power sums arising from the probability of Eve's correct decision in a wiretap channel as well as from the pairwise error probability. In the wiretap case, the sum was studied both in the fast and block Rayleigh fading case, based on well-known number field lattice codes. Most of the example codes were based on the full diversity rotations of $\mathbb{Z}^n$. For the fading case, we further provided lower and upper bounds for the norm sums arising from Dedekind zeta functions. Dedekind zeta functions can also be exploited in the context of DMT, as shown in other recent works.

It was pointed out that, in some cases, using a performance-wise suboptimal lattice may in a suitable SNR range significantly enhance the secrecy. Secrecy may also be increased by using skewed lattices, but at a cost of increased complexity.

Our next goal is to find out through simulations whether Bob's pairwise error probabilities and/or Eve's probabilities of correct decision for different lattice codes are ordered according to their normalized zeta functions. This would be a nice result, as even though the bounds were not that tight, they would still predict the performance order, if not the performance itself. The examples in the paper indeed indicate that this may well be the case at least for the PEP.

The analysis carried out in this paper will be extended to complex lattices as well. We will also try to derive tighter bounds arising from geometric ananlysis. Here we have studied the norm sums detached from the probability expression by normalizing the lattice to a unit volume. It is probably worthwhile to study the whole probability expression and the required normalization to properly do that.

## Acknowledgments

The research of C. Hollanti is supported by the Emil Aaltonen Foundation's Young Researcher's Project, and by the Academy of Finland (grant #131745).

Dr. Roope Vehkalahti is gratefully acknowledged for useful discussions.

## References

[1] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451 – 456, jul 1978.

[2] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap gaussian channel: Construction and analysis," submitted to *IEEE Trans. Inf. Theory*, 2011, arxiv.org/abs/1103.4086.

[3] J.-C. Belfiore and P. Solé, "Unimodular lattices for the gaussian wiretap channel," CoRR, abs/1007.0449, 2010.

[4] J.-C. Belfiore and F. E. Oggier, "Secrecy gain: A wiretap lattice code design," in *ISITA*, 2010, pp. 174–178.

[5] J.-C. Belfiore and F. Oggier, "Lattice code design for the rayleigh fading wiretap channel," in *ICC 2011*, 2011, arxiv.org/pdf/1012.4161.

[6] A.-M. Ernvall-Hytnen and C. Hollanti, "On the eavesdropper's correct decision in gaussian and fading wiretap channels using lattice codes," submitted to IEEE ITW 2011, arxiv.org/abs/1106.2756.

[7] R. Vehkalahti and H.-F. F. Lu, "An algebraic look into MAC-DMT of lattice space-time codes," in *Proc. IEEE ISIT 2011*, to appear.

[8] ——, "Diversity-multiplexing gain tradeoff: a tool in algebra?" submitted to IEEE ITW 2011.

[9] F. Oggier and E. Viterbo, "Algebraic number theory and code design for rayleigh fading channels," *Commun. Inf. Theory*, vol. 1, no. 3, pp. 333–416, 2004.

[10] N. Childress, *Class Field Theory*. Springer Universitext, New York, 2009.

[11] "Sage open source mathematics software system." [Online]. Available: http://www.sagemath.org/

[12] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, 1975.

[13] E. Viterbo, optimal rotations for number field lattices. [Online]. Available: http://www1.tlc.polito.it/ viterbo/rotations/rotations.html
[14] C. Hollanti and E. Viterbo, "Probability bounds for wiretap lattice codes based on dedekind zeta functions and geometric analysis," 2011, manuscript.