Karrila, Alex; Hollanti, Camilla

A comparison of skewed and orthogonal lattices in Gaussian wiretap channels

Published in:
2015 IEEE Information Theory Workshop, ITW 2015

DOI:
10.1109/ITW.2015.7133106

Published: 24/06/2015

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

A Comparison of Skewed and Orthogonal Lattices in Gaussian Wiretap Channels

Alex Karrila and Camilla Hollanti, *Member, IEEE*
Department of Mathematics and Systems Analysis
Aalto University, Finland
Emails: firstname.lastname@aalto.fi

***Abstract*—We consider lattice coset-coded transmissions over a wiretap channel with additive white Gaussian noise (AWGN). Examining a function that can be interpreted as either the legitimate receiver's error probability or the eavesdropper's correct decision probability, we rigorously show that, albeit offering simple bit labeling, orthogonal nested lattices are suboptimal for coset coding in terms of both the legitimate receiver's and the eavesdropper's probabilities.**

I. Introduction

We consider a wiretap set-up, in which a message is transmitted to its legitimate receiver Bob in the presence of Eve the eavesdropper. Eve is assumed to have unlimited computational power, but to experience an additional noise compared to Bob. Lattice coset coding is utilized to maximize Eve's confusion, cf. [1], [2]. Bob's lattice is referred to as the code lattice or dense lattice, and Eve's lattice as the sparse or coarse lattice. The channel is assumed to exhibit additive white Gaussian noise (AWGN) but no fading. The respective channel equations for Bob and Eve are

$$\mathbf{y}_b = \mathbf{x} + \mathbf{n}_b, \quad \mathbf{y}_e = \mathbf{x} + \mathbf{n}_e,$$

where $\mathbf{y}$ is the received vector, $\mathbf{x}$ the transmitted coset-coded vector, and $\mathbf{n}$ is AWGN with respective variances $\sigma_b^2 < \sigma_e^2$.

In finding optimal lattice wiretap codes, there are three main objectives:

i) Maximizing the data rate R, which is determined by the size of the codebook $\mathcal{C}$ and the decoding delay n as
$$R = \frac{\log_2 |\mathcal{C}|}{n}$$
bits per channel use (bpcu).
ii) Minimizing the legitimate receiver's decoding error probability.
iii) Minimizing the eavesdropper's probability of correct decision.

Considering only the first two problems, the largest codebooks for a fixed transmission power and an upper bound for the receiver's error probability are the solutions to the widely investigated sphere-packing problem. This results in lattices that are typically nonorthogonal (see, e.g., [4]). Orthogonal lattices have still traditionally been preferred due to an easy-to-implement bit-labeling algorithm, namely the Gray-mapping. Due to this mapping, the encoding and decoding procedures are more straightforward for orthogonal lattices than for nonorthogonal, i.e., skewed lattices. Nevertheless, computationally efficient closest-point algorithms such as the sphere decoder also exist for nonorthogonal lattices (for an explicit construction, see [3], Sec. 4). In [5], [6], it was also demonstrated how skewed lattices can be efficiently encoded and decoded by using a modified power-controlled sphere decoder or sphere decoding adjoined with minimum-mean-square-error generalized-decision-feedback-equalization (MMSE-GDFE), both resulting in optimal (maximum-likelihood) performance. Hence, skewed lattices should not be excluded when searching for optimal lattices, in particular in the light of the present paper showing that they are not only better in terms of Bob's performance, but also in terms of confusing the eavesdropper.

Similarly to the sphere-packing problem in Bob's case, we now include the third objective in our consideration. Our approach is to fix the data rate and the transmission power and then compare skewed and orthogonal lattices from the point of view of the latter two objectives in an AWGN channel. We study an expression that has two alternative interpretations as either the receiver's error probability (REP) for any lattice code in an AWGN channel or the eavesdropper's correct decision probability (ECDP) for a lattice coset code in an AWGN channel. We prove the following results (notation will be defined in the subsequent section).

i) Skewing Bob's orthogonal code lattice Λ_b will decrease the REP of any code.
ii) Skewing Eve's orthogonal sparse lattice Λ_e will decrease the ECDP of any lattice coset code.
iii) Combining the previous two results, the common set-up of the dense lattice Λ_b being orthogonal and the commonly used choice of an orthogonal sublattice $\Lambda_e = 2^k\Lambda_b$ are suboptimal in terms of both the ECDP and the REP. According to whether Gray-labeling is insisted or not, this common set-up can be improved by either choosing a skewed sublattice of the same orthogonal dense lattice Λ_b, leaving Bob's lattice orthogonal and the REP suboptimal, or skewing both lattices.

These results suggest that skewed lattices deserve more attention in the study of the AWGN wiretap channels even though their encoding and decoding are admittedly somewhat more complicated than that of orthogonal lattices. It is also worthwhile to keep in mind that in any practical system, an

outer error correcting code, e.g., a low-density parity-check (LDPC) code, is used in addition to the inner lattice code. The true decoding bottle-neck in this case is the outer code requiring soft input, not the lattice code.

II. Preliminaries

In this section, we present some necessary definitions and their information-theoretic interpretations.

Definition 2.1: A *lattice* is a discrete additive subgroup of $\mathbb{R}^n$.

Any point in a lattice $\Lambda \subset \mathbb{R}^n$ can be expressed in terms of a *generator matrix* $M \in \mathbb{R}^{n\times m}$ as follows

$$\Lambda = \{\mathbf{x} \in \mathbb{R}^n | \mathbf{x} = M\omega, \omega \in \mathbb{Z}^m\}.$$

We assume that the columns of M are linearly independent over $\mathbb{Z}$ and hence, the *lattice coordinates* ω of a lattice point are unique. If $m = n$, the lattice is of *full rank*. A *sublattice* of a lattice of dimension m in $\mathbb{R}^n$ is an additive subgroup; it has a generator matrix MZ, where $Z \in \mathbb{Z}^{m\times k}$. Here k is the dimension of the sublattice and for a square matrix Z,

$$|\Lambda_b/\Lambda_e| = |\det Z|.$$

The *volume* $\mathrm{Vol}(\Lambda)$ of the lattice Λ is the volume of the fundamental parallellotope spanned by the column vectors of M, given by

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

for full-rank lattices.

Remark 2.2: Differing from some information theory references, here vectors are identified with *column* matrices and the lattice generator vectors with the *columns* of the generator matrix M.

Definition 2.3: The *dual lattice* $\Lambda^\star$ of a full-rank lattice Λ generated by M is the one generated by

$$M^{-T} := (M^{-1})^T = (M^T)^{-1}.$$

Theorem 2.4 (The Poisson formula for lattices): Let Λ be a full-rank lattice with generator M and let $f : \mathbb{R}^n \to \mathbb{C}$ be a continuous function with $\int_{\mathbf{x}\in\mathbb{R}^n} |f(\mathbf{x})| d^n x < \infty$ and $\sum_{\mathbf{t}\in\Lambda^\star} |\hat{f}(\mathbf{t})| < \infty$ such that the partial sums of $\sum_{\mathbf{t}\in\Lambda} |f(\mathbf{t}+\mathbf{u})|$ converge uniformly whenever $\mathbf{u}$ is restricted onto a compact set. Then,

$$\sum_{\mathbf{t}\in\Lambda} f(\mathbf{t}) = |\det M|^{-1} \sum_{\mathbf{t}\in\Lambda^\star} \hat{f}(\mathbf{t})$$

where the Fourier transform is defined as

$$\hat{f}(\mathbf{t}) = \int_{\mathbf{y}\in\mathbb{R}^n} e^{-i2\pi\mathbf{y}\cdot\mathbf{t}} f(\mathbf{y}) dy.$$

Proof: The proof is given in [7]. We point out that the condition on the continuity of f is essential for the proof and is missing in the book. ∎

The function that we will optimize is the following.

Definition 2.5: The *psi function* $\psi_\Lambda(x)$ of a lattice Λ at a point $x \in \mathbb{R}_+$ is given by

$$\psi_\Lambda(x) = \sum_{\mathbf{t}\in\Lambda} e^{-x\|\mathbf{t}\|^2}.$$

This is a variant of lattice theta series restricted on the imaginary axis, $\psi_\Lambda(x) = \Theta_\Lambda(ix/\pi)$. The convergence properties of the psi series follow from those of the theta series.

Interpretation 2.6: In [2], an upper approximation for the ECDP $P_{c,e}$ for a lattice coset code is derived as

$$P_{c,e} \le \frac{\mathrm{Vol}(\Lambda_b)}{(\sqrt{2\pi}\sigma_e)^n} \psi_{\Lambda_e}\left(\frac{1}{2\sigma_e^2}\right). \tag{1}$$

Here Λ_b is the dense and Λ_e the sparse lattice, inteded for the receiver and the eavesdropper, respectively. The lattices are assumed to be of full rank and the eavesdropper's noise is assumed to be AWGN with variance σ_e^2. The inequality (1) is tight for large σ_e. For small σ_e, the upper bound is larger than 1 and hence useless.

On the other hand, using the union bound technique as is done in [8, Appendix II] for Rayleigh-fading channels and setting the Rayleigh fading coefficients equal to one, the REP can be approximated from above as:

$$P_{e,b} \le 1/2 \left(\psi_{\Lambda_b}\left(\frac{1}{8\sigma_b^2}\right) - 1\right). \tag{2}$$

This formula is valid for any lattice code Λ_b (not just a coset code) in an AWGN channel and the approximation is good for small receiver's noise variances σ_b^2.

Based on these two formulae and the fact that the variances σ_e^2 and σ_b^2 vary with the random channels, our subsequent aim will be to provide inequalities of the form $\psi_{\Lambda_1}(x) < \psi_{\Lambda_2}(x)$ for all $x \in \mathbb{R}_+$. When comparing different lattices sharing the same dimension, their volumes are first normalized to one. This ensures that for a relatively large fixed transmission power, the finite codebooks carved from the infinite lattices will be approximately equally large, and hence we can fairly compare the lattice codes without considering the actual data rates, as these will coincide.

Remark 2.7: Due to the obvious connection between the formulae (2) and (1) for the REP and ECDP, respectively, one would intuitively guess that a solution for the sphere-packing problem also yields an optimal ECDP. This, however, does not seem to work on the level of mathematical proofs; Eq. (2) is obtained by the union bound technique, whereas in the sphere-packing problem, the upper bound for REP is based on integrating a Gaussian function over a ball, yielding a much tighter bound for large receiver's noise variances σ_b or, equivalently, for small arguments of ψ. To minimize the ECDP, we want to minimize ψ for small arguments. Hence, even if the sphere-packing probability bound is small, it does not provide us with immediate information as to how small the ψ function is for small arguments, i.e., how small the ECDP is.

III. Skewing an orthogonal lattice

In this section, we show that skewing a lattice will always improve a code both in terms of Eve's and Bob's probabilities.

Lemma 3.1: For any full-rank lattice Λ,

$$\psi_\Lambda(x) > \sum_{\mathbf{t}\in\Lambda} e^{-x\|\mathbf{t}+\mathbf{u}\|^2} \tag{3}$$

for any $\mathbf{u} \notin \Lambda$.

Proof: Denote summands of the respective sides as $g(\mathbf{t}) = e^{-x\|\mathbf{t}\|^2}$ and $f(\mathbf{t}) = e^{-x\|\mathbf{t}+\mathbf{u}\|^2}$, so $f(\mathbf{t}) = g(\mathbf{t}+\mathbf{u})$. Then, by the elementary properties of Fourier transform, we have $\hat{f}(\mathbf{t}) = \hat{g}(\mathbf{t})e^{-i2\pi\mathbf{t}\cdot\mathbf{u}}$. Hence, using the Poisson formula,

$$\begin{aligned} & \sum_{\mathbf{t}\in\Lambda} e^{-x\|\mathbf{t}+\mathbf{u}\|^2} \\ = & \sum_{\mathbf{t}\in\Lambda} f(\mathbf{t}) \\ = & |\det M|^{-1} \sum_{\mathbf{t}\in\Lambda^\star} \hat{g}(\mathbf{t}) e^{-i2\pi\mathbf{t}\cdot\mathbf{u}}, \end{aligned}$$

where M is the generator matrix of Λ. In continuation, we will use the knowledge that the Fourier transform of the gaussian function g is another gaussian, hence a real, positive and even function. (The explicit form of $\hat{g}$ could be calculated but it is not necessary.) First, since $\hat{g}$ is even, the imaginary parts $-i\hat{g}(\pm\mathbf{t})\sin(\pm 2\pi\mathbf{t}\cdot\mathbf{u})$ of the summand for lattice $\Lambda^\star$ points $\pm\mathbf{t}$ cancel out, yielding

$$\begin{aligned} & \sum_{\mathbf{t}\in\Lambda} e^{-x\|\mathbf{t}+\mathbf{u}\|^2} \\ = & |\det M|^{-1} \sum_{\mathbf{t}\in\Lambda^\star} \hat{g}(\mathbf{t}) \cos(2\pi\mathbf{t}\cdot\mathbf{u}). \end{aligned}$$

Next, we need the positivity of $\hat{g}$ to be able to approximate the cosine by 1. First, note that we assumed $\mathbf{u} \notin \Lambda$, equivalently, $\mathbf{u} = M\omega_1$ with some component of ω_1, say the j^{th} one $\omega_{1,j}$, not integer. Also note that $\Lambda^\star \ni \mathbf{t} = M^{-T}\omega_2$, where $\omega_2 \in \mathbb{Z}^n$. Hence, $\mathbf{t}\cdot\mathbf{u} = \omega_2^T M^{-1} M\omega_1 = \omega_2^T\omega_1$. Now, choosing the lattice point $\mathbf{t}$ such that $\omega_2 = \mathbf{e}_j$, we immediately see that $\mathbf{t}\cdot\mathbf{u} = \omega_{1,j} \notin \mathbb{Z}$ and $\cos(2\pi\mathbf{t}\cdot\mathbf{u}) < 1$. Hence, replacing $\cos(2\pi\mathbf{t}\cdot\mathbf{u})$ by 1 in the preceding step, we get a strict inequality

$$\begin{aligned} & \sum_{\mathbf{t}\in\Lambda} e^{-x\|\mathbf{t}+\mathbf{u}\|^2} && (4) \\ < & |\det M|^{-1} \sum_{\mathbf{t}\in\Lambda^\star} \hat{g}(\mathbf{t}) && (5) \\ = & |\det M|^{-1} |\det M^{-T}|^{-1} \sum_{\mathbf{t}\in\Lambda} \hat{\hat{g}}(\mathbf{t}) && (6) \\ = & \sum_{\mathbf{t}\in\Lambda} \hat{\hat{g}}(\mathbf{t}), && (7) \end{aligned}$$

where we have again applied the the Poisson formula to (5). Finally, the double Fourier transform is in general a reflection operator, so $\hat{\hat{g}}(\mathbf{t}) = g(-\mathbf{t})$, and using the fact that $g(-\mathbf{t}) = g(\mathbf{t})$ we obtain the result,

$$\begin{aligned} & \sum_{\mathbf{t}\in\Lambda} e^{-x\|\mathbf{t}+\mathbf{u}\|^2} \\ < & \sum_{\mathbf{t}\in\Lambda} g(\mathbf{t}) \\ = & \psi_\Lambda(x). \end{aligned}$$

■

Definition 3.2: Let Λ_o be a full-rank orthogonal lattice in $\mathbb{R}^n$ with generator vectors $a_1\mathbf{e}_1, ..., a_n\mathbf{e}_n$, $a_i > 0$ for $1 \le i \le n$. We call a lattice $\Lambda_s \neq \Lambda_o$ a *skewing* of Λ_o, if it has a generator matrix that is an upper triangular matrix with the diagonal elements $a_1, ..., a_n$.

This definition has a simple geometric interpretation, depicted in Fig. 1.

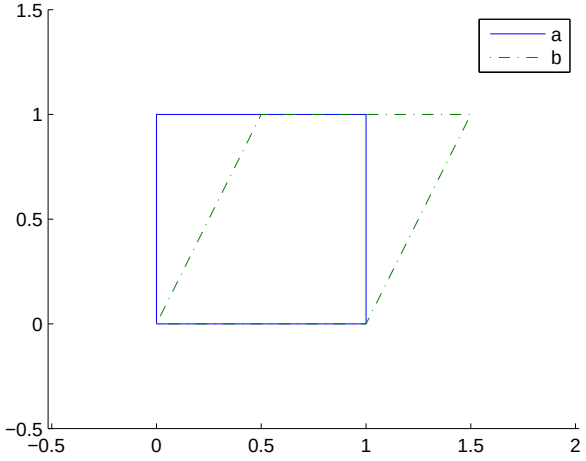

Fig. 1. The fundamental parellellotopes of (a) a square lattice (b) its skewing.

We point out that skewing can be interpreted as a matrix operation. If M_o and M_s are the generator matrices of Λ_o and Λ_s, respectively, then the non-singular skewing matrix S can be solved from the matrix equation

$$M_s = SM_o. \tag{8}$$

This equation is non-singular, since

$$\det M_o = \prod_{i=1}^{n} a_i \neq 0$$

and

$$\det M_s = \prod_{i=1}^{n} a_i = \det M_o$$

by the determinant rule of upper triangular matrices. This also implies that $\det S = 1$.

Now we are ready to state the main theorem. After this, we will provide an illustrative interpretation of the theorem and prove it.

Theorem 3.3: For a skewing Λ_s of a full-rank orthogonal lattice Λ_o,

$$\psi_{\Lambda_s}(x) < \psi_{\Lambda_o}(x)$$

for all $x > 0$.

Interpretation 3.4: Skewings provide several easy ways to improve lattice coset codes. We point out that since skewing

keeps the lattice volume constant ($\det S = 1$ in matrix representation), it will not affect the size of a spherical codebook. Hence, a lattice comparison between skewings only requires considering the ECDP and the REP. With ths knowledge, the theorem has the following immediate implications.

i) Comparing a dense lattice $\Lambda_{b,o}$ and its skewings $\Lambda_{b,s}$, Theorem 3.3 applied to Eq. (2) shows that the REP is always smaller for the skewings $\Lambda_{b,s}$. This holds for all codes, not just coset codes.

ii) Consider a coset code arising from a fixed nonorthogonal lattice Λ_b. Then, to minimize the ECDP (1), it seems that Λ_e should not be chosen orthogonal (if orthogonal sublattices exist). Note that then no skewing of the orthogonal Λ_e is necessarily a sublattice of Λ_b, so this is just heuristics.

iii) Consider a typical set-up of $\Lambda_{b,o}$ generated by $M = \text{diag}(a_1, ...a_n)$ being orthogonal and $\Lambda_{e,o} = 2^k\Lambda_{b,o}$. In this case both the REP and the OCDP are suboptimal. There are two remedies:

- First, we can skew both $\Lambda_{e,o}$ and $\Lambda_{b,o}$. Skewing by S so that the skewed lattices $\Lambda_{b,s}$ and $\Lambda_{e,s}$ are generated by SM and 2^kSM, respectively, will yield a nonorthogonal lattices but preserve the volumes: $\text{Vol}(\Lambda_{b,s}) = \text{Vol}(\Lambda_{b,o})$ (since $\det S = 1$). Hence, applying this and Theorem 3.3 in Eqs. (2) and (1), we see that skewing will decrease both the REP and the ECDP. However, the skewed lattice will not allow for a simple Gray mapping, or in other words, the Gray mapping is not guaranteed to give an optimal bit-labeling.
- Second, we can only opt for skewing the sublattice Λ_e, while leaving Λ_b orthogonal. This means that the REP will remain suboptimal, but the lattice will allow for Gray labeling and maintains simpler encoding and decoding for Bob along the lines discussed in the introduction. Moreover, the ECDP is decreased. The idea is that if $\Lambda_{b,o}$ is orthogonal and generated by $\text{diag}(a_1, ...a_n)$, and $\Lambda_{e,o} = 2^k\Lambda_b$, then any sublattice $\Lambda_{e,s}$ generated by MZ, where Z is an upper triangular integer matrix with diagonal etries 2^k, is easily proven to be a skewing of $\Lambda_{e,o}$ (or equal to $\Lambda_{e,o}$). Then, applying Theorem 3.3 to Eq. (1), we see that $\Lambda_{e,s}$ will yield a lower ECDP.

Proof of Theorem 3.3:

Let us use the notation of Definition 3.2. Furthermore, denote by $\Lambda_{s,k}$ the embedding into $\mathbb{R}^k$, $k \leq n$, of $\Lambda_s \cap \mathbb{R}^k \times 0^{n-k}$. Equivalently, $\Lambda_{s,k}$ is the lattice in $\mathbb{R}^k$ generated by the k first columns of the generator M_s of Λ_s. Continuing to ease the notation, denote the projection of the k^{th} column of M_s onto $\mathbb{R}^{k-1}$ by $\mathbf{m}_k$, so the k^{th} column is $a_k\mathbf{e}_k + \mathbf{m}_k$.

Now, it is apparent from the definition of $\Lambda_{s,k}$ that

$$\psi_{\Lambda_s}(x) = \psi_{\Lambda_{s,n}}(x), \tag{9}$$

and that

$$\psi_{\Lambda_{s,1}}(x) = \sum_{\omega_1 \in \mathbb{Z}} e^{-x\omega_1^2 a_1^2}. \tag{10}$$

On the other hand, using Lemma 3.1 for the lattice $\Lambda_{s,k-1}$, $2 \leq k \leq n$, which is a full-rank lattice of $\mathbb{R}^{k-1}$, we obtain

$$\begin{aligned}
&\psi_{\Lambda_{s,k}}(x) \\
&= \sum_{\mathbf{t} \in \Lambda_{s,k}} e^{-x\|\mathbf{t}\|^2} \\
&= \sum_{\omega_k \in \mathbb{Z}} \sum_{\mathbf{t}^{(k-1)} \in \Lambda_{s,k-1}} e^{-x\omega_k^2 a_k^2 - x\|\mathbf{t}^{(k-1)} + \omega_k \mathbf{m}_k\|^2} \\
&= \sum_{\omega_k \in \mathbb{Z}} e^{-x\omega_k^2 a_k^2} \sum_{\mathbf{t}^{(k-1)} \in \Lambda_{s,k-1}} e^{-x\|\mathbf{t}^{(k-1)} + \omega_k \mathbf{m}_k\|^2} \\
&\leq \sum_{\omega_k \in \mathbb{Z}} e^{-x\omega_k^2 a_k^2} \sum_{\mathbf{t}^{(k-1)} \in \Lambda_{s,k-1}} e^{-x\|\mathbf{t}^{(k-1)}\|^2} \\
&= \left(\sum_{\omega_k \in \mathbb{Z}} e^{-x\omega_k^2 a_k^2} \right) \psi_{\Lambda_{s,k-1}}(x)
\end{aligned} \tag{11}$$

and, as stated in Lemma 3.1, the equality holds if and only if $\omega_k \mathbf{m}_k \in \Lambda_{s,k-1}$ for all $\omega_k \in \mathbb{Z}$, equivalently, $\mathbf{m}_k \in \Lambda_{s,k-1}$. This is furthermore equivalent to that the k^{th} column $a_k\mathbf{e}_k + \mathbf{m}_k$ of M_s can be replaced by $a_k\mathbf{e}_k$ without changing the lattice Λ_s.

Next, starting from Eq. (9), using the identity (11) inductively, and finally using Eq. (10), we obtain

$$\begin{aligned}
\psi_{\Lambda_{s,n}}(x) &\leq \prod_{i=1}^{n} \left(\sum_{\omega_i \in \mathbb{Z}} e^{-x\omega_i^2 a_i^2} \right) \\
&= \psi_{\Lambda_{s,o}}(x).
\end{aligned}$$

The equality holds if and only if it has been possible to modify, for all k, the k^{th} column of M_s into $a_k\mathbf{e_k}$ without changing the lattice generated by M_s. But this is equivalent to M_s and $(a_1\mathbf{e}_1, ..., a_n\mathbf{e}_n) = M_o$ generating the same orthogonal lattice Λ_o. This is impossible by the definition of a skewing. Hence, for any skewing Λ_s of Λ_o, we have a strict inequality

$$\psi_{\Lambda_s}(x) < \psi_{\Lambda_o}(x)$$

for all $x > 0$. This completes the proof. ∎

Example 3.5: The Gosset lattice E_8 has the generator matrix M_s given by [4]

$$\begin{pmatrix}
2 & -1 & 0 & 0 & 0 & 0 & 0 & 1/2 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 1/2 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 1/2 \\
0 & 0 & 0 & 1 & -1 & 0 & 0 & 1/2 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 1/2 \\
0 & 0 & 0 & 0 & 0 & 1 & -1 & 1/2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1/2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2
\end{pmatrix},$$

so it is a skewing of the orthogonal lattice Λ generated by $M_o = \text{diag}(2, 1, ..., 1, 1/2)$. The theta series of the Gosset lattice is expressible by the Jacobi theta functions as [4]

$$\Theta_{E_8}(z) = 1/2(\vartheta_2(q)^8 + \vartheta_3(q)^8 + \vartheta_4(q)^8),$$

where $q = e^{i\pi z}$. The theta series of the orthogonal lattice Λ is

$$\Theta_\Lambda(z) = \prod_{j=1}^{n} \vartheta_3(q_j), \tag{12}$$

where $q_j = e^{i\pi a_j^2 z}$ and a_j is the j^{th} diagonal element of M_o. Now, recalling that $\psi_\Lambda(x) = \Theta_\Lambda(ix/\pi)$, we can compare the psi series of these two lattices by evaluating Jacobi theta functions. The plots of the psi functions are depicted in Fig. 2. The figure shows that $\psi_{E_8}(x) < \psi_\Lambda(x)$ for all x, as predicted by Theorem 3.3.

In coset coding, this has the following interpretation: E_8 and Λ are both index 2^8 subgroups of $\frac{1}{2}\mathbb{Z}^8$. If Bob's lattice is $\frac{1}{2}\mathbb{Z}^8$, then the coset lattices E_8 and Λ will yield the same code rates, but E_8 with a better secrecy.

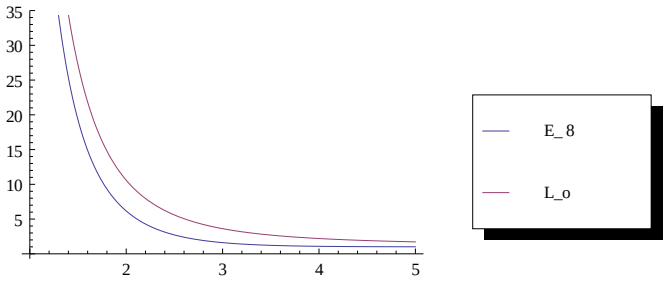

Fig. 2. The psi functions of an orthogonal lattice $\Lambda = L_o$ and its skewing E_8.

IV. Conclusions

In the construction of lattice codes for AWGN wiretap channels, skewed lattices should be taken more seriously. Namely, we have proved that orthogonal lattices are suboptimal not only in terms of the receiver's error probability as we already know from the sphere-packing theorems, but also in terms of the eavesdropper's correct decision probability when using lattice coset codes. Hence, the design of secure lattice codes should ideally be based on skewed lattices. However, due to implementation purposes, one may opt for only skewing the eavesdropper's lattice, while preserving the orthogonality of the legitimate receiver's lattice, which results in suboptimal performance but easy-to-implement algorithms for Bob, as well as improved security.

V. Acknowledgments

This work was carried out during A. Karrila's MSc thesis project. The Department of Mathematics and Systems Analysis at Aalto University is gratefully acknowledged for the financial support.

C. Hollanti is financially supported by the Academy of Finland grants #276031, #282938, and #283262, and by a grant from Magnus Ehrnrooth Foundation, Finland.

The support from the European Science Foundation under the ESF COST Action IC1104 is also gratefully acknowledged.

References

[1] A. D. Wyner, "The wire-tap channel", *Bell System Technical Journal*, Vol. 54, Oct 1975.

[2] F. Oggier, P. Solé and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: construction and analysis", arXiv 1103.4086v3, 2013.

[3] E. Viterbo and F. Oggier, "Algebraic number theory and code design for Rayleigh fading channels", *Foundations and Trends in Communications and Information Theory*, Vol. 1, No. 3, Now Publishers Inc., 2004.

[4] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, 1988.

[5] C. Hollanti and K. Ranto, "Maximal orders in space–time coding: construction and decoding", *International Symposium on Information Theory and Its Applications ISITA 2008*, pp.1–5, 7-10 Dec. 2008.

[6] K. R. Kumar and G. Caire, "Space–time codes from structured lattices", *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 547–556, Feb. 2009.

[7] W. Ebeling, *Lattices and codes. A course partially based on lectures by Friedrich Hirzebruch*, 3rd Ed., Springer Spectrum, 2013.

[8] J. Boutros, E. Viterbo, C. Rastello and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels", *IEEE Transactions on Information Theory*, vol. 42, no 2, March 1996.