Aalto University

OPEN ACCESS

This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Damir, Taoufiq; Gnilke, Oliver; Amoros, Laia; Hollanti, Camilla

Analysis of Some Well-Rounded Lattices in Wiretap Channels

Published in:
2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications, SPAWC 2018

DOI:
10.1109/SPAWC.2018.8445937

Published: 24/08/2018

Document Version
Peer reviewed version

Please cite the original version:
Damir, T., Gnilke, O., Amoros, L., & Hollanti, C. (2018). Analysis of Some Well-Rounded Lattices in Wiretap Channels. In *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications, SPAWC 2018* (Vol. 2018-June, pp. 496-500). [8445937] (IEEE International Workshop on Signal Processing Advances in Wireless Communications). IEEE.
https://doi.org/10.1109/SPAWC.2018.8445937

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.

Analysis of Some Well-Rounded Lattices in Wiretap Channels

Mohamed Taoufiq Damir, Oliver Gnilke, Laia Amorós, and Camilla Hollanti
Department of Mathematics and Systems Analysis
Aalto University School of Science, Finland
{mohamed.damir, oliver.gnilke, laia.amoros, camilla.hollanti}@aalto.fi

***Abstract*—Recently, various criteria for constructing wiretap lattice coset codes have been proposed, most prominently the minimization of the so-called flatness factor. However, these criteria are not constructive *per se*. As explicit constructions, well-rounded lattices have been proposed as possible minimizers of the flatness factor, but no rigorous proof has been given. In this paper, we study various well-rounded lattices, including the best sphere packings, and analyze their shortest vector lengths, minimum product distances, and flatness factors, with the goal of acquiring a better understanding of the role of these invariants regarding secure communications. Simulations are carried out in dimensions four and eight, yielding the conclusion that the best sphere packing does not necessarily yield the best performance, not even when compared to other well-rounded lattices having the same superlattice. This motivates further study and construction of well-rounded lattices for physical layer security.**

***Index Terms*—Algebraic number fields, coset coding, ideals, single-input single-output (SISO) channels, sphere packings, well-rounded lattices, wiretap channels.**

I. Introduction

Wiretap channels were first described by Wyner [1] as a communication model where an eavesdropper (Eve) is trying to intercept the data transmitted between two legitimate parties (Alice and Bob). In our setting, Alice transmits data over a fading channel to a receiver Bob, while Eve receives the data over another, degraded[1] fading channel. See [2] for a more general introduction to physical layer security.

We will consider a single-input single-output (SISO) fast Rayleigh fading channel model [3], which after phase cancellation is equivalent to sending real codewords $x \in \mathcal{C} \subset \mathbb{R}^n$ component-wise through the (real) channel. The vectors received by Bob and Eve are respectively given by

$$y_B = H_B x + n_B \text{ and } y_E = H_E x + n_E \tag{1}$$

where $H_B = \operatorname{diag}(h_i)$ (resp. H_E) is an $n \times n$ diagonal matrix with Rayleigh distributed fading coefficients h_i normalized to $\mathrm{E}[(h_i)^2] = 1$, and $n_B \in \mathbb{R}^n$ (resp. n_E) is a real Gaussian noise vector where each entry has variance σ_B^2 (resp. σ_E^2). See [3], [4] for more details.

Lattice coset codes for fading wiretap channels were proposed in [4]. The overall codebook consists of vectors from a lattice Λ_B, which is chosen such that Bob is able to decode correctly with high probability. A second lattice $\Lambda_E \subset \Lambda_B$ is chosen in order to confuse the eavesdropper. A codeword x is the sum of the message $m \in \Lambda_B/\Lambda_E$ (for chosen coset representatives) and a random vector $r \in \Lambda_E$, $x = m + r$. Consequently, the *information rate* is determined by the nesting index (=ratio of the fundamental parallelotope volumes) $[\Lambda_B : \Lambda_E] := \frac{\operatorname{vol}(\Lambda_E)}{\operatorname{vol}(\Lambda_B)}$, not the actual codebook size. The vector x is chosen as a random representative of the coset belonging to the intended message, chosen from a finite region.

For a finite codebook $\mathcal{C} \subsetneq \mathbb{R}^n$ the data rate $R := \frac{1}{n}\log_2(|\mathcal{C}|)$ in bits per channel use (bpcu) is split between the information rate R_i from Alice to Bob, *i.e.*, the actual amount of information transmitted, and random bits R_c added to confuse the eavesdropper

$$R = R_i + R_c = \frac{1}{n}\left(\log_2([\Lambda_B : \Lambda_E]) + \log_2\left(\frac{|\mathcal{C}|}{[\Lambda_B : \Lambda_E]}\right)\right).$$

Increasing the number of coset representatives and thus increasing R_c reduces border effects but increases the average energy by increasing the codebook size.

In [5]–[7], a connection between Eve's correct decoding probability (ECDP) and the mutual information between Eve's received signal and the message has been established, in that both of these secrecy measures can be upper bounded by the flatness factor [7]. Thus, we can use Eve's correct decoding probability ECDP to measure how much information she can acquire from y_E[2].

An analytic approximation for ECDP is developed in [4] as

$$\mathrm{ECDP} \approx (2\sigma_E)^{-n} \operatorname{vol}(\Lambda_B) \sum_{r \in \Lambda_E} \prod_{i=1}^{n} \left(1 + \left(\frac{r_i}{\sigma_E}\right)^2\right)^{-\frac{3}{2}}. \tag{2}$$

This work is supported in part by the Academy of Finland, under grants #276031, #282938, and #303819 to C. Hollanti, and by the Technical University of Munich – Institute for Advanced Study, funded by the German Excellence Initiative and the EU 7th Framework Programme under grant agreement #291763, via a *Hans Fischer Fellowship* held by C. Hollanti. O. W. Gnilke is partially supported by the Finnish Cultural Foundation.

[1] A common assumption made is that the channel to the eavesdropper experiences a lower signal-to-noise ratio (SNR) than the one to the legitimate receiver. Such a situation can arise naturally or can be artificially enforced by beamforming and jamming techniques.

[2] Note that even a relatively high ECDP does not mean that Eve gains any information. Due to coset coding, there will be a coset representative close-by regardless of how big the noise is, as demonstrated by the lower bound $\frac{1}{[\Lambda_B:\Lambda_E]}$. Hence $\mathrm{ECDP} = \frac{1}{[\Lambda_B:\Lambda_E]}$ amounts to Eve guessing uniformly at random among the message set, corresponding to zero information between the message and Eve's received signal.

A. Related work and contributions

In [8], a Universal Software Radio Peripherals (USRP) implementation of a wiretap channel was carried out, demonstrating the advantages of lattice coset coding vs lattice codes without coset coding. Well-rounded lattices have been previously proposed [9]–[11] as good lattices for coset codes, based on various performance measures (ECDP, flatness factor, mutual information) [4]–[7], and shown to outperform non-well-rounded ones — this serves as our starting point here.

The main contribution of this paper is to show by actual fading wiretap simulations that the choice within the family of well-rounded lattices is nontrivial. Namely, well-rounded lattices which are not optimal sphere packings seem to outperform the best sphere packings at the low SNR regime wiretap channels. This seems to be, not so surprisingly, thanks to a good combination of the (long) shortest vector length and the (small) kissing number, hinting towards *generic well-rounded lattices*, which have not been studied in this context before. Generic well-rounded lattices are well-rounded lattices with minimal kissing number. For instance, $\mathbb{Z}^n$ is generic well-rounded, but on the other hand has the worst possible shortest vector length among well-rounded lattices. Constructing a variety of good (generic) well-rounded lattices will hence be an interesting future research task.

For computing the expected flatness factors of the lattices under study, we use the approximation derived in [12], also utilized in [11].

II. Preliminaries on lattices

A *lattice* Λ is a discrete subgroup of $\mathbb{R}^n$, *i.e.*, there exist basis vectors $\{v_1, \ldots, v_k\}$ of $\mathbb{R}^n$ such that $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k$. If the rank k of the lattice equals the dimension, $k = n$, Λ is called a full (rank) lattice. A lattice is called fully diverse, if its nonzero vectors have no zero coordinates. In this paper, we only consider full-rank full-diversity lattices.

Let Λ be a lattice in $\mathbb{R}^n$ for $n \geq 2$. For $x = (x_1, \ldots, x_n) \in \Lambda$ we denote by

- $||x|| = \sqrt{\sum_{i=1}^n x_i^2}$ the Euclidean norm of x.
- $\lambda_1(\Lambda) = \min_{0 \neq x \in \Lambda} ||x||$ the Euclidean minimum of Λ.
- $S(\Lambda) = \{x \in \Lambda \ : \ ||x|| = \lambda_1(\Lambda)\}$ the set of shortest vectors.
- $d_{p,\min}(\Lambda) = \inf_{0 \neq x \in \Lambda} \prod_{i=1}^n |x_i|$ the minimum product distance of Λ.
- $\kappa(\Lambda) = \#S(\Lambda)$ the kissing number of Λ.

We review next the definition of the flatness factor as given in [13]. The flatness factor was first introduced as a design criterion for wiretap channels in [7], and has been also considered in [5], [6], [11]. The flatness factor characterizes the deviation of the lattice Gaussian PDF from the uniform distribution on the voronoi region $\mathcal{V}(\Lambda)$:

Definition 1: The *flatness factor* of a full-rank lattice is defined as

$$\varepsilon_\Lambda(\sigma) := \max_{u \in \mathbb{R}^n} \left| \frac{g_n(\Lambda_E + u; \sigma)}{1/\operatorname{vol}(\Lambda)} - 1 \right|, \tag{3}$$

where $g_n(\Lambda_E + u; \sigma)$ is the n-dimensional Gaussian zero-mean probability density function with variance σ^2, and we can maximize over $\mathbb{R}^n$ by periodicity.

The Poisson summation formula yields the following useful equality:

$$\varepsilon_\Lambda(\sigma) = \operatorname{vol}(\Lambda) g_n(\Lambda; \sigma) - 1 = \frac{\operatorname{vol}(\Lambda)}{(\sqrt{2\pi}\sigma)^n} \Theta_\Lambda(e^{-1/2\sigma^2}) - 1, \tag{4}$$

where Θ_Λ is the lattice theta series.

It has been suggested in the literature that one should *minimize the expected flatness factor of the faded lattice* $\Lambda_{H,E} = H_E \Lambda_E$, where the expectation is taken over H_E. Namely, the ECDP can be upper bounded by the average flatness factor (see e.g. [13, Eq. (12)] and references therein):

$$\text{ECDP} \leq \frac{1}{[\Lambda_B : \Lambda_E]} (\mathbb{E}_{H_E}[\varepsilon_{\Lambda_{H,E}}(\sigma)] + 1) \tag{5}$$

A. Well-rounded lattices

In the traditional wireless communications setting, for a fixed dimension n, it is well known that to protect against additive noise one should choose a lattice with a large λ_1, *i.e.*, good sphere packing. On the other hand, in order to protect against fading (in the high SNR range), we should choose a lattice with a large $d_{p,\min}(\Lambda)$. Unfortunately, there is no obvious tradeoff between maximizing the sphere packing density and maximizing the minimum product distance.

In wiretap channels using lattice coset codes, the performance of the eavesdropper is closely related to the flatness factor and hence to the lattice theta series. A crude estimate of the theta series is given by truncation to the first term, since the shortest vectors contribute the most. However, this is not the entire truth as we know, namely the kissing number also plays a role. If we blindly maximize the shortest vector length, we end up with the best lattice sphere packing. As the best sphere packings are not known in every dimension and may not be constructible as a sublattice of a given index of a given superlattice as required in wiretap coset coding, a possible strategy to get good sphere packing/product distance is to use *well-rounded (WR)* lattices. Namely, the local maxima of the lattice sphere packings are called extremal, and by a well-known theorem of Voronoi, a lattice is extremal if and only if it is perfect and eutactic [14]. Furthermore, all perfect lattices belongs to a larger class of lattices called well-rounded, see Definition 3 below. Hence, all the optimal sphere packing lattices are well-rounded.

If we on the other hand would like to minimize the kissing number, the right concept is that of *generic well-rounded lattices* [15]. To get an understanding of the interplay of the shortest vector length and the kissing number, one may consider a range of well-rounded lattices between optimal sphere packings and generic well-rounded lattices (*e.g.* $\mathbb{Z}^n$) [15]. On the other hand, it is often preferred to use an orthogonal lattice for Bob, so it is particularly interesting to consider (non-orthogonal) well-rounded sublattices of orthogonal lattices. We will next define these concepts more rigorously.

Definition 2: A rank n lattice Λ is *well-rounded* (WR), if $\operatorname{span}_{\mathbb{R}}(S(\Lambda)) = \mathbb{R}^n$.

Definition 3: A rank n lattice Λ is *generic well-rounded* (GWR), if it is well-rounded and $\kappa(\Lambda) = 2n$.

Definition 4: The *Hermite constant* in dimension n is defined as $\gamma_n := \max_{\Lambda \subset \mathbb{R}^n} \frac{\lambda_1(\Lambda)}{\mathrm{vol}(\Lambda)^{\frac{2}{n}}}$.

The following simple lemma [9] relates the volume of a WR sublattice to the length of its minimal vectors using Hermite constants.

Lemma 1: For a full-rank WR lattice of volume V it holds that $V^{\frac{2}{n}} \leq \lambda_1 \leq \gamma_n V^{\frac{2}{n}}$, where γ_n is the Hermite constant for dimension n.

It is possible to find all WR sublattices of a given lattice and a given index by searching through all possible combinations of vectors of suitable lengths, as described by Lemma 1. For instance, the WR nonorthogonal lattices used in our simulations were found after few minutes of randomly testing combinations of integer vectors of same length for linear independence, and then using the LLL-algorithm to determine λ_1 for the lattice they generate.

B. Well-rounded lattices from number fields

Let us next give a short recap on lattice construction from canonical embeddings of real number fields and their ideals. Real number fields are known to provide a reasonable solution to the problem of constructing lattices that are good for both Rayleigh fading and Gaussian channel. For more details, see [3].

A number field K is a finite extension of the field of rationals $\mathbb{Q}$. The ring of integers of K is denoted by $\mathcal{O}_K$. If the degree of K over $\mathbb{Q}$ is $[K : \mathbb{Q}] = n$, then K has r_1 real embeddings and $2r_2$ complex embeddings into $\mathbb{C}$, where $n = r_1 + 2r_2$. If $r_2 = 0$, then the field is called *totally real*. In this paper we only consider totally real number fields as they provide full diversity $r_1 + r_2 = r_1 + 0 = n$ [3]. Let now K be a totally real number field and denote its embeddings by $\{\sigma_1, \ldots, \sigma_n\}$. The canonical embedding $\sigma : K \to \mathbb{R}^n$, $\sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x))$, gives a lattice $\Lambda = \sigma(\mathcal{O}_K)$ when restricted to $\mathcal{O}_K$. Note that the minimum product distance in this case becomes $d_{p,\min}(\Lambda) = \inf_{0 \neq x \in \mathcal{O}_K} N_K(x)$, where $N_K(x) = \prod_{i=1}^n \sigma_i(x)$ is the field norm. For I a nonzero ideal of $\mathcal{O}_K$, $\Lambda_I = \sigma(I)$ is also a full rank lattice in $\mathbb{R}^n$. In fact, if $I \subset \mathcal{O}_K$ is a principal ideal, then $d_{p,\min}(\Lambda_I) = \frac{\mathrm{vol}(\Lambda_I)}{\sqrt{d_K}}$, where d_K is the discriminant of K. If we normalize Λ_I to Λ'_I with $\mathrm{vol}(\Lambda'_I) = 1$, *i.e.*, $\Lambda'_I = \frac{1}{\mathrm{vol}(\Lambda_I)^{1/n}} \Lambda_I$, then Λ'_I has $d_{p,\min}(\Lambda_I) = \frac{1}{\sqrt{d_K}}$.

In [16], [17], some of the best known sphere packings in low dimensions were constructed from real number fields. In our simulations we will consider the construction of D_4 from [16] and E_8 from [17], which we explain in more detail in the next section.

III. Constructions of $\mathbb{Z}^4$, $\mathbb{Z}^8$, D_4, and E_8 lattices from number field extensions

We will also consider WR sublattices of the optimal rotations of $\mathbb{Z}^4$ and $\mathbb{Z}^8$ in terms of the minimum product distance proposed by Viterbo *et al.* [18], [19]. We refer to these rotated $\mathbb{Z}^n$ lattices by 'Krus4' and 'Cyclo8' respectively. The basis matrices are given in Appendix. The Cyclo8 lattice has a rotated $2E_8$ as a sublattice since $2E_8 \subseteq \mathbb{Z}^8$. We will compare the sublattices having the best sphere packing shape to randomly found nonorthogonal well-rounded sublattices of Krus4 and Cyclo8 (denoted by 'WR nonortho' in the tables below), which are not isometric to the best sphere packigns. The generator matrices are given in the previous footnote. For the generators of the rotations, see [19]. The choice of these sublattices is based on trying to simultaneously obtain a long shortest vector and a low kissing number, along the lines suggested in the previous section.

Lattice	$d_{p,\min}^{1/n}$	λ_1^2	κ	E_{av}
Krus4 (Viterbo [19])	0.43899	1	8	84
4Krus4		16	8	
WR nonortho		20	12	
$\mathbf{D_4}$ (Costa [16])	0.38554	1.41421	24	118
$4D_4$		22.62735	24	

TABLE I: Viterbo et al. $\mathbb{Z}^4$ algebraic rotation vs Costa et al. D_4 algebraic rotation. Superlattices **boldfaced** and normalized to unit volume. E_{av} stands for the average energy of the overall codebook with 8-PAM.

Lattice	$d_{p,\min}^{1/n}$	λ_1^2	κ	E_{av}
Cyclo8 (Viterbo [18])	0.289520	1	16	40
2Cyclo8		4	16	
WR nonortho		6	40	
$2E_8$		8	240	
$\mathbf{E_8}$ (Costa [17])	0.293826	2	240	80
$2E_8$		8	240	

TABLE II: Viterbo et al. $\mathbb{Z}^8$ algebraic rotation vs Costa et al. E_8 algebraic rotation. Superlattices **boldfaced** and normalized to unit volume. E_{av} stands for the average energy of the overall codebook with 4-PAM.

In addition to the rotated $\mathbb{Z}^4$ lattice, we will consider an algebraic construction of the best sphere packing lattice D_4 in dimension 4. It is preferable to construct the desired lattice as a twisted embedding [16] of a (principal) ideal, as we then have a simple formula to calculate the minimum product distance as explained above. The lattice is constructed as an algebraic rotation of the D_4 lattice using the maximal real subfield of a cyclotomic field, namely a field of the form $K_s = \mathbb{Q}(\zeta_s + \zeta_s^{-1})$, where ζ_s stands for a primitive $s-th$ root of unity. The degree of K over $\mathbb{Q}$ is $\varphi(s)/2$, where φ is the Euler totient function. Hence, to construct D_4, the candidates will be the fields K_s such that $s = 15, 16, 20, 24, 30$.

The case $s = 15$ can be discarded using a simple number theoretic argument, leaving $s = 16$ as the next option, see [16] for more details. As a sublattice for Eve, we take $4D_4$ which has nesting index $4^4 = 256$. This yields an information rate of 2 bpcu with a confusion rate of 1 bpcu (8-PAM) or 2 bpcu (16-PAM).

In order to construct E_8 from K_s similarly as above, the possible candidates are $s = 17, 32, 34, 40, 48, 60$. One can also use the fact that $2E_8$ is a sublattice of $\mathbb{Z}^8$, then use a rotated

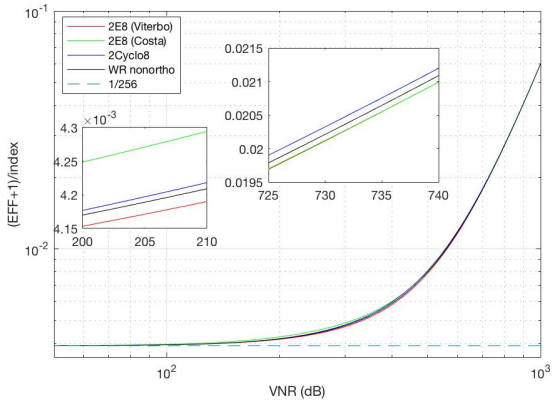

Fig. 1. Comparison of the ECDP upper bounds $(\mathrm{EFF}+1)/\mathrm{index}$ (cf. (5)) for 8-dimensional WR sublattices with respect to the volume-to-noise ratio (VNR).

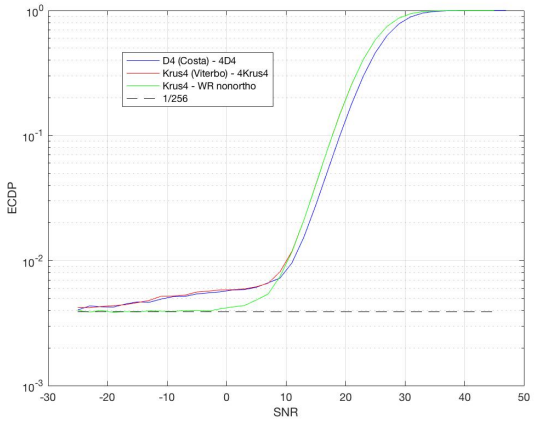

Fig. 2. Comparison of 4-dimensional WR lattices with 16-PAM. Sublattice index 256.

version of $\mathbb{Z}^8$ in order to get a rotated E_8 with a good product distance. In fact, the optimal rotation Cyclo8 of $\mathbb{Z}^8$ [18] is constructed on K_{17}. Hence, we can use it to get E_8 as an embedding of a $\mathbb{Z}$-module in K_{17} (see [20]). However, this construction has a smaller product distance than another version of E_8 from [17] constructed from an ideal in $\mathcal{O}_{K_{60}}$, which we use for our simulations. As a sublattice, we choose $2E_8$ having nesting index 256. This yields an information rate of 1 bpcu with a confusion rate of 1 bpuc (4-PAM) or 2 bpcu (8-PAM).

A. Comparison of the key lattice invariants

In Tables I and II, we depict the minimum product distance, shortest vector length, kissing number, and the average energy for the lattices under comparison. We can see how the PAM signaling causes suboptimal average energy for the D_4 and E_8 superlattices due to their skewness. It is also evident from the simulations in the next section that the relationship between the shortest vector length and kissing number is nontrivial.

Fig. 1 displays the ECDP upper bounds in terms of the expected flatness factors (EFF) (cf. (5)) computed by using the approximation from [12]. We can see that for 8-dimensional WR lattices (behavior of 4-dimensional lattices is very similar) the curves almost coincide, and the small differences do not necessarily give the performance order observed in the simulations in the next section. Hence, choosing the lattice with the smallest EFF alone may not yield the desired outcome. Furthermore, even though the differences in the EFFs of the lattices are negligible, the simulations show a very clear difference in the actual ECDP performance, even beyond 10 dB depending on the SNR range.

IV. Simulation results

When using coset coding every message (coset) is being assigned several different codewords. A sender (Alice) chooses and sends a random codeword that represents the intended message. From the decoding perspective, two codewords λ, μ in the lattice Λ_B represent the same message if $\lambda - \mu \in \Lambda_E$, where $\Lambda_E \subset \Lambda_B$ is a sublattice. The choice of Λ_E can heavily influence the information leakage to a possible eavesdropper. We use the *Planewalker* sphere decoder implementation [21] for our coset code simulations, with around 10^6 channel realizations per SNR. The depicted SNR is the SNR observed by Eve. However, the same plot can be used for Bob's correct decision probability, by looking at relatively higher SNRs compared to Eve's as we assume $\sigma_E^2 > \sigma_B^2$.

Both in dimension 4 and 8, the well-rounded nonorthogonal lattice outperforms the other lattices in the regime close to the asymptote corresponding to uniform guessing. The curves cross at higher SNRs, after which the Costa D_4, E_8 constructions become better, so the choice of the best lattice also depends on the target ECDP. Fig. 2 shows the performance of different 4-dimensional lattices using 16-PAM. The results with 8-PAM are very similar, except that the crossing point of the curves is slightly above $\mathrm{ECDP} = 10^{-2}$. In Fig. 3 (top), different 8-dimensional lattices are compared with 8-PAM. Again, the results with 4-PAM are very similar, except that all the curves ultimately get to the asymptote, and the crossing point is slightly higher, just above $\mathrm{ECDP} = 10^{-2}$.

We also remark again that using PAM signaling for the non-orthogonal superlattices is suboptimal (more so than for orthogonal lattices) in terms of average transmission energy. To this end, we also ran simulations with spherical shaping, depicted in Fig. 3 (bottom). The differences get a lot smaller, and the crossing point seems to disappear. In the interesting low SNR regime, the WR nonorthogonal sublattice still outperforms the others. Furthermore, spherical encoding and decoding are much more complex than that of cubic (*i.e.*, with a symmetric PAM coefficient set) constellations. It also makes bit labeling a delicate problem.

V. Discussion

As future work, it remains to rigorously prove that the minimizer of the flatness factor arises from the family of well-

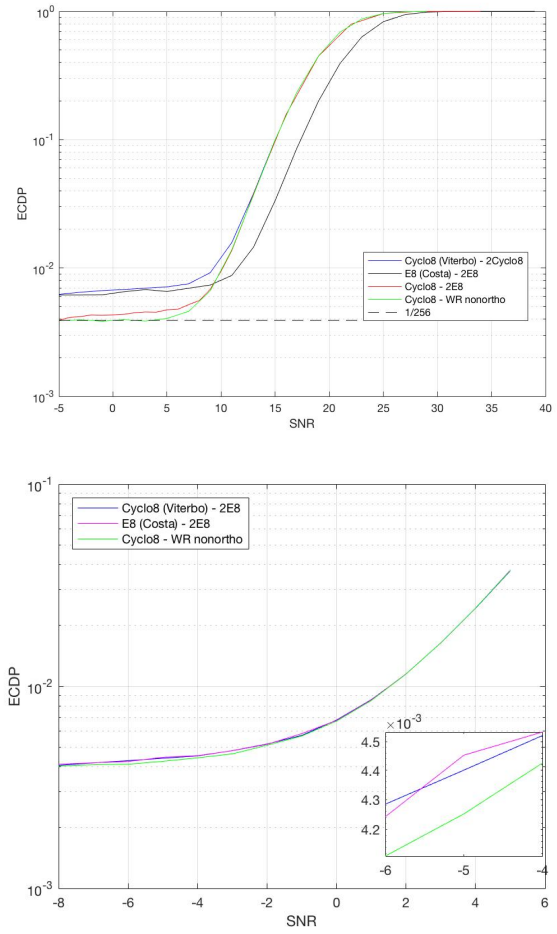

Fig. 3. Comparison of 8-dimensional WR lattices with 8-PAM (top) and with spherical shaping; 2^{16} shortest vectors chosen out of the 2^{24} vectors gotten from 8-PAM (bottom). Sublattice index 256.

rounded lattices. As we have seen, the relationship between the kissing number and shortest vector is subtle and also deserves more attention — a lattice with a shorter shortest vector yields worse worst case performance, while a lattice with a bigger kissing number but with a longer shortest vector yields a better worst-case scenario, but hits the worst case more often. To this end, (generic) well-rounded lattices should be studied in more detail, in particular with the goal of finding the ones with large λ_1 and small κ, possibly identifying an explicit tradeoff between the two. Furthermore, the simulation results imply that the flatness factor (approximation) may not be sufficient for predicting the performance gap and order of different coset codes. Nevertheless, choosing lattices with small flatness factor to start with is still worthwhile as this guarantees good upper bounds for the ECDP.

References

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

[2] A. Chorti, C. Hollanti, J. Belfiore, and H. Poor, *Physical layer security: A paradigm shift in data confidentiality*, ser. Lecture Notes in Electrical Engineering. Springer Verlag, 2016, vol. 358, pp. 1–15.

[3] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," *IEEE Trans. Inf. Theory*, vol. 50, pp. 702–714, 2004.

[4] J. C. Belfiore and F. Oggier, "Lattice code design for the Rayleigh fading wiretap channel," in *IEEE Int. Comm. Workshop (ICC)*, June 2011.

[5] L. Luzzi, C. Ling, and R. Vehkalahti, "Almost universal codes for fading wiretap channels," in *IEEE Int. Symp. Inf. Theory (ISIT)*, 2016.

[6] H. Mirghasemi and J.-C. Belfiore, "Lattice code design criterion for MIMO wiretap channels," in *IEEE Inf. Theory Workshop, (ITW) 2015*, 2015.

[7] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, 2014.

[8] J. Lu, J. Harshan, and F. Oggier, "Performance of lattice coset codes on Universal Software Radio Peripherals," *Physical Communication*, 2017.

[9] O. W. Gnilke, H. Tran, A. Karrila, and C. Hollanti, "Well-rounded lattices for reliability and security in Rayleigh fading SISO channels," *IEEE Inf. Theory Workshop (ITW)*, 2016.

[10] O. W. Gnilke, H. Tran, A. Barreal, A. Karrila, D. Karpuk, and C. Hollanti, "Well-rounded lattices for coset coding in MIMO wiretap channels," *IEEE Int. Telecomm. Networks and App. Conf. (ITNAC), arXiv:1609.07666*, 2016.

[11] A. Barreal, A. Karrila, D. Karpuk, and C. Hollanti, "Information bounds and flatness factor approximation for fading wiretap MIMO channels," *IEEE Int. Telecomm. Networks and App. Conf. (ITNAC), arXiv:1606.06099*, 2016.

[12] A. Barreal, D. Karpuk, and C. Hollanti, "Theta series approximation with applications to compute-and-forward relaying," *arXiv:1601.05596*, 2016.

[13] A. Karrila, D. Karpuk, and C. Hollanti, "On analytical and geometric lattice design criteria for wiretap coset codes," *arXiv:1609.07723*, 2016.

[14] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*. Springer, 1993.

[15] M. Levin, U. Shapira, and B. Weiss, "Closed orbits for the diagonal group and well-rounded lattices," *Groups, Geometry and Dynamics*, vol. 10, pp. 1211–1225, 2016, arXiv:1405.5682.

[16] G. C. Jorge, A. J. Ferrari, and S. I. R. Costa, "Rotated D_n lattices," *Journal of Number Theory*, vol. 132, pp. 2397–2406, 2012.

[17] G. C. Jorge, A. A. deAndrade, S. R. Costa, and J. E. Strapasson, "Algebraic constructions of densest lattices," *Journal of Algebra*, vol. 429, pp. 218–235, 2015.

[18] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 50, pp. 702–714, 2004.

[19] E. Viterbo, "Full-diversity rotations." [Online]. Available: http://www.ecse.monash.edu.au/staff/eviterbo/rotations/rotations.html

[20] J. C. Jorge, "Reticulados q-ários e algébricos," *PhD thesis*, 2012.

[21] P. Pyrrö, O. Gnilke, C. Hollanti, and M. Greferath, "*Planewalker* sphere decoder implementation," 2018. [Online]. Available: https://version.aalto.fi/gitlab/pasi.pyrro/sphere-decoder/tree/SPAWC

Appendix: Generator matrices of WR sublattices of rotated $\mathbb{Z}^4$ (Krus4) and $\mathbb{Z}^8$ (Cyclo8)

$$\begin{pmatrix} 2.6179140488 & -2.414499458 & -2.6174487992 & 0.6824076544 \\ -3.0009700976 & -2.338015074 & 2.3164903194 & 0.4021649334 \\ 3.4332588812 & -1.6385571204 & 1.3956732198 & -1.8920783058 \\ 0.8223162707 & -1.4725414834 & 3.5158030921 & 2.1896452076 \end{pmatrix}$$

$$\begin{pmatrix} 0.7007035387 & -1.8196532242 & 0.5098308731 & 0.5436478577 \\ -0.1711086948 & -1.2014038879 & 0.2876791984 & -0.8163368876 \\ 0.40388427868 & -0.3992399381 & 0.359383021 & -0.3556171703 \\ 0.5710190406 & 1.817991942 & 0.7541367758 & 0.607964929 \\ -0.84701159571 & -1.0127325492 & 0.8324416454 & 0.0586435438 \\ -0.04341452009 & -0.3892212211 & 1.5903470277 & -0.8144416018 \\ 1.70075388399 & -0.6502044959 & 0.3252620337 & -1.1219451349 \\ -1.5754499665 & 0.8921488186 & 0.5880215656 & -0.3340078386 \end{pmatrix}$$

$$\begin{pmatrix} -0.354502581 & 1.0846703755 & -0.47456554011 & -0.3391191908 \\ 0.70784566949 & -0.3945408211 & -0.8973956636 & 1.5218930146 \\ -0.8543195887 & -0.4910135947 & -1.6941162987 & -1.2573300636 \\ 0.1228109789 & -0.9716075716 & -0.13023119099 & -0.6741179039 \\ -0.09880446362 & -1.7873172339 & -0.5616527529 & 0.2020567981 \\ 0.8859851713 & -0.084615344 & 1.3643633956 & -0.022051583 \\ -0.89655915559 & -0.3737755366 & 0.10194674011 & -0.6051400279 \\ -1.0081995324 & 1.0730373751 & 0.0358312991 & -0.3090920604 \end{pmatrix}$$