Secrecy gain, flatness factor, and secrecy-goodness of even unimodular lattices

Fuchun Lin
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
linf0007@e.ntu.edu.sg

Cong Ling
Department of Electrical and
Electronic Engineering
Imperial College London
United Kingdom
cling@ieee.org

Jean-Claude Belfiore
Département Communications
et Electronique
Télécom-ParisTech
Paris, France
belfiore@telecom-paristech.fr

***Abstract*—Nested lattices $\Lambda_e \subset \Lambda_b$ have previously been studied for coding in the Gaussian wiretap channel and two design criteria, namely, the secrecy gain and flatness factor, have been proposed to study how the coarse lattice Λ_e should be chosen so as to maximally conceal the message against the eavesdropper. In this paper, we study the connection between these two criteria and show the secrecy-goodness of even unimodular lattices, which means exponentially vanishing flatness factor as the dimension grows.**

I. Introduction

The wiretap channel was introduced by Wyner [1] as a discrete memoryless broadcast channel where the sender Alice transmits confidential messages to a legitimate receiver Bob, in the presence of an eavesdropper Eve. Both reliable and confidential communication between Alice and Bob should be provided at the same time via coding. The original wiretap channel model have been extended to various classes of channels including continuous channels such as the Gaussian channel and both information-theoretic and coding results are available in the literature [2], [3], [4].

In this paper, we discuss coding for the Gaussian wiretap channel, whose *secrecy capacity*, which is by definition the maximal information rate achievable with *strong* secrecy, was computed in [5], [6] as the difference of the capacities of Bob and Eve's channels, provided that the noise variance σ_b^2 of Bob's channel is smaller than σ_e^2 of Eve's. Examples of existing Gaussian wiretap codes were designed for binary inputs, as in [7]. Another line of research considers lattice coding, which is the dominant coding technique for the Gaussian channel. In particular, a pair of nested lattices $\Lambda_e \subset \Lambda_b$ are considered, where Λ_e is designed with the intention to confuse Eve and Λ_b to enable Bob to correct errors. Pioneering works along this line consider a lattice design criterion called the *secrecy gain* [8] which measures how much better an n-dimensional lattice can cause confusion to Eve than the cubic lattice $\mathbb{Z}^n$. The secrecy gain of the *ℓ-modular* lattices, namely, lattices that are geometrically similar to their duals with a similarity that multiplies the *norm* by ℓ, were studied in small dimensions for $\ell = 1, 2, 3$ [9], [10], [11]. The study shows that certain lattices can do much better than the others in concealing the message. The asymptotic result on the secrecy gain is only available for the so called *even unimodular* lattices, i.e. *even* and $\ell = 1$. It is shown that the secrecy gain of even unimodular lattices goes to infinity as the dimension n grows [9].

Recent progress in [12], [13] introduced the *flatness factor* and showed that it is proportional to the absolute mutual information. Further, it demonstrated the existence of mod-p lattices with an exponentially vanishing flatness factor, thereby obtaining strong secrecy. However, the proof of [13] relied on the Minkowski-Hlawka theorem, and thus did not give concrete lattices that are good for secrecy. In this paper, we elucidate the relation between the secrecy gain and the flatness factor; more importantly, we analyze the flatness factor of even unimodular lattices and by an asymptotic analysis show that they are good for secrecy.

II. Preliminaries

A Gaussian wiretap channel is a broadcast Gaussian channel modeled by

$$\begin{array}{ll} \mathbf{y} & = \mathbf{x} + \mathbf{v_b} \\ \mathbf{z} & = \mathbf{x} + \mathbf{v_e}, \end{array} \tag{1}$$

where $\mathbf{x}$ is the codeword sent by Alice, $\mathbf{y}$ and $\mathbf{z}$ are the received signals of Bob and Eve, with respective noise vectors $\mathbf{v_b}$ and $\mathbf{v_e}$, whose components are i.i.d. Gaussian distributed with zero mean and have respective variance σ_b^2 and σ_e^2. In other words, $\mathbf{v_b}$ and $\mathbf{v_e}$ satisfy the *Gaussian distribution*

$$\varphi_{\sigma^2}(\mathbf{v}) = \frac{1}{(2\pi\sigma^2)^{\frac{n}{2}}} e^{-\frac{||\mathbf{v}||^2}{2\sigma^2}}$$

with respective variance. It is assumed that $\sigma_b^2 < \sigma_e^2$ in order to have a positive secrecy capacity [5].

We suppose that $\mathbf{x} \in \mathbb{R}^n$ is a lattice codeword, where by a lattice Λ we mean a discrete set of vectors in $\mathbb{R}^n$, which can be conveniently described by

$$\Lambda = \{\mathbf{u}M | \mathbf{u} \in \mathbb{Z}^n\},$$

where the *generator matrix* M contains a basis of $\mathbb{R}^n$. The *Voronoi cell* $\mathcal{V}_\Lambda(\mathbf{x})$ of a lattice vector $\mathbf{x}$ is defined to be the set of vectors in $\mathbb{R}^n$ that are closer to $\mathbf{x}$ than to any other lattice vectors of Λ. The *volume* $\mathrm{vol}(\Lambda)$ of a lattice Λ is the cell volume of a Voronoi cell, which is also the cell volume of the *fundamental parallelotope* defined by the row vectors of M and hence is computed by $\text{vol}(\Lambda) = \det(M)$.

Definition 2.1: Let $\mathcal{H} = \{a + ib \in \mathbb{C} | b > 0\}$ denote the upper half complex plane and set $q = e^{\pi i \tau},\ \tau \in \mathcal{H}$. The theta series of a lattice Λ is defined by

$$\Theta_\Lambda(\tau) = \Sigma_{\mathbf{t} \in \Lambda} q^{||\mathbf{t}||^2},$$

where $||\mathbf{t}||^2 = \mathbf{t} \cdot \mathbf{t}$ is called the *norm* of a lattice vector.

The *dual* of a lattice Λ of dimension n is defined to be

$$\Lambda^* = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \lambda \in \mathbb{Z}, \lambda \in \Lambda\}.$$

Λ is said to be an *integral* lattice if $\Lambda \subset \Lambda^*$. The norm of any lattice vector in an integral lattice Λ is always an integer. If the norm is even for any lattice vector, then Λ is called an *even* lattice. Otherwise, it is called an *odd* lattice. The theta series of an integral lattice has a neat representation:

$$\Theta_\Lambda(\tau) = \Sigma_{m=0}^{\infty} A_m q^m, \tag{2}$$

where A_m counts the number of lattice vectors of norm m.

As an initial work, we will solely consider a very special class of lattices called *even unimodular* lattices, which are by definition even lattices satisfying $\Lambda = \Lambda^*$.

Lattice encoding for the Gaussian wiretap channel (1) is done via a generic coset coding strategy: let $\Lambda_e \subset \Lambda_b$ be two nested lattices, specially chosen such that the quotient group Λ_b/Λ_e is of size 2^k. A k-bit message is then mapped to a particular coset in Λ_b/Λ_e, from which a vector is randomly chosen as the encoded word [9]. The lattice Λ_e will be interpreted as introducing confusion for Eve, while Λ_b as ensuring reliability for Bob. There have been two new lattice design criteria devised to characterize the performance of a lattice Λ_e in this task of confusing Eve.

The *flatness factor* is our major concern in this paper.

Definition 2.2: [13][1]The flatness factor of a lattice Λ of dimension n is defined by

$$\epsilon_\Lambda(\sigma) = \max_{\mathbf{x} \in \mathcal{V}(\Lambda)} \left| \frac{\sum_{\mathbf{t} \in \Lambda} \varphi_{\sigma^2}(\mathbf{x} - \mathbf{t})}{1/\text{vol}(\Lambda)} - 1 \right|.$$

The function $f_{\sigma,\Lambda}(\mathbf{x}) \triangleq \sum_{\mathbf{t} \in \Lambda} \varphi_{0,\sigma^2}(\mathbf{x} - \mathbf{t})$, $\mathbf{x} \in \mathcal{V}(\Lambda)$ is a probability density, whose expectation $\mathbb{E}[f_{\sigma,\Lambda}(\mathbf{x})]$ achieves $\frac{1}{\text{vol}(\Lambda)}$, when $\mathbf{x}$ is sampled uniformly in $\mathcal{V}(\Lambda)$. The flatness factor thus characterises how "flat" the distribution $f_{\sigma,\Lambda}(\mathbf{x})$ is against the background uniform distribution. It is shown that

$$\epsilon_\Lambda(\sigma) = \left(\frac{\gamma_\Lambda(\sigma)}{2\pi}\right)^{\frac{n}{2}} \Theta_\Lambda\left(\frac{i}{2\pi\sigma^2}\right) - 1, \tag{3}$$

where

$$\gamma_\Lambda(\sigma) \triangleq \frac{\text{vol}(\Lambda)^{\frac{2}{n}}}{\sigma^2} \tag{4}$$

is the *volume-to-noise ratio (VNR)* [13].

The following bound on the information leakage in the *mod-Λ Gaussian wiretap channel* was given in [13]. Let $\epsilon_n = \epsilon_{\Lambda_e^{(n)}}(\sigma_e)$, where $\Lambda_e^{(n)}$ is a lattice of dimension n. Assume that $\epsilon_n < \frac{1}{2}$ for all n. Then the mutual information between the confidential message $\mathbf{m}$ and the eavesdropper's signal $\mathbf{z}$ is bounded as follows:

$$\mathrm{I}(\mathbf{m}; \mathbf{z}) \leq 2\epsilon_n nR - 2\epsilon_n \log 2\epsilon_n. \tag{5}$$

A wiretap coding scheme is secure in the sense of *strong secrecy* if $\lim_{n\to\infty} \mathrm{I}(\mathbf{m}; \mathbf{z}) = 0$. From (5), a flatness factor $\varepsilon_n = o(\frac{1}{n})$ would be enough. In practice, an exponential decay of the information leakage is desired, and this motivates the notion of secrecy-good lattices:

Definition 2.3 (Secrecy-good lattices): A sequence of lattices $\Lambda^{(n)}$ is *secrecy-good* if

$$\epsilon_{\Lambda^{(n)}}(\sigma) = e^{-\Omega(n)}, \quad \forall \gamma_{\Lambda^{(n)}}(\sigma) < 2\pi, \tag{6}$$

where $\Omega(n)$ is a function asymptotically larger than n or as large as n.

The *secrecy gain* gives an intuition to find good lattices for secrecy. Intuitively, Eve can successfully decode as long as her received vector $\mathbf{z}$ lies in the Voronoi cell of any lattice vector in the coset $\Lambda_e + \mathbf{x}$. Thus the probability $P_{c,e}$ of correct decoding for Eve is upper bounded as follows.

$$\begin{aligned} P_{c,e} &\leq \textstyle\sum_{\mathbf{t} \in \Lambda_e + \mathbf{x}} \int_{\mathcal{V}_{\Lambda_b}(\mathbf{t})} \varphi_{\sigma^2}(\mathbf{z} - \mathbf{t}) \mathrm{d}\mathbf{z} \\ &= \tfrac{1}{(\sigma\sqrt{2\pi})^n} \textstyle\sum_{\mathbf{t} \in \Lambda_e + \mathbf{x}} \int_{\mathcal{V}_{\Lambda_b}(\mathbf{t})} e^{-\frac{||\mathbf{z}-\mathbf{t}||^2}{2\sigma^2}} \mathrm{d}\mathbf{z} \\ &\vdots \quad \text{(see [8] for details)} \\ &\leq \tfrac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{\frac{n}{2}}} \textstyle\sum_{\mathbf{r} \in \Lambda_e} e^{-\frac{||\mathbf{r}||^2}{2\sigma_e^2}} \\ &= \tfrac{\text{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{\frac{n}{2}}} \Theta_{\Lambda_e}(\tfrac{i}{2\pi\sigma_e^2}), \end{aligned}$$

Comparing the bound for a lattice Λ against that for the $\mathbb{Z}^n$ lattice scaled to the same volume leads to the notion of the *secrecy function* [8].

Definition 2.4: Let Λ be an n-dimensional lattice. The secrecy function of Λ is given by

$$\Xi_\Lambda(\tau) = \frac{\Theta_{\sqrt[n]{\text{vol}(\Lambda)}\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \tau = yi,\ y > 0. \tag{7}$$

The secrecy gain is then the maximum of the secrecy function.

Note that both criteria involve the theta series of a lattice. Theta series of even unimodular lattices are modular forms of even weight for the full modular group $\mathrm{SL}_2(\mathbb{Z})$ [14]. Other examples of modular forms for the full modular group are the Eisenstein series for even k, which can be computed by

$$E_k(\tau) = 1 - \frac{2k}{B_k} \sum_{m=1}^{+\infty} m^{k-1} \frac{q^{2m}}{1 - q^{2m}}, \tag{8}$$

where B_k is the Bernoulli number [15].

III. Flatness factor of even unimodular lattices

Firstly, a bigger secrecy function value at $\tau = yi = \frac{i}{2\pi\sigma^2}$ implies a smaller flatness factor value at σ if two lattices are of the same dimension and volume. Indeed, assume two n-dimensional lattices Λ_1, Λ_2 with $\text{vol}(\Lambda_1) = \text{vol}(\Lambda_2)$. From (7), $\Xi_{\Lambda_1}(\frac{i}{2\pi\sigma^2}) > \Xi_{\Lambda_2}(\frac{i}{2\pi\sigma^2})$ implies $\Theta_{\Lambda_1}(\frac{i}{2\pi\sigma^2}) <$

[1] Definition 2.2 is defined for any fundamental region. Here we specify the Voronoi region $\mathcal{V}(\Lambda)$ for simplicity.

$\Theta_{\Lambda_2}(\frac{i}{2\pi\sigma^2})$. And from (3), $\Theta_{\Lambda_1}(\frac{i}{2\pi\sigma^2}) < \Theta_{\Lambda_2}(\frac{i}{2\pi\sigma^2})$ implies $\epsilon_{\Lambda_1}(\sigma) < \epsilon_{\Lambda_2}(\sigma)$.

The *weak secrecy gain*, secrecy function value at $y = 1$, of even unimodular lattices was shown to go to infinity as the dimension n grows [9]. We will adapt this result to characterise the asymptotic behaviour of the flatness factor of even unimodular lattices around the point $y = 1$ (equivalently $\sigma = \frac{1}{\sqrt{2\pi}}$).

Lemma 3.1 (Siegel-Weil): [15] Let Ω_n be the set of all inequivalent even unimodular n-dimensional lattices and Aut(Λ) be the group of automorphisms of Λ. Then

$$\sum_{\lambda\in\Omega_n} \frac{\Theta_\Lambda(\tau)}{|\text{Aut}(\Lambda)|} = M_n E_{\frac{n}{2}(\tau)}, \tag{9}$$

where $M_n = \sum_{\lambda\in\Omega_n} \frac{1}{|\text{Aut}(\Lambda)|}$.

Lemma 3.1 says that the average behaviour of the theta series of an n-dimentional even unimodular lattice is characterised by the Eisenstein series $E_{\frac{n}{2}}$. Even unimodular lattices only exist in dimensions a multiple of 8. So we can alternatively write $E_{4t}(\tau)$ assuming $n = 8t$. One then only needs to study the asymptotic behaviour of $E_{4t}(\tau)$. By (8),

$$E_{4t}(\tau) = 1 + \frac{8t}{|B_{4t}|} \sum_{m=1}^{+\infty} \frac{m^{4t-1}}{e^{-2\pi i\tau m} - 1}, \tag{10}$$

where the Bernoulli number $|B_{4t}|$ satisfies asymptoticly [15]

$$|B_{4t}| \sim 2\frac{4t!}{(2\pi)^{4t}}.$$

Let $\tau = \frac{i}{2\pi\sigma^2} = yi$. The infinite sum on the right hand side of (10) satisfies

$$\sum_{m=1}^{+\infty} \frac{m^{4t-1}}{e^{2\pi ym} - 1} \sim \sum_{m=1}^{+\infty} \frac{m^{4t-1}}{e^{2\pi ym}},$$

as long as $e^{2\pi y} >> 1$, for which we may impose $y > \frac{1}{2}$. Moreover, it is shown in [9] that asymptoticly

$$\sum_{m=1}^{+\infty} \frac{m^{4t-1}}{e^{2\pi ym}} \sim \frac{(4t-1)!}{(2\pi y)^{4t}}.$$

Now we compute the asymptotic behaviour of the flatness factor of even unimodular lattices. By (3),

$$\begin{aligned} \epsilon_{\Lambda^{(\infty)}}(\sigma) &= \lim_{n\to\infty} \epsilon_{\Lambda^{(n)}}(\sigma) \\ &= \lim_{n\to\infty} \left(\tfrac{1}{2\pi\sigma^2}\right)^{\frac{n}{2}} \Theta_\Lambda(\tfrac{i}{2\pi\sigma^2}) - 1 \\ &= \lim_{n\to\infty} y^{\frac{n}{2}} E_{\frac{n}{2}}(yi) - 1 \\ &= \lim_{t\to\infty} y^{4t} \left(1 + \tfrac{8t}{2\cdot 4t!/(2\pi)^{4t}} \tfrac{(4t-1)!}{(2\pi y)^{4t}}\right) - 1 \\ &= \lim_{t\to\infty} y^{4t} \left(1 + \tfrac{1}{y^{4t}}\right) - 1 \\ &= \lim_{t\to\infty} y^{4t} \\ &= \begin{cases} 0, & y < 1 \text{ (or } \gamma_\Lambda < 2\pi); \\ 1, & y = 1 \text{ (or } \gamma_\Lambda = 2\pi); \\ \infty, & y > 1 \text{ (or } \gamma_\Lambda > 2\pi). \end{cases} \end{aligned}$$

From the point of view of secrecy gain, the secrecy gained by choosing a particular even unimodular lattice is maximised at $y = 1$ and measures should be taken to force Eve to operate at $\sigma^2 = \frac{1}{2\pi}$. However, from the point of view of flatness factor, the asymptotic result at $y = 1$ suggests that we don't have strong secrecy when Eve is operating at $\sigma^2 = \frac{1}{2\pi}$ since the flatness factor approaches $1 \neq 0$. To achieve a vanishing flatness factor, one has to operate at $\sigma^2 > \frac{1}{2\pi}$, namely, $\gamma_\Lambda < 2\pi$. From this point of view, even unimodular lattices are in average secrecy-good lattices.

IV. Mod-2 even unimodular lattices

In this section, we will take a close look at the mod-2 even unimodular lattices. We first introduce the mod-p lattices, where p is a prime number, or lattices constructed from linear codes over the finite field $\mathbb{F}_p$ via the Construction A. It is shown in [13] that there exists a sequence of mod-p lattices, whose flatness factor can respectively vanish and explode as $n \to \infty$ and $p \to \infty$ when $\gamma_\Lambda < 2\pi$ (equivalently $y < \frac{1}{\sqrt{\ell}}$) and respectively $\gamma_\Lambda > 2\pi$ (equivalently $y > \frac{1}{\sqrt{\ell}}$). Unfortunately, the existence result was shown based on the average behaviour of theta series of mod-p lattices and no construction of lattices were given. Let

$$\rho : \mathbb{Z}^n \to \mathbb{F}_p^n$$

be the map of component-wise reduction modulo p on $\mathbb{Z}^n$. Terminology of error-correcting codes can be found in [16].

Definition 4.1: [17] Let C be a binary $[n, k, d]$ code. The lattice Λ_C generated by C is defined by

$$\Lambda_C := \frac{1}{\sqrt{2}}\rho^{-1}(C).$$

It is shown in [17] that Λ_C is an even unimodular lattice if and only if C is a doubly even self-dual code, the so called type II code. Note that a binary type II code gives rise to an even unimodular lattice. But a random even unimodular lattice is not necessarily a mod-2 lattice associates with a binary type II code. In fact, mod-2 even unimodular lattices are very few among the even unimodular lattices in the same dimension, which will be proved in the journal version of this paper.

A. Average flatness factor of mod-2 even unimodular lattices

In order to have the same kind of result for a mod-2 even unimodular lattice, we consider a mass formula for the weight enumerator polynomial of a binary type II code. This mass formula can be found in [18]. It states that, if C is a type II binary self-dual code of length $n = 2m$, if $A_r(C)$ is the number of codewords of weight $r \equiv 0\ (4)$ and if Γ is the set of all inequivalent type II binary self-dual code of length n, then,

$$\sum_{C\in\Gamma} \frac{A_r(C)}{|\text{Aut}(C)|} = \frac{2}{r!\,(n-r)!} \prod_{i=1}^{m-3} \left(2^i + 1\right) \tag{11}$$

with

$$\sum_{C\in\Gamma} \frac{1}{|\text{Aut}(C)|} = \frac{2}{n!} \prod_{i=1}^{m-2} \left(2^i + 1\right). \tag{12}$$

Also, we will need this result from [16, Chap. 19], *Lemma 4.2:* The total number of even self-dual codes of length n is

$$2\prod_{i=1}^{m-2}\left(2^{i}+1\right) \tag{13}$$

From Equations (11) and (12), as we want, we get the average behaviour for a binary type II code,

$$\begin{aligned}\bar{A}_r &= \mathbb{E}_C\left[A_r\left(C\right)\right]\\ &= \frac{1}{\sum_{C\in\Gamma}\frac{1}{|\mathrm{Aut}(C)|}}\sum_{C\in\Gamma}\frac{A_r(C)}{|\mathrm{Aut}(C)|}\\ &= \binom{n}{r}\frac{1}{2^{m-2}+1}\end{aligned}$$

for all $r \equiv 0\,(4)$ and $r \neq 0$.

Let

$$W_C\left(x,y\right) \triangleq \sum_{c\in C} x^{n-w(\mathbf{c})}y^{w(\mathbf{c})} = \sum_{k=1}^{n/4} A_{4k}\left(C\right)x^{n-4k}y^{4k}$$

be the weight enumerator polynomial of C. As the theta series of the lattice Λ obtained by construction A with C is

$$\begin{aligned}\Theta_\Lambda\left(\tau\right) &= W_C\left(\vartheta_3(2\tau),\vartheta_2(2\tau)\right)\\ &= 1+\sum_{k=1}^{n/4} A_{4k}\left(C\right)\vartheta_3^{n-4k}(2\tau)\vartheta_2^{4k}(2\tau),\end{aligned}$$

where ϑ_2 and ϑ_3 (as well as ϑ_4) are the Jacobi theta functions, we get an average theta series for mod-2 even unimodular lattices:

$$\begin{aligned}\bar{\Theta}_{2,n}\left(\tau\right) &= 1+\sum_{k=1}^{n/4}\bar{A}_{4k}\vartheta_3^{n-4k}(2\tau)\vartheta_2^{4k}(2\tau)\\ &= 1+\frac{1}{2^{m-2}+1}\sum_{k=1}^{n/4}\binom{n}{r}\vartheta_3^{n-4k}(2\tau)\vartheta_2^{4k}(2\tau).\end{aligned}$$

Fig. 1 compares the average flatness factor of mod-2 even unimodular lattices in dimension 168 computed by using the above equation with the average flatness factor of any even unimodular lattice computed by using $\bar{\Theta}_n(\tau) = E_m\left(2\tau\right)$. The horizontal axis is in dB and the vertical axis shows $\log_e \epsilon_\Lambda(\sigma)$.

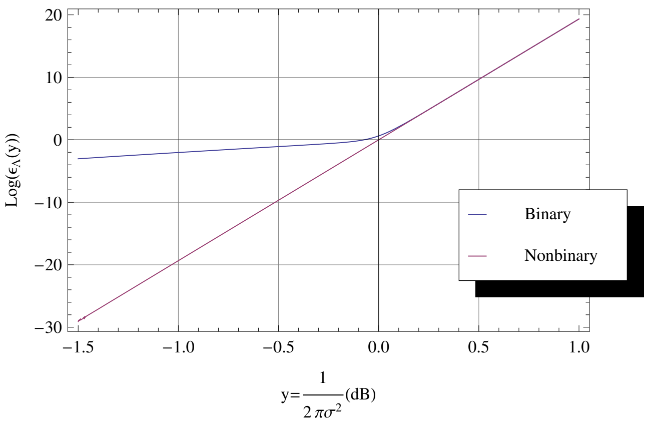

Fig. 1. Average flatness factors of both mod-2 and general even unimodular lattices

B. Examples of mod-2 lattices in finite dimensions

The following example compares the flatness factor of mod-2 lattices in different dimensions. The horizontal axis is again in dB and the vertical axis shows $\log_e \epsilon_\Lambda(\sigma)$.

Example 4.3: Binary self-dual codes were enumerated in lengths up to 32 with the weight distribution of each code given in [19]. The number of self-dual codes grows rapidly when n grows. For example, there are 85 type II codes and 3210 type I codes when $n = 32$. We pick the Type II code with the biggest minimum weight and smallest number of codewords at that weight for $n = 8, 16, 24, 32$. The theta series of the corresponding mod-2 lattices are computed using the technique in [20]. And in order to see the change in a bigger scale, we consider a Type II code of length 168. The binary *Extended Quadratic Residue* code EQR168 associate with the prime 167 [21] is a binary Type II code. The theta series of the corresponding mod-2 lattice was computed in [20]

$$\begin{aligned}\Theta_{\Lambda_{\mathrm{EQR}_{168}}} = {} & E_4^{21}-4704E_4^{18}\Delta+8123136E_4^{15}\Delta^2\\ & -6299181056E_4^{12}\Delta^3+2152218034176E_4^{9}\Delta^4\\ & -272078324367360E_4^{6}\Delta^5\\ & +8116766634934272E_4^{3}\Delta^6\\ & -1397733218844672 0\Delta^7,\end{aligned}$$

where $E_4 = \frac{1}{2}\left(\vartheta_2(\tau)^8+\vartheta_3(\tau)^8+\vartheta_4(\tau)^8\right)$ and $\Delta = \frac{1}{256}\vartheta_2(\tau)^8\vartheta_3(\tau)^8\vartheta_4(\tau)^8$.

Fig. 2 shows the flatness factor of the mod-2 lattice generated by the sequence of binary Type II codes of length $n = 8, 16, 24, 32, 168$ described above. One sees that when $y > 0$ dB (equivalently $y > 1$), the flatness factor increases as n grows, which agrees with the asymptotic analysis in the previous section. But when $y < 0$ dB (equivalently $y < 1$), the expected asymptotic behaviour, namely, the flatness factor vanishes exponentially as n grows does not appear, not even when $n = 168$. Indeed, one sees that the flatness factor of the even unimodular lattice generated by the EQR_{168} (blue) is bigger than the flatness factor of the even unimodular lattice generated by the Golay code (yellow).

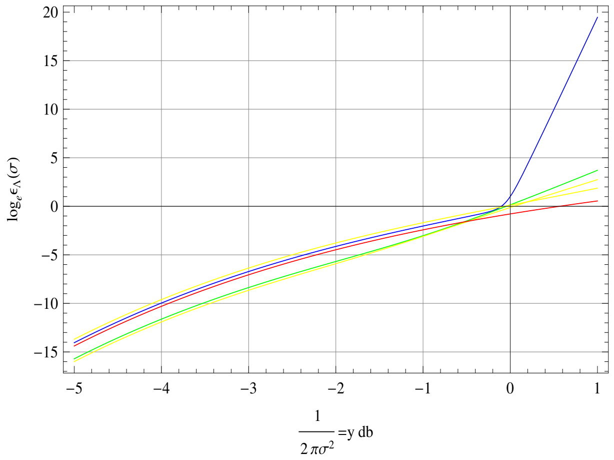

Fig. 2. Flatness factors of a sequence of mod-2 lattices of dimension 8 (red), 16 (orange), 24 (yellow), 32 (green), 168 (blue)

V. Conclusion and future works

The connection between the secrecy gain and the flatness factor of a lattice is studied, which leads to the discovery of even unimodular lattices having exponentially vanishing flatness factor, implying lattice Gaussian wiretap codes with strong secrecy. A subclass of even unimodular lattices, the mod-2 even unimodular lattices is studied intensively to compare with the average even unimodular lattices and mod-2 even unimodular lattices in small dimensions are plotted as examples.

Sequence of mod-p lattices for bigger p with better asymptotic behaviour is now under investigation. Flatness factor of ℓ-modular lattices is also under consideration. The ultimate goal is to find secrecy capacity achieving Gaussian wiretap lattice codes.

Acknowledgment

The research of Fuchun Lin was supported by the Singapore National Research Foundation under the Research Grant NRF-RF2009-07 and the work of Cong Ling and Jean-Claude Belfiore was supported in part by FP7 project PHYLAWS (EU FP7-ICT 317562).

References

[1] A. D. Wyner, "The wire-tap channel," Bell. Syst. Tech. Journal, vol. 54, October 1975.

[2] Y. Liang, H.V. Poor and S. Shamai, Information Theoretic Security, Foundations and Trends in Communications and Information Theory, Vol. 5, Issue 4-5, 2009, Now Publishers.

[3] M. Bloch and J. Barros, Physical-layer security: from information theory to security engineering, Cambridge University Press, 2011.

[4] F. Lin and F. Oggier, "Coding for wiretap channels," in Physical Layer Security in Wireless Communications, Auerbach Publications, CRC Press, Taylor&Francis Group, 2013.

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

[6] I. Csiszár, "Almost independence and secrecy capacity," Problems of Information Transmission, vol. 32, pp. 4047, 1996.

[7] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. ITW*, Oct. 2009.

[8] J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design," ISITA 2010.http://arXiv:1004.4075v2 [cs.IT].

[9] F. Oggier, J.-C. Belfiore, and P. Solé, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis", http://arxiv.org/abs/1103.4086 [cs.IT], 09 Jan 2013.

[10] F. Lin and F. Oggier, "A classification of unimodular lattice wiretap codes in small dimensions", *IEEE Trans. Inf. Theory*, vol.59, no. 6, pp. 3295-3303, Jun. 2013.

[11] F. Lin, F. Oggier and P. Solé, "2- and 3-modular lattice wiretap codes in small dimensions," http://arXiv:1304.4440 [math.NT].

[12] C. Ling, L. Luzzi and J. C. Belfiore, "Lattice codes achieving strong secrecy over the mod-Λ Gaussian channel," *IEEE Int. Symp. Inform. Theory (ISIT)*, Cambridge, MA, USA, Jul. 2012.

[13] C. Ling, L. Luzzi, J.-C. Belfiore and D. Stehle, "Semantically secure lattice codes for the Gaussian wiretap channel", http://arXiv:1210.6673 [cs.IT].

[14] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Graduate Texts in Math. No. 97, Springer-Verlag, New York, Second edition, 1993.

[15] J. P. Serre, A Course in Arithmetic, ser. Graduate Texts in Mathematics, Springer, 1996.

[16] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[17] W. Ebeling, "Lattices and Codes", Advanced Lectures in Mathematics, Vieweg & Sohn, Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1994.

[18] J. G. Thompson, "Weighted averages associated to some codes," Scripta Math. 29, no. 3-4, 449–452. (1973).

[19] Online available, http://www.cs.umanitoba.ca/~umbilou1/SelfDualCodes/toc.html.

[20] F. Lin and F. Oggier, "Gaussian wiretap lattice codes from binary self-dual codes," *2012 IEEE Information Theory Workshop (ITW)* pp. 662-666.

[21] W. K. Su, P.Y. Shih, T.C. Lin and T.K. Truong, "On the minimum weights of binary extended quadratic residue codes", ICACT 2009. pp. 1912 - 1913.