Lattice codes for the Gaussian wiretap channel

Belfiore, Jean-Claude; Oggier, Frederique; Sole, Patrick

2011

Belfiore, J. C., Oggier, F., & Solé, P. (2011). Lattice Codes for the Gaussian Wiretap Channel. IWCC 2011.

https://hdl.handle.net/10356/91439

https://doi.org/10.1007/978-3-642-20901-7_3

Lattice Codes for the Gaussian Wiretap Channel

Jean-Claude Belfiore[1], Frédérique Oggier[2], and Patrick Solé[1]

[1] Dept of Communications & Electronics
Telecom ParisTech, CNRS/LTCI
Paris, France
[2] Division of Mathematical Sciences School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore

Abstract. It has been shown recently that coding for the Gaussian Wiretap Channel can be done with nested lattices. A fine lattice intended to the legitimate user must be designed as a usual lattice code for the Gaussian Channel, while a coarse lattice is added to introduce confusion at the eavesdropper, whose theta series must be minimized. We study, here, the behavior of this invariant for a class of lattices.

1 Introduction

The wiretap channel was introduced by Wyner [1] as a discrete memoryless broadcast channel where the sender, Alice, transmits confidential messages to a legal receiver Bob, in the presence of an eavesdropper Eve. Wyner defined the perfect secrecy capacity as the maximum amount of information that Alice can send to Bob while insuring that Eve gets a negligeable amount of information. He also described a generic coding strategy known as coset coding. While coset coding has been used in many coding scenarios (for ex. [2,3]), Wyner used it to encode both data and random bits to confuse the eavesdropper. The question of determining the secrecy capacity of many classes of channels has been addressed extensively recently, yielding a plethora of information theoretical results on secrecy capacity.

There is a sharp contrast with the situation of wiretap code designs, where very little is known. The most exploited approach to get practical codes so far has been to use LDPC codes (for example [4] for binary erasure and symmetric channels, [5] for Gaussian channels with binary inputs). We also note that wiretap II codes have been extended to more general settings such as network coding in [6]. Finally, lattice codes for Gaussian channels have been considered from an information theoretical point of view in [7].

In [8], a design criterion for constructing explicit lattice codes, has been proposed, based on the analysis of Eve's correct decision probability. This design criterion relies on a new lattice invariant called "secrecy gain" based on theta series. In this paper, we analyze the secrecy gain of unimodular lattices.

2 Notations and previous results

2.1 Notations and system model

We analyze more deeply the secrecy gain introduced in [8] for even unimodular lattices and give the asymptotic behavior of this secrecy gain when the dimension of the lattices grows to infinity. Figure 1 gives the model considered in this

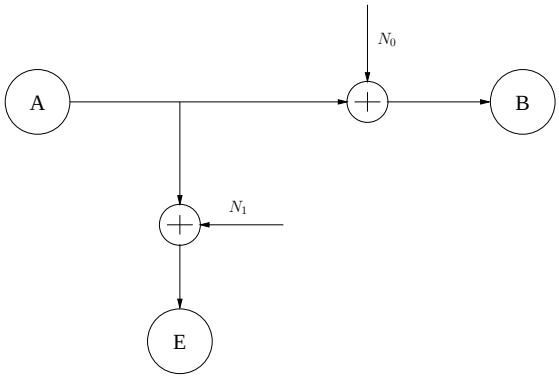

Fig. 1. The Gaussian Wiretap Channel

paper where Alice wants to send data to Bob on a Gaussian channel whose noise variance is given by σ_b^2. Eve is the eavesdropper trying to intercept data through another Gaussian channel whose noise variance is σ_e^2. In order to have a positive secrecy capacity, we will assume that $\sigma_e^2 > \sigma_b^2$. Bits are transmitted by Alice at a rate equal to $R = R_s + R_r$ where R_s is the secrecy rate of this transmission and R_r is the rate of pseudo-random bits. Indeed, we use Wyner's generic coding strategy [9]. We give the remaining parameters,

- Λ_b is the fine lattice (used to minimize Bob's probability of error)
- Λ_e is the coarse lattice (used to minimize Eve's probability of correct decision)
- n is the dimension of both lattices
- $\mathcal{V}(\Lambda_b)$ (resp. $\mathcal{V}(\Lambda_e)$) is the fundamental parallelotope of Λ_b (resp. Λ_e)
- $\mathrm{Vol}(\mathcal{P})$ is the volume of $\mathcal{P}$

Data bits label cosets in Λ_b/Λ_e while pseudo-random bits label points of Λ_e. The reader can refer to [8] for a more detailed description of the coding scheme. Still according to [8], and under the assumption of a moderate to high secrecy rate, the expression of the probability of correct decision at the eavesdropper can be expressed as

$$P_{c,e} \simeq \left(\frac{1}{\sqrt{2\pi}\sigma_e}\right)^n \mathrm{Vol}\left(\mathcal{V}(\Lambda_b)\right) \sum_{\mathbf{r}\in\Lambda_e} e^{-\frac{\|\mathbf{r}\|^2}{2\sigma_e^2}}. \tag{1}$$

In eq. (1), we recognize the theta series of lattice Λ_e.

2.2 Theta series of a lattice

Definition 1. *Let Λ be a Euclidean lattice, then the theta series of Λ is [10]*

$$\Theta_\Lambda(z) \triangleq \sum_{\boldsymbol{x}\in\Lambda} q^{\|\boldsymbol{x}\|^2}, q = e^{i\pi z}, \mathrm{Im}(z) > 0 \tag{2}$$

Some exceptional lattices have theta series that can be expressed as functions of the Jacobi theta functions $\vartheta_i(q)$, $i = 2, 3, 4$ with

$$\vartheta_2(q) = \sum_{n=-\infty}^{+\infty} q^{\left(n+\frac{1}{2}\right)^2}$$

$$\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}$$

$$\vartheta_4(q) = \sum_{n=-\infty}^{+\infty} (-1)^n q^{n^2}$$

For instance, table 1 gives the theta series of some exceptional lattices.

Lattice Λ	Theta series Θ_Λ
Cubic lattice $\mathbb{Z}^n$	ϑ_3^n
D_n	$\frac{1}{2}\left(\vartheta_3^n + \vartheta_4^n\right)$
Gosset lattice E_8	$\frac{1}{2}\left(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8\right)$

Table 1. Theta series of some lattices

2.3 Minimization of the theta series

One problem that arises naturally when studying theta series is the following. In eq. (1), set $y = iz$ and restrict to real values of y. We are now interested in studying

$$\Theta_\Lambda(y) = \sum_{\boldsymbol{x}\in\Lambda} q^{\|\boldsymbol{x}\|^2}, q = e^{-\pi y}, y > 0.$$

Equation (1), giving Eve's probability of correct decision, can be written as

$$P_{c,e} \simeq \left(\frac{1}{\sqrt{2\pi}\sigma_e}\right)^n \mathrm{Vol}\left(\mathcal{V}\left(\Lambda_b\right)\right) \Theta_{\Lambda_e}\left(\frac{1}{2\pi\sigma_e^2}\right) \tag{3}$$

So, for a given dimension n, the problem to solve is to find a lattice Λ^{opt} that minimizes $\Theta_\Lambda(y)$ for a given value of y in order to minimize expression (3).

3 The secrecy gain

3.1 Definitions

We recall here some definitions given in [8].

We remark that, if we do not use any specific coarse lattice Λ_e, we can assume that Λ_e is equal to a scaled version of $\mathbb{Z}^n$ with same volume as Λ_e. Consequently, for a lattice Λ, it is natural to define the secrecy function. For a lattice Λ with fundamental volume $\mathrm{Vol}(\mathcal{V}(\Lambda))$, we have

Definition 2. *Let Λ be an $n-$dimensional lattice. The secrecy function of Λ is*

$$\Xi_\Lambda(y) \triangleq \frac{\Theta_{\lambda\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \frac{\vartheta_3(\lambda^2 y)^n}{\Theta_\Lambda(y)}$$

where $\lambda = \mathrm{Vol}(\mathcal{V}(\Lambda_b))^{\frac{1}{n}}$ and defined for $y > 0$.

Then of course, as we want to minimize the expression of Eve's probability of correct decision in eq. (3), we are interested in the maximum value of the secrecy function. So, we define the secrecy gain,

Definition 3. *The secrecy gain of an $n-$dimensional lattice Λ is*

$$\chi_\Lambda \triangleq \sup_{y>0} \Xi_\Lambda(y).$$

For lattices equivalent to their dual, the secrecy function exhibits a multiplicative symmetry point at $y_0 = \mathrm{Vol}(\mathcal{V}(\Lambda))^{-\frac{2}{n}}$ for which we conjecture that

$$\Xi_\Lambda(y_0) = \chi_\Lambda.$$

3.2 The secrecy gain of unimodular lattices

Theta series are difficult to analyze. Nevertheless, for some lattices, these functions have nice properties. It is the case of even unimodular lattices whose theta series are modular forms with integer weight. We mainly restrict this paper to the study of even unimodular lattices and will use tools from modular forms.

Definitions and formulas We recall the definition of an integral lattice [10],

Definition 4. *A lattice Λ is integral if its Gram matrix has entries in $\mathbb{Z}$. Note that an integral lattice has the property*

$$\Lambda \subseteq \Lambda^\star \subseteq \frac{1}{Vol(\mathcal{V}(\Lambda))^2}\Lambda$$

From this definition, we can now define unimodular lattices,

Definition 5. *A lattice Λ is unimodular if*

1. *Λ is integral*

2. Λ is equal to its dual

Note that a unimodular lattice has fundamental volume equal to 1.

Let $\Lambda^\star$ be the dual lattice of the $n-$dimensional lattice Λ. Then Jacobi's formula [10] gives the theta series of $\Lambda^\star$ as a function of the theta series of Λ,

$$\Theta_{\Lambda^\star}(y) = \mathrm{Vol}\left(\mathcal{V}(\Lambda)\right) y^{-\frac{n}{2}} \Theta_\Lambda\left(\frac{1}{y}\right) \tag{4}$$

If Λ is unimodular, then using (4), we deduce

$$\Theta_\Lambda(y) = \Theta_{\Lambda^\star}(y) = y^{-\frac{n}{2}} \Theta_\Lambda\left(\frac{1}{y}\right).$$

So, since $\mathbb{Z}^n$ itself is unimodular, the secrecy function of Λ has the property,

$$\Xi_\Lambda(y) = \Xi_\Lambda\left(\frac{1}{y}\right).$$

If we express y in decibel (in our case, $y = \frac{1}{2\pi\sigma_e^2}$ and is related to Eve's signal to noise ratio), then the secrecy function becomes an even function.

Conjecture 1. The secrecy gain of unimodular lattices is achieved by the secrecy function at $y = 1$.

Using conjecture 1 in what follows, we can evaluate the secrecy gain of unimodular lattices as

$$\chi_\Lambda = \Xi_\Lambda(1)$$

Some formulas Some formulas are useful to calculate the secrecy gain of unimodular lattices. The most important ones, found in [11], are

$$\begin{aligned} \vartheta_2\left(e^{-\pi}\right) &= \vartheta_4\left(e^{-\pi}\right) \\ \vartheta_3\left(e^{-\pi}\right) &= \sqrt[4]{2}\vartheta_4\left(e^{-\pi}\right) \end{aligned} \tag{5}$$

Secrecy gain of some exceptional unimodular lattices

Gosset Lattice E_8 E_8 is unimodular even. From table 1 and eq. (5), we get

$$\begin{aligned} \frac{1}{\Xi_{E_8}(1)} &= \frac{\frac{1}{2}\left(\vartheta_2(e^{-\pi})^8 + \vartheta_3(e^{-\pi})^8 + \vartheta_4(e^{-\pi})^8\right)}{\vartheta_3(e^{-\pi})^8} \\ &= \tfrac{1}{2}\left(1 + \frac{1}{4} + \frac{1}{4}\right) \\ &= \frac{3}{4} \end{aligned}$$

We deduce, then, the secrecy gain of E_8,

$$\boxed{\chi_{E_8} = \Xi_{E_8}(1) = \frac{4}{3} = 1.33333}$$

As an illustration, figure 2 gives the secrecy function of E_8.

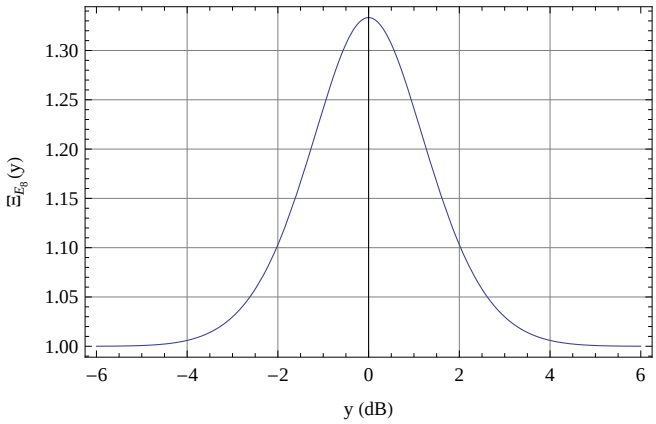

Fig. 2. Secrecy function of E_8

Leech Lattice Λ_{24} Λ_{24} is also unimodular even. From table 1, we get (with simplified notations)

$$\begin{aligned}\frac{1}{\Xi_{\Lambda_{24}}(1)} &= \frac{\frac{1}{8}\left(\vartheta_2^8+\vartheta_3^8+\vartheta_4^8\right)^3 - \frac{45}{16}\vartheta_2^8\vartheta_3^8\vartheta_4^8}{\vartheta_3^{24}} \\ &= \frac{27}{2^6} - \frac{45}{2^8} \\ &= \frac{63}{256}\end{aligned}$$

We deduce, then, the secrecy gain of Λ_{24},

$$\boxed{\chi_{\Lambda_{24}} = \Xi_{\Lambda_{24}}(1) = \frac{256}{63} = 4.0635}$$

As an illustration, figure 3 gives the secrecy function of Λ_{24}.

3.3 Higher dimension unimodular extremal lattices

E_8 and Λ_{24} are extremal even unimodular lattices in dimensions 8 and 24 respectively [10]. Extremal means that their minimum distance is maximal for a given dimension [10]. We can give same type of results for extremal even unimodular lattices of higher dimensions. For instance, we can derive the secrecy functions and secrecy gains of extremal even unimodular lattices in dimensions 32, 48, and 72 using derivations of [12]. The same can be done in dimension 80 by solving a linear system [13]. Please note that, until now, nobody knows if an extremal lattice in dimension 72 exists. Results are summarized in table 2. Here we introduce the function

$$\Delta(q) = \frac{E_4^3(q) - E_6^2(q)}{12^3}$$

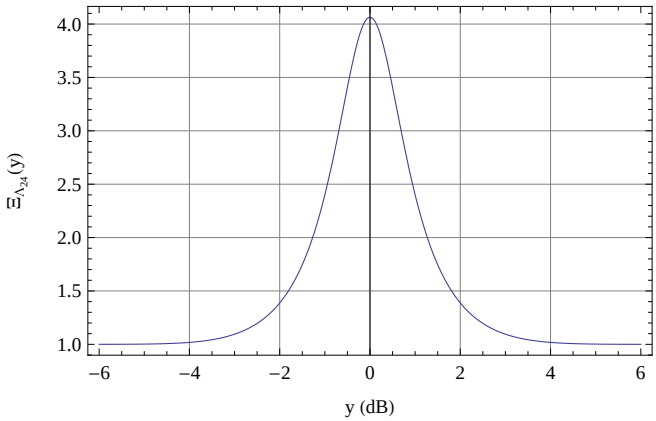

Fig. 3. Secrecy function of Λ_{24}

Dimension	Lattice Λ	Θ_Λ
8	E_8	E_4
24	Λ_{24}	$E_4^3 - 720\Delta$
32	BW_{32}	$E_4^4 - 960E_4\Delta$
48	P_{48}	$E_4^6 - 1440E_4^3\Delta + 125280\Delta^2$
72	L_{72}	$E_4^9 - 2160E_4^6\Delta + 965520E_4^3\Delta^2 - 27302400\Delta^3$
80	L_{80}	$E_4^{10} - 2400E_4^7\Delta + 1360800E_4^4\Delta^2 - 103488000E_4\Delta^3$

Table 2. Theta series of extremal lattices

where E_k are the Eisenstein series [13] defined as

$$E_k(q) = 1 + \frac{2}{\zeta(1-k)} \sum_{m=1}^{+\infty} m^{k-1} \frac{q^m}{1-q^m} \tag{6}$$
$$= 1 - \frac{2k}{B_k} \sum_{m=1}^{+\infty} m^{k-1} \frac{q^m}{1-q^m}$$

where B_k are the Bernouilli numbers [14] and $\zeta(s)$ is the Riemann zeta function

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}.$$

Relations with Jacobi functions are (in symbolic notation)

$$\begin{cases} E_4 & = \frac{1}{2}\left(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8\right) \\ \Delta & = \frac{1}{256}\vartheta_2^8\vartheta_3^8\vartheta_4^8 \end{cases}$$

and give rise to the expressions of theta series evaluated below.

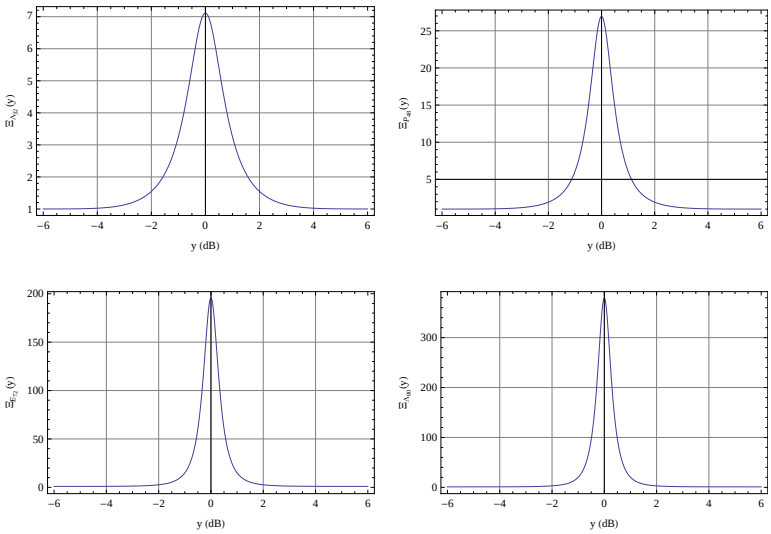

Fig. 4. Secrecy functions of extremal lattices in dimensions 32, 48, 72 and 80

Barnes Wall lattice BW_{32} In dimension 32, Barnes-Wall lattice BW_{32} is an extremal lattice. We have

$$\begin{aligned}\Theta_{BW_{32}} = \frac{1}{16}\left(\vartheta_2^8+\vartheta_3^8+\vartheta_4^8\right)\Big[\left(\vartheta_2^8+\vartheta_3^8+\vartheta_4^8\right)^3 \\ -30\cdot\vartheta_2^8\cdot\vartheta_3^8\cdot\vartheta_4^8\Big]\end{aligned}$$

so,

$$\begin{aligned}\frac{1}{\Xi_{BW_{32}}(1)} &= \frac{1}{16}\left(1+\frac{1}{2}\right)\left[\left(1+\frac{1}{2}\right)^3-30\cdot\frac{1}{16}\right] \\ &= \frac{9}{64}.\end{aligned}$$

Hence,

$$\chi_{BW_{32}} = \frac{64}{9} \simeq 7.11$$

Extremal lattices in dimensions 48, 72 and 80 In the same way, from table 2, we can compute the secrecy gain for extremal even unimodular lattices in dimensions 48, 72 and 80. We have

$$\begin{aligned}\chi_{\Lambda_{48}} &= \tfrac{524288}{19467} &&\simeq 26.93\\ \chi_{\Lambda_{72}} &= \tfrac{134217728}{685881} &&\simeq 195.69\\ \chi_{\Lambda_{80}} &= \tfrac{536870912}{1414413} &&\simeq 379.57\end{aligned}$$

Table 3 summarizes all these results.

Dimension	8	24	32	48	72	80
Secrecy gain	1.3	4.1	7.11	26.9	195.7	380

Table 3. Secrecy gains of extremal lattices

4 Asymptotic Analysis

We propose, here to find a lower bound of the best secrecy gain as a function of the dimension n, and deduce some asymptotic results (when n is large enough). For a fixed dimension n, we compute bounds on the theta series of an optimal unimodular lattice. By optimal, we mean a lattice which maximizes the secrecy gain. We will use the Siegel-Weil formula to compute these bounds.

4.1 A Siegel-Weil formula for theta series of even unimodular lattices

Let $n \equiv 0 (\text{mod } 8)$, Ω_n be the set of all inequivalent even unimodular $n-$dimensional lattices. Let $k = n/2$. Then, one has [14]

$$\sum_{\Lambda \in \Omega_n} \frac{\Theta_\Lambda(q)}{|\text{Aut}(\Lambda)|} = M_n \cdot E_k(q)$$

where

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

and $E_k(q)$ is the Eisenstein series with weight k even whose expression is given in eq. (6).

Let $\Theta_{\min}^{(n)} = \min_{\Lambda \in \Omega_n} \Theta_\Lambda$. Then

$$\Theta_{\min}^{(n)} M_n \leq \sum_{\Lambda \in \Omega_n} \frac{\Theta_\Lambda}{|\text{Aut}(\Lambda)|} = M_n E_k$$

giving rise to

$$\Theta_{\min}^{(n)} \leq E_k.$$

Define

$$\chi_n \triangleq \max_{\Lambda \in \Omega_n} \chi_\Lambda = \frac{\vartheta_3^n\left(e^{-\pi}\right)}{\Theta_{\min}^{(n)}\left(e^{-\pi}\right)}$$

then we get,

$$\boxed{\chi_n \geq \frac{\vartheta_3^n\left(e^{-\pi}\right)}{E_k\left(e^{-2\pi}\right)}}$$

4.2 Limit of E_k

Assume q to be a real number $0 < q < 1$. We have

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

Replacing q by $e^{-2\pi}$ gives

$$E_k\left(e^{-2\pi}\right) = 1 + \frac{2k}{|B_k|} \sum_{m=1}^{+\infty} \frac{m^{k-1}}{e^{2\pi m} - 1}$$

which converges to 2 when k is a multiple of 4 that tends to infinity [15]. Moreover, according to [11], we have

$$\vartheta_3\left(e^{-\pi}\right) = \frac{\pi^{\frac{1}{4}}}{\Gamma\left(\frac{3}{4}\right)} \simeq 1.086 > 1$$

so,

$$\boxed{\chi_n \gtrsim \frac{1}{2}\left(\frac{\pi^{\frac{1}{4}}}{\Gamma\left(\frac{3}{4}\right)}\right)^n \simeq \frac{1.086^n}{2}} \tag{7}$$

which tends exponentially to infinity. Figure 5 gives the asymptotic expression of

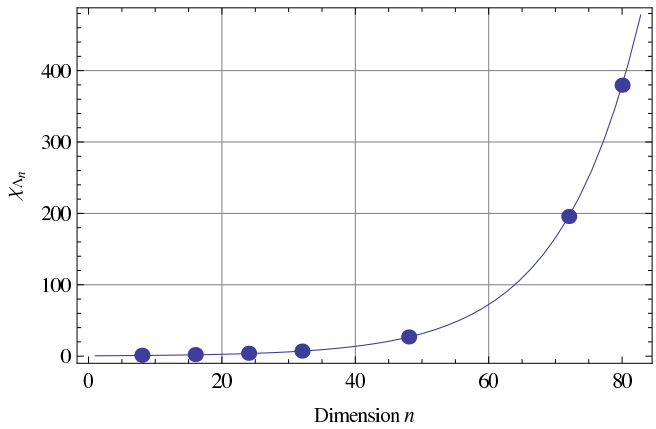

Fig. 5. Lower bound of the minimal secrecy gain as a function of n from Siegel-Weil formula. Points correspond to extremal lattices.

the secrecy gain as a function of the dimension n, as well as points corresponding to extremal lattices in dimensions $8, 16, 24, 32, 48, 72$ and 80.

4.3 Consequences

We proved that there exists a family of even unimodular lattices whose secrecy gains exponentially grows up with the dimension, which means that Eve's probability of correct decision exponentially tends to 0. But as we can remark in figure 4, around its maximum, the secrecy function becomes sharper and sharper when n grows up, which means that, for high dimensions, the communication system absolutely has to operate at $y = 1$. We show now, in section 5, that it is possible to do the same with any integral lattice.

5 Integral lattices

5.1 Level of a lattice (*resp.* a quadratic form)

There is an equivalence between lattices and quadratic forms. In what follows, we will either deal with lattices or with quadratic forms, thanks to this equivalence. Some classical definitions follow. Let

$$f(\boldsymbol{x}) = \sum_{i,j} f_{ij} x_i x_j \tag{8}$$

be a quadratic form. Then, f is integral whenever

$$f_{ij} \in \mathbb{Z}, \forall i, j.$$

The form is primitive when

$$\gcd(f_{i,j}) = 1$$

Now, let $f(\boldsymbol{x})$ be a primitive integral positive definite quadratic form in an even number

$$n = 2k \geq 4$$

of variables. We write f in the shape

$$f(\boldsymbol{x}) = \frac{1}{2} \boldsymbol{x}^t \cdot \boldsymbol{F} \cdot \boldsymbol{x}$$

so that the elements of matrix $\boldsymbol{F}$ are integers and those on the principal diagonal are even. We define the *level* of f as being the integer $N > 0$ such that

$$N\boldsymbol{F}^{-1}$$

corresponds in the same way to a primitive integer-valued form. It may be easily verified that N and $\det \boldsymbol{F}$ have the same prime factors.

5.2 Dirichlet character

We define now the character

$$\chi(a) = \left(\frac{(-1)^k \det \boldsymbol{F}}{a} \right) \tag{9}$$

where the symbol on the right side is the Kronecker symbol and a is any integer. The definition of the Kronecker symbol $\left(\frac{b}{n}\right)$ follows [16, Chap. 4]. If $n = p$ is an odd prime, then, for any integer b,

$$\left(\frac{b}{p}\right) = \begin{cases} 0 & \text{if } \gcd(b,p) \neq 1, \\ 1 & \text{if } b \text{ is a square mod } p, \\ -1 & \text{if } b \text{ is not a square mod } p. \end{cases}$$

If $p = 2$, then

$$\left(\frac{b}{2}\right) = \begin{cases} 0 & \text{if } b \text{ is even}, \\ 1 & \text{if } b \equiv \pm 1 \pmod 8, \\ -1 & \text{if } b \equiv \pm 3 \pmod 8. \end{cases}$$

More generally, if $n = \prod_i p_i^{e_i}$ where the p_i are prime, then

$$\left(\frac{b}{n}\right) = \prod_i \left(\frac{b}{p_i}\right)^{e_i}.$$

It can be shown that the character χ, defined in eq. (9), is a Dirichlet character of modulus N [17, Appendix B].

5.3 Theta series as a modular form

Consider the quadratic form of eq. (8) with n variable ($n = 2k \geq 4$). This quadratic form is associated to a $n-$dimensional Euclidean lattice Λ via its Gram matrix. Define the theta series of Λ as

$$\Theta_\Lambda(q) = \sum_{\boldsymbol{x} \in \Lambda} q^{\|x\|^2} = \sum_{\boldsymbol{u} \in \mathbb{Z}^n} q^{f(\boldsymbol{u})}.$$

Λ is said to be integral, of level N, as the quadratic form f.

Theorem 1. *The theta series of Λ is a modular form, for the congruence group*

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} \star & \star \\ 0 & \star \end{bmatrix} \ (mod\ N) \right\},$$

of weight k and Dirichlet character χ of eq. (9).

5.4 Properties of $M_k(\Gamma_0(N), \chi)$

The space of modular forms $M_k(\Gamma_0(N), \chi)$ is the sum of a subspace of Eisenstein series and of cusp forms

$$M_k(\Gamma_0(N), \chi) = \mathcal{E}_k(\Gamma_0(N), \chi) \oplus \mathcal{S}_k(\Gamma_0(N), \chi). \tag{10}$$

But here, the dimension of the space of Eisenstein series can be more than 1. So, from (10), we deduce that

$$\boxed{\Theta_\Lambda(q) = \Theta_{\Lambda,e}(q) + \Theta_{\Lambda,s}(q)} \tag{11}$$

where $\Theta_{\Lambda,e}(q)$ is a linear combination of Eisenstein series and $\Theta_{\Lambda,s}(q)$ is a cusp form.

5.5 Example in dimension 4

D_4 is a lattice of level $N = 2$. Gram matrix is

$$\boldsymbol{F} = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & -1 & 0 \\ 1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix}$$

and $\det \boldsymbol{F} = 4$. Take $a = \prod p^{\alpha(p)}$. Then, the Dirichlet character is

$$\chi(a) = \left(\frac{4}{a}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod 2 \\ 1 & \text{if } a \equiv 1 \pmod 2 \end{cases}.$$

The congruence modular group defining the modular form where $\Theta_{D_4}(q)$ lives is $\Gamma_0(2)$. Weight of the modular form is $k = 2$. There is, in $M_2(2, \chi)$ one Eisenstein series $E_{2,0}(q)$ and no cusp form. So,

$$\Theta_{D_4}(q) = E_{2,0}(q) = 1 + 24q^2 + 24q^4 + 96q^6 + \cdots$$

Figure 6 gives the secrecy function of D_4. Note that the secrecy gain is now achieved at $y_0 = \frac{1}{\sqrt{2}}$.

5.6 Asymptotic analysis

For a lattice Λ, whose theta series is given in eq. (11), the series in the Eisenstein subspace, $\Theta_{\Lambda,e}(q)$ is called the singular series. It only depends on the genus of the lattice Λ. When n is large enough, then, the coefficients of $\Theta_{\Lambda,e}(q)$ are asymptotic estimates of the coefficients of the theta series of Λ since they are of a larger order of magnitude than those of the cusp form $\Theta_{\Lambda,s}(q)$. So, there is a concentration result which says that, for n large enough, all lattices in the same genus have a theta series approximately given by $\Theta_{\Lambda,e}(q)$.

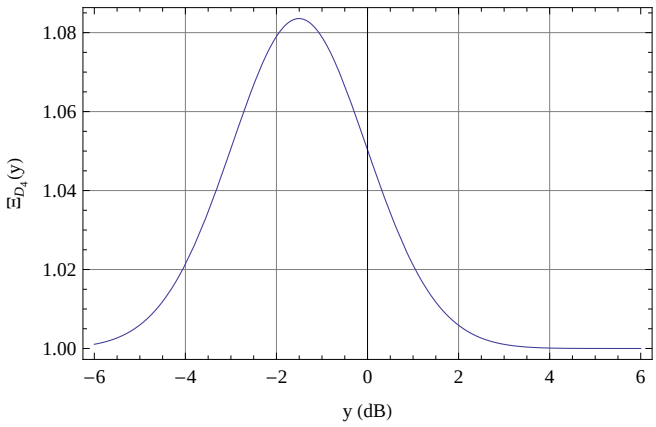

Fig. 6. Secrecy function of the checkerboard lattice D_4

6 Conclusion

The secrecy gain introduced in [8] is a new lattice invariant that measures how much confusion the eavesdropper will experience. This parameter is based on the value of the theta series of lattice Λ_e at some point that depends on the lattice itself. We can analyze how secrecy gain behaves, when dimension grows up, It depends on some Eisenstein series calles the singular series. Next step consists now in studying the behavior of this series and relating these parameters to the system parameters.

References

1. L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. Journal*, vol. 63, no. 10, pp. 2135–2157, December 1984.
2. R. Zamir, S. Shamai, and U. Erez, "Linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, June 2002.
3. S. Pradhan and K. Ramchandran, "Generalized coset codes for distributed binning," *IEEE Trans. Inf. Theory*, October 2005.
4. A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, August 2007.
5. D.Klinc, J.Ha, S. McLaughlin, J.Barros, and B. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. Information Theory Workshop*, October 2009.
6. S. Y. El Rouayheb and E. Soljanin, "On wiretap networks II," in *Proceedings ISIT*, 2007.
7. X. He and A. Yener, "Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels," July 2009. [Online]. Available: http://arxiv.org/pdf/0907.5388
8. J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design," ISITA 2010, 2010. [Online]. Available: arXiv:1004.4075v1 [cs.IT]

9. A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, October 1975.
10. J. Conway and N. Sloane, *Sphere packings, Lattices and Groups*, 3rd ed. Springer-Verlag, 1998.
11. E. Weisstein, "Jacobi Theta Functions," MathWorld – A Wolfram Web Resource. [Online]. Available: http://mathworld.wolfram.com/JacobiThetaFunctions.html
12. N.-P. Skoruppa, "Reduction mod ℓ of Theta Series of level ℓ^n." [Online]. Available: arXiv:0807.4694v2 [math.NT]
13. W. Ebeling, *Lattices and Codes*. Advanced Lectures in Mathematics, 1994.
14. J.-P. Serre, *A course in arithmetic*, ser. Graduate Texts in Mathematics. Springer, 1996.
15. F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap gaussian channel: Construction and analysis," *IEEE Trans. Inf. Theory*, 2011, submitted, on line on ArXiv.
16. W. Stein, *Modular Forms, a Computational Approach*, ser. Graduate Studies in Mathematics. AMS, 2007, vol. 79.
17. J. Cassels, *Rational Quadratic Forms*, ser. Dover Books on Mathematics. Dover, 1978.