Secrecy gain of Gaussian wiretap codes from unimodular lattices

Lin, Fuchun; Oggier, Frederique

2011

Lin, F., & Oggier, F. (2011). Secrecy Gain of Gaussian Wiretap Codes from Unimodular Lattices. Paper presented at the Information Theory Workshop (ITW), 2011 IEEE, 718-722.

<https://hdl.handle.net/10356/93876>

<https://doi.org/10.1109/ITW.2011.6089529>

© 2011 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [DOI: <http://dx.doi.org/10.1109/ITW.2011.6089529>]

Downloaded on 26 Apr 2023 13:05:41 SGT

Secrecy Gain of Gaussian Wiretap Codes from Unimodular Lattices

Fuchun Lin and Frédérique Oggier

Division of Mathematical Sciences

School of Physical and Mathematical Sciences

Nanyang Technological University

Singapore 637371

Email: linf0007@e.ntu.edu.sg and frederique@ntu.edu.sg

Abstract—We consider lattice coding over a Gaussian wiretap channel, where an eavesdropper listens to the transmissions between a transmitter and a legitimate receiver. In [1], a new lattice invariant called the secrecy gain was introduced as a code design criterion for wiretap lattice codes, shown to characterize the confusion that a chosen lattice code can cause at the eavesdropper: the higher the secrecy gain of the lattice, the more confusion. In this paper, a formula for the secrecy gain of unimodular lattices is derived. Secrecy gains of extremal odd unimodular lattices as well as unimodular lattices in dimension 16 are computed and compared. Finally, best wiretap lattice codes coming from unimodular lattices in dimension n , $8 \leq n \leq 16$ are classified.

I. INTRODUCTION

The wiretap channel was introduced by Wyner [2] 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 ensured at the same time, by exploiting (via coding) the physical difference between the channel to Bob and that to Eve. Many results of information theoretical nature are available in the literature for various classes of channels (see e.g. [3] for a survey) capturing the trade-off between reliability and secrecy and aiming at determining the highest information rate that can be achieved with perfect secrecy, the so-called *secrecy capacity*. Coding results focusing on constructing concrete codes that can be implemented in a specific channel are much fewer (see [4], [5] for examples of wiretap codes dealing with channels with erasures).

In this paper, we will concentrate on Gaussian wiretap channels, whose secrecy capacity was established in [6]. Examples of existing Gaussian wiretap codes were designed for binary inputs, as in [7]. A different approach was adopted in [1], where lattice codes were proposed, using as design criterion a new lattice invariant called *secrecy gain*, which was shown to characterize the confusion at the eavesdropper. This suggests the study of the secrecy gain of lattices as a way to understand how to design a good Gaussian wiretap code. *Unimodular* lattices were shown to be good candidates in [8] and for *even unimodular* lattices, both secrecy gains for a special class of lattices called *extremal* lattices were computed and the asymptotic behavior of the average secrecy gain as

a function of the dimension n was investigated. These two papers were further developed in [9], where coding examples were detailed and it was shown that as n grows to infinity, all even unimodular lattices behave in the same way, so that optimizing the secrecy gain makes sense in small dimensions.

The work of [8] deals with even unimodular lattices, which only exist in dimension a multiple of 8. We pursue the study of unimodular lattices by considering odd unimodular lattices, which on the contrary exist in every dimension and in great number, giving thus more flexibility in the code design. We will also show an example in dimension 16 where an odd unimodular lattice outperforms even unimodular lattices.

The paper is organized as follows. In Section II, we recall the definition of the secrecy gain and the previous results concerning this lattice invariant. An explicit formula for the secrecy gain of unimodular lattices, which generalizes the one for even case in [9], is derived in Section III. Extremal unimodular lattices are considered and the secrecy gains for the odd case are computed in Section IV. The secrecy gains of the three unimodular lattices in dimension 16, one odd and two even, are computed in Section V and for the first time the secrecy gains of nontrivial odd and even unimodular lattices in the same dimension are compared. Finally, in Section VI, best wiretap lattice codes coming from unimodular lattices in dimension n , $8 \leq n \leq 16$ are classified.

II. PREVIOUS RESULTS

Let us start by recalling the definition of a unimodular lattice. The dual Λ^* of a lattice Λ of dimension n is

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

The lattice Λ is called *integral* if $\Lambda \subset \Lambda^*$, and in particular, *unimodular* if $\Lambda = \Lambda^*$. Consequently, the (squared) *norm* $\mathbf{x} \cdot \mathbf{x}$ of a vector $\mathbf{x}$ in an integral lattice, especially in a unimodular lattice Λ , is an integer. If the norm is an even integer for any vector in Λ , then Λ is called an *even unimodular* lattice, also called *type II* lattice. Otherwise, it is called an *odd unimodular* lattice, also called *type I* lattice. The *volume* $\text{vol}(\mathbb{R}^n/\Lambda)$ of a lattice Λ is defined to be the volume of the *fundamental parallelepiped*. Then Λ is a unimodular lattice if and only if Λ is integral and $\text{vol}(\mathbb{R}^n/\Lambda) = 1$.

Unimodular lattices will be used for coding over a Gaussian wiretap channel, which is modeled as follows: 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 with noise variance σ_e^2 , where $\sigma_b^2 \leq \sigma_e^2$, in order to have a positive secrecy capacity [6]. Lattice encoding is done via a generic coset coding strategy [1]: let $\Lambda_e \subset \Lambda_b$ be two nested lattices. The information vector is mapped to a coset in Λ_b/Λ_e , after which a vector is randomly chosen from the coset as the encoded word. Since Eve's probability of correct decoding can be seen [1] to depend on

$$\sum_{\mathbf{x} \in \Lambda_e} e^{-\mathbf{x} \cdot \mathbf{x} / 2\sigma_e^2}, \quad (1)$$

the lattice Λ_e can be interpreted as introducing confusion for Eve, while Λ_b is intended to ensure reliability for Bob. This quantity can now be connected to an invariant of the lattice Λ_e called its theta series. In what follows, we set

$$q = e^{\pi i \tau}, \tau \in \mathcal{H},$$

where $\mathcal{H}$ denotes the *upper half-plane* of complex numbers with strictly positive imaginary part.

Definition II.1. *The theta series of a lattice Λ is defined by*

$$\Theta_\Lambda(\tau) = \sum_{\lambda \in \Lambda} q^{\lambda \cdot \lambda}.$$

This definition extends naturally to that of a lattice translate.

The theta series of an integral lattice Λ can be written as

$$\Theta_\Lambda(\tau) = \sum_{m=0}^{\infty} A_m q^m. \quad (2)$$

It is a book keeping device recording the number of vectors $\lambda \in \Lambda$ with norm n in the coefficient A_n . Theta series of well known lattices can often be formulated in terms of the following *Jacobi theta functions*:

$$\begin{aligned} \vartheta_2(\tau) &= \sum_{n \in \mathbb{Z}} q^{(n+\frac{1}{2})^2}, \\ \vartheta_3(\tau) &= \sum_{n \in \mathbb{Z}} q^{n^2}, \\ \vartheta_4(\tau) &= \sum_{n \in \mathbb{Z}} (-q)^{n^2}. \end{aligned}$$

Take the one-dimensional lattice $\mathbb{Z}$ for example. We have

$$\Theta_{\mathbb{Z}}(\tau) = 1 + 2q^1 + 2q^4 + 2q^9 + \dots = \vartheta_3(\tau). \quad (3)$$

The following two equalities can also be deduced immediately from the definition of theta series:

$$\Theta_{\mathbb{Z}^k}(\tau) = \vartheta_3^k(\tau) \text{ and } \Theta_{k\Lambda}(\tau) = \Theta_\Lambda(k^2\tau). \quad (4)$$

Motivated by (1), the confusion brought by the lattice Λ_e with respect to no coding (namely, use a scaled version of the lattice $\mathbb{Z}^n$ with the same volume) is measured as follows:

Definition II.2. *Let Λ be an n -dimensional lattice of volume v^n . The secrecy function of Λ is given by*

$$\Xi_\Lambda(\tau) = \frac{\Theta_{v\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \tau \in \mathcal{H}.$$

The secrecy gain is then the maximal value of the secrecy function and is denoted by χ_Λ .

A large class of lattices were shown to have a point of symmetry in their secrecy function (called *weak secrecy gain*) through the *Poisson summation formula*, conjectured to achieve the maximal value of the secrecy function [8], [9]. Among them are the unimodular lattices whose secrecy functions have a symmetry point at $\tau = i$, namely,

$$\chi_\Lambda = \Xi_\Lambda(i) = \frac{\vartheta_3^n(i)}{\Theta_\Lambda(i)}. \quad (5)$$

It was a conjecture by Belfiore and Solé [8], proven by A.-M. Ernvall-Hytönen [10], that for even unimodular lattices, $\tau = i$ is not only the symmetry point, but also the point achieving the secrecy gain.

To conclude this section, let us recall the definition of a few special functions¹ that will be needed to compute the secrecy gain of odd unimodular lattices in the rest of the paper.

Definition II.3. *The Eisenstein series $E_k(q)$ of weight k with k even and greater than 2 is defined by*

$$E_k(\tau) = \frac{1}{2\zeta(k)} \sum_{(c,d) \in \mathbb{Z}^2 - \{(0,0)\}} \frac{1}{(c\tau + d)^k},$$

where $\zeta(k)$ is the Riemann zeta function

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

Many Eisenstein series have a very nice expression in terms of Jacobi theta functions. For example,

$$E_4(\tau) = \frac{1}{2}(\vartheta_2^8(\tau) + \vartheta_3^8(\tau) + \vartheta_4^8(\tau)). \quad (6)$$

Definition II.4. *The discriminant function $\Delta_8(\tau)$ is defined by*

$$\Delta_8(\tau) = \frac{1}{24}(\vartheta_3^8(\tau) - E_4(\tau)) \quad (7)$$

and has Fourier expansion

$$\Delta_8(\tau) = q - 8q^2 + 28q^3 - 64q^4 + \dots \quad (8)$$

III. THE SECRECY GAIN OF UNIMODULAR LATTICES

We are now ready to give our first result, namely a general formula for the secrecy gain of unimodular lattices, which relies on the following lemma:

Lemma III.1. (Hecke)[11] *If Λ is a unimodular lattice then*

$$\Theta_\Lambda(\tau) \in \mathbb{C}[\vartheta_3(\tau), \Delta_8(\tau)].$$

From this lemma we have the following decomposition of the theta series of a unimodular lattice Λ

$$\Theta_\Lambda(\tau) = \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \vartheta_3^{n-8r}(\tau) \Delta_8^r(\tau), a_r \in \mathbb{Z}. \quad (9)$$

¹They are actually modular forms [11], [12], [13].

Consequently, the reciprocal of the secrecy gain of Λ is

$$\begin{aligned}
\frac{1}{\chi_\Lambda} &= \frac{\Theta_\Lambda(i)}{\vartheta_3(i)^n} \\
&= \frac{\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \vartheta_3^{n-8r}(i) \Delta_8^r(i)}{\vartheta_3^n(i)} \\
&= \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{\Delta_8(i)}{\vartheta_3^8(i)} \right)^r \\
&= \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{\frac{1}{2^4}(\vartheta_3^8(i) - E_4(i))}{\vartheta_3^8(i)} \right)^r \\
&= \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{\frac{1}{2^5}(\vartheta_3^8(i) - \vartheta_2^8(i) - \vartheta_4^8(i))}{\vartheta_3^8(i)} \right)^r \\
&= \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{\frac{1}{2^5}(4\vartheta_4^8(i) - \vartheta_3^8(i) - \vartheta_4^8(i))}{4\vartheta_4^8(i)} \right)^r \\
&= \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{1}{2^6} \right)^r,
\end{aligned}$$

where the first equality follows from (5), the second from (9), the fourth from (7), the fifth from (6) and the sixth from the following two useful equations concerning the Jacobi theta functions at $\tau = i$:

$$\vartheta_2(i) = \vartheta_4(i) \text{ and } \vartheta_3(i) = \sqrt[4]{2} \vartheta_4(i). \quad (10)$$

To summarize:

Theorem III.1. *The secrecy gain of a unimodular lattice Λ of dimension n can be written as*

$$\chi_\Lambda = \frac{1}{\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{1}{2^6} \right)^r}, \quad (11)$$

where the a_i 's are the coefficients in (9).

This generalizes the formula for the even case in [9].

IV. SECRECY GAINS OF EXTREMAL UNIMODULAR LATTICES

In order to find good Gaussian wiretap lattice codes, we look for unimodular lattices with high secrecy gain. In this section, we start by restricting our search to the class of extremal unimodular lattices.

Definition IV.1. *Let Λ be a lattice of dimension n . Λ is said to be an extremal lattice if its minimal norm is $\lfloor \frac{n}{8} \rfloor + 1$.²*

By definition, an extremal unimodular lattice Λ of dimension n contains no vector of norm $1, 2, \dots, \lfloor \frac{n}{8} \rfloor$, thus the coefficients of $q, q^2, \dots, q^{\lfloor \frac{n}{8} \rfloor}$ in the theta series given in (2) are all 0's. But by expanding (9), we can form another formal sum with coefficients represented as linear combinations of a_i 's. By comparing the first $\lfloor \frac{n}{8} \rfloor + 1$ terms of the two formal sums, we have a system of $\lfloor \frac{n}{8} \rfloor$ linear equations in $\lfloor \frac{n}{8} \rfloor$ unknowns $a_1, a_2, \dots, a_{\lfloor \frac{n}{8} \rfloor}$ (a_0 is obviously 1), from which a unique solution can be found. In this way, the secrecy gain of each extremal unimodular lattice can be computed.

The secrecy gain of the extremal lattice *Gosset Lattice* E_8 was computed in [8], [9]. We will compute it again here, as an example, solving the linear equations associated with extremal lattices. The theta series of E_8 looks like

$$\Theta_{E_8}(\tau) = 1 + 0q + A_2 q^2 + \dots, \quad A_2 \neq 0.$$

²The definition of extremal has changed. Here we use the earlier version.

TABLE I
SECRECY GAINS OF EXTREMAL ODD UNIMODULAR LATTICES

dim	lattices	theta series	secrecy gain
12	D_{12}^+	$\vartheta_3^{12} - 24\vartheta_3^4 \Delta_8$	$\frac{8}{5}$
14	E_7^{2+}	$\vartheta_3^{14} - 28\vartheta_3^6 \Delta_8$	$\frac{16}{9}$
15	A_{15}^+	$\vartheta_3^{15} - 30\vartheta_3^7 \Delta_8$	$\frac{32}{17}$
23	O_{23}	$\vartheta_3^{23} - 46\vartheta_3^{15} \Delta_8$	$\frac{32}{9}$

By (9), (3) and (8)

$$\begin{aligned}
\Theta_{E_8}(\tau) &= \vartheta_3^8(\tau) + a_1 \Delta_8(\tau) \\
&= (1 + 2q + \dots)^8 + a_1(q + \dots) \\
&= (1 + 16q + \dots) + a_1(q + \dots) \\
&= 1 + (16 + a_1)q + \dots
\end{aligned}$$

We now have one linear equation in one unknown a_1

$$16 + a_1 = 0,$$

which gives $a_1 = -16$, yielding the secrecy gain

$$\chi_{E_8} = \frac{1}{1 - 16 \times \frac{1}{2^6}} = \frac{4}{3}. \quad (12)$$

Let us compute one more example of extremal lattice, the *Shorter Leech Lattice* O_{23} . The theta series of O_{23} looks like

$$\Theta_{O_{23}}(\tau) = 1 + 0q + 0q^2 + A_3 q^3 + \dots, \quad A_3 \neq 0.$$

By (9), (3) and (8)

$$\begin{aligned}
\Theta_{O_{23}}(\tau) &= \vartheta_3^{23}(\tau) + a_1 \vartheta_3^{15}(\tau) \Delta_8(\tau) + a_2 \vartheta_3^7(\tau) \Delta_8^2(\tau) \\
&= (1 + 2q + \dots)^{23} + a_1 (1 + 2q + \dots)^{15} (q - 8q^2 + \dots) \\
&\quad + a_2 (1 + 2q + \dots)^7 (q - 8q^2 + \dots)^2 \\
&= (1 + 46q + 1012q^2 + \dots) + a_1 (q + 22q^2 + \dots) \\
&\quad + a_2 (q^2 + \dots) \\
&= 1 + (46 + a_1)q + (1012 + 22a_1 + a_2)q^2 + \dots
\end{aligned}$$

This time, we have two linear equations in a_1 and a_2

$$\begin{cases} 46 + a_1 = 0 \\ 1012 + 22a_1 + a_2 = 0 \end{cases},$$

which gives $a_1 = -46$ and $a_2 = 0$, yielding

$$\chi_{O_{23}} = \frac{1}{1 - 46 \times \frac{1}{2^6}} = \frac{32}{9}. \quad (13)$$

By applying this method, we have computed the secrecy gain for each extremal odd unimodular lattice in dimension ≥ 10 (see [11] for a classification), as shown in Table I³. A similar table for the even case can be found in [8], [9].

V. SECRECY GAINS OF UNIMODULAR LATTICES IN DIMENSION 16

There are three unimodular lattices in dimension 16, two even lattices D_{16}^+ , E_8^2 and one odd lattice D_{8+}^{2+} . We can use (9) again to compute the secrecy gains. Take D_{8+}^{2+} for example. It is a *root lattice*, which means it does not contain vector of norm 1. So $A_1 = 0$. Its *kissing number* is 224, which means

³“+” is used to emphasize the existence of *glue vectors*.

that the first nonzero coefficient $A_2 = 224$. So the theta series of D_8^{2+} looks like

$$\Theta_{D_8^{2+}}(\tau) = 1 + 0q + 224q^2 + A_3q^3 + \dots \quad (14)$$

On the other hand, we have by (9)

$$\Theta_{D_8^{2+}}(\tau) = \vartheta_3^{16}(\tau) + a_1\vartheta_3^8(\tau)\Delta_8(\tau) + a_2\Delta_8^2(\tau). \quad (15)$$

Linear equations in a_1 and a_2 can be derived by comparing (14) and (15). And the solution is $a_1 = -32$ and $a_2 = 0$ yielding the secrecy gain

$$\chi_{D_8^{2+}} = \frac{1}{1 - 32 \times \frac{1}{2^6}} = 2. \quad (16)$$

But we want to introduce another way of computing secrecy gain. When lattice codes are obtained from error correction codes via the so-called *Construction A*, their secrecy gain can be computed thanks to the weight enumerator of the code considered.

Let $\rho : \mathbb{Z}^n \rightarrow \mathbb{F}_2^n$ be the map of component wise reduction modulo 2 defined on $\mathbb{Z}^n$. Let C be a binary $[n, k, d]$ code. Then $\rho^{-1}(C)$ is a free Abelian group of rank n and hence is a lattice in $\mathbb{R}^n$.

Definition V.1. The lattice Γ_C generated by C is defined by

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

There is a connection between the theta series of Γ_C and the weight enumerator of C , which we can exploit to compute the theta series of a lattice.

Theorem V.1. [11] Let C be a linear binary code with weight enumerator $W_C(x, y)$. Then the theta series of Γ_C is given by

$$\Theta_{\Gamma_C}(\tau) = W_C(\vartheta_3(2\tau), \vartheta_2(2\tau)). \quad (17)$$

Let us begin with a trivial example. The lattice $\frac{1}{\sqrt{2}}\mathbb{Z}^n$ is generated by the universal code C with weight enumerator $W_C(x, y) = (x + y)^n$. By (17) we have

$$\Theta_{\frac{1}{\sqrt{2}}\mathbb{Z}^n}(\tau) = (\vartheta_3(2\tau) + \vartheta_2(2\tau))^n,$$

from which we further deduce through (3) and (4) that

$$\vartheta_3^n\left(\frac{1}{2}\tau\right) = (\vartheta_3(2\tau) + \vartheta_2(2\tau))^n \quad (18)$$

and

$$\vartheta_4^n\left(\frac{1}{2}\tau\right) = (\vartheta_3(2\tau) - \vartheta_2(2\tau))^n. \quad (19)$$

The Checkerboard Lattice D_n can be constructed from the $[n, n-1, 2]$ even-weight code C by taking $D_n = \rho^{-1}(C)$, which is a scaled version of Γ_C , namely, $D_n = \sqrt{2}\Gamma_C$. The weight enumerator of C is

$$W_C(x, y) = \frac{1}{2}((x + y)^n + (x - y)^n).$$

By (4), (17), (18) and (19), we get

$$\Theta_{D_n}(\tau) = \frac{1}{2}(\vartheta_3^n(\tau) + \vartheta_4^n(\tau)). \quad (20)$$

The lattice D_n^+ with n even is defined by

$$D_n^+ = D_n \cup \left(\frac{1}{2}, \dots, \frac{1}{2}\right) + D_n.$$

It can be shown that the translate $(\frac{1}{2}, \dots, \frac{1}{2}) + D_n$ has theta series $\frac{1}{2}\vartheta_2^n(\tau)$. By (20) we have

$$\Theta_{D_n^+}(\tau) = \frac{1}{2}(\vartheta_2^n(\tau) + \vartheta_3^n(\tau) + \vartheta_4^n(\tau)). \quad (21)$$

The secrecy gain of D_{16}^+ can be computed from the theta series of D_n^+ :

$$\begin{aligned} \chi_{D_{16}^+} &= \frac{\vartheta_3^{16}(i)}{\Theta_{D_{16}^+}(i)} \\ &= \frac{\vartheta_3^{16}(i)}{\frac{1}{2}(\vartheta_2^{16}(i) + \vartheta_3^{16}(i) + \vartheta_4^{16}(i))} \\ &= \frac{16\vartheta_4^{16}(i)}{\frac{1}{2}(\vartheta_4^{16}(i) + 16\vartheta_4^{16}(i) + \vartheta_4^{16}(i))} \\ &= \frac{16}{9}, \end{aligned}$$

where the first equality follows from (5), the second from (21) and the third from (10).

Finally, the secrecy gain of E_8^2 follows from (12):

$$\chi_{E_8^2} = \chi_{E_8}^2 = \frac{16}{9}.$$

Now that we have computed the secrecy gain of both odd and even unimodular lattices in dimension 16, we can for the first time compare the performance of odd and even unimodular lattices in the same dimension. It is somewhat surprising and thus promising to remark that the secrecy gain of D_8^{2+} is greater than that of D_{16}^+ and E_8^2 .

VI. ENUMERATION OF UNIMODULAR LATTICES IN DIMENSION n , $8 \leq n \leq 16$

As mentioned in Section II, the secrecy gain of a lattice Λ characterizes the amount of the confusion at Eve that is gained by using this lattice Λ as Λ_e in the Gaussian wiretap code $\Lambda_e \subset \Lambda_b$. We naturally wish to use lattices with large secrecy gain. In this section, we classify the best unimodular lattice wiretap codes in dimension n , $8 \leq n \leq 16$.

To start with, Table II provides a list of all unimodular lattices of dimension n , $8 \leq n \leq 16$. It suffices to compute the secrecy gains of the underlined lattices, since “adding” $\mathbb{Z}^k$ to a lattice does not change its secrecy gain. More precisely:

$$\chi_{\mathbb{Z}^k + \Lambda} = \frac{\vartheta_3^n(i)}{\vartheta_3^k(i)\Theta_\Lambda(i)} = \frac{\vartheta_3^{n-k}(i)}{\Theta_\Lambda(i)} = \chi_\Lambda.$$

The underlined lattices happen to be extremal unimodular lattices except for those in dimension 16, whose secrecy gains are computed in Section V.

Now that we have established the secrecy gain of all the unimodular lattices in dimension smaller than 16, we need to be able to use these lattices (in particular those with the highest secrecy gain) to provide lattice codes. To do so, lattice encoding should be performed, which can be handled via Construction A, assuming that we can associate to the chosen lattice a suitable error correction code. To help identify which, if any, error correction code corresponds to a given lattice, we use the following known result:

TABLE II
UNIMODULAR LATTICES OF DIMENSION n , $8 \leq n \leq 16$

type I	type II
$\mathbb{Z}^8$	$\underline{E_8}$
$\mathbb{Z}^9, E_8 + \mathbb{Z}$	
$\mathbb{Z}^{10}, E_8 + \mathbb{Z}^2$	
$\mathbb{Z}^{11}, E_8 + \mathbb{Z}^3$	
$\mathbb{Z}^{12}, E_8 + \mathbb{Z}^4, D_{12}^+$	
$\mathbb{Z}^{13}, E_8 + \mathbb{Z}^5, D_{12}^+ + \mathbb{Z}$	
$\mathbb{Z}^{14}, E_8 + \mathbb{Z}^6, D_{12}^+ + \mathbb{Z}^2, E_7^{2+}$	
$\mathbb{Z}^{15}, A_{15}^+, E_8 + \mathbb{Z}^7, D_{12}^+ + \mathbb{Z}^3, \overline{E_7^{2+}} + \mathbb{Z}$	
$\mathbb{Z}^{16}, A_{15}^+ + \mathbb{Z}, E_8 + \mathbb{Z}^8, D_{12}^+ + \mathbb{Z}^4, E_7^{2+} + \mathbb{Z}^2, D_8^{2+}$	E_8^2, D_{16}^+

TABLE III
BINARY SELF-DUAL CODES OF LENGTH n , $8 \leq n \leq 16$

length	type I codes	type II codes
8		$[8, 4, 4]$
9		
10		
11		
12	$[12, 6, 4]$	
13		
14	$[14, 7, 4]$	
15		
16	$[16, 8, 4]$	$[16, 8, 4]^\dagger, [16, 8, 4]^\ddagger$

Theorem VI.1. [13] *Let C be a binary linear code and Γ_C be the lattice generated by C . Then*

- 1) $C \subset C^\perp$ if and only if Γ_C is an integral lattice;
- 2) C is doubly even if and only if Γ_C is an even lattice;
- 3) C is self-dual if and only if Γ_C is unimodular.

A self-dual code is always an even code. It is called a *type II* code if it is doubly even and *type I* otherwise. By Theorem VI.1, C is a type I (respectively type II) code if and only if Γ_C is a type I (respectively type II) lattice. Table III⁴ gives a list of all binary self-dual codes of length n , $8 \leq n \leq 16$.

To summarize what have been computed and reasoned so far, we combine Table I, II, III and other results to give a classification of the best unimodular lattice Gaussian wiretap codes in dimension n , $8 < n \leq 16$ as shown in Table IV.

VII. CONCLUSION AND FUTURE WORK

A recent line of work on lattice codes for Gaussian wiretap channels introduced a new lattice invariant called secrecy gain as a code design criterion which captures the confusion that lattice coding can introduce at an eavesdropper. So far, only the secrecy gain of even unimodular lattices was studied. In this paper, we pursued the study of unimodular lattices by investigating the case of odd unimodular lattices, which exist in greater number and, unlike even lattices, in any dimension. We provided a general formula for the secrecy gain of unimodular lattices in general. We then computed the secrecy gain for odd unimodular lattices, both extremal, and in small dimensions. As a result, we gave a classification of the best unimodular lattice wiretap codes in small dimensions.

${}^4[16, 8, 4]^\dagger, [16, 8, 4]^\ddagger$ are two distinct type II codes with the same weight distribution.

TABLE IV
UNIMODULAR LATTICES WITH BEST SECRECY GAIN

n	type I lattices (codes)	type II lattices (codes)	secrecy gain
8		$E_8 \sim [8, 4, 4]$	$\frac{4}{3}$
9	$E_8 + \mathbb{Z}$		$\frac{4}{3}$
10	$E_8 + \mathbb{Z}^2$		$\frac{4}{3}$
11	$E_8 + \mathbb{Z}^3$		$\frac{4}{3}$
12	$D_{12}^+ \sim [12, 6, 4]$		$\frac{5}{3}$
13	$D_{12}^+ + \mathbb{Z}$		$\frac{5}{3}$
14	$E_7^{2+} \sim [14, 7, 4]$		$\frac{9}{16}$
15	A_{15}^+		$\frac{32}{17}$
16	$D_8^{2+} \sim [16, 8, 4]$	$E_8^2 \sim [16, 8, 4]^\dagger$ $D_{16}^+ \sim [16, 8, 4]^\ddagger$	$\frac{16}{9}$ $\frac{16}{9}$ 2

The encoding/labeling of the proposed wiretap codes, taking into account both channel parameters and power constraint are being naturally elaborated.

Future work on unimodular wiretap lattice codes concerns the asymptotic behavior of odd unimodular lattices. More generally, it is of interest to generalize the existing work on unimodular lattices to other classes of lattices.

ACKNOWLEDGMENT

The research of both F. Lin and F. Oggier for this work is supported by the Singapore National Research Foundation under the Research Grant NRF-RF2009-07.

The authors would like to thank the reviewers for their comments.

REFERENCES

- [1] J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design," ISITA 2010. <http://arXiv:1004.4075v2> [cs.IT].
- [2] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, October 1975.
- [3] 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.
- [4] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. Journal*, vol. 63, no. 10, pp. 2135-2157, Dec. 1984.
- [5] A. Thangaraj, S. Dihidar, A. R. Calderbank, S.W. McLaughlin, and J.-M. Merolla, "Applications of LDPC Codes to the Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 53, No. 8, Aug. 2007
- [6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel", *IEEE Trans. Inform. Theory*, vol. IT-24, no. 4, pp. 451-456, July 1978.
- [7] D. Kline, 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 P. Solé, "Unimodular lattices for the Gaussian Wiretap Channel," *ITW 2010*, Dublin. <http://arXiv:1007.0449v1> [cs.IT].
- [9] F. Oggier, J.-C. Belfiore, and P. Solé, "Lattice Coding for the Wiretap Gaussian Channel", <http://arXiv:1103.4086v1> [cs.IT], 21 Mar 2011.
- [10] A.-M. Ernvall-Hytönen, "On a Conjecture by Belfiore and Solé on some Lattices", http://arxiv.org/PS_cache/arxiv/pdf/1104/1104.3739v2.pdf
- [11] J.H. Conway, N.J.A. Sloane, "Sphere packings, Lattices and Groups," Third edition, Springer-Verlag, New York, 1998.
- [12] J. W. S. Cassels, "Rational Quadratic Forms", Academic Press, NY, 1978.
- [13] W. Ebeling, "Lattices and Codes", *Advanced Lectures in Mathematics*, Vieweg & Sohn, Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1994.