Secrecy gain of Gaussian wiretap codes from 2- and 3-modular lattices

Lin, Fuchun; Oggier, Frederique

2012

Lin, F., & Oggier, F. (2012). Secrecy Gain of Gaussian Wiretap Codes from 2- and 3-Modular Lattices. 2012 IEEE International Symposium on Information Theory Proceedings, pp.1747-1751.

https://hdl.handle.net/10356/94795

https://doi.org/10.1109/ISIT.2012.6283577

Secrecy Gain of Gaussian Wiretap Codes from 2- and 3-Modular Lattices

Fuchun Lin and Frédérique Oggier
Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, 21 Nanyang Link, Singapore 637371
Emails: linf0007@e.ntu.edu.sg and frederique@ntu.edu.sg

***Abstract*—Lattice coding over a Gaussian wiretap channel is considered with respect to a lattice invariant called the secrecy gain, which was introduced in [1] to characterize the confusion that a chosen lattice can cause at the eavesdropper: the higher the secrecy gain of the lattice, the more confusion. In this paper, secrecy gains of several 2- and 3-modular lattices are computed. Most are shown to have a secrecy gain larger than the best unimodular lattices can achieve.**

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 the physical difference between the channel to Bob and that to Eve via coding. A survey on this topic is available in [3]. Many results of information theoretical nature are available for various classes of channels 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 on constructing concrete codes that can be implemented in a specific channel are much fewer (see e.g. [4], [5] for examples of wiretap codes dealing with channels with erasures).

In this paper, we discuss 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. So far, the special class of unimodular lattices has been studied with particular emphasis on even unimodular lattices [8], [9]: the secrecy gain of extremal even unimodular lattices was computed, and the asymptotic behavior of the average secrecy gain as a function of the dimension n was investigated. The results show that maximizing the secrecy gain is meaningful in small dimensions and infinite secrecy gain (implying complete secrecy) is possible as n grows to infinity. Unimodular lattices in small dimensions, both odd and even, were considered in [10], [11] resulting in a complete classification in dimension n, $n \leq 23$, featuring some odd lattices outperforming their even counter parts. It is natural to wonder whether other classes of lattices would have a better secrecy gain. The contribution of this paper is to initiate the study of the secrecy gain of other modular lattices. Since the secrecy gain depends on the *theta series* of the lattice considered, it makes sense to start with even 2- and 3-modular lattices, whose theta series have a decomposition formula similar to that of even unimodular lattices. Our results show that 2- and 3-modular lattices indeed achieve a secrecy gain larger than that of unimodular lattices in all the dimensions treated so far, but for $n = 22$.

II. Preliminaries and previous results

A Gaussian wiretap channel is a broadcast Gaussian channel modeled by

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

where $\mathbf{x}$ is the codeword sent by the transmitter (Alice), $\mathbf{y}$ and $\mathbf{z}$ are the received signals at the legitimate receiver (Bob), respectively at the eavesdropper (Eve), with corresponding noise vectors $\mathbf{v_b}$ and $\mathbf{v_e}$, whose components are i.i.d. Gaussian distributed with zero mean and respective variance σ_b^2 and σ_e^2.

It is assumed that $\sigma_b^2 < \sigma_e^2$ in order to have a positive secrecy capacity [6]. We suppose that $\mathbf{x} \in \mathbb{R}^n$ is a lattice codeword, where by a lattice Λ we mean a discrete set of points in $\mathbb{R}^n$, which can be conveniently described by

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

where the *generator matrix* M stores as row vectors a basis for the lattice.

Lattice encoding for the wiretap channel (1) is done via a generic coset coding strategy [1]: 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 coset in Λ_b/Λ_e, after which a vector is randomly chosen from the coset as the encoded word. The lattice Λ_e will be interpreted as introducing confusion for Eve, while Λ_b as ensuring reliability for Bob. A bound on Eve's probability $P_{c,e}$ of correct decoding shows [1] that to minimize $P_{c,e}$ is to minimize

$$\sum_{\mathbf{t} \in \Lambda_e} e^{-||\mathbf{t}||^2/2\sigma_e^2}, \tag{2}$$

where $||\mathbf{t}||^2$ is the *norm (squared length)* of a lattice point. Let $\mathcal{H} = \{a + ib \in \mathbb{C} | b > 0\}$ denote the upper half plane and set

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

Definition 2.1: The theta series of a lattice Λ is defined by

$$\Theta_\Lambda(\tau) = \Sigma_{\lambda \in \Lambda} q^{||\lambda||^2}.$$

It can be easily recognized that (2) is in fact the theta series of Λ_e at $\tau = \frac{i}{2\pi\sigma_e^2}$. Motivated by the above argument, the confusion brought by the lattice Λ_e with respect to no coding (namely, use the lattice $\mathbb{Z}^n$ scaled to the same *volume*, where the volume vol(Λ) of a lattice Λ is by definition the determinant of its generator matrix) is measured as follows [1]:

Definition 2.2: Let Λ be an n-dimensional lattice of volume V. The *secrecy function* of Λ is given by

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

The *secrecy gain* is then the maximal value of the secrecy function with respect to τ and is denoted by χ_Λ.

The theta series of a lattice is in general difficult to analyze except for special classes of lattices. We will take a closer look at one of them, the family of ℓ-modular lattices. 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 point in an integral lattice Λ is always an integer. If the norm is even for any lattice point, 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. Since the norms are all integers, we can combine the terms with the same norm and write

$$\Theta_\Lambda(\tau) = \Sigma_{n=0}^{\infty} A_n q^n. \tag{3}$$

A lattice is said to be *equivalent*, or geometrically similar to its dual, if it differs from its dual only by possibly a rotation, reflection and change of scale. An integral lattice that is equivalent to its dual is called a *modular* lattice. Or as it was first defined by H.-G. Quebbemann [12], an n-dimensional integral lattice Λ is modular if there exists a similarity σ of $\mathbb{R}^n$ such that $\sigma(\Lambda^*) = \Lambda$. If σ multiplies norms by ℓ, Λ is said to be ℓ-*modular*. In the particular case when the similarity factor $\ell = 1$, such lattices are *unimodular* lattices, corresponding to the more familiar definition $\Lambda = \Lambda^*$. It can be shown that if Λ is an ℓ-modular lattice of dimension n, then

$$\text{vol}(\Lambda) = \ell^{\frac{n}{4}}. \tag{4}$$

We will need the following concepts and formulae from analytic number theory for our discussion, for which we refer the readers to [13], [14] for more details.

Definition 2.3: The Jacobi theta functions are defined as follows:

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

Definition 2.4: The Dedekind eta function is defined by

$$\eta(\tau) = q^{\frac{1}{12}} \prod_{n=1}^{\infty} (1 - q^{2n}).$$

The Jacobi theta functions and the Dedekind eta function are connected as follows [13]:

$$\begin{cases} \vartheta_2(\tau) & = \frac{2\eta(2\tau)^2}{\eta(\tau)}, \\ \vartheta_3(\tau) & = \frac{\eta(\tau)^5}{\eta(\frac{\tau}{2})^2 \eta(2\tau)^2}, \\ \vartheta_4(\tau) & = \frac{\eta(\frac{\tau}{2})^2}{\eta(\tau)}. \end{cases} \tag{5}$$

The following lemma [12] will play a crucial role.

Lemma 2.5: The theta series of an even ℓ-modular lattice of dimension $n = 2k$ when $\ell = 1,\ 2,\ 3$ belongs to a space of *modular forms* of weight k generated by the functions $\Theta_{2k_0}^{\lambda}(\tau)\Delta_{2k_1}^{\mu}(\tau)$ with integers $\lambda,\ \mu \geq 0$ satisfying $k_0\lambda + k_1\mu = k$, where for $\ell = 1,\ 2,\ 3$, $k_0 = 4,\ 2,\ 1$ respectively, $k_1 = \frac{24}{1+\ell}$, $\Theta_{2k_0}(\tau)$ denote the theta series of the modular lattices $E_8,\ D_4$ and A_2, respectively, and $\Delta_{2k_1}(\tau) = (\eta(\tau)\eta(\ell\tau))^{k_1}$.

Example 2.6: If $\ell = 1$, corresponding to the unimodular case, we know from Lemma 2.5 that $k_0 = 4$, $k_1 = \frac{24}{2} = 12$, $\Theta_{2k_0}(\tau) = \Theta_{E_8}(\tau)$, $\Delta_{2k_1}(\tau) = \eta^{24}(\tau)$, from which we deduce that if Λ is an even unimodular lattice of dimension $n = 2k$ then

$$\Theta_\Lambda(\tau) = \sum_{4\lambda + 12\mu = k} a_\mu \Theta_{E_8}^{\lambda}(\tau)\Delta_{24}^{\mu}(\tau). \tag{6}$$

The formula (6) was adopted in [8], [9] to compute the secrecy gains of several even unimodular lattices.

III. Secrecy gain of 2- and 3-modular lattices

Lattices that are equivalent to their duals were shown to have a symmetry point, called *weak secrecy gain*, at $\tau = \frac{i}{\text{vol}(\Lambda)^{\frac{2}{n}}}$ in their secrecy function [9]. It was conjectured in the same paper that for these lattices, the weak secrecy gain is actually the secrecy gain. Here we still use χ_Λ to denote the weak secrecy gain. This conjecture was recently proven by A.-M. Ernvall-Hytönen [15] for a special class of lattices called *extremal* even unimodular lattices and by F. Lin and F. Oggier [11] for unimodular lattices in dimension n, $8 < n \leq 23$. In this paper, we will compute the weak secrecy gain of known even 2- and 3-modular lattices, and claim that their secrecy gains are larger than that of unimodular lattices in the same dimension, since the secrecy gain is by definition the maximum of the secrecy function.

In order to write the secrecy function, we need to have the theta series of $\mathbb{Z}^n$ scaled to the right volume. Recall the

definition of the theta series of a lattice and the Jacobi theta function $\vartheta_3(\tau)$. We have that

$$\begin{cases} \Theta_{\mathbb{Z}}(\tau) & = \vartheta_3(\tau), \\ \Theta_{\mathbb{Z}^k}(\tau) & = \vartheta_3^k(\tau), \\ \Theta_{k\mathbb{Z}}(\tau) & = \vartheta_3(k^2\tau). \end{cases} \tag{7}$$

Now it follows from (4) and (7) that the theta series is

$$\Theta_{\ell^{\frac{1}{4}}\mathbb{Z}^n}(\tau) = \vartheta_3^n(\sqrt{\ell}\tau). \tag{8}$$

A. 2-modular lattices

According to Lemma 2.5, the theta series of an even 2-modular lattice Λ of dimension $n = 2k$ can be written as

$$\Theta_\Lambda(\tau) = \sum_{2\lambda+8\mu=k} a_\mu \Theta_{D_4}^\lambda(\tau)\Delta_{16}^\mu(\tau), \tag{9}$$

where

$$\Theta_{D_4}(\tau) = \frac{1}{2}\left(\vartheta_3^4(\tau) + \vartheta_4^4(\tau)\right) = 1 + 24q^2 + 24q^4 + 96q^6 + \cdots \tag{10}$$

and

$$\Delta_{16}(\tau) = \left(\eta(\tau)\eta(2\tau)\right)^8.$$

By (5), we can write $\Delta_{16}(\tau)$ in terms of Jacobi theta functions and compute the first few terms:

$$\Delta_{16}(\tau) = \frac{1}{256}\vartheta_2^8(\tau)\vartheta_3^4(\tau)\vartheta_4^4(\tau) = q^2 - 8q^4 + 12q^6 + \cdots. \tag{11}$$

The secrecy function of an even 2-modular lattice Λ of dimension n is then written as

$$\Xi_\Lambda(\tau) = \frac{\vartheta_3^n(\sqrt{2}\tau)}{\sum_{2\lambda+8\mu=k} a_\mu \Theta_{D_4}^\lambda(\tau)\Delta_{16}^\mu(\tau)},$$

or more conveniently,

$$\begin{aligned} 1/\Xi_\Lambda(\tau) &= \textstyle\sum_{2\lambda+8\mu=k} a_\mu \frac{\Theta_{D_4}^\lambda(\tau)\Delta_{16}^\mu(\tau)}{\vartheta_3^n(\sqrt{2}\tau)} \\ &= \textstyle\sum_{2\lambda+8\mu=k} a_\mu \left(\frac{\Theta_{D_4}(\tau)}{\vartheta_3^4(\sqrt{2}\tau)}\right)^\lambda \left(\frac{\Delta_{16}(\tau)}{\vartheta_3^{16}(\sqrt{2}\tau)}\right)^\mu. \end{aligned}$$

Now we only need to know the coefficients a_μ in order to compute the weak secrecy gain of a 2-modular lattice, once the following two quotients are computed:

$$\frac{\Theta_{D_4}(\tau)}{\vartheta_3^4(\sqrt{2}\tau)}\Big|_{\tau=\frac{i}{\sqrt{2}}} \text{ and } \frac{\Delta_{16}(\tau)}{\vartheta_3^{16}(\sqrt{2}\tau)}\Big|_{\tau=\frac{i}{\sqrt{2}}}.$$

Approximating $\alpha_2 = \frac{\Theta_{D_4}(\tau)}{\vartheta_3^4(\sqrt{2}\tau)}|_{\tau=\frac{i}{\sqrt{2}}}$:

We recognize that α_2 is basically the weak secrecy gain of the 2-modular lattice D_4 (or rather its inverse). Fig. 1 gives a plot of the secrecy function of D_4, where (i) we set $y = -i\tau$ and restrict to real positive values of y, since by (2) we are only interested in the values of $\Theta_{D_4}(\tau)$ with $\tau = yi,\ y > 0$ and (ii) y is plotted in decibels to transform the multiplicative symmetry point into an additive symmetry point. We can see clearly that the secrecy function has a symmetry point at $y \approx -1.5$ dB corresponding to $\tau = \frac{i}{\sqrt{2}}$. The value of the secrecy function $\Theta_{D_4}(\tau) = \frac{\vartheta_3^4(\sqrt{2}\tau)}{\Theta_{D_4}(\tau)}$ at $\tau = \frac{i}{\sqrt{2}}$, namely, the weak secrecy gain can be approximated by

$$\chi_{D_4} \approx 1.08356 \tag{12}$$

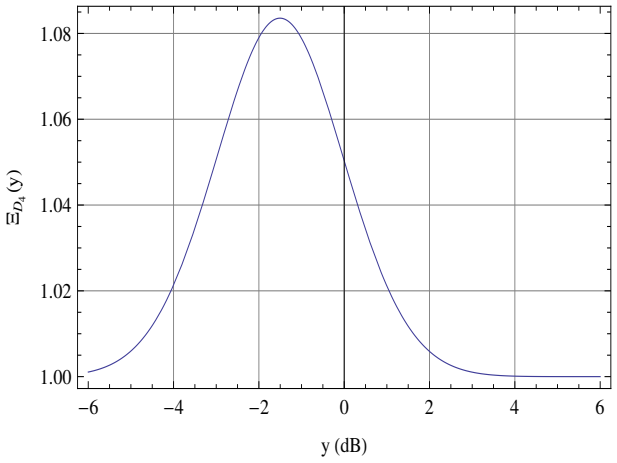

Fig. 1. Secrecy function of D_4

and hence

$$\alpha_2 = \frac{1}{\chi_{D_4}} \approx 0.922883. \tag{13}$$

Approximating $\beta_2 = \frac{\Delta_{16}(\tau)}{\vartheta_3^{16}(\sqrt{2}\tau)}|_{\tau=\frac{i}{\sqrt{2}}}$:

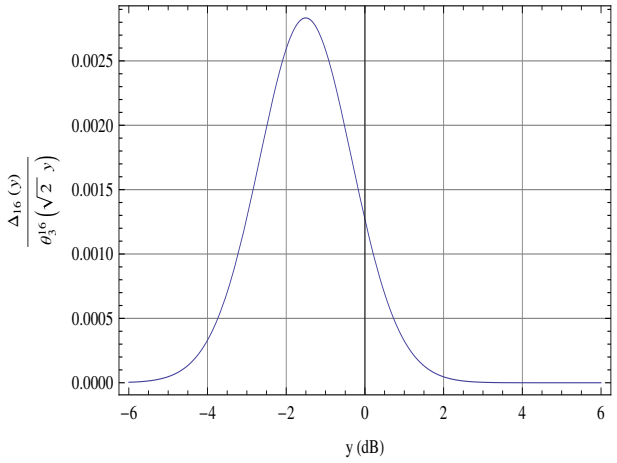

Fig. 2. Values of $\frac{\Delta_{16}(\tau)}{\vartheta_3^{16}(\sqrt{2}\tau)}$

Fig. 2 gives a plot of the ratio $\frac{\Delta_{16}(\tau)}{\vartheta_3^{16}(\sqrt{2}\tau)}$. The value of the ratio at $\tau = \frac{i}{\sqrt{2}}$ can be approximated by

$$\beta_2 \approx 0.00283366. \tag{14}$$

We start by explaining how the coefficients a_μ's in (9) are computed. By substituting (10) and (11) into (9), we have a formal sum with coefficients represented by the a_μ's. Then by comparing this formal sum with (3), we obtain a number of linear equations in the a_μ's. When we have enough equations, the a_μ's can be recovered by solving a linear system. Now, let us compute the weak secrecy gain of the 16-dimensional 2-modular Barnes-Wall lattice BW_{16} as an example.

Example 3.1: BW_{16} is an even lattice with minimum norm 4. The theta series of BW_{16} looks like

$$\Theta_{BW_{16}}(\tau) = 1 + 0q^2 + A_4q^4 + \cdots,\ A_4 \neq 0.$$

On the other hand, by (9), (10) and (11),

$$\begin{aligned}\Theta_{BW_{16}}(\tau) &= a_0\Theta_{D_4}^4(\tau) + a_1\Delta_{16}(\tau)\\ &= a_0(1+24q^2+\cdots)^4 + a_1(q^2+\cdots)\\ &= a_0(1+96q^2+\cdots) + a_1(q^2+\cdots)\\ &= a_0 + (96a_0+a_1)q^2+\cdots.\end{aligned}$$

We now have two linear equations in two unknowns a_0 and a_1

$$\begin{cases} a_0 &= 1\\ 96a_0+a_1 &= 0\end{cases}$$

which gives $a_0 = 1$ and $a_1 = -96$, yielding the weak secrecy gain

$$\chi_{BW_{16}} = \frac{1}{\alpha_2^4 - 96\beta_2} \approx 2.20564. \tag{15}$$

See Figure 3 for a plot of the secrecy function of BW_{16} for verification.

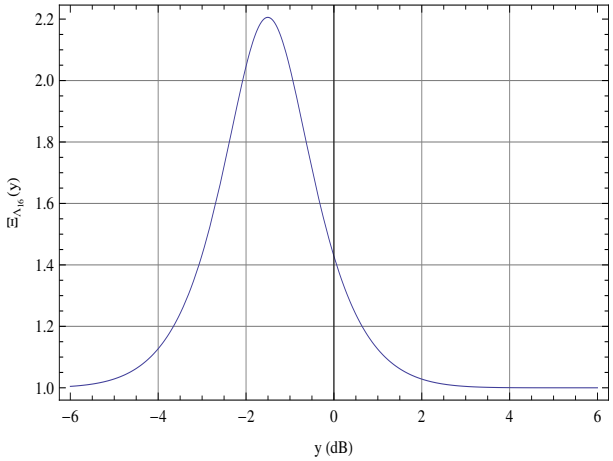

Fig. 3. Secrecy function of BW_{16}

In this way, we have computed the weak secrecy gains of the even 2-modular lattices we found in [16] in dimensions smaller than 24 as shown in Table I.

B. 3-modular lattices

According to Lemma 2.5, the theta series of an even 3-modular lattice Λ of dimension $n = 2k$ can be written as

$$\Theta_\Lambda(\tau) = \sum_{\lambda+6\mu=k} a_\mu \Theta_{A_2}^\lambda(\tau)\Delta_{12}^\mu(\tau), \tag{16}$$

where

$$\begin{aligned}\Theta_{A_2}(\tau) &= \vartheta_2(2\tau)\vartheta_2(6\tau) + \vartheta_3(2\tau)\vartheta_3(6\tau)\\ &= 1 + 6q^2 + 0q^4 + 6q^6 + \cdots\end{aligned} \tag{17}$$

and

$$\Delta_{12}(\tau) = \left(\eta(\tau)\eta(3\tau)\right)^6.$$

We can also compute the first few terms of $\Delta_{12}(\tau)$:

$$\Delta_{12}(\tau) = q^2 - 6q^4 + 9q^6 + \cdots. \tag{18}$$

The secrecy function of an even 3-modular lattice Λ of dimension n is

$$\begin{aligned}1/\Xi_\Lambda(\tau) &= \textstyle\sum_{\lambda+6\mu=k} \frac{a_\mu \Theta_{A_2}^\lambda(\tau)\Delta_{12}^\mu(\tau)}{\vartheta_3^n(\sqrt{3}\tau)}.\\ &= \textstyle\sum_{\lambda+6\mu=k} a_\mu \left(\frac{\Theta_{A_2}(\tau)}{\vartheta_3^2(\sqrt{3}\tau)}\right)^\lambda \left(\frac{\Delta_{12}(\tau)}{\vartheta_3^{12}(\sqrt{3}\tau)}\right)^\mu.\end{aligned}$$

We can similarly approximate the two quotients

$$\begin{cases} \alpha_3 &= \frac{\Theta_{A_2}(\tau)}{\vartheta_3^2(\sqrt{3}\tau)}|_{\tau=\frac{i}{\sqrt{3}}} &\approx 0.982424\\ \beta_3 &= \frac{\Delta_{12}(\tau)}{\vartheta_3^{12}(\sqrt{3}\tau)}|_{\tau=\frac{i}{\sqrt{3}}} &\approx 0.00832474\end{cases}$$

where we recognize in the first term the inverse of the weak secrecy gain of the 3-modular lattice A_2. Fig. 4 gives a plot of the secrecy function of A_2 and the weak secrecy gain is approximated by

$$\chi_{A_2} \approx 1.01789. \tag{19}$$

The second term β_3 is approximated numerically as we did for β_2 and is omitted.

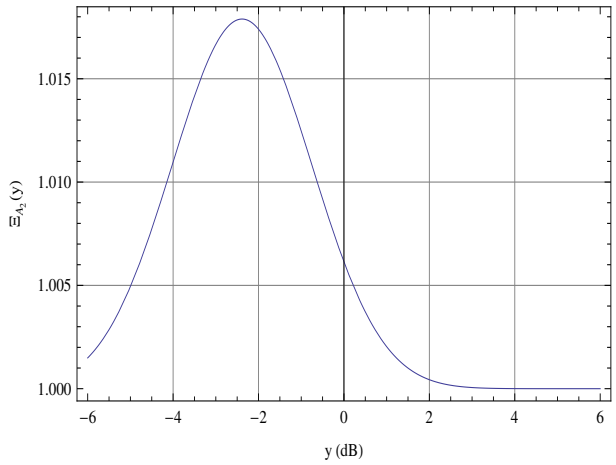

Fig. 4. Secrecy function of A_2

Now let us compute the weak secrecy gain of the Coxeter-Todd Lattice K_{12} as an example.

Example 3.2: The Coxeter-Todd Lattice K_{12} is an even lattice with minimum norm 4. The theta series of K_{12} looks like

$$\Theta_{K_{12}}(\tau) = 1 + 0q^2 + A_4q^4 + \cdots,\ A_4 \neq 0.$$

On the other hand, by (16), (17) and (18),

$$\begin{aligned}\Theta_{K_{12}}(\tau) &= a_0\Theta_{A_2}^6(\tau) + a_1\Delta_{12}(\tau)\\ &= a_0(1+6q^2+\cdots)^6 + a_1(q^2+\cdots)\\ &= a_0(1+36q^2+\cdots) + a_1(q^2+\cdots)\\ &= a_0 + (36a_0+a_1)q^2+\cdots.\end{aligned}$$

We now have two linear equations in two unknowns a_0 and a_1

$$\begin{cases} a_0 &= 1\\ 36a_0+a_1 &= 0\end{cases}$$

which gives $a_0 = 1$ and $a_1 = -36$, yielding the weak secrecy gain

$$\chi_{K_{12}} = \frac{1}{\alpha_3^6 - 36\beta_3} \approx 1.66839. \tag{20}$$

TABLE I
WEAK SECRECY GAINS OF 2- AND 3-MODULAR LATTICES

dim	lattice	ℓ	theta series	χ_Λ
2	A_2	3	Θ_{A_2}	1.01789
4	D_4	2	Θ_{D_4}	1.08356
12	K_{12}	3	$\Theta_{A_2}^6 - 36\Delta_{12}$	1.66839
14	$C_2 \times G(2,3)$	3	$\Theta_{A_2}^7 - 42\Theta_{A_2}\Delta_{12}$	1.85262
16	BW_{16}	2	$\Theta_{D_4}^4 - 96\Delta_{16}$	2.20564
20	HS_{20}	2	$\Theta_{D_4}^5 - 120\Theta_{D_4}\Delta_{16}$	3.03551
22	$A_2 \times A_{11}$	3	$\Theta_{A_2}^{11} - 66\Theta_{A_2}^5\Delta_{12}$	3.12527

See Fig. 5 for a plot of the secrecy function of K_{12} for verification.

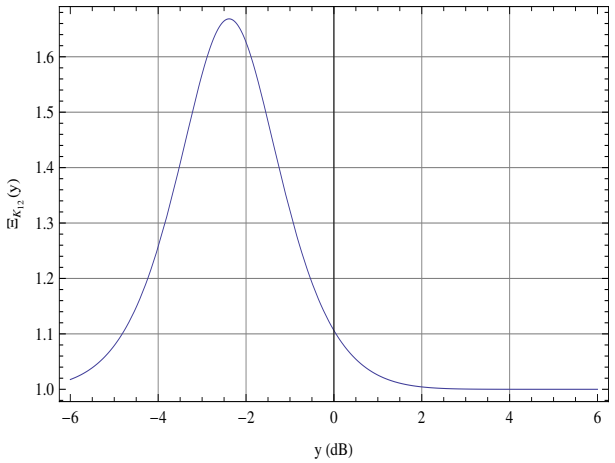

Fig. 5. Secrecy function of K_{12}

Weak secrecy gains of the even 3-modular lattices in dimensions smaller than 24 in [16] are also shown in Table I.

C. 2- and 3-modular lattices v.s. unimodular lattices

Now that we have computed the weak secrecy gains of several 2- and 3-modular lattices, we want to compare them with the best unimodular lattices in their respective dimensions. Table II lists the secrecy gains of the best unimodular lattices and the weak secrecy gains of the even 2- and 3-modular lattices we have computed. We can see that all 2- and 3-modular lattices outperform the unimodular lattices except for the 22-dimensional 3-modular lattice $A_2 \times A_{11}$.

IV. CONCLUSION AND FUTURE WORKS

In this paper, we investigate the secrecy gain of even 2- and 3-modular lattices. A formula similar to that for even unimodular lattices [8], [9] is derived and weak secrecy gains of even 2- and 3-modular lattices in dimensions smaller than 24 are computed. They are found to be larger than that of the best unimodular lattices, classified in [11], with an exception of that of the lattice $A_2 \times A_{11}$. One direction of future work will be naturally to look at the performance of ℓ-modular lattices, $\ell > 3$. Another direction would be to study the asymptotic behavior of the weak secrecy gain of the even 2- and 3-modular lattices. Besides, it is likely that one can prove the conjecture for these particular cases using the same proof technique as in [11], however it would be nice to have a more general proof. Also, the encoding/labeling of the proposed wiretap codes, taking into account both channel parameters and power constraint are being naturally elaborated.

TABLE II
2- AND 3-MODULAR LATTICES V.S. UNIMODULAR LATTICES

dim	lattice	ℓ	χ_Λ
2	$\mathbb{Z}^2$	1	1
2	A_2	3	≥ 1.01789
4	$\mathbb{Z}^4$	1	1
4	D_4	2	≥ 1.08356
12	D_{12}^+	1	1.6
12	K_{12}	3	≥ 1.66839
14	$(E_7^2)^+$	1	1.77778
14	$C_2 \times G(2,3)$	3	≥ 1.85262
16	$(D_8^2)+$	1	2
16	BW_{16}	2	≥ 2.20564
20	$(A_5^4)^+$	1	2.66667
20	HS_{20}	2	≥ 3.03551
22	$(A_1^{22})^+$	1	3.2
22	$A_2 \times A_{11}$	3	≥ 3.12527

ACKNOWLEDGMENT

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

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. 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 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] F. Lin and F. Oggier, "Secrecy gain of Gaussian wiretap codes from unimodular lattices," ITW 2011, Paraty. pp. 718-722.

[11] F. Lin and F. Oggier, "Unimodular Lattice Codes for Gaussian Wiretap Channel", http://arXiv:1201.3688v1 [cs.IT], 18 Jan 2012.

[12] H.-G. Quebbemann, Modular Lattices in Euclidean Spaces, Journal of Number Theory 54 (1995), 190-202.

[13] T.M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, 1976.

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

[15] A.-M. Ernvall-Hytönen and C. Hollanti, "On the Eavesdroppers Correct Decision in Gaussian and Fading Wiretap Channels Using Lattice Codes," ITW 2011, Paraty. pp. 210-214.

[16] http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/