British Journal of Mathematics & Computer Science
18(3): 1-10, 2016, Article no.BJMCS.28543
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

A New Secrecy Function for Modular Lattices

Y. Diop[1*], Cheikh Thiécoumba Gueye[1] and Patrick Solé[2]

[1] *Department of Mathematics, Laboratoire d'Algebre de Cryptographie de Geometrie Algebrique et Applications (LACGAA), UCAD, Dakar, Senegal.*
[2] *CNRS, LTCI, Telecom Paris Tech, Paris, France.*

Authors' contributions

This work was carried out in collaboration between all authors throughout a very fruitful exchange of ideas and comments. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/28543
Editor(s):
(1) Morteza Seddighin, Indiana University East Richmond, USA.
Reviewers:
(1) Sanjib Kumar Datta, University of Kalyani, West Bengal, India.
(2) Vipin Saxena, Bababsaheb Bhimrao Ambedkar University, Lucknow, India.
Complete Peer review History: http://www.sciencedomain.org/review-history/15982

Received: 25th July 2016
Accepted: 23rd August 2016
Published: 30th August 2016

Short Research Article

Abstract

A recent line of work to improve the secrecy capacity within wiretap gaussian channel has introduced a new lattice invariant called secrecy gain. Belfiore and Solé made a conjecture about the point at which the the secrecy gain is maximum. Verified by most unimodular lattices, this conjecture does not hold in general for l-modular lattices ($l \geq 2$). Ernvall-Hytönen modified the secrecy function and proved that it satisfies the conjecture for 2-odd modular lattices. In this paper, the authors introduce a new secrecy function for 2-modular lattices. They show that, by using the lattice D_4 instead of $D^l = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$, the conjecture holds for both 2-even and odd modular lattices in dimension $n \geq 4$. Using that result, they further prove that the modified secrecy function of A.-M. Ernvall-Hytönen holds for both 2-even and odd modular lattices.

Keywords: Gaussian wiretap channel; lattice codes; secrecy gain; modular lattices; theta series.

2010 AMS Mathematics Subject Classification: 94B60.

**Corresponding author: E-mail: yakhyadiop2000@yahoo.fr;*

1 Introduction

In his seminal work, Wyner introduced the wiretap channel, a discrete memoryless channel where the sender Alice transmits confidential messages to a legitimate receiver Bob, in the presence of an eavesdropper Eve [1].Wyner defined the perfect secrecy capacity as the maximum amount of information that Alice can send to Bob while insuring that Eve gets a negligible amount of information. He used a coset coding technique known as wiretap II codes to encode both data and random bits to confuse the eavesdropper. The secrecy capacity of Gaussian wiretap channel was established in [2] and J. C. Belfiore and F. Oggier studied in [3] lattice codes, using as design criterion a new lattice invariant called secrecy gain. In [4], Belfiore and Solé introduced the secrecy function as a measure of efficiency of a gaussian wiretap channel. Let Λ be an $n-$dimensional lattice of volume v^n. The secrecy function is given by

$$\Xi_{\Lambda}(\tau) = \frac{\Theta_{v\mathbb{Z}^n}\ (\tau)}{\Theta_{\Lambda}(\tau)} \qquad \tau = yi,\ y > 0 \tag{1.1}$$

The secrecy gain is then the maximal value of the secrecy function with respect to τ and is denoted χ_{Λ} . A scaled version of the cubic lattice $v\mathbb{Z}^n$ is used because the optimization must be performed between lattices of the same volume.

Belfiore and Solé proved in [5], that the secrecy function of a lattice equivalent to its dual has a multiplicative symmetry at the point $y_0 = vol(\Lambda)^{-\frac{2}{n}}$ (If Λ isodual, then $y_0 = 1$). They conjecture that the maximum of the secrecy function is met at that point y_0. The conjecture holds for almost all known unimodular lattices (see [6], [7], [8] and [9])but fails to be verified by other modular lattices in general[10]. A.-M. Ernvall-Hytönen modified the secrecy function, using the lattice $D^l = \mathbb{Z}\oplus\sqrt{l\mathbb{Z}}$ instead of $\mathbb{Z}$ and proved that it satisfies the conjecture for 2-odd modular lattices [10].

In this paper is introduced a new secrecy function for 2-modular lattices. It is shown that, by using the lattice D_4 instead of $D^l = \mathbb{Z}\oplus\sqrt{l\mathbb{Z}}$ the conjecture holds for both 2-even and odd modular lattices in dimension $n \geq 4$. Using that result, it is proved further that the conjecture for the modified secrecy function of A.-M. Ernvall-Hytönen holds for both 2-even and odd modular lattices.

The paper is organized as follows. In section II we recall some basic definitions about lattice theory and review some previous results regard the secrecy function. In Section III, we prove that the 2-even modular lattice D_4 satisfies the new secrecy function defined by A.-M. Ernvall-Hytönen. Section IV expose the new secrecy function for 2-modular lattices. In section V and VI, we prove respectively that the conjecture holds for both 2-even and odd-modular lattices. Using those previous results, the final section gives a proof of the conjecture for the secrecy function redefined by A.-M. Ernvall-Hytönen, for either odd and even-modular lattices.

2 Primary Works and Previous Results

Definition 2.1. A lattice Λ is an additive subgroup of $\mathbb{R}^n$, which can be described by

$$\Lambda = \{x = uM/u \in \mathbb{Z}^m\} \tag{2.1}$$

where

$$\begin{pmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,n} \\ v_{2,1} & v_{2,2} & \dots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m,1} & v_{m,2} & \dots & v_{m,n} \end{pmatrix}$$

$v_i = (v_{i,1}, ..., v_{i,n})$, $i = 1, 2, ..., m$ form a basis of the lattice Λ.

The matrix $G = MM^T$, where M^T denotes the transpose of M is called the Gram matrix of the lattice.

Definition 2.2. The determinant $det(\Lambda)$ of a lattice Λ is the determinant of the matrix G.

Definition 2.3. For any lattice point P_i of the lattice Λ , its voronoi cell is defined by:

$\mathcal{V}_\Lambda(P_i) = \{x \in \mathbb{R}^n,\, d(P_i, x) \leqslant (P_j, x) \text{ for all } P_j \in \Lambda\}$.

All voronoi cells are the same, therefore, the volume of a lattice is defined as the volume of a voronoi cell. The volume of the lattice Λ $vol(\Lambda)$ is equal to $\sqrt{det(\Lambda)}$.

Definition 2.4. The dual of of a lattice is defined by

$$\Lambda^* = \{x \in \mathbb{R}^n : x.\lambda \in \mathbb{Z}, \forall\ \lambda \in \Lambda\}. \tag{2.2}$$

Definition 2.5. A lattice Λ is called integral lattice if $\Lambda \subset \Lambda^*$.

Definition 2.6. An integral lattice is called an even lattice if the norm is even for any lattice point. Otherwise, it is called an odd lattice.

Definition 2.7. An integral lattice that is equivalent to its dual is called a modular lattice.
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. The determinant of an l-modular lattice Λ of dimension n is given by $det(\Lambda) = l^{\frac{n}{2}}$

Definition 2.8. The theta series of a lattice Λ is defined by

$$\Theta_\Lambda(\tau) = \sum_{\lambda \in \Lambda} q^{\|\lambda\|^2} \tag{2.3}$$

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

$\mathcal{H}$ =$\{$a+ib$\in \mathbb{C}$, b¿0$\}$ denotes the upper half plane.

The theta series of an integral lattice has a neat representation since all the norms are integers.

Let us consider the class of lattices Λ such that Λ is equivalent to its dual. More precisely, the dual lattice Λ^* can be obtained from the lattice Λ by a rotation, a reflection, or a rescaling.

If $\alpha > 0$, then $\Lambda \simeq \alpha\Lambda^*$.
If $\alpha = 1$, then Λ is isodual.
$vol(\Lambda) = \alpha^n vol(\Lambda^*)$.
But since Λ and Λ^* are dual, then $vol(\Lambda) = \frac{1}{vol(\Lambda^*)}$
We get $\alpha = vol(\Lambda)^{\frac{2}{n}}$.

Belfiore and Solé proved in [2], that the secrecy function of a lattice equivalent to its dual has a multiplicative symmetry at the point $y_0 = vol(\Lambda)^{-\frac{2}{n}}$ (If Λ isodual, then $y_0 = 1$). For a lattice equivalent to its dual, they conjecture that the secrecy function attains its maximum at $y_0 = vol(\Lambda)^{\frac{-2}{n}}$. This has been verified for a large number of lattices (see [6], [7], [8] and [9]).

A.- M. Ernvall-Hytönen showed in [10] that the conjecture is not verified in general for ℓ-modular lattices. She modified the conjecture by using the lattice $D^l = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$ instead of $v\mathbb{Z}^n$. She proved then that the modified secrecy function conjecture holds for odd 2-modular lattices.

In this paper we introduce a new secrecy function for 2-modular lattices. We show that by using the lattice D_4 instead of $D^l = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$ the conjecture holds for both 2-even and odd modular lattices in dimension $n \geq 4$. Using that result, we further prove that the modified secrecy function of A.-M. Ernvall-Hytönen holds for both 2-even and odd modular lattices.

3 The 2-modular Lattices D_4

Definition 3.1. Jacobi theta functions are defined as follows:

$$\vartheta_2(\tau) = \sum_{n\in\mathbb{Z}} q^{(n+\frac{1}{2})^2} \tag{3.1}$$

$$\vartheta_3(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2} \tag{3.2}$$

$$\vartheta_4(\tau) = \sum_{n\in\mathbb{Z}} (-q)^{n^2} \tag{3.3}$$

with $q = e^{\pi i \tau}$.

When working with the variable y instead of q, we will write $\vartheta(y)$ for $\vartheta_3(q)$.

Exceptional lattices have theta series that can be expressed as functions of the Jacobi theta functions.

Let Λ be an n-dimensional 2-modular lattice. The secrecy function is defined by A.-M. Ernvall-Hytönen as follows

$$\Xi_{l,\Lambda}(y) = \frac{\{\Theta_D^{(l)}(y)\}^k}{\Theta_\Lambda(y)}, \tag{3.4}$$

with $n = 2k$ for $l > 1$.

Let us study now the new modified secrecy function $\Xi_{2,D_4}(y)$.
$\Xi_{2,D_4}(y) = \frac{\Theta_{D^{(2)}(y)^2}}{\Theta_{D_4}(y)} = \frac{\Theta_{\mathbb{Z}\oplus\sqrt{2}\mathbb{Z}}(y)^2}{\Theta_{D_4}(y)}$

$\Theta_{\mathbb{Z}\oplus\sqrt{2}\mathbb{Z}}(y) = \vartheta_3(y)\vartheta_3(2y)$

$\vartheta_3^2(2y) = \frac{1}{2}[\vartheta_3^2(y) + \vartheta_4^2(y)]$

$\Xi_{2,D_4}(y) = \frac{\Theta_{D^{(2)}(y)^2}}{\Theta_{D_4}(y)} = \frac{\frac{1}{4}\vartheta_3^2(y)[\vartheta_3^2(y)+\vartheta_4^2(y)]}{[\vartheta_3^4(y)+\vartheta_4^4(y)]} = \frac{1}{4}(\frac{1+\alpha}{1+\alpha^2})$

where $\alpha = \frac{\vartheta_4^2(y)}{\vartheta_3^2(y)}$

Let

$$f_2(y) = \frac{\frac{1}{4}\vartheta_3^2(y)[\vartheta_3^2(y) + \vartheta_4^2(y)]}{[\vartheta_3^4(y) + \vartheta_4^4(y)]} \tag{3.5}$$

Lemma 3.1. *([10]) The function $\frac{\vartheta_4}{\vartheta_3}(y)$ is strictly increasing for (positive) real y, and as $y \to 0$, the function approaches 0, and as $y \to \infty$, the function approaches 1.*

Lemma 3.2. *The function $f(x) = \frac{1+x}{(1+x^2)}$ has a unique maximum in the open interval (0,1), and this maximum is met at the point $x = \sqrt{2} - 1$.*

Proof. $f'(x) = \frac{-x^2-2x+1}{(1+x^2)^2}$.

The quadratic $-x^2 - 2x + 1 = 0$ if and only if $x = -1 \pm \sqrt{2}$.

The root $-1 + \sqrt{2}$ lies on the interval $0 \le x \le 1$.

Furthermore, when $0 \leq x \leq \sqrt{2}-1$, the function $f(x)$ is increasing since $f'(x) > 0$, and when $\sqrt{2}-1 < x < 1$ the function is decreasing. Hence, this point is a maximum. □

Lemma 3.3. *[10] The quantity* $\frac{\vartheta_4^2}{\vartheta_3^2}(y)$ *take the value* $\sqrt{2}-1$ *precisely when* $y = \frac{1}{\sqrt{2}}$.

It follows from lemma III.2, III.3 and III.4 that the secrecy function as redefined in **[10]** will have a global maximum at $y = \frac{1}{\sqrt{2}}$. Therefore the even lattice D_4 satisfies the modified secrecy function conjecture.

4 Secrecy Function of 2-modular Lattices Redefined

Definition 4.1. Let Λ be an n-dimensional 2-modular lattice, $n \geq 4$. The secrecy function is defined by

$$\Xi_{D_4,\Lambda}(\tau) = \frac{\Theta_{D_4}^{\frac{n}{4}}(\tau)}{\Theta_\Lambda(\tau)} \tag{4.1}$$

Remark 4.1. Instead of using of scaled version of $\mathbb{Z}^n$ or $D^{(l)}$, we have used a scaled version of D_4.

Recall that if Λ be an n-dimensional 2-modular lattice, $vol(\Lambda) = 2^{\frac{n}{4}}$.

The volume of the lattice D_4 is $vol(D_4) = 2$.

Remark 4.2. Clearly without $n \geq 4$, the lattice $D^{(2)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$ will violate the conjecture.

Proposition 4.1. *The secrecy function of a lattice equivalent to its dual has a multiplicative symmetry at* $y_0 = \frac{1}{\sqrt{2}}$.

Proof

$$\Xi_{D_4,\Lambda}(yy_0) = \frac{\Theta_{D_4^{\frac{n}{4}}}}{\Theta_\Lambda}(yy_0)$$

By dividing the numerator and the denominator with $\Theta_{\alpha\mathbb{Z}^n}$ where $\alpha = 2^{\frac{1}{4}}$, we get

$$\Xi_{D_4,\Lambda}(yy_0) = \frac{\Xi_{D_4^{\frac{n}{4}}}}{\Xi_\Lambda}(yy_0) = \frac{\Xi_{D_4^{\frac{n}{4}}}}{\Xi_\Lambda}(\frac{y}{y_0}) = \frac{\Theta_{D_4^{\frac{n}{4}}}}{\Theta_\Lambda}(\frac{y}{y_0}) = \Xi_{D_4,\Lambda}(\frac{y}{y_0})$$

Since $y_0 = (vol(\Lambda))^{\frac{-2}{n}}$, $vol(\Lambda) = 2^{\frac{n}{4}}$, we have $y_0 = (2^{\frac{n}{4}})^{\frac{-2}{n}} = 2^{-\frac{1}{2}}$

5 Secrecy Function for 2-even Modular Lattices

Lemma 5.1. *Let* Λ *be an even 2-modular lattice of dimension* $n = 2k$, $n \geq 4$, *then*

$$\Theta_\Lambda(\tau) = \sum_{2\lambda+8\mu=k} a_\mu \Theta_{D_4}^\lambda(\tau)\Delta_{16}^\mu(\tau) \tag{5.1}$$

where $\Theta_{D_4}(\tau) = \frac{1}{2}(v_3^4(\tau) + v_4^4(\tau))$
$\Delta_{16}(\tau) = (\eta(\tau)\eta(2\tau))^8$

$\eta(\tau)$ is the Dedekind eta function and is defined by

$$\eta(\tau) = q^{\frac{1}{12}} \prod_{n=1}^{\infty}(1-q^{2n}). \tag{5.2}$$

The Jacobi theta function and the Dedekind eta function are connected as follows:

$$\vartheta_2(\tau) = \frac{2\eta(2\tau)^2}{\eta(\tau)} \tag{5.3}$$

$$\vartheta_3(\tau) = \frac{\eta(\tau)^5}{\eta(\frac{\tau}{2})^2\eta(2\tau)^2} \tag{5.4}$$

$$\vartheta_4(\tau) = \frac{\eta(\frac{\tau}{2})^2}{\eta(\tau)} \tag{5.5}$$

We can write Δ_{16}

$$\Delta_{16}(\tau) = (\eta(\tau)\eta(2\tau))^8 = \frac{1}{256}v_2^8(\tau)v_3^4(\tau)v_4^4(\tau) \tag{5.6}$$

Proposition 5.1. *Let Λ be an even n-dimensional 2-modular lattice*
$\Xi_{D_4,\Lambda}(\tau) = [\sum_{\lambda+4\mu=\frac{n}{4}} a_\mu(\frac{\Delta_{16}(\tau)}{\Theta_{D_4}^4(\tau)})^\mu \ ]^{-1} = [\sum_{\lambda+4\mu=\frac{n}{4}} a_\mu(\frac{v_2(\tau)^2 \ v_3(\tau) \ v_4(\tau)}{v_3(\tau)^4+v_4(\tau)^4})^{4\mu} \ ]^{-1}$

Proof

From lemma V.1 we get: $\Xi_{D_4,\Lambda}(\tau) = [\sum_{\lambda+4\mu=\frac{n}{4}} a_\mu \frac{(\Delta_{16}(\tau))^\mu}{\Theta_{D_4}(\tau)(\frac{n}{4}-\lambda)} \ ]^{-1}$

but $\frac{n}{4} - \lambda = 4\mu$

Theorem 5.2. *The secrecy function of an even 2-modular lattices in dimension $n = 2k$ is:*

$$\Xi_{D_4,\Lambda}(y) = [\sum_{2\lambda+8\mu=k} a_\mu f_2^\mu]^{-1}, \tag{5.7}$$

where $f_2(y) = [\frac{\vartheta_2(y)^2\vartheta_3(y)\vartheta_4(y)}{\vartheta_3(y)^4+\vartheta_4(y)^4}]^4$.

Proof from the proposition V.2 we have: $\Xi_{D_4,\Lambda}(\tau) = [\sum_{\lambda+4\mu=\frac{n}{4}} a_\mu(\frac{v_2(\tau)^2 \ v_3(\tau) \ v_4(\tau)}{v_3(\tau)^4+v_4(\tau)^4})^{4\mu} \ ]^{-1}$

We have $f_2(y) = \frac{(\vartheta_3(y)^4-\vartheta_4(y)^4)^2\vartheta_3(y)^4\vartheta_4(y)^4}{(\vartheta_3(y)^4+\vartheta_4(y)^4)^4} = \frac{(1-\alpha^2)^2\alpha^2}{(1+\alpha^2)^4}$

where $\alpha = \alpha(y) = \frac{\vartheta_4(y)^2}{\vartheta_3(y)^2}$

Lemma 5.3. *The function $f(x) = \frac{x^2(1-x^2)^2}{(1+x^2)^4}$ has a unique maximum in the open interval (0,1), and this maximum is met at the point $x = \sqrt{2}-1$.*

Proof

$f(x) = g(x)^2$ where $g(x) = \frac{x(1-x^2)}{(1+x^2)^2}$.
$g'(x) = \frac{x^4-6x^2+1}{(1+x^2)^3}$.
$x^4 - 6x^2 + 1 = 0$ if and only if $x^2 = 3 \pm \sqrt{2}$.

The root $3-\sqrt{2}$ lies on the interval $0 \le x^2 \le 1$ and $(\sqrt{2}-1)^2 = 3-2\sqrt{2}$. Which means that

$x = \sqrt{2} - 1$.

Furthermore, when $0 \leq x \leq \sqrt{2} - 1$, the function $g(x)$ is increasing since $g'(x) > 0$, and when $\sqrt{2} - 1 < x < 1$ the function is decreasing. Hence, this point is a maximum.

Proposition 5.2. *[10] A sufficient condition for $\Xi_{D_4,\Lambda}(y)$ to have a global maximum at $y = \frac{1}{\sqrt{2}}$ is that the polynomial in the variable f_2 whose inverse appear in theorem V.3 be decreasing in the range of $0 < f_2 \leq \beta$, where $\beta = f_2(\sqrt{2} - 1) \approx 0.0429$.*

Let us now consider the even 2-modular lattices in [11] Table 1. The authors have computed their theta series in terms of Θ_{D_4} and Δ_{16}.

The maximum of the secrecy function of both lattices is expected to be met at $y = \frac{1}{\sqrt{2}}$ to satisfy the conjecture. It seems to be the case in Fig. 1 and Fig. 2.

Table. 1. Verification of the conjecture for most known even 2-modular lattices

Dim	lattice	Theta series	$[\Xi_{D_4,\Lambda}(f_2)]^{-1}$	$d/df_2[\Xi_{D_4,\Lambda}(f_2)]^{-1}$	Neg. in $(0, \beta]$?
16	BW_{16}	$\Theta_{D_4}^4 - 96\Delta_{16}$	$1 - 96f_2$	-96	yes
20	HS_{20}	$\Theta_{D_4}^5 - 120\Theta_{D_4}\Delta_{16}$	$1 - 120f_2$	-120	yes
32	Q_{32}	$\Theta_{D_4}^8 - 192\Theta_{D_4}^4\Delta_{16} + 576\Delta_{16}^2$	$1 - 192f_2 + 576{f_2}^2$	$-192 + 1152f_2$	yes

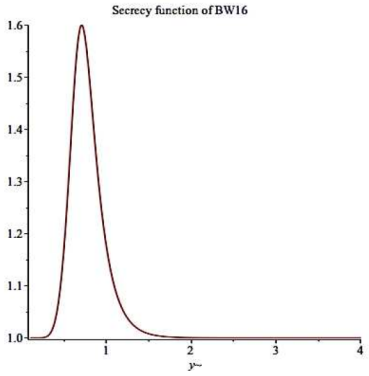

Fig. 1. Secrecy function of the 16-dimensional Barns-Wall lattice BW16

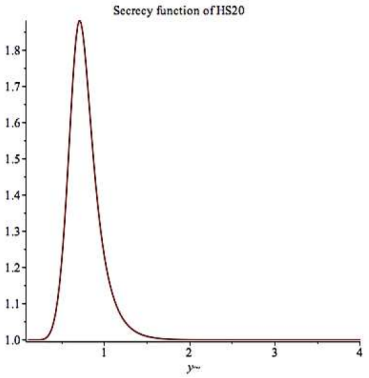

Fig. 2. Secrecy function of the lattice HS20

6 Secrecy Function for 2-odd Modular Lattices

Lemma 6.1. *[10] . The theta series of an function 2-odd modular lattice Λ in dimension $n = 2k$ is a polynomial*

$$\Theta_\Lambda(\tau) = [f_1(y)^k][\sum_{i=0}^{[k/2]} a_i f_2(y)^i], \tag{6.1}$$

where $f_1(y) = \Theta_{\mathbb{Z}\oplus\sqrt{2}\mathbb{Z}}(y) = \vartheta_3(y)\vartheta_3(2y)$ *and* $f_2(y) = \frac{\frac{1}{4}\vartheta_2^2(2y)[\vartheta_4^2(y)]}{[\vartheta_3^2(y)\vartheta_3^2(2y)]}$

Theorem 6.2. *The secrecy function of a 2-odd modular lattices in dimension $n = 2k$ is:*

$$\Xi_{D_4,\Lambda}(y) = [f_0(y)]^{\frac{k}{2}}[\sum_{i=0}^{[k/2]} a_i f_2^i(y)]^{-1} \tag{6.2}$$

where $f_0(y) = \frac{\Theta_{D^{(2)}(y)^2}}{\Theta_{D_4}(y)}$.

Proof. We have

$$\Xi_{D_4,\Lambda}(y) = \frac{\Theta_{D_4}^{\frac{k}{2}}(y)}{\Theta_\Lambda(y)} = [\frac{[f_1(y)^k][\sum_{i=0}^{[k/2]} a_i f_2(y)^i]}{\Theta_{D_4}^{\frac{k}{2}}(y)}]^{-1} =$$

$$(\frac{\Theta^2_{\mathbb{Z}\oplus\sqrt{2}\mathbb{Z}}}{\Theta_{D_4}})^{\frac{k}{2}}(\sum_{i=0}^{[k/2]} a_i f_2(y)^i)^{-1}$$ □

Theorem 6.3. *The secrecy function of a 2-odd modular lattices in dimension $n = 2k$ has a unique maximum in the open interval (0,1), and this maximum is met at the point $y = \frac{1}{\sqrt{2}}$.*

Proof

We have $\Xi_{D_4,\Lambda}(y) = [f_0(y)]^{\frac{k}{2}}[\sum_{i=0}^{[k/2]} a_i f_2^i(y)]^{-1}$

$f_0(y) = \frac{\Theta_{D^{(2)}(y)^2}}{\Theta_{D_4}(y)} = \frac{\frac{1}{4}\vartheta_3^2(y)[\vartheta_3^2(y)+\vartheta_4^2(y)]}{[\vartheta_3^4(y)+\vartheta_4^4(y)]} = \frac{1}{4}(\frac{1+\alpha}{1+\alpha^2})$

where $\alpha = \frac{\vartheta_4^2(y)}{\vartheta_3^2(y)}$

The function f_0 has already been studied in section 2. It has a unique maximum in the open interval (0,1), and this maximum is met at the point $y = \frac{1}{\sqrt{2}}$. It has already been proven in [4] that has $[\sum_{i=0}^{[k/2]} a_i f_2^i(y)]^{-1}$ a unique maximum in the open interval (0,1), and this maximum is met at the point $y = \frac{1}{\sqrt{2}}$. Therefore the Belfiore-Sole conjecture is verified by the odd 2-modular lattices.

7 A.-M. Ernvall-Hytönen Secrecy Function for 2 Modular Lattices

Theorem 7.1. *The secrecy function of a 2-modular lattices in dimension $n = 2k$ as redefined by A.-M. Ernvall-Hytönen satisfies the Belfiore-Sole conjecture. Namely the secrecy function of 2-modular lattices attains its maximum at $y = \frac{1}{\sqrt{2}}$.*

Proof
Let Λ be an n-dimensional 2-modular lattice. The secrecy function is defined by A.-M. Ernvall-Hytönen as follows

$\Xi_{l,\Lambda}(y) = \frac{\Theta_D^{(l)}(y)^k}{\Theta_\Lambda(y)}$, n=2k for l¿1.
$\Xi_{2,\Lambda}(y) = \frac{\Theta_{D^{(2)}(y)^k}}{\Theta_\Lambda(y)}$

By dividing the numerator and the denominator with $\Theta_{D_4}^{\frac{n}{4}}$, we get:

$$\Xi_{2,\Lambda}(y) = \Xi_{2,D_4}(y)^k \Xi_{D_4,\Lambda}(y)$$

$\Xi_{2,D_4(y)}$ has already been studied; it has its maximum at $y = \frac{1}{\sqrt{2}}$. $\Xi_{D_4,\Lambda}(y)$ attains its maximum at $y = \frac{1}{\sqrt{2}}$ for both even and odd 2-modular lattices.

8 Conclusion and Future Works

The new secrecy function defined with a scaled version of D_4 has been inspired by the fact that the theta series of 2-modular lattices can be expressed easily with the one of D_4. More importantly, for theory application purpose, D_4 is of more interest than $D^{(2)}$. We have proved that this new secrecy function verifies the Belfiore-Sole conjecture for both 2-even and odd modular lattices. In addition we have used this new secrecy function to show that the modified Belfiore-Sole conjecture holds for both 2-odd and even modular lattices. Currently, we are trying to use the same approach to prove the modified conjecture for 3-modular lattices, using a scaled version of A_3.

Acknowledgement

This work is carry out with the activities of CEA-MITIC for CBC project for fruitful comments.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Wyner AD. The wire-tap channel. Bell. Syst. Tech. Journal. 1975;54.

[2] Leung-Yan-Cheong SK, Hellman ME. The Gaussian wire-tap channel. IEEE Trans. Inf. Theory. 1978;IT-24(4):451-456.

[3] Belfiore JC, Oggier F. Secrecy gain: A wiretap lattice code design. ISITA; 2010.
Available:http://arXiv:1004.4075v2 [cs.IT]

[4] Belfiore JC, Sol P. Unimodular lattices for the Gaussian wiretap channel. ITW 2010, Dublin.
Available:http://arXiv:1007.0449v1 [cs.IT]

[5] Oggier F, Sol P, Belfiore JC. Lattice codes for the wiretap Gaussian channel: Construction and analysis. Submitted, March; 2011

[6] Ernvall-Hytñen AM. On a conjecture by Belfiore and Sol on some lattices. IEEE Transactions on Information Theory. 58(9):5950-5955.
Available:http://arxiv.org/abs/1104.3739

[7] Fuchun Lin, Frdrique Oggier. A classification of unimodular lattice wiretap codes in small dimensions. IEEE Transactions on Information Theory. 2013;59(6):3295-3303.
Available:http://arxiv.org/pdf/1201.3688.pdf

[8] Julia Pinchak. Wiretap codes: Families of lattices satisfying the belfiore-sol secrecy function conjecture. Proceedings of ISIT. 2013;2617-2620.

[9] Julia Pinchak, Sethuraman BA. The Belfiore-sol conjecture and a certain technique for verifying it for a given lattice. Proceedings of ITA; 2014.
Available:http://www.csun.edu/asethura/papers/ITA 2014Mod.pdf

[10] Ernvall-Hytönen AM, Sethuraman BA. Conterexample to the generalized Belfiore-sol secrecy function conjecture for 1-modular lattices.

[11] Fuchun Lin, Frédérique Oggier, Patrick Sol. 2- and 3-modular lattice wiretap codes in small dimensions.
Available:http://arxiv.org/abs/1104.3739

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/15982