On The Secrecy Gain Of Extremal Even Γ -modular Lattices

Oggier, Frédérique; Belfiore, Jean-Claude

2018

Oggier, F., & Belfiore, J.-C. (2018). On The Secrecy Gain Of Extremal Even Γ -modular Lattices. Experimental Mathematics, in press.

<https://hdl.handle.net/10356/86844>

<https://doi.org/10.1080/10586458.2017.1423249>

© 2018 Taylor & Francis. This is the author created version of a work that has been peer reviewed and accepted for publication by Experimental Mathematics, Taylor & Francis. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<http://dx.doi.org/10.1080/10586458.2017.1423249>].

Downloaded on 26 Apr 2023 18:48:55 SGT

ON THE SECRECY GAIN OF EXTREMAL EVEN l -MODULAR LATTICES

FRÉDÉRIQUE OGGIER AND JEAN-CLAUDE BELFIORE

ABSTRACT. The secrecy gain is a lattice invariant that appears in the context of wiretap lattice coding. It has been studied for unimodular lattices, for 2-, 3- and 5-modular lattices. This paper studies the secrecy gain for extremal even l -modular lattices, for $l \in \{2, 3, 5, 6, 7, 11, 14, 15, 23\}$. We compute the highest secrecy gains as a function of the lattice dimension and the lattice level l . We show in particular that $l = 2, 3, 6, 7, 11$ are best for the respective ranges of dimensions $\{80, 76, 72\}$, $\{68, 64, 60, 56, 52, 48\}$, $\{44, 40, 36\}$, $\{34, 32, 30, 28, 26, 24, 22\}$, $\{18, 16, 14, 12, 10, 8\}$. This suggests that within a range of dimensions where different levels exist, the highest value of l tends to give the best secrecy gain. [A lower bound computation on the maximal secrecy gain](#) further shows that extremal lattices provide secrecy gains which are very close to this lower bound, thus confirming the good behavior of this class of lattices with respect to the secrecy gain.

1. INTRODUCTION

Let V be an n -dimensional Euclidean vector space, and $\sigma : V \rightarrow V$ a similarity of norm l , $l > 0$, i.e., σ is a map possibly including a rotation or reflection, such that $\sigma(v) \cdot \sigma(w) = lv \cdot w$, $v, w \in V$, for the usual inner product. For a lattice $\Lambda \subset V$, its dual lattice Λ^* is defined to be

$$\Lambda^* = \{v \in V, v \cdot w \in \mathbb{Z}, \text{ for all } w \in \Lambda\}.$$

A lattice $\Lambda \subset V$ is said to be integral if $\Lambda \subset \Lambda^*$, if the norm of any integral lattice point is even, then Λ is called even, and odd otherwise. We are only interested in even lattices. An integral lattice for which $\sigma(\Lambda^*) = \Lambda$ and $l = \frac{\sigma(\|v\|^2)}{\|v\|^2}$ for all $v \in \Lambda^*$ is called an l -modular lattice. We may use the term “of level l ”, and alternatively write $\Lambda^* \cong \frac{1}{\sqrt{l}}\Lambda$. Apart for l a square of an integer, a case we will not consider in this paper, modular lattices must have even dimension [Subsection 1.1][1], we will thus assume that n is even, say $n = 2k$ for k a positive integer, throughout the paper.

Let $k_l = 24/\sum_{d|l} d$ be integral. If l is prime, this means $k_l = 24/(1+l)$ is integral, or alternatively, $l \in \mathcal{L} = \{1, 2, 3, 5, 7, 11, 23\}$. If l is the product of some (not necessarily distinct) primes, then $l \in \{6, 14, 15\}$.

In what follows, z is taken to be in the upper half of the complex plane. Let $\eta(z) = q^{1/12} \prod_{m=1}^{\infty} (1 - q^{2m})$, $q = e^{\pi iz}$, be the Dedekind eta function, and set

$$(1) \quad \Delta_l(z) = \prod_{d|l} \eta(dz)^{k_l}$$

for $l \in \mathcal{L} \cup \{6, 14, 15\}$.

If $l \in \mathcal{L} = \{1, 2, 3, 5, 7, 11, 23\}$, then the theta series

$$\Theta(z) = \sum_{v \in \Lambda} q^{v \cdot v}$$

of an even modular lattice of level l and dimension $n = 2k$ can be written [1, Thm. 7] as a linear combination of all

$$(2) \quad \Theta_{2k_0}^\lambda \Delta_l^\mu, \quad \lambda, \mu \geq 0,$$

of weight k (as a modular form), where $\Theta_{2k_0}(z)$ denotes the theta series of an even modular lattice of level l and lowest positive dimension. The notation Θ_{2k_0} reflects that for an even l -modular lattice of dimension $2k_0$, its weight is k_0 [1, Thm. 1]. Since Δ_l has weight k_l , the constraint of weight k translates into saying that

$$(3) \quad k_0 \lambda + k_l \mu = k, \quad \lambda, \mu \geq 0.$$

If $l \in \{6, 14, 15\}$, the notion of strong modularity is needed to obtain an equivalent result for theta series [2]. Given an integral lattice Λ of level l , the partial dual $D_d \Lambda$ of Λ , for d an exact divisor of l , is [3, Definition 1.1]

$$(4) \quad D_d \Lambda = \sqrt{d} \left(\frac{1}{d} \Lambda \cap \Lambda^* \right)$$

and Λ an integral lattice is said to be strongly modular if $D_d \Lambda \cong \Lambda$ for all exact divisors d of l . Note that the weakest condition $D_l \Lambda \cong \Lambda$ is that of modularity of level l . Indeed [2, Proposition 1] $\sqrt{l}(D_d \Lambda)^* = D_{d'} \Lambda$ for $l = dd'$, thus

$$\Lambda \cong D_l \Lambda = \sqrt{l}(\Lambda \cap \Lambda^*)^* = \sqrt{l} \Lambda^*$$

as needed. In particular, if l is prime, the notion of strongly modular is the same as that of modular, since $D_1 \Lambda = \Lambda$. We will thus often speak of strongly modular lattices, instead of distinguishing modular for $l \in \mathcal{L}$ and strongly modular for $l \in \{6, 14, 15\}$.

For $l = 6, 14, 15$, the theta series of an even strongly modular lattice of level l and dimension $n = 2k$ can be written [2, Proposition 3] as a linear combination of

$$(5) \quad \Theta_4^\lambda \Delta_l^\mu, \quad \lambda, \mu \geq 0,$$

where $2\lambda + 2k_l \mu = k$ since Δ_l here has weight $2k_l$. The term Θ_4 is the theta series of some 4-dimensional strongly modular even lattice of level $l = 6, 14, 15$.

The minimum, or minimum norm

$$\min(\Lambda) = \min\{\|x\|^2, \quad x \in \Lambda, \quad x \neq 0\}$$

of an even strongly l -modular lattice, $l \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$ satisfies

$$(6) \quad \min(\Lambda) \leq 2 + 2 \left\lfloor \frac{n \sum_{d|l} d}{24 \sum_{d|l} 1} \right\rfloor$$

and lattices meeting the bound are called *extremal*. The minimum corresponds to the first non-constant coefficient of the theta series, which is called the kissing number of the lattice. This bound was proven in [1] for even lattices and l prime, and in [4, Theorem 2] more generally for strongly l -modular lattices which are rationally equivalent to the direct sum of $n/\dim C^{(l)}$ copies of $C^{(l)} = \sum_{d|l} \sqrt{d} \mathbb{Z}$, where it was further shown that there is for l odd one exceptional dimension $(\sum_{d|l} 1) \left(\frac{24}{\sum_{d|l} d} - 1 \right)$ for which the bound on the minimum is 3 instead of 2.

The purpose of this paper is to study the secrecy gain of even extremal l -modular lattices, for $l \in \mathcal{L} \cup \{6, 14, 15\}$. The secrecy gain is a lattice invariant (see Section 3 for a precise definition) that characterizes the performance of a lattice when used as a lattice wiretap code [5], and depends on the theta series of the lattice considered. It has been studied for unimodular lattices, in [6] for unimodular lattices up to dimensions 23, in [5, 7] for higher dimensional and extremal unimodular lattices, and in [8] for unimodular lattices constructed from direct sums and from codes. It was shown that lattices with large minimum norm tend to have a large (thus good) secrecy gain. Then 2-, 3- and 5-modular lattices and their secrecy gain were considered respectively in [9, 10], and a generic construction of l -modular lattices from a general Construction A over number fields was proposed in [11], where a few secrecy gains were computed. All the evidence obtained so far confirms that lattices with a large minimum norm tend to have the best secrecy gain, but what is less clear, is which level allows to obtain best secrecy gains. To tackle this question, this paper studies the secrecy gain of l -modular lattices, for $l \in \mathcal{L} \cup \{6, 14, 15\}$, focusing on lattices with large minimum norm, especially extremal lattices.

The methodology, which shapes the paper organization, is as follows. Using the above results, we will construct theta series of extremal lattices in high dimensions. To do so, we need to identify the theta series of even l -modular lattices for $l \in \mathcal{L} \cup \{6, 14, 15\}$ in the smallest dimension (see Section 2), and when there are several of them, we will see that considering those extremal is enough. Equipped with these theta series, we then recall the concept of secrecy gain, and compute it for extremal theta series of level l in Section 3. We will skip the case $l = 1$, since unimodular lattices have already been studied in [5, 6, 7, 8]. We then compare the numerical results obtained. We show in particular that $l = 2, 3, 6, 7, 11$ are the best levels for the respective ranges of dimensions $\{80, 76, 72\}$, $\{68, 64, 60, 56, 52, 48\}$, $\{44, 40, 36\}$, $\{34, 32, 30, 28, 26, 24, 22\}$, $\{18, 16, 14, 12, 10, 8\}$. This suggests that within a range of dimensions where different levels exist, the highest value of l tends to give the best secrecy gain. We conclude by giving a lower bound on the maximal secrecy gain given l and n , using Siegel's formula.

The results presented in this paper have been computed using the software SAGE 7.3 [12]. Since the only way to verify the given computations is to redo them, we provide the code used to compute the results presented in the paper here:

<https://github.com/feog/ExtremalLattices>.

2. THETA SERIES OF EVEN MODULAR LATTICES

To evaluate (2) and (5), it is needed to know the lowest dimensional even strongly l -modular lattices for $l \in \mathcal{L} \cup \{6, 14, 15\}$, and their respective theta series. We will focus mostly on extremal such lattices, and will argue why a posteriori, namely that these are enough to obtain all higher dimensional extremal theta series (in Section 3). The relevant parameters are listed in Table 1 for convenience.

Recall first the Jacobi theta functions:

$$\vartheta_2(z) = \sum_{m=-\infty}^{\infty} q^{(m+\frac{1}{2})^2}, \quad \vartheta_3(z) = \sum_{m=-\infty}^{\infty} q^{m^2}, \quad \vartheta_4(z) = \sum_{m=-\infty}^{\infty} (-1)^m q^{m^2}.$$

Note that $\vartheta_3(cz) = \sum_{m=-\infty}^{\infty} q^{cm^2}$, and similarly for $\vartheta_2(cz)$ and $\vartheta_4(cz)$ for c some constant.

We start with $l \in \mathcal{L} = \{1, 2, 3, 5, 7, 11, 23\}$.

l	$n = 2k_0$	lattice	$2 + 2 \lfloor \frac{n \sum_{d l} d}{24 \sum_{d l} 1} \rfloor$	k_l
2	4	D_4	2	8
3	2	A_2	2	6
5	4	QQF.4.a	2	4
7	2	L_7	2	3
11	2	L_{11}	2	2
23	2	L_{23}	4	1
6	4	QQF.4.g, QQF.4.i	2	2
14	4	E(14)	4	1
15	4	E(15)	4	1

TABLE 1. Lattices in the smallest dimension $2k_0$ which are even, strongly l -modular and extremal. For $l \in \{2, 3, 5, 7, 11\}$, such a lattice is unique [3, 3.1]. For $l = 14, 15, 23$, such a lattice has minimum 4, and therefore is also unique [3, 3.2]. For $l = 6$, there are exactly two such lattices [3, 3.2]. The 4th column gives the minimum for extremal lattices.

2.1. Lowest Dimensional Even l -Modular Lattices, $l \in \mathcal{L}$. The lowest dimensions in which l -modular even lattices exist are [3, 3.1] 4 for $l = 2, 5$, and 2 for $l = 3, 7, 11$. Recall that we do not consider $l = 1$ in this paper. For $l = 23$, we will exhibit a 2-dimensional even l -modular lattice, and since such lattices exist only in even dimensions, this will give 2 as the lowest dimension.

The cases $l = 2, 3$. For $l = 2, 3$, we thus have $k_0 = 2, 1$, and $\Theta_{2k_0}(z)$ denotes the theta function of the lattices D_4 [13, chap 2 (37)] and A_2 [13, chap 4(60)] respectively:

$$\begin{aligned}
 \Theta_{D_4}(z) &= \frac{1}{2}(\vartheta_3(z)^4 + \vartheta_4(z)^4) \\
 &= 1 + 24q^2 + 24q^4 + 96q^6 + 24q^8 + \dots
 \end{aligned}
 \tag{7}$$

$$\begin{aligned}
 \Theta_{A_2}(z) &= \vartheta_3(z) \vartheta_3(3z) + \vartheta_2(z) \vartheta_2(3z) \\
 &= 1 + 6q^2 + 6q^6 + 6q^8 + 12q^{14} + \dots
 \end{aligned}
 \tag{8}$$

The case $l = 5$. There is a unique even extremal 5-modular lattice of lowest dimension, the so-called QQF.4.a lattice [14] of dimension 4. Its theta series can be computed numerically from its Gram matrix (given e.g. in [14]). It could alternatively be computed from that of the 8-dimensional 5-modular even Maass lattice, also known as Q8(1) or H4 [14] whose theta series can be computed numerically¹ to be

$$\Theta_{Maass}(z) = 1 + 120q^4 + 240q^6 + 600q^8 + \dots$$

We have $k_5 = 24/6 = 4$ and $k_0 = 2$. From (3), we get the constraint

$$2\lambda + 4\mu = 4$$

thus we only have $(\lambda, \mu) = (0, 1)$ and $(2, 0)$, and

$$\Theta_{Maass}(z) = a_0 \Theta_4^2 + a_1 \Delta_5$$

¹We provide the computations for the sake of demonstrating a method to compute a theta series of lattice using another one.

where Θ_4 is the theta series of a 4-dimensional 5-modular even lattice. We next determine the values of a_0 and a_1 , using that

$$\Delta_5 = q^2 - 4q^4 + 2q^6 + \dots$$

Since Θ_4^2 has a constant term which is 1, $a_0 = 1$. Then

$$\Theta_{Maass}(z) = 1 + 120q^4 + 240q^6 + 600q^8 + \dots = \Theta_4^2 + a_1(q^2 - 4q^4 + \dots)$$

and if Θ_4 has a linear term in q , so has Θ_4^2 , a contradiction. Thus $\Theta_4 = \Theta_{QQF.4.a}$ is the theta series of QQF.4.a which we are interested in, since QQF.4.a is the unique extremal 5-modular lattice in dimension 4, whose kissing number is 6 [14]. Then

$$\Theta_{Maass}(z) = 1 + 120q^4 + 240q^6 + 600q^8 + \dots = (1 + 6q^2 + \dots)^2 + a_1(q^2 - 4q^4 + \dots)$$

and $a_1 = -12$. Thus

$$\Theta_{QQF.4.a} = \sqrt{\Theta_{Maass}(z) + 12\Delta_5}$$

whose firm terms are given by

$$1 + 6q^2 + 18q^4 + 24q^6 + 42q^8 + \dots$$

The case $l = 7$. An even extremal 7-modular lattice L_7 of lowest positive dimension has [3, 3.1] Gram matrix

$$\begin{bmatrix} 2 & 1 \\ 1 & c \end{bmatrix} = \begin{bmatrix} x \cdot x & x \cdot y \\ x \cdot y & y \cdot y \end{bmatrix}, \quad c = 4,$$

for x, y two basis vectors of this lattice. Thus for $v \in L_7$, $v = v_1x + v_2y$, $v_1, v_2 \in \mathbb{Z}$, and $v \cdot v = (v_1x + v_2y) \cdot (v_1x + v_2y) = 2v_1^2 + 2v_1v_2 + cv_2^2$, $c = 4$. The theta series of L_7 is then

$$\Theta_{L_7}(z) = \sum_{v \in L_7} q^{v \cdot v} = \sum_{(v_1, v_2) \in \mathbb{Z}^2} q^{2(v_1^2 + v_1v_2 + \frac{c}{2}v_2^2)} = \sum_{(v_1, v_2) \in \mathbb{Z}^2} q^{2[(v_1 + \frac{v_2}{2})^2 + (2c-1)\frac{v_2^2}{4}]}$$

The terms in which v_2 is even contribute, setting $u_1 = v_1 + v_2/2$, $u_2 = v_2/2$

$$\sum_{(u_1, u_2) \in \mathbb{Z}^2} q^{2[u_1^2 + (2c-1)u_2^2]} = \vartheta_3(2z)\vartheta_3(2(2c-1)z) = \vartheta_3(2z)\vartheta_3(14z)$$

while the terms in which v_2 is odd contribute, setting $u_1 = v_1 + (v_2 - 1)/2$, $u_2 = (v_2 - 1)/2$

$$\sum_{(v_1, v_2) \in \mathbb{Z}^2} q^{2[(v_1 + \frac{v_2-1}{2} + \frac{1}{2})^2 + (2c-1)(\frac{v_2-1}{2} + \frac{1}{2})^2]} = \sum_{(u_1, u_2) \in \mathbb{Z}^2} q^{2[(u_1 + \frac{1}{2})^2 + (2c-1)(u_2 + \frac{1}{2})^2]}$$

showing that

$$(9) \quad \Theta_{L_7}(z) = \vartheta_3(2z)\vartheta_3(14z) + \vartheta_2(2z)\vartheta_2(14z).$$

For $c = 4$,

$$\Theta_{L_7}(z) = \vartheta_3(2z)\vartheta_3(14z) + \vartheta_2(2z)\vartheta_2(14z) = 1 + 2q^2 + 4q^4 + 6q^8 + 2q^{14} + \dots$$

The case $l = 11$. An even extremal 11-modular lattice L_{11} of lowest positive dimension has [3, 3.1] Gram matrix

$$\begin{bmatrix} 2 & 1 \\ 1 & c \end{bmatrix}, \quad c = 6,$$

with, from (9), theta series

$$\Theta_{L_{11}}(z) = \vartheta_3(2z)\vartheta_3(22z) + \vartheta_2(2z)\vartheta_2(22z) = 1 + 2q^2 + 4q^6 + 2q^8 + 4q^{10} + \dots$$

The case $l = 23$. It is known [13, Table 15.1] that reduced positive definite 2-dimensional integral quadratic forms with determinant 23 are

$$\begin{bmatrix} 1 & 0 \\ 0 & 23 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 12 \end{bmatrix}, \begin{bmatrix} 3 & \pm 1 \\ \pm 1 & 8 \end{bmatrix}, \begin{bmatrix} 4 & \pm 1 \\ \pm 1 & 6 \end{bmatrix}$$

out of which only two are even. An even 23-modular lattice L'_{23} of lowest positive dimension has Gram matrix

$$G'_{23} = \begin{bmatrix} 2 & 1 \\ 1 & c \end{bmatrix}, \quad c = 12,$$

and, from (9), theta series

$$\Theta_{L'_{23}}(z) = \vartheta_3(2z)\vartheta_3(46z) + \vartheta_2(2z)\vartheta_2(46z) = 1 + 2q^2 + 2q^8 + 4q^{12} + \dots$$

This lattice is clearly even, and of the lowest positive dimension 2. It is indeed 23-modular, since

$$\frac{1}{23} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 12 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \frac{1}{23} \begin{bmatrix} 12 & -1 \\ -1 & 2 \end{bmatrix} = (G'_{23})^{-1}.$$

In words, up to a change of basis, $\frac{1}{23}G'_{23}$ is a Gram matrix of the dual lattice, as needed. However, it is clearly not extremal, because it contains a basis vector of norm 2.

The lattice L_{23} with following Gram matrix

$$\begin{bmatrix} 4 & 1 \\ 1 & c \end{bmatrix}, \quad c = 6$$

is for the same reason as above even, of lowest positive dimension, and 23-modular. It is however extremal, as can be seen from this theta series, computed numerically and given by

$$\Theta_{L_{23}}(z) = 1 + 2q^4 + 2q^6 + 2q^8 + 2q^{12} + \dots$$

2.2. The cases $l = 6, 14, 15$. We need to consider strongly modular lattices, as defined in the introduction. The lowest dimensions in which strongly l -modular even lattices exist are [2, Proposition 3] 4 for $l = 6, 14, 15$.

To construct a strongly even l -modular lattice, for $l = pq$, p, q distinct primes, take a p -modular even lattice L of dimension 2, then the orthogonal sum

$$L \oplus \sqrt{q}L$$

is a strongly l -modular even lattice [2, Example 1].

This lattice has theta series

$$\Theta_{L \oplus \sqrt{q}L}(z) = \Theta_L(z)\Theta_L(qz).$$

The case $l = 6$. We apply the above method to construct a strongly 6-modular lattice of dimension 4. Recall that A_2 is a 3-modular even lattice of dimension 2. Then the orthogonal sum

$$A_2 \oplus \sqrt{2}A_2$$

is a strongly 6-modular lattice with theta series $\Theta_{A_2}(z)\Theta_{A_2}(2z)$, where from (8)

$$\Theta_{A_2}(z) = \vartheta_3(z)\vartheta_3(3z) + \vartheta_2(z)\vartheta_2(3z).$$

Since A_2 has a minimum of 2, the theta series of the 6-modular lattice cannot contain a term in q , and contains a term in q^2 , thus this lattice is extremal, and is in fact called QQF.4.g [14]:

$$\Theta_{QQF.4.g}(z) = \Theta_{A_2}(z)\Theta_{A_2}(2z) = 1 + 6q^2 + 6q^4 + 42q^6 + 6q^8 + 36q^{10} + \dots$$

This theta series can also be obtained by another method [4, Thm 9]. Set $C^{(6)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \sqrt{6}\mathbb{Z}$,

$$g_1(z) = \Theta_{C^{(6)}}(z) = \vartheta_3(q)\vartheta_3(q^2)\vartheta_3(q^3)\vartheta_3(q^6)$$

which has weight 2 and

$$g_2(z) = \left(\frac{\eta(z/2)\eta(3z/2)\eta(4z)\eta(12z)}{\eta(z)\eta(3z)\eta(2z)\eta(6z)} \right).$$

Then the theta series of a strongly 6-modular lattice, whose weight is k times the weight of $\Theta_{C^{(6)}}(z)$, is given [4, Thm 9] by

$$g_1(z)^k \sum_{i=0}^{\lfloor k \frac{1}{6} \sum_{d|6} d \rfloor} c_i g_2(z)^i = g_1(z) \sum_{i=0}^2 c_i g_2(z)^i$$

where we choose $k = 1$ to obtain a lattice of dimension 4 and thus weight 2. We are left to identify c_i in

$$a_0 + a_1 g_1(z) + a_2 g_1(z)^2$$

to get the theta series of an extremal lattice, whose minimum is 4. Since

$$g_1(z) = 1 + 2q + 2q^2 + 6q^3 + 6q^4 + \dots,$$

$$g_1(z)g_2(z) = q - q^3 - 2q^5 + \dots,$$

$$g_1(z)g_2(z)^2 = q^2 - 2q^3 - 2q^5 + \dots,$$

and $c_0 g_1(z)$ is the only term that contains a constant term, it must be that $c_0 = 1$, that $c_2 = 4$ and consequently that $c_1 = -2$. The advantage of the first computation is that it gives a construction of the lattice itself. The advantage of the second computation is that it shows that uniqueness of a strongly 6-modular lattice which is even, extremal, and rationally equivalent to $C^{(6)}$.

The technique from [4, Thm 9] does not apply if the lattice is not rationally equivalent to $C^{(6)}$, and such a lattice is known to exist, namely the lattice QQF.4.i is strongly 6-modular, even and extremal, but not rationally equivalent to $C^{(6)}$. As already mentioned earlier, QQF.4.i and QQF.4.g are the only extremal even 6-strongly modular lattices in dimension 4. Since the Gram matrix of QQF.4.i is known, we compute its theta series numerically:

$$\Theta_{QQF.4.i}(z) = 1 + 4q^2 + 20q^4 + 4q^6 + 52q^8 + 24q^{10} + \dots$$

The case $l = 14$. To construct a strongly 14-modular lattice of dimension 4, we can use the same method with the 2-dimensional 7-modular lattice L_7 built above. The orthogonal sum

$$L_{14} = L_7 \oplus \sqrt{2}L_7$$

is a strongly 14-modular lattice. This lattice has theta series

$$\Theta_{L_{14}}(z) = \Theta_{L_7}(z)\Theta_{L_7}(2z)$$

where Θ_{L_7} is the theta series of the extremal even 7-modular lattice of dimension 2. However since this lattice has minimum norm of 2, $\Theta_{L_{14}}$ will contain a term in q^2 and will not be extremal.

Set $C^{(14)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus \sqrt{7}\mathbb{Z} \oplus \sqrt{14}\mathbb{Z}$,

$$g_1(z) = \Theta_{C^{(14)}}(z) = \vartheta_3(q)\vartheta_3(q^2)\vartheta_3(q^7)\vartheta_3(q^{14})$$

which has weight 2 and

$$g_2(z) = \left(\frac{\eta(z/2)\eta(7z/2)\eta(4z)\eta(28z)}{\eta(z)\eta(7z)\eta(2z)\eta(14z)} \right).$$

Then the theta series of weight k times the weight of $\Theta_{C^{(14)}}(z)$ of a strongly 14-modular lattice is given [4, Thm 9] by

$$g_1(z)^k \sum_{i=0}^{\lfloor k \frac{1}{6} \sum_{d|14} d \rfloor} c_i g_2(z)^i.$$

To obtain an extremal lattice of dimension 4 and thus weight 2, whose minimum is 4, we choose $k = 1$, and we identify the c_i in

$$g_1(z) \sum_{i=0}^4 c_i g_2(z)^i$$

to be $c_0 = 1$, $c_1 = -2$, $c_2 = 0$, $c_3 = -4$, and $c_4 = 4$.

We already know from the introduction the unicity of the even strongly 14-modular extremal lattice in dimension 4, the above further shows that it is rationally equivalent to $C^{(14)}$. We thus obtain the theta series

$$\Theta_{E(14)}(z) = g_1(z)(1 - 2g_2(z) - 4g_2(z)^3 + 4g_2(z)^4) = 1 + 8q^4 + 8q^6 + 16q^8 + 8q^{10} + 24q^{12} + \dots$$

which is the theta series of the extremal strongly 14-modular even lattice in dimension 4, called $E(14)$ [14].

The case $l = 15$. Set $C^{(15)} = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \sqrt{5}\mathbb{Z} \oplus \sqrt{15}\mathbb{Z}$,

$$g_1(z) = \Theta_{C^{(15)}}(z) = \vartheta_3(q)\vartheta_3(q^3)\vartheta_3(q^5)\vartheta_3(q^{15})$$

which has weight 2 and

$$g_2(z) = \left(\frac{\prod_{d|15} \eta(dz/2)\eta(d2z)}{\prod_{d|15} \eta(dz)^2} \right).$$

Then, using the same technique as above, the theta series of weight k times the weight of $\Theta_{C^{(15)}}(z)$ of a strongly 15-modular lattice, that is here, $k = 1$, is given [4, Thm 9] by

$$g_1(z) \sum_{i=0}^{\lfloor k \frac{1}{8} \sum_{d|15} d \rfloor} c_i g_2(z)^i = g_1(z) \sum_{i=0}^3 c_i g_2(z)^i$$

where

$$\begin{aligned} g_1(z) &= 1 + 2q + 2q^3 + 6q^4 + 2q^5 + 4q^6 + \dots, \\ g_2(z) &= q - q^2 + q^3 - 3q^4 + 3q^5 - 5q^6 + \dots \end{aligned}$$

We are looking for c_i to get the theta series of an extremal lattice, whose minimum is 4. It must be that $c_0 = 1$, $c_1 = -2$, $c_2 = 2$, $c_3 = -4$. We thus obtain the theta series of the lattice E(15) [14]

$$\Theta_{E(15)}(z) = g_1(z)(1 - 2g_2(z) + 2g_2(z)^2 - 4g_2(z)^3) = 1 + 6q^4 + 12q^6 + 12q^8 + 30q^{12} + \dots$$

We already know from the introduction the unicity of this strongly 15-modular even lattice, the above showed that it is rationally equivalent to $C^{(15)}$. There is another extremal lattice in dimension 4, the lattice QQF.4.e [14] which is however odd, and not rationally equivalent to $C^{(15)}$.

3. THETA SERIES AND SECRECY GAIN OF EVEN LATTICES

Let Λ be an n -dimensional lattice in $\mathbb{R}^n$, with generator matrix M . The *secrecy function* of Λ is given [5] by

$$(10) \quad \Xi_{\Lambda}(y) = \frac{\Theta_{\sqrt[n]{\text{vol}(\Lambda)}\mathbb{Z}^n}(y)}{\Theta_{\Lambda}(y)}, y = -iz, y > 0,$$

where $\text{vol}(\Lambda) = |\det(M)|$ is the volume of the lattice Λ . The *secrecy gain* χ_{Λ} is then the maximum of the secrecy function (10). It characterizes the gain in secrecy brought by lattice coding, versus the uncoded case.

The similarity of an ℓ -modular lattice induces a symmetry in its secrecy function with a local optimum achieved at $y = \frac{1}{\sqrt{\ell}}$, which is hence called the *weak secrecy gain* χ_{Λ}^W and conjectured to be the secrecy gain itself [5]. The conjecture has been checked for infinitely many unimodular lattices [15, 8]. For l -modular lattices, one case has been found (for $l = 4$) where the optimum is a minimum [18], exhibiting a case where coding is actually worse in terms of terms of secrecy than not coding, while all other known cases [9, 10, 11] support the conjecture, suggesting a refinement of the conjecture, to include (and understand) cases for which a minimum is reached instead of a maximum. In this paper, all the best secrecy gains are maximum, and therefore we are in the situation where $\chi_{\Lambda}^W = \chi_{\Lambda}$, or in words, the symmetry point is the secrecy gain.

We next compute theta series of extremal strongly l -modular lattices for $l \in \mathcal{L} \cup \{6, 14, 15\}$, after which we will evaluate the weak secrecy gain that each theta series yields.

3.1. Extremal Theta Series of Even l -modular Lattices. We start with the level $l = 23$, for which the number of extremal lattices is small, and then consider levels in decreasing order until $l = 2$. We will apply the general method (already applied to compute the theta series of the 5-modular even extremal lattice of dimension 4).

- For each level and each dimension, we are looking at integer linear combinations of terms of the form

$$\Theta_{2k_0}^{\lambda} \Delta_l^{\mu}, \lambda, \mu \geq 0$$

where λ, μ satisfies a weight constraint $k_0\lambda + k_l\mu = k$ for l prime or $k_0\lambda + 2k_l\mu = k$ for l composite. In all cases, $(\lambda, \mu) = (k/k_0, 0)$ will turn out to be a valid integer solution. Since whenever $\mu \geq 1$, the term Δ_l^{μ} has no constant term, and we are looking for a theta series whose constant term is necessarily 1, this means that in the integer linear combination, the

l	n	theta series
2	4	$\Theta_{D_4} = 1 + 24q^2 + 24q^4 + 96q^6 + \dots$
3	2	$\Theta_{A_2} = 1 + 6q^2 + 6q^6 + 6q^8 + 12q^{14} + \dots$
5	4	$\Theta_{QQF.4.a} = 1 + 6q^2 + 18q^4 + 24q^6 + 42q^8 + \dots$
7	2	$\Theta_{L_7} = 1 + 2q^2 + 4q^4 + 6q^8 + 2q^{14} + \dots$
11	2	$\Theta_{L_{11}} = 1 + 2q^2 + 4q^6 + \dots$
23	2	$\Theta_{L_{23}} = 1 + 2q^4 + 2q^6 + 2q^8 + \dots$ $\Theta_{L'_{23}} = 1 + 2q^2 + 2q^8 + 4q^{12} + \dots$
6	4	$\Theta_{QQF.4.g} = 1 + 6q^2 + 6q^4 + 42q^6 + 6q^8 + \dots$ $\Theta_{QQF.4.i} = 1 + 4q^2 + 20q^4 + 4q^6 + 52q^8 + \dots$
14	4	$\Theta_{E(14)} = 1 + 8q^4 + 8q^6 + 16q^8 + 8q^{10} + 24q^{12} + \dots$
15	4	$\Theta_{E(15)} = 1 + 6q^4 + 12q^6 + 12q^8 + 30q^{12} + \dots$ $\Theta_{L_{15}} = 1 + 4q^2 + 4q^4 + 12q^8 + \dots$ $\Theta_{L'_{15}} = 1 + 2q^2 + 4q^4 + 10q^6 + 10q^8 + \dots$

TABLE 2. Lattices in the smallest dimension n which are even, strongly l -modular and extremal (except for $l = 14, 15, 23$ where $L_{14}, L'_{14}, L_{15}, L'_{15}, L_{23}$ are not extremal) and their theta series.

coefficient of $\Theta_{2k_0}^\lambda$ is always 1. We will illustrate this in detail for the case $l = 23$, and then will always use this fact without repeating it.

- We are interested in extremal lattices. We will thus look for extremal theta series, that is theta series whose first nonzero power of q is $2 + 2\lfloor \frac{n \sum_{d|l} d}{24 \sum_{d|l} 1} \rfloor$. We will discuss later the question of possibly finding the corresponding lattice, assuming it exists. To do so, we collect all the terms of the form

$$\Theta_{2k_0}^\lambda \Delta_l^\mu, \quad \lambda, \mu \geq 0$$

where λ, μ satisfy the weight constraint for the chosen l , and we look for integer coefficients that cancel out the terms in small powers of q , so that the minimum norm corresponds to that of an extremal lattice. To make sure we get them all, we rely on an exhaustive list of extremal lattices in the smallest dimension. We will show that it is enough to consider for Θ_{2k_0} the theta series of an extremal lattice.

- We use the table [14] as a reference. Thus if we find a theta series whose kissing number corresponds to a lattice listed in the table, we give its name.

The case $l = 23$. For $l = 23$, extremal even lattices are known [3, Table 2.4] to exist only in dimensions $n = 2$ and $n = 4$. The case $n = 2$ is the case of minimal dimension, which was treated in the previous section. We thus consider the case $n = 4$. From (2)-(3), the general form of a theta series of a strongly 23-modular even lattice of dimension 4 is

$$\Theta_2^\lambda \Delta_{23}^\mu, \quad \lambda + \mu = 2, \quad \lambda, \mu \geq 0,$$

where Θ_2 is the theta series of a 2-dimensional even 23-modular lattice, and

$$\Delta_{23} = q^2 - q^4 - q^6 + q^{12} + q^{16} + \dots$$

This gives

$$a_0 \Theta_2^2 + a_1 \Theta_2 \Delta_{23} + a_2 \Delta_{23}^2$$

and a_0 must be 1 so that the resulting series starts with 1. If we choose $\Theta_2 = \Theta_{L_{23}} = 1 + 2q^4 + 2q^6 + 2q^8 + \dots$, then the term $\Theta_2 \Delta_2$ contains a term in q^2 which can only be cancelled out if $a_1 = 0$. Then

$$\begin{aligned} & (1 + 2q^4 + 2q^6 + 2q^8 + \dots)^2 + a_2(q^2 - q^4 - q^6 + \dots)^2 \\ &= 1 + 4q^4 + 4q^6 + 8q^8 + 8q^{10} + \dots + a_2(q^4 - 2q^6 - q^8 + 2q^{10} + \dots) \end{aligned}$$

and $a_2 = -4$, which gives

$$\boxed{\Theta_{L_{23}}^2 - 4\Delta_{23}^2 = 1 + 12q^6 + 12q^8 + 12q^{12} + 24q^{16} + 12q^{18} + 24q^{20} + \dots}$$

Now we try $\Theta_2 = \Theta_{L'_{23}} = 1 + 2q^2 + 2q^8 + \dots$, since we saw there are only two even 23-modular lattices in dimension 2. Then

$$\begin{aligned} & (1 + 2q^2 + \dots)^2 + a_1(1 + 2q^2 + \dots)(q^2 - q^4 - \dots) + a_2(q^2 - q^4 - \dots)^2 \\ &= 1 + 4q^2 + 4q^4 + \dots + a_1(q^2 + q^4 + \dots) + a_2(q^4 - \dots) \end{aligned}$$

and we set $a_1 = -4$, $a_2 = 0$, to obtain

$$\boxed{\Theta_{L'_{23}}^2 - 4\Theta_2 \Delta_{23} = 1 + 12q^6 + 12q^8 + 12q^{12} + 24q^{16} + 12q^{18} + 24q^{20} + \dots,}$$

which turns out to be the same theta series.

Since the bound on the minimum for $l = 23$ gives $2 + 2\lfloor \frac{n}{2} \rfloor$, this theta series corresponds to that of an extremal lattice, and since we exhausted both choices for Θ_2 and for determining a_1, a_2 , this is the unique extremal theta series we can obtain.

The case $l = 15$. From (5), a generic theta series for even strongly 15-modular lattices is

$$\Theta_4^\lambda \Delta_{15}^\mu, \quad 2\lambda + 2\mu = k$$

with

$$\Delta_{15} = q^2 - q^4 - q^6 - q^8 + \dots$$

and the upper bound for the minimum of these lattices is

$$2 + 2\lfloor \frac{n}{4} \rfloor.$$

For example, for $n = 8$, we have a minimum of 6, and

$$\Theta_4^2 + a_1 \Theta_4 \Delta_{15} + a_2 \Delta_{15}^2.$$

We notice that Θ_4 could be the theta series of the extremal even strongly 15-modular lattice $E(15)$, but other 4-dimensional strongly 15-modular lattices could be used as well.

According to [16], there are exactly five 4-dimensional even 15-modular lattices. Among them, only three are strongly modular, including $E(15)$. This can be checked by computing explicitly the partial duals. The other two lattices have Gram matrices

$$\begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 10 & 5 \\ 0 & 0 & 5 & 10 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 & 0 & 1 \\ 0 & 4 & 1 & 0 \\ 0 & 1 & 4 & 0 \\ 1 & 0 & 0 & 8 \end{bmatrix}$$

and theta series

$$\begin{aligned} \Theta_{L_{15}} &= 1 + 6q^2 + 6q^6 + 6q^8 + 6q^{10} + 36q^{12} + O(q^{14}) \\ \Theta_{L'_{15}} &= 1 + 2q^2 + 4q^4 + 10q^6 + 10q^8 + 2q^{10} + 32q^{12} + 12q^{14} + O(q^{16}) \end{aligned}$$

respectively.

The values of n for which 15-modular even extremal lattices exist are from [3, Table 2.4]. We list below the extremal theta series found using for Θ_4 the theta series of $E(15)$, L_{15} and L'_{15} . No matter the choice of Θ_4 among these three theta series, the result is the same.

n	Θ	name
8	$1 + 48q^6 + 72q^8 + 144q^{10} + 288q^{12} + O(q^{13})$	st15moddim8a
12	$1 + 270q^8 + 432q^{10} + 1260q^{12} + O(q^{13})$	(C2 x C3.Alt6).(C2 x C2)
16	$1 + 1440q^{10} + 2400q^{12} + O(q^{13})$	(SL(2,5) Y SL(2,9)):C2
20	$1 + 7860q^{12} + 9720q^{14} + O(q^{15})$	

The case $l = 14$. From (5), a generic theta series for even strongly 14-modular lattices is

$$\Theta_4^\lambda \Delta_{14}^\mu, \quad 2\lambda + 2\mu = k$$

with

$$\Delta_{14} = q^2 - q^4 - 2q^6 + q^8 + \dots$$

and the upper bound for the minimum of these lattices is

$$2 + 2\lfloor \frac{n}{4} \rfloor.$$

Similarly to what happened with $l = 15$, there are exactly five 4-dimensional even 14-modular lattices [16] whose series could a priori be used for Θ_4 . Among them, only three are strongly modular, including $E(14)$. This can be check by computing explicitly the partial duals. The other two lattices have Gram matrices

$$\begin{bmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 1 & 1 & 8 & 1 \\ 1 & 1 & 1 & 8 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 2 & 8 \end{bmatrix}$$

and theta series

$$\begin{aligned} \Theta_{L_{14}} &= 1 + 4q^2 + 4q^4 + 20q^8 + 8q^{10} + 32q^{12} + O(q^{14}) \\ \Theta_{L'_{14}} &= 1 + 2q^2 + 6q^4 + 4q^6 + 18q^8 + 8q^{10} + 28q^{12} + 2q^{14} + O(q^{16}) \end{aligned}$$

respectively.

The values of n for which 14-modular even extremal lattices exist are from [3, Table 2.4]. The extremal theta series obtained using $\Theta_4 = \Theta_{E(14)}$ (as for $= 15$, using L_{14} or L'_{14} does not change the result) are listed below.

n	Θ	name
8	$1 + 48q^6 + 144q^8 + 48q^{10} + 336q^{12} + O(q^{13})$	8QF.8.e
12	$1 + 336q^8 + 672q^{10} + 1064q^{12} + O(q^{13})$	(PSL(2,7) x D8):C2
16	$1 + 1920q^{10} + 4320q^{12} + O(q^{13})$	
20	$1 + 11480q^{12} + O(q^{13})$	

The case $l = 11$. Extremal lattices exist in dimension $n = 2, 4, 6, 8, 10, 12, 14, 18$ [3, Table 2.4], and their minimum reaches

$$2 + 2\lfloor \frac{n}{4} \rfloor.$$

We start with $n = 4$. From (2), the general form of a theta series of a strongly 11-modular even lattice of dimension 4 is

$$\Theta_2^\lambda \Delta_{11}^\mu, \quad \lambda + 2\mu = 2, \quad \lambda, \mu \geq 0,$$

where

$$\Delta_{11} = q^2 - 2q^4 - q^6 + 2q^8 + q^{10} + 2q^{12} - 2q^{14} \dots$$

Thus, using that Θ_2 is the theta series of L_{11} (a lattice with minimum norm 1 gives a term in q that cannot be simplified and thus a theta series that has q as lowest power)

$$\Theta_2^2 + a_1 \Delta_{11} = (1 + 2q^2 + 4q^6 + \dots)^2 + a_1(q^2 - 2q^4 - q^6 + \dots)$$

and $a_1 = -4$ ensures that the term in q^2 cancels out, to give

$$1 + 12q^4 + 12q^6 + 12q^8 + \dots$$

which corresponds to the lattice QQF.4.b [14], and

$$\Theta_{QQF.4.b}(z) = \Theta_{L_{11}}(z)^2 - 4\Delta_{11}.$$

For $n = 6$, we have from (2)

$$a_1 \Theta_2 \Delta_{11} + \Theta_2^3,$$

choosing $\Theta_2 = \Theta_{L_{11}}$ (if Θ_2 had a term in q , it would remain in Θ_2^3) thus $a_1 = -6$ and we get the theta series of the lattice 6QF.6.b [14]:

$$\Theta_{6QF.6.b}(z) = -6\Theta_2 \Delta_{11} + \Theta_2^3$$

whose series is

$$1 + 12q^4 + 50q^6 + \dots$$

We repeat the same computations for other available dimensions. Note that every term $\Theta_2^i \Delta_{11}^j$, for $j > 0$, has no term in q , therefore, Θ_2 must be $\Theta_{L_{11}}$ so as not to have a term in q in the resulting theta series.

n	Θ	name
4	$1 + 12q^4 + 12q^6 + 12q^8 + 12q^{10} + 24q^{12} + O(q^{13})$	QQF.4.b
6	$1 + 12q^4 + 50q^6 + 30q^8 + 90q^{10} + 120q^{12} + O(q^{13})$	6QF.6.b
8	$1 + 120q^6 + 120q^8 + 120q^{10} + 600q^{12} + O(q^{13})$	8QF.8.a
10	$1 + 110q^6 + 330q^8 + 462q^{10} + 1320q^{12} + O(q^{13})$	A10(3)
12	$1 + 1044q^8 + 288q^{10} + 1908q^{12} + O(q^{13})$	
14	$1 + 854q^8 + 2184q^{10} + 2996q^{12} + O(q^{13})$	
18	$1 + 6732q^{10} + 10560q^{12} + O(q^{13})$	

The case $l = 7$. From (2), a generic theta series for even 7-modular lattices is

$$\Theta_2^\lambda \Delta_7^\mu, \lambda + 3\mu = k$$

with

$$\Delta_7 = q^2 - 3q^4 + 5q^8 - 7q^{14} - 3q^{16} + \dots$$

and the upper bound for the minimum of these lattices is

$$2 + 2\lfloor \frac{n}{6} \rfloor.$$

Note that as above, for every term $\Theta_2^i \Delta_7^j$, for $j > 0$, has no term in q , therefore, Θ_2 must be Θ_{L_7} so as not to have a term in q in the resulting theta series. The values of n for which 7-modular even extremal lattices exist are from [3, Table 2.4].

n	Θ	name
4	$1 + 4q^2 + 12q^4 + 16q^6 + O(q^7)$	
6	$1 + 42q^4 + 56q^6 + 84q^8 + O(q^9)$	A(6)2
8	$1 + 48q^4 + 144q^6 + 384q^8 + O(q^9)$	
10	$1 + 50q^4 + 240q^6 + 900q^8 + O(q^9)$	
12	$1 + 616q^6 + 1176q^8 + O(q^9)$	
14	$1 + 560q^6 + 2394q^8 + O(q^9)$	Sch14
16	$1 + 480q^6 + 3360q^8 + O(q^9)$	dim16mod7
18	$1 + 7434q^8 + O(q^9)$	
20	$1 + 6160q^8 + O(q^9)$	
22	$1 + 4906q^8 + O(q^9)$	
24	$1 + 84672q^{10} + 91728q^{12} + O(q^{13})$	
26	$1 + 66612q^{10} + 256620q^{12} + O(q^{13})$	
28	$1 + 50848q^{10} + 348264q^{12} + O(q^{13})$	
30	$1 + 944720q^{12} + O(q^{13})$	
32	$1 + 719040q^{12} + O(q^{13})$	
34	$1 + 534072q^{12} + O(q^{13})$	

The case $l = 6$. From (5), a generic theta series for even strongly 6-modular lattices is

$$\Theta_4^\lambda \Delta_6^\mu, \quad 2\lambda + 4\mu = k, \quad \Delta_6 = q^2 - 2q^4 - 3q^6 + 4q^8 + 6q^{10} + \dots$$

and the upper bound for the minimum of these lattices is $2 + 2\lfloor \frac{n}{8} \rfloor$. There are only two choices for Θ_4 , it is necessarily the theta series of one of the two extremal lattices QQF.4.g and QQF.4.i, since there is no non-extremal lattice which is 6-modular in dimension 4 (see [16]).

The values of n for which 6-modular even extremal lattices exist are from [3, Table 2.4].

The extremal theta series obtained from QQF.4.g and QQF.4.i are shown below. For a given dimension, the first row comes from QQF.4.g, the second row comes from QQF.4.i, and a single row means both lattices give the same extremal series.

n	Θ	name
8	$1 + 72q^4 + 192q^6 + 504q^8 + O(q^9)$	A2xD4
12	$1 + 54q^4 + 720q^6 + 1998q^8 + O(q^9)$	
	$1 + 84q^4 + 448q^6 + 2940q^8 + O(q^9)$	Q(A6(2),1,1,1)
16	$1 + 960q^6 + 6480q^8 + O(q^9)$	((Sp(4,3) x C3) Y SL(2,3)).C2
20	$1 + 660q^6 + 8910q^8 + O(q^9)$	
	$1 + 640q^6 + 9180q^8 + O(q^9)$	
24	$1 + 10584q^8 + O(q^9)$	(C6.PSL(3,4).C2 Y D8).C2
28	$1 + 5670q^8 + O(q^9)$	
	$1 + 6020q^8 + O(q^9)$	
32	$1 + 103680q^{10} + O(q^{11})$	
36	$1 + 51516q^{10} + O(q^{11})$	
	$1 + 53424q^{10} + O(q^{11})$	
40	$1 + 997920q^{12} + O(q^{13})$	
44	$1 + 463716q^{12} + O(q^{13})$	
	$1 + 481536q^{12} + O(q^{13})$	

The case $l = 5$. From (2), a generic theta series for even 5-modular lattices is

$$\Theta_4^\lambda \Delta_5^\mu, \quad 2\lambda + 4\mu = k$$

with

$$\Delta_5 = q^2 - 4q^4 + 2q^6 + \dots$$

and the upper bound for the minimum of these lattices is

$$2 + 2\lfloor \frac{n}{8} \rfloor \geq 2.$$

Note that here, every term $\Theta_4^\mu \Delta_5^\lambda$, for $\lambda > 0$, has no term in q , therefore, Θ_4 cannot have a term in q (which would remain when computing Θ_4^λ , $\lambda \geq 1$), so it must be that $\Theta_4 = \Theta_{QQF.4.a}$ so as not to have a term in q in the resulting theta series. From [3, Table 2.4], extremal even 5-modular lattices exist in dimensions which are multiples of 4, until 44.

The extremal theta series are given in the table below.

n	Θ	name
8	$1 + 120q^4 + 240q^6 + 600q^8 + O(q^9)$	Q8(1)
12	$1 + 126q^4 + 1008q^6 + 4410q^8 + O(q^9)$	ext12m5
16	$1 + 2400q^6 + 10800q^8 + O(q^9)$	C2.Alt10
20	$1 + 1740q^6 + 22590q^8 + O(q^9)$	
24	$1 + 37800q^8 + O(q^9)$	(C2.J2 Y SL(2,5)):C2

n	Θ	name
28	$1 + 23310q^8 + O(q^9)$	J2dim14
32	$1 + 552960q^{10} + 4152000q^{12} + O(q^{13})$	Beis16
36	$1 + 310716q^{10} + 5537700q^{12} + O(q^{13})$	
40	$1 + 7854000q^{12} + O(q^{13})$	
44	$1 + 4156284q^{12} + O(q^{13})$	

The case $l = 3$. From (2), a generic theta series for even 3-modular lattices is

$$\Theta_2^\lambda \Delta_3^\mu, \quad \lambda + 6\mu = k$$

with

$$\Delta_3 = q^2 - 6q^4 + 9q^6 + 4q^8 + 6q^{10} + \dots$$

and the upper bound for the minimum of these lattices is

$$2 + 2\lfloor \frac{n}{12} \rfloor.$$

Note that as in the three cases above, for every term $\Theta_2^i \Delta_{12}^j$, for $j > 0$, has no term in q , therefore, Θ_2 must be Θ_{A_2} so as not to have a term in q in the resulting theta series. The values of n for which 3-modular even extremal lattices exist are from [3, Table 2.4].

n	Θ	name
4	$1 + 12q^2 + 36q^4 + 12q^6 + 84q^8 + O(q^9)$	
6	$1 + 18q^2 + 108q^4 + 234q^6 + 234q^8 + O(q^9)$	
8	$1 + 24q^2 + 216q^4 + 888q^6 + 1752q^8 + O(q^9)$	
10	$1 + 30q^2 + 360q^4 + 2190q^6 + 7230q^8 + O(q^9)$	
12	$1 + 756q^4 + 4032q^6 + 20412q^8 + O(q^9)$	
14	$1 + 756q^4 + 8736q^6 + 44226q^8 + O(q^9)$	
16	$1 + 720q^4 + 13440q^6 + 97200q^8 + O(q^9)$	
18	$1 + 648q^4 + 17712q^6 + 179334q^8 + O(q^9)$	
20	$1 + 540q^4 + 21120q^6 + 286740q^8 + O(q^9)$	
22	$1 + 396q^4 + 23232q^6 + 411642q^8 + O(q^9)$	
24	$1 + 26208q^6 + 530712q^8 + O(q^9)$	
26	$1 + 21840q^6 + 663390q^8 + O(q^9)$	
28	$1 + 17472q^6 + 741636q^8 + O(q^9)$	
30	$1 + 13320q^6 + 765450q^8 + O(q^9)$	
32	$1 + 9600q^6 + 738720q^8 + O(q^9)$	
34	$1 + 6528q^6 + 669222q^8 + O(q^9)$	
36	$1 + 646380q^8 + O(q^9)$	
40	$1 + 360360q^8 + O(q^9)$	
44	$1 + 173844q^8 + O(q^9)$	
48	$1 + 14152320q^{10} + O(q^{11})$	
52	$1 + 7115472q^{10} + O(q^{11})$	
56	$1 + 3193344q^{10} + O(q^{11})$	
60	$1 + 294356160q^{12} + O(q^{13})$	
64	$1 + 138458880q^{12} + O(q^{13})$	
68	$1 + 59324832q^{12} + O(q^{13})$	

The case $l = 2$. From (2), a generic theta series for even 2-modular lattices is

$$\Theta_4^\lambda \Delta_2^\mu, \quad 2\lambda + 8\mu = k$$

with

$$\Delta_2 = q^2 - 8q^4 + 12q^6 + 64q^8 + \dots$$

and the upper bound for the minimum of these lattices is

$$2 + 2\lfloor \frac{n}{16} \rfloor.$$

Note that as above, for every term $\Theta_4^\mu \Delta_2^\lambda$, for $\lambda > 0$, there is no term in q , therefore, Θ_4 must be Θ_{D_4} so as not to have a term in q in the resulting theta series. The values of n for which 2-modular even extremal lattices exist are from [3, Table 2.4]. Extremal theta series are given below.

n	Θ	name
8	$1 + 48q^2 + 624q^4 + 1344q^6 + 5232q^8 + O(q^9)$	D4 + D4
12	$1 + 72q^2 + 1800q^4 + 17568q^6 + 57096q^8 + O(q^9)$	D4+D4+D4
16	$1 + 4320q^4 + 61440q^6 + 522720q^8 + O(q^9)$	BW16
20	$1 + 3960q^4 + 168960q^6 + 2094840q^8 + O(q^9)$	
24	$1 + 3024q^4 + 258048q^6 + 6317136q^8 + O(q^9)$	(C6.PSU(4,3).C2 Y SL(2,3)).C2
28	$1 + 1512q^4 + 301056q^6 + 12484584q^8 + O(q^9)$	E7xD4
32	$1 + 261120q^6 + 18947520q^8 + O(q^9)$	Q32
36	$1 + 164160q^6 + 21976920q^8 + O(q^9)$	
40	$1 + 84480q^6 + 20314800q^8 + O(q^9)$	
44	$1 + 35904q^6 + 15246792q^8 + O(q^9)$	
48	$1 + 9828000q^8 + O(q^9)$	
52	$1 + 5012280q^8 + O(q^9)$	
56	$1 + 2232720q^8 + O(q^9)$	
60	$1 + 867240q^8 + O(q^9)$	
64	$1 + 310210560q^{10} + O(q^{12})$	
68	$1 + 141269184q^{10} + O(q^{12})$	
72	$1 + 57915648q^{10} + O(q^{12})$	
76	$1 + 21373632q^{10} + O(q^{12})$	
80	$1 + 9092160000q^{12} + O(q^{13})$	

3.2. Secrecy Gain of Even l -modular Lattices. We recall from (10) that the secrecy function of a lattice Λ of dimension n is

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

Having computed the theta series of extremal even strongly l -modular lattices in the previous subsection, we can now compute the corresponding secrecy function and secrecy gain (that is the value of the secrecy function at the symmetry point $1/\sqrt{l}$) for all of them. The secrecy function tends to have a typical bell shape, illustrated in Figures 1,3 and in Figures 2,4.

There is no proof or conjecture regarding the actual shape, however all the known examples are in bell shapes. However, when doing numerical computations, one should be aware that truncating the theta series alters a bit the shape on the left-hand side of the graph.

Thus given l , all the secrecy functions are bells centered at $1/\sqrt{l}$ (or $10 \log_{10}(1/\sqrt{l})$ in dB), whose height depends on the dimension n , the larger n , the highest the bell shape. This typical behavior is illustrated in Figures 1 and 3. The secrecy gain for the smallest dimension is 1.17, while it reaches already 26.9 in dimension 48.

The goal of this paper is to investigate the behavior of the secrecy gain as a function of l . In Table 3, all the secrecy gains are listed, per dimension, as a function of l .

We first look at dimensions above 50, for which the only levels available are $l = 1, 2, 3$. The case $l = 1$ was studied in [5], where a lower bound on the secrecy gain of unimodular lattices was computed. It is shown for reference as a line on Figure 5. While the secrecy gains for unimodular lattices are close to the bound, for dimensions larger than 50, clearly 2-modular lattices have higher secrecy gains

FIGURE 1. The secrecy function of 2-modular lattices is shown, as a function of y in dB, for dimensions $n = 8, 12, 16, 20, 24$. When the dimension increases, the secrecy function takes larger values. The fluctuations of the curves on the left-hand side are an artefact of numerical computations, due to the fact that the theta series are cut after q^{20} . The further the theta series is cut, the better the convergence to 1.

FIGURE 2. The secrecy function of 2-modular lattices as shown on Figure 1 is "idealized" on this figure, namely, we removed the fluctuations of the curves on the left-hand side by considering a vertical mirror reflection of the right hand side of the function.

n	l	χ	n	l	χ	n	l	χ
						30	3	6.19485846185629
						30	7	7.45800699280051
			16	3	2.07439466633825	32	3	7.31070898498036
			16	7	2.11146417687778	32	2	7.34311251334145
			16	6	2.13771064516831	32	5	8.67975173139095
4	7	0.934308088166843	16	6	2.14465583503537	32	6	9.24496999294425
4	3	1.03610035533730	16	15	2.18233560402147	32	6	9.24496999294425
4	11	1.05576807829855	16	5	2.18797684818377	32	7	9.68143631704078
6	3	1.05463634502544	16	2	2.20563186526554	34	3	8.69258326273837
6	11	1.12232906165442	16	14	2.20580051821853	34	7	12.4452652369373
6	7	1.16112679066250	16	11	2.36140988370374	36	2	10.0108159932432
8	3	1.07350394633017	18	3	2.34625291308239	36	3	10.6821050127287
8	2	1.17410387776836	18	7	2.59162594961600	36	5	13.0992287248336
8	7	1.24048199122864	18	11	2.71107706714450	36	6	14.4099702909642
8	15	1.25692830085922	20	3	2.68715132688271	36	6	14.4148670699685
8	6	1.26619645091434	20	2	2.81168952543272	40	2	13.8258463013556
8	6	1.26622384361356	20	6	2.81643245399610	40	3	15.4823926077998
8	14	1.28103401682433	20	6	2.82002681754229	40	5	20.0495071395879
8	5	1.29699014311406	20	5	2.84128605481637	40	6	22.8348609921443
8	11	1.30634643555445	20	7	2.99576593981754	40	6	22.8348609921443
10	3	1.09270909183336	20	15	3.02293502788966	44	2	19.2097069187744
10	7	1.34051954155635	20	14	3.03250727662081	44	3	23.2453075611330
10	11	1.43737398939708	22	3	3.12707214224509	44	5	32.0405619805763
12	2	1.27221286690191	22	7	3.51264381322524	44	6	34.9058393072533
12	6	1.48125678418812	24	2	3.69948703753252	44	6	35.0233154488461
12	5	1.54873042901311	24	3	3.93540920240693	48	2	26.9523678766376
12	6	1.55111910381996	24	5	4.06849420320518	48	3	36.3316599878072
12	15	1.63331505155184	24	6	4.10027243329783	52	2	37.3698836775058
12	14	1.65104747837729	24	6	4.10027243329783	52	3	56.2826430705642
12	7	1.66727983818128	24	7	4.43336964412975	56	2	51.9799334818195
12	3	1.66839005589934	26	3	4.54730044219185	56	3	86.6860836582169
12	11	1.71322678377175	26	7	5.29371401574958	60	2	72.4498477070877
14	3	1.85263348496772	28	2	5.10187862601113	60	3	131.017725322748
14	7	1.86571730071328	28	3	5.28879298782093	64	2	101.392259925365
14	11	1.94661200919659	28	5	5.68134297564759	64	3	192.102020627847
			28	6	5.90475746201462	68	2	141.939037487267
			28	6	5.92395522365662	68	3	274.952750535550
			28	7	6.44784540275033	72	2	199.964256599310
						76	2	284.207739663152
						80	2	408.840270452132

TABLE 3. We summarize the value χ_Λ of the secrecy function at the symmetry point of the theta series, as a function of the lattice dimension n , and level l .

FIGURE 3. The secrecy function of 2-modular lattices is shown, as a function of y in dB, for dimensions $n = 32, 36, 40, 44, 48$. When the dimension increases, the secrecy function takes larger values.

FIGURE 4. The secrecy function of 2-modular lattices as shown on Figure 3 is “idealized” on this figure, namely, we removed the fluctuations of the curves on the left-hand side by considering a vertical mirror reflection of the right hand side of the function.

than unimodular, while 3-modular lattices have higher secrecy gains than 2-modular lattices. For lower dimensions, the differences are less clear.

We next look at dimensions between 20 and 50 on Figure 6. To avoid too clustered a figure, we focus on levels $l = 5, 6, 7$ while keeping the case $l = 1$ as a reference. For this range of dimensions, the behavior is also clear: the case $l = 7$

FIGURE 5. Secrecy gains of l -modular lattices for $l = 1, 2, 3$. The curve is a lower bound on the secrecy gain for unimodular lattices. The secrecy gains of unimodular lattices are the closest from the curve. For large dimensions, larger than 50, 3-modular lattices have highest secrecy gains.

FIGURE 6. Secrecy gains of l -modular lattices for $l = 1, 5, 6, 7$. The curve is a lower bound on the secrecy gain for unimodular lattices. For dimensions between 20 and 50, 7-modular lattices have highest secrecy gains, closely.

gives the best gains, closely to the case $l = 6$, and when the dimensions stop for $l = 7$, $l = 6$ gives the best gains.

We then look at small dimensions, up to 20 on Figure 8. The behaviors are pretty close to each other, with still the case $l = 11$ slightly above the other cases.

FIGURE 7. Secrecy gains of l -modular lattices for $l = 1, 2, 3$. The curve is a lower bound on the secrecy gain for unimodular lattices. The secrecy gains of unimodular lattices are the closest from the curve. For large dimensions, larger than 50, 3-modular lattices have highest secrecy gains.

We mentioned in the introduction that evidence so far has shown that extremal lattices, or at least lattices with high minimal norm, tend to have a secrecy gain higher than that of other lattices. We finally compare extremal 11-modular lattices with 11-modular lattices that are not extremal. We consider lattices obtained by taking the direct sum of the 4-dimensional 11-modular lattice, and one 11-modular lattice in dimension 12 with high norm, whose construction is given below, though not the highest. Clearly the extremal lattices have a higher secrecy gain. In fact, the lattices obtained by direct product performs below the lower bound given for unimodular lattices. The choice of a direct product for this comparison is motivated by the fact that this construction is in a sense the "opposite" of extremal lattices: the smallest norm increases as much as possible for extremal lattices, while it remains constant for direct products. We also notice that the 11-modular lattice in dimension 12 with high norm has a high secrecy gain.

3.3. A Lower Bound on the Maximal Secrecy Gain. For a square free l , let $W(l)$ be the elementary abelian 2-group formed by the Atkin-Lehner involutions. By Proposition 4 in [2], it is known that for an even k , and a character χ of $W(l)$ satisfying $\chi(w_l) = (-1)^{k/2}$, Siegel's formula is

$$\mu_{n,l,\chi}^{-1} \sum_{G_n(l,\chi)} |\text{Aut}(\Lambda)|^{-1} \Theta_\Lambda = \left(\sum_{m|l} \chi(w_m) m^{k/2} \right)^{-1} \sum_{m|l} \chi(w_m) m^{k/2} E_k(mz)$$

for $n = 2k$, where $\mu_{n,l,\chi} = \sum_{G_n(l,\chi)} |\text{Aut}(\Lambda)|^{-1}$, E_k denotes the normalized Eisenstein series of weight k for $SL_2(\mathbb{Z})$ and $\sum_{G_n(l,\chi)}$ means a summation over all classes

FIGURE 8. Secrecy gains of 11-modular lattices. The curve is a lower bound on the secrecy gain for unimodular lattices. We compare extremal modular lattices (the upper series of points), with direct sums of the 11-modular lattice of dimension 4.

of lattices of genus $G_n(l, \chi)$. We can equivalently write

$$\sum_{m|l} \chi(w_m) m^{k/2} \sum_{G_n(l, \chi)} |\text{Aut}(\Lambda)|^{-1} \Theta_\Lambda = \sum_{G_n(l, \chi)} |\text{Aut}(\Lambda)|^{-1} \sum_{m|l} \chi(w_m) m^{k/2} E_k(mz).$$

Now set $\Theta_{\min}^{(n)}(e^{-\pi/\sqrt{l}}) = \min \Theta_\Lambda(e^{-\pi/\sqrt{l}})$ where the minimum is understood over all classes of lattices of genus $G_n(l, \chi)$. Then

$$\begin{aligned} & \Theta_{\min}^{(n)}(e^{-\pi/\sqrt{l}}) \sum_{m|l} \chi(w_m) m^{k/2} \sum_{G_n(l, \chi)} |\text{Aut}(\Lambda)|^{-1} \\ & \leq \sum_{m|l} \chi(w_m) m^{k/2} \sum_{G_n(l, \chi)} |\text{Aut}(\Lambda)|^{-1} \Theta_\Lambda(e^{-\pi/\sqrt{l}}) \\ & = \sum_{G_n(l, \chi)} |\text{Aut}(\Lambda)|^{-1} \sum_{m|l} \chi(w_m) m^{k/2} E_k(e^{-m\pi/\sqrt{l}}) \end{aligned}$$

and

$$\Theta_{\min}^{(n)}(e^{-\pi/\sqrt{l}}) \sum_{m|l} \chi(w_m) m^{k/2} \leq \sum_{m|l} \chi(w_m) m^{k/2} E_k(e^{-m\pi/\sqrt{l}}),$$

or equivalently

$$\Theta_{\min}^{(n)}(e^{-\pi/\sqrt{l}}) \leq \frac{\sum_{m|l} \chi(w_m) m^{k/2} E_k(e^{-m\pi/\sqrt{l}})}{\sum_{m|l} \chi(w_m) m^{k/2}}.$$

A lower bound on the maximal secrecy gain is thus given by

$$\frac{\Theta_{\sqrt[l]{l}\mathbb{Z}^n}(\frac{i}{\sqrt{l}})}{\Theta_{\min}^{(n)}(\frac{i}{\sqrt{l}})} = \frac{\vartheta_3(e^{-\pi})^n}{\Theta_{\min}^{(n)}(\frac{i}{\sqrt{l}})}$$

FIGURE 9. Lower bounds on the maximum secrecy gain of unimodular lattices: the dots are the numerically computed values for (11), while the line is an asymptotic lower bound given by $\frac{(1.08)^n}{2}$.

where the numerator $\vartheta_3(e^{-\pi})^n$ is not involved in the optimization, and $\vartheta_3(e^{-\pi}) = \frac{\pi^{1/4}}{\Gamma(3/4)} \simeq 1.086$. The denominator was upper bounded above, yielding

$$\frac{\vartheta_3(e^{-\pi})^n}{\Theta_{\min}^{(n)}(\frac{i}{\sqrt{l}})} \geq \vartheta_3(e^{-\pi})^n \frac{\sum_{m|l} \chi(w_m) m^{k/2}}{\sum_{m|l} \chi(w_m) m^{k/2} E_k(e^{-m\pi/\sqrt{l}})}.$$

This simplifies to

$$(11) \quad \frac{\vartheta_3(e^{-\pi})^n}{E_k(e^{-\pi})}$$

for the unimodular case ($l = 1$), as computed in [5], where it was further shown that asymptotically, when n grows, this lower bound tends to $\frac{(1.08)^n}{2}$. Figure 9 compares the lower bound (used as benchmark in previous figures) with numerically computed values for (11).

For the case where $l = p$ is prime, we get

$$\frac{\vartheta_3(e^{-\pi})^n}{\Theta_{\min}^{(n)}(\frac{i}{\sqrt{l}})} \geq \vartheta_3(e^{-\pi})^n \frac{\chi(w_1) + \chi(w_p) p^{k/2}}{\chi(w_1) E_k(e^{-\pi/\sqrt{p}}) + \chi(w_p) p^{k/2} E_k(e^{-\sqrt{p}\pi})}.$$

Since $\chi(w_1) = 1$ (w_1 is the identity element in $W(p)$) and $\chi(w_p) = (-1)^{k/2}$, we need to distinguish $k \equiv 0 \pmod{4}$, and the lower bound becomes

$$\begin{cases} \vartheta_3(e^{-\pi})^n \frac{1+p^{k/2}}{E_k(e^{-\pi/\sqrt{p}}) + p^{k/2} E_k(e^{-\sqrt{p}\pi})} & k \equiv 0 \pmod{4} \\ \vartheta_3(e^{-\pi})^n \frac{1-p^{k/2}}{E_k(e^{-\pi/\sqrt{p}}) - p^{k/2} E_k(e^{-\sqrt{p}\pi})} & k \equiv 2 \pmod{4} \end{cases}$$

Figure 10 shows the above lower bounds for $l = 2$. The two lines correspond to the two cases, $k \equiv 0 \pmod{4}$ and $k \equiv 2 \pmod{4}$. The dots are the values of the secrecy gain for $l = 2$. We observe that the two lines for the two cases of k are close to each

FIGURE 10. Lower bounds on the maximal secrecy gain for $l = 2$: the two lines correspond to the two cases for k , $k \equiv 0 \pmod{4}$ and $k \equiv 2 \pmod{4}$. The dots are the secrecy gain values.

other, and close to the known secrecy gain values. Figure 11 shows the behavior for $l = 3$: the two cases of k give lines close to each other, below the known secrecy gain values. This is a bit unexpected, since for $l = 1, 2$, the known constructions are not better than the bounds. We then compare the different lower bounds. Figure 12 illustrates the lower bounds for $l = 1, 2, 3$. We observe no significant difference between the lower bound for $l = 1$, and for $l = 2, l = 3$. All of them are hard to distinguish until dimension 60, after which the case $l = 3$ gives a slightly better bound. There is no notable different behavior for other values of prime l , namely the bounds cannot be visually distinguished (the numerical values differ in digits after the decimal point).

We next consider the case $l = pq$, for $p \neq q$ two primes, which for us comprises $l = 6, 14, 15$. For $k \equiv 0 \pmod{4}$, a character χ such that $\chi(w_{pq}) = (-1)^{k/2} = 1$ means that χ could be either the trivial character, or such that $\chi(w_p) = \chi(w_q) = -1$. For $k \equiv 2 \pmod{4}$, a character χ such that $\chi(w_{pq}) = (-1)^{k/2} = -1$ means that χ either satisfies $\chi(w_p) = 1, \chi(w_q) = -1$, or $\chi(w_p) = -1, \chi(w_q) = 1$. Figure 13 shows the case $l = 6$. There are two lines, one for each case of k , and for each of them, the line itself was calculated based on one character, while the dots are coming from the other character. This shows that the difference between one character and another is hardly distinguishable.

Finally we compare the lower bounds for $l = 6$ with those for $l = 1, 2$ in Figure 14. They are hardly distinguishable from those for $l = 2$. The same observations hold for $l = 14, 15$: there is hardly any difference between the choice of a character or another, and their corresponding bound can only be differentiated from that of $l = 2$ by looking at digits after the decimal point.

3.4. An 11-modular Lattice of Dimension $n = 12$. Consider the field extension $L = \mathbb{Q}(\sqrt{-11}, \sqrt{5}, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}$, where ζ_7 is a primitive 7th root of unity, whose integral basis is the compositum of the integral basis of K and of $\{1, \zeta_7 + \zeta_7^{-1}, (\zeta_7 +$

FIGURE 11. Lower bounds on the maximal secrecy gain for $l = 3$: the two lines correspond to the two cases for k , $k \equiv 0 \pmod{4}$ and $k \equiv 2 \pmod{4}$. The dots are the secrecy gain values.

FIGURE 12. Lower bounds on the maximal secrecy gain: comparison among $l = 1, l = 2, l = 3$. All cases are very close to each other.

$\zeta_7^{-1})^2\}$. Let $\mathfrak{p}_5, \mathfrak{p}_7$ be primes above 5 and 7 in L . The ideal lattice $\Lambda_{\mathfrak{p}_5\mathfrak{p}_7}$ obtained by embedding $\mathfrak{p}_5\mathfrak{p}_7$, whose generator matrix is scaled by $1/\sqrt{35}$, is an 11-modular

FIGURE 13. The case $l = 6$: for each line corresponding to a case of k , the line itself is calculated based on one character, while the dots are coming from the other character. The dots without line are the known secrecy gain values.

FIGURE 14. Lower bounds on the maximal secrecy gain for $l = 1, 2, 6$. The case $l = 1$ gives the lowest lower bound, $l = 2, 6$ give lower bounds very close to each other.

lattice, whose smallest vector has length 6. A Gram matrix is

$$\begin{bmatrix} 6 & -2 & -2 & 2 & 2 & 0 & -2 & 0 & -2 & 1 & -2 & 0 \\ -2 & 6 & 2 & 0 & 2 & 2 & 2 & 2 & 3 & 2 & 2 & 0 \\ -2 & 2 & 6 & 2 & -2 & 2 & 3 & -2 & 0 & 2 & 0 & -2 \\ 2 & 0 & 2 & 6 & -2 & 2 & 2 & -2 & -2 & 2 & -2 & 1 \\ 2 & 2 & -2 & -2 & 8 & 2 & -2 & 4 & 1 & -1 & -1 & -1 \\ 0 & 2 & 2 & 2 & 2 & 6 & 0 & 1 & -1 & 0 & -2 & -2 \\ -2 & 2 & 3 & 2 & -2 & 0 & 6 & -2 & 0 & 0 & 0 & -1 \\ 0 & 2 & -2 & -2 & 4 & 1 & -2 & 6 & 3 & 0 & 2 & 0 \\ -2 & 3 & 0 & -2 & 1 & -1 & 0 & 3 & 6 & 0 & 2 & 0 \\ 1 & 2 & 2 & 2 & -1 & 0 & 0 & 0 & 0 & 6 & 2 & 2 \\ -2 & 2 & 0 & -2 & -1 & -2 & 0 & 2 & 2 & 2 & 6 & 2 \\ 0 & 0 & -2 & 1 & -1 & -2 & -1 & 0 & 0 & 2 & 2 & 6 \end{bmatrix}.$$

n	l	χ	
4	11	1.05576807829855	QQF.4.b
6	7	1.16112679066250	A(6)2
8	11	1.30634643555445	8QF.8.a
10	11	1.43737398939708	A10(3)
12	11	1.71322678377175	
14	11	1.94661200919659	
16	11	2.36140988370374	
18	11	2.71107706714450	
20	14	3.03250727662081	
22	7	3.51264381322524	
24	7	4.43336964412975	
26	7	5.29371401574958	
28	7	6.44784540275033	
30	7	7.45800699280051	
32	7	9.68143631704078	
34	7	12.4452652369373	
36	6	14.4148670699685	
40	6	22.8348609921443	
44	6	35.0233154488461	
48	3	36.3316599878072	
52	3	56.2826430705642	
56	3	86.6860836582169	
60	3	131.017725322748	
64	3	192.102020627847	
68	3	274.952750535550	
72	2	199.964256599310	
76	2	284.207739663152	
80	2	408.840270452132	

TABLE 4. We summarize the best value χ_A of the secrecy function at the symmetry point of the theta series, as a function of the lattice dimension n , and level l .

Table 4 summarizes the best secrecy gains found, and the corresponding lattices as per Table [14].

We note that the construction of the 4-dimensional 11-modular lattice QQF.4.b can be obtained as an algebraic lattice. Consider the field extension $K = \mathbb{Q}(\sqrt{-11}, \sqrt{5})/\mathbb{Q}$, whose integral basis is the compositum of $\{1, \frac{1+\sqrt{-11}}{2}\}$ and $\{1, \frac{\sqrt{5}}{2}\}$. Let $\mathfrak{p}_5$ be a prime above 5 in K . The ideal lattice $\Lambda_{\mathfrak{p}_5}$ obtained by embedding $\mathfrak{p}_5$, whose generator matrix is scaled by $1/\sqrt{5}$, is an 11-modular lattice, whose smallest vector has length 4. A Gram matrix is

$$\begin{bmatrix} 4 & 2 & 0 & 1 \\ 2 & 4 & -1 & 0 \\ 0 & -1 & 4 & 2 \\ 1 & 0 & 2 & 4 \end{bmatrix}.$$

The construction of these extremal lattices is left open. For coding purposes, it would also be interesting to obtain them via Construction A. The study of the lower bound on the maximal secrecy gain further suggests to investigate other classes of lattices than extremal lattices, that would give a secrecy gain significantly higher than the lower bound. A possible hint could be to look at kissing numbers, as pinpointed in [6] for unimodular lattices.

4. ACKNOWLEDGMENTS

Part of this work was done while F. Oggier was visiting the Huawei France Research Center, whose hospitality is gratefully acknowledged. We also would like to thank the anonymous reviewer whose suggestions enriched this paper.

REFERENCES

- [1] H.-G. Quebbemann, "Modular Lattices in Euclidean Spaces", *Journal of Number Theory*, 54, 1995.
- [2] H.-G. Quebbemann, "Atkin-Lehner eigenforms and strongly modular lattices", *L'Enseign. Math.*, 43, 1997.
- [3] R. Scharlau, R. Schulze-Pillot, "Extremal Lattices", *Algorithmic Algebra and Number Theory* (Heidelberg, 1997), Springer, Berlin, 1999.
- [4] E.M. Rains and N.J.A. Sloane, "The Shadow Theory of Modular and Unimodular Lattices, *Journal of Number Theory*, Vol. 73 (1998), pp. 359-389.
- [5] F. Oggier, J.-C. Belfiore, and P. Solé, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis", *IEEE Trans. on Information Theory*, vol. 62, no. 10, Oct. 2016.
- [6] F. Lin, F. Oggier, "A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions", *IEEE Trans. Inf. Theory*, vol. 59, no. 6, June 2013.
- [7] F. Lin, F. Oggier, "Gaussian Wiretap Lattice Codes from Binary Self-dual Codes", *IEEE Information Theory Workshop 2012*, Lausanne.
- [8] J. Pinchak, "Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé Secrecy Function Conjecture", *IEEE International Symposium on Information Theory 2013*, Istanbul.
- [9] F. Lin, F. Oggier and P. Solé, "2- and 3-modular Lattice Wiretap Codes in Small Dimensions," *Applicable Algebra in Engineering, Communication and Computing*, 25:571, 2015
- [10] X. Hou, F. Lin, F. Oggier, "Construction and Secrecy Gain of a Family of 5-modular Lattices," *IEEE Information Theory Workshop (ITW) 2014*, Hobart, Tasmania, Australia.
- [11] X. Hou, F. Oggier, "Modular Lattices from a Variation of Construction A over Number Fields," *Advances in Mathematics of Communication*, 11 (4): 719-745, 2017, <https://www.arxiv.org/abs/1604.01583>.
- [12] SageMath, the Sage Mathematics Software System (Version 7.3), The Sage Developers, <http://www.sagemath.org>.
- [13] J. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups", 3rd edition, *Springer*, 1999.
- [14] <http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/modular.html>
- [15] A.-M. Ernvall-Hytönen, "On a Conjecture by Belfiore and Solé on some Lattices", *IEEE Trans. Inf. Theory*, vol. 58, no. 9, September 2012.
- [16] G.L. Nipp, "Quaternary Quadratic Forms", Springer Verlag, 1991.
- [17] J. Pinchak, B.A. Sethuraman, "The Belfiore-Solé Conjecture and a Certain Technique for Verifying it for a Given lattice", *Information Theory and Applications 2014*.
- [18] A.-M. Ernvall-Hytönen, B. A. Sethuraman, "Counterexample to the Generalized Belfiore-Solé Secrecy Function Conjecture for l -modular lattices", *International Symposium on Information Theory*, Hong Kong, 2015.

DIVISION OF MATHEMATICAL SCIENCES, NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE
E-mail address: **frederique@ntu.edu.sg**

TELECOM PARISTECH, DEPT OF COMMUNICATIONS AND ELECTRONICS, 46, RUE BARRAULT
75634 PARIS CEDEX 13 FRANCE, AND HUAWEI MATHEMATICAL AND ALGORITHMIC SCIENCES
LAB, 20 QUAI DU POINT DU JOUR, 92100 BOULOGNE-BILLANCOURT, FRANCE
E-mail address: **belfiore@enst.fr**