Construction and secrecy gain of a family of 5-modular lattices

Hou, Xiaolu; Lin, Fuchun; Oggier, Frédérique

2014

Hou, X., Lin, F., & Oggier, F. (2014). Construction and secrecy gain of a family of 5-modular lattices. 2014 IEEE Information Theory Workshop (ITW), 117-121.

<https://hdl.handle.net/10356/100072>

<https://doi.org/10.1109/ITW.2014.6970804>

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/ITW.2014.6970804>].

Downloaded on 26 Apr 2023 22:46:16 SGT

Construction and Secrecy Gain of a Family of 5-modular Lattices

Xiaolu Hou

Division of Mathematical Sciences
Nanyang Technological University
Singapore

Email: HO0001LU@e.ntu.edu.sg

Fuchun Lin

Dept. of Electrical and Electronic Engineering
Imperial College London
London SW7 2AZ, United Kingdom

Email: linf0007@e.ntu.edu.sg

Frédérique Oggier

Division of Mathematical Sciences
Nanyang Technological University
Singapore

Email: frederique@ntu.edu.sg

Abstract—The secrecy gain of a lattice is a lattice invariant used to characterize wiretap lattice codes for Gaussian channels. The secrecy gain has been classified for unimodular lattices up to dimension 23, and so far, a few sparse examples are known for l -modular lattices, with $l = 2, 3$. We propose some constructions of 5-modular lattices via the Construction A of lattices from linear codes, and study the secrecy gain of the resulting lattices.

I. INTRODUCTION

We consider the problem of designing lattice wiretap codes for the Gaussian wiretap channel, a Gaussian broadcast channel where Alice sends a message to Bob in the presence of an eavesdropper Eve. The transmitted message $\mathbf{x} \in \mathbb{R}^n$ is a lattice codeword, where by a lattice Λ we mean a discrete set of vectors in $\mathbb{R}^n$, which can be described by $\Lambda = \{\mathbf{u}M | \mathbf{u} \in \mathbb{Z}^n\}$, where the generator matrix M contains a basis of $\mathbb{R}^n$. Lattice encoding for the Gaussian wiretap channel is done via a generic coset coding strategy: let $\Lambda_e \subset \Lambda_b$ be two nested lattices. The message Alice intends to Bob is mapped to a particular coset in Λ_b/Λ_e , from which a vector is randomly chosen as the encoded word [1]. The lattice Λ_e is interpreted as introducing confusion for Eve, while Λ_b as ensuring reliability for Bob. Two lattice design criteria have been recently proposed to characterise the confusion created by Λ_e , the *secrecy gain* [1], and the *flatness factor* [2], which turn out to be related [3]. Both rely on the theta series of the lattice Λ_e .

Definition 1. Let $\mathcal{H} = \{a + ib \in \mathbb{C} | b > 0\}$ denote the upper half complex plane and set $q = e^{\pi i \tau}$, $\tau \in \mathcal{H}$. The theta series of a lattice Λ is defined by

$$\Theta_{\Lambda}(\tau) = \sum_{\mathbf{t} \in \Lambda} q^{||\mathbf{t}||^2},$$

where $||\mathbf{t}||^2 = \mathbf{t} \cdot \mathbf{t}$ is the norm of a lattice vector.

We will focus on the secrecy gain.

Definition 2. [1] Let Λ be an n -dimensional lattice. The secrecy function of Λ is given by

$$\Xi_{\Lambda}(\tau) = \frac{\Theta_{\sqrt{\text{vol}(\Lambda)}\mathbb{Z}^n}(\tau)}{\Theta_{\Lambda}(\tau)}, \tau = yi, y > 0, \quad (1)$$

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.

The higher the secrecy gain of a lattice, the more confusion this lattice, as a wiretap code, is expected to create at an eavesdropper. This motivated the study of the secrecy gain as a lattice invariant, focusing on l -modular lattices, and lattices constructed from linear codes (which may or may not be l -modular). The notion of modularity relies on the relation between a lattice and its dual.

Definition 3. If $\Lambda \subset \mathbb{R}^n$ is a lattice, then its dual lattice Λ^* is by definition $\{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \lambda \in \mathbb{Z}, \forall \lambda \in \Lambda\}$.

Definition 4. A lattice Λ is said to be an integral lattice if $\Lambda \subset \Lambda^*$. If the norm is even for any lattice vector, then Λ is called an even lattice. Otherwise, it is called an odd lattice.

A lattice Λ is said to be equivalent to another lattice Λ' if $\tau(\Lambda') = \Lambda$ for τ a similarity map, possibly including a rotation, reflection and change of scale.

An integral lattice that is equivalent to its dual is called a modular lattice. In particular, let $\tau(\Lambda^*) = \Lambda$ and $\ell = \frac{||\tau(\mathbf{u})||^2}{||\mathbf{u}||^2}$ for all $\mathbf{u} \in \Lambda^*$. Then Λ is called an ℓ -modular lattice.

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 [1]. The secrecy gain of unimodular lattices (i.e., $\ell = 1$) up to dimension 23 is classified [4], some examples of 2- and 3- modular lattices are known to give a better secrecy gain than unimodular lattices [5], but no conclusion has been reached yet, as to which class of lattices provides the best secrecy gain. Asymptotic results on the weak secrecy gain are only available for even unimodular lattices: their weak secrecy gain goes to infinity as the dimension n grows [1]. As for the secrecy gain conjecture, a technique to verify its correctness for a specific unimodular lattice is known [6], which justifies the secrecy gains of unimodular lattices computed so far. Recently, the proof of this technique was improved and more examples of unimodular lattices constructed from binary codes were shown to satisfy the secrecy gain conjecture [7], [8].

An open question is the impact of the choice of l on the secrecy gain, namely whether considering l -modular lattices where l increases will tend to increase or decrease the secrecy gain. To start addressing this question, we consider the secrecy

gain of 5-modular lattices, for which we need to obtain constructions of 5-modular lattices whose theta series can be computed. In Section II, we present a systematic construction of 5-modular lattices from the number field $\mathbb{Q}(\sqrt{5})$, which we use to build higher dimensional 5-modular lattices via the classical Construction A from linear codes in Section III. The corresponding weak secrecy gains are computed in Section IV, which turn out to be generally better than that of unimodular lattices, though there are instances of 2- or 3- modular lattices [9] with better gains [5].

II. A 2-DIMENSIONAL 5-MODULAR LATTICE

Consider the quadratic field $K = \mathbb{Q}(\sqrt{5})$, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, integral basis $\{1, \frac{1+\sqrt{5}}{2}\}$ and Galois group $\{\sigma_1, \sigma_2\}$, where σ_1 is the identity, and $\sigma_2 : a + b\sqrt{5} \mapsto a - b\sqrt{5}$. Let $\Lambda(\mathcal{O}_K)$ be the lattice given by the generator matrix

$$M = \begin{bmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \quad (2)$$

that is basis vectors are $\mathbf{v}_1 = (1, 1)$ and $\mathbf{v}_2 = (\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2})$, and $\Lambda(\mathcal{O}_K)$ is formed by linear integral combinations of $\mathbf{v}_1$ and $\mathbf{v}_2$. The corresponding Gram matrix G is by definition

$$G = MM^T = \begin{bmatrix} \text{Tr}(1) & \text{Tr}(\frac{1+\sqrt{5}}{2}) \\ \text{Tr}(\frac{1+\sqrt{5}}{2}) & \text{Tr}(\frac{(1+\sqrt{5})^2}{4}) \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}. \quad (3)$$

In other words, $\Lambda(\mathcal{O}_K)$ is obtained from $\mathcal{O}_K$ endowed with the bilinear form $\text{Tr} : (x, y) \mapsto \text{Tr}(xy) = \sigma_1(xy) + \sigma_2(xy)$.

Remark 1. Note that the generator matrix M is not unique, and a change of basis, that is $M' = UM$ for U an integral matrix with determinant ± 1 , will give the same lattice.

Let $\mathbf{u}_1, \mathbf{u}_2$ be the rows of $(M^T)^{-1}$, the inverse of M^T , with M in (2). Since $(M^T)^{-1}M^T$ is the identity matrix, $\mathbf{u}_i \cdot \mathbf{v}_j = \delta_{i,j}$, $i, j = 1, 2$ where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise. Take now $\mathbf{y}$ an arbitrary lattice point in $\Lambda(\mathcal{O}_K)^*$, the dual lattice of $\Lambda(\mathcal{O}_K)$:

$$\mathbf{y} = \mathbf{y}M^T(M^T)^{-1} = \sum_{i=1}^2 (\mathbf{y}\mathbf{v}_i)\mathbf{u}_i$$

where $\mathbf{y}\mathbf{v}_i \in \mathbb{Z}$ since y belongs to the dual lattice, showing that $\mathbf{y}$ is a $\mathbb{Z}$ -linear combination of $\mathbf{u}_1, \mathbf{u}_2$, which forms a $\mathbb{Z}$ -basis of $\Lambda(\mathcal{O}_K)^*$. A generator matrix for the dual lattice is then $(M^T)^{-1}$ (which is true in general, and in fact, the same proof recalled here for the sake of completeness holds), which is computed as follows:

$$(MM^T)^{-1} = \frac{1}{5} \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} \Rightarrow (M^T)^{-1} = \frac{1}{5} \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} M.$$

Thus

$$(M^T)^{-1} = \frac{1}{5} \begin{bmatrix} 3v_1 - v_2 \\ -v_1 + 2v_2 \end{bmatrix},$$

and after a change of basis (recall Remark 1)

$$M^* = \frac{1}{5} \begin{bmatrix} -v_1 + 2v_2 \\ -3v_1 + v_2 \end{bmatrix} = \frac{1}{5} \begin{bmatrix} \sqrt{5} & -\sqrt{5} \\ \frac{-5+\sqrt{5}}{2} & \frac{-5-\sqrt{5}}{2} \end{bmatrix}$$

is a generator matrix of the dual lattice.

With the above notations, we conclude:

Lemma 1. *The lattice $\Lambda(\mathcal{O}_K)$ is 5-modular.*

Proof: A Gram matrix of the dual lattice is

$$M^*(M^*)^T = \frac{1}{5} \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} = \frac{1}{5} MM^T$$

thus the similarity τ which scales (the generator matrix of) Λ^* by $\sqrt{5}$ satisfies $5 = \frac{\|\tau(\mathbf{u})\|^2}{\|\mathbf{u}\|^2}$. ■

III. 5-MODULAR LATTICES FROM CONSTRUCTION A

As above, we take $K = \mathbb{Q}(\sqrt{5})$ with ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Consider the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$, for p a prime in $\mathbb{Z}$ which is inert, i.e., $p\mathcal{O}_K = (p)$ and denote by $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2}$) the finite field with p elements (resp. p^2 elements). Recall ([11], pp 91) that a prime p is inert in K if and only if $x^2 - 5$ has no solution modulo p , if and only if 5 is a quadratic non-residue modulo p . By the reciprocity law

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right),$$

and p is inert in K if and only if $p \equiv 2, 3 \pmod{5}$.

Define the map ρ of reduction componentwise modulo $p\mathcal{O}_K$, $p \equiv 2, 3 \pmod{5}$ that is

$$\begin{aligned} \rho : \mathbb{Z}[\frac{1+\sqrt{5}}{2}]^N &\rightarrow \mathbb{F}_{p^2}^N, \\ (x_1, \dots, x_N) &\mapsto (x_1 \bmod p\mathcal{O}_K, \dots, x_N \bmod p\mathcal{O}_K) \end{aligned}$$

for N some positive integer. Let C be a linear (N, k) code (that is, of length N and dimension k) over $\mathbb{F}_{p^2}$. Then $\rho^{-1}(C)$ is a lattice of dimension N over $\mathcal{O}_K$, with corresponding bilinear form

$$(x, y) \mapsto \sum_{i=1}^N \text{Tr}(x_i y_i),$$

that is, a lattice of dimension $2N$ as a $\mathbb{Z}$ -lattice. This way of obtaining a lattice by lifting a linear code is broadly referred to as *Construction A* [10].

Proposition 1. *A generator matrix of $\rho^{-1}(C)$ is*

$$M_C = \begin{bmatrix} I_k \otimes M & A \tilde{\otimes} M \\ \mathbf{0}_{2N-2k, 2k} & I_{N-k} \otimes pM \end{bmatrix} \quad (4)$$

with M as in (2), A such that $(I_k \ (A \bmod p\mathcal{O}_K))$ is a generator matrix of C , and denoting the columns of M (resp. A) by M_i , $i = 1, 2$ (resp. A_i , $i = 1, \dots, N-k$), $A \tilde{\otimes} M = [\sigma_1(A_1) \otimes M_1, \sigma_2(A_1) \otimes M_2, \dots, \sigma_1(A_{N-k}) \otimes M_1, \sigma_2(A_{N-k}) \otimes M_2]$, where σ_2 is applied componentwise.

Proof: We first show that the lattice generated by M_C has the same volume as $\rho^{-1}(C)$:

$$\begin{aligned} \det(M_C M_C^T) &= \det(I_k \otimes M)^2 \det(I_{N-k} \otimes pM)^2 \\ &= 5^k \det(pM)^{2(N-k)} = 5^k p^{4(N-k)} 5^{N-k} \end{aligned}$$

that is the lattice generated by M_C has volume

$$|\det(M_C)| = \sqrt{\det(M_C M_C^T)} = (5^N p^{4(N-k)})^{1/2}. \quad (5)$$

Now the bilinear form $(x, y) \mapsto \text{Tr}(xy)$, $x, y \in \mathcal{O}_K$ has determinant 5 over $\mathcal{O}_K$ since $5 = \det(MM^T)$, implying that the bilinear form $(x, y) \mapsto \sum_{i=1}^N \text{Tr}(x_i y_i)$ has determinant 5^N over $\mathcal{O}_K^N$. The map ρ of reduction mod (p) is surjective, and $\rho^{-1}(C)$ is of index $p^{2(N-k)}$, therefore the volume of $\rho^{-1}(C)$ is $(5^N p^{4(N-k)})^{\frac{1}{2}}$ and both lattices have the same volume. It is furthermore clear from the shape of the generator matrix M_C that the lattice it generates has the right rank.

We are left to show that lattice points are indeed mapped to codewords in C by ρ . Let us write $u_i = (u_{i1}, u_{i2}) \in \mathbb{Z}^2$, then $x_i = u_{i1} + u_{i2} \frac{1+\sqrt{5}}{2}$, $i = 1, \dots, N$ is an element in $\mathcal{O}_K$, and define $\sigma = (\sigma_1, \sigma_2) : \mathcal{O}_K \hookrightarrow \mathbb{R}^2$ to be the canonical embedding of K . We have

$$\sigma_1(x_i) = u_{i1}M_1, \quad \sigma_2(x_i) = u_{i2}M_2$$

and a lattice point $\mathbf{x} = [u_1, \dots, u_N]M_C$ is explicitly given by

$$[u_1, \dots, u_k, \dots, u_N] \begin{bmatrix} I_k \otimes M & A\tilde{\otimes}M \\ \mathbf{0}_{2N-2k, 2k} & I_{N-k} \otimes pM \end{bmatrix} = [\sigma(x_1), \dots, \sigma(x_k), \sigma(\sum_{j=1}^k a_{j1}x_j + x'_{k+1}), \dots, \sigma(\sum_{j=1}^k a_{j, N-k}x_j + x'_N)],$$

where $x'_{k+1}, \dots, x'_N$ are in the ideal (p) . Define $\psi : \sigma(x_i) \mapsto x_i \in \mathcal{O}_K$, then since x'_i reduces to zero mod (p) , we have

$$\psi(\mathbf{x}) = (\psi(\sigma(x_1)), \dots, \psi(\sigma(\sum_{j=1}^k a_{j1}x_j + x'_{k+1})), \dots),$$

and $\rho\psi(\mathbf{x})$ is indeed a codeword of C :

$$\begin{aligned} \rho\psi(\mathbf{x}) &= (x_1 \bmod(p), \dots, \sum_{j=1}^k a_{j1}x_j + x'_{k+1} \bmod(p), \dots) \\ &= (x_1 \bmod(p), \dots, x_k \bmod(p)) \cdot (I_k \ A \bmod(p)) \end{aligned}$$

Definition 5. A linear (N, k) code is said to be self-orthogonal if $C \subset C^\perp$.

Lemma 2. The Gram matrix $G_C = M_C M_C^T$ for $(x, y) \mapsto \sum_{i=1}^N \text{Tr}(x_i y_i)$ is

$$G_C = \begin{bmatrix} \text{Tr}((I + AA^T) \otimes M_1 M_1^T) & p \text{Tr}(A \otimes M_1 M_1^T) \\ p \text{Tr}(A \otimes M_1 M_1^T)^T & I_k \otimes p^2 M M^T \end{bmatrix} \quad (6)$$

where $\text{Tr} = \text{Tr}_{K/\mathbb{Q}}$ is taken componentwise. Suppose furthermore that C is self-orthogonal. The lattice $\rho^{-1}(C)$ with $(x, y) \mapsto \frac{1}{p} \sum_{i=1}^N \text{Tr}(x_i y_i)$ is then integral.

Proof: For M_C in (4), a direct computation gives

$$\begin{bmatrix} I_k \otimes M M^T + (A\tilde{\otimes}M)(A\tilde{\otimes}M)^T & (A\tilde{\otimes}M)(I_{N-k} \otimes pM^T) \\ (I_{N-k} \otimes pM)(A\tilde{\otimes}M)^T & I_{N-k} \otimes p^2 M M^T \end{bmatrix}$$

for G_C , where, using that $M_2 = \sigma_2(M_1)$

$$\begin{aligned} (A\tilde{\otimes}M)(A\tilde{\otimes}M)^T &= \text{Tr}(AA^T \otimes M_1 M_1^T) \\ I_k \otimes M M^T &= \text{Tr}(I_k \otimes M_1 M_1^T) \end{aligned}$$

thus showing that

$$I_k \otimes M M^T + (A\tilde{\otimes}M)(A\tilde{\otimes}M)^T = \text{Tr}((I_k + AA^T) \otimes M_1 M_1^T).$$

Moreover,

$$\begin{aligned} &(A\tilde{\otimes}M)(I_{N-k} \otimes M^T) \\ &= \begin{bmatrix} a_{11}M_1 & \dots & \sigma_2(a_{1k})M_2 \\ \vdots & & \vdots \\ a_{N-k,1}M_1 & \dots & \sigma_2(a_{N-k, N-k})M_2 \end{bmatrix} \begin{bmatrix} M_1^T & 0 & \dots & 0 \\ M_2^T & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_1^T \\ 0 & 0 & \dots & M_2^T \end{bmatrix} \\ &= (A \otimes M_1 M_1^T) + \sigma_2(A \otimes M_1 M_1^T) \\ &= \text{Tr}(A \otimes M_1 M_1^T), \end{aligned}$$

An equivalent definition of integral lattice is that its Gram matrix has integral coefficients, which is the case. Indeed, MM^T has integral coefficients, A has coefficients in $\mathcal{O}_K$, thus $\text{Tr}(A \otimes M_1 M_1^T)$ has integral coefficients. Finally, as C is self-orthogonal and $(I_k \ A \bmod(p))$ is a generator matrix for C , $I_k + AA^T \equiv 0 \bmod(p)$. Hence $(I_k + AA^T) \otimes M_1 M_1^T \in (p)$ and $\text{Tr}((I_k + AA^T) \otimes M_1 M_1^T) \in p\mathbb{Z}$. ■

Definition 6. A linear (N, k) code is said to be self-dual if $C = C^\perp$.

Proposition 2. Let C be a self-dual code. The lattice $\rho^{-1}(C)$ with bilinear form $(x, y) \mapsto \frac{1}{p} \sum_{i=1}^N \text{Tr}(x_i y_i)$ is 5-modular.

Proof: From (4), a generator matrix for the dual of $\rho^{-1}(C)$ with respect to the bilinear form $(x, y) \mapsto \frac{1}{p} \sum_{i=1}^N \text{Tr}(x_i y_i)$ is $(M_C^T)^{-1}$. This can be computed using Schur complement:

$$\begin{aligned} &\sqrt{p} \begin{bmatrix} I_k \otimes M^* & \mathbf{0} \\ -\frac{1}{p}(I_k \otimes M^*)(A\tilde{\otimes}M)^T(I_k \otimes M^*) & \frac{1}{p}I_k \otimes M^* \end{bmatrix} \\ &= \frac{1}{\sqrt{p}} \begin{bmatrix} I_k \otimes pM^* & \mathbf{0} \\ -(I_k \otimes M^*)(A\tilde{\otimes}M)^T(I_k \otimes M^*) & I_k \otimes M^* \end{bmatrix} \end{aligned}$$

By a change of basis, we get that the generator matrix M_C^* is

$$\begin{aligned} &\frac{1}{\sqrt{p}} \begin{bmatrix} -(I_k \otimes M^*)(A\tilde{\otimes}M)^T(I_k \otimes M^*) & I_k \otimes M^* \\ I_k \otimes pM^* & \mathbf{0} \end{bmatrix} \\ &= \frac{1}{\sqrt{5p}} \begin{bmatrix} -\sqrt{5}(I_k \otimes M^*)(A\tilde{\otimes}M)^T(I_k \otimes M^*) & I_k \otimes M^* \\ I_k \otimes pM & \mathbf{0} \end{bmatrix}. \end{aligned}$$

Since

$$\frac{1}{\sqrt{p}} \begin{bmatrix} -A^T \tilde{\otimes} M & I_k \otimes M^* \\ I_k \otimes pM & \mathbf{0} \end{bmatrix}$$

can be seen to be another generator matrix for $\rho^{-1}(C)$, it suffices now to prove $\sqrt{5}(I_k \otimes M^*)(A\tilde{\otimes}M)^T(I_k \otimes M^*) = A^T \tilde{\otimes} M$, which is equivalent to

$$\begin{aligned} &(I_k \otimes M)(A\tilde{\otimes}M)^T(I_k \otimes M^*) = A^T \tilde{\otimes} M \\ \iff &(I_k \otimes M)(A\tilde{\otimes}M)^T = (A^T \tilde{\otimes} M)(I_k \otimes M^T) \\ \iff &(A\tilde{\otimes}M)(I_k \otimes M^T) = (I_k \otimes M)(A^T \tilde{\otimes} M)^T \\ \iff &\text{Tr}(A \otimes M_1 M_1^T) = (I_k \otimes M)(A^T \tilde{\otimes} M)^T \end{aligned}$$

which can be checked by direct computations. ■

A. A Family of 4-dimensional 5-modular Lattices

Choose C to be a self-dual code of length $N = 2$ over $\mathbb{F}_{p^2}$, with generator matrix $(1 \ a)$, with a an integer mod p . Then C is self-dual if and only if $a^2 + 1 = 0 \pmod{p}$. Thus there exists such a code C over $\mathbb{F}_{p^2}$ if and only if -1 is a quadratic residue mod $p \iff p \equiv 1 \pmod{4}$ or $p = 2$. The above discussion yields a family a 4-dimensional 5-modular lattices.

Corollary 1. *Let p be a prime such that $p \equiv 13, 17 \pmod{20}$ or $p = 2$, and a be a square root of -1 modulo p . Then the code $C \subseteq \mathbb{F}_{p^2}$ generated by $(1 \ a)$ is self-dual, and the lattice $\rho^{-1}(C)$ with the bilinear form $(x, y) \mapsto \frac{1}{p} \sum_{i=1}^N \text{Tr}(x_i y_i)$ is a 5-modular lattice.*

The generator matrices of $\rho^{-1}(C)$ (resp. its dual) are

$$M_C = \frac{1}{\sqrt{p}} \begin{bmatrix} 1 & a \\ 0 & p \end{bmatrix} \otimes M, \quad M_C^* = \frac{1}{\sqrt{p}} \begin{bmatrix} a & -1 \\ p & 0 \end{bmatrix} \otimes M^*.$$

Example 1. Take $p = 2$ and consider the $(2, 1)$ repetition code C over $\mathbb{F}_4$. Then $\rho^{-1}(C)$ is a 5-modular lattice of dimension 4 with bilinear form $(x, y) \mapsto \frac{1}{2} \sum_{i=1}^2 \text{Tr}(x_i y_i)$, and generator matrix

$$M_C = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \otimes M.$$

B. Higher dimensional Constructions for $p = 2$

We provide a few higher dimensional constructions of 5-modular lattices from self-dual codes over $\mathbb{F}_4$.

Example 2. Let $p = 2$, ω be the root of the polynomial $x^2 + x + 1$ over $\mathbb{F}_2$, then $\mathbb{F}_4 \cong \mathbb{F}_2(\omega)$. Consider the self-dual code $C = \langle (1 \ \omega \ \omega + 1 \ 0), (1 \ 1 \ 1 \ 1) \rangle$. We have

$$(I_2 \ A \pmod{(2)}) = \begin{pmatrix} 1 & 0 & \omega & \omega + 1 \\ 0 & 1 & \omega + 1 & \omega \end{pmatrix}.$$

as a generator matrix for C . Lift $A \pmod{(2)}$ to

$$A = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{\sqrt{5}+3}{2} \\ \frac{\sqrt{5}+3}{2} & \frac{1+\sqrt{5}}{2} \end{pmatrix}$$

Then $\rho^{-1}(C)$ with $(x, y) \mapsto \frac{1}{2} \sum_{i=1}^2 \text{Tr}(x_i y_i)$ is a 5-modular lattice of dimension 8 with generator matrix

$$M_C = \frac{1}{\sqrt{2}} \begin{bmatrix} I_2 \otimes M & A \tilde{\otimes} M \\ \mathbf{0}_{4,4} & I_2 \otimes 2M \end{bmatrix}$$

for M as in (2) and

$$A \tilde{\otimes} M = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} & \frac{3+\sqrt{5}}{2} & \frac{3-\sqrt{5}}{2} \\ \frac{3+\sqrt{5}}{2} & \frac{3-\sqrt{5}}{2} & 2+\sqrt{5} & 2-\sqrt{5} \\ \frac{3+\sqrt{5}}{2} & \frac{3-\sqrt{5}}{2} & \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 2+\sqrt{5} & 2-\sqrt{5} & \frac{3+\sqrt{5}}{2} & \frac{3-\sqrt{5}}{2} \end{pmatrix}.$$

Example 3. Consider the self-dual code $C \subset \mathbb{F}_4^6$ with generator matrix

$$(I_3 \ A \pmod{(2)}) = \begin{pmatrix} 1 & 0 & 0 & \omega + 1 & \omega + 1 & 1 \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & 0 & \omega + 1 & \omega \end{pmatrix}$$

The matrix A is obtained from $A \pmod{(2)}$ by lifting ω to $\frac{1+\sqrt{5}}{2}$. Then $\rho^{-1}(C)$ with the bilinear form $(x, y) \mapsto \frac{1}{2} \sum_{i=1}^6 \text{Tr}(x_i y_i)$ is a lattice of dimension 12.

Example 4. Consider the self-dual code $C \subset \mathbb{F}_4^{12}$ with generator matrix $(I_6 \ A \pmod{(2)})$ with

$$A \pmod{(2)} = \begin{pmatrix} 1 & \omega^2 & 1 & 1 & \omega & 1 \\ \omega & 0 & 1 & \omega^2 & \omega & \omega^2 \\ \omega & \omega^2 & \omega & \omega^2 & 0 & 1 \\ 0 & \omega & \omega^2 & \omega & \omega^2 & 1 \\ \omega^2 & \omega & 1 & 0 & \omega^2 & \omega \\ \omega^2 & 1 & 1 & \omega & 1 & 1 \end{pmatrix}$$

Lift $A \pmod{(2)}$, using that ω is lifted to $\frac{1+\sqrt{5}}{2}$ and hence ω^2 is lifted to $\frac{3+\sqrt{5}}{2}$. Then $\rho^{-1}(C)$ with the bilinear form $(x, y) \mapsto \frac{1}{2} \sum_{i=1}^{12} \text{Tr}(x_i y_i)$, is a lattice of rank dimension 24.

IV. THE SECRECY GAIN OF 5-MODULAR LATTICES

From Definition (1), the secrecy gain of a lattice Λ is the maximum of the secrecy function

$$\Xi_\Lambda(\tau) = \frac{\Theta_{\sqrt{\text{vol}(\Lambda)}\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \tau = yi, \ y > 0.$$

To compute it, the theta series of Λ must be known. For an integral lattice, the norm of any lattice vector is an integer, and the theta series from Definition 1 becomes $\Theta_\Lambda(\tau) = \sum_{m=0}^\infty A_m q^m$, where A_m is the number of lattice vectors with norm m . We will need the following Jacobi's theta functions to represent the theta series computed:

$$\vartheta_3(\tau) = \sum_{m \in \mathbb{Z}} q^{m^2}, \vartheta_2(\tau) = \sum_{m \in \mathbb{Z}} q^{(m+\frac{1}{2})^2}.$$

We start by computing the theta series of the lattice $\Lambda(\mathcal{O}_K)$:

$$\begin{aligned} \Theta_{\Lambda(\mathcal{O}_K)}(\tau) &= \sum_{x \in \mathcal{O}_K} q^{\text{Tr}(x^2)} \\ &= \sum_{a,b \in \mathbb{Z}} q^{2a^2 + 2ab + 3b^2} \\ &= \sum_{a,b \in \mathbb{Z}} q^{2(a+\frac{b}{2})^2 + \frac{5}{2}b^2} \\ &= \sum_{a,b_1 \in \mathbb{Z}} q^{2(a+b_1)^2 + 10b_1^2} + \\ &\quad \sum_{a,b_1 \in \mathbb{Z}} q^{2(a+b_1+\frac{1}{2})^2 + 10(b_1+\frac{1}{2})^2} \\ &= \vartheta_3(2\tau)\vartheta_3(10\tau) + \vartheta_2(2\tau)\vartheta_2(10\tau). \end{aligned}$$

We move on to the theta series of 5-modular lattices constructed from self-dual codes over $\mathbb{F}_4$. When we take $p = 2$, the quotient ring is $\mathcal{O}_K/2\mathcal{O}_K = \{\bar{0}, \bar{1}, \frac{1+\sqrt{5}}{2}, \frac{-1+\sqrt{5}}{2}\}$, and

$$\begin{aligned} \theta_0(\tau) &= \sum_{x \in \bar{0}} q^{\frac{1}{2}\text{Tr}(x^2)}, \theta_1(\tau) = \sum_{x \in \bar{1}} q^{\frac{1}{2}\text{Tr}(x^2)} \\ \theta_2(\tau) &= \sum_{x \in \frac{1+\sqrt{5}}{2}} q^{\frac{1}{2}\text{Tr}(x^2)} = \sum_{x \in \frac{-1+\sqrt{5}}{2}} q^{\frac{1}{2}\text{Tr}(x^2)}. \end{aligned}$$

$\theta_0(\tau)$ is a simple substitution

$$\theta_0(\tau) = \vartheta_3(4\tau)\vartheta_3(20\tau) + \vartheta_2(4\tau)\vartheta_2(20\tau),$$

while $\theta_1(\tau)$ follows from a similar argument

$$\begin{aligned} \theta_1(\tau) &= \sum_{x \in 1+2\mathcal{O}_K} q^{\frac{1}{2}\text{Tr}(x^2)} \\ &= \sum_{a,b \in \mathbb{Z}} q^{2(2(a+\frac{1}{2})^2 + 2(a+\frac{1}{2})b + 3b^2)} \\ &= \vartheta_3(4\tau)\vartheta_2(20\tau) + \vartheta_2(4\tau)\vartheta_3(20\tau). \end{aligned}$$

Fig. 1. The secrecy function of the lattice of Example 3: the symmetry point at $y = -3.49485$ dB = $\frac{1}{\sqrt{5}}$ corresponds to the weak secrecy gain.

$\theta_2(\tau)$ asks for more work:

$$\begin{aligned}\theta_2(\tau) &= \sum_{x \in \frac{1+\sqrt{5}}{2} + 2\mathcal{O}_{c_K}} q^{\frac{1}{2}\text{Tr}(x^2)} \\ &= \sum_{a,b \in \mathbb{Z}} q^{2(2a^2 + 2a(b + \frac{1}{2}) + 3(b + \frac{1}{2})^2)} \\ &= \sum_{a,b \in \mathbb{Z}} q^{2(2(a+b_1 + \frac{1}{4})^2 + 10(b_1 + \frac{1}{4})^2)} + \\ &\quad \sum_{a,b \in \mathbb{Z}} q^{2(2(a+b_1 + \frac{3}{4})^2 + 10(b_1 + \frac{3}{4})^2)},\end{aligned}$$

which involves sum types like $\sum_{m \in \mathbb{Z}} q^{(m + \frac{1}{4})^2}$ and $\sum_{m \in \mathbb{Z}} q^{(m + \frac{3}{4})^2}$. We first observe that

$$\Theta_{4\mathbb{Z}+1}(\tau) = \Theta_{4\mathbb{Z}+3}(\tau). \quad (7)$$

On the other hand, a decomposition of $\mathbb{Z}$ gives

$$\Theta_{\mathbb{Z}}(\tau) = \Theta_{4\mathbb{Z}}(\tau) + \Theta_{4\mathbb{Z}+1}(\tau) + \Theta_{4\mathbb{Z}+2}(\tau) + \Theta_{4\mathbb{Z}+3}(\tau). \quad (8)$$

(7) and (8) yield

$$\begin{aligned}\theta_{\frac{1}{4}}(\tau) &\triangleq \sum_{m \in \mathbb{Z}} q^{(m + \frac{1}{4})^2} = \sum_{m \in \mathbb{Z}} q^{(m + \frac{3}{4})^2} \\ &= \frac{1}{2} (\vartheta_3(\frac{1}{16}\tau) - \vartheta_3(\tau) - \vartheta_2(\tau))\end{aligned}$$

and $\theta_2(\tau) = 2\theta_{\frac{1}{4}}(4\tau)\theta_{\frac{1}{4}}(20\tau)$. The length weight of a code-word $\mathbf{c}$ over $\mathbb{F}_4$ is a triple (n_0, n_1, n_2) that counts the number of components equal to, respectively, 0, 1 and w or w^2 .

Lemma 3. Let $\text{lwe}_C(x, y, z)$ be the length weight enumerator of a linear code over $\mathbb{F}_4$. Then

$$\Theta_{\rho^{-1}(C)}(\tau) = \text{lwe}_C(\theta_0, \theta_1, \theta_2).$$

Proof: The theta series $\Theta_{\rho^{-1}(C)}(\tau)$ is given by

$$\begin{aligned}&= \sum_{\lambda \in \rho^{-1}(C)} q^{||\lambda||^2} = \sum_{\mathbf{c} \in C} \sum_{\mathbf{x} \in \mathbf{c} + 2\mathcal{O}_{\frac{N}{K}}} q^{\frac{1}{2}\text{Tr}(\mathbf{x} \cdot \mathbf{x})} \\ &= \sum_{\mathbf{c} \in C} \theta_0^{n_0(\mathbf{c})} \theta_1^{n_1(\mathbf{c})} \theta_2^{n_2(\mathbf{c})} = \text{lwe}_C(\theta_0, \theta_1, \theta_2).\end{aligned}$$

We next compute the length weight enumerator of C for the proposed constructions, and their corresponding theta series. For Example 1, $\text{Wt}_C(x, y, z) = x^2 + y^2 + 2z^2$, and

$$\Theta_{\rho^{-1}(C)}(\tau) = \theta_0^2 + \theta_1^2 + 2\theta_2^2 = 1 + 4q^2 + 8q^3 + 4q^4 + \dots$$

For Example 2, $\text{Wt}_C(x, y, z) = x^4 + y^4 + 2z^4 + 12xyz^2$, and

$$\Theta_{\rho^{-1}(C)}(\tau) = \theta_0^4 + \theta_1^4 + 2\theta_2^4 + 12\theta_0\theta_1\theta_2^2 = 1 + 120q^4 + 240q^6 + \dots$$

dim	Λ	χ_Λ^w	$l=1$	$l=2$	$l=3$
2	$\Lambda(\mathcal{O}_K)$	1.00049	1		1.01789
4	$\rho^{-1}((1 \ a))$	1.00099	1	1.08356	
8	Example 2	1.29699	1.33333		
12	Example 3	1.60475	1.60000		1.66839
24	Example 4	3.76168	4.06349		

TABLE I

KNOWN SECRECY GAINS IN SMALL DIMENSIONS, FOR UNIMODULAR LATTICES ($l=1$), 2-MODULAR LATTICES ($l=2$, FOR THE LATTICE D_4), AND 3-MODULAR LATTICES ($l=3$, FOR THE LATTICES A_2 AND K_{12}).

For Example 3, its secrecy function is shown in Fig. 1, and

$$\begin{aligned}\text{Wt}_C(x, y, z) &= x^6 + y^6 + 2z^6 + 6x^3yz^2 + 18x^2y^2z^2 \\ &\quad + 9x^2z^4 + 6xy^3z^2 + 12xyz^4 + 9y^2z^4, \\ \Theta_{\rho^{-1}(C)}(\tau) &= 1 + 60q^4 + 288q^5 + 520q^6 + \dots\end{aligned}$$

The theta series of the lattice in Example 4 is computed through a method based on modular form theory [5], [12]:

$$\begin{aligned}\Theta_{\rho^{-1}(C)}(\tau) &= f_1(\tau)^{12} - 24f_1(\tau)^{12}f_2(\tau) + 216f_1(\tau)^{12}f_2(\tau)^2 \\ &\quad - 944f_1(\tau)^{12}f_2(\tau)^3 + 2160f_1(\tau)^{12}f_2(\tau)^4 - 2688f_1(\tau)^{12}f_2(\tau)^5 \\ &\quad + 1376f_1(\tau)^{12}f_2(\tau)^6 - 3840f_1(\tau)^{12}f_2(\tau)^7 \\ &\quad + 6144f_1(\tau)^{12}f_2(\tau)^8 - 4096f_1(\tau)^{12}f_2(\tau)^9 \\ &= 1 + 24q^4 + 48q^6 + 38280q^8 + 237600q^{10} + 2296320q^{12} \\ &\quad + 12108144q^{14} + \dots\end{aligned}$$

where $f_1(\tau) = \vartheta_3(\tau)\vartheta_3(5\tau)$ and $f_2(\tau) = \left(\frac{\eta(\frac{\tau}{5})\eta(\frac{5\tau}{2})\eta(2\tau)\eta(10\tau)}{\eta(\tau)\eta(5\tau)}\right)^{\frac{8}{5}}$, for $\eta(\tau) = q^{\frac{1}{24}} \prod_{m=1}^{\infty} (1 - q^{2m})$.

Corresponding secrecy gains are reported in Table I, compared to known constructions.

ACKNOWLEDGEMENT

The work is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07. The research of X. Hou is partially supported by a Nanyang President Graduate Scholarship.

REFERENCES

- [1] F. Oggier, J.-C. Belfiore, and P. Solé, "Lattice Coding for the Wiretap Gaussian Channel", <http://arXiv:1103.4086v1> [cs.IT], 21 Mar 2011.
- [2] C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehlé, "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel", <http://arxiv.org/abs/1210.6673>.
- [3] F. Lin, C. Ling, J.-C. Belfiore, "Secrecy gain, flatness factor, and secrecy-goodness of even unimodular lattices", *IEEE International Symposium on Information Theory 2014*, Hawaii.
- [4] F. Lin, F. Oggier, "A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions", *IEEE Trans. Inf. Theory*, vol. 59, no. 6, June 2013.
- [5] F. Lin, F. Oggier and P. Solé, "2- and 3-modular Lattice Wiretap Codes in Small Dimensions," <http://arXiv:1304.4440> [math.NT].
- [6] A.-M. Ernvall-Hytönen, "On a Conjecture by Belfiore and Solé on some Lattices", *IEEE Trans. Inf. Theory*, vol. 58, no. 9, September 2012.
- [7] J. Pinchak, "Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé Secrecy Function Conjecture", *IEEE International Symposium on Information Theory 2013*, Istanbul.
- [8] 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*, available at <http://ita.ucsd.edu/workshop/14/>.
- [9] P. Gaborit, A. M. Natividad, P. Solé, "Eisenstein Lattices, Galois Rings and Quaternary Codes", *Int. J. of Number Theory*, vol. 2, no. 2, 2006.
- [10] J. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups", 3rd edition, *Springer*, 1999.
- [11] G. Everest, T. Ward, *An Introduction to Number Theory*, Graduate Texts in Mathematics. Springer-Verlag, London, 2005.

- [12] E.M. Rains and N.J.A. Sloane, "The Shadow Theory of Modular and Unimodular Lattices," J. Number Theory, 73 (1998), 359-389.