On the Design of Physical Layer Security Schemes Based on Lattices

Hassan Khodaiemehr

Department of Mathematics, K. N. Toosi University of Technology
School of Mathematics, Institute for Research in Fundamental Sciences (IPM)

Shahid Beheshti University, 2019. Tehran, Iran

Outline

1. Introduction
   - Physical layer security
   - Wiretap channels
   - Lattices and Their Applications

Outline

Outline

1. Introduction
   - Physical layer security
   - Wiretap channels
   - Lattices and Their Applications
2. Preliminaries
   - Algebraic Number Theory
   - Lattices in Algebraic Number Theory
3. Lattice Construction using Codes
   - Construction A Lattices

Outline

1. Introduction
   - Physical layer security
   - Wiretap channels
   - Lattices and Their Applications
2. Preliminaries
   - Algebraic Number Theory
   - Lattices in Algebraic Number Theory
3. Lattice Construction using Codes
   - Construction A Lattices
4. Secrecy gain of modular lattices

Outline

Outline

Outline

Physical layer security

- In modern wireless communications secrecy plays an ever increasing role.

Physical layer security

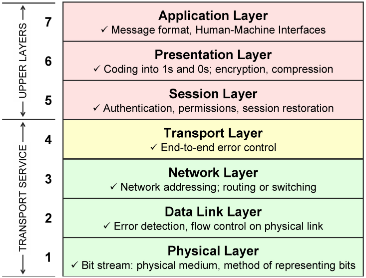
- Inherent openness in the wireless communications channel causes two types of attacks: eavesdropping and jamming.

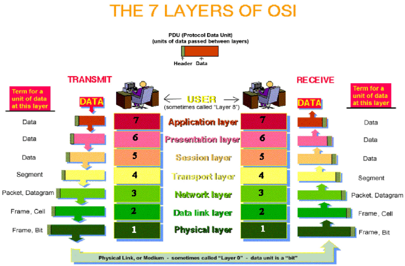
Physical layer security

- What is the Physical Layer?

Physical layer security

- The lowest layer of the 7-layer OSI protocol stack.





Physical layer security

Current state-of-the-art security techniques:

Physical layer security

1) **Cryptography**, is at higher layers of network and based on limited computational power at the adversary.

Physical layer security

1) **Cryptography**, is at higher layers of network and based on limited computational power at the adversary.

- It includes two types of algorithms: secret-key encryption and public-key encryption algorithms.

Physical layer security

1) **Cryptography**, is at higher layers of network and based on limited computational power at the adversary.

- It includes two types of algorithms: secret-key encryption and public-key encryption algorithms.
- Secret-key algorithms are computationally efficient, while have challenges for key management.

Physical layer security

1) **Cryptography**, is at higher layers of network and based on limited computational power at the adversary.

- It includes two types of algorithms: secret-key encryption and public-key encryption algorithms.
- Secret-key algorithms are computationally efficient, while have challenges for key management.
- Public-key algorithms are simple in terms of key management, but require considerable computational resources.

Physical layer security

1) **Cryptography**, is at higher layers of network and based on limited computational power at the adversary.

- It includes two types of algorithms: secret-key encryption and public-key encryption algorithms.
- Secret-key algorithms are computationally efficient, while have challenges for key management.
- Public-key algorithms are simple in terms of key management, but require considerable computational resources.
- Hence, hybrid cryptosystems are employed in practice.

Physical layer security

Several disadvantages:

Physical layer security

Several disadvantages:

1. Using public-key algorithms to distribute secret keys adds complexity in the design of networks,

Physical layer security

Several disadvantages:

1. Using public-key algorithms to distribute secret keys adds complexity in the design of networks,
2. Public-key algorithms are not provably perfectly secure and are vulnerable to the so-called man-in-the-middle attack.

Physical layer security

2) **Spread spectrum**, e.g., frequency hopping and CDMA:

Physical layer security

2) **Spread spectrum**, e.g., frequency hopping and CDMA:

- At the physical layer,

Physical layer security

2) **Spread spectrum**, e.g., frequency hopping and CDMA:

- At the physical layer,
- Based on limited knowledge at the adversary.

Physical layer security

3) **Physical layer security:**

Physical layer security

3) **Physical layer security:**

- At the physical layer,

Physical layer security

3) **Physical layer security:**

- At the physical layer,
- No assumption on adversary's computational power,

Physical layer security

3) **Physical layer security:**

- At the physical layer,
- No assumption on adversary's computational power,
- No assumption on adversary's available information,

Physical layer security

3) **Physical layer security:**

- At the physical layer,
- No assumption on adversary's computational power,
- No assumption on adversary's available information,
- Provable and quantifiable(in bits/sec/hertz),

Physical layer security

3) **Physical layer security:**

- At the physical layer,
- No assumption on adversary's computational power,
- No assumption on adversary's available information,
- Provable and quantifiable(in bits/sec/hertz),
- Implementable using signal processing and coding techniques.

Outline

Wiretap channels

- Wiretap channels were introduced by Aaron D. Wyner already in 1975

Wiretap channels

- Wiretap channels were introduced by Aaron D. Wyner already in 1975
- It assumes Bob's signal-to-noise ratio (SNR) is sufficiently large compared to Eve's SNR.

Wiretap channels

- Wiretap channels were introduced by Aaron D. Wyner already in 1975
- It assumes Bob's signal-to-noise ratio (SNR) is sufficiently large compared to Eve's SNR.
- Wyner introduced coset coding strategy in order to confuse Eve. In coset coding, random bits are transmitted in addition to the data bits.

Wiretap channels

- Wiretap channels were introduced by Aaron D. Wyner already in 1975
- It assumes Bob's signal-to-noise ratio (SNR) is sufficiently large compared to Eve's SNR.
- Wyner introduced coset coding strategy in order to confuse Eve. In coset coding, random bits are transmitted in addition to the data bits.
- Due to the SNR assumption, Bob can retrieve the data bits with high probability, while Alice is only able to retrieve the random bits.

Wiretap channels

- Assume Alice and Bob are discussing over a table in a noisy restaurant, and Eve is eavesdropping in a table located far enough not to hear the essential contents of the conversation.

Wiretap channels

- Assume Alice and Bob are discussing over a table in a noisy restaurant, and Eve is eavesdropping in a table located far enough not to hear the essential contents of the conversation.
- Random bits could be thought of as Alice yelling something irrelevant (Eve hears this), and data bits are whispered just loud enough so that Bob can hear.

Wiretap channels

- Assume Alice and Bob are discussing over a table in a noisy restaurant, and Eve is eavesdropping in a table located far enough not to hear the essential contents of the conversation.
- Random bits could be thought of as Alice yelling something irrelevant (Eve hears this), and data bits are whispered just loud enough so that Bob can hear.
- We assume Alice is using a lattice code for coset coding.

Wiretap channels

- Assume Alice and Bob are discussing over a table in a noisy restaurant, and Eve is eavesdropping in a table located far enough not to hear the essential contents of the conversation.
- Random bits could be thought of as Alice yelling something irrelevant (Eve hears this), and data bits are whispered just loud enough so that Bob can hear.
- We assume Alice is using a lattice code for coset coding.
- The finer lattice intended to Bob is denoted by Λ_b (whispering), and the coarse lattice is denoted by Λ_e (yelling).

Outline

Lattices

- A lattice Λ is a discrete subgroup of rank m in the real m-dimensional space $\mathbb{R}^m$.

Lattices

- A lattice Λ is a discrete subgroup of rank m in the real m-dimensional space $\mathbb{R}^m$.
- Every lattice Λ has a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$.

Lattices

- A lattice Λ is a discrete subgroup of rank m in the real m-dimensional space $\mathbb{R}^m$.
- Every lattice Λ has a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$.
- The matrix $\mathbf{M}$ with $\mathbf{b}_1, \ldots, \mathbf{b}_n$ as rows is a generator matrix for the lattice.

Lattices

- A lattice Λ is a discrete subgroup of rank m in the real m-dimensional space $\mathbb{R}^m$.
- Every lattice Λ has a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$.
- The matrix $\mathbf{M}$ with $\mathbf{b}_1, \ldots, \mathbf{b}_n$ as rows is a generator matrix for the lattice.
- The matrix $\mathbf{G} = \mathbf{M}\mathbf{M}^t$ is called a Gram matrix for the lattice.

Lattices

- A lattice Λ is a discrete subgroup of rank m in the real m-dimensional space $\mathbb{R}^m$.
- Every lattice Λ has a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$.
- The matrix $\mathbf{M}$ with $\mathbf{b}_1, \ldots, \mathbf{b}_n$ as rows is a generator matrix for the lattice.
- The matrix $\mathbf{G} = \mathbf{M}\mathbf{M}^t$ is called a Gram matrix for the lattice.
- A lattice Λ in $\mathbb{R}^m$ is an integral lattice if and only if its Gram matrix has coefficients in $\mathbb{Z}$.

Coset encoding in Gaussian wiretap channels

- We consider a Gaussian wiretap channel, that is, a broadcast channel. This channel is modeled by

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

where x is the transmitted signal, v_b and v_e denote the Gaussian noise at Bob and Eve's side, respectively, both with zero mean, and respective variance σ_b^2 and σ_e^2. Eve has a poor $\mathtt{SNR}$, in particular with respect to Bob, that is $\sigma_b^2 \ll \sigma_e^2$.

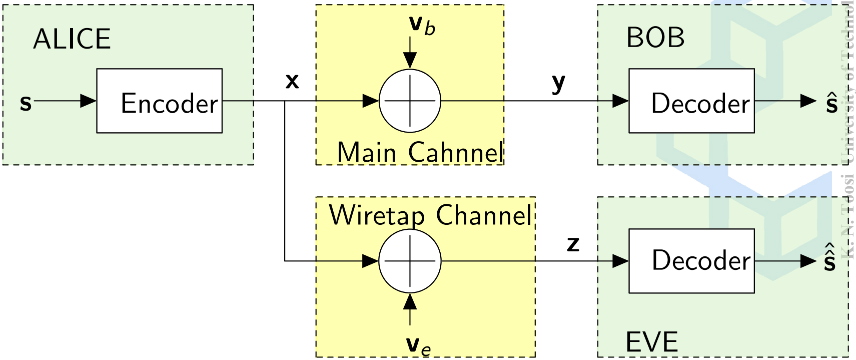
Coset encoding in Gaussian wiretap channels

- Alice's encoder maps l bits $s_1, \ldots, s_l$ to a codeword $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{R}^n$. Over a transmission of n symbols, we get

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + \mathbf{v}_b, \\ \mathbf{z} &= \mathbf{x} + \mathbf{v}_e, \end{aligned} \tag{1}$$

$\mathbf{v}_b$ and $\mathbf{v}_e$ are Gaussian noise vectors at Bob and Eve's side, respectively, with zero mean, and variance σ_b^2 and σ_e^2 and $\sigma_b^2 \ll \sigma_e^2$. We consider the case where Alice uses lattice codes, namely $\mathbf{x} \in \Lambda_b$, where Λ_b is an n-dimensional real lattice intended to the legitimate receiver Bob.

Coset encoding in Gaussian wiretap channels



Coset encoding in Gaussian wiretap channels

- In coset coding, we map **s** to a coset. Then, the point to be actually transmitted is chosen randomly inside that coset. Consequently, k bits ($k \leq l$) of **s** carry the information, and $l - k$ bits, the randomness.

Coset encoding in Gaussian wiretap channels

- We partition the lattice Λ_b into a union of disjoint cosets of the form $\Lambda_e + \mathbf{c}$, with $\Lambda_e \subset \Lambda_b$ and $\left|\frac{\Lambda_b}{\Lambda_e}\right| = 2^k = \frac{\mathrm{vol}(\mathcal{V}(\Lambda_e))}{\mathrm{vol}(\mathcal{V}(\Lambda_b))}$, and $\mathbf{c}$ an n-dimensional vector. We need 2^k cosets to be labeled by the information vector $\mathbf{s}_d \in \{0,1\}^k$:

$$\Lambda_b = \bigcup_{j=1}^{2^k} (\Lambda_e + \mathbf{c}_j)\,. \tag{2}$$

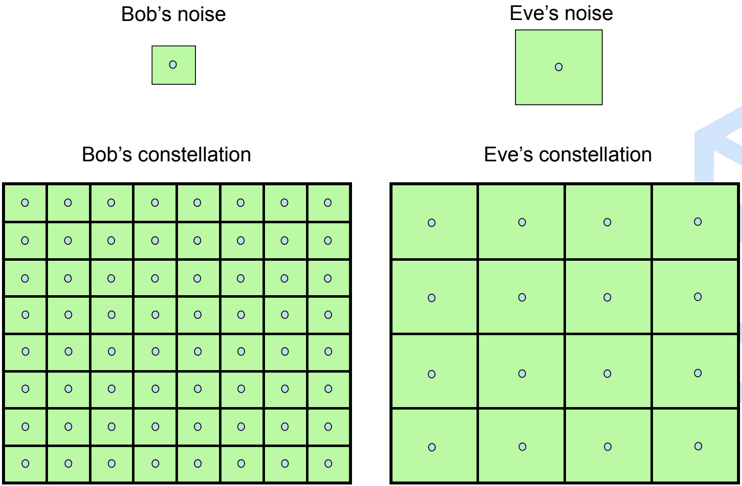
Coset encoding in Gaussian wiretap channels

- Once the following mapping is done

$$\mathbf{s}_d \mapsto \Lambda_e + \mathbf{c}_{j(\mathbf{s}_d)}, \tag{2}$$

the coset encoding means that a random vector $\mathbf{r} \in \Lambda_e$ is chosen and the transmitted lattice point $\mathbf{x} \in \Lambda_b$ is

$$\mathbf{x} = \mathbf{r} + \mathbf{c}_{j(\mathbf{s}_d)} \in \Lambda_e + \mathbf{c}_{j(\mathbf{s}_d)}. \tag{3}$$

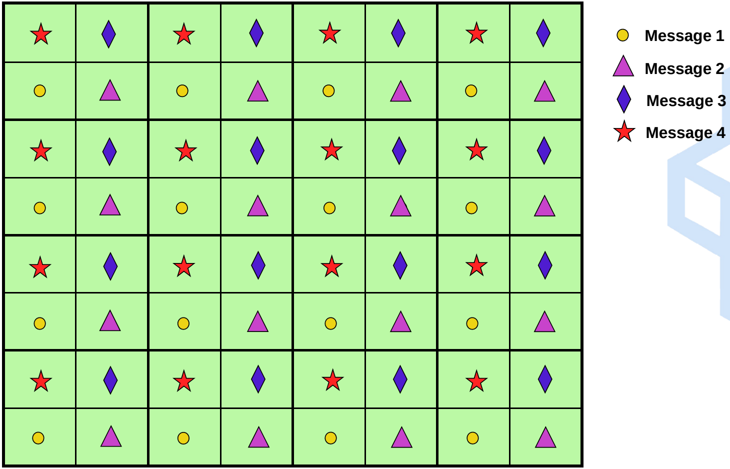


$C_B = \log_2 64 = 6$ b/s

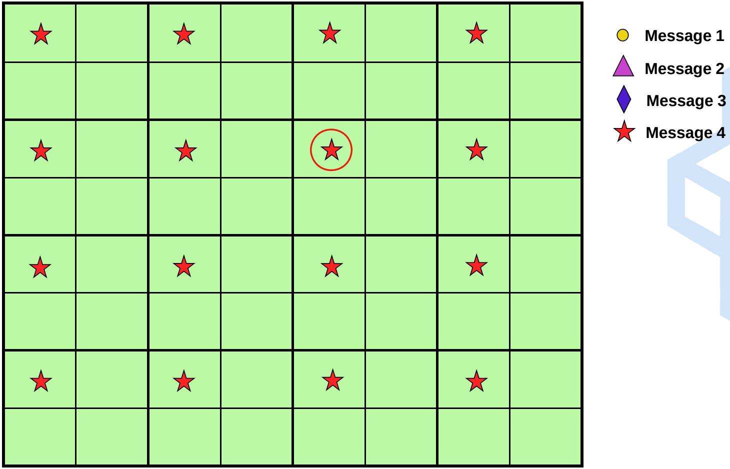
$C_E = \log_2 16 = 4$ b/s

$C_s = C_B - C_E = 2$ b/s

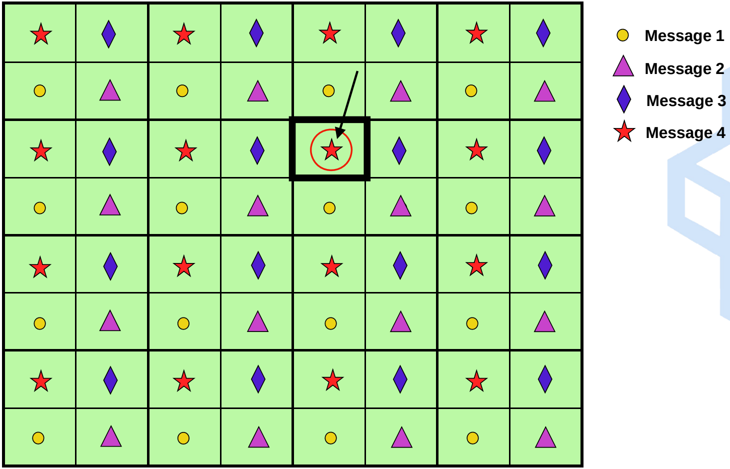
Divide Bob's constellation into 4 subsets.



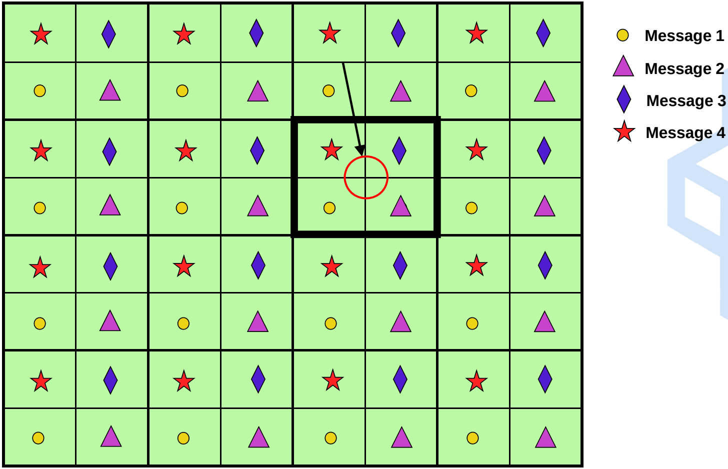
All red stars denote the same message. Pick one randomly.



Bob can decode the message reliably.



For Eve, all 4 messages are equally-likely.



Design of good wiretap codes

- Considering the wiretap channel where Alice transmits lattice codewords from an n-dimensional lattice Λ_b, we get that the probabilities $P_{c,b}$ and $P_{c,e}$, which are the correct decision probabilities for Bob and Eve, respectively, as follows

$$P_{c,b} \approx \frac{1}{(\sigma_b\sqrt{2\pi})^n} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}\|^2/2\sigma_b^2} d\mathbf{u}. \tag{4}$$

$$P_{c,e} \approx \frac{1}{(\sigma_e\sqrt{2\pi})^n} \mathrm{vol}(\mathcal{V}(\Lambda_b)) \sum_{\mathbf{r}\in\Lambda_e} e^{-\|\mathbf{u}\|^2/2\sigma_e^2}. \tag{5}$$

Design of good wiretap codes

- Considering the wiretap channel where Alice transmits lattice codewords from an n-dimensional lattice Λ_b, we get that the probabilities $P_{c,b}$ and $P_{c,e}$, which are the correct decision probabilities for Bob and Eve, respectively, as follows

$$P_{c,b} \approx \frac{1}{(\sigma_b\sqrt{2\pi})^n} \int_{\mathcal{V}(\Lambda_b)} e^{-\|\mathbf{u}\|^2/2\sigma_b^2} d\mathbf{u}. \tag{4}$$

$$P_{c,e} \approx \frac{1}{(\sigma_e\sqrt{2\pi})^n} \mathrm{vol}(\mathcal{V}(\Lambda_b)) \sum_{\mathbf{r}\in\Lambda_e} e^{-\|\mathbf{u}\|^2/2\sigma_e^2}. \tag{5}$$

- In order to minimize the probability $P_{c,e}$, while keeping $P_{c,b}$ unchanged, we should find a lattice Λ_b which is as good as possible for the Gaussian channel, its sublattice Λ_e minimizes $\sum_{\mathbf{r}\in\Lambda_e} e^{-\|\mathbf{u}\|^2/2\sigma_e^2}$ and $\log_2 |\Lambda_b/\Lambda_e| = k$.

Secrecy gain

- Two lattice design criteria have been recently proposed to characterize the confusion created by Λ_e: the **secrecy gain**, and the **flatness factor**.
- The secrecy gain originally captures the loss in Eve's probability of correctly decoding when Λ_e is used instead of $\mathbb{Z}^n$.
- Both the flatness factor and the secrecy gain involve the theta series of Λ_e at a particular point.

Secrecy gain

Definition

Let $\mathcal{H} = \{a + ib \in \mathbb{C} \mid b > 0\}$ 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

$$\Theta_\Lambda(\tau) = \sum_{\mathbf{t} \in \Lambda} q^{\|\mathbf{t}\|^2}, \tag{6}$$

where $\|\mathbf{t}\|^2 = \langle \mathbf{t}, \mathbf{t} \rangle$ is the norm of a lattice vector, in which $\langle , \rangle : \Lambda \times \Lambda \to \mathbb{R}$ is the bilinear form that Λ is defined based on it.
If $\Lambda \subset \mathbb{R}^n$, we can consider $\|\mathbf{t}\|^2 = \sum_{i=1}^n t_i^2$, for $\mathbf{t} = (t_1, \ldots, t_n) \in \Lambda$.
If Λ is integral, the theta series of Λ can be written as $\sum_{m \in \mathbb{Z}} A_m q^m$, where $A_m = |\{\mathbf{x} \in \Lambda : \|\mathbf{x}\|^2 = m\}|$.

How flat the sum of Gaussian measures is ?

This slide is taken from: https://www.lnt.ei.tum.de/fileadmin/w00bxt/www/events/MCM2015/mcm2015_belfiore.pdf

Sum of Gaussian measures

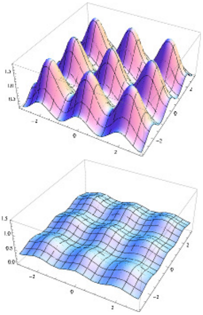


Figure : Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 0.6$

How far is the folded noise distribution from the uniform distribution on $\mathcal{V}(\Lambda_c)$?

Flatness factor (L_∞−distance w.r.t. uniform)

$$\varepsilon_{\Lambda_c}(\sigma) = \max_{\mathbf{x}\in\mathcal{V}(\Lambda_c)} \left| \frac{\sum_{\boldsymbol{\lambda}\in\Lambda_c} \left(\frac{1}{2\pi\sigma^2}\right)^{\frac{n}{2}} e^{-\frac{\|\mathbf{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}}{1/\mathrm{Vol}(\Lambda_c)} - 1 \right|$$

The flatness factor can be computed

$$\varepsilon_{\Lambda_c}(\sigma) = \left(\frac{\mathrm{Vol}(\Lambda_c)^{\frac{2}{n}}}{2\pi\sigma^2}\right)^{\frac{n}{2}} \underbrace{\sum_{\boldsymbol{\lambda}\in\Lambda_c} e^{-\frac{\|\boldsymbol{\lambda}\|^2}{2\sigma^2}}}_{\Theta_{\Lambda_c}\left(-\frac{\imath}{2\sigma^2}\right)} - 1$$

Secrecy gain

- Exceptional lattices have theta series that can be expressed as functions of the Jacobi theta functions $\vartheta_i(q)$, $q = e^{i\pi z}$, $\Im(z) > 0$, $i = 2, 3, 4$, themselves defined by

$$\vartheta_2(q) = \sum_{n=-\infty}^{+\infty} q^{\left(n+\frac{1}{2}\right)^2}, \tag{7}$$

$$\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2}, \tag{8}$$

$$\vartheta_4(q) = \sum_{n=-\infty}^{+\infty} (-1)^n q^{n^2}. \tag{9}$$

Secrecy gain

- A few examples of theta series of exceptional lattices are given in Table.

Table: Theta series of some exceptional lattices.

Lattice Λ	Theta series Θ_Λ
Cubic lattice $\mathbb{Z}^n$	ϑ_3^n
Checkerboard lattice D_n	$\frac{1}{2}(\vartheta_3^n + \vartheta_4^n)$
Gosset lattice E_8	$\frac{1}{2}(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8)$
Leech lattice Λ_{24}	$\frac{1}{8}(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8)^3 - \frac{45}{16}(\vartheta_2 \cdot \vartheta_3 \cdot \vartheta_4)^8$

Secrecy gain

- The information leaked to the eavesdropper is measured in terms of equivocation[1], that is $H(S^l|Z^n)$, where S and Z denote respectively to Alice's data and Eve's data.

[1] Given discrete random variables X with domain $\mathcal{X}$ and Y with domain $\mathcal{Y}$, the conditional entropy of Y given X is defined as

$$H(Y|X) = \sum_{x\in\mathcal{X},y\in\mathcal{Y}} p(x,y)\log\frac{p(x)}{p(x,y)}.$$

Mutual information of two discrete random variables X and Y can be expressed as

$$I(X;Y) = H(Y) - H(Y|X),$$

where

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log p(x).$$

Secrecy gain

- The best possible secrecy is achieved when $H(S^l|Z^n) = H(S^l)$, or equivalently when $I(S^l;Z^n) = H(S^l) - H(S^l|Z^n) = 0$. It was shown for the Gaussian wiretap channel that

$$I(S^l;Z^n) \leq \epsilon_n(nR - \log \epsilon_n), \qquad (7)$$

where

$$\epsilon_n = \frac{\mathrm{vol}(\Lambda_e)\Theta_{\Lambda_e}(1/2\pi\sigma_e^2)}{(\sqrt{2\pi\sigma_e^2})^n} - 1, \qquad (8)$$

and R is the total rate

$$R = R_s + R_e, \qquad (9)$$

where $R_s = \frac{2k}{n}$ is the information bits rate intended to Bob, and $R_e = \frac{2r}{n}$, with r the number of random bits, is the random bit rate, for complex channel uses.

Secrecy gain

- In order to show the benefit of a good coding strategy with respect to no coding at all, we compare the terms $\epsilon_n + 1$ obtained when Λ_e is a lattice introduced to confuse Eve with the uncoded case corresponding to $\Lambda_e = \lambda\mathbb{Z}^n$, where the factor $\lambda = \sqrt[n]{\mathrm{vol}(\Lambda)}$ is introduced to fairly compare Λ_e and $\lambda\mathbb{Z}^n$ (the comparison is done under the rate constraint $|\Lambda_b/\Lambda_e| = 2^k$):

$$\frac{\epsilon_n(\lambda\mathbb{Z}^n)+1}{\epsilon_n(\Lambda_e)+1} = \frac{\Theta_{\lambda\mathbb{Z}^n}(1/2\pi\sigma_e^2)}{\Theta_{\Lambda_e}(1/2\pi\sigma_e^2)}.$$

Secrecy gain

Definition

Let Λ be an n-dimensional lattice. The secrecy function of Λ is given by

$$\Xi_\Lambda(\tau) = \frac{\Theta_{\sqrt[n]{\mathrm{vol}(\Lambda)}\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \quad \tau = yi, \; y > 0. \tag{7}$$

The *strong secrecy gain* $\chi_{\Lambda,\mathrm{strong}}$ of an n-dimensional lattice Λ is defined by

$$\chi_{\Lambda,\mathrm{strong}} = \sup_{y>0} \Xi_\Lambda(yi). \tag{8}$$

Secrecy gain

Since the above maximum value is not easy to calculate for a general lattice, a weaker definition of secrecy gain has been introduced.

Secrecy gain

Since the above maximum value is not easy to calculate for a general lattice, a weaker definition of secrecy gain has been introduced.

Definition

A multiplicative symmetry point is a point y_0 such that $\Xi_\Lambda(y_0 \cdot y) = \Xi_\Lambda(y_0/y)$ for all $y > 0$ (in terms of $\log y$ and $\log y_0$, yielding $\Xi_\Lambda(\log y_0 + \log y) = \Xi_\Lambda(\log y_0 - \log y)$).

Secrecy gain

Since the above maximum value is not easy to calculate for a general lattice, a weaker definition of secrecy gain has been introduced.

Definition

A multiplicative symmetry point is a point y_0 such that $\Xi_\Lambda(y_0 \cdot y) = \Xi_\Lambda(y_0/y)$ for all $y > 0$ (in terms of $\log y$ and $\log y_0$, yielding $\Xi_\Lambda(\log y_0 + \log y) = \Xi_\Lambda(\log y_0 - \log y)$).

Definition

Suppose that Λ is an n-dimensional lattice, whose secrecy function has a symmetry point y_0. Then the *weak secrecy gain* χ_Λ of Λ is given by

$$\chi_\Lambda = \Xi_\Lambda(y_0) = \frac{\Theta_{\sqrt[n]{\mathrm{vol}(\Lambda)}\mathbb{Z}^n}(y_0 i)}{\Theta_\Lambda(y_0 i)}. \tag{9}$$

Outline

Preliminaries

Algebraic Number Fields

- A number field is a finite extension of $\mathbb{Q}$.

Preliminaries

Algebraic Number Fields

- A number field is a finite extension of $\mathbb{Q}$.
- An element $\alpha \in K$ is an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers of K is the ring of integers of K, denoted by $\mathcal{O}_K$.

Preliminaries

Algebraic Number Fields

- A number field is a finite extension of $\mathbb{Q}$.
- An element $\alpha \in K$ is an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers of K is the ring of integers of K, denoted by $\mathcal{O}_K$.
- If K is a number field, then $K = \mathbb{Q}(\theta)$ for an algebraic integer $\theta \in \mathcal{O}_K$.

Preliminaries

Embeddings of Number Fields

- For a number field K of degree n, the ring of integers $\mathcal{O}_K$ forms a free $\mathbb{Z}$-module of rank n.

Preliminaries

Embeddings of Number Fields

- For a number field K of degree n, the ring of integers $\mathcal{O}_K$ forms a free $\mathbb{Z}$-module of rank n.
- Every basis $\{\omega_1, \dots, \omega_n\}$ of the $\mathbb{Z}$-module $\mathcal{O}_K$ is an integral basis of K.

Preliminaries

Embeddings of Number Fields

- For a number field K of degree n, the ring of integers $\mathcal{O}_K$ forms a free $\mathbb{Z}$-module of rank n.
- Every basis $\{\omega_1, \ldots, \omega_n\}$ of the $\mathbb{Z}$-module $\mathcal{O}_K$ is an integral basis of K.
- Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. There are exactly n embeddings $\sigma_1, \ldots, \sigma_n$ of K into $\mathbb{C}$ defined by $\sigma_i(\theta) = \theta_i$, for $i = 1, \ldots, n$, where the θ_i's are the distinct zeros in $\mathbb{C}$ of the minimal polynomial of θ over $\mathbb{Q}$.

Preliminaries

Trace and Norm

Let K be a number field of degree n and $x \in K$. The elements $\sigma_1(x), \ldots, \sigma_n(x)$ are the conjugates of x, and

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad \mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x), \qquad (10)$$

are the norm and the trace of x, respectively.

Discriminant of Number Field

Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of K. The discriminant of K is defined as

$$d_K = (\det[(\sigma_j(\omega_i))_{i,j=1}^{n}])^2. \qquad (11)$$

Preliminaries

Signature of a Number Field

- Let r_1 be the number of embeddings with image in $\mathbb{R}$ and $2r_2$ the number of embeddings with image in $\mathbb{C}$ so that $r_1+2r_2 = n$.

Preliminaries

Signature of a Number Field

- Let r_1 be the number of embeddings with image in $\mathbb{R}$ and $2r_2$ the number of embeddings with image in $\mathbb{C}$ so that $r_1 + 2r_2 = n$.
- The pair (r_1, r_2) is the signature of K.

Preliminaries

Signature of a Number Field

- Let r_1 be the number of embeddings with image in $\mathbb{R}$ and $2r_2$ the number of embeddings with image in $\mathbb{C}$ so that $r_1 + 2r_2 = n$.
- The pair (r_1, r_2) is the signature of K.
- If $r_2 = 0$ we have a totally real algebraic number field.

Preliminaries

Canonical Embedding

Order the σ_i's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. The canonical embedding $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is

Preliminaries

Canonical Embedding

Order the σ_i's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. The canonical embedding $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)). \tag{12}$$

Preliminaries

Canonical Embedding

Order the σ_i's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. The canonical embedding $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)). \quad (12)$$

If we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$, the canonical embedding can be rewritten as $\sigma : K \to \mathbb{R}^n$

Preliminaries

Canonical Embedding

Order the σ_i's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. The canonical embedding $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)). \quad (12)$$

If we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$, the canonical embedding can be rewritten as $\sigma : K \to \mathbb{R}^n$

$$\begin{aligned}\sigma(x) &= (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x),\\ &\quad \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),\end{aligned} \quad (13)$$

where $\Re\sigma_i$ and $\Im\sigma_i$ denote the real and imaginary parts of σ_i.

Preliminaries

Decomposition of Prime Ideals over Number Fields

- Let K be a number field and L be a finite separable extension of K. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ with following factorization into the primes of $\mathcal{O}_L$

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \tag{14}$$

where $e_i \geq 1$.

Preliminaries

Decomposition of Prime Ideals over Number Fields

- Let K be a number field and L be a finite separable extension of K. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ with following factorization into the primes of $\mathcal{O}_L$

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \tag{14}$$

  where $e_i \geq 1$.
- Each e_i is the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$, and it is denoted by $e(\mathfrak{P}_i/\mathfrak{p})$.

Preliminaries

Decomposition of Prime Ideals over Number Fields

- Let K be a number field and L be a finite separable extension of K. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ with following factorization into the primes of $\mathcal{O}_L$

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \tag{14}$$

  where $e_i \geq 1$.
- Each e_i is the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$, and it is denoted by $e(\mathfrak{P}_i/\mathfrak{p})$.
- If $\mathfrak{P}_i$ lies above $\mathfrak{p}$ in $\mathcal{O}_L$, we denote by $f(\mathfrak{P}_i/\mathfrak{p})$ the degree of the residue field extension $\mathcal{O}_L/\mathfrak{P}_i$ over $\mathcal{O}_K/\mathfrak{p}$; which is called the residue class degree or inertia degree.

Preliminaries

Theorem

Let K be a number field and L be a finite separable extension of K. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Then

Preliminaries

Theorem

Let K be a number field and L be a finite separable extension of K. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Then

$$[L:K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}). \quad (15)$$

Preliminaries

Theorem

Let K be a number field and L be a finite separable extension of K. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Then

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}). \quad (15)$$

Remark

- When L/K is a Galois extension of degree n, $e(\mathfrak{P}/\mathfrak{p}) = e$ and $f(\mathfrak{P}/\mathfrak{p}) = f$ for all $\mathfrak{P}|\mathfrak{p}$ and above equation simplifies to $n = efg$, where g is the number primes of $\mathcal{O}_L$ above $\mathfrak{p}$.

Preliminaries

Theorem

Let K be a number field and L be a finite separable extension of K. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Then

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}). \tag{15}$$

Remark

- When L/K is a Galois extension of degree n, $e(\mathfrak{P}/\mathfrak{p}) = e$ and $f(\mathfrak{P}/\mathfrak{p}) = f$ for all $\mathfrak{P}|\mathfrak{p}$ and above equation simplifies to $n = efg$, where g is the number primes of $\mathcal{O}_L$ above $\mathfrak{p}$.
- If $[L : K] = e(\mathfrak{P}/\mathfrak{p})$, $\mathfrak{P}$ is totally ramified above $\mathfrak{p}$.

Outline

Preliminaries

Definition

An integral lattice Γ is a free $\mathbb{Z}$-module of finite rank together with a positive definite symmetric bilinear form $\langle , \rangle : \Gamma \times \Gamma \to \mathbb{Z}$.

Preliminaries

Properties of Algebraic Lattices

- The discriminant of a lattice Γ, denoted by $\mathrm{disc}(\Gamma)$, is the determinant of $\mathbf{M}\mathbf{M}^t$ where $\mathbf{M}$ is a generator matrix for Γ.

Preliminaries

Properties of Algebraic Lattices

- The discriminant of a lattice Γ, denoted by $\text{disc}(\Gamma)$, is the determinant of $\mathbf{M}\mathbf{M}^t$ where $\mathbf{M}$ is a generator matrix for Γ.
- The volume $\text{vol}(\mathbb{R}^n/\Gamma)$ of a lattice Γ is defined to be $|\det(\mathbf{M})|$.

Preliminaries

Properties of Algebraic Lattices

- The discriminant of a lattice Γ, denoted by $\mathrm{disc}(\Gamma)$, is the determinant of $\mathbf{MM}^t$ where $\mathbf{M}$ is a generator matrix for Γ.
- The volume $\mathrm{vol}(\mathbb{R}^n/\Gamma)$ of a lattice Γ is defined to be $|\det(\mathbf{M})|$.
- The discriminant is related to the volume of a lattice by

$$\sqrt{\det(\mathbf{G})} = \mathrm{vol}(\mathbb{R}^n/\Gamma) = \sqrt{\mathrm{disc}(\Gamma)}. \qquad (16)$$

Preliminaries

Preliminaries

Theorem

Let K be a number field and $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of O_K. The n vectors $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^n$, $i = 1, \ldots, n$ are linearly independent, and define a full rank lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.

Preliminaries

Theorem

Let K be a number field and $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of O_K. The n vectors $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^n$, $i = 1, \ldots, n$ are linearly independent, and define a full rank lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.

Theorem

Let d_K be the discriminant of a number field K. The volume of the fundamental parallelotope of $\Lambda(\mathcal{O}_K)$ is given by

$$\mathrm{vol}(\Lambda(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|d_K|}. \quad (16)$$

Outline

Construction A Lattices

- Let K be a Galois number field of degree n which is either totally real or a CM field (that is, a totally imaginary quadratic extension of a totally real number field),
- $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above the prime p.
- $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$.
- Let $\mathcal{C}$ be an (N, k) linear code over $\mathbb{F}_{p^f}$.
- Then, a Construction A lattice using underlying code $\mathcal{C}$ and number field K is given next.

Construction A Lattices

Definition

Let $\rho : \mathcal{O}_K^N \to \mathbb{F}_{p^f}^N$ be the mapping defined by the reduction modulo the ideal $\mathfrak{p}$ in each of the N coordinates:

$$\begin{aligned} \rho : \mathcal{O}_K^N &\to \mathbb{F}_{p^f}^N, \\ (x_1, \ldots, x_N) &\mapsto (x_1 \bmod \mathfrak{p}, \ldots, x_N \bmod \mathfrak{p}) \end{aligned} \tag{17}$$

Define $\Gamma_{\mathcal{C}}$ to be the preimage of $\mathcal{C}$ in $\mathcal{O}_K^N$, i.e.,

$$\Gamma_{\mathcal{C}} = \left\{ \mathbf{x} \in \mathcal{O}_K^N \mid \rho(\mathbf{x}) = \mathbf{c},\ \mathbf{c} \in \mathcal{C} \right\}. \tag{18}$$

Then, $\sigma^N(\Gamma_{\mathcal{C}}) \subset \mathbb{R}^n$ is the Construction A lattice with underlying code $\mathcal{C}$.

Remark

- $\Gamma_{\mathcal{C}}$ is a $\mathbb{Z}$-module of rank nN.

Remark

- $\Gamma_{\mathcal{C}}$ is a $\mathbb{Z}$-module of rank nN.
- Let K be a totally real or a CM field. Consider the following symmetric bilinear form $b_\alpha : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R}$

Remark

- $\Gamma_{\mathcal{C}}$ is a $\mathbb{Z}$-module of rank nN.
- Let K be a totally real or a CM field. Consider the following symmetric bilinear form $b_\alpha : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R}$

$$b_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(\alpha x_i \bar{y}_i), \tag{19}$$

Remark

- $\Gamma_{\mathcal{C}}$ is a $\mathbb{Z}$-module of rank nN.
- Let K be a totally real or a CM field. Consider the following symmetric bilinear form $b_\alpha : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R}$

$$b_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(\alpha x_i \bar{y}_i), \tag{19}$$

where $\mathbf{x} = (x_1, \ldots, x_N)$ and $\mathbf{y} = (y_1, \ldots, y_N)$ are vectors in $\mathcal{O}_K^N$, $\alpha \in \mathcal{O}_K$ is a totally positive element, meaning that $\sigma_i(\alpha) > 0$ for all i.

Remark

- $\Gamma_{\mathcal{C}}$ is a $\mathbb{Z}$-module of rank nN.
- Let K be a totally real or a CM field. Consider the following symmetric bilinear form $b_\alpha : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R}$

$$b_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(\alpha x_i \bar{y}_i), \tag{19}$$

  where $\mathbf{x} = (x_1, \ldots, x_N)$ and $\mathbf{y} = (y_1, \ldots, y_N)$ are vectors in $\mathcal{O}_K^N$, $\alpha \in \mathcal{O}_K$ is a totally positive element, meaning that $\sigma_i(\alpha) > 0$ for all i.
- The pair $(\rho^{-1}(\mathcal{C}), b_\alpha)$ forms a lattice of rank nN, which is integral when α is in the codifferent of K which is the set $\mathcal{D}_K^{-1} = \{x \in K : \mathrm{Tr}(xy) \in \mathbb{Z} \text{ for all } y \in \mathcal{O}_K\}$, but also in other cases, depending on the choice of $\mathcal{C}$.

Construction A Lattices from cyclotomic number fields

Example

- For p a prime, take for K the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p^{th} root of unity and $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

Construction A Lattices from cyclotomic number fields

Example

- For p a prime, take for K the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p^{th} root of unity and $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- Take $\mathfrak{p} = (1 - \zeta_p)$ the prime ideal above p, and $\alpha = 1/p$.

Construction A Lattices from cyclotomic number fields

Example

- For p a prime, take for K the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p^{th} root of unity and $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- Take $\mathfrak{p} = (1 - \zeta_p)$ the prime ideal above p, and $\alpha = 1/p$.
- Since $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, this construction involves linear codes over $\mathbb{F}_p$.

Construction A Lattices from cyclotomic number fields

Example

- For p a prime, take for K the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p^{th} root of unity and $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- Take $\mathfrak{p} = (1 - \zeta_p)$ the prime ideal above p, and $\alpha = 1/p$.
- Since $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, this construction involves linear codes over $\mathbb{F}_p$.
- The case $p = 2$ is the original binary Construction A, proposed by Forney.

Generator Matrix of Construction A Lattices

- Let K be a Galois extension.

Generator Matrix of Construction A Lattices

- Let K be a Galois extension.
- Choose the prime $\mathfrak{p}$ so that $\mathfrak{p}$ is totally ramified and $p\mathcal{O}_K = \mathfrak{p}^n$.

Generator Matrix of Construction A Lattices

- Let K be a Galois extension.
- Choose the prime $\mathfrak{p}$ so that $\mathfrak{p}$ is totally ramified and $p\mathcal{O}_K = \mathfrak{p}^n$.
- Let $\{\omega_1, \ldots, \omega_n\}$ and $\{\mu_1, \ldots, \mu_n\}$, where $\mu_i = \sum_{j=1}^{n} \mu_{i,j}\omega_j$, be the $\mathbb{Z}$-bases of $\mathcal{O}_K$ and $\mathfrak{p}$, respectively.

Generator Matrix of Construction A Lattices

- Let K be a Galois extension.
- Choose the prime $\mathfrak{p}$ so that $\mathfrak{p}$ is totally ramified and $p\mathcal{O}_K = \mathfrak{p}^n$.
- Let $\{\omega_1, \ldots, \omega_n\}$ and $\{\mu_1, \ldots, \mu_n\}$, where $\mu_i = \sum_{j=1}^{n} \mu_{i,j}\omega_j$, be the $\mathbb{Z}$-bases of $\mathcal{O}_K$ and $\mathfrak{p}$, respectively.
- A generator matrix for the lattice $\mathcal{O}_K$ together with the trace form $\langle w, z\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(wz)$, $w, z \in \mathcal{O}_K$, is

Generator Matrix of Construction A Lattices

- Let K be a Galois extension.
- Choose the prime $\mathfrak{p}$ so that $\mathfrak{p}$ is totally ramified and $p\mathcal{O}_K = \mathfrak{p}^n$.
- Let $\{\omega_1, \ldots, \omega_n\}$ and $\{\mu_1, \ldots, \mu_n\}$, where $\mu_i = \sum_{j=1}^{n} \mu_{i,j}\omega_j$, be the $\mathbb{Z}$-bases of $\mathcal{O}_K$ and $\mathfrak{p}$, respectively.
- A generator matrix for the lattice $\mathcal{O}_K$ together with the trace form $\langle w, z \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(wz)$, $w, z \in \mathcal{O}_K$, is

$$\mathbf{M} = [\sigma_j(\omega_i)]_{i,j=1}^{n}. \tag{20}$$

Generator Matrix of Construction A Lattices

- Let K be a Galois extension.
- Choose the prime $\mathfrak{p}$ so that $\mathfrak{p}$ is totally ramified and $p\mathcal{O}_K = \mathfrak{p}^n$.
- Let $\{\omega_1, \ldots, \omega_n\}$ and $\{\mu_1, \ldots, \mu_n\}$, where $\mu_i = \sum_{j=1}^{n} \mu_{i,j}\omega_j$, be the $\mathbb{Z}$-bases of $\mathcal{O}_K$ and $\mathfrak{p}$, respectively.
- A generator matrix for the lattice $\mathcal{O}_K$ together with the trace form $\langle w, z\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(wz)$, $w, z \in \mathcal{O}_K$, is

$$\mathbf{M} = [\sigma_j(\omega_i)]_{i,j=1}^{n}. \tag{20}$$

By applying the embeddings over the basis of $\mathfrak{p}$ we have

$$[\sigma_j(\mu_i)]_{i,j=1}^{n} = \mathbf{DM}, \tag{21}$$

where $\mathbf{D} = [\mu_{i,j}]_{i,j=1}^{n}$.

Generator Matrix of Construction A Lattices

Let $\mathcal{C} \subset \mathbb{F}_p^N$ be a linear code. The lattice $\Gamma_{\mathcal{C}}$ is a sublattice of $\mathcal{O}_K^N$ with discriminant

Generator Matrix of Construction A Lattices

Let $\mathcal{C} \subset \mathbb{F}_p^N$ be a linear code. The lattice $\Gamma_{\mathcal{C}}$ is a sublattice of $\mathcal{O}_K^N$ with discriminant

$$\mathrm{disc}(\Gamma_{\mathcal{C}}) = d_K^N (p^f)^{2(N-k)}, \tag{22}$$

Generator Matrix of Construction A Lattices

Let $\mathcal{C} \subset \mathbb{F}_p^N$ be a linear code. The lattice $\Gamma_{\mathcal{C}}$ is a sublattice of $\mathcal{O}_K^N$ with discriminant

$$\mathrm{disc}(\Gamma_{\mathcal{C}}) = d_K^N (p^f)^{2(N-k)}, \tag{22}$$

where $d_K = (\det([\sigma_i(\omega_j)]_{i,j=1}^n))^2$ is the discriminant of K.

Generator Matrix of Construction A Lattices

Let $\mathcal{C} \subset \mathbb{F}_p^N$ be a linear code. The lattice $\Gamma_{\mathcal{C}}$ is a sublattice of $\mathcal{O}_K^N$ with discriminant

$$\mathrm{disc}(\Gamma_{\mathcal{C}}) = d_K^N (p^f)^{2(N-k)}, \tag{22}$$

where $d_K = (\det([\sigma_i(\omega_j)]_{i,j=1}^n))^2$ is the discriminant of K. The lattice $\Gamma_{\mathcal{C}}$ is given by the generator matrix

Generator Matrix of Construction A Lattices

Let $\mathcal{C} \subset \mathbb{F}_p^N$ be a linear code. The lattice $\Gamma_{\mathcal{C}}$ is a sublattice of $\mathcal{O}_K^N$ with discriminant

$$\mathrm{disc}(\Gamma_{\mathcal{C}}) = d_K^N (p^f)^{2(N-k)}, \tag{22}$$

where $d_K = (\det([\sigma_i(\omega_j)]_{i,j=1}^n))^2$ is the discriminant of K. The lattice $\Gamma_{\mathcal{C}}$ is given by the generator matrix

$$\mathbf{M}_{\mathcal{C}} = \begin{bmatrix} \mathbf{I}_k \otimes \mathbf{M} & \mathbf{A} \otimes \mathbf{M} \\ \mathbf{0}_{n(N-k)\times nk} & \mathbf{I}_{N-k} \otimes \mathbf{DM} \end{bmatrix}, \tag{23}$$

Generator Matrix of Construction A Lattices

Let $\mathcal{C} \subset \mathbb{F}_p^N$ be a linear code. The lattice $\Gamma_{\mathcal{C}}$ is a sublattice of $\mathcal{O}_K^N$ with discriminant

$$\mathrm{disc}(\Gamma_{\mathcal{C}}) = d_K^N (p^f)^{2(N-k)}, \tag{22}$$

where $d_K = (\det([\sigma_i(\omega_j)]_{i,j=1}^n))^2$ is the discriminant of K. The lattice $\Gamma_{\mathcal{C}}$ is given by the generator matrix

$$\mathbf{M}_{\mathcal{C}} = \begin{bmatrix} \mathbf{I}_k \otimes \mathbf{M} & \mathbf{A} \otimes \mathbf{M} \\ \mathbf{0}_{n(N-k)\times nk} & \mathbf{I}_{N-k} \otimes \mathbf{DM} \end{bmatrix}, \tag{23}$$

where $\otimes$ is the tensor product of matrices, $\begin{bmatrix} \mathbf{I}_k & \mathbf{A} \end{bmatrix}$ is a generator matrix of $\mathcal{C}$, $\mathbf{M}$ and $\mathbf{DM}$ are the matrices of the embeddings of $\mathbb{Z}$-bases of $\mathcal{O}_K$ and $\mathfrak{p}$, respectively.

Modular lattices

Definition

- Given an arbitrary lattice (L, b), the dual lattice of (L, b) is the pair (L^*, b), where

Modular lattices

Definition

- Given an arbitrary lattice (L, b), the dual lattice of (L, b) is the pair (L^*, b), where

$$L^* = \{\mathbf{x} \in L \otimes_{\mathbb{Z}} \mathbb{R} \,|\, b(\mathbf{x}, \mathbf{y}) \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}\,. \tag{24}$$

Modular lattices

Definition

- Given an arbitrary lattice (L, b), the dual lattice of (L, b) is the pair (L^*, b), where

$$L^* = \{\mathbf{x} \in L \otimes_{\mathbb{Z}} \mathbb{R} \,|\, b(\mathbf{x}, \mathbf{y}) \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}. \tag{24}$$

- If $L \subset L^*$, (L, b) is integral.

Modular lattices

Definition

- Given an arbitrary lattice (L, b), the dual lattice of (L, b) is the pair (L^*, b), where

$$L^* = \{\mathbf{x} \in L \otimes_{\mathbb{Z}} \mathbb{R} \,|\, b(\mathbf{x}, \mathbf{y}) \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}\,. \tag{24}$$

- If $L \subset L^*$, (L, b) is integral.
- An integral lattice (L, b) is called even if $b(\mathbf{x}, \mathbf{x}) \in 2\mathbb{Z}$ for all $\mathbf{x} \in L$ and odd otherwise.

Modular lattices

Definition

- Given an arbitrary lattice (L, b), the dual lattice of (L, b) is the pair (L^*, b), where

$$L^* = \{\mathbf{x} \in L \otimes_{\mathbb{Z}} \mathbb{R} \mid b(\mathbf{x}, \mathbf{y}) \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\} . \qquad (24)$$

- If $L \subset L^*$, (L, b) is integral.
- An integral lattice (L, b) is called even if $b(\mathbf{x}, \mathbf{x}) \in 2\mathbb{Z}$ for all $\mathbf{x} \in L$ and odd otherwise.
- If $(L, b) \cong (L^*, b)$, i.e., there exists a $\mathbb{Z}$-module homomorphism $\tau : L \to L^*$ such that $b(\tau(\mathbf{x}), \tau(\mathbf{y})) = b(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in L$, then (L, b) is unimodular.

Modular lattices

Definition

- Given an arbitrary lattice (L, b), the dual lattice of (L, b) is the pair (L^*, b), where

$$L^* = \{\mathbf{x} \in L \otimes_{\mathbb{Z}} \mathbb{R} \,|\, b(\mathbf{x}, \mathbf{y}) \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}. \tag{24}$$

- If $L \subset L^*$, (L, b) is integral.
- An integral lattice (L, b) is called even if $b(\mathbf{x}, \mathbf{x}) \in 2\mathbb{Z}$ for all $\mathbf{x} \in L$ and odd otherwise.
- If $(L, b) \cong (L^*, b)$, i.e., there exists a $\mathbb{Z}$-module homomorphism $\tau : L \to L^*$ such that $b(\tau(\mathbf{x}), \tau(\mathbf{y})) = b(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in L$, then (L, b) is unimodular.
- If (L, b) is integral and $(L, b) \cong (L^*, db)$, it is d-modular.

Self dual linear codes

Self-dual codes thus provide a systematic way to obtain modular lattices.

Self dual linear codes

Self-dual codes thus provide a systematic way to obtain modular lattices.

Definition

- Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a linear code of dimension k, q a prime power.

Self dual linear codes

Self-dual codes thus provide a systematic way to obtain modular lattices.

Definition

- Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a linear code of dimension k, q a prime power.
- Dual code is $C^\perp = \left\{ \mathbf{x} \in \mathbb{F}_q^N \,|\, \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^N x_i y_i = 0 \ \forall \ \mathbf{y} \in \mathcal{C} \right\}$.

Self dual linear codes

Self-dual codes thus provide a systematic way to obtain modular lattices.

Definition

- Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a linear code of dimension k, q a prime power.
- Dual code is $C^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^N \,|\, \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{N} x_i y_i = 0 \ \forall \ \mathbf{y} \in \mathcal{C} \right\}$.
- $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$.

Self dual linear codes

Self-dual codes thus provide a systematic way to obtain modular lattices.

Definition

- Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a linear code of dimension k, q a prime power.
- Dual code is $C^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^N \,|\, \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{N} x_i y_i = 0 \; \forall \; \mathbf{y} \in \mathcal{C} \right\}$.
- $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$.
- For $K = \mathbb{Q}(\zeta_p)$, if $\mathcal{C} \subset \mathbb{F}_p^N$ is self-dual, then $(\rho^{-1}(\mathcal{C}), b_{\frac{1}{p}})$ is unimodular.

Secrecy gain of modular lattices

Remark

- The volume of a d-modular lattice is $\mathrm{vol}(\Lambda) = d^{\frac{n}{4}}$.

Secrecy gain of modular lattices

Remark

- The volume of a d-modular lattice is $\mathrm{vol}(\Lambda) = d^{\frac{n}{4}}$.
- Let Λ be an n-dimensional d-modular lattice. The weak secrecy gain of Λ is given by

$$\chi_\Lambda = \frac{\Theta_{\sqrt[4]{d}\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \quad \tau = \frac{i}{\sqrt{d}}. \tag{25}$$

Secrecy gain of modular lattices

Remark

- The volume of a d-modular lattice is $\mathrm{vol}(\Lambda) = d^{\frac{n}{4}}$.
- Let Λ be an n-dimensional d-modular lattice. The weak secrecy gain of Λ is given by

$$\chi_\Lambda = \frac{\Theta_{\sqrt[4]{d}\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \quad \tau = \frac{i}{\sqrt{d}}. \tag{25}$$

- Belfiore and Solé discovered a symmetry point in the secrecy function of ℓ-modular ($\ell = 1, 2, 3, 5, 6, 7, 11, 14, 15, 23$) lattices and the weak secrecy gain χ_Λ is conjectured to be the secrecy gain for these lattices.

Problem statement

Conclusion about the weak secrecy gain of modular lattice

- Fixing dimension, the length of the shortest nonzero vector, kissing number, a smaller level d gives a bigger χ_Λ. However, the lattices with high level d are more likely to have a large length for the shortest nonzero vector.

Construction of modular lattices using Construction A and cyclotomic number fields

W. Kositwattanarerk, S. S. Ong and F. Oggier, 2013

- Let p be an odd prime and consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

Construction of modular lattices using Construction A and cyclotomic number fields

W. Kositwattanarerk, S. S. Ong and F. Oggier, 2013

- Let p be an odd prime and consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- Take the prime ideal $\mathfrak{p} = (1 - \zeta_p)$ with the residue field $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, and the bilinear form $b_{1/p}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i / p)$, where $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=0}^{p-2} \sigma_i(x) = \sum_{i=1}^{p-1} x^i$, for $x \in K$.

Construction of modular lattices using Construction A and cyclotomic number fields

W. Kositwattanarerk, S. S. Ong and F. Oggier, 2013

- Let p be an odd prime and consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- Take the prime ideal $\mathfrak{p} = (1-\zeta_p)$ with the residue field $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, and the bilinear form $b_{1/p}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i/p)$, where $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=0}^{p-2} \sigma_i(x) = \sum_{i=1}^{p-1} x^i$, for $x \in K$.
- Given a code $\mathcal{C}$ over $\mathbb{F}_p$, if $\mathcal{C} \subset \mathcal{C}^{\perp}$ then $(\rho^{-1}(\mathcal{C}), b_{1/p})$ is an even integral lattice of rank $N(p-1)$.

Construction of modular lattices using Construction A and cyclotomic number fields

W. Kositwattanarerk, S. S. Ong and F. Oggier, 2013

- Let p be an odd prime and consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- Take the prime ideal $\mathfrak{p} = (1-\zeta_p)$ with the residue field $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, and the bilinear form $b_{1/p}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i\bar{y}_i/p)$, where $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=0}^{p-2} \sigma_i(x) = \sum_{i=1}^{p-1} x^i$, for $x \in K$.
- Given a code $\mathcal{C}$ over $\mathbb{F}_p$, if $\mathcal{C} \subset \mathcal{C}^\perp$ then $(\rho^{-1}(\mathcal{C}), b_{1/p})$ is an even integral lattice of rank $N(p-1)$.
- If $\mathcal{C}$ is self-dual, then $(\rho^{-1}(\mathcal{C}), b_{1/p})$ is an even unimodular lattice.

Construction of modular lattices using Construction A and cyclotomic number fields

W. Kositwattanarerk, S. S. Ong and F. Oggier, 2015

- Let $K^{+} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and let $\mathcal{C} \subset \mathbb{F}_p^N$ be a k-dimensional code such that $\mathcal{C} \subset \mathcal{C}^{\perp}$.

Construction of modular lattices using Construction A and cyclotomic number fields

W. Kositwattanarerk, S. S. Ong and F. Oggier, 2015

- Let $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and let $\mathcal{C} \subset \mathbb{F}_p^N$ be a k-dimensional code such that $\mathcal{C} \subset \mathcal{C}^\perp$.
- Then the lattice $(\rho^{-1}(\mathcal{C}), b_\alpha)$ together with the bilinear form $b_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^N \mathrm{Tr}_{K^+/\mathbb{Q}}(\alpha x_i y_i)$, where $\alpha = 1/p$, is an integral lattice of rank $N(p-1)/2$.

Construction of modular lattices using Construction A and cyclotomic number fields

W. Kositwattanarerk, S. S. Ong and F. Oggier, 2015

- Let $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and let $\mathcal{C} \subset \mathbb{F}_p^N$ be a k-dimensional code such that $\mathcal{C} \subset \mathcal{C}^\perp$.
- Then the lattice $(\rho^{-1}(\mathcal{C}), b_\alpha)$ together with the bilinear form $b_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^N \mathrm{Tr}_{K^+/\mathbb{Q}}(\alpha x_i y_i)$, where $\alpha = 1/p$, is an integral lattice of rank $N(p-1)/2$.
- In addition, if $\mathcal{C}$ is self-dual, then $(\rho^{-1}(\mathcal{C}), b_\alpha)$ is an odd unimodular lattice.

Construction of modular lattices using Construction A and cyclotomic number fields

We consider the generalizations of these results to $K = \mathbb{Q}(\zeta_{p^r})$ and $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$, or $K = \mathbb{Q}(\zeta_n)$, with $n \neq p^r$.

Construction of modular lattices using Construction A and cyclotomic number fields

We consider the generalizations of these results to $K = \mathbb{Q}(\zeta_{p^r})$ and $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$, or $K = \mathbb{Q}(\zeta_n)$, with $n \neq p^r$.

Panario, Sadeghi and Khodaiemehr

- Let $K = \mathbb{Q}(\zeta_{p^r})$, with $r > 1$ and p an odd prime number, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.

Construction of modular lattices using Construction A and cyclotomic number fields

We consider the generalizations of these results to $K = \mathbb{Q}(\zeta_{p^r})$ and $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$, or $K = \mathbb{Q}(\zeta_n)$, with $n \neq p^r$.

Panario, Sadeghi and Khodaiemehr

- Let $K = \mathbb{Q}(\zeta_{p^r})$, with $r > 1$ and p an odd prime number, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.
- K is a CM field and the prime p totally ramifies in K as $p\mathcal{O}_K = \mathfrak{P}^{p^{r-1}(p-1)}$, with residue field $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_p$, where $\mathfrak{P} = (1 - \zeta_{p^r})$.

Construction of modular lattices using Construction A and cyclotomic number fields

We consider the generalizations of these results to $K = \mathbb{Q}(\zeta_{p^r})$ and $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$, or $K = \mathbb{Q}(\zeta_n)$, with $n \neq p^r$.

Panario, Sadeghi and Khodaiemehr

- Let $K = \mathbb{Q}(\zeta_{p^r})$, with $r > 1$ and p an odd prime number, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.
- K is a CM field and the prime p totally ramifies in K as $pO_K = \mathfrak{P}^{p^{r-1}(p-1)}$, with residue field $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_p$, where $\mathfrak{P} = (1 - \zeta_{p^r})$.
- Let $\mathcal{C} \subset \mathbb{F}_p^N$ be an (N, k) self-dual code over $\mathbb{F}_p$.

Construction of modular lattices using Construction A and cyclotomic number fields

We consider the generalizations of these results to $K = \mathbb{Q}(\zeta_{p^r})$ and $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$, or $K = \mathbb{Q}(\zeta_n)$, with $n \neq p^r$.

Panario, Sadeghi and Khodaiemehr

- Let $K = \mathbb{Q}(\zeta_{p^r})$, with $r > 1$ and p an odd prime number, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.
- K is a CM field and the prime p totally ramifies in K as $p\mathcal{O}_K = \mathfrak{P}^{p^{r-1}(p-1)}$, with residue field $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_p$, where $\mathfrak{P} = (1 - \zeta_{p^r})$.
- Let $\mathcal{C} \subset \mathbb{F}_p^N$ be an (N, k) self-dual code over $\mathbb{F}_p$.
- Then, $(\rho^{-1}(\mathcal{C}), b_{1/p})$ with $b_{1/p}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i / p)$, is d-modular if and only if $d = 1$ and $r = 1$.

Construction of modular lattices using Construction A and cyclotomic number fields

Panario, Sadeghi and Khodaiemehr

- Let $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$ and p an odd prime number, be the totally real maximal subfield of a cyclotomic field with the ring of integers $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$.

Construction of modular lattices using Construction A and cyclotomic number fields

Panario, Sadeghi and Khodaiemehr

- Let $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$ and p an odd prime number, be the totally real maximal subfield of a cyclotomic field with the ring of integers $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$.
- K^+ is a totally real number field and the prime p totally ramifies in K^+ as $pO_{K^+} = \mathfrak{p}^{\frac{p^{r-1}(p-1)}{2}}$, with residue field $\mathcal{O}_{K^+}/\mathfrak{p} \cong \mathbb{F}_p$, where $\mathfrak{p} = (2 - \zeta_{p^r} - \zeta_{p^r}^{-1})$.

Construction of modular lattices using Construction A and cyclotomic number fields

Panario, Sadeghi and Khodaiemehr

- Let $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$ and p an odd prime number, be the totally real maximal subfield of a cyclotomic field with the ring of integers $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$.
- K^+ is a totally real number field and the prime p totally ramifies in K^+ as $p\mathcal{O}_{K^+} = \mathfrak{p}^{\frac{p^{r-1}(p-1)}{2}}$, with residue field $\mathcal{O}_{K^+}/\mathfrak{p} \cong \mathbb{F}_p$, where $\mathfrak{p} = (2 - \zeta_{p^r} - \zeta_{p^r}^{-1})$.
- Let $\mathcal{C} \subset \mathbb{F}_p^N$ be an (N, k) self-dual code over $\mathbb{F}_p$.

Construction of modular lattices using Construction A and cyclotomic number fields

Panario, Sadeghi and Khodaiemehr

- Let $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$ and p an odd prime number, be the totally real maximal subfield of a cyclotomic field with the ring of integers $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$.
- K^+ is a totally real number field and the prime p totally ramifies in K^+ as $p\mathcal{O}_{K^+} = \mathfrak{p}^{\frac{p^{r-1}(p-1)}{2}}$, with residue field $\mathcal{O}_{K^+}/\mathfrak{p} \cong \mathbb{F}_p$, where $\mathfrak{p} = (2 - \zeta_{p^r} - \zeta_{p^r}^{-1})$.
- Let $\mathcal{C} \subset \mathbb{F}_p^N$ be an (N, k) self-dual code over $\mathbb{F}_p$.
- Then, $(\rho^{-1}(\mathcal{C}), b_{1/p})$ with $b_{1/p}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i/p)$, is d-modular if and only if $d = 1$ and $r = 1$.

- Let $n = 2k$ be the lattice dimension. Let $k_l = 24/\sum_{d|l} d$ be integral. If the number of divisors is less than or equal 2, $l \in \{1, 2, 3, 5, 7, 11, 23\}$. If l is the product of some (not necessarily distinct) primes, then $l \in \{6, 14, 15\}$.

- Let $n = 2k$ be the lattice dimension. Let $k_l = 24/\sum_{d|l} d$ be integral. If the number of divisors is less than or equal 2, $l \in \{1, 2, 3, 5, 7, 11, 23\}$. If l is the product of some (not necessarily distinct) primes, then $l \in \{6, 14, 15\}$.
- For $z \in \mathcal{H}$ and $q = e^{\pi iz}$, let $\eta(z) = q^{1/12} \prod_{m=1}^{\infty}(1 - q^{2m})$ be the Dedekind eta function, and set $\Delta_l(z) = \prod_{d|l} \eta(dz)^{k_l}$, for $l \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$.
- If $l \in \{1, 2, 3, 5, 7, 11, 23\}$ then the theta series of an even l-modular lattice of dimension $2k$ can be written as a linear combination of all modular forms $\Theta_{2k_0}^{\lambda} \Delta_l^{\mu}$, $\lambda, \mu \geq 0$, of weight k, in which $\Theta_{2k_0}(z)$ denotes the theta series of an even l-modular lattice of lowest positive dimension. We have $k_0\lambda + k_l\mu = k$.

Strongly modular lattices

- Given an integral lattice Λ of level l, the partial dual $D_d\Lambda$ of Λ, for d an exact divisor of l, is $D_d\Lambda = \sqrt{d}\left(\frac{1}{d}\Lambda \cap \Lambda^*\right)$, and Λ an integral lattice is said to be **strongly modular** if $D_d\Lambda \cong \Lambda$ for all exact divisors d of l.

Strongly modular lattices

- Given an integral lattice Λ of level l, the partial dual $D_d\Lambda$ of Λ, for d an exact divisor of l, is $D_d\Lambda = \sqrt{d}\left(\frac{1}{d}\Lambda \cap \Lambda^*\right)$, and Λ an integral lattice is said to be **strongly modular** if $D_d\Lambda \cong \Lambda$ for all exact divisors d of l.
- If l is prime, the notion of strongly modular is the same as that of modular. We distinguish modular and strongly modular for $l \in \{6, 14, 15\}$.
- For $l \in \{6, 14, 15\}$, the theta series of an even strongly modular lattice of level l and dimension $n = 2k$ can be written as a linear combination of $\Theta_4^{\lambda}\Delta_l^{\mu}$, $\lambda, \mu \geq 0$, where $2\lambda + 2k_l\mu = k$. Θ_4 is the theta series of some four-dimensional strongly modular even lattice of level $l = 6, 14, 15$.

Extremal Lattices

- The minimum, or minimum norm $\mu_\Lambda = \min(\Lambda) = \min\{|||x|||^2, \ x \in \Lambda, x \neq 0\}$ of an even strongly l-modular lattice,

$$l \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$$

satisfies

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

Extremal Lattices

- The minimum, or minimum norm $\mu_\Lambda = \min(\Lambda) = \min\{|||x|||^2,\ x \in \Lambda, x \neq 0\}$ of an even strongly l-modular lattice,

$$l \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$$

satisfies

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

- 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.

Available Results

- Secrecy gain is a lattice invariant and depends on theta series.

Available Results

- Secrecy gain is a lattice invariant and depends on theta series.
- It has been studied for unimodular lattices, in [Lin and Oggier 13] for unimodular lattices up to dimensions 23, in [Lin and Oggier 12, Oggier et al. 16] for higher dimensional and extremal unimodular lattices, and in [Pinchak 13] for unimodular lattices constructed from direct sums and from codes.

Available Results

- Secrecy gain is a lattice invariant and depends on theta series.
- It has been studied for unimodular lattices, in [Lin and Oggier 13] for unimodular lattices up to dimensions 23, in [Lin and Oggier 12, Oggier et al. 16] for higher dimensional and extremal unimodular lattices, and in [Pinchak 13] 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.

Available Results

- Secrecy gain is a lattice invariant and depends on theta series.
- It has been studied for unimodular lattices, in [Lin and Oggier 13] for unimodular lattices up to dimensions 23, in [Lin and Oggier 12, Oggier et al. 16] for higher dimensional and extremal unimodular lattices, and in [Pinchak 13] 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 [Hou et al. 14, Lin et al. 15], and a generic construction of *l*-modular lattices from a general Construction A over number fields was proposed in [Hou and Oggier 17], where a few secrecy gains were computed.

Available Results

- 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?

Available Results

- 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, the secrecy gain of l-modular lattices, for $l \in \mathcal{L} = \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$, focusing on lattices with large minimum norm, especially extremal lattices, have been studied in [Oggier, Belfiore, 18].

Methodology

- Using the above results, we need to 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 $l \in \mathcal{L}$ in the smallest dimension, and when there are several of them, considering those extremal is enough.

Methodology

- Using the above results, we need to 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 $l \in \mathcal{L}$ in the smallest dimension, and when there are several of them, considering those extremal is enough.
- Equipped with these theta series, we compute the secrecy gain for extremal theta series of level l using the software SAGE.

Methodology

- Using the above results, we need to 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 $l \in \mathcal{L}$ in the smallest dimension, and when there are several of them, considering those extremal is enough.
- Equipped with these theta series, we compute the secrecy gain for extremal theta series of level l using the software SAGE.
- Comparing the numerical results shows that $l = 2, 3, 6, 7, 11$ are the best levels for the respective ranges of dimensions $\{80, 76, 72\}$, $\{68, 64, 60, 56, 52, 48\}$, $\{44, 40, 36\}$, $\{34, 32, 30, 28, 26, 24, 22\}$, $\{18, 16, 14, 12, 10, 8\}$.

Methodology

- Using the above results, we need to 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 $l \in \mathcal{L}$ in the smallest dimension, and when there are several of them, considering those extremal is enough.
- Equipped with these theta series, we compute the secrecy gain for extremal theta series of level l using the software SAGE.
- Comparing the numerical results shows that $l = 2, 3, 6, 7, 11$ are the best levels for the respective ranges of dimensions $\{80, 76, 72\}$, $\{68, 64, 60, 56, 52, 48\}$, $\{44, 40, 36\}$, $\{34, 32, 30, 28, 26, 24, 22\}$, $\{18, 16, 14, 12, 10, 8\}$.
- Hence, within a range of dimensions where different levels exist, the highest value of l tends to give the best secrecy gain.

Theta series of lowest dimensional even strongly l-modular and extremal lattices

l	$n = 2k_0$	lattice	$2 + 2\left\lfloor \frac{n\sum_{d\mid l} d}{24\sum_{d\mid l} 1} \right\rfloor$	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

Figure: Lattices in the smallest dimension $2k_0$ which are even, strongly l-modular, and extremal.

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

Figure: 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.

Example ($l = 15$)

- A generic theta series for even strongly 15-modular lattices is $\Theta_4^{\lambda}\Delta_{15}^{\mu}$, $2\lambda + 2\mu = k$, with $\Delta_{15} = q^2 - q^4 - q^6 - q^8 + \cdots$ and the upper bound for the minimum of these lattices is $2 + 2\lfloor \frac{n}{4} \rfloor$.

Example ($l = 15$)

- A generic theta series for even strongly 15-modular lattices is $\Theta_4^{\lambda}\Delta_{15}^{\mu}$, $2\lambda + 2\mu = k$, with $\Delta_{15} = q^2 - q^4 - q^6 - q^8 + \cdots$ 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 fourd imensional strongly 15-modular lattices could be used as well.

Example ($l = 15$)

- A generic theta series for even strongly 15-modular lattices is $\Theta_4^{\lambda}\Delta_{15}^{\mu}$, $2\lambda + 2\mu = k$, with $\Delta_{15} = q^2 - q^4 - q^6 - q^8 + \cdots$ 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 fourd imensional strongly 15-modular lattices could be used as well.

- The values of n for which 15-modular even extremal lattices exist are listed in the next slide.It containes extremal theta series found using $\Theta_4 = E(15)$, L_{15} and L'_{15}.

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	$1+7860q^{12}+9720q^{14}$ $+O(q^{15})$	

Figure: The values of n for which 15-modular even extremal lattices exist.

Secrecy gain of even l-modular lattices

- Having computed the theta series of extremal even strongly l-modular lattices, we can compute the corresponding secrecy function and secrecy gain (that is, the value of the secrecy function at $1/\sqrt{l}$ for all of them. The secrecy function tends to have a typical bell shape.

Secrecy gain of even l-modular lattices

- Having computed the theta series of extremal even strongly l-modular lattices, we can compute the corresponding secrecy function and secrecy gain (that is, the value of the secrecy function at $1/\sqrt{l}$ for all of them. The secrecy function tends to have a typical bell shape.
- The secrecy function of two-modular lattices is shown next, as a function of $y = -iz$ 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 artifact 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.

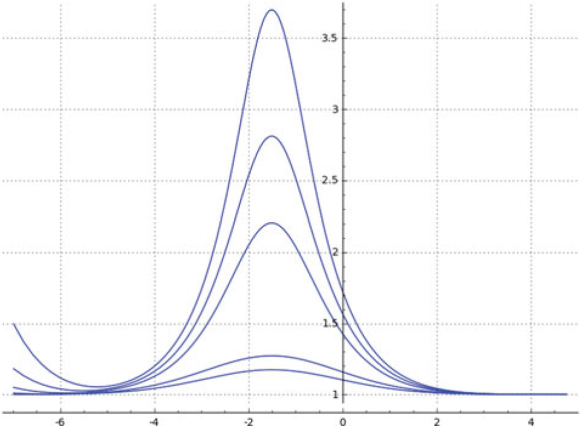


Figure: The secrecy function of two-modular lattices for dimensions $n = 8, 12, 16, 20, 24$.

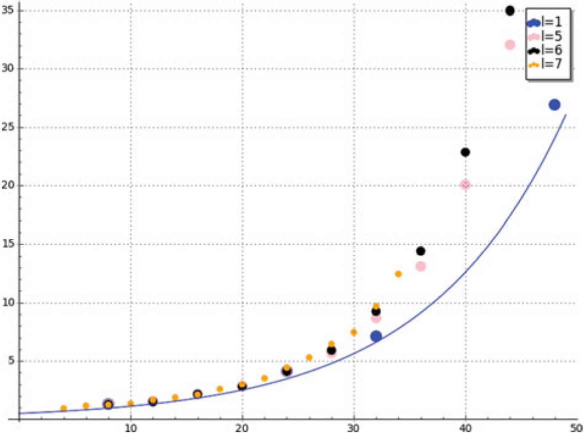


Figure: Secrecy gains of l-modular lattices for $l = 1, 5, 6, 7$. For dimensions between 20 and 50, 7-modular lattices have highest secrecy gains, closely.

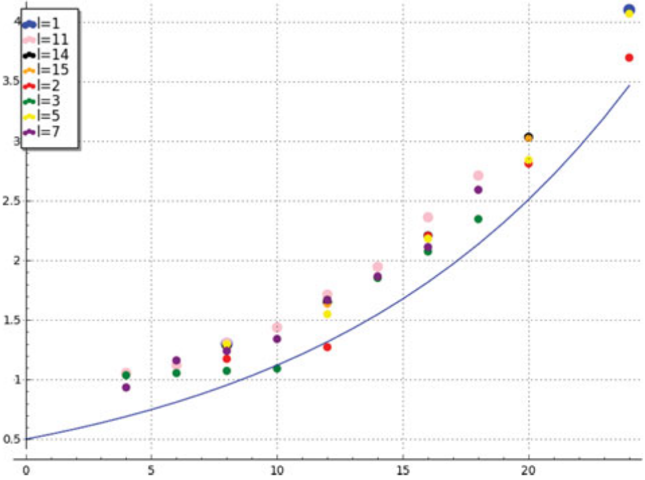


Figure: Secrecy gains of l-modular lattices for $l = 1, 2, 3, 5, 7, 11, 14, 15$.

Weak secrecy gain of dimension 8 Construction A latices from number fields

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
1	8	3	2	8	1.2077	1	0	8	64	120	192	424	576	920	1600
2	8	5	2	8	1.0020	1	0	8	16	24	96	128	208	408	480
3	8	5	4	120	1.2970	1	0	0	0	120	0	240	0	600	0
4	8	6	3	16	1.1753	1	0	0	16	24	48	128	144	216	400
5	8	7	2	8	0.8838	1	0	8	0	24	64	32	128	120	192
6	8	7	3	16	1.1048	1	0	0	16	16	16	80	128	224	288
7	8	11	3	8	1.0015	1	0	0	8	8	8	24	48	72	88
8	8	14	2	8	0.5303	1	0	8	0	24	0	32	8	24	64
9	8	14	3	8	0.9216	1	0	0	8	0	8	32	0	48	80
10	8	15	3	8	0.8869	1	0	0	8	0	8	24	0	64	32
11	8	15	4	8	1.0840	1	0	0	0	8	16	0	16	32	64
12	8	23	3	8	0.6847	1	0	0	8	0	0	24	0	8	40
13	8	23	5	16	1.0396	1	0	0	0	0	16	0	0	16	0
14	8	23	5	8	1.1394	1	0	0	0	0	8	0	8	24	24

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
15	12	3	1	12	0.4692	1	12	60	172	396	1032	2524	4704	8364	17164
16	12	3	1	4	0.8342	1	4	28	100	332	984	2236	5024	9772	16516
17	12	3	1	4	0.9385	1	4	12	100	428	984	2092	5024	9708	16516
18	12	3	2	24	1.2012	1	0	24	64	228	960	2200	5184	10524	16192
19	12	3	2	12	1.3650	1	0	12	64	300	960	2092	5184	10476	16192
20	12	3	3	64	1.5806	1	0	0	64	372	960	1984	5184	10428	16192
21	12	5	2	12	1.0030	1	0	12	24	60	240	400	984	2172	3440
22	12	5	4	60	1.6048	1	0	0	0	60	288	520	960	1980	3680
23	12	6	1	12	0.1820	1	12	60	160	252	312	556	1104	1740	2796
24	12	6	1	6	0.3845	1	6	20	58	132	236	460	936	1564	2478
25	12	6	2	8	0.9797	1	0	8	20	36	144	264	544	1244	2016
26	12	6	3	16	1.3580	1	0	0	16	36	96	256	624	1308	2112
27	12	6	3	12	1.3974	1	0	0	12	40	100	244	668	1284	2076
28	12	6	3	12	1.5044	1	0	0	4	36	132	256	660	1308	1980
29	12	7	1	12	0.1452	1	12	60	160	252	312	544	972	1164	1596
30	12	7	1	4	0.4645	1	4	12	32	60	168	416	580	876	1684
31	12	7	1	4	0.5806	1	4	4	16	84	152	208	580	1268	1908
32	12	7	2	12	0.7584	1	0	12	16	36	144	112	384	852	1056
33	12	7	2	8	0.8795	1	0	8	16	28	112	160	384	772	1152
34	12	7	3	4	1.4023	1	0	0	4	36	84	64	384	972	1368
35	12	11	1	8	0.1765	1	8	24	36	60	180	356	424	612	1204
36	12	11	1	4	0.2173	1	4	16	48	88	152	204	144	316	772
37	12	11	3	12	1.0726	1	0	0	12	0	12	108	72	108	436
38	12	14	1	8	0.1331	1	8	24	36	56	148	264	320	544	912
39	12	14	1	4	0.1534	1	4	16	48	88	152	204	144	280	628
40	12	14	3	12	0.9134	1	0	0	12	0	0	72	48	72	256
41	12	15	1	8	0.1313	1	8	24	32	32	112	292	352	328	744
42	12	15	1	4	0.3899	1	4	4	0	12	56	96	80	132	388
43	12	15	1	2	0.4661	1	2	0	10	32	30	44	96	128	186
44	12	15	2	6	0.5455	1	0	6	8	4	42	46	74	136	154
45	12	15	2	6	0.9217	1	0	2	2	4	24	20	46	100	154
46	12	15	3	4	1.0031	1	0	0	4	8	18	28	36	64	104
47	12	15	4	4	1.3573	1	0	0	0	4	10	12	48	72	108
48	12	15	5	4	1.5265	1	0	0	0	0	4	12	44	108	112
49	12	23	1	8	0.0698	1	8	24	36	56	144	228	192	316	652
50	12	23	1	4	0.0735	1	4	16	48	88	152	204	144	280	628
51	12	23	3	12	0.5690	1	0	0	12	0	0	60	0	0	172

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
52	16	3	2	16	1.4585	1	0	16	128	304	1408	6864	19584	47600	112768
53	16	3	2	12	1.6669	1	0	12	48	440	1808	6332	18864	47648	113968
54	16	3	2	8	1.7612	1	0	8	48	416	1808	6440	18864	48016	113968
55	16	3	2	4	1.8303	1	0	4	64	360	1728	6676	19008	48448	113728
56	16	5	2	2	1.7671	1	0	2	4	72	216	884	2452	6432	14520
57	16	5	4	240	1.6822	1	0	0	0	240	0	480	0	15600	0
58	16	5	4	112	1.9213	1	0	0	0	112	0	1248	2048	5872	16384
59	16	5	4	64	1.9855	1	0	0	0	64	192	864	2432	6448	14656
60	16	5	4	48	2.0079	1	0	0	0	48	256	736	2560	6640	14080
61	16	6	2	16	0.8582	1	0	16	16	112	256	560	1792	2928	7616
62	16	6	3	18	1.5662	1	0	0	18	44	122	392	1050	2896	7126
63	16	6	3	8	1.7693	1	0	0	8	32	124	376	1112	3000	7156
64	16	6	3	8	1.8272	1	0	0	8	16	120	448	1128	2992	7176
65	16	7	3	32	1.2206	1	0	0	32	32	32	416	768	1216	3648
66	16	7	3	6	1.7604	1	0	0	6	12	74	252	560	1536	3968
67	16	7	3	2	1.8381	1	0	0	2	16	86	212	496	1556	4072
68	16	11	3	16	1.0985	1	0	0	16	0	16	176	96	192	1072
69	16	11	3	16	1.1138	1	0	0	16	0	12	164	100	240	1092
70	16	14	3	16	0.8864	1	0	0	16	0	0	128	64	96	640
71	16	14	3	16	0.8933	1	0	0	16	0	0	124	52	100	676
72	16	15	4	6	1.5187	1	0	0	0	6	10	22	54	78	182
73	16	15	4	4	1.6192	1	0	0	0	4	4	34	40	74	182
74	16	15	4	4	1.7660	1	0	0	0	4	0	14	24	134	156
75	16	15	4	2	1.8018	1	0	0	0	2	4	10	38	84	208
76	16	15	5	4	1.9146	1	0	0	0	0	4	8	26	100	178
77	16	15	5	4	1.9344	1	0	0	0	0	4	4	36	74	170
78	16	15	5	2	1.8890	1	0	0	0	0	2	16	42	70	160
79	16	23	3	16	0.4715	1	0	0	16	0	0	112	0	0	464
80	16	23	3	16	0.4720	1	0	0	16	0	0	112	0	0	460

Observations

- Take take $\tau = i/\sqrt{l}$ the numerator of secrecy function is

$$\Theta_{\sqrt[4]{l}\mathbb{Z}^n}(\frac{i}{\sqrt{l}}) = \sum_{x \in \sqrt[4]{l}\mathbb{Z}^n} q^{||x||^2} = \sum_{x \in \mathbb{Z}^n} q^{\sqrt{l}||x||^2}$$

$$= \sum_{x \in \sqrt[4]{l}\mathbb{Z}^n} q^{||x||^2} = \sum_{x \in \mathbb{Z}^n} e^{\pi \cdot i \cdot i \cdot \frac{1}{\sqrt{l}} \cdot \sqrt{l}||x||^2} = \sum_{x \in \mathbb{Z}^n} e^{-\pi||x||^2},$$

which is a constant. The denominator is

$$\Theta_L(\frac{i}{\sqrt{l}}) = \sum_{x \in L} q^{||x||^2} = \sum_{x \in L} e^{\pi \cdot i \cdot i \cdot \frac{1}{\sqrt{l}} \cdot ||x||^2}$$

$$= \sum_{x \in L} e^{-\frac{\pi}{\sqrt{l}}||x||^2} = \sum_{m \in \mathbb{Z}_{\geq 0}} A_m \left(e^{-\frac{\pi}{\sqrt{l}}}\right)^m,$$

where A_m is the number of vectors in L with norm m.

Observations

- Hence the denominator can be viewed as a power series in $e^{-\frac{\pi}{\sqrt{l}}}$, which is a positive real number less than 1. Then the following will be preferable for achieving a large weak secrecy gain.

Observations

- Hence the denominator can be viewed as a power series in $e^{-\frac{\pi}{\sqrt{l}}}$, which is a positive real number less than 1. Then the following will be preferable for achieving a large weak secrecy gain.
- Large minimum, which determines the lowest power of $e^{-\frac{\pi}{\sqrt{l}}}$ in the power series.

Observations

- Hence the denominator can be viewed as a power series in $e^{-\frac{\pi}{\sqrt{l}}}$, which is a positive real number less than 1. Then the following will be preferable for achieving a large weak secrecy gain.
- Large minimum, which determines the lowest power of $e^{-\frac{\pi}{\sqrt{l}}}$ in the power series.
- Small value of A_m, i.e., small kissing number.

Observations

- Hence the denominator can be viewed as a power series in $e^{-\frac{\pi}{\sqrt{l}}}$, which is a positive real number less than 1. Then the following will be preferable for achieving a large weak secrecy gain.
- Large minimum, which determines the lowest power of $e^{-\frac{\pi}{\sqrt{l}}}$ in the power series.
- Small value of A_m, i.e., small kissing number.
- Small value of l, so that $e^{-\frac{\pi}{\sqrt{l}}}$ is small.

Observations

- Hence the denominator can be viewed as a power series in $e^{-\frac{\pi}{\sqrt{l}}}$, which is a positive real number less than 1. Then the following will be preferable for achieving a large weak secrecy gain.
- Large minimum, which determines the lowest power of $e^{-\frac{\pi}{\sqrt{l}}}$ in the power series.
- Small value of A_m, i.e., small kissing number.
- Small value of l, so that $e^{-\frac{\pi}{\sqrt{l}}}$ is small.
- However, from the three tables, the minimum seems to be more dominant than other factors.

No.	Dim	d	μ_L	ks	χ_L^W	Θ_L									
69	16	11	3	16	1.1138	1	0	0	16	0	12	164	100	240	1092
68	16	11	3	16	1.0985	1	0	0	16	0	16	176	96	192	1072
71	16	14	3	16	0.8933	1	0	0	16	0	0	124	52	100	676
70	16	14	3	16	0.8864	1	0	0	16	0	0	128	64	96	640
80	16	23	3	16	0.4720	1	0	0	16	0	0	112	0	0	460
79	16	23	3	16	0.4715	1	0	0	16	0	0	112	0	0	464

Figure: Dimension 16 Construction A latices from number fields

References

- J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*. New York: Springer, 1998.
- I. N. Stewart and D. O. Tall, *Algebraic Number Theory*. Chapman and Hall, 1979.
- S. Lang, *Algebraic Number Theory*. Springer-Verlag, 1994.
- F. Oggier and E. Viterbo, "Algebraic number theory and code design for rayleigh fading channels," *Found. Trends Commun. Inform. Theory*, vol. 1, no. 3, pp. 333–415, 2004.
- L. H. Ozarow, S. Shamai, and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. on Vehicular Technology*, vol. 43, no. 2, pp. 359–378, May 1994.
- W. Kositwattanarerk, S. S. Ong, and F. Oggier, "Construction A of lattices over number fields and block fading (wiretap) coding," *IEEE Trans. on Inform. Theory*, vol. 61, no. 5, pp. 2273–2282, May 2015.
- E. Bayer-Fluckiger and I. Suarez, Modular lattices over cyclotomic fields, *J. of Number Theory* **114**(2) (2005) 394–411.

J.-C. Belfiore and F. Oggier, Secrecy gain: a wiretap lattice code design, in *International Symposium on Inform. Theory and its Applications (ISITA)* (2010), pp. 174–178.

J.-C. Belfiore and F. Oggier, Lattice code design for the Rayleigh fading wiretap channel, in *IEEE International Conference on Commun. Workshops (ICC)* (2011), pp. 1–5.

J.-C. Belfiore and P. Solé, Unimodular lattices for the Gaussian wiretap channel, in *IEEE Inform. Theory Workshop (ITW)* (2010), pp. 1–5.

A.-M. Ernvall-Hytönen and B. A. Sethuraman, Counterexample to the generalized Belfiore-Solé secrecy function conjecture for ℓ-modular lattices, in *IEEE International Symposium on Inform. Theory (ISIT)* (2015), pp. 2466–2469.

F. Lin and F. Oggier, Gaussian wiretap lattice codes from binary self-dual codes, in *IEEE Inform. Theory Workshop (ITW)* (2012), pp. 662–666.

F. Lin and F. Oggier, Secrecy gain of Gaussian wiretap codes from 2-and 3-modular lattices, in *IEEE International Symposium on Inform. Theory (ISIT)* (2012) pp. 1747–1751.

F. Lin and F. Oggier, A classification of unimodular lattice wiretap codes in small dimensions, *IEEE Trans. on Inform. Theory* **59**(6) (2013) 3295–3303.

F. Lin, F. Oggier and P. Solé, 2- and 3-modular lattice wiretap codes in small dimensions, *AAECC* **26**(6) (2015) 571–590.

Thank You!