A Função de Sigilo de Reticulados Bi-dimensionais

Giselle Strey e Antonio Campello

***Resumo*— A série teta de um reticulado nos fornece várias informações valiosas de um reticulado, como o seu raio de empacotamento, o seu *kissing number* e a sua densidade. O objetivo deste trabalho é estudar as séries teta e suas aplicações em Segurança da Informação. Motivados pelo canal com escuta gaussiano, consideramos o problema de minimizar a probabilidade de um intruso decodificar corretamente uma mensagem enviada por um usuário para um receptor legítimo. Essa probabilidade é limitada pela função de sigilo, intrinsecamente associada à série teta. Neste trabalho estudamos a otimização da função de sigilo de reticulados l-modulares, em particular bi-dimensionais, e problemas analíticos associados.**

***Palavras-Chave*— Série teta, Função de sigilo, Reticulado.**

I. Introdução

A série teta de um reticulado é uma estrutura matemática importante com aplicações em Teoria dos Números e Comunicação. Ela nos fornece várias informações valiosas de um reticulado, como o seu raio de empacotamento, o seu *kissing number* e a sua densidade.

O objetivo deste trabalho é estudar as séries teta, tendo como motivação a função de sigilo, definida no contexto de Segurança da Informação em [1]. A partir de um canal gaussiano com escuta (*Gaussian wiretap channel*), visamos minimizar a probabilidade de um intruso decodificar corretamente uma mensagem enviada por um usuário para um receptor legítimo. No esquema proposto em [1], e subsequentemente analisado em [7], [8], essa probabilidade é limitada pela *função de sigilo*, um parâmetro intrinsecamente relacionado à série teta do reticulado utilizado para a codificação (descrevemos estas relações com mais detalhes na Seção IV). Estudamos aqui problemas analíticos de minimização envolvendo a função de sigilo e a série teta, em especial, as conjecturas propostas em [8]. Essas conjecturas estão relacionadas com a busca do melhor código para o canal gaussiano com escuta.

Consideramos construções algébricas de reticulados, via Homomorfismo de Minkowski [9]. Faremos um estudo sobre os pontos críticos da função de sigilo de reticulados l-modulares. Vamos também caracterizar a série teta e a função de sigilo de reticulados l-modulares construídos via corpos quadráticos e analisar nestes reticulados a validade da conjectura feita por Belfiore, Oggier e Solé em [8].

Vale notar que grande parte dos códigos propostos para o canal gaussiano com escuta são construídos a partir de reticulados uni ou bi-dimensionais e então estendidos para dimensões maiores via produto tensorial [6]. Os reticulados aqui analisados podem ser vistos, portanto, como elementos de base para possíveis extensões e análises futuras de códigos em dimensão mais alta.

Departamento de Matemática Aplicada, IMECC-Unicamp, Campinas-SP, Brasil. E-mails: ra154119@ime.unicamp.br, campello@ime.unicamp.br.

Este artigo está organizado da seguinte forma: na Seção II apresentaremos algumas definições e propriedades iniciais de reticulados. Na Seção III introduziremos o conceito da série teta. Na Seção IV apresentaremos o canal gaussiano com escuta e a função de sigilo, e demonstraremos uma proposição sobre o ponto crítico de reticulados l-modulares. Na Seção V introduziremos o conceito de construções de reticulados via corpos quadráticos. Na seção VI apresentaremos os conceitos de reticulados via corpos de números e na seção VII analisaremos a função de sigilo de reticulados algébricos, construídos por corpos quadráticos.

II. Conceitos Preliminares

Um reticulado Λ é um subgrupo aditivo e discreto de $\mathbb{R}^n$. Em [2] vemos que Λ pode ser descrito em termos de uma matriz geradora M de dimensão $m \times n$ e posto m da seguinte forma:

$$\Lambda := \{\boldsymbol{x} = \boldsymbol{u}M : \boldsymbol{u} \in \mathbb{Z}^m\},$$

em que

$$M = \begin{pmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{m1} & \cdots & v_{mn} \end{pmatrix}.$$

Os vetores linha $\boldsymbol{v}_i = (v_{i1}, \ldots, v_{in})$ formam uma base para o reticulado Λ. O número de vetores de uma base do reticulado é chamado de dimensão ou posto do reticulado. Quando $m = n$, dizemos que Λ possui posto completo. A matriz $G = MM^T$ é chamada de matriz de Gram do reticulado. O determinante do reticulado Λ, denotado por $\det \Lambda$ é definido como o determinante da matriz de Gram, isto é, $\det \Lambda = \det G$.

A soma direta de dois reticulados $\Lambda_1 \subset \mathbb{R}^n$ e $\Lambda_2 \subset \mathbb{R}^m$ é dada por $\Lambda_1 \oplus \Lambda_2 \subset \mathbb{R}^{n+m}$ tal que

$$\Lambda_1 \oplus \Lambda_2 = \{(u, v) : \boldsymbol{u} \in \Lambda_1 \text{ e } \boldsymbol{v} \in \Lambda_2\}.$$

Dados dois vetores $\boldsymbol{x} = (x_1, \ldots, x_n)$ e $\boldsymbol{y} = (y_1, \ldots, y_n)$ em $\mathbb{R}^n$, definimos o produto interno de $\boldsymbol{x}$ e $\boldsymbol{y}$ como $\boldsymbol{x} \cdot \boldsymbol{y} = x_1y_1 + \cdots + x_ny_n$. Temos também que $\boldsymbol{x} \cdot \boldsymbol{x} = \|\boldsymbol{x}\|^2$.

O reticulado dual de Λ é definido como

$$\Lambda^* := \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{x} \cdot \boldsymbol{y} \in \mathbb{Z}, \forall \boldsymbol{y} \in \Lambda\}. \quad (1)$$

Um reticulado Λ é dito *integral* se $\boldsymbol{x} \cdot \boldsymbol{y} \in \mathbb{Z}$, para quaisquer $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$.

Uma similaridade σ é uma aplicação linear de $\mathbb{R}^n \to \mathbb{R}^n$ que satisfaz

$$\sigma(\boldsymbol{x}) \cdot \sigma(\boldsymbol{y}) = c\boldsymbol{x} \cdot \boldsymbol{y}, \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$$

para algum $c \in \mathbb{R}$. Neste caso, dizemos que a similaridade tem norma c.

Um reticulado integral Λ é dito l-modular se existir uma similaridade σ de norma $l \in \mathbb{R}_+$ tal que $\sigma(\Lambda^*) = \Lambda$.

Denotamos $\Lambda^* \sim \sqrt{l}\Lambda$. Quando $l = 1$, chamamos o reticulado de unimodular.

III. A Série Teta

Definição 1: Seja Λ um reticulado em $\mathbb{R}^n$. Definimos a série teta de Λ como

$$\Theta_\Lambda(q) := \sum_{\boldsymbol{x}\in\Lambda} q^{\boldsymbol{x}\cdot\boldsymbol{x}} \tag{2}$$

onde $z \in \mathbb{C}$, $q = e^{\pi i z}$ e $Im(z) > 0$.

Na literatura é usual encontrar a série teta escrita em função de z, isto é, $\Theta_\Lambda(z)$, como podemos ver em [3] e [2], e no decorrer do trabalho utilizaremos essa notação.

De maneira análoga, define-se a série teta de translações de um reticulado Λ por um vetor $\boldsymbol{v}$ como

$$\Theta_{\Lambda+\boldsymbol{v}}(z) := \sum_{\boldsymbol{x}\in\Lambda+\boldsymbol{v}} q^{\boldsymbol{x}\cdot\boldsymbol{x}} \tag{3}$$

A série teta de um reticulado converge uniformemente e absolutamente para todo $z \in \mathbb{C}$, com $Im(z) > 0$ (ver [3]).

Diversas séries teta de interesse podem ser escritas em função das séries *teta de Jacobi*. Estas são $\theta_2(z)$ e $\theta_3(z)$, definidas como:

$$\theta_2(z) := \sum_{n=-\infty}^{+\infty} q^{(n+\frac{1}{2})^2} \text{ e } \theta_3(z) := \sum_{n=-\infty}^{+\infty} q^{n^2}. \tag{4}$$

Temos também o seguinte resultado que relaciona a série teta de um reticulado com a série teta de seu dual:

Lema 1: (Fórmula da Soma de Poisson para Reticulados). [3] Seja Λ um reticulado em $\mathbb{R}^n$. Então,

$$\Theta_{\Lambda^*}(z) = det(\Lambda)^{1/2}(i/z)^{n/2}\Theta_\Lambda(-1/z). \tag{5}$$

IV. O Canal Gaussiano com Escuta

Em [8] foi apresentado um esquema de codificação em reticulados para o canal gaussiano com escuta. O sistema de transmissão encontra-se ilustrado no diagrama de blocos da Figura 1. Um transmissor (Bob) visa enviar uma mensagem a um receptor legítimo (Alice) através de um canal gaussiano com variância do ruído igual a σ_b^2. Neste processo, um intruso (Eva) recebe uma versão distorcida da mensagem, através de um canal gaussiano com variância σ_e^2. Assume-se que o canal do intruso é mais ruidoso que o legítimo, isto é, $\sigma_e^2 > \sigma_b^2$. O objetivo é maximizar (minimizar) a probabilidade de decisão correta do usuário legítimo (intruso). No esquema proposto em [8], escolhem-se dois reticulados aninhados, $\Lambda_e \subset \Lambda_b \subset \mathbb{R}^n$, e um conjunto de mensagens $\{1, 2, \ldots, M\}$ é mapeado em representantes do quociente Λ_b/Λ_e. A mensagem enviada $\mathbf{x} \in \Lambda_b$ é composta por $\mathbf{x} = \mathbf{c}+\mathbf{r}$, em que $\mathbf{c}$ é um representante do quociente, e $\mathbf{r}$ é um ponto em Λ_e escolhido aleatoriamente, para gerar confusão no intruso.

Demonstrou-se em [8] que a probabilidade de decisão correta do receptor ilegítimo é limitada superiormente por

$$P_{c,e} \leq \frac{1}{(\sqrt{2\pi}\sigma_e)^n}\det(\Lambda_b)^{1/2}\sum_{\boldsymbol{t}\in\Lambda_e} e^{-\|\boldsymbol{t}\|^2/2\sigma_e^2} \tag{6}$$

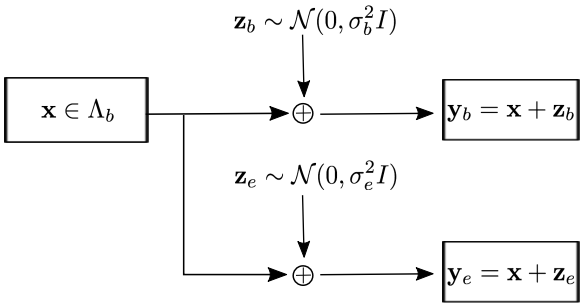

Fig. 1. Sistema de codificação em reticulados para o canal gaussiano com escuta

enquanto a taxa (eficiência) do código, em bits, é a quantidade de possíveis mensagens por dimensão, isto é, $1/n \log_2 |\Lambda_b/\Lambda_e|$.

Desejamos minimizar a probabilidade do intruso decodificar corretamente a mensagem enviada pelo usuário, que é equivalente a minimizar (6), isto é, encontrar um reticulado Λ_b tão bom quanto possível para o canal gaussiano, e que contém o sub-reticulado Λ_e tal que

$$\text{minimize} \quad \sum_{\boldsymbol{t}\in\Lambda_e} e^{-\|\boldsymbol{t}\|^2/2\sigma_e^2}, \tag{7}$$

$$\text{sujeito a} \quad \log_2 |\Lambda_b/\Lambda_e| = k. \tag{8}$$

De (7), precisamos minimizar

$$\sum_{\boldsymbol{t}\in\Lambda_e} e^{-\|\boldsymbol{t}\|^2/2\sigma_e^2} = \sum_{\boldsymbol{t}\in\Lambda_e} \left(e^{-1/2\sigma_e^2}\right)^{\|\boldsymbol{t}\|^2} \tag{9}$$

$$= \sum_{\boldsymbol{t}\in\Lambda_e} \left((e^{\pi i})^{-1/2i\pi\sigma_e^2}\right)^{\|\boldsymbol{t}\|^2} \tag{10}$$

$$= \Theta_{\Lambda_e}\left(z = \frac{-1}{2i\pi\sigma_e^2}\right). \tag{11}$$

em que $q = e^{\pi i z}$ e

$$Im\left(\frac{-1}{2i\pi\sigma_e^2}\right) = Im\left(\frac{i}{2\pi\sigma_e^2}\right) > 0.$$

Assim, minimizar a probabilidade do intruso de decodificar corretamente é equivalente a minimizar a série teta de Λ_e, com $z = \frac{i}{2\pi\sigma_e^2}$.

Para abordar esse problema, vamos tomar $y = -iz$ e restringir os valores reais positivos de y, de modo que

$$\Theta_{\Lambda_e}(y) = \sum_{\boldsymbol{t}\in\Lambda_e} q^{\boldsymbol{t}\cdot\boldsymbol{t}}, q = e^{-\pi i z}, y > 0. \tag{12}$$

sobre todo Λ_e, onde $y = \frac{1}{2\pi\sigma_e^2}$.

Definição 2: Seja Λ um reticulado n-dimensional com volume λ^n. A função de sigilo de Λ é dada por

$$\Xi_\Lambda(y) = \frac{\Theta_{\lambda\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)}, \tag{13}$$

para $y > 0$.

À luz da Equação (6), a função de sigilo compara a segurança de um sistema sem codificação (isto é, se assumíssemos $\Lambda_e = \mathbb{Z}^n$) e um sistema codificado com o reticulado Λ_e. Para realizarmos a comparação, é necessário

aplicar um fator de escala ($\lambda = |det(MM^T)|^{1/n}$), de modo que ambos os reticulados tenham o mesmo volume. Nosso interesse é calcular a função de sigilo no ponto $y = \frac{1}{2\pi\sigma_e^2}$. Podemos alternativamente, fixar um reticulado Λ_e e considerarmos σ_e^2 como uma variável. Desta maneira, minimizar a expressão da probabilidade do intruso decodificar corretamente em (6) é equivalente a maximizar a função de sigilo, para $y > 0$.

V. Função de Sigilo para Reticulados l-modulares

Nesse contexto da função de sigilo, Belfiore, Oggier e Solé conjecturaram em [8] o seguinte resultado:

Conjectura 1: [8] A função de sigilo de reticulados l-modulares atinge o máximo em $y = \frac{1}{\sqrt{l}}$.

Um exemplo da conjectura é o reticulado 3-modular $\sqrt{2}\Lambda_3$, definido na Seção VII. Sua função de sigilo possui ponto de máximo em $y = \frac{1}{\sqrt{3}}$, como é esperado pela conjectura. Na Figura 2 podemos observar o gráfico da função de sigilo do reticulado $\sqrt{2}\Lambda_3$.

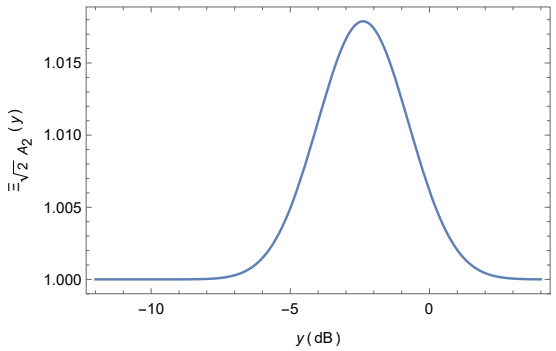

Fig. 2. Função de sigilo do reticulado $\sqrt{2}\Lambda_3$.

Em [5] foi demonstrado que a função de sigilo do reticulado 4-modular $C^{(4)} = \mathbb{Z} \oplus \sqrt{2}2\mathbb{Z} \oplus 2\mathbb{Z}$ possui ponto de mínimo em $y = \frac{1}{2}$, provando assim que a Conjectura 1 é falsa.

Utilizando a Fórmula da Soma de Poisson para reticulados, mostramos os seguintes resultados para a função de sigilo de reticulados l-modulares. As demonstrações do caso $l = 1$ podem ser encontradas em [8], Proposição 1, pág.18. Abaixo, generalizamos essa proposição para qualquer $l \geq 1$.

Proposição 1: A função de sigilo de um reticulado l-modular possui ponto de simetria multiplicativo em $y = \frac{1}{l}$, isto é, $\Xi_\Lambda(y) = \Xi_\Lambda(1/ly)$.

Demonstração: Seja Λ um reticulado l-modular, isto é, $\Lambda^* \sim \sqrt{l}\Lambda$. Neste caso $\det \Lambda = l^{n/2}$. Temos que:

$$\Theta_\Lambda(y) = \Theta_{\sqrt{l}\Lambda^*}(y) = \Theta_{\Lambda^*}(ly).$$

Note que, tomando $y = iz$ e depois $z = y$ na Fórmula da Soma de Poisson para reticulados, temos

$$\begin{aligned}\Theta_{\Lambda^*}(y) &= (\det \Lambda)^{1/2}(i/y)^{n/2}\Theta_\Lambda(-1/y) \\ &= |(\det M)| \left(\frac{1}{\sqrt{y}}\right)^n \Theta_\Lambda(1/y).\end{aligned}$$

Logo,

$$\Theta_\Lambda(y) = |(\det M)|^{-1} \left(\frac{1}{\sqrt{y}}\right)^n \Theta_{\Lambda^*}(1/y).$$

Pela fórmula acima, obtemos:

$$\begin{aligned}\Theta_\Lambda(y) &= |(\det M)|^{-1} \left(\frac{1}{\sqrt{y}}\right)^n \Theta_{\Lambda^*}(1/y) \\ &= \frac{1}{(ly)^{n/2}}\Theta_\Lambda(1/ly).\end{aligned}$$

E, de maneira análoga,

$$\Theta_{\mathbb{Z}^n}(ly) = \frac{1}{(ly)^{n/2}}\Theta_{\mathbb{Z}^n}(1/ly).$$

Logo,

$$\begin{aligned}\Xi_\Lambda(y) &= \frac{\Theta_{l\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \frac{\Theta_{\mathbb{Z}^n}(ly)}{\Theta_\Lambda(ly)} \\ &= \frac{(1/ly)^{n/2} \cdot \Theta_{\mathbb{Z}^n}(1/ly)}{(1/ly)^{n/2} \cdot \Theta_\Lambda(1/ly)} \\ &= \frac{\Theta_{\mathbb{Z}^n}(1/ly)}{\Theta_{\Lambda(1/ly)}} = \Xi_\Lambda\left(\frac{1}{ly}\right).\end{aligned}$$

■

Proposição 2: A função de sigilo de um reticulado l-modular Λ possui $y = \frac{1}{\sqrt{l}}$ como ponto crítico.
Demonstração: Temos, pela Proposição 1 que:

$$\Xi_\Lambda(y) = \Xi_\Lambda\left(\frac{1}{ly}\right) \Rightarrow \Xi'_\Lambda(y) = -\frac{1}{ly^2} \cdot \Xi'_\Lambda\left(\frac{1}{ly}\right).$$

Tomando $y = \frac{1}{\sqrt{l}}$, temos:

$$\begin{aligned}\Xi'_\Lambda\left(\frac{1}{\sqrt{l}}\right) &= -\frac{1}{l(1/\sqrt{l})^2} \cdot \Xi'_\Lambda\left(\frac{1}{l}\right) \Rightarrow \Xi'_\Lambda\left(\frac{1}{\sqrt{l}}\right) \\ &= -\Xi'_\Lambda\left(\frac{1}{\sqrt{l}}\right) \Rightarrow \Xi'_\Lambda\left(\frac{1}{\sqrt{l}}\right) = 0.\end{aligned}$$

■

O reticulado $\Lambda = \mathbb{Z} \oplus 2\mathbb{Z}$ possui a mesma função de sigilo do reticulado $C^{(4)}$. Logo possui ponto de mínimo em $y = \frac{1}{2}$. Em meio aos nossos estudos sobre a função de sigilo, chegamos a seguinte conjectura sobre reticulados l-modulares.

Conjectura 2: A função de sigilo de reticulados l-modulares bidimensionais do tipo $\Lambda = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$ atinge o mínimo em $y = \frac{1}{\sqrt{l}}$, para $l > 1$.

Observe no gráfico da Figura 3 uma ilustração da Conjectura 2 para valores de $l = 3, 5$ e 10.

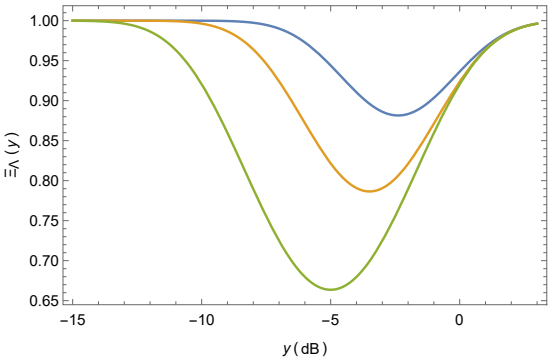

Fig. 3. Função de sigilo de $\Lambda = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$. A curva verde representa o valor $l = 3$, o gráfico laranja representa o valor $l = 5$ e o gráfico azul representa o valor $l = 10$.

VI. Reticulados via Corpos Quadráticos

Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos. Dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$ se $\mathbb{K} \subset \mathbb{L}$. A dimensão do $\mathbb{K}$-espaço vetorial $\mathbb{L}$ é chamada grau da extensão e denotada por $[\mathbb{L} : \mathbb{K}]$. Um corpo de números $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$ e denotamos por $\mathbb{K}(\theta)$ o menor corpo contendo o corpo $\mathbb{Q}$ e o elemento θ. Dizemos que um elemento $\alpha \in \mathbb{K}$ é um inteiro algébrico sobre $\mathbb{Z}$ se α é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$.

Proposição 3: [9] Seja $\mathbb{K}$ um corpo de números. O conjunto

$$\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K} : x \text{ é inteiro algébrico sobre } \mathbb{Z}\}$$

é um anel, chamado de anel de inteiros de $\mathbb{K}$.

Definição 3: Um corpo quadrático $\mathbb{K}$ é uma extensão de $\mathbb{Q}$ de grau 2.

Proposição 4: [9] Todo corpo quadrático $\mathbb{K}$ é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados (isto é, não existe um primo p tal que p^2 divide d), em que $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$.

Sejam $\mathbb{K}$ um corpo quadrático e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$. Chamamos de base integral de $\mathbb{K}$ ou de $\mathcal{O}_{\mathbb{K}}$ uma $\mathbb{Z}$-base para o grupo aditivo $\mathcal{O}_{\mathbb{K}}$.

Teorema 1: [10] Se $\mathbb{K} = \mathbb{Q}(\theta)$ é uma extensão de $\mathbb{Q}$ de grau 2, então existem exatamente 2 homomorfismos distintos $\{\sigma_1, \sigma_2\}$ de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$.

Teorema 2: [9] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com $d \in \mathbb{Z}$ livre de quadrados e $d \not\equiv 0 \pmod 4$.

1) Se $d \equiv 1 \pmod 4$, então o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ sobre $\mathbb{Z}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$, em que $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \{a + b((1+\sqrt{d})/2) : a, b \in \mathbb{Z}\}$;
2) Se $d \equiv 2$ ou $d \equiv 3 \pmod 4$, então o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ sobre $\mathbb{Z}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é $\{1, \sqrt{d}\}$, em que $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$.

Proposição 5: [10] Seja d um inteiro livre de quadrados. Os homomorfismos de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ em $\mathbb{C}$ são dados por $\{\sigma_1, \sigma_2\}$, onde $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$.

A. Homomorfismo de Minkowski

Seja $\mathbb{K}$ um corpo de números de grau 2. Pelo Teorema 1 temos que existem exatamente 2 homomorfismos distintos $\sigma_j : \mathbb{K} \longrightarrow \mathbb{C}$ para $j = 1, 2$, que fixam $\mathbb{Q}$. Se $\sigma_j(\mathbb{K}) \subset \mathbb{R}$ diz-se que σ_j é real. Caso contrário, σ_j é dito imaginário. Quando todos os homomorfismos são reais diz-se que $\mathbb{K}$ é um corpo totalmente real e quando os homomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um corpo totalmente imaginário.

Definição 4: Seja $\mathbb{K}$ um corpo de números de grau 2. Considere o homomorfismo injetivo de anéis $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^2$ dado por $\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \sigma_2(x))$, se o corpo for totalmente real, e $\sigma_{\mathbb{K}}(x) = (\mathcal{R}(\sigma_1(x)), \mathcal{I}(\sigma_1(x)))$, se o corpo for totalmente complexo, onde $\mathcal{R}$ representa a parte real e $\mathcal{I}$ representa a parte imaginária do número complexo. Tal homomorfismo é chamado de homomorfismo canônico ou homomorfismo de Minkowski.

Proposição 6: [10] Sejam $\mathbb{K}$ um corpo de números de grau 2 e $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^2$ o homomorfismo de Minkowski. Então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é um reticulado de posto 2 em $\mathbb{R}^2$.

Exemplo 1: Considere o corpo de números $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ o anel de inteiros sobre $\mathbb{K}$ e $\{\sigma_1, \sigma_2\}$ os homomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde σ_1 é a identidade e $\sigma_2(a + \sqrt{5}b) = a - \sqrt{5}b$. Usando a Proposição 6 obtemos o reticulado bidimensional Λ gerado pelos vetores $\mathbf{u} = (1, 1)$ e $\mathbf{v} = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$. Na figura 4 temos uma ilustração do reticulado Λ.

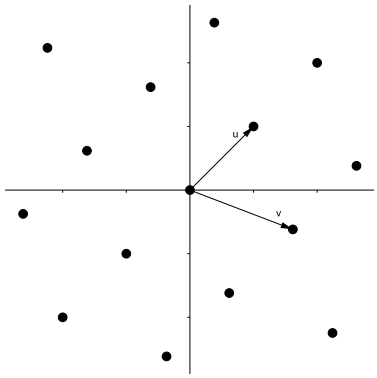

Fig. 4. Reticulado construído via corpo de números $\mathbb{K} = \mathbb{Q}(\sqrt{5})$.

VII. Função de Sigilo de Reticulados Algébricos

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{l})$ um corpo quadrático, onde l é um inteiro livre de quadrados. Usando o Teorema 2 e as Proposições 5 e 6, vamos gerar reticulados, calcular sua função de sigilo e assim verificar a validade da Conjectura 1.

Aqui, vamos analisar os casos de congruência módulo 4 quando $l > 0$ e $l < 0$.

Pelo Teorema 2, se $l > 0$ e $l \equiv 1 \pmod 4$, o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ sobre $\mathbb{Z}$ é igual a $\mathbb{Z}\left[\frac{1+\sqrt{l}}{2}\right]$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é $\left\{1, \frac{1+\sqrt{l}}{2}\right\}$. Aqui o corpo é totalmente real. Usando as Proposições 5 e 6, temos que o reticulado Λ_1 gerado por essa base possui matriz geradora e matriz de Gram, respectivamente,

$$M_1 = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{l}}{2} & \frac{1-\sqrt{l}}{2} \end{pmatrix} \text{ e } G_1 = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+l}{2} \end{pmatrix}.$$

Se $l > 0$ e $l \equiv 2$ ou $l \equiv 3 \pmod 4$, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ sobre $\mathbb{Z}$ é igual a $\mathbb{Z}[\sqrt{l}]$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é $\{1, \sqrt{l}\}$. O corpo é totalmente real. Usando as Proposições 5 e 6, temos que o reticulado Λ_2 gerado por essa base possui matriz geradora e matriz de Gram, respectivamente,

$$M_2 = \begin{pmatrix} 1 & 1 \\ \sqrt{l} & -\sqrt{l} \end{pmatrix} \text{ e } G_2 = \begin{pmatrix} 2 & 0 \\ 0 & 2l \end{pmatrix}.$$

Pelo Teorema 2, se $l < 0$ e $l \equiv 1 \pmod 4$, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ sobre $\mathbb{Z}$ é igual a $\mathbb{Z}\left[\frac{1+\sqrt{l}}{2}\right]$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é $\left\{1, \frac{1+\sqrt{l}}{2}\right\}$. Aqui o corpo é totalmente complexo.

Usando as Proposições 5 e 6, temos que

$$\begin{aligned}\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) &= (\mathcal{R}(\sigma_1(\mathcal{O}_{\mathbb{K}})), \mathcal{I}(\sigma_1(\mathcal{O}_{\mathbb{K}}))) \\ &= a_0(1,0) + a_1\left(\frac{1}{2}, \frac{\sqrt{l}}{2}\right).\end{aligned}$$

Logo, temos que $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é gerado pelos vetores $\boldsymbol{u} = (1,0)$ e $\boldsymbol{v} = \left(\frac{1}{2}, \frac{\sqrt{l}}{2}\right)$. Vamos tomar $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) = \Lambda_3$. Vamos trabalhar com $\sqrt{2}\Lambda_3$, um reticulado integral. Sua matriz geradora e de Gram são, respectivamente:

$$M_3 = \sqrt{2}\begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{l}}{2} \end{pmatrix} \text{ e } G_3 = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+l}{2} \end{pmatrix}.$$

Se $l < 0$ $l \equiv 2$ ou $l \equiv 3 \pmod 4$, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ sobre $\mathbb{Z}$ é igual a $\mathbb{Z}[\sqrt{l}]$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é $\{1, \sqrt{l}\}$. Neste caso o corpo é totalmente complexo. Usando as Proposições 5 e 6, temos que

$$\begin{aligned}\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) &= (\mathcal{R}(\sigma_1(\mathcal{O}_{\mathbb{K}})), \mathcal{I}(\sigma_1(\mathcal{O}_{\mathbb{K}}))) \\ &= a_0(1,0) + a_1(0, \sqrt{l}).\end{aligned}$$

Logo, $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é gerado pelos vetores $\boldsymbol{u} = (1,0)$ e $\boldsymbol{v} = (0, \sqrt{l})$. Vamos tomar $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) = \Lambda_4$. Sua matriz geradora e matriz de Gram são, respectivamente,

$$M_4 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{l} \end{pmatrix} \text{ e } G_4 = \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}.$$

Note que $\Lambda_4 = \Lambda = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$.

Os reticulados $\Lambda_1, \sqrt{2}\lambda_3$ e Λ_4 são l-modulares e o reticulado Λ_2 é $4l$-modular.

Temos que a série teta e a função de sigilo de $\Lambda_1, \Lambda_2, \sqrt{2}\Lambda_3$ e Λ_4 são, respectivamente,

$$\Theta_{\Lambda_1}(y) = \theta_3(2y)\theta_3(2ly) + \theta_2(2y)\theta_2(2ly) \quad (14)$$

$$\Xi_{\Lambda_1}(y) = \frac{\theta_3(\sqrt{l}y)^2}{\theta_3(2y)\theta_3(2ly) + \theta_2(2y)\theta_2(2ly)} \quad (15)$$

$$\Theta_{\Lambda_2}(y) = \theta_3(2y)\theta_3(2ly) \quad (16)$$

$$\Xi_{\Lambda_2}(y) = \frac{\theta_3(2\sqrt{l}y)^2}{\theta_3(2y)\theta_3(2ly)} \quad (17)$$

$$\Theta_{\sqrt{2}\Lambda_3}(y) = \theta_3(2y)\theta_3(2ly) + \theta_2(2y)\theta_2(2ly) \quad (18)$$

$$\Xi_{\sqrt{2}\Lambda_3}(y) = \frac{\theta_3(\sqrt{l}y)^2}{\theta_3(2y)\theta_3(2ly) + \theta_2(2y)\theta_2(2ly)} \quad (19)$$

$$\Theta_{\Lambda_4}(y) = \theta_3(y)\theta_3(ly) \quad (20)$$

$$\Xi_{\Lambda_4}(y) = \frac{\theta_3(\sqrt{l}y)^2}{\theta_3(y)\theta_3(ly)} \quad (21)$$

Vamos mostrar a título de exemplo a equação (14), que é igual a equação (18). As demais são análogas.

$\Theta_{\Lambda_1}(y) = \sum_{x_1,x_2\in\mathbb{Z}} q^{2\left(x_1+\frac{x_2}{2}\right)^2+\frac{l}{2}x_2^2}$

- Para $x_2 = 2k$ par,

$$\sum_{x_1,x_2\in\mathbb{Z}} q^{2\left(x_1+\frac{x_2}{2}\right)^2+\frac{l}{2}x_2^2} = \sum_{x_1\in\mathbb{Z}}\sum_{k\in\mathbb{Z}} q^{2(x_1+k)^2} q^{2lk^2}.$$

Fazendo $r = x_1 + k$, temos:

$$\sum_{r\in\mathbb{Z}}\sum_{k\in\mathbb{Z}} q^{2(r)^2} q^{2lk^2} = \theta_3(2y)\theta_3(2ly)$$

- Para $x_2 = 2k+1$ ímpar,

$$\sum_{x_1,x_2\in\mathbb{Z}} q^{2\left(x_1+\frac{x_2}{2}\right)^2+\frac{l}{2}x_2^2} = \sum_{x_1\in\mathbb{Z}}\sum_{k\in\mathbb{Z}} q^{2\left(x_1+k+\frac{1}{2}\right)^2+2l\left(k+\frac{1}{2}\right)^2}$$

Fazendo $r = x_1 + k$, temos:

$$\sum_{r\in\mathbb{Z}} q^{2\left(r+\frac{1}{2}\right)^2}\sum_{k\in\mathbb{Z}} q^{2l\left(k+\frac{1}{2}\right)^2} = \theta_2(2y)\theta_2(2ly).$$

Logo, $\Theta_{\Lambda_1}(y) = \theta_3(2y)\theta_3(2ly) + \theta_2(2y)\theta_2(2ly)$.

A partir das relações que obtivemos das famílias de reticulados Λ, Λ_1, Λ_2, $\sqrt{2}\Lambda_3$ e Λ_4 temos a Tabela I:

Família de Reticulados	Ponto de máximo global	Ponto de mínimo global
Λ	-	$y = \frac{1}{\sqrt{l}}$, $\forall l \in \mathbb{N}^* \setminus \{1\}$
Λ_1	$y = \frac{1}{\sqrt{l}}$ em $l = 5$	$y = \frac{1}{\sqrt{l}}$ em $l = 13, 17$ e 21
Λ_2	-	$y = \frac{1}{2\sqrt{l}}$ em $l = 3, 7, 11, 15, 19$ e 23
$\sqrt{2}\Lambda_3$	$y = \frac{1}{\sqrt{l}}$ em $l = 3$	$y = \frac{1}{\sqrt{l}}$ em $l = 7, 11, 15, 19$ e 23
Λ_4	-	$y = \frac{1}{\sqrt{l}}$, $l = 5, 13, 17$ e 21

TABELA I

PONTOS DE MÁXIMO E MÍNIMO DA FUNÇÃO DE SIGILO DAS FAMÍLIAS DE RETICULADOS

VIII. CONCLUSÕES

Neste trabalho, fizemos um estudo da função de sigilo de reticulados l-modulares, bem como algumas propriedades e aplicações. Apresentamos a conjectura proposta por Belfiore, Oggier e Solé e testamos a validade dela para algumas classes de reticulados construídos usando o Homomorfismo de Minkowski. Na Tabela I temos o ponto de máximo e de mínimo das famílias de reticulados estudadas. Além disso, apresentamos a Conjectura 2 sobre a função de sigilo de uma classe de reticulados l-modulares e por fim caracterizamos a série teta e a função de sigilo de reticulados bidimensionais obtidos via corpos quadráticos.

Caso a Conjectura 2 aqui proposta confirme-se verdadeira, o único caso em que a Conjectura 1 pode ser válida é $l = 1$ (reticulados unimodulares).

REFERÊNCIAS

[1] J.-C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design", *Information Theory and its Applications (ISITA)*, pp. 174-178, 2010.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 3rd Ed. 1998.

[3] W. Ebeling, , *Lattices and Codes*, Springer Spektrum, Germany, 3rd Ed. 2013.

[4] A.-M. Ernvall-Hytönen, "On a Conjecture by Belfiore and Solé on Some Lattices", *IEEE Transactions on Information Theory*, pp. 5950-5955, v.58, 2012.

[5] A.-M. Ernvall-Hytönen and B. A. Sethuraman, "Counterexample to the Generalized Belfiore-Solé Secrecy Function Conjecture for l-modular lattices", *IEEE International Symposium on Information Theory (ISIT)*, pp. 2466-2469, 2015.

[6] X. Hou, F. Lin and F. Oggier, "Construction and Secrecy Gain of a Family of 5-modular Lattices", *IEEE Information Theory Workshop*, 2014.

[7] F. Lin, F. Oggier, P. Solé, "2- and 3-Modular lattice wiretap codes in small dimensions", *Applicable Algebra in Engineering, Communication and Computing*, pp. 571-590, 2015.

[8] F. Oggier, P. Solé and J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis", available on http://arxiv.org/pdf/1103.4086.pdf, 2013.

[9] P. Samuel, , *Algebraic Theory of Numbers*, Hermann, Paris, 1970.

[10] I. N. Stewart and D. O. Tall, , *Algebraic Number Theory*, Chapman and Hall, London, 1987.