Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

A Função de Sigilo de um Reticulado

Giselle R. A. S. Strey[1]
Instituto de Matemática, Estatística e Computação Científica, UNICAMP, Campinas, SP
Antonio Campello[2]
Instituto de Matemática, Estatística e Computação Científica, UNICAMP, Campinas, SP

1 Introdução

A série teta de um reticulado é uma estrutura matemática importante com várias aplicações em teoria dos números e comunicação. O objetivo deste trabalho é estudar a série teta e suas aplicações em segurança da informação. Motivados pelo canal de 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.

Dado um reticulado Λ em $\mathbb{R}^n$, definimos a série teta de Λ por

$$\Theta_\Lambda(z) = \sum_{\boldsymbol{x}\in\Lambda} q^{\boldsymbol{x}\cdot\boldsymbol{x}}, \tag{1}$$

onde $z \in \mathbb{C}$, $q = e^{\pi i z}$, $Im(z) > 0$, e $\boldsymbol{x}\cdot\boldsymbol{x}$ é o produto interno usual em $\mathbb{R}^n$.

2 Aplicação da série teta

Dados dois reticulados Λ_b e Λ_e aninhados fixos, desejamos calcular a probabilidade do intruso decodificar corretamente a mensagem enviada pelo remetente. Usando um canal de escuta gaussiano, onde temos σ_e^2 como a variância do ruído gaussiano do intruso e σ_b^2 a variância do ruído gaussiano do receptor legítmo, demonstrou-se em [2] que minimizar essa probabilidade, para Λ_b fixo, é equivalente a minimizar $\sum_{\boldsymbol{t}\in\Lambda_e} e^{-\|\boldsymbol{t}\|^2/2\sigma_e^2}$, que é facilmente reconhecida como a série teta de Λ_e, com $z = i/2\pi\sigma_e^2$.

Define-se a função de sigilo de um reticulado n-dimensional Λ com volume λ^n como

$$\Xi_\Lambda(y) = \frac{\Theta_{\lambda\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)}, \text{ para } y > 0. \tag{2}$$

Belfiore, Oggier e Solé conjecturaram em [2] que a função de sigilo de reticulados l-modulares atinge o máximo em $y = \frac{1}{\sqrt{l}}$. Em [1], foi mostrado que a função de sigilo

[1]ra154119@ime.unicamp.br
[2]campello@ime.unicamp.br

do reticulado 4-modular $C^{(4)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus 2\mathbb{Z}$ possui ponto de mínimo em $y = \frac{1}{2}$, contradizendo a conjectura proposta.

Analisando a função de sigilo de alguns reticulados, chegamos à seguinte conjectura.

Conjectura 2.1. *A função de sigilo de reticulados l-modulares bidimensionais do tipo $\Lambda = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$ atinge o mínimo em $y = 1/\sqrt{l}$, para $l > 1$.*

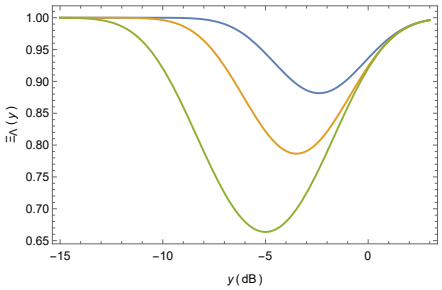

Figura 1: Ilustração da conjectura 2.1 para valores de $l = 3, 5$ e 10.

Estudamos a função de sigilo de reticulados algébricos construídos via Homomorfismo de Minkowski, aplicando-o no anel de inteiros do corpo de números $\mathbb{Q}(\sqrt{l})$, e as comparamos com $\Lambda = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$. Quando $l \equiv 1 (mod\ 4)$ o anel de inteiros sobre $\mathbb{Z}$ é $\mathbb{Z}\left[\frac{1+\sqrt{l}}{2}\right]$ e uma $\mathbb{Z}$-base é $\left\{1, \frac{1+\sqrt{l}}{2}\right\}$. A partir daí, construímos Λ_1 (para $l > 0$, o corpo é totalmente real) e $\sqrt{2}\Lambda_3$ (para $l < 0$, o corpo é totalmente complexo). Quando $l \equiv 3 (mod\ 4)$ o anel de inteiros sobre $\mathbb{Z}$ é $\mathbb{Z}[\sqrt{l}]$ e uma $\mathbb{Z}$-base é $\{1, \sqrt{l}\}$. Construímos então Λ_2 (para $l > 0$, considerando o corpo totalmente real) e Λ_4 (para $l < 0$, considerando o corpo totalmente complexo). Na Tabela 1 temos o valor de máximo e mínimo de cada classe de reticulados.

Família de Reticulados	Modularidade	Ponto de máximo global	Ponto de mínimo global
Λ	l-modular	-	$y = \frac{1}{\sqrt{l}}$, $\forall l \in \mathbb{N}^* \setminus \{1\}$
Λ_1	l-modular	$y = \frac{1}{\sqrt{l}}$ em $l = 5$	$y = \frac{1}{\sqrt{l}}$ em $l = 13, 17$ e 21
Λ_2	$4l$-modular	-	$y = \frac{1}{2\sqrt{l}}$ em $l = 3, 7, 11, 15, 19$ e 23
$\sqrt{2}\Lambda_3$	l-modular	$y = \frac{1}{\sqrt{l}}$ em $l = 3$	$y = \frac{1}{\sqrt{l}}$ em $l = 7, 11, 15, 19$ e 23
Λ_4	l-modular	-	$y = \frac{1}{\sqrt{l}}$, $l = 5, 13, 17$ e 21

Tabela 1: Pontos de máximo e mínimo da Função de Sigilo das famílias de reticulados

Referências

[1] 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*, 2466–2469, 2015.

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