Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Reticulados e Aplicações em Criptografia

Fábio C. C. Meneghetti [1]
IMECC — UNICAMP
Sueli I. R. Costa[2]
IMECC — UNICAMP

1 Introdução

Este trabalho tem por objetivo estudar reticulados, com foco em aplicações a esquemas de criptografia. A importância deste estudo vem do fato que vários métodos de criptografia baseada em reticulados são conjecturados resistentes a ataques em computadores quânticos, uma vez que os métodos mais clássicos são comprovadamente suscetíveis. Criptografia baseada em reticulados é uma das atuais sub-áreas da chamada criptografia pós-quântica, que, independente do advento dos computadores quânticos, visa também uma maior eficiência e segurança nos computadores atuais.

Além do aspecto de segurança, métodos baseados em reticulados têm implementação relativamente simples e, mais recentemente, tornaram-se competitivos do ponto de vista de desempenho. Observamos inclusive que 28 das 82 submissões ao projeto "Post-Quantum Cryptography Standardization" do NIST são baseados em reticulados (2019) [2].

Nosso projeto tem por objetivo estudar os problemas *short integer solution* (SIS) e *learning with errors* (LWE), bem como suas respectivas generalizações para anéis. Dentre as perspectivas estão verificar se a utilização de reticulados gerados por códigos e outros métodos para definir parâmetros de distribuições, podem melhorar a segurança ou a eficiência [5].

2 Reticulados em criptografia

Dado um conjunto linearmente independente de vetores $\beta = \{b_1, \ldots, b_k\}$ em $\mathbb{R}^n$, o *reticulado gerado* por β é o conjunto de todas as combinações lineares inteiras destes:

$$\Lambda = \{\alpha_1 b_1 + \cdots + \alpha_k b_k : \alpha_i \in \mathbb{Z},\ \forall i \in \{1, \ldots, k\}\}. \tag{1}$$

O uso de reticulados em esquemas criptográficos é baseado na NP-dificuldade da resolução de problemas em dimensões altas, como o problema de encontrar o vetor de norma mínima (SVP), e o de encontrar o vetor do reticulado mais próximo de um ponto dado (CVP).

[1] fabiom@riseup.net
[2] sueli@ime.unicamp.br

Por razões técnicas, em vez de CVP e SVP, atualmente utiliza-se dois outros problemas NP-difíceis, redutíveis a problemas em reticulados: SIS, introduzido em 1996 por Ajtai [1] e LWE, introduzido em 2005 por Regev [6]. Estamos particularmente interessados neste último, bem como na sua generalização para anéis (Ring-LWE) [3].

Sejam n, q inteiros positivos, e $s \in \mathbb{Z}_q^n$ um elemento chamado *segredo*. Uma distribuição $A_{s,\psi}$ sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ é denominada *distribuição LWE* se for determinada por amostras

$$(a, b = \langle a, s \rangle + e \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q, \tag{2}$$

onde e é amostrado de uma distribuição de erros ψ sobre $\mathbb{Z}$ e a é escolhido uniformemente em $\mathbb{Z}_q^n$.

O problema LWE consiste em, dadas m amostras da distribuição LWE, descobrir o segredo s. Sua versão decisional consiste em distinguir se, dadas m amostras, estas foram escolhidas usando a distribuição LWE, ou a distribuição uniforme.

Neste trabalho, visamos o estudo de parâmetros que permitam uma maior eficiência e segurança na utilização dos problemas LWE e SIS, tais como o *parâmetro de suavização*, que é (informalmente) a menor quantidade de ruído Gaussiano necessária para "suavizar" a estrutura discreta de um reticulado [4]. Em particular, queremos ver como o uso de noções diferentes de distância entre distribuições alteram este parâmetro.

Agradecimentos

Os autores agradecem os suportes do CNPq (313326/2017-7 e 131290/2018-5) e da FAPESP (13/25977-7).

Referências

[1] M. Ajtai. Generating hard instances of lattice problems (extended abstract), *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing – STOC'96*, pages 99–108, 1996. DOI: 10.1145/237814.237838.

[2] G. Alagic et al. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.IR.8240.

[3] V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors Over Rings, *Advances in Cryptology – EUROCRYPT 2010*, Lecture Notes in Computer Science, Springer-Verlag, volume 6110, pages 1–23, 2010.

[4] J. N. Ortiz. Amostragem Gaussiana aplicada à Criptografia Baseada em Reticulados, Dissertação de Mestrado, UNICAMP, 2016.

[5] C. Peikert. A Decade of Lattice Cryptography, disponível em `https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf`, 2016.

[6] O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography, *Proceedings of the thirty-seventh annual ACM symposium on Theory of Computing – STOC'05*, pages 84–93, 2005. DOI: 10.1145/1060590.1060603.