UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

CÂMPUS TOLEDO

ENGENHARIA DE COMPUTAÇÃO

Graduando: Willian Augusto Soder de Souza

Criptografia pós-quântica baseada em reticulados

Toledo, 2025

1. Introdução

O presente documento tem como objetivo registrar de forma clara e concisa os estudos realizados sobre criptografia pós-quântica baseada em reticulados. Esta área da criptografia tem ganhado destaque por oferecer resistência a ataques realizados por computadores quânticos, baseando-se em problemas matemáticos considerados difíceis mesmo para algoritmos quânticos, como o Shortest Vector Problem (SVP) e o Learning With Errors (LWE).

Serão abordados os principais conceitos, aplicações e algoritmos associados a esse ramo da criptografia, com ênfase na análise e implementação de técnicas como as reduções BKZ , LLL, Gauss Reduction e variantes do problema LWE, como o 1-bit LWE. Estes algoritmos serão discutidos em termos de funcionamento, relevância prática e papel no desenvolvimento de sistemas criptográficos resistentes à computação quântica.

2. Criptografia pós-quântica baseada em reticulados

2.1. O que é a criptografia pós-quântica baseada em reticulados

É um tipo de criptografia que utiliza reticulados, que são um tipo de estrutura matemática, para construir sistemas criptográficos. Em termos simplificados, um reticulado consiste em uma grade infinita no espaço multidimensional, gerada por combinações lineares inteiras de vetor base.

A criptografia pós-quântica refere-se a algoritmos criptográficos projetados para permanecerem seguros mesmo diante do poder computacional dos computadores quânticos em ascensão, os quais tornarão obsoletos muitos dos esquemas clássicos como o RSA (Rivest–Shamir–Adleman) e ECC (Elliptic Curve Cryptography). Algoritmos baseados em reticulados destacam-se como promissores para a era pós-quântica, pois se baseiam em problemas computacionais que continuam difíceis de resolver, mesmo com computadores quânticos.

2.2. Como funciona a criptografia baseada em reticulados

A segurança da criptografia baseada em reticulados é baseado em problemas matemáticos, como:

- SVP (Shortest Vector Problem): dado um reticulado, encontrar o vetor mais curto possível dentro dele é um problema computacional difícil.
- CVP (Closest Vector Problem): dado um ponto arbitrário fora do reticulado, encontrar o vetor mais próximo dentro mais próximo dentro do reticulado também é difícil.
- LWE (Learning With Errors): problemas onde, mesmo conhecendo pares de entradas e saídas, é computacionalmente difícil recuperar a função original devido a pequenos “erros” introduzidos nos dados.

Esses problemas são utilizados como base para criar algoritmos de criptografia que permitem operações como criptografia de chave pública, assinaturas digitais e troca de chaves, todas com segurança quântica.

Um exemplo de aplicação é o exemplo de kyber, um algoritmo de encapsulamento de chave baseado em reticulados que foi selecionado pelo NIST como padrão pós-quântico. Ele se baseia na versão do LWE chamada Module-LWE, e é projetado para ser eficiente, seguro e adequado para uma ampla gama de dispositivos.

2.3. Para que serve a criptografia baseada em reticulados

A criptografia baseada em reticulados serve como base para algoritmos criptográficos resistentes a computadores quânticos. Suas principais aplicações incluem:

- Criptografia de chave pública: geração de chaves seguras que não ´pdem ser quebradas facilmente, mesmo com computadores quânticos.

- Assinaturas digitais: validação de autenticidade de mensagens e documentos.
- Protocolos de segurança na internet: inclusão em protocolos como TLS (Transport Layer Security) para comunicação segura.
- Segurança de dados em nuvem e dispositivos IoT: devido à sua eficiência e baixo custo computacional em implementações específicas.

Além disso, muitos esquemas baseados em reticulados são versáteis e eficientes, o que os torna adequados para ambientes com restrições de recursos, como dispositivos embarcados.

3. Algoritmos baseados em reticulados

3.1. Gauss Reduction

- O que é: método de redução de redução ótimo em dimensão 2, modelo mais simples de reticulados.
- Como funciona: iterativamente aplica uma versão vetorial do algoritmo de Euclides, reduz o vetor maior subtraindo múltiplos inteiros do menor até obter comprimento mínimo e boa ortogonalidade.
- Aplicação: perfeito para ensinar conceitos básicos ou validar implementações, mas impraticável em altas dimensões.

3.2. LLL (Lenstra-Lenstra-Lovász)

- O que é: um algoritmo de tempo polinomial para reduzir uma base de reticulado, tornando os vetores mais curtos e quase ortogonais.
- Como funciona: usa projeções de Gram-Schmidt, repetidamente faz redução de tamanho (mantendo coeficientes menores ou iguais a 1/2) e troca vetores sempre que a condição de Lovász falha.
- Resultado: garante que o primeiro vetor seja apenas um fator moderado mais longo que o vetor mais curto do reticulado, suficiente para muitas aplicações criptográficas.

3.3. BKZ (Block Korkine–Zolotarev)

- O que é: generalização poderosa do LLL, utilizando blocos de vetores para melhorar a redução, base para criptoanálise moderna.
- Como funciona: escolhe um parâmetro bloco β. Para cada bloco consecutivo, resolve o SVP (problema do vetor mais curto) localmente (por enumeração), insere o vetor mínimo encontrado, e então executa LLL no escopo global. Repete enquanto houver melhorias.
- Comportamentos: equilibra qualidade e tempo, blocos maiores resultam em bases mais reduzidas porém com custo exponencial crescente.
- BKZ 2.0: inclui otimizações como poda (pruning), pré-processamento recursivo e heurísticas para saber quando parar. É o algoritmo mais usado atualmente para atacar reticulados.

3.4. 1-bit LWE (Learning With Errors)

- O que é: variante do problema LWE, com saída apenas 0 ou 1, que mantém suas propriedades de dificuldade criptográfica.

- Como funciona: apresenta pares (a,b), onde b = round(⟨a,s⟩/q + e)mod 2 mas o que se observa é apenas o bit de b (ou seja, redução de módulo 2). O objetivo é descobrir o vetor secreto s.

- Uso: serve como base para esquemas eficientes de criptografia (como assinaturas e chaves públicas), oferecendo garantias teóricas e utilidade prática.

3.5. Alkaline

$$m = \lfloor \frac{\langle v1 , v2 \rangle}{\|v1\|^2} \rceil$$

4. Gauss Reduction

A redução gaussiana é uma técnica de redução de reticulados, usada como bloco básico em algoritmos mais avançados (ex: BKZ) que são aplicados na criptoanálise de sistemas pós-quânticos. Seu valor é mais conceitual e local, mas ela é crucial para entender a base matemática da segurança em de próxima geração.

4.1. Gaussian Lattice reduction algorithm

Seja L $\subset$ R^2 um reticulado com vetores de base V1 e V2. O algoritmo abaixo quando termina fornece uma boa base para L.

Loop

Se ||V2||<||V1||, troque V1 e V2.

Calcule $m = \lfloor \frac{V1 \cdot V2}{\|V1\|^2} \rceil$.

Se $m = 0$, retorna os vetores base V1 e V2.

V2 = V2 – mV1.

Continuar o loop

Quando o algoritmo termina, o vetor v1 é o menor vetor não nulo no reticulado L

4.2. Aplicação na criptografia

Supondo que a base original (ruim) é V1 = (66586820, 65354729) e V2 = (6513996, 6393464). Após aplicada a redução gaussiana por 6 passos (até m=0) obtemos a base reduzida:

V1 = (2280, −1001) e V2 = (−1324, −2376).

Portanto, temos agora a base boa, sendo (2280, -1001) a solução do SVP(Shortest Vector Problem) para o reticulado L. Agora em termos de criptografia temos:

- Chave pública: {(66586820, 65354729), (6513996, 6393464)}
- Chave privada: {(2280, −1001), (−1324, −2376)}

Ou seja, o objetivo dessa criptografia é garantir que apenas o dono possua a chave privada, enquanto qualquer outro usuário tenha acesso à chave pública para criptografar mensagens.

No contexto da redução de Gauss, que é usada aqui apenas com fins didáticos, pois trabalha com base em dimensão 2, seria fácil quebrar a segurança, já que um atacante pode aplicar o mesmo algoritmo e descobrir a chave privada com pouco esforço.

No entanto, essa ideia serve como base para algoritmos mais avançados, como o LLL (Lenstra–Lenstra–Lovász), que opera sobre bases em dimensões extremamente grandes.

Nesse cenário, torna-se computacionalmente inviável, até mesmo para computadores quânticos, descobrir a chave privada a partir da base pública, visto que a base ruim é gerada a partir da base boa por transformações complexas.

Esse processo segue a mesma lógica da criptografia por números primos e fatoração, como ocorre no RSA, porém, esse método tende a se tornar obsoleto com o avanço da computação quântica, reforçando a importância e o potencial das soluções baseadas em reticulados para a criptografia pós-quântica.-