Presantation for NGE-06-03

Tools for lattice based cryptography: LLL & BKZ - Algorithms

Alexandros Korkos

Aristotle University of Thessaloniki
Computer Science Department

May 30, 2023

Contact: alexkork@csd.auth.gr

Licence

Overview

Introduction

Lattice - based cryptography

Lattice-based cryptographic constructions hold a great promise for post-quantum cryptography, as they enjoy very strong security proofs based on worst-case hardness, relatively efficient implementations, as well as great simplicity. In addition, lattice-based cryptography is believed to be secure against quantum computers.

Some lattice based schemes:

- NTRU encryption scheme
- GGH encryption scheme
- The Ajtai-Dwork Public Key Cryptosystem
- ...

Lattice (1)

So what is a lattice?

Lattice

Given n-linearly independent vectors $\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n} \in \mathbb{R}^n$, the lattice generated by them is the set of vectors

$$\mathcal{L}(\mathbf{b_1}, ..., \mathbf{b_n}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z} \right\}$$

The vectors $\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n}$ are known as a basis of the lattice.

Lattice (2)

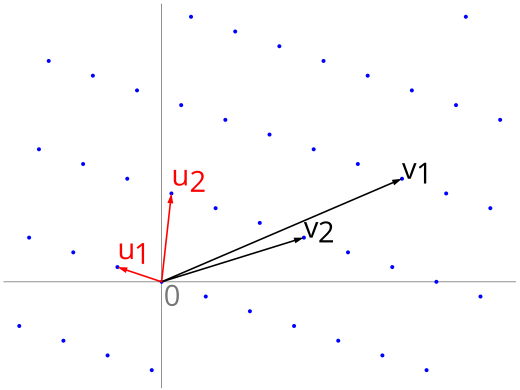

Figure 1: A two-dimensional lattice and two possible bases.

Lattice reduction

Lattice reduction

It aims to find a basis that minimizes the length of the lattice vectors while preserving the important properties of the lattice, or more generally finding reasonably short vectors and reasonably good bases.

Lattice reduction problems

The most well known computational problems on lattices are the following:

- Shortest Vector Problem (SVP): Given a lattice basis $\mathbf{B}$, find the shortest nonzero vector in $\mathcal{L}(\mathbf{B})$.
- Closest Vector Problem (CVP)
- Shortest Independent Vectors Problem (SIVP)

One of the best algorithms for lattice reduction and for solving the Shortest Vector Problem (SVP) is the LLL - Algorithm.

LLL - Algorithm

The LLL algorithm, short for Lenstra-Lenstra-Lovász algorithm, was introduced by Arjen Lenstra, Hendrik Lenstra, and László Lovász in 1982.

One the key attributes of the LLL, is its *polynomial* time for lattice reducing.

More precise, given an integral basis $\mathbf{B} \in \mathbb{Z}^{n \times n}$, the LLL algorithm outputs an LLL-reduced basis of $\mathcal{L} = \mathcal{L}(\mathbf{B})$ in time $poly(n, |\mathbf{B}|)$, where $|\mathbf{B}|$ denotes the bit length of the input basis.

The LLL - Algorithm, finds an approximate solution to SVP. The SVP is still reaming as $\mathcal{NP} - hard$.

Definition of LLL

Definition

Let $\{\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n}\}$ be a basis for a n-dimensional Lattice $\mathcal{L}$, and $\{\mathbf{b_1^*}, \mathbf{b_2^*}, ..., \mathbf{b_n^*}\}$ be a orthogonal basis, and we have $\mu_{i,j} = \frac{\mathbf{b_j} \cdot \mathbf{b_i^*}}{\mathbf{b_i^*} \cdot \mathbf{b_i^*}}$. We say $\{\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n}\}$ is a LLL reduced basis if it satisfies two conditions:

1. $|\mu_{i,j}| \leq \frac{1}{2}, \forall 1 \leq j < i \leq n$ (Size-reduction condition)
2. $\delta \|\mathbf{b_{k-1}^*}\|^2 \leq \|\pi_{k-1}(\mathbf{b_k})\|^2, \forall k \in [2, n]$ (Lovász condition).

Implementation of LLL

Algorithm 1: LLL - Algorithm

Input : A basis $\mathbf{B} = \{\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n}\}$ of a lattice L, and a reduction parameter $\delta \in (0.25, 1]$

Output : A δ - LLL reduced basis $\mathcal{L}(\mathbf{B})$

Compute Gram–Schmidt information $\mu_{i,j}$ and $\|\mathbf{b_i^*}\|^2$ of the input basis B

$k = 2$

while $k \leq n$ **do**

  // At each k, we recursively change $\mathbf{b_k} = \mathbf{b_k} - \lfloor \mu_{k,j} \rceil \mathbf{b_j}$ for $j \in [1, k-1]$

  Size-reduce **B**

  if $\delta \|\mathbf{b_{k-1}^*}\|^2 \leq \|\pi_{k-1}(\mathbf{b_k})\|^2$ **then**

    $k = k + 1$

  else

    Swap $\mathbf{b_k}$ with $\mathbf{b_{k-1}}$, and update Gram–Schmidt information of **B**

    $k = \max(k-1, 2)$

BKZ - Algorithm

The first version of BKZ algorithm was proposed by Schnorr and Euchner in 1994 as a generalization of the LLL algorithm

The BKZ algorithm finds a β-BKZ-reduced basis, and it calls LLL to reduce every local block before finding the shortest vector over the block lattice. (As β increases, a shorter lattice vector can be found, but the running time is more costly.)

BKZ has *exponential* complexity versus the *polynomial* complexity of the LLL reduction algorithm.

Implementation of BKZ

Algorithm 2: BKZ - Algorithm

Input : A basis $\mathbf{B} = \{\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n}\}$ of a lattice L, a blocksize $\beta \in [2, n]$, and a reduction parameter$\delta \in (0.25, 1]$ of LLL

Output : A β - BKZ reduced basis $\mathcal{L}(\mathbf{B})$

$\mathbf{B} = LLL(\mathbf{B}, \delta)$

$z = 0, j = 0$

while $z < n - 1$ **do**

  $j = (j \mod (n-1)) + 1, k = \min(j + \beta - 1, n), h = \min(k + 1, n)$

  Find $\mathbf{v} \in L$ such that $\|\pi_j(\mathbf{v})\| = \lambda_1(L_{[j,k]})$ by enumeration or sieve

  if $\|\pi_j(\mathbf{v})\|^2 < \|\mathbf{b_j^*}\|^2$ **then**

    $z = 0$ and call $LLL((\mathbf{b_1}, ..., \mathbf{b_{j-1}}, \mathbf{v}, \mathbf{b_j}, ..., \mathbf{b_h}), \delta)$

  else

    $z = z + 1$ and call $LLL((\mathbf{b_1}, ..., \mathbf{b_h}), \delta)$

Comparison

Lattice reduction comes in flavours.

If we examine:

- Reduction Quality: The BKZ algorithm can achieve significantly better reduction quality compared to LLL. It strives to find a basis with shorter and more orthogonal lattice vectors.
- Computational Complexity: The BKZ algorithm has a higher computational complexity (*exponential*) compared to LLL (*polynomial*).

Conclusion

In summary, the LLL algorithm is suitable for many practical applications, offering a good balance between reduction quality and computational efficiency. On the other hand, the BKZ algorithm is employed when stronger reductions are needed, especially in lattice-based cryptography, despite its higher computational cost.

References

Masaya Yasuda (2021)
A Survey of Solving SVP Algorithms and Recent Strategies for Solving the SVP Challenge
International Symposium on Mathematics, Quantum Theory, and Cryptography.

Daniele Micciancio, Oded Regev (2008)
Lattice-based Cryptography

Yan Wang (2013)
Lecture 3: LLL, Coppersmith
Lattices in Cryptography.

The End