# VE475 Introduction to Cryptography

## Lattice-based Cryptography


| Jiang, Sifan | Wu, Hao | Su, Jingyu | Song, Gaopeng |
|---|---|---|---|
| 515370910040 | 515370910041 | 516370910123 | 516370910227 |


June 19, 2019

## 1 Introduction

A quantum computer is a computer whose operation exploits certain very special transformations of its internal state based on the laws of quantum mechanics and under very carefully controlled conditions [1]. In theory, any particles, like atom, electron, photon, can be used for quantum computing. The reason why quantum computers can have higher computing performance than any regular computers is that one particle can be viewed as a binary $0$, a binary $1$, or a $0$ and $1$ at the same time because of "Quantum Superposition". In such way, the computer can conduct parallel computing very efficiently and try all the possible solutions in very short time to realize complex computation. Based on such theory, *Shor* discovered the quantum factoring algorithm with time complexity $O((\log N)^3)$, making factoring-based cryptosystems no longer secure.

New cryptosystems are needed especially nowadays, companies like IBM has developing their own quantum computers, such as *IBM Q System One*. One of the possible post-quantum cryptosystem solution is lattice-based cryptography.

Lattices have been introduced to the field of mathematics first in the $18^{th}$ century in number theory by mathematicians such as Gauss and Lagrange. The study of lattices was advanced by Minkowski in his "Geometry of Numbers".

In 1982, Arjen Lenstra, Hendrik Lenstra, and László Lovász introduced their famous "LLL" basis-reduction algorithm in *Factoring Polynomials with Rational Coefficients* [2], which is used for factoring integer polynomials.

In 1996, Miklós Ajtai issued *Generating hard instances of lattice problems* and introduced "worst-case to average-case reduction" for lattice problems , providing a cryptographic one-way function based on worst-case hardness conjectures [3]. And the Short Integer Solution problem (SIS) serve as a foundation of numerous lattice-based cryptographic protocols: For positive integer parameters $n$, $m$, and $q$, find a short non-zero solution $\mathbf{z} \in \mathbb{Z}^m$ to the honogeneous linear system $\mathbf{Az} = 0 \mod q$ for uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ [4]. Another main problem, as the foundation, is the Learning With Errors problem.

### 1.1 General Lattices

A lattice is a set of points in $n$-dimensional space with a periodic structure , such as the one illustrated in Figure 1, which is a simple example shows the two-dimensional space lattice and two groups of possible, as long as vectors are independent, bases (black and grey ones) [5].

Formally, given $n$-independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n \in \mathbb{R}^n$, the lattice generated by these vectors is the set of vectors

$$\mathcal{L}(\mathbf{b}_1, \cdots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b_i} \ : \ x_i \in \mathbb{Z} \right\}. \tag{1}$$

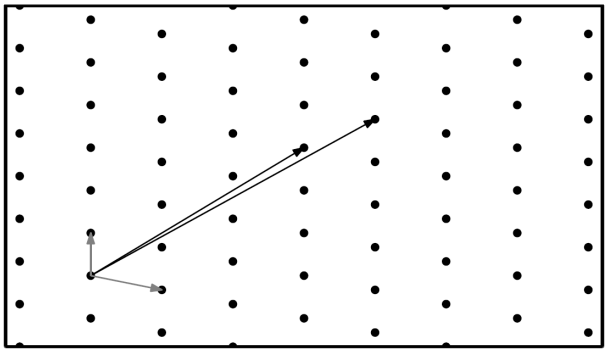

Figure 1: A two-dimensional lattice and two possible bases.

The vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ are known as a basis, denoted $\mathbf{B}$, of the lattice. For example, $[1, 5, -9]^T$, $[-2, 2, 0]^T$, and $[13, 1, 4]^T$ form an basis for $\mathbb{Z}^3$ and

$$\mathbf{B} = \begin{bmatrix} 1 & -2 & 13 \\ 5 & 2 & 1 \\ -9 & 0 & 4 \end{bmatrix}.$$

Notice that there exists multiple lattice bases which makes lattice-based cryptography possible. Any lattice can be obtained by applying some non-singular linear transformation to the integer lattice. Also, given $\mathbf{B}_1$, $\mathbf{B}_2$ two bases for lattice $\mathcal{L}$, there exist uni-modular matrices $\mathbf{U}$ such that $\mathbf{B}_1 = \mathbf{B}_2\mathbf{U}^{-1}$ [5].

Since lattice is in a periodic structure, the concept of fundamental region is used to formalize this idea. A set $\mathcal{F} \subseteq \mathbb{R}^n$ is a fundamental region of a lattice $\mathcal{L}$ if its translates $\mathbf{X} + \mathcal{F} = \{\mathbf{x} + \mathbf{y} \ : \ y \in \mathcal{F}\}$, taken over all $x \in \mathcal{L}$, form a partition of $\mathbb{R}^n$. And the fundamental parallelepiped of a lattice basis $\mathbf{B}$ is defined as

$$\mathcal{P}(\mathbf{B}) := \mathbf{B} \cdot \left[-\frac{1}{2}, \frac{1}{2}\right)^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i \ : \ c_i \in \left[-\frac{1}{2}, \frac{1}{2}\right) \right\}. \tag{2}$$

Then, the determinant of a lattice $\mathcal{L}$, denoted $\det(\mathcal{L})$, can be defined as $\mathrm{vol}(\mathcal{F})$.

Since a lattice $\mathcal{L}$ is discrete, it has two non-zero elements $\pm\mathbf{v} \in \mathcal{L}$ of minimum Euclidean distance. The exact definition of the minimum distance of a lattice $\mathcal{L}$ is defined as

$$\lambda_1(\mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{v}\|. \tag{3}$$

With Minkowski's First Theorem, we have for any lattice $\mathcal{L}$, we have $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$. And using the exact formula for the volume of an $n$-dimensional ball, we can obtain a slightly tiger bound $\lambda_1(\mathcal{L}) \leq \sqrt{n/(2\pi e)} \cdot \det(\mathcal{L})^{1/n}$.

## 1.2 Lattice Problems

### 1.2.1 Shortest Vector Problem

Shortest Vector Problem (SVP) is the most important lattice-based computational problem, which requires the approximate of the minimal Euclidean length of a non-zero lattice vector. The definition of Approximated Shortest Vector Problem (SVP$_\gamma$) is: find a vector $\mathbf{v} \in \mathcal{L}(\mathbf{B}) \setminus \{\mathbf{0}\}$ such that

$$\|\mathbf{v}\| \leq \gamma \cdot \min_{\mathbf{w} \in \mathcal{L}(\mathbf{B}) \setminus \mathbf{0}} \|\mathbf{w}\|$$

Where $\gamma \geq$ and when $\gamma = 1$, it's a non-approximated problem. There are three common variants of SVP [6]:

1. Decision (GapSVP$_\gamma$): given a lattice basis $\mathbf{B}$ and a positive integer $d$, distinguish between the cases $\lambda_1(\mathcal{L}(\mathbf{B})) \leq d$ and $\lambda_1(\mathcal{L}(\mathbf{B})) > \gamma \cdot d$.

2. Estimate (EstSVP$_\gamma$): given a lattice basis $\mathbf{B}$, compute $\lambda_1(\mathcal{L}(\mathbf{B}))$ up to a $\gamma$ factor, i.e., output some $d \in [\lambda_1(\mathcal{L}(\mathbf{B})), \gamma \cdot \lambda_1(\mathcal{L}(\mathbf{B}))]$.

3. Search: with is SVP$_\gamma$ itself.

To efficiently compute bounds on the minimum distance, and even find relatively short non-zero lattice vectors, Lenstra-Lenstra-Lovász (LLL) algorithm can be applied. It yields a polynomial-time solution to SVP$_\gamma$ with an approximation factor $\gamma = 2^{n-1} - 2$, which is exponential in the dimension. It "converts an arbitrary lattice into one that generates the same lattice, and which is reduced in the following sense" [6].

#### 1.2.2 Shortest Independent Vectors Problem

Approximated Shortest Independent Vector Problem (SIVP$_\gamma$) is: find $\mathbf{U} \in \mathrm{Gl}_n(\mathbb{Z})$ with

$$\|\mathbf{BU}\| \leq \gamma \cdot \min_{\mathbf{V} \in \mathrm{Gl}_n(\mathbb{Z})} \|\mathbf{BV}\|$$

#### 1.2.3 Closet Vector Problem

Approximated Closet Vector Problem (CVP$_\gamma$) is: for $\mathbf{t} \in \mathbb{R}^n$, find a lattice point $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\mathbf{v} - \mathbf{t}\| \leq \gamma \cdot \min_{\mathbf{w} \in \mathcal{L}(\mathbf{B})} \|\mathbf{w} - \mathbf{t}\|$$

## 2 GGH/HNF [7]

Though The GGH/HNF cryptosystem, proposed by Goldreich, Goldwasser and Halevi has already been broken in practice, it's still valuable to learn it while studying lattice based cryptography.

### 2.1 Related Knowledge

For any $n \times m$ matrices $A \in \mathbb{Z}^{n \times m}$ with rank m, there exists a uni-modular matrix $U$(i.e. $\det(U) = \pm 1$) such that

$$UA = H,$$

where $h_{ii}$ is positive for $1 \leq i \leq m$, $h_{ij} = 0$ for $j > i$, and $|h_{ij}| < h_{ii}$ for $i > j$ [8]. $H$ is called the Hermite normal form of A.

### 2.2 Key Generation

For a chosen lattice base $B$, we can calculate its Hermite Normal Form $H$ by finding a uni-modular matrix $U$(i.e. $\det(U) = \pm 1$) and

$$H = BU.$$

Then $B$ is the private key and $H$ is the public key.

### 2.3 Encryption

If the message is $m \in \mathbb{Z}^n$, then the ciphertext $c \in \mathbb{Q}^n$ is

$$c = Hm + r,$$

where $r \in \mathbb{Q}^n$ is a small noise vector chosen such that the lattice vector closest to c is $Hm$.

### 2.4 Decryption

For the ciphertext message $c \in \mathbb{Q}^n$, the private key $B$ and the public key $H = BU$, first compute:

$$B^{-1} \cdot c = B^{-1} \cdot (Hm + r) = B^{-1}BUm + B^{-1}r = Um + B^{-1}r.$$

Then since r is a small noise by definition, use the babai rounding method [9] to remove the term $B^{-1}r$. Finally get m by

$$U^{-1}Um = m$$

## References


[1] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[2] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, 1982.

[3] M. Ajtai, "Generating hard instances of lattice problems," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 99–108, ACM, 1996.

[4] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.

[5] D. Micciancio, "Lattice-based cryptography," *Encyclopedia of Cryptography and Security*, pp. 713–715, 2011.

[6] "Svp, gram-schmidt, lll," 2013.

[7] J. Hüttenhain and L. Wallenborn, "Topics in post-quantum cryptography: Lattice-based methods," 2011.

[8] R. Melissa, K. Sosuke, I. Naoya, and G. Andrew, "An rnn-based binary classifier for the story cloze test.," in *Proceedings of the 2nd Workshop on Linking Models of Lexical, Sentential and Discourse-level Semantics (LSDSem)*, 2017.

[9] L. Babai, "On lovászlattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.