Cryptanalysis of Lattice-based Cryptosystems

Undergraduate Thesis

Submitted in partial fulfillment of the requirements of
BITS F421T Thesis

By

Ritik Bavdekar
ID No. 2017B4A70349P

Under the supervision of:

Dr. Ashutosh Bhatia
&
Dr. Divesh Aggarwal

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE PILANI, PILANI CAMPUS
December 2021

Declaration of Authorship

I, Ritik BAVDEKAR, declare that this Undergraduate Thesis titled, 'Cryptanalysis of Lattice-based Cryptosystems' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

Certificate

This is to certify that the thesis entitled, "*Cryptanalysis of Lattice-based Cryptosystems*" and submitted by Ritik Bavdekar ID No. 2017B4A70349P in partial fulfillment of the requirements of BITS F421T Thesis embodies the work done by him under my supervision.

Supervisor
Dr. Ashutosh Bhatia
Asst. Professor,
BITS-Pilani Pilani Campus
Date:

Co-Supervisor
Dr. Divesh Aggarwal
Asst. Professor,
National University of Singapore
Date:

“Always work with passion! On your lucky day, the right idea will strike you when you watch the apple fall.”

Ritik Bavdekar

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE PILANI, PILANI CAMPUS

Abstract

Bachelor of Engineering (Hons.) Computer Science

Cryptanalysis of Lattice-based Cryptosystems

by Ritik Bavdekar

RSA, Diffie-Helman Key Exchange Protocol and Elliptic Curve cryptography are the most widely used cryptosystems in the present world. Their security relies on the hardness of their underlying mathematics problem, the discrete logarithm problem and the prime factorization problem. The advent of quantum computers renders these cryptosystems insecure and easy to crack. Lattice-based cryptography is one of the major candidates for cryptosystems in the post-quantum computer era. Lattice-based cryptosystems have a variety of underlying hard mathematics problem. Fundamental hard mathematics problems in lattices include the Shortest Vector Problem and the Clostest Vector Problem. This thesis conducts a study on hard problems in lattices and algorithms like the LLL algorithm. The research work is on a hard lattice problem called the Bounded Distance Decoding problem(special case of Closest Vector Problem). The research work analyses how the approximation factor for the BDD problem varies with different q-ary lattices.

Acknowledgements

I would like to thank Dr. Divesh Aggarwal for guiding and helping me throughout the research work. He gave me the opportunity to work under his guidance, helped me understand research papers, guided me with all his new and unique ideas and gave me a lot of constructive feedback. I would also like to thank Dr. Ashutosh Bhatia who helped me ideate in the thesis and provided any resource I would require for the thesis. I would also like to thank the Computer Science and Information Systems Department, BITS Pilani and NUS Computing for giving me the opportunity to pursue a thesis in a topic of my interest. I want to express gratitude towards my parents who have always been there to support me.

Contents

Abbreviations

PQC	**P**ost **Q**uantum **C**ryptography
LWE	**L**earning **W**ith **E**rror
BDD	**B**ounded **D**istance **D**ecoding
SVP	**S**hortest **V**ector **P**roblem
CVP	**C**losest **V**ector **P**roblem
LLL	**L**enstra **L**enstra **L**ovasz

Dedicated to my parents

Chapter 1

Introduction

1.1 Introduction

Today's world revolves around communication. Modern society depends on Internet as a fundamental building block for any interaction between two parties. There comes a need to protect and maintain the privacy of data being transmitted. Cryptography is a field devoted to the sole purpose of data security, where countless researchers work to ensure that the privacy and integrity of data are maintained through the implementation of various security algorithms.

A new paradigm of computing is slowly emerging in form of quantum computers which is going to drastically change the capabilities of classical computers that we are using currently. Quantum computers will be able to perform certain computations which are not possible by present day high performance multicore systems. The idea of quantum computer is strongly based on quantum physics i.e., understanding how things work on the sub-atomic level, initiated in the early 20th century by several great scientists like Schrödinger, Bohr, Heisenberg and Einstein, among others. Later in 1980s scientist applied quantum physics and its mathematics to model the computers that could perform computations at amazingly high rate than the classical computers. Quantum computers take input in the form of quantum bits and produce output. They leverages concepts of quantum mechanics for computing. Quantum computers can be used to solve problems that are not feasible to be solved by classical computers within a bounded time. Quantum computers can be used to compute results which are not possible even by present day super computers. The applications of quantum computers are countless including navigation systems, seismology, physics research, pharmaceuticals, etc[12]. Quantum computers can be used to solve complex science problems which even present day supercomputers fail to solve. They will revolutionize artificial intelligence by giving a massive boost in computation power. The applications of quantum computers are countless.

There are always two faces of a coin. On one hand, quantum computers provide us the hope to solve several problems across different verticals within a bounded time. On the other hand, their arrival may become a potential threat for us in certain scenarios. One such scenario is cryptanalysis.

Cryptanalysis is the study of different techniques which can be used to find the meaning of encrypted data, without access to secret information used by the sender and receiver to encrypt and decrypt the data. Cryptanalysis is the art of code-breaking. An unfortunate fact is that the hard problems of mathematics upon which our present day cryptographic algorithms are built will become solvable on quantum computers. This will make it easy to crack the cryptographic algorithms widely used in digital communication. The symmetric cryptographic algorithms[22] that are widely used include Advanced Encryption Standard (AES) and 3DES (Data Encryption Statndard). Their bit security will be halved with the help of Grover's algorithm. Asymmetric cryptosystems[21] like RSA, Diffie Hellman and ECC are based on the classically hard problems of Prime Factorisation and Discrete Logarithm. Quantum computers can be used to solve these computationally secure problems in no time. This severely compromises the security of the asymmetric cryptosystems.

Post-quantum cryptography[6] is the study of new cryptosystems which cannot be cracked by both quantum and classical computers. The cryptosystems are divided into several families based on the underlying problem upon which the security is established. Lattice-based cryptography is a significant family in post-quantum cryptography. Its security is based on NP-hard lattice problems. In the NIST post-quantum cryptography standardization process lattice-based cryptosystems are a leading contender. A lattice-based digital signature scheme and asymmetric cryptosystem will be standardized and used for security all over the world.

The thesis focuses on a lattice problem called the Bounded Distance Decoding problem. This problem is a special case of the Closest Vector Problem.

Definition 1.1. Bounded Distance Decoding Problem: Given a lattice L with Basis B and target vector $t \in span(L(B))$ such that $t = v + e$ where $v \in L(B)$ and $|e| < r$ (r is the approximation factor). Find v. (Note for solution to be unique $r < \frac{\lambda_1}{2}$)

The BDD problem involves finding the closest point in the lattice to a given perturbed point which is at a distance of less than r from the lattice.

The research work found particular classes of lattices for which the approximation factor r can be larger. On a general lattice the approximation factor for which the problem can be solved is of the form $r = \frac{1}{2^{O(n)}}$. Here n is the dimension of the lattice. The thesis found classes of q-ary lattices for which $r = \frac{1}{2^{O(\sqrt{n})}}$. The work found that the BDD problem can be solved better for particular lattices. It contains of a mathematical analysis which shows how the approximation factor improves for particular lattices. The solution to BDD can be found by first applying the LLL algorithm to the lattice basis and then using Babai's Nearest Plane algorithm. To read the mathematical analysis and results navigate to chapter 4.

Chapter 2 gives an introduction to post-quantum cryptography. It explains the importance of post-quantum cryptography and introduces the cryptosystems in the NIST competition. Chapter 3 provides an introduction to all the mathematics that will be required for understanding the results of work. It introduces lattices and all the important theorems in lattice-based crypotgraphy. It then proceeds to explain and proves theorems for an important type of lattices called q-ary lattices. These lattices are the special lattices for which the results for the BDD problem have been proved in Chapter 4.

Chapter 2

Post-Quantum Cryptography

2.1 Introduction

Post-quantum cryptography[6] is the study of new cryptosystems which cannot be cracked by both quantum and classical computers. The cryptosystems are divided into several families based on the underlying problem upon which the security is established. These underlying problems are believed to be unsolvable by both classical and quantum computers. The major families are lattice-based cryptography, isogeny-based cryptography, non-commutative cryptography, code-based cryptography, hash-based digital signatures, and multivariate cryptography.

The need for better cryptographic algorithms has led to various initiatives by the NIST to create Quantum Secure' algorithms. In a drive to expedite current research into the Screation of a standard, entries from all across the world were received and deliberated upon to create an appropriate standard for when the need arises.

The advent of quantum computers has called into question the security of classical cryptographic algorithms. Symmetric cryptography's security (AES,DES,3DES) has been halved in bits by quantum computers. Asymmetric cryptography(RSA, Diffie Hellman, Elliptic Curve Cryptography) will turn obsolete with quantum computational resources.

2.2 The 6 families of Post-quantum cryptography

Post-quantum cryptography is the field of cryptography where encryption algorithms are developed which are secure from an adversary with quantum computers. They use new hard problems and are primarily classified into 6 families. NIST is holding a post-quantum cryptography competition to select cryptosystems for the next generation. There are candidates from all the families in the competition.

Lattice-based cryptography: Lattice-based cryptography[20] is based on hard problems in lattices. Read more about it in 3. 27 of the 69 algorithms submitted to NIST for the PQC Standardization process are lattice-based. The cryptosystems that made it to the third round include CRYSTALS-KYBER[7], SABER[1] and NTRU[11]. The digital signature candidates that made it to the third round include FALCON[2] and CRYSTALS-DILITHIUM[8].

Hash-based digital signatures: Hash-based digital signatures can be used an alternative for the present day digital signature schemes that rely on asymmetric cryptosystems like RSA and ECC.Their security depends on the underlying hash function. A disadvantage they have is that a signing key can only be used once, so a new one is generated for each digital signature. 2 of the 69 schemes in the NIST competition are hash-based digital signatures. SPHINCS+[3] is an alternative candidate for the third round.

Code-based cryptography: Code-based cryptography is based on error-correction codes. McEliece[4] cryptosystem is code-based cryptosystem that was introduced in 1978 and it is still believed to be secure. They rely on introducing random errors in the message to be sent. This way the adversary cannot decode the message without knowing the private key that helps removes errors from the message. 21 of the 69 algorithms submitted to NIST for PQC Standardization process are code-based. The cryptosystem that made it to the third round as a finalist is Classic McEliece. The alternative candidates that made it to round-3 include BIKE and HQC.

Non-commutative cryptography: Non-commutative cryptography relies on non-abelian algebraic groups($A * B \neq B + A$). It makes use of a problem called the conjugacy problem ie in a non-abelian group $\mathbb{G}$ find $X \in \mathbb{G}$ such that given $A, B \in \mathbb{G}$ the equation $X + A - X = B$ holds. Only 1 algorithm was submitted in the NIST competition that got broken in the first round. A post-quantum key exchange protocol that shows promise is the Stickel Key Exchange Protocol[24].

Multivariate cryptography: Multivariate cryptography is mainly used for digital signature schemes. It relies on the hardness of solving a system of multivariate polynomials. The scheme uses a quadratic map $\mathbb{P}$ as public key and to sign a message t the signer finds s such that $\mathbb{P}(s) = t$. The oil and vinegar scheme was one of the first multivariate digital signatures. It works only for particular parameters. Rainbow[9] is a scheme that uses multiple unbalanced oil and vinegar layers. It was introduced in 2005. It is a contender for digital signatures in the third round for NIST PQC Standardization process.

Isogeny-based cryptography: Isogeny-based cryptosystems use elliptic curves. An isogeny is a homomorphic rational map between 2 elliptic curves $\Phi : E_0 \mapsto E_1$. Supersingular Isogeny-based Diffie Hellman(SIDH)[14] was introduced in 2011. It uses two private isogenies between two users. They apply the isogenies to a common elliptic curve E and then share the results with each other. A key encapsulation mechanism SIKE(Supersingular Isogeny-Based Key Encapsulation)[25] is based on the SIDH and is part of the 3rd round alternate candidates for Key Encapsulation Mechanisms in the NIST PQC Standardization process.

There were also candidates that did not belong to these families. PICNIC[23] is a digital signature algorithm that provides security against both quantum and classical attacks. Unlike the other families PICNIC does not depend on any number-theoretic result for digital signatures.It is based on zero-knowledge proof system and symmetric-key primitives like hash functions and block ciphers

Chapter 3

Lattice-based cryptography

3.1 Introduction

Lattices are points in an n-dimensional space with a periodic structure[15]. They can be found in nature in the form of crystals. A few common lattice forms found in molecules and atoms include ccp,fcc,bcc and hcp. Lattices have been studied since the late 18th Century. Only recently it has become interesting to researchers in computer science. They have applications in cryptography , cryptanalysis and even other problems.

Definition 3.1. Lattice: A lattice is points in an n-dimensional space that can be defined using k linearly independent vectors $b_1 \dots b_k$ where $b_i \in \mathbb{Z}^{\Bbbk}\ \forall i$. Points in the lattice can be formed by taking integer linear combinations of $b_1 \dots b_k$.

$$L(b_1, \dots b_k) = \{\sum x_i b_i | x_i \in \mathbb{Z}\} \tag{3.1}$$

Definition 3.2. Fundamental Parallelepiped: For any lattice basis B,

$$P(B) = \{Bx | x \in \mathbb{R}^k \, \forall i : 0 \leq x_i < 1\} \tag{3.2}$$

We can tile the entire span(L(B)) by placing a fundamental parallelepiped at each point of the lattice.

Lemma 3.3. *$L(B_1) = L(B_2)$ iff $B_2 = B_1 U$ for some unimodular matrix $U \in Z^{k*k}$.($|det(U)| = 1$)*

Definition 3.4. Determinant of a lattice: The determinant of a lattice $\Lambda(B)$ is $\sqrt{B^T B}$. For a square basis B it is $det(B)$.

Definition 3.5. Successive minima: Let Λ be a lattice of rank n. For $i \in \{1, \ldots, n\}$ i^{th} successive minimum is

$$\lambda_i(\Lambda) = inf\{r|dim(span(\Lambda \cap \mathbb{B}(0,r))) \geq i\} \tag{3.3}$$

Here $\mathbb{B}(0,r)$ is a closed ball of radius r around 0. $\mathbb{B}(0,r) = \{x \in \mathbb{R}^n|||x|| \leq r\}$

Theorem 3.6. ***Blichfeld:*** *For any full-rank lattice $\Lambda \subset \mathbb{R}^n$ and measurable set $S \subset \mathbb{R}^n$ with $vol(S) > det\Lambda$ there exist 2 nonequal points $z_1, Z_2 \in S$ such that $z_1 - z_2 \in \Lambda$ [13]*

Theorem 3.7. ***Minkowski's Convex Body Theorem:*** *Let Λ be a full rank lattice of rank n. Then for any centrally-symmetric convex set S, if $vol(S) > 2^n det(\Lambda)$ then S contains a nonzero lattice point.[13]*

Theorem 3.8. ***Minkowski's First Theorem:*** *For any full-rank lattice Λ of rank n [13]*

$$\lambda_1(\Lambda) \leq \sqrt{n}(det\Lambda)^{\frac{1}{n}} \tag{3.4}$$

Theorem 3.9. ***Minkowski's Second Theorem:*** *For any full-rank lattice Λ of rank n[13],*

$$(\prod_{i=1}^{n} \lambda_i(\Lambda))^{\frac{1}{n}} \leq \sqrt{n}(det\Lambda)^{\frac{1}{n}} \tag{3.5}$$

3.1.1 Lattice Problems

Lattice problems are considered NP-Hard problems on an average-case. A few lattice problems are also worst-case hard. These can be used for very secure cryptosystems. The worst-case hardness of the problems make researchers believe they are hard to solve even by quantum computers.

Definition 3.10. Shortest Vector Problem(SVP): Given a basis B for a lattice L find $v \in L(B)$ such that $||v|| = \lambda_1(L(B))$

There are many different versions of SVP. The above statement is for Search-SVP.

Definition 3.11. Optimization SVP: Given a basis B for lattice L find $\lambda_1(L(B))$

Definition 3.12. SVP-γ (Approximate SVP) : Given a basis B for lattice L find $v \in L(B)$ such that $||v|| \leq \gamma * \lambda_1(L(B))$

Definition 3.13. Closest Vector Problem(CVP): Given a basis B for a lattice L of dimension n and a target vector $t \in \mathbb{Z}^n$ where $t \in span(L(B))$ find $v \in L(B)$ such that $||v - t||$ is minimum.

Definition 3.14. CVP-γ (Approximate CVP) : Given a basis B for a lattice L of dimension n and a target vector $t \in \mathbb{Z}^n$ where $t \in span(L(B))$ find $v \in L(B)$ such that $||v - t|| \leq \gamma * ||s - t||$ where s is a vector such that $||s - t||$ is minimum.

Definition 3.15. Gap-SVP(β): Given a lattice L(B) with basis B find if $\lambda(L) \leq 1$ or $\lambda(L) > \beta$. β is a function of the dimension of the lattice L(B)

Definition 3.16. SIVP (Shortest Independent Vector Problem): Given a basis $B \in \mathbb{Z}^{\ltimes * \ltimes}$ find n-linearly independent vectors $u_1, \ldots, u_n$ such that $||u_i|| \leq \lambda_n \; \forall i \in \{1, 2, \ldots, n\}$

Definition 3.17. Bounded Distance Decoding Problem: Given a lattice L with Basis B and target vector $t \in span(L(B))$ such that $t = v + e$ where $v \in L(B)$ and $|e| < r$ (r is the approximation factor). Find v. (Note for solution to be unique $r < \frac{\lambda_1}{2}$)

Definition 3.18. Shortest Integer Solution (SIS): Given a matrix $A \in Z_q^{m*n}$ find a non-trivial short $z \in \mathbb{Z}^m$ such that $Az = 0$

Definition 3.19. Learning with Errors (LWE): Given a matrix $A \in Z^{m*n}$ and $B \in Z^m$ find s such that $B = A * s + e$. (Note: $e \in Z^m$ is a small error term).

3.2 LLL Algorithm

The Lenstra-Lenstra-Lovasz(LLL)[19] algorithm is a polynomial time approximation algorithm for the Shortest Vector Problem(SVP). It gives an approximation factor of $(\frac{2}{\sqrt{3}})^n$ (where n is the dimension of the lattice). It also has multiple other applications like finding integer relations, factoring polynomials, Integer programming, solving other lattice problems like CVP and cryptanalysis of knapsack-based cryptosystems.

Definition 3.20. Basis Reduction: The process of reducing the basis B to a shorter and more orthogonal basis B' while keeping the lattice the same ie $L(B) = L(B')$.

Common ways to modify a basis without changing the lattice L involves swapping 2 vectors in the basis matrix, multiplying a basis vector by -1 or adding a linear combination of other basis vectors to a basis vector. For $L(B) = L(B')$ we must have $B = UB'$ where $|det(U)| = 1$ ie multiply by a unimodular matrix U.

3.2.1 Gram-Schmidt Orthogonalization

Gram-Schmidt Orthogonalization[17] is a mathematical procedure that takes in n linearly independent vectors and creates a set of n orthogonal vectors in the same space.

Definition 3.21. Gram-Schmidt Orthogonalization: For a sequence of n linearly independent vectors $b_1, b_2, \ldots, b_n$, GSO is a a sequence of vectors $b_1^*, \ldots, b_n^*$ such that

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \, where \, \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \tag{3.6}$$

Definition 3.22. δ-LLL reduced basis: A basis $B = \{b_1, b_2, \ldots, b_n\} \in \mathbb{R}^n$ is *delta*-LLL reduced ($\frac{1}{4} < \delta < 1$) if the following conditions hold:-

$$1.\forall i, 1 \leq i \leq n \forall j < i \, we \, have \, \mu_{i,j} \leq 1/2 \tag{3.7}$$

$$2.\forall i, 1 \leq i < n \, we \, have \, \delta||b_i^*||^2 \leq ||\mu_{i+1,i} b_i^* + b_{i+1}^*||^2 \tag{3.8}$$

The LLL algorithm is used to convert a basis for lattice to a $\delta-$reduced basis. It contains of 2 major steps: the reduction step and the swap step. In the reduction step we make condition 1 (eqn 2.7) true for all vectors. In the swap step we swap vectors if the condition 2 (eqn 2.8) fails for any pair of i and i+1. These 2 steps are repeated until the second condition is true for all (i,i+1) pairs and can be skipped.

Algorithm:

```
for i=2:n:
    for j=i-1 to 1:
        $b_i = b_i - \mu_{i,j} b_j$
for i=1:n-1
    if ($\delta||b_i^*||^2 > ||\mu_{i+1,i} b_i^* + b_{i+1}^*||^2$):
        swap($b_i, b_{i+1}$)
        go back to start
```

Lemma 3.23. *If LLL procedure described above terminates then the output is δ-LLL reduced*

Proof. The swap step ensures that the second condition(eqn 2.8) always holds if the algorithm terminates.

To prove the first condition let us select a random i and j such that $i > j$ We replace b_i with $b_i - round(\mu_{i,j}) b_j$. Let $round(\mu_{i,j}) = c_{i,j}$ So calculating new $|\mu'_{i,j}|$

$|\mu'_{i,j}| = |\frac{\langle b_i - c_{i,j} b_j, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}|$

$|\mu'_{i,j}| = |\frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} - \frac{\langle c_{i,j}) b_j, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}|$

$|\mu'_{i,j}| = |\frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} - c_{i,j} \frac{\langle b_j, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}|$

$|\mu'_{i,j}| = |\frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} - round(\frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}) * \frac{\langle b_j, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}|$

$|\mu'_{i,j}| \leq 1/2$

□

Lemma 3.24. *The number of iterations in LLL algorithm are a polynomial in* $M = max\{n, log(max_i||b_i||)\}$

Definition 3.25. For a lattice $B = \{b_1, \ldots, b_n\}$,the potential D_B is

$$D_B = \prod_{i=1}^{n} ||b_i^*||^{n-i+1} = \prod_{i=1}^{n} ||b_1^*|| \ldots ||b_i^*|| = \prod_{i=1}^{n} D_{B,i} \tag{3.9}$$

Note: $D_{B,i} = det(\Lambda_i)$. Here Λ_i is the lattice spanned by $b_1, \ldots, b_i$

Proof. We know that $||b_i^*|| \leq ||b_i||$, so we have that $D_B \leq (max_i||b_i||)^{\frac{n(n+1)}{2}}$

As we know during reduction the Gram Schmidt vectors do not change so D_B won't change.

So the change in D_B occurs in the swap step. Suppose b_i and b_{i+1} are swapped. Then the value of $D_{B,i}$ will change to $D_{B,i-1} * ||b_{i+1}^*||$. Let the new value be $D'_{B,i}$

So $\frac{D'_{B,i}}{D_{B,i}} = \frac{D_{B,i-1} * ||b_{i+1}^*||}{D_{B,i}}$
$\implies \frac{\prod_{j=1}^{i-1}(||b_j^*||)||\mu_{i+1,i}b_i^* + b_{i+1}^*||}{\prod_{j=1}^{i}||b_j^*||}$

$$\frac{||\mu_{i+1,i}b_i^* + b_{i+1}^*||}{||b_j^*||} \leq \sqrt{\delta} \tag{3.10}$$

Note: This equation is called Lazslo's Condition and is used in the next chapter.

Now clearly D_B decreases by a multiplicative factor of $\sqrt{\delta}$. Initial maximum possible value of D_B is $(max_i||b_i||)^{\frac{n(n+1)}{2}}$ As D_B is an integer and determinant it has to be at least 1. So number of iterations are $log_{\frac{1}{\sqrt{\delta}}} D_{B,initial}$
$\implies \frac{logD_{B,initial}}{log\frac{1}{\sqrt{\delta}}}$
So maximum possible iterations are $\frac{\frac{n(n+1)}{2}log(max_i(||b_i||))}{log\frac{1}{\sqrt{\delta}}}$

This is a polynomial in M. □

3.3 q-ary Lattices

There are different ways to define a q-ary lattice.

Definition 3.26. q-ary lattice: A lattice Λ is q-ary for some $q \in \mathbb{Z}^+$ if $q\mathbb{Z}^n \subset \Lambda$.[18] We can define them using a matrix $A \in Z_q^{k*n}$. 2 different q-ary lattices can be defined for a given $A \in Z_q^{k*n}$ where q,n,k are positive integers such that $k \leq n$.

$$\Lambda^{\perp}(A) = \{x \in Z^n | A * x \, modq = 0\} \tag{3.11}$$

$$\Lambda(A) = \{x \in Z^n | x \, mod \, q = A^T * s, s \in Z_q^k\} \tag{3.12}$$

3.3.1 Few Results for q-ary Lattices

We start by defining a simple group theory theorem that will come in handy later.

Theorem 3.27. *Fundamental Homomorphism Theorem(FHT): If $\phi : G \mapsto H$ is a homomorphism , then $Im(\phi) \cong \frac{G}{Ker(\phi)}$*

Now we define a few simple results on q-ary lattices:

Lemma 3.28. *i)*$\Lambda(A) = q.\widehat{\Lambda^{\perp}(A)}$ *ii)* $\Lambda^{\perp}(A) = q.\widehat{\Lambda(A)}$

Proof. i) Let $y \in \Lambda(A)$
$\implies y \, mod \, q = A^T s$ where $s \in Z_q^k$
$\implies y = A^T s + qu$ where $u \in Z^n$

Let $y' \in \Lambda^{\perp}(A)$ $Ay' \, mod \, q = 0$
$\implies Ay' = qu'$ where $u' \in Z^k$
Now $\frac{y}{q} = \frac{A^T * s}{q} + u$
If $\frac{\Lambda(A)}{q} = \widehat{\Lambda^{\perp}(A)}$
then $\frac{\Lambda(A)}{q}$ and $\Lambda^{\perp}(A)$ should be each others dual
Inner product between elements of $\frac{\Lambda(A)}{q}$ and $\Lambda^{\perp}(A)$ must be an integer

$\langle \frac{y}{q}, y' \rangle \implies \langle \frac{A^T s}{q} + u, y' \rangle$
$\implies \langle \frac{A^T s}{q}, y' \rangle + \langle u, y' \rangle$
$\implies \frac{\langle s, Ay' \rangle}{q} + \langle u, y' \rangle$
$\implies \frac{\langle s, qu' \rangle}{q} + \langle u, y' \rangle$
$\implies \langle s, u' \rangle + \langle u, y' \rangle$
$\langle s, u' \rangle \in Z$ as $s \in Z_q^k andu' \in Z^k$ and $\langle u, y' \rangle \in Z$ as $u \in Z^n$ and $y' \in Z^n$

Hence $\frac{\Lambda(A)}{q} = \widehat{\Lambda^{\perp}(A)}$

ii) Let $y' \in \Lambda^{\perp}(A)$
So $Ay' = qu$
Let $y \in \Lambda(A)$
So $y = A^T s + qu$
Inner product of $\frac{y'}{q}$ and y must be an integer for the lemma to be true.
$\langle \frac{y'}{q}, y \rangle \implies \langle \frac{y'}{q}, A^T s \rangle + \frac{q}{q} \langle y', u \rangle$
Now $\langle y', u \rangle \in Z$
Also $\langle \frac{y'}{q}, A^T s \rangle \implies \langle \frac{Ay'}{q}, s \rangle$
$\implies \langle \frac{qu}{q}, s \rangle$
$\implies \langle u, s \rangle$ Now $\langle u, s \rangle \in Z$ and $\langle y', u \rangle \in Z$ so their sum is in Z.

So $\frac{\Lambda^{\perp}(A)}{q}$ and $\Lambda(A)$ are duals of each other. Hence $\Lambda^{\perp}(A) = q.\widehat{\Lambda(A)}$

Hence Proved. □

Lemma 3.29. *$det(\Lambda(A)) * det(\Lambda^{\perp}(A)) = q^n$*

Proof. Lemma 2.28 shows that $\frac{\Lambda(A)}{q}$ and $\Lambda^{\perp}(A)$ are duals of each other.

Hence $det(\frac{\Lambda(A)}{q}) * det(\Lambda^{\perp}(A)) = 1$
$\implies \frac{det(\Lambda(A))}{q^n} * det(\Lambda^{\perp}(A)) = 1$
$\implies det(\Lambda(A)) * det(\Lambda^{\perp}(A)) = q^n$

So product of determinant of q-ary matrix and its q-scaled dual is always q^n □

Lemma 3.30. *L is a lattice $L \subset R^n$ and $L' \subset L$ is a sublattice of L.*[16]
1. $|\frac{L}{L'}| < \infty$ iff span(L)=span(L')
2. if $|\frac{L}{L'}| < \infty$ then $|\frac{L}{L'}| = \frac{det(L')}{det(L)}$

Lemma 3.31. *For any $A \in Z_q^{k*n}$ $det(\Lambda(A)) = \frac{q^n}{|AZ_q^n|}$*

Proof. Let L= Z^n and L'=$\Lambda^{\perp}(A)$ We know $|\frac{L}{L'}| = |\frac{Z^n}{\Lambda^{\perp}(A)}| = \frac{det(\Lambda^{\perp}(A))}{det(Z^n)} = det(\Lambda^{\perp}(A))$

We define a function $f : Z^n \mapsto Z_q^k$ such that $f(x) = Ax\, mod q$
Now we show f is a homomorphism
f(x*y)=f(x)*f(y)

select $x, y \in Z^n$
f(x)=Ax modq and f(y) = Ay modq
f(x*y) = A(x+y) mod q

$\implies$ ((Ax mod q) + (Ay mod q))mod q

$\implies$ (f(x)+f(y))mod q

$\implies$ f(x)+f(y) as f(x) and f(y) are in the field Z_q^k

Hence f is a homomorphism

Now we use Fundamental Theorem of Homomorphism on $f : Z^n \mapsto Z_q^k$

$$Im(f) \cong \frac{Z^n}{Ker(f)}$$

Since they are isomorphic they have the same order

$$|Z^n/Ker(f)| = |Im(f)|$$

As

$$\Lambda^{\perp}(A) = \{x \in Z^n | A * x\, modq = 0\}$$

we have that $\Lambda^{\perp}(A)$ is the kernel as it maps to identity element 0. Ker(f)=$\Lambda^{\perp}(A)$

$$|\frac{Z^n}{Ker(f)}| = |Im(f)|$$

$$\implies |\frac{Z^n}{\Lambda^{\perp}(A)}| = |Im(f)|$$

Im(f)= $AZ^n\, modq = AZ_q^n$ —Im(f)— = $|AZ_q^n|$

Hence det($\Lambda^{\perp}(A)$) = —Im(f)—= $|AZ_q^n|$

Now from lemma 2.29

$$det(\Lambda(A)) = \frac{q^n}{|AZ_q^n|}$$

□

Corollary 3.32. $q^{(n-k)} \leq Vol(\Lambda(A)) \leq q^n$

Proof. In a q-ary lattice $qZ^n \subset \Lambda(A)$ we have $vol(\Lambda(A) \leq vol(qZ^n) \implies vol(\Lambda(A)) \leq q^n$
Now $Vol(\Lambda(A)) = det(\Lambda(A)) = \frac{q^n}{|AZ_q^n|}$ (Using Lemma 2.31)
The maximum value possible for $|AZ_q^n| = q^k$ So minimum determinant possible is when $|AZ_q^n| = q^k$
$det(\Lambda(A)) \geq q^{(n-k)}$ □

Lemma 3.33. *For any q and $A \in Z_q^{k*n}$ the following conditions are equivalent: i) $det(\Lambda^{\perp}(A)) = q^k$ ii)$det(\Lambda(A)) = q^{n-k}$ iii)$AZ_q^n = Z_q^k$*

Proof. i-ii) is trivial using Lemma 2.29
ii)-iii) Using Lemma 2.31 we get $|AZ_q^n| = q^k$
AZ_q^n forms vectors in Z_q^k
Hence $AZ_q^n \subset Z_q^k$
Also $|Z_q^k| = q^k$ and from lemma 4 we got $AZ_q^n = q^k$ So we have $AZ_q^n \subset Z_q^k$ and $|Z_q^k| = |AZ_q^n|$ so $AZ_q^n = Z_q^k$
iii)-i) Since $AZ_q^n = Z_q^k$ we have $|AZ_q^n| = |Z_q^k| = q^k$
Now using lemma 2.31 we get $det(\Lambda(A)) = q^{n-k}$
Using lemma 2.29 we get $det(\Lambda^{\perp}(A)) = q^k$
Hence Proved. □

Lemma 3.34. *Let L(B) be an integer lattice with basis $B \in Z^{n*n}$. Let q be any positive integer multiple of det(B). Then L(B) is q-ary.[26]*

Proof. Let us have a vector of the form qx where $x \in Z^n$. Clearly $qx \in qZ^n$
If we show $qx = By$ for some $y \in Z^n$ it possible to form all vectors in qZ^n from the lattice.
$y = B^{-1} * qx$. We can compute adjoint of matrix. Since it involves calculating co-factors and as all entries of matrix are in Z we have $adj(B) \in Z^{n*n}$. $y = \frac{q}{det(B)} * adj(B)x$ as q is multiple of det(B) we have $y \in Z^n$
So such a y exists. Hence proved. □

Lemma 3.35. *Every rational lattice is q-ary for some positive integer q. [26]*

Proof. Let lattice L have basis $B \in Q^{n*n}$ We find the lcm of all the denominators of rational numbers in B. Let it be $p \in N$.
So $B' = pB \in Z^{n*n}$
Let $q = det(B')$. Then L(B') is pq-ary lattice as pq is a multiple of det(B'). So $L(B) = \frac{L(B')}{p}$ is a q-ary lattice. □

Lemma 3.36. *Left over volume for q-ary lattices for $i = \{1, 2, \ldots, n\}$ we have $\sum_{j=i+1}^{n} l_j \leq (n-i)lnq$*

Chapter 4

An Analysis of the Bounded Distance Decoding Problem for q-ary lattices

4.1 Introduction

The Bounded Distance Decoding problem is a special case of CVP where the maximum distance between the given point and the lattice is bound.

Definition 4.1. Bounded Distance Decoding Problem: Given a lattice L with Basis B and target vector $t \in span(L(B))$ such that $t = v + e$ where $v \in L(B)$ and $|e| < r$ (r is the approximation factor). Find v. (Note for solution to be unique $r < \frac{\lambda_1}{2}$)

The classical polynomial time algorithm to solve the BDD problem requires an exponential factor of $r = \frac{1}{2^{\theta(n)}}$. Recently Eldar and Hallgren[5] demonstrated a polynomial-time quantum algorithm which can solve the BDD problem for a special class of lattices with an approximation factor of $r = \frac{1}{2^{\theta(\sqrt{n})}}$. The special class of lattices is

$$L_a = q\mathbb{Z}^n + a\mathbb{Z} \tag{4.1}$$

where $a \in \mathbb{Z}^n$

Revisit the definition:

$$\Lambda(A) = \{x \in Z^n | x \, mod \, q = A^T * s, s \in Z_q^k\}$$

Note for the special case of $k = 1$ we get L_a

Ducas and Woerden[10] gave a mathematical proof showing how the same approximation factor is achieved classically for the special class of lattice L_a. This work extends the same proofs for a lattice $\Lambda(A)$ with varying k.

To solve the BDD problem we first reduce the basis using the LLL algorithm or any other lattice basis reduction algorithm. After that we apply Babai's Nearest Plane algorithm.

Babai's Nearest Plane algorithm: Given a basis (b_i) of a lattice L, with associated Gram-Schmidt basis (b_i^*), Babai's Nearest Plane algorithm solves BDD for radius upto $r = \frac{min||b_i^*||}{2}$

4.2 Analysis of $\Lambda(A)$ for varying k

for $i \leq \sqrt{n}$ we have $l_i \geq l_{i-1} - iln\delta$
$\implies l_i \geq ln\lambda_1 - \sqrt{n}ln\delta$

$$l_i \geq ln\lambda_1 - \sqrt{n}ln\delta \tag{4.2}$$

Hence for $i \leq \sqrt{n}$ we always have l_i greater than a polynomial of $\sqrt{n}$
Using Corollary 1 we get

$$(n-k)lnq \leq \sum_{j=1}^{n} l_j \leq nlnq$$

Subtracting fact 4 from this we get

$$(i-k)lnq \leq \sum_{j=1}^{i} l_j$$

$$\sum_{j=1}^{i} l_j \leq \sum_{j=1}^{i} l'_j \leq i\,lnq$$

as maximum value of l'_i is lnq

$$(i-k)lnq \leq \sum_{j=1}^{i} l_j \leq i\,lnq$$

Let $d = \sqrt{n}$

4.2.1 Case 1: $k < d$

For $i = \{1, 2, \ldots, d\}$ we have equation (3.1). for $i = \{d+1, d+2, \ldots, n\}$, we prove inequality below

$$(i-k)lnq \leq \sum_{j=1}^{i} l_j$$

$$\sum_{j=1}^{i-d} l_j \leq (i-d)lnq$$

Subtract the 2 equations

$$(d-k)lnq \leq \sum_{j=i-d+1}^{i} l_j$$

Using Lazslo's condition

$$l_j \leq l_i + (i-j)ln\delta$$

$$(d-k)lnq \leq dl_i + ln\delta \sum_{i=0}^{d-1} i$$

$$\implies (d-k)lnq \leq dl_i + ln\delta \frac{d(d-1)}{2}$$

$$\implies (1-\frac{k}{d})lnq \leq l_i + ln\delta \frac{(d-1)}{2}$$

$$\implies min(l_i)\, i \in \{d, d+1, \ldots, n\} \geq \frac{d-k}{d}lnq - \frac{d-1}{2}ln\delta$$

Now we have $q = c^n$

$$\implies min(l_i) \geq lnq - \frac{knlnc}{d} - \frac{dln\delta}{2}$$

$$\implies min(l_i) \geq ln\lambda_1 - \sqrt{n}klnc - \frac{\sqrt{n}ln\delta}{2}$$

$min(l_i)$ for $\{i = d, d+1 \ldots, .., n\} \geq ln(\frac{\lambda_1}{c^{\sqrt{n}k}\sqrt{\delta}^{\sqrt{n}}})$

Hence the Approximation factor has a power of $O(\sqrt{n}k)$

4.2.2 Case 2: $k = d$

for $i = \{1, 2, \dots, k\}$, we have $l_i \geq ln\lambda_1 - \sqrt{n}ln\delta$
for $i = \{k+1, k+2 \dots, 2k\}$
We have using Lazslo's condition

$$l_j \leq l_i + (i-j)ln\delta$$

$$\implies l_{i-k} \leq l_i + k * ln\delta$$

As $i-k$ has range $\{1, 2 \dots, k\}$ we can use condition for $i \leq \sqrt{n}$

$$ln\lambda_1 - \sqrt{n}ln\delta \leq l_i + k * ln\delta$$

$$\implies ln\lambda_1 - 2 * \sqrt{n} * ln\delta \leq l_i$$

for $i = \{2k+1, 2k+2 \dots, n\}$

$$\sum_{j=1}^{i-2d} l_j \leq (i-2d)lnq$$

$$\sum_{j=1}^{i} l_j \geq (i-k)lnq$$

Subtracting above 2 equations we get:

$$\sum_{j=i-2d+1}^{i} l_j \geq (2d-k)lnq$$

$$\implies \sum_{j=i-2d+1}^{i} l_j \geq klnq$$

Using Lazslo's condition

$$\sum_{j=i-2d+1}^{i} \{l_i + (i-j)ln\delta\} \geq klnq$$

$$\implies 2dl_i + \frac{(2d-1)*2d}{2} * ln\delta \geq klnq$$

$$\implies 2l_i \geq lnq - (2d-1)ln\delta$$

$$\implies l_i \geq \frac{lnq - (2d-1)ln\delta}{2}$$

$$l_i \geq \frac{ln\lambda_1}{2} - dln\delta$$

$$l_i \geq ln\frac{\sqrt{\lambda_1}}{\delta^{\sqrt{n}}}$$

or

$$2dl_i + \frac{(2d-1)*2d}{2} * ln\delta \geq klnq$$

$$\implies 2dl_i + \frac{(2d-1)*2d}{2} * ln\delta \geq klnq$$

$$\implies l_i \geq \frac{lnq - (2d-1)ln\delta}{2}$$

$$\implies l_i \geq \frac{n * lnc}{2} - dln\delta$$

$$\implies l_i \geq ln\frac{c^{n/2}}{\delta^{\sqrt{n}}}$$

Hence

$$minl_i \geq min(ln\frac{\sqrt{\lambda_1}}{\delta^{\sqrt{n}}}, ln\frac{\lambda_1}{\delta^{2\sqrt{n}}})$$

By graphical analysis $ln\frac{\lambda_1}{\delta^{2*\sqrt{n}}}$ is smaller.

4.2.3 Case 3: $k > d$

We break the range into 3 different subranges. First range varies from $\{1 \dots d\}$, second range varies from $\{d+1, \dots, pd\}$ where $p = ceil(\frac{k}{d})$ and $\{pd+1, pd+2 \dots, n\}$

for $i = \{1, 2 \dots, d\}$ we have ,

$l_i \geq ln\lambda_1 - \sqrt{n}ln\delta$

for $i = \{d+1, \dots, pd\}$ p is defined as the smallest positive integer such that $pd > k$ So $p = ceil(\frac{k}{d})$ for $i = \{d+1, \dots, 2d\}$ $l_j \leq l_i + (i-j)ln\delta$ $l_{i-d} \leq l_i + d * ln\delta$ range of $i - d$ is $\{1, 2, \dots, d\}$ Hence $l_{i-d} \geq ln\lambda_1 - \sqrt{n}ln\delta$
So $l_i \geq ln\lambda_1 - 2 * \sqrt{n}ln\delta$

Similarly for $i = \{2d+1, 2d+2, \ldots, 3d\}$ we have $l_i \geq ln\lambda_1 - 3 * \sqrt{n} ln\delta$
and for $i = \{(p-1)d+1, \ldots, pd\}$ $l_i \geq ln\lambda_1 - p * \sqrt{n} ln\delta$

$$l_i \geq ln\frac{\lambda_1}{\delta^{p*\sqrt{n}}}$$

Now for $i = \{pd+1, pd+2 \ldots, n\}$

$$\sum_{j=1}^{i-pd} l_j \leq (i-pd)lnq$$

$$\sum_{j=1}^{i} l_j \geq (i-k)lnq$$

Subtracting the equations:

$$\sum_{j=i-pd+1}^{i} l_j \geq (pd-k)lnq$$

$$\sum_{j=i-pd+1}^{i} (l_i + (i-j)ln\delta) \geq (pd-k)lnq$$

$$pd * l_i + \frac{(pd-1)*pd}{2} ln\delta \geq (pd-k)lnq$$

$$l_i \geq lnq - \frac{klnq}{pd} - \frac{pd}{2} ln\delta$$

$$l_i \geq ln(\frac{q}{q^{k/pd}\delta^{pd/2}})$$

$$l_i \geq ln(\frac{\lambda_1}{q^{k/pd}\delta^{pd/2}})$$

or Now $k/pd = 1 - \epsilon$ where $\epsilon \in 0$ and 1

$$l_i \geq ln(\frac{q^{\epsilon}}{\delta^{k/2}})$$

Table 4.1: Approximation factor for varying k

Conditions	Approximation Ratio
$k < \sqrt{n}$	$\frac{\lambda_1}{2*c^{\sqrt{n}k}\sqrt{\delta}^{\sqrt{n}}}$
$k = \sqrt{n}$	$\frac{\lambda_1}{4*c^{\sqrt{n}k}\sqrt{\delta}^{\sqrt{n}}}$
$k > \sqrt{n}$	$min(\frac{\lambda_1}{2*c^n\delta^{k/2}}, \frac{\lambda_1}{2*\delta^k})$

Hence for $i = \{1, 2, \ldots, n\}$

$$l_i \geq min(ln(\frac{\lambda_1}{c^{nk/pd}\delta^{pd/2}}), ln\frac{\lambda_1}{\delta^{p*\sqrt{n}}}, ln(\frac{\lambda_1}{\delta\sqrt{n}}))$$

or

$$l_i \geq min(ln(\frac{\lambda_1}{q^{1-\epsilon}\delta^{k/2}}), ln\frac{\lambda_1}{\delta^{p*\sqrt{n}}}, ln(\frac{\lambda_1}{\delta\sqrt{n}}))$$

Approximating by disregarding ceil function we get,

$$l_i \geq min(ln(\frac{\lambda_1}{c^n\delta^{k/2}}), ln(\frac{\lambda_1}{\delta^k}), ln(\frac{\lambda_1}{\delta\sqrt{n}}))$$

4.3 Results

The above analysis showed how the Bounded Distance Decoding problem can be solved with better approximations for certain lattices. These lattices are q-ary lattices generated by equation 2.11 and 2.22. Depending on the count of generating vectors and the dimension of the lattice the approximation factor may get more relaxed.

Table 3.1 shows how the approximation factor changes with changes with the conditions between $\sqrt{n}$ and d. If the number of generating vectors(k) $k \leq \sqrt{n}$ the approximation factor is subexponential. The radius of the Euclidean ball from the vector $v \in L(B)$ for which the target vector t can be solved is of the form $\frac{c_1}{2^{c_2*\sqrt{n}}}$ instead of the form $\frac{c_1}{2^{c_2*n}}$. For $k > \sqrt{n}$ the approximation factor does not change.

4.4 Conclusion

The work in this thesis attempted to solve a special case of an NP-Hard problem. The work found a new class of lattices for which the BDD problem can be solved better. A study in the relation between the BDD problem and other hard lattice problems can show how the LLL algorithm can give better results for q-ary lattices with special conditions. This work helped increase the understanding of lattices. NIST is in the final round of the Post-quantum Cryptography Standardization Process. Any new information about lattices can prove crucial into finding an attack against one of the cryptosystems. The work found new results on one hard problem and this can be used as a tool when searching for vulnerabilities in any of the NIST-PQC lattice candidates

Bibliography

[1] URL: https://www.esat.kuleuven.be/cosic/pqcrypto/saber/.

[2] URL: https://falcon-sign.info/.

[3] URL: https://sphincs.org/.

[4] URL: https://classic.mceliece.org/.

[5] *An Efficient Quantum Algorithm for Lattice Problems Achieving Subexponential Approximation Factor.* https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/Bgcj5HgHOHO. (Accessed on 12/09/2021).

[6] D.J. Bernstein. "Introduction to post-quantum cryptography". English. In: *Post Quantum Cryptography.* Ed. by D.J. Bernstein, J. Buchmann, and E. Dahmen. Germany: Springer, 2009, pp. 1–14. ISBN: 978-3-540-88701-0.

[7] *CRYSTALS.* URL: https://pq-crystals.org/kyber/.

[8] *CRYSTALS.* URL: https://pq-crystals.org/dilithium/.

[9] Jintai Ding and Dieter Schmidt. "Rainbow, a New Multivariable Polynomial Signature Scheme". In: *Applied Cryptography and Network Security.* Ed. by John Ioannidis, Angelos Keromytis, and Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 164–175. ISBN: 978-3-540-31542-1.

[10] Léo Ducas and Wessel van Woerden. *A note on a Claim of Eldar Hallgren: LLL already solves it.* Cryptology ePrint Archive, Report 2021/1391. https://ia.cr/2021/1391. 2021.

[11] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. "NTRU: A ring-based public key cryptosystem". In: *Algorithmic Number Theory.* Ed. by Joe P. Buhler. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 267–288. ISBN: 978-3-540-69113-6.

[12] Travis S. Humble. "Consumer Applications of Quantum Computing: A Promising Approach for Secure Computation, Trusted Data Storage, and Efficient Applications". In: *IEEE Consumer Electronics Magazine* 7.6 (Oct. 2018). ISSN: 2162-2248. DOI: 10.1109/MCE.2017.2755298. URL: https://www.osti.gov/biblio/1490615.

[13] *introduction.pdf.* https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/ln/introduction.pdf. (Accessed on 12/09/2021).

[14] David Jao and Luca De Feo. “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies”. In: *Post-Quantum Cryptography.* Ed. by Bo-Yin Yang. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 19–34. ISBN: 978-3-642-25405-5.

[15] *Lattices in Computer Science (Fall 2009).* `https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/`. (Accessed on 12/09/2021).

[16] *lecture-2.pdf.* `https://homepages.cwi.nl/~dadush/teaching/lattices-2018/notes/lecture-2.pdf`. (Accessed on 12/09/2021).

[17] *lecture-3.pdf.* `https://homepages.cwi.nl/~dadush/teaching/lattices-2018/notes/lecture-3.pdf`. (Accessed on 12/09/2021).

[18] *Lecture2.pdf.* `https://homes.esat.kuleuven.be/~nsmart/FHE-MPC/Lecture2.pdf`. (Accessed on 12/09/2021).

[19] *lll.pdf.* `https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/ln/lll.pdf`. (Accessed on 12/09/2021).

[20] Daniele Micciancio and Oded Regev. “Lattice-based Cryptography”. In: *Post-Quantum Cryptography.* Ed. by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191. ISBN: 978-3-540-88702-7. DOI: `10.1007/978-3-540-88702-7_5`. URL: `https://doi.org/10.1007/978-3-540-88702-7_5`.

[21] Christof Paar and Jan Pelzl. “Introduction to Public-Key Cryptography”. In: *Understanding Cryptography: A Textbook for Students and Practitioners.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 149–171. ISBN: 978-3-642-04101-3. DOI: `10.1007/978-3-642-04101-3_6`. URL: `https://doi.org/10.1007/978-3-642-04101-3_6`.

[22] Christof Paar and Jan Pelzl. “The Data Encryption Standard (DES) and Alternatives”. In: *Understanding Cryptography: A Textbook for Students and Practitioners.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 55–86. ISBN: 978-3-642-04101-3. DOI: `10.1007/978-3-642-04101-3_3`. URL: `https://doi.org/10.1007/978-3-642-04101-3_3`.

[23] *Picnic.* 2020. URL: `https://www.microsoft.com/en-us/research/project/picnic/`.

[24] Eberhard Stickel. “A New Method for Exchanging Secret Keys”. In: *Proceedings of the Third International Conference on Information Technology and Applications (ICITA’05) Volume 2 - Volume 02.* ICITA ’05. USA: IEEE Computer Society, 2005, 426–430. ISBN: 0769523161. DOI: `10.1109/ICITA.2005.33`. URL: `https://doi.org/10.1109/ICITA.2005.33`.

[25] *Supersingular Isogeny Key Encapsulation.* URL: `https://sike.org/`.

[26] *Talk-Post-Quantum-Cryptography-lattice-based-cryptosystems.pdf.* `https://www.wallenborn.net/download/Talk-Post-Quantum-Cryptography-lattice-based-cryptosystems.pdf`. (Accessed on 12/09/2021).