International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I1P214
Volume 69 Issue 1, 92-96, January 2021

Survey of Lattice to Design Post Quantum Cryptographic Algorithm Using Lattice

Dr. Uma Pujeri[#1], Dr. P. S. Aithal[*2], & Dr. Ramachandra Pujeri[#3]

[#1] *Research scholar, Computer Engineering, Srinivas University, Mangaluru, Karnataka, India*
[#2]*Vice Chancellor,* Srinivas University, Mangaluru, Karnataka, *India*
[#3]*Director, MIT ADT University, Loni Kalbhor, Pune, Maharashtra, India*

[1]umaresearch81@gmail.com, [2] psaithal@gmail.com, [3] sriramu_vp@gmail.com

Abstract *— **Objective:** Quantum algorithms are stronger and more secure than classical computers because they run on faster, harder ones and require fewer steps. With Quantum computers, the attackers have high computing power, and with a quantum, the algorithm can easily break the cryptographic system. Lattice is a regularly spaced grid of points stretching to infinity. Quantum safe security algorithms are resistant to both attacks caused by quantum computers and attacks caused by classical computers. Lattice-based cryptography is the post-quantum cryptographic standards resistant to the attacks from quantum computers, hence having the advantage of strong security and high efficiency. The paper's main objective is to study Lattice, lattice properties, Lattice – based cryptographic algorithm to design new Lattice-based cryptographic algorithms that are quantum resistant in the future.*

Methods: *In this paper, lattice-based cryptography is discussed right from its seminal work to its efficient cryptographic schemes. Paper discusses Lattice, lattice properties, lattice problem, the algorithmic solution to lattice problem, and lattice-based cryptography.*

Findings: *After studying post-quantum cryptographic algorithms using Lattice, lattice-based post-quantum cryptographic algorithms are resistant to quantum computer attacks.*

Novelty: *The paper discusses Lattice, properties of Lattice in a simple way. Widely used cryptographic algorithms like RSA, Diffie-Hellman Key exchange, Elliptic Curve Cryptography are not resistant to quantum computer attacks. Paper discusses the importance of a post-quantum algorithm using Lattice that is resistant to quantum computer attacks.*

Keywords *— Cryptography, Quantum Computer, Post Quantum Cryptography, Lattice, Lattice-based cryptography.*

I. INTRODUCTION

A lattice can be defined as a set of basis vectors in a regularly spaced grid of points.

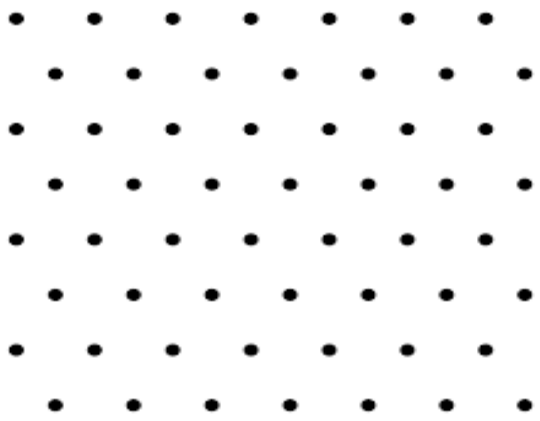

Figure 1. Two Dimensional Lattice where points represent vector and Lattice is evenly spaced vectors.

A two-dimensional lattice vector means points, and a lattice is an evenly spaced vector. For the origin vector, all coordinates are set to zero(0,0). The vector is termed a long vector if it is far away from the origin, and it is termed as a short vector if it is near the origin vector. So a lattice is n linearly independent vectors where b1, b2,…….bn are the basis of the lattices, and lattices generated by this set of vectors is

$$L(b1, b2, b3, \ldots\ldots\ldots bn) = \sum_{n} xi\ bi \qquad xi \in Z \text{ and } bi \in R^n \text{ [1].}$$

Quantum safe security is the algorithm resistant to both classical attacks and several attacks done by quantum computers.

Post-quantum cryptography can also be called quantum-safe cryptography, quantum-resistant cryptography, or quantum-proof cryptography. Post Quantum cryptographic algorithms are unbreakable, secure, and resistant to a quantum computer's attack. Lattice-based cryptography is post-quantum cryptography that is resistant, efficient, and simple in implementation.

This paper discusses lattice properties, lattice problem, an algorithm that provides a lattice problem, Lattice-based cryptography, conclusion, and future work.

II. LATTICE PROPERTIES [2]

Important properties that lead to interesting special classes of lattices are discussed in this session.

A. Completeness [3][5]

A poset is a complete lattice if all its subsets have both supremum (join) and infimum (meet). A partially ordered set is a complete lattice if every subset of a Lattice L has the greatest lower bound **Λ(meet)** and least upper bound **V(join).**

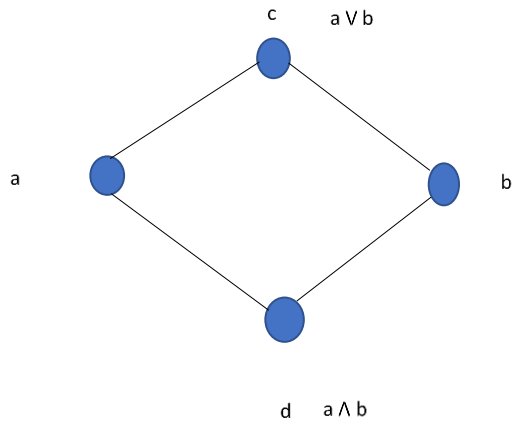

Figure 2. Complete Lattice where a V b is the Join and is a Λ b meet

B. POSET and Lattice [3][4][5]

Let R be a set A, then R is a partial order on A if it is reflexive, anti-symmetric, and transitive. Set A with partial ordering relation R is called POSET and is denoted by (S, R)

a) Comparability

"Two elements u and v of a set S that are partially ordered are said to be comparable if either u < = v or v <= u else u and v are incomparable."[3]

Example: - In the POSET (Z+, /) where Z+ is set of all positive integers and / is division relation, then elements 2 and 4 are comparable since 2/4 2 divides 4, but element 2 and 15 are not comparable since 2 ł 15 since 2 does not divide 15.

b) Total Order

"In a POSET, any pair of distinct elements are comparable that is u < v or v < u then such POSET is called total order. A ordered set is also called as a chain".[3]

c) Extremums in POSETS

Elements in POSET have external properties, which are important for many applications.

1) Maximal Element

An element x is maximal if no element y is greater than x in the POSET.

2) Minimal Element

An element x is minimal if there is no element y, which is smaller than x in the POSET.

c) Bounds in a POSET][3] [4]

The largest element in set A of a POSET is called the upper bound. Similarly smallest element in a set A of a POSET is called lower bound for set A. The least lower bounds are the elements that are lesser than other lower bounds, and the greatest upper bound are the elements that are greater than another upper bound. Consider figure for a set b and c upper bound are e,g and h least upper bound is e, greatest upper bound is h. For a set b and c, lower bounds a and greatest lower bound is also a.

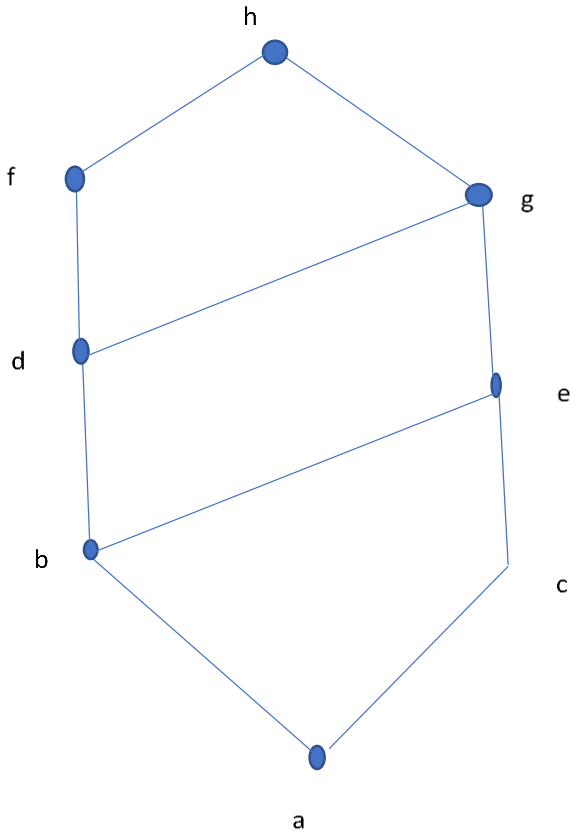

Figure 3. Consider set b and c, and then upper bound are e g h and least upper bound is e. The lower bound is a hence the greatest lower bound is a.

d) Lattice

"A POSET in which every pair element has both least upper bound and a greatest lower bound is called lattice"[2].

C. Algebra of Lattice[5]

Two binary operations Join and Meet in Lattice

a) Join

Join of a two-element is denoted by V and is called least upper bound.

b) Meet

The meet of a two-element is denoted by **Λ** and is called the greatest lower bound.

Identities of Join and Meet

Table 1: Identities for Join and Meet.

Sr. No	Identity	Meet	Join
1	Commutativity	A Λ B = BΛ A	A V B = B V A
2	Associativity	(A Λ B) Λ C = A Λ (B Λ C)	(A V B) V C = A V (B V C)
3	Idempotency	A Λ A = A	AV A = A
4	Absorption law	A V (A Λ B) = A	A Λ (A V B) = A

D. Distributive Lattice

A distributive lattice is a lattice in which join V and meet **Λ** distribute over each other. For x, y, z in the lattices following is the distributive law, which is satisfied

Distributive **Λ over V A Λ (B V C) = (A Λ B) V C.**

Distributive V over **Λ A V (B Λ C) = (A V B) Λ C.**

E. Linear Order [4]

A linear order on a set S is a (binary) relation < with the following properties

- Reflexivity: a ≮ a
- Asymmetry if a < b then b ≮ a
- Transitivity if a < b < c then a < c
- Connectedness if a ≮ b and b ≮ a then a = b

Any linear order is a distributive lattice.

F. Boolean Lattice

A Boolean lattice is a POSET such that there is an element ⊤ (a top element) such that x <= ⊤ always holds if there is an element ⊥ (a bottom element) such that ⊥ <= x always holds.

- Given an element a and b, there is an element a Λ b such that x <= a Λ b holds if and only if x <= a and x <=b.
- Given an element a and b, there is an element a V b such that a V b <= x holds if and only if a <= x and b<=x
- Given an element a there is an element ¬ a such that a **Λ** ¬ a <= ⊥ and **⊤ <= a V** ¬ a.
- Given an element a, b and c, we have a Λ (b V c) <= (a Λ b) V (a Λ c).

G. Complemented Lattice

A complemented lattice is bounded with least element as 0 greatest element as 1 where every element has a complement that is an element b satisfying

a V b = 1 and a Λ b = 0

H. Ortho Complementation

An Ortho complementation on a bounded lattice is a function that maps each element a to an ortho complement ⊥ such that the following axioms are satisfied

a ⊥ V a = 1 and a ⊥ Λ a = 0.

Involution law – a ⊥⊥ = a

Order reversing – if a <= b then b ⊥ <= a ⊥

I. Modular Identity

The modular identity is If a < = c a V (b Λ c) = (a V b) Λ c for elements a, b, c of lattice L.

J. Birkhoff Theorem [6]

The lower set is also called the down set, which is a subset L of U such that U is in L any V < = U then V is in L.

i.e. ∀ U ∈ L ∀ V ∈ U : V<= U -> V ∈ L

Birkhoff Theorem – Birkhoff theorem for distributive Lattice states that any distributive lattice elements can be represented as a finite set such that lattice operations form Union and Intersection of sets.

The Join operation corresponds to Union. The meet operation corresponds to the set Intersection. Union and Intersection obey the distributive law, and any lattice that obeys distributive law is distributive. The Birkhoff theorem states that it is possible to create any finite distributive lattice this way.

Table 2: Distributive Lattice.

Sr. No	Distributive Lattice	Set	POSET	Boolean
1	Join Operation V	Union U	Least Upper bound (supremum)	OR
2	Meet Operation Λ	Intersection ∩	The greatest lower bound (infimum)	AND

III. LATTICE PROBLEM AND ALGORITHMIC SOLUTION TO LATTICE PROBLEM

Several problems related to Lattice are believed to be computationally hard in high dimensions. Following are few lattice problems that are computationally hard.

- Closest Vector Problem (CVP) – Discover the nearest grid vector to a given vector [7]
- Shortest Vector Problem (SVP) – Discovers shortest non-zero vector in Lattice.
- Shortest Independent Vector Problem (SVIP) – Discover n independent and short vectors.

A. Closest Vector Problem and Algorithmic Solution [9][10]

A computational problem on lattices closely related to the shortest vector problem is the closest vector problem. CVP requests to discover the lattice point nearest to the target point a, given a Lattice L and a target point a. To find the nearest point to the target point, Euclidean norms are widely used. A more relaxed technique measures the distance from the target point's Lattice without necessarily finding the nearest lattice vector.

Many CVP applications only require finding the lattice vector that is not too far from the target, which may not

necessarily be the nearest vector. CVP is seen in computer science as an NP-Hard problem. For CVP, the g-approximation algorithm considers the lattice vector at most g times the distance from the ideal solution within the distance. Babai and Kannan suggested a polynomial-time algorithm to solve CVP based on reducing the Lattice and achieving an exponential approximation factor in the lattice dimension. When the Lattice dimension is sufficiently small, the heuristic method fairly finds a reasonable approximation to CVP in relatively less time. CVP is considered NP-Hard to solve roughly with any constant factor or even any sub-polynomial function of a dimension n approximate to small polynomial factor g = O√n/log n the CVP is unlikely to be NP-Hard slowly increasing.

In different cryptosystems, CVP is used where the method of decryption corresponds to CVP computation. In addition to cryptography, CVP has numerous computer science applications. Finding good CVP approximation factors that develop as a polynomial in the lattice dimension is one of the key open research problems in this period.

B. Shortest Vector Problem and Algorithmic Solution [11][12][13]

In a lattice, the Shortest Vector Problem (SVP) finds non-zero vectors. The Euclidean norm is widely used for the shortest vector problem to find a non-zero vector in Lattice. The SVP approximation algorithm's objective is to find the non-zero lattice vector nearly g (approximation factor) times the length of the optimal solution, where g is normally a lattice dimension parameter.

a) Exact Algorithm

There are three approaches in the n-dimensional lattice that provide the solution to the SVP

1) Enumeration

Enumeration have an exponential running time of $n^{(O(n))}$ and only use polynomial space to be deterministic. Many heuristic and optimization methods are produced that are used with a relatively limited dimension in practice.

2) Voronoi Cell Computation

This approach's running time to solve SVP and other lattice problem is $O(2^{2n})$ using exponential space $O(2^{n})$. These are deterministic algorithms but not competitive in practice with other applications.

3) Sieving

The running time of the sieving approach is $O(2^{n})$. Many heuristic approaches are developed in many applications with small dimensions (n=40 or n=50).

b) Approximation Algorithm

Lenstra, Lenstra, and Lovaz's approximate the shortest vector problem (SVP). The LLL algorithm transforms an arbitrary lattice base into one that generates the same reduced Lattice. Approximating SVP in the Euclidean norm is NP-Hard.

IV. LATTICE-BASED CRYPTOGRAPHIC ALGORITHM [14]

Cryptography based on Lattice is used to build cryptosystems or is used for proof of security. For post-quantum cryptography, Lattice-based cryptographic algorithms are commonly used. The most frequently used public-key algorithms and key exchange algorithms such as RSA, Diffie Hellman, and the elliptic curve chain are easily attacked by quantum computers, but both classical and quantum computers are immune to attack lattice-based cryptographic algorithms. The cryptographic algorithm based on Lattice is more stable, assuming that the computational lattice problem cannot be solved effectively.

Lattice-based cryptography includes the algorithm such as learning with errors (LWE), Ring-LWE (ring- learning with errors) key exchange, NTRE signature, BLISS signature, GGH (Goldrich Goldwasser Haleri) encryption scheme. Lattice-based cryptographic algorithms are widely used in public key post-quantum cryptography. The classical public-key cryptographic algorithm is constructed based on the hardness of factoring discrete logarithm and related problems. However, both factoring and discrete logarithmic problem are solvable in polynomial time by quantum computers. Many lattices based cryptographic algorithms are more secure, unhackable, or unsolvable by classical and quantum computers.

V. CONCLUSION AND FUTURE WORK

In this paper, we studied Lattice, where Lattice is defined as a set of basis vectors in a regularly spaced grid. Properties of Lattice, different lattice problems, Lattice-based cryptography are discussed in this paper. Well Known cryptographic algorithms like advanced AES, RSA is not resistant to attacks of quantum computers. Many Lattice-based cryptographic algorithms are unhackable or unsolvable by a classical and quantum computer.

Future Work:

To design a post-quantum cryptographic algorithm using Lattice.

REFERENCES

[1] Arora, S., L. Babai, J. Stern, and E.Z. Sweedyk. The Hardness of Approximate Optima in Lattices, Codes, and Systems of Linear Equations. Journal of Computer and System Sciences.,54(2)(1997) 317–331.

[2] George Grätzer. Latice Theory. Springer Publication.,(2011).

[3] Mathematics | Partial Orders and Lattices. https://www.geeksforgeeks.org/mathematics-partial-orders-lattices/ (accessed: 15/12/2019).

[4] Jhon B. distributive lattice. https://ncatlab.org/nlab/show/distributive+lattice (accessed 1 April 2020).

[5] Lattice. https://www.euclideanspace.com/maths/discrete/structure/lattice/index.htm (accessed 2 April 2020).

[6] Birkhoff representation theorem https://en.wikipedia.org/wiki/Birkhoff%27s_representation_theorem#:~:text=In%20mathematics%2C%20Birkhoff%27s%20representation%20theorem,unions%20and%20intersections%20of%20sets (accessed 4 April 2020).
[7] Advance topic in cryptography https://people.csail.mit.edu/vinodv/6876-Fall2015/L3.pdf (accessed 14 April 2020).
[8] Lattice Cryptography http://cseweb.ucsd.edu/~daniele/LatticeLinks/SVP.html (accessed 1 May 2020).
[9] Babai L. On Lovasz' Lattice Reduction and the Nearest Lattice Point Problem. Combinatorica 1986; 6(1): 1-13.
[10] Daniele M. Closest Vector Problem. https://cseweb.ucsd.edu/~daniele/papers/CryptoEncyclopediaCVP.pdf (accessed 10-September-2020).
[11] Shortest Vector Problem https://web.eecs.umich.edu/~cpeikert/lic13/lec02.pdf (accessed 20-September-2020).
[12] Voulgaris, Panagiotis. Algorithms for the Closest and Shortest Vector Problems on General Lattices. https://escholarship.org/content/qt4zt7x45z/qt4zt7x45z.pdf?t=ml518a (accessed 25 September 2020).
[13] Lattice and Cryptography https://www.isical.ac.in/~shashank_r/lattice.pdf (accessed 25-September-2020).
[14] Micciancio D., Regev O.,Lattice-based Cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_5., (2009).