ISAC - 2024

Beyond Classical: The Rise of Lattice-Based Encryption

Ritayudh Laha, Sauvik Dutta

Department of Computer Science, Ramakrishna Mission Vivekananda Centenary College,Rahara - 700118

Introduction

A lattice is a periodic set of points in n-dimensions formed by all vectors that are linearly independent on a set of linearly independent vectors called the basis. The fundamental region of the lattice is an n-dimensional convex shape that fills the entire space with no overlapping when repeated at every lattice point.[2]
The idea is to set the hurdles for the attacker by adding enough noise to a vector of inner products of a secret vector with random vector making the problem harder.

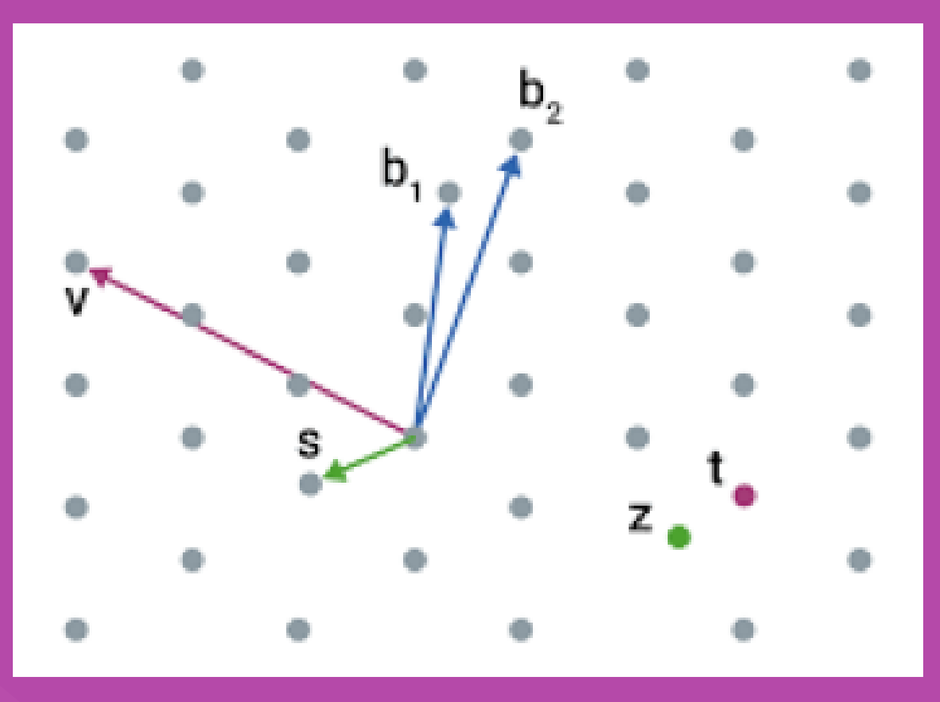


Figure 1: Diagrammatic representation of a lattice structure

Security
Key Distribution
No Cloning

Quantum over Classical

Based on fundamental quantum techniques

Protection from quantum computers

Detection of Eavesdropping

Lattice Based Public Key Cryptosystem

The system works something like this- for a positive integer n, the private key is defined as an n-dimensional secret vector. The secret vector describes a periodic set of parallel equidistant hyperplanes in n-dimensional space, the secret vector is inversely proportional to the distance between consequent hyperplanes. The decryption is done by project the ciphertext point on the secret vector from the private key, the output is 1 if the point is close to one of the hyperplanes and 0 otherwise.[2]

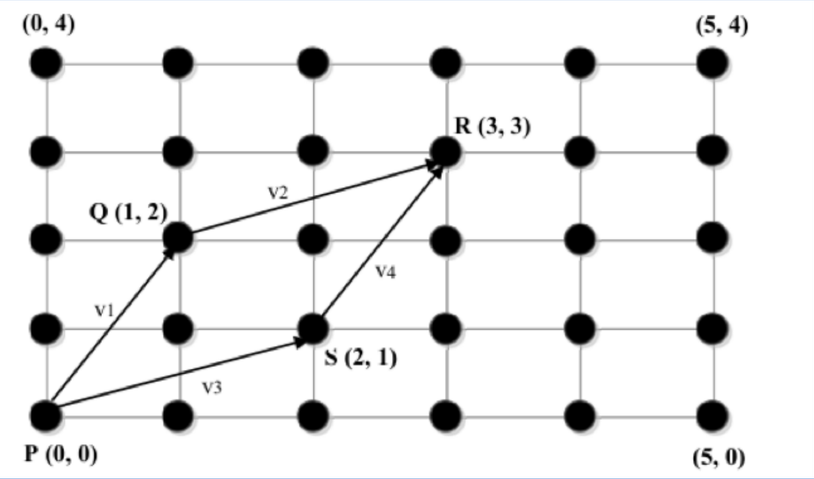


Figure 4: Example of lattice formed by two-dimensional vectors (one represented in solid red lines, the other in a blacked dashed line).[4]

LWE Public Key Cryptosystem

One of most important problems in Lattice Based Cryptography is Learning with Error (LWE) problem. The problem states that given some pairs in the form (a[i], b[i]) where a[i] is a polynomial and b[i] is a single value - all module q, it is required to differentiate where is uniformly random, or is dependent on the first component a[i] plus some small noise value:
b[i] = a[i]*s+ e[i], where s is a secret vector and e[i] is a small vector belong from Gaussian Distribution. Usually, the pairs a[i] and b[i] are given and the target is to find the secret vector s.[3]

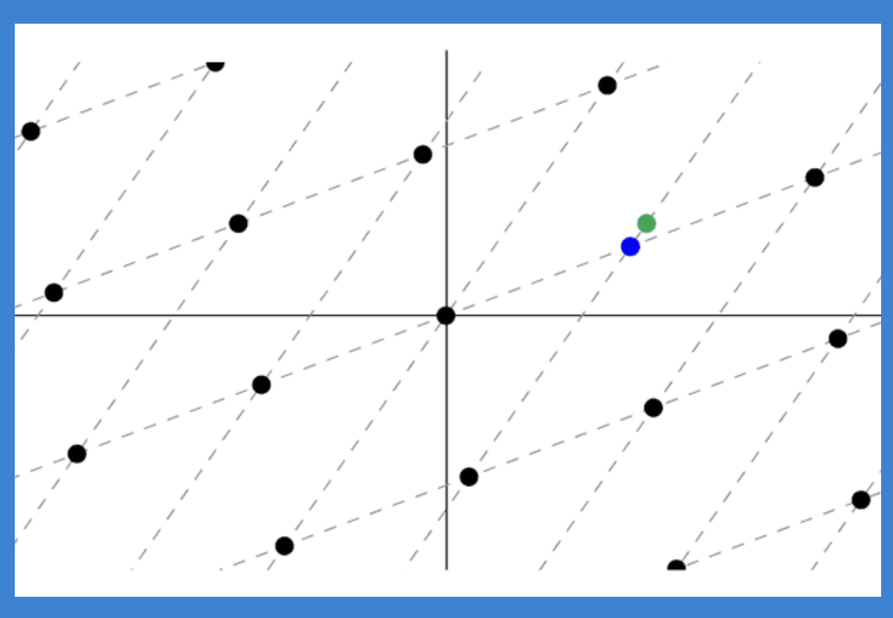
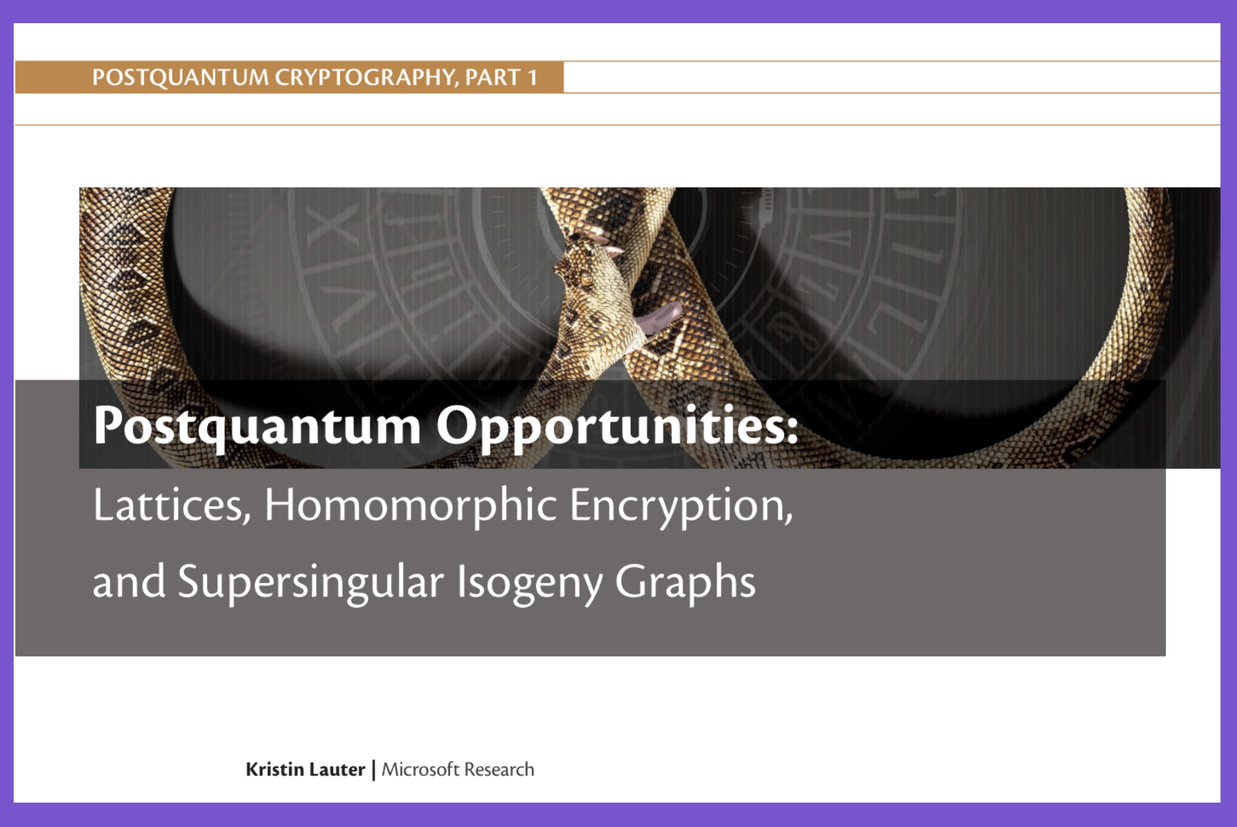


Figure 5 : LWE problem in Lattice Based Cryptography. The LWE problem can be intuitively thought as being given a point of the form b[i] = a[i]*s + e[i] (the green point) and being asked to find the point on the grid that is close to the blue point.[3]

Literature Survey

Here, we are discussing the study of Lattice Based Encryption. It was introduced in two forms independently in two different communities- mathematics and computer science. It is receiving the attentions from both the communities for standardization as a post quantum safe solution for cryptography. [2]
It encompasses protocols for both key exchange and encryption. Key exchange protocols like LWE establish shared secret keys between parties. Encryption schemes, such as NTRU Encrypt and Kyber, use lattice-based problems for secure data transmission.



POSTQUANTUM CRYPTOGRAPHY, PART 1

Postquantum Opportunities:
Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs

Kristin Lauter | Microsoft Research

Figure 2: Postquantum Opportunities: Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs
IEEE Security & Privacy
(Volume: 15, Issue: 4, 2017)

Methodology

The main idea is that to encrypt a plaintext, blind it by adding a vector of random inner products with the receiver secret key and adding a small error vector. The blinding is different each time of sending the cypher text. This makes the problem more tough for the eavesdroppers. The security of this method relies on hardness of learning with errors (LWE) problems.[2]

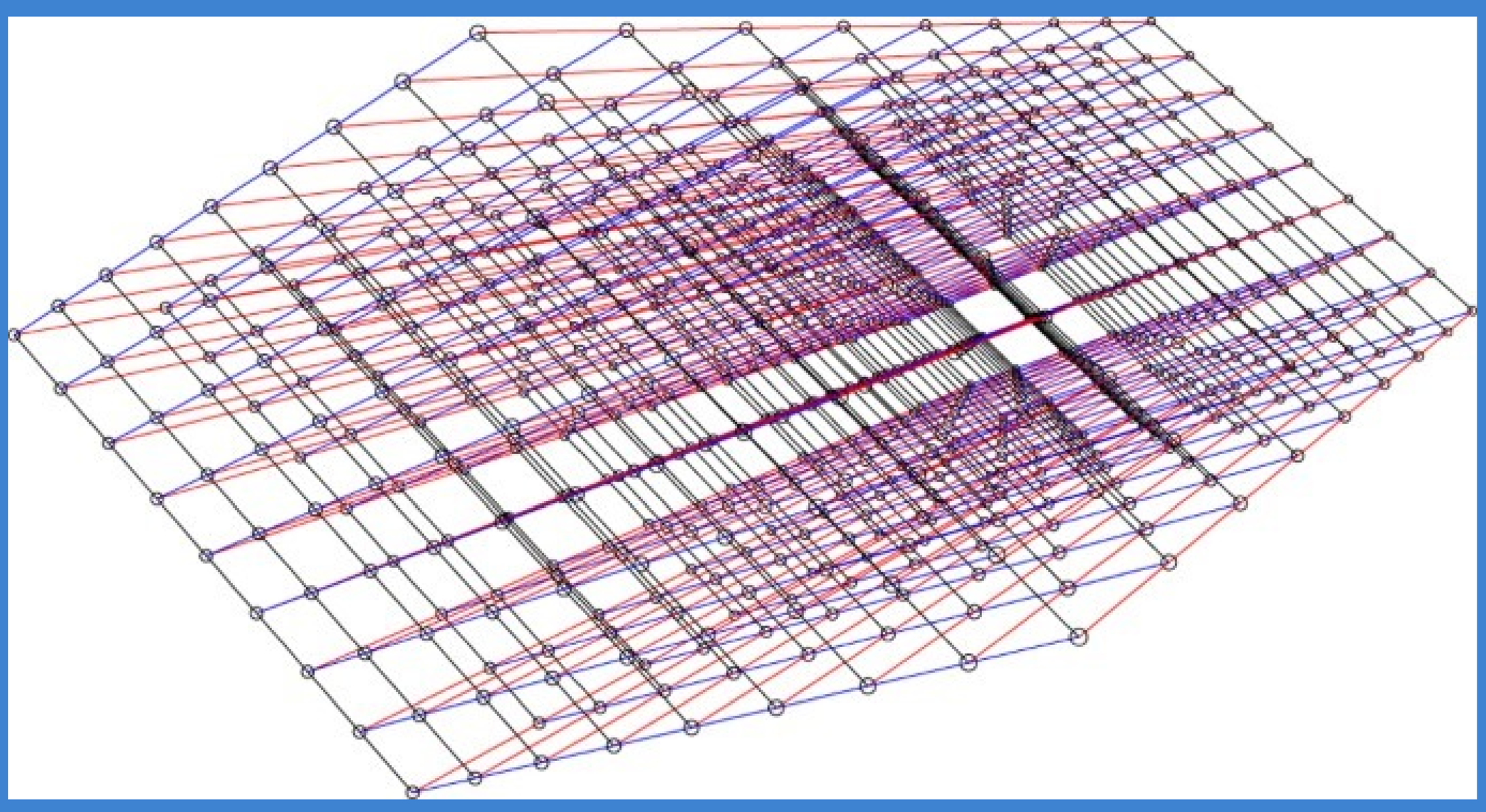


Figure 3: Perspective view of a 9 × 9 × 9 subset of a non-orthogonal 3-dimensional lattice.[1]

Conclusion and Future Scope

There are some potential attacks might occur against NTRU and other lattice-based cryptosystem. Some attempts are made to break some lattice-based cryptosystem by an extension of Shor’s Algorithm. But there are no known attacks exploiting NTRU. But this phenomenon is new and has not yet explored widely. Extensive research is essential to bolster confidence in security of lattice based cryptography.[1]

References

1. Bernstein, D.J. and Lange, T., 2017. Post-quantum cryptography. Nature, 549(7671), pp.188-194.
2. Lauter, K., 2017. Postquantum opportunities: lattices, homomorphic encryption, and supersingular isogeny graphs. IEEE Security & Privacy, 15(4), pp.22-27.
3. Mohsen, A.W., Bahaa-Eldin, A.M. and Sobh, M.A., 2017, December. Lattice-based cryptography. In 2017 12th International Conference on Computer Engineering and Systems (ICCES) (pp. 462-467). IEEE.
4. Chaudhary, Rajat, Gagangeet Singh Aujla, Neeraj Kumar, and Sherali Zeadally. "Lattice-based public key cryptosystem for internet of things environment: Challenges and solutions." IEEE Internet of Things Journal 6, no. 3 (2018): 4897-4909.