Role of Lattices in Post Quantum Cryptography

Ravinder Kaur

School of Chemical Engineering and Physical Sciences, Lovely Professional University, Phagwara-144411, Punjab

Abstract

The paper is a about implementation of Lattices in cryptosystem schemes in particular Learning with Error first introduced by Oded Regev [3].Lattices are proven to be best candidate for post quantum cryptography. Lattice based cryptography is also one of the candidate for post quantum computing cryptography as once the quantum computers will be built the existing standard cryptosystem which are based on number theory , particularly based on hard to factorizing large numbers, will no longer be secure as these existing hard problem on standard computers that enable quantum computers to calculate within polynomial time.

1.Introduction:

Post quantum cryptography is all about public key cryptography because quantum computers can break all a known quantum cryptography and public key cryptosystem [5]. In public key encryption there comes two important technologies that have public and secret key . Plain text is encrypted using the public key we obtain the ciphertext decrypted using the secret key and obtain the plaintext back. Once the quantum computers will com into existence that become very threating and the chances of breaking of the existing encryption schemes will be possible

Peter Shor[4] algorithm developed in 1994 proved to break key exchange and digital signature security. The encryptions which are very sophisticated could be cracked within a minute by quantum computers whereas the normal computers cannot crack those in years. There is a huge difference between the functionality of quantum computers from the existing classical computers.

Hardness of a problem in cryptography requires that problem which is easy to construct but hard to crack and one of the existing As we know that RSA[1] a public key cryptosystem make it secure because of hardness of factoring . Lattice based cryptography has given new direction to public key cryptography based on idea that with an available integer constrain the lattice can express certain problem that are actually very hard to solve. Particular advantage for lattice problems is that till now there not existing an efficient algorithm classical or quantum that can crack such problems even in an exponential time. Ajtai[2] contribution about worst-case to average case reduction for lattice problems gave new direction to lattice based public key cryptosystem. Two computational problems associated with integer lattices :SVP, CVP. Regev [3] contributed in lattice based cryptosystem with an efficient method called Learning with Error(LWE) for SVP.

2.Definition:-

Lattice :- For n numbers of linearly independent vectors $\overrightarrow{b_1}, \overrightarrow{b_2}, \dots, \overrightarrow{b_n} \in \mathbb{R}^n$ the lattice developed by these is defined as

$\mathcal{L}(\overrightarrow{b_1}, \overrightarrow{b_2}, \dots, \overrightarrow{b_n}) = \left(\sum \mathfrak{x}_i \overrightarrow{b_\imath} \,/\, \mathfrak{x}_i \in \mathbb{Z}\right)$, where $\overrightarrow{b_1}, \overrightarrow{b_2}, \dots, \overrightarrow{b_n}$ forms the basis of the Lattice.

Let's say if $\{\overrightarrow{\mathfrak{v}_1}, \overrightarrow{\mathfrak{v}_2}\}$ forms the basis for $\mathbb{R}^2$ then $(\alpha\overrightarrow{\mathfrak{v}_1} + \beta\overrightarrow{\mathfrak{v}_2})$ form a two dimensional lattice $\mathcal{L}(\overrightarrow{\mathfrak{v}_1}, \overrightarrow{\mathfrak{v}_2})$ where $\alpha, \beta \in \mathbb{Z}$

3.Some Hard Problems of Lattices

1. Shortest Vector Problem (SVP) :- Find the non-zero shortest vector within lattice when the basis of the lattice are given .
2. Closest Vector Problem (CVP):- When basis of the lattice are given and vector $\vec{\mathfrak{v}}$ which is not part of the lattice find the vector closest to $\vec{\mathfrak{v}}$ that is within the Lattice
3. Bounded Distance Decoding:- Similar to the closest vector problem, find the lattice point 's' closed given that v is known to be close to s.
4. Covering Radius Problem:-Given a basis for a Lattice find the smallest sphere that when placed at every lattice point it includes Lattice points 2 in numbers.

In this chapter we will focus on one of the above problem that is shortest vector problem
To find the shortest vector in a given Lattice might not be hard with few entries but when it has to be dealt with thousands of entries it would be actually quiet difficult and to find exact answer takes exponential time and that makes very useful for constructing cryptosystem based on that hard problem to make it secure.

Just like RSA Alica chooses a private key and publishes a public key then Bob uses the public key to encrypt a private message and sent his encrypted message back to Alica . Now Alica uses her secret key she can easily decipher his message but for eavesdropper it is a very hard problem to find what exactly Bob sent to Alica. In this case the hard problem is Learning with error. In this chapter we discuss the basic concept behind the construction of cryptosystem for a beginner to understand in a simple way.

4.Algorithm to find SVP using learning with error LWE

Alica and Bob choses a random matrix A and large integer q

Public Keys : Matrix A and q

where

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \ , a_{ij} < q \ \ and \ \ a_{ij} \in \mathbb{Z} ,$$

each of a_{ij} in the matrix is taken under (mod q)

Alica Private Key: vector $\vec{\mathcal{X}}$ (unique each entry either 0 or 1)

Alica Public Key: $=\vec{\mathcal{U}} = \mathrm{A}\vec{\mathcal{X}}$

finding $\vec{\mathcal{X}}$ is difficult for eavesdropper to find $\vec{\mathcal{X}}$ as multiplication $A^{-1}\vec{\mathcal{U}}$ is actually collision resistant hash function.

Encryption:

Bob will send his secret message by encrypting it by computing two vectors $\overrightarrow{\mathscr{b}_1}$, $\overrightarrow{\mathscr{b}_2}$ usig his private keys and will send them both to Alica.

Bob private keys: $\vec{\mathcal{S}}$ **(**random vector m entries) ; $\overrightarrow{e_1}$ (random vector with very small values) and error e_2 value (much less than q)

$$\overrightarrow{\mathscr{b}_1} = A\vec{\mathcal{S}} + \overrightarrow{e_1}$$

$$\overrightarrow{b_2} = \vec{S}.\vec{U} + e_2 + bit\frac{q}{2}$$

Here bit is a secret message 0 or 1 which he wants to send to Alica and $\frac{q}{2}$ is an integer of substantial magnitude modq and it is much larger than the error value.

Decryption:

Alica received the secret message form Bob $\overrightarrow{b_1}, \overrightarrow{b_2}$

She will multiply her private key $\vec{X}$ with $\overrightarrow{b_1}$ and will subtract it from $\overrightarrow{b_2}$

$$\overrightarrow{b_1}\vec{X} = \vec{S}.\vec{U} + \vec{e_1}.\vec{X}$$

$$\overrightarrow{b_2} - \overrightarrow{b_1} = (\vec{S}.\vec{U} + e_2 + bit\tfrac{q}{2}) - (\vec{S}.\vec{U} + \vec{e_1}.\vec{X})$$

$$\overrightarrow{b_2} - \overrightarrow{b_1} = (e_2 - \vec{e_1}.\vec{X}) + bit\frac{q}{2}$$

Here $(e_2 - \vec{e_1}.\vec{X})$ very small as compare to $\frac{q}{2}$

If bit is 0 then $bit\ \frac{q}{2} = 0$ and the given value will be very small i.e. very close to 0 so Alica will recognize that Bob sent her 0 and if bit is 1 then the given value will be far from 0 and Alica will be able to find the message sent by Bob is 1

5.Conclusion:

We can observe that it is a hard problem because in above algorithm we saw that cracking cryptosystem above is as hard as solving the learning with error problem and LWE problem is hard in the same way we think of factorizing is hard on standard computers. Finding very short vectors in high dimensions is currently exponentially hard

6. References:

[1] Adi Shamir Ronald Rivest and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21:120–126, 1978.

[2] M. Ajtai, C. Dwork, A public-key cryptosystem with worst case/average case equivalence, Proc. 29th ACM Symposium on Theory of Computing, pp. 284-293.

[3] Oded Regev. New lattice-based cryptographic constructions. J. ACM , 51(6):899–942, 2004.

[4] Peter W. Shor. Algorithms for quantum computation: Discrete logarithmsand factoring. In 35th FOCS, pages 124–134. IEEE Computer Society Press,November 1994.

[5] Stallings W., Cryptography and Network Security, Fourth Edition, Prentice Hall, 2005