Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019)
IEEE Xplore Part Number: CFP19K25-ART; ISBN: 978-1-5386-7808-4

LATTICE BASED CRYPTOGRAPHY

Its Applications, Areas of Interest & Future Scope.

Pawan Kumar Pradhan
School of Computer Engineering
Kalinga Institute of Industrial Technology
Bhubaneswar, India
p.pradhan1997@gmail.com

Sayan Rakshit
School of Computer Engineering
Kalinga Institute of Industrial Technology
Bhubaneswar, India
sayanrakshit96@gmail.com

Sujoy Datta
School of Computer Engineering
Kalinga Institute of Industrial Technology
Bhubaneswar, India
sdattafcs@kiit.ac.in

***Abstract*—With a recent increase in the advancement of the technology, computer system and it's sensitive data are getting exhibited to unauthorised users, with steadily corroding the fundamentals of computer security. This, in fact, demanded fundamental innovations that require several cryptographic paradigms and security protocol. Previously it was thought that asymmetric cryptographic key like RSA, Diffie-Hellman, are very hard to decrypt by classical computation, but with the implementation of quantum computation, it is proved that this kind of cryptographic algorithm is very easy to decrypt and hackers can steal important Data[3,6]. After the release of Ajtai's research paper "*Generating Hard Instances of Lattice Problem*"[2], a million reasons arose in the minds of the researchers to develop on methods based on lattice-based cryptography to improve their security needs. Firstly, it provided much stronger security, and the average-case of several problems in lattice-based cryptography seems equivalent to the worst-case problem of these problems [2]. Moreover, lattices have the potential to persuade the cryptanalytic attacks created by any quantum computers i.e Quantum Computational Secure[3]. In this paper, we will discuss lattice-based cryptosystem, it's security dimensions, a general brief on how it works, future scope, applications and areas of Interest.**

***Keywords*—Cryptography; Lattice-based Cryptosystem; Lattice; Post-Quantum Cryptography; Quantum Computation; Shor's Algorithm.**

I. INTRODUCTION

With the advances in technology and quantum computer generation, threats of cryptanalytic attacks will pose a serious impact on our computer security, thereby making conventional cryptographic schemes obsolete. Considering the following trends, there is Moore's Law[14], appearing to continue relentlessly, making our recent computers capable of coping up with future technologies and computation. On another hand, there is the emergence of quantum computers which are obvious enough to destroy convention computation schemas[5,14].

In future, classical computing will be replaced by quantum computing, thereby compromising our security. To prevent data breaching, eavesdropping from unauthorised users and hacking, we need to introduce advance & secured cryptosystem. This can be achieved by the implementation of the hardness of a lattice in cryptography. By this time the most likely scheme is believed to be the one based on the troublesome mathematics problems of lattices, multi-dimensional and reproducing points on the grids with limitless possibilities. It's the most promising candidate for post-quantum cryptography[4]. Ajtai in 1996 through his works proved that lattices have the potential to persuade the cryptanalytic attacks created by the quantum computers. It was considered to be the first lattice-based public key cryptosystem[4]. Similarly, another cryptosystem named Gold-Goldwasser-Halevi

cryptosystem (GGH) came into existence which mainly offered a realistic alternative to number theory[15].
And as a need to enhance current practices in cyber-security, adding such variety in cryptography will aid our security at the very fundamental level.

With substantial changes and improvements in technology, the diversity in technology tends to increase a lot thus requiring several diverse platforms to run such tech. And so would Lattice-based cryptographic Algorithms, in order to tackle Quantum Computation e.g. Cloud vs IoT platforms. There are several other fields where they provide enhanced and efficient security for both long-term and short-term devices and systems e.g. On the medical grounds like smart medical implants which have to stay put for years and security is a major concern here. On Military grounds like missiles with smart embedded systems where it has to hit a particular target and the info of target is stored on the system only, so security plays a critical role here.

The paper is organised in the following way: Firstly an overview of what exactly is lattice and basis, its representation and some general formula. Then, concepts of Lattice theory and development of lattice-based cryptosystems, a brief on some commonly used cryptosystems followed by its applications, areas of interest and finally its future scope. And lastly summarising it with an overwhelming conclusion.

A. LATTICES

In general, Lattice can be defined as an infinite arrangement of "Regularly spaced" points on any vector space.

Since lattices are infinitely large objects and in cryptography, we need to feed them on computers to work on them, whereas a computer has a limited amount of memory. So, we use a concise way to tackle the problem and here comes the concept of basis. A Basis can be defined as the collection of small vectors which are capable of reproducing any point on the grid that forms a lattice.
Mathematically, a lattice is defined as a discrete subgroup of $\mathbb{R}^n$, or the set $L(b_1, b_2, b_3, ...b_n)$ of all linear combination $\sum x_i b_i$ where $x_i \varepsilon Z$, and the b_i's are linearly independent vectors over $\mathbb{R}$, where $(b_1, b_2, b_3, ...b_n)$ are basis vectors[7].

$$L=\{ \Sigma x_i b_i \mid x_i \in Z x_1 \}$$

According to the concepts of lattices, lattice sharing same bases are hence equivalent. So no two lattices can share the same basis.

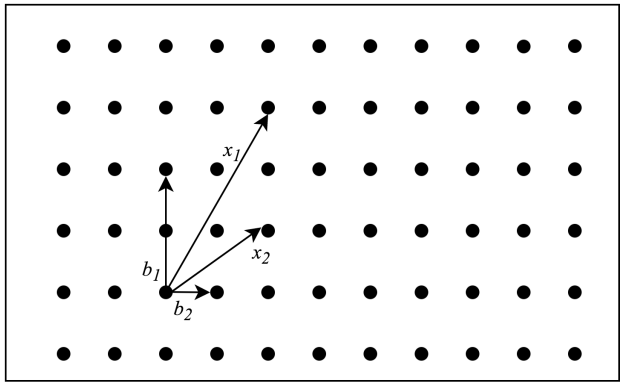


Fig.1 Lattice representation by basis [x1,x2] and [b1,b2].

In the above diagram i.e Fig 1, lattice generated using [x1,x2] and [b1,b2] are totally different. Where, Basis [x1,x2] is referred to as a bad basis and Basis[b1,b2] is a good basis, as the vectors are orthogonal in [b1,b2].

★ A Lattice is Infinite, but lattice-cryptography actually uses the *Finite Abelian group* Z^d/L : it works modulo the lattice L [7].

B. LATTICE THEORY

Lattice-based Cryptography is the recent innovation in the fundamentals of cyber-security, laying foundations to strengthen the weak cryptographic policies & the unstructured security protocols and is even capable of handling Quantum-Computation, which had been a great issue over such a time where quantum computers are a reality and can be a resource of misuse too, despite having it wonderful uses[5]. Its construction is based on the presumed hardness of the lattice problems.

Some general Lattice problems used in cryptographic primitives are:-

- *Shortest-Vector Problem (SVP)*: For a given basis X of lattice L, another basis X' is created, such that the $L_X = L_{X'}$, where vectors of X' are shortest for any norm[8].

- *Approximate-Shortest Vector Problem* (***α****-SVP)*: For a given lattice L, the problem is solved by finding a non-zero vector 'x' where, $x \varepsilon L,\ \forall\ y \varepsilon L,\ ||x|| \leq \alpha||y||$ [8].

- *Shortest In-dependent Vector Problem (SIVP).*

- *Closest-Vector Problem (CVP).*

- *Approximate Closest Vector Problem* (***α****-CVP).*

- *Bounded Distance Decoding (BDD).*

- *Shortest Integer Solution problem(SIS).*

Various Algorithmic Solutions for those Lattice Problems include Gram-Schmidt Orientation, LLL Algorithm, which is to be the best known polynomial time algorithm, BKZ & the most widely used Algorithm Babai's Round-Off Algorithm[8], who proved that the CVP in R^n can be approximated to 2^n.

II. LATTICE CRYPTOSYSTEM

Since we all know the drawbacks of Classical Cryptosystem which includes RSA.
RSA uses large finite Abelian Groups $G = (Z/NZ)^x$ [5]. In order to speed things up we introduced:

- *Elliptic Curve Cryptography* which uses smaller groups, whose operation are more expensive[8].
- *Lattice-Based Cryptography* which uses larger groups, whose operation are much cheaper[8].

Lattice-Based Cryptography uses high-dimensional geometric structures to hide information, creating problems that are considered impossible to solve without the key even by universal fault-tolerant quantum computers.

In order to make such cryptography possible, first of all, we need to build a prototype of the system and test it under several severe conditions. As till now we Clearly know about the Lattices and its Theory. We are well aware of the fact that this cryptosystem totally relies on the hardness of the problem.

Considering it to be a candidate of post-quantum cryptography, the tough problem considered should be sufficiently tough enough to trick quantum computational schemas too.[8].
Various cryptosystems that are implemented nowadays are utilizing SVP/CVP/BDD as the hardness used in those problems using the concepts of Lattice Equality as one-way trapdoor function.

Some Commonly used Cryptosystems are:-

- *GGH.*
- *Piekert's Ring - Learning with Errors(Ring LWE) Key Exchange.*
- *NTRUEncrypt.*
- *The Micciancio Cryptosystem.*
- *Other CVP Based Cryptosystems.*

III. APPLICATIONS

With the emergence of various computing paradigms, the need to contain their security definitions has become a real threat for the computer scientists by now. As technological services like Cloud Computing, high-performance (real-time) virtualized environments, Internet of Things, Quantum computation etc. demand highly secure/encrypted software-defined networks for their communications.

In IoT, the classical cryptographic measures seem to fail because the IoT space demands an increased number of keys. In order to tackle this increased generation of the key by classical cryptographic measures demanded some development of some standard lightweight cryptographic schemas and cyphers with increased agility and performance. This development calls out for Lattice-based public key cryptosystem and hence becomes an area of Interest for its implementation/Application.

Similar, for cloud computing the channel or the software-defined network which it demands, need to have high agility and performance, should be energy-efficient

and must be of low latency. This couldn't have been achieved by primitive cryptosystems, which furthermore demands an accelerated system, capable enough to run more than one cryptic algorithm with full agility and efficiency like that of an Application-Specific Integrated Circuits(ASCI's)[5].

After those diverse applications of Lattice-based cryptosystems. There are some Applications, which are used on an everyday basis and is shared by classical-public key cryptography also. Though both cryptosystems have applications on the same field, lattice cryptosystem is applied on areas where security is the utmost priority.

A. AREAS OF INTEREST

End-to-End Encryption: The one field of communication that is widely used, but is the least encrypted is the E-mail. Since the content of our emails is not sensitive enough we least care for encryption. But, for people out there who care for their sensitive information, like information related to military or political purpose where the whole country has to suffer if the information gets leaked out, they can't have an uncertainty of even 0.01%.

Electronic Money: As we can see this is the era of Digital Cash or Electronic cash. On simple terms, we can say that Electronic money includes the transfer of money between individuals electronically using an encryption algorithm. The level of Encryption used here is the key factor. Great encryption will secure the transactions from getting hacked by anonymous users whereas a small flaw in encryption will lead to a huge loss. As we know the alteration of a single bit/digit over the database can change a million to a billion. *Example*:- Suppose if an unauthorised user just gets into the database using the flaw on encryption and just add two more zeros on the end of this account balance. That makes a huge difference, this was just a small example to illustrate what he/she can do.

Secure Network Communications*:* In order to have a secure medium to communicate through others, the extent of the encryption standard must have to be increased. To do so network protocols based on public-key cryptography have been made such as Secure Socket Layer(SSL) developed by Netscape, Kerberos an authentication service developed by MIT.

Anonymous Remailers: Remailing, is a service that receives messages with embedded instructions of where to send them next while stripping off the header information like the originating address from the electronic message and forwarding only the message. So, in this process, only the first remailer retains your identity and instead of trusting the operator, uses many anonymous remailers to relay the message before sending it to the recipient. Using this method only the first remailer know the identity of the sender and it becomes impossible for anyone to retrace back to the sender from the end-point. The user wanting anonymity for their messages uses such kind of service whose encryption is based on lattices.

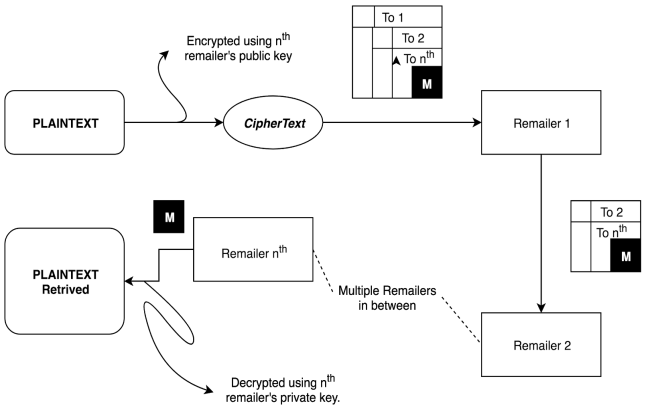
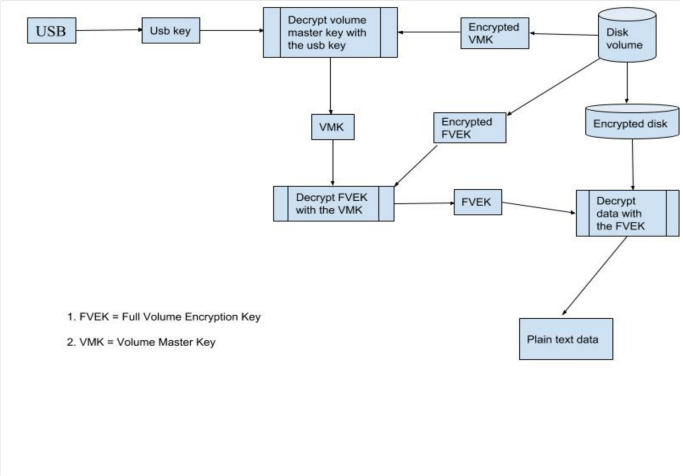


Fig. 2. Representation of how a message flows through n-numbers of Re-mailers.

Disk Encryption: This method involves encryption of whole disks so the user won't have to worry about leaving any traces of unencrypted data on the disk. The disk is protected by an encryption algorithm defined by the user. And a password-protected system used by the user to gain access to the disk. Thereby making the overall system secure and inaccessible to any unauthorized user.

Along with them, there are several other fields to look on to such as Authentication/Digital Signatures, Time

Stamping, Pseudonymous Remailers etc. and several other areas which are yet to be discovered.



IV. FUTURE SCOPE

Several fields such as IoT, Embedded Devices, Cloud computing, etc. Employing classical cryptography here can create a lot of fuss, as of individual field requests their own specific key generation method with varied performance and agility ratio, which can only be provided by the implementation of Lattices.

One great field where the use of lattices is mandatory is embedded devices. They totally rely on decisions to act on. They only care for the reliability of the decisions and does not acknowledge who gets that decision. So, just by tampering with the decisions the whole system can be exploited. Hence the need for a cryptographic hashing algorithm arises.
Similarly, for Machine Learning, Artificial Intelligence & Neural Network where the whole system depends upon the integrity of the decision. Further, there are also scope in Computer Networking and Web-Technology where Encryption is the key requirement for everything to operate.

The exponential growth of technology and its limitless possibilities makes us wonder where would technology go from 10 years by now. And the need to encrypt our personal data/belongings have become a great deal now. Hence we presume, this technology of lattice-based cryptography will make these threats hypothetical.
There is a varied scope of this tech in future. Observing the emergence of Quantum Computation.

CONCLUSION

As we can see that cryptography plays a vital role in securing our data transfer, digital communications, transactions, transfers of sensitive information by encrypting modern-day applications, systems, digital signatures, HTTP etc. And it continues to play its crucial role in securing all aspects of our life.

The scale and sophistication of cyber-attacks escalate every year as well as the risk of gaining or losing sensitive information. This concept of lattices and its hardness is mainly used as an update to the current cryptographic schemas. Lattice-based cryptography is a complex cryptic method which is meant to protect our data and secure us from cyber threats generated from the quantum computing system consisting of millions of qubits. Though the implementation of such type of computers is still many years away. Moreover, by increasing the dimension of a lattice, cryptographers can create problems so hard that many believe no algorithm will ever crack them - not even universal fault-tolerant Quantum Computers.

As of now, we can say that Lattices and Cryptography are just like a match made in Heaven.

ACKNOWLEDGMENT

We owe our deepest gratitude to *Mr Sujoy Datta, Asst. Professor, School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar*, for his helpful guidance, support, motivation and encouragement throughout our work. We are immensely grateful to have him by our side sharing his pearls of wisdom during the entire course of this research.

We would also like to acknowledge our friends who have always supported us through our bad times and kept us ever motivated to keep going. And lastly, our parents to

ever support us and make us credible enough to reach successful heights.

REFERENCES

[1] Regev, O. (2006, August). Lattice-based cryptography. In *Annual International Cryptology Conference* (pp. 131-141). Springer, Berlin, Heidelberg.

[2] Dadheech, A. (2018, September). Preventing Information Leakage from Encoded Data in Lattice Based Cryptography. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1952-1955). IEEE.

[3] Shor, P. W. (1994, November). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). Ieee.

[4] Ajtai, M. (1996, July). Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 99-108). ACM.

[5] Nejatollahi, H., Dutt, N., & Cammarota, R. (2017, October). Special session: trends, challenges and needs for lattice-based cryptography implementations. In *2017 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)* (pp. 1-3). IEEE.

[6] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), 303-332.

[7] Nguyen, P. Q., & Stern, J. (2001, March). The two faces of lattices in cryptology. In *International Cryptography and Lattices Conference* (pp. 146-180). Springer, Berlin, Heidelberg.

[8] Rose, M. (2011). Lattice-based cryptography: a practical implementation.

[9] Micciancio, D. (2011). Lattice-based cryptography. *Encyclopedia of Cryptography and Security*, 713-715.

[10] Nyang, D., & Song, J. (1998). Method for hiding information in lattice. *Electronics Letters*, *34*(23), 2226-2228.

[11] Schaller, R. R. (1997). Moore's law: past, present and future. *IEEE spectrum*, *34*(6), 52-59.

[12] Micciancio, D. (2001). Improving lattice based cryptosystems using the Hermite normal form. In *Cryptography and lattices*(pp. 126-145). Springer, Berlin, Heidelberg.