**Literature Survey on Information Leakage from Encoded Data in**

**Lattice Based Cryptography**

**Introduction:**

Protecting information is one of the security goals and still even protected information can sometimes leak. This leakage is termed as Information Leakage in the cybersecurity world. Though the leaked information might or might not reveal everything, it still has risks of compromising the whole system. Some examples for information leakage are improper or failed scrubbing of HTML/Script comments that contain sensitive information like security codes, improper configurations for server or applications, or different page responses for valid and invalid data.

Improvements in technology comes with its cons. Quantum Computing is going to change a lot of things. One of those is in the field of cryptography. The current public key cryptosystems work based on the number theory problems. The complete security comes from the toughness of these problems. Though there are not many algorithms to solve these tough problems efficiently on classical computers. However, quantum computers can solve these problems in polynomial time by using Shor’s algorithm [1]. As soon as these quantum computers become a reality, these public key cryptosystems will no longer be secure enough. Consequently, cybersecurity researchers are looking towards post-quantum cryptography, as it is believed to be even quantum-proof.

One of the promising candidates for post-quantum cryptography is lattice-based cryptography. The concept of lattices is not something that is new. In 1996, the first lattice-based cryptographic construction was introduced by Ajtai and the security was based on the hardness of some well-studied lattice problems [2]. The best thing about these problems is that even the average-case of several problems is equivalent to the worst-case problems of non-lattice-based problems. But it was Goldreich–Goldwasser–Halevi (GGH) cryptosystem that put a practical alternative on table for number theory [3] [4].

This was not spill proof, Phong Nguyen showed that the encoded data of GGH leaks information on the plain text and this was a major flaw in the design of the GGH cryptosystem [5]. This flaw has limited the GGH cryptosystem extent. Recently, some methods, an improvised GGH encryption and decryption functions were suggested by Aarti Dadheech in which this flaw can be removed making the GGH cryptosystem more reliable to use [6].

**Significance of Lattices:**

A lattice is generally defined as any grid of points that are regularly spaced and stretched out to infinity. These points are also called as vectors. Therefore, an even more technical definition for lattice is as follows, a collection of evenly spaced vectors. Any lattice consists of a special vector known as origin. An origin has all its co-ordinates set to 0.

Lattices are infinitely large entities and computers which technically have limited amount of memory cannot represent these entities straightforward. So, the concept of basis was introduced to solve this issue. A Basis is defined as a small collection of vectors that can be used for reproducing any point on the grid that makes a lattice.

Mathematically, a lattice is defined as a discrete subgroup of Ｒ*n* , or the set *L*(*b*1, *b*2, *b*3, ......*bn*) of all linear combination Σ*nibi* where *ni* ε *Z*, and the *bi* ’s are linearly independent vectors over Ｒ, where (*b*1, *b*2, *b*3, ......*bn*) are basis vectors [7].

L = { }



Figure 1 Lattice Representation by basis [x1, x2] and [b1, b2]. [8]

Some lattice problems over which the security has been constructed are:

* Shortest-Vector Problem (SVP)
* Closest-Vector Problem (CVP)
* Shortest Integer Solution Problem (SIS)
* Shortest Independent Vector Problem (SIVP)

**The Goldreich–Goldwasser–Halevi (GGH) cryptosystem:**

Most of these problems are easy to solve if the basis chosen is a “good basis” and are hard to solve with a “bad basis”. The GGH cryptosystem has been designed to work on the hard lattice problem to find the closest vector in lattice (CVP). CVP states that for a given basis of a lattice and a vector ‘c’, find a vector ‘v∈L’ that is closest to ‘c’ among all points of L.

The algorithm GGH employs is difficult to be broken even in the average case making it one of the best lattice-based cryptosystems. Yet, there was some information leakage on the encoded data of the GGH that leaks plain text. This flaw was suggested to be corrected by an improvised encryption and decryption functions to enhance the safeness and increasing the extent of the GGH cryptosystem.

The suggested methods by Aarti Dadheech were implemented only on grayscale images but is stated that the same can be extended to text and color images with further work. Also, it was suggested that the scheme suggested by Aarti Dadheech can be improved in terms of space complexity as the public key size and their corresponding cipher text is much larger.



Figure Visual Differences in the leakages [6].

We would like to implement the methods suggested by Aarti Dadheech and try to implement it on text as an additional work.

# References

|  |  |
| --- | --- |
| [1] | P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science,* 1994. |
| [2] | M. Ajtai, "Generating hard instances of lattice problems," *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing,* 1996. |
| [3] | O. Goldreich, S. Goldwasser and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *CRYPTO ’97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, London: Springer-Verlag, 1997. |
| [4] | H. Nejatollahi, N. Dutt and R. Cammarota, "Special Session: Trends, Challenges and Needs," in *International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*, 2017. |
| [5] | P. Q. Nguyen, " Cryptanalysis of the Goldreich–Goldwasser–Halevi Cryptosystem from Crypto '97," in *CRYPTO ’99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, London: Springer-Verlag, 1999. |
| [6] | A. Dadheech, "Preventing Information Leakage from Encoded Data in Lattice Based Cryptography," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, 2018. |
| [7] | P. Q. Nguyen and J. Stern, "The Two Faces of Lattices in Cryptology," in *In International Cryptography and Lattices Conference*, 2001. |
| [8] | P. K. Pradhan, S. Rakshit and S. Datta, "LATTICE BASED CRYPTOGRAPHY: Its Applications, Areas of Interest & Future Scope.," in *Third International Conference on Computing Methodologies and Communication (ICCMC)*, 2019. |