LATTICE CRYPTOGRAPHY & ITS ENCRYPTION SCHEMES

A brief on the fundamentals of Quantum computing and cryptography along with analysis on the current Lattice cryptography schemes

BY

Pranav Sarma Venkatramanan

CSEC.604.02 – Crypto & Authentication (ONLINE)/ First semester

Rochester Institute of Technology

25th November 2020

INTRODUCTION:

Being a fan of science fiction stories I was intrigued about how humans have rapidly become dependent on computers and networks in the past 3 decades. With all kinds of data moving towards digital storage, questions & theories arose in my mind as to what would happen when these same systems of computers and networks get compromised as per an adversary's wish? Is it first possible to happen? Do we have the necessary resources, technology & manpower to achieve such a thing? Even if it became a reality, how do we protect our systems and the data they store?

My research seeks to find out those answers about the effects of Quantum computing and how Quantum cryptography, especially Lattice cryptography in particular, can prove to be an effective barrier to it. While doing my research, though I found many papers which helped in explaining about their concepts, almost all of them were highly dosed with mathematics and physics. Though it is true that both of them are totally unavoidable if one wants to thoroughly understand about these topics, I found this to be sort of a hindrance to lay men who are interested in the topic but do not have a good & simple launch pad before delving into the specifics. Hence, I have tried my best in explaining the concepts in simple English with real life examples wherever I could

My analysis part involved studying the parameters regarding the lattice cryptography schemas and deciding what was the best of them. Though it has been in research for long, not much could be said with respect to various factors due to the lack of practical testing under quantum computers. Hence mine will only present about the soundness in each scheme's mathematical problems and probable implementation results. In order to retain the essence of simplicity in my paper, I have cited the papers responsible for performing the core analysis and which also influenced my analysis results too

PROBLEM DEFINITION:

Researches in Quantum computing have crossed many strides ever since its initial discussion and though unknown, it is expected to be viable to real world computing sooner or later. Along with it, quantum cryptography has also been a huge source of discussion to protect data which is currently encrypted with less powerful cryptographic methods. This paper examines the basics of both, how they work and their impact in the digital world. Also, it explains the cryptographic methods of 3 lattice cryptographic schemas and which is currently the best candidate for post quantum encryption

A BRIEF HISTORY ON CRYPTOGRAPHY:

Language in speaking, reading and writing formats has played a very important part in communication between humans for centuries and more to go. But what if a couple of people want to communicate something secretively, something which should be kept only between themselves and not be overheard by others, especially the wrong kind of people else it might get misused? It was due to this necessity that codes and symbols became an important part of communication. These two with proper usage & technique could significantly alter the way how the meant-to-be-secret information would be normally communicated and thus help the necessary parties in the cause of secrecy. Hence the term "Cryptography", which in Greek meant "Secret Writing" was coined. In general terms, Cryptography is defined as the manner of communicating information secretly between the concerned parties only, without leaking it to others

In technical terms, "Cryptology", as we know is defined as the art or science of creating/deciphering codes for secure communication against adversaries. Creation of these codes comes under the branch of "Cryptography" while deciphering them comes under the term "Cryptoanalysis".

Cryptography has been in existence for centuries as we know, helping people share information safely and securely. Ever since its inception, the art or science of Cryptographic methods has significantly evolved over the years. Starting with hieratic/demotic languages, symbolic illustrations, skytale **[Fig. 1]** apparatus and sympathetic inks – we have come a long way now to currently using NP-Hard mathematical problems and trying our luck on quantum mechanical principles. Furthermore, the initial focus which was only on confidentiality during the olden days has now moved over to include other equally important & necessary factors like Integrity and Authentication. Modern cryptography, other than mathematics, now equally depend on other fields to remain viable in current world like Computer Science, Electrical Engineering and on Electronics & Communication

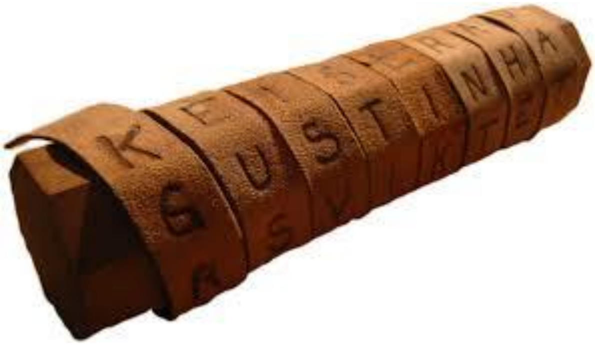


Figure 1: Skytale[1]

QUANTUM COMPUTERS:

A quantum computer is one which executes algorithms, whose method of working is similar to the phenomenon of quantum mechanics and which also provides high speed and high performance computation. While the traditional computers are known to work based on the classic electrical circuit phenomenon, the quantum computers work based on the theory of quantum mechanics

In January 2019 when IBM unveiled the prototype for the world's first integrated quantum computing system for commercial use **[Figure 2]**, it was found that it had no keyboard or screen like a traditional computer but was just a bell shaped machine covered with copper wires. Also it was not handled directly and by all- only specific people were made to come close to it. Even if one wanted to interact with it, traditional computers and cloud technologies were used.

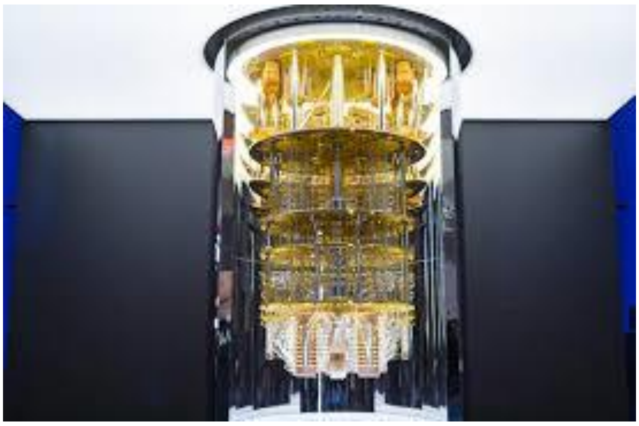


Figure 2: Quantum Computer unveiled by IBM [2]

Why is it so, one may think. It is because of the difference between how interactions and interferences are dealt differently by traditional and quantum computers. In traditional computers, if interference occurs the system will correct itself and continue to run smoothly as it did earlier. But in the case of quantum computers, when interference occurs the Qubits lose their superposition and coherent properties. To maintain the quietness of the atoms and avoid the interaction between them and external noises, the quantum system must be kept in a still state, which is only possible when the device is maintained at particular environments of -273 °C (-459 °F) temperature, zero atmospheric pressure and isolation from the magnetic fields of the earth. Also, they currently do not perform all the day to day tasks and are restricted to very few in that fashion.

Again, one might think as to why this many hassles just to make a computer run? Quantum computers have the potential to process some programs and data lot faster than a traditional computer would be able to, in a lesser amount of time. Also with the principles of Quantum superpositioning, we will be able to work on some highly complex algorithms which would not be possible with the technology supporting on traditional computers. With the proper algorithms & programs, it also has the ability to break the encryption of a lot of modern day cryptography techniques too. One day, it might overtake the traditional computer's work in a very long way after which quantum computers will rule

Furthermore, the day when quantum supremacy will become a reality is still unclear due to various problems associated with running quantum computers properly as expected. Researchers are still finding out more ways to make qubits stay stable for longer periods of time and in a less complex environment. Also, the current processes on qubits are said to give out a high error rate and it is tough to implement quantum principles with the existing hardware. But according to Moore's Law which loosely states that- "processing power of computers will increase exponentially in comparatively lesser amount of time", meaning that the perfect quantum computer can one day, sooner or later, become a reality

QUANTUM MECHANICS:

Quantum mechanics comprise of a set of theories which explain the various physical aspects of particles which exist in the atomic and subatomic size levels. This theory is very different from the classical theory of physics. While the classical theory revolves around the electrical state (positively charged or negatively charged), the quantum mechanics theory revolves around the energy states and angular momentum of its particles, hence warranting for a separate branch of physics to explain it.

Some important quantum mechanics principles integral to Quantum computing we need to know:

- **QUBITS**:

  The traditional computers which work on the classical theory of physics where the unit of data is measured using the term "bits". A bit has only 2 values – 1 & 0- similar to the electrical state of a conductor theory. These values are definite, i.e., unless or otherwise they are changed on purpose it remains the same. Consider it as something similar to that of the working of an electric switch, which only remains in either ON or OFF state. Only if someone goes and presses the switch, will it change into the corresponding other state (OFF it was already on ON and vice versa) else remain in the same one. All data being run and communicated using the traditional computer are represented in these 2 states only

  The quantum computers which work in the theory of quantum mechanics have their unit of data measured using the term "Quantum bits" or "Qubits". The values of a Qubit include 0, 1 and in between 0 & 1, similar to the spin of an electron and polarisation of a proton in quantum mechanics theory. This is highly different from that of a traditional computer which has definite values until tampered with. Consider a coin with a head and a tail on either one of the sides being tossed. When it is in motion, the result value is undefined- it can be either 0 or 1 or in between them too. Only when it lands or it is caught, we get a definite value. It works the same in Qubit too- once a Qubit value is read, it is either 1 or 0

  A n-bit traditional computer can store only n amplitudes of information, whereas a n-qubit quantum computer can store 2^n amplitudes of information. Moreover, a quantum computer can actually calculate the probability of a qubit in superposition mode falling into a particular state before observation by changing the probabilities in various ways through logic gates and then read out the required result by measuring it. Because of this factor, the quantum computers have the potential to process high amounts of data in way lesser time. This makes them the right systems to break the current encryption algorithms existing today, which might take years and years to do for a traditional computer

- **OBSERVER EFFECT**:

The Observer state is defined as action where if a quantum system in superposition is observed and noted down, the superposition factor which made the quantum system oscillate between 2 different states at the same time will cease and the system tend to remain only in one of those 2 states at the moment it was observed.

Considering the coin toss example, if the coin tossed -which was both in heads & tails position at the same time- is suddenly stopped, the coin will cease to rotate any further and will remain in the position where it was when made to stop

- **QUANTUM SUPERPOSITION**:

Generally, the term "Superposition" is defined as a factor where a system can exist in 2 different states at the same time. The same coin example can be used here, where the coin can be in both head position and tail position when it is in the tossed state. Also in the case of an electron, it can spin either both upwards and downwards almost at the same time before it gets observed

The term "Quantum superposition" **[Figure 3]** is loosely explained by the English theoretical physicist Paul Dirac (who contributed greatly to early developments of Quantum mechanics) as- "A system has the capability to be in 2 or more states and there exists a relationship between them which cannot be explained on classical ideas, such that whenever the system is definitely in a particular state, it also partly exists in other states too.

"Also the non-classical nature of superposition can be explained with an example- Let us consider that a quantum system A 's value after observation results as X and a quantum system B's value after observation results as Y. Now if both systems A and B are superimposed together, the final value will sometimes be X and sometimes be Y, based on a probability which depends on various factors found in A and B in the superposition process and not anything other than those 2".

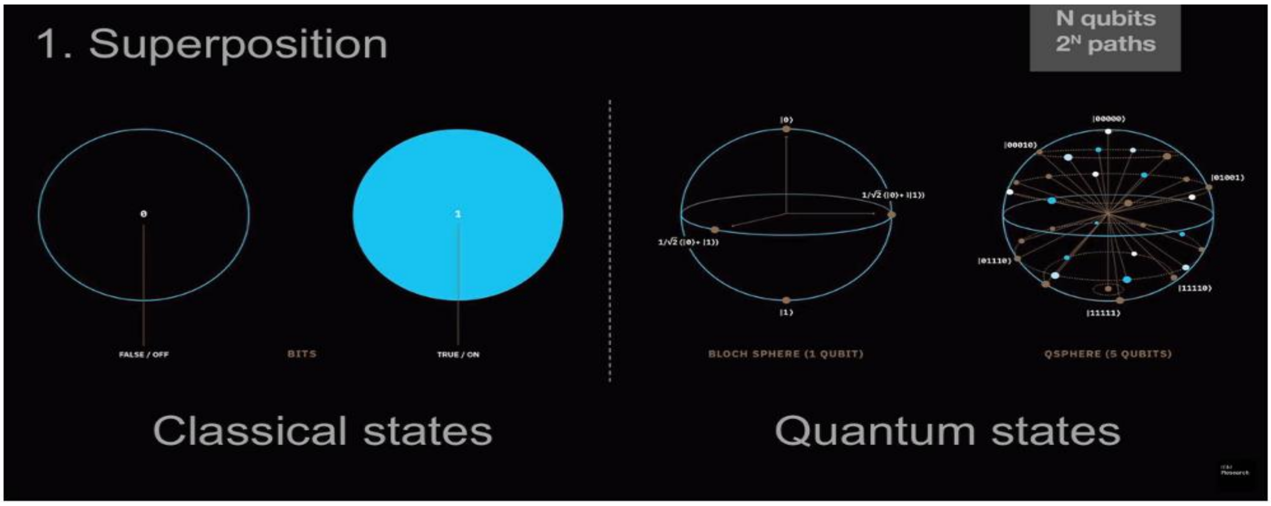


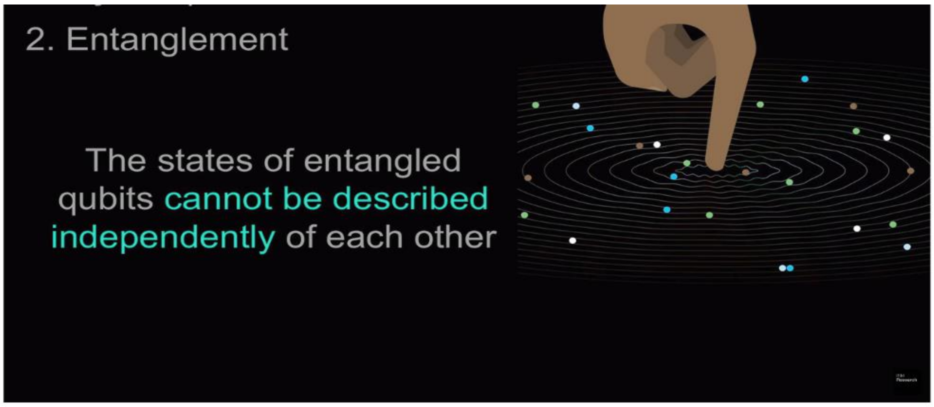
Figure 3: Quantum Superposition [3]

Juan José García Ripoll, a researcher at the Institute of Fundamental Physics within the Spanish National Research Council, provided more insight: "In traditional computing we know how to solve problems thanks to computer language (*AND, OR NOT*) used when programming. Operations that are not feasible in bit computing can be performed with a quantum computer. In a quantum computer all the numbers and possibilities that can be created with N qubits are superimposed (if there are 3 qubits, there will be 8 simultaneous possible permutations.) With 1,000 qubits the exponential possibilities far exceed those that we have in traditional computing**".**

- **QUANTUM ENTANGLEMENT**:

Quantum entanglement is the phenomenon where a group of particles interact together in such a way that the final quantum state of each particle depend on each other such that one particle's state cannot be independently observed & measured without influencing the other unobserved particles. In this way, if a particle belonging to an entangled group is observed & measured of its state, the action gets reverberated to all the other particles in the entangled group.

For example, if the total spin of a pair of quantum particles is observed to be zero, if one of them has a clockwise spin then the other is said to have an anti-clockwise spin. Also, if one particle in a group is observed & ceases to have superposition, then similarly the particles belonging in the same group as it is also ceases to have superposition too. This can also be compared with the domino effect on a group of coins stacked somewhat close to each other horizontally with the face of coin perpendicular to the ground. Assuming that the coin can never fall but instead turn- if we try to turn and look at what side (head/tail) the coin is facing us, consequentially the coin next to it will get disturbed and turns its direction. So if that second coin was showing a head, it might turn and show a tail instead. This same effect happens to the other coins next to it too. In technical terms, if a traditional computer's logic gate connects itself one by one to every bit of memory, the quantum computer using quantum entanglement is seen as the one where the logic gate connects every one bit of memory to another



2. Entanglement

The states of entangled qubits cannot be described independently of each other

Figure 4: Quantum Entanglement [3]

Because of the entangled states between the group of particles and that one small change in one of them would affect the entire set, quantum cryptographic methods can use this to their advantage during data transfers, where it can be made to check whether there had been a Man in the middle who had tried to intercept and view the data while it was being shared to receiver by the sender. This kind of operation leads to a more trustable repudiation technique than what can be achieved with a traditional computer. Its principle also used in "Quantum teleportation" and "Super dense coding" techniques where information is communicated between parties

POST QUANTUM CRYPTOGRAPHY:

As mentioned before, Moore's Law loosely states that- "processing power of computers will increase exponentially in comparatively lesser amount of time"- meaning that the perfect quantum computer can one day, sooner or later, become a reality and with all the necessary factors acting together in its strength, it also has the ability to break the encryption models of a lot of cryptography techniques, including the ones used currently.

Despite the complexities involved in creating and properly running one, lot of investment and research is going for its realisation and are also technologically supported by many large & reputed companies like IBM & Google. Though the perfect quantum computer still is yet to be realised, researchers have already started to theorise on the possibilities of how the face of computing will drastically change and how cryptography too will follow suit. With that theory as basis, one important term to note is “Quantum supremacy”.

Technically, Quantum supremacy is used to theorise that a quantum computer would be able to solve a given problem within a fairly given time, which would not be possible in the case of a traditional computer. Other than proving the above, it also involves the tasks of finding such a problem to solve and also developing a high performance quantum computer to compute it & one which do not have a significant error rate. Generally it can also be defined as the ability of quantum computers to outperform the traditional ones in all formats

So when that day comes, especially if an adversary has their hands on such a quantum computer, what can we do to protect our data?

“Quantum cryptography” is a term used to define the set of cryptographic techniques which uses the principles of quantum mechanics in order to protect information against attacks from adversaries, while “Post Quantum Cryptography” is used to define the techniques to protect information against adversaries who have quantum computers.

Furthermore, all cryptographic encryption techniques depend on how hard it is to solve the mathematical problem, which is generally also the basis for cryptography. Even with the advent of the theory of quantum computers, the stance regarding the incorporation of mathematical problems as the basis for cryptography has not changed. Especially with lot of mathematical questions and theories still not cracked by the best mathematicians, they serve as the best option for cryptographic developers to develop the best cryptographic protocols/algorithms

A cryptographic problem’s strength is defined by the relation between the toughness in finding a solution versus the time needed to solve it. Most of the problems, especially the ones used for encryption purposes strive for a particular relationship where the time steadily increases whenever toughness does. But some problems exist where time exponentially increases even for a smallest increase in toughness. For example, consider a chess board. If we keep a coin on one square found in the edge of the board & keep doubling the amount of coins kept as & when while filling the other squares, at one point it would become impossible to calculate the number of coins required to fill a particular square. These kinds of problems are what called as Non deterministic Polynomial time (NP) problems or generally known as NP-Hard problems. Some NP Hard problems like the factorisation of large numbers can be easily solved by a quantum computer using the Shor’s algorithm, while some cannot. The ones which cannot are more favourably considered for building quantum cryptography protocols

Here are a few of the well-known post quantum cryptographic schemes:

- LATTICE CRYPTOGRAPHY:
  This involves creating cryptographic encryption schemes based on the principles of solving lattice based problems. Commonly known schemes created from this principle include Ring-LWE (Learning with errors), NTRU & GGH schemes

- MULTIVARIATE CRYPTOGRAPHY:
  This involves creating cryptographic encryption schemes based on the principles of solving multivariate based problems. Schemes created from this principle include the UOV algorithm and the variants of HFE schemes

- HASH BASED CRYPTOGRAPHY:
  This involves creating cryptographic encryption schemes based on the principles of hash functions. So far, they are limited only to creating signature schemes

- CODE BASED CRYPTOGRAPHY:
  This involves creating cryptographic encryption schemes based on the principles of error correcting codes. Commonly known schemes created from this principle include the McEliece and Niederreiter encryption

schemas

- SYMMETRIC KEY QUANTUM RESISTANCE:
  This involves in creating cryptographic encryption schemes based on the principles of using sufficiently large key sizes. Commonly known schemes created from this principle include the AES & SNOW 3G

LATTICE CRYPTOGRAPHY:

In general terms, a lattice is can be defined as a multidimensional figure found in a grid of points spaced apart from one another in all directions possible. This lattice is formed from a 'basis' which is a set of vectors in the grid associated with integer numbers. Though lattices can be easily calculated and formed accordingly, problems like close vector (CVP), short vector (SVP) are found to be NP-Hard problems when the dimensions of a lattice increases. Also, it serves as a trapdoor function where if you start to solve the problem and encounter an error in your way, you will not be able to go back and rectify it, serving as an apt scheme which can counter brute force analytical attacks by adversaries where they try all possibilities to get the result. With these factors, cryptoanalysis in the field of lattices became a widely discussed, researched & analysed topic for post quantum cryptography

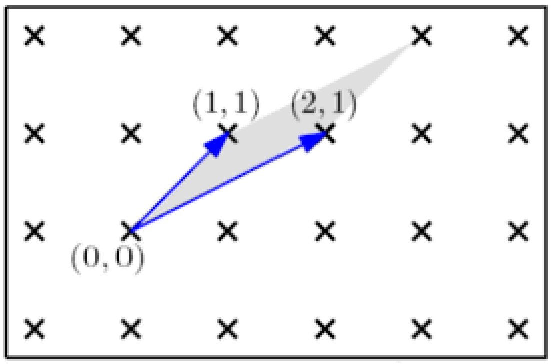


Figure 5: A two-dimensional lattice [4]

Lattice cryptosystems are one of the top leading candidates for post quantum cryptography techniques against quantum computers themselves. As it is being researched as we speak to make it viable for real world use, lot of analysis have been going on to create new algorithms, find out flaws from the existing ones and on suggesting recommendations to improve them. Next, I shall be explaining the working in brief of the 3 main lattice cryptography schemes and referring to the analysis study made by W.C. Easttom in the *A Comparative Study of Lattice Based Algorithms for Post Quantum Computing* paper[5]. I will brief about its advantages, disadvantages and the improvements made in it till now. To warrant simplicity, I have cited the necessary papers from which my results were taken from so that readers interested more in the technicalities can have a look

MAIN SCHEMES IN LATTICE CRYPTOGRAPHY:

- **Ring - Learning With Errors (RLWE) encryption**:

  This scheme works by using the Learning with Errors (LWE) problem, which is said to have strong asymptotic behaviour (where a function of expressions may seem to approach a end as it is getting solved & solved, but would never end up giving the final result)such that even the average case of a LWE problem is least as hard to solve the worst case lattice problem. Many lattice based functions have been created based on this problem, which includes- public key encryption, identity key encryption and key exchange.

  But due to a drawback of giving result to a large key size, a variation of the LWE problem known as the Ring

LWE (RLWE) problem was introduced, which would be equally hard to solve few very hard problems in ideal lattices

In a general sense, the search version of RLWE is to find the secret ring element within a given multiple random ring products which are "noisy"(highly non uniform) while its decision version is to find out the difference between the uniformly random ring products from the non-uniform ones.

To mathematically describe it[20]- Its parameters include:

a) Ring 'R' represented as $R = \mathrm{Z}[X]/(f(X))$ where $f(X)$ is an irreducible function
b) Quotient ring 'R_q' represented as $R_q := R/qR$ where q is a positive integer modulus
c) An error distribution represented as 'χ' over R
d) Number of samples provided to the attacker

Now the problem is to find a uniformly random secret 's' where $s \in R_q$, when given the individual samples of the form: $(\boldsymbol{a_i}, \boldsymbol{b_i} = \boldsymbol{s} \cdot \boldsymbol{a_i} + \boldsymbol{e_i}) \in \boldsymbol{R_q} \times \boldsymbol{R_q}$, where each $ai \in Rq$ is uniformly random and each $ei \leftarrow \chi$ is drawn from the error distribution. The main thing now needed to solve the problem is to distinguish samples of the above form from uniformly random samples over $Rq \times Rq$

From the various analyses done by various researchers, it comes to the conclusion that RLWE can be a secure scheme only if implemented properly. From the Crockett study[6] (2017), one important parameter they had found to look out for making a secure scheme was to have a good quality lattice vector as determined by the Hermite factor. Also, they demonstrated from their analysis on having proper selection of variables and block size for better implementation results. Also from the Fluhrer study[7] (2016), it was noted that reusing the shared key in this scheme can bring on a heavy dent to the security and pressed on avoiding it.

- **Goldreich–Goldwasser–Halevi (GGH) Encryption**:

This Goldreich–Goldwasser–Halevi (GGH) cryptosystem scheme works by using the Closest Vector Problem (CVP) with a one-way function. The CVP works by providing a given lattice with a vector space, a lattice vector which need not be under the vector space and a metric, where we need to find a vector in the lattice closest to the given vector. Also the one way function tries to make sure that once started to find the solution, it would be impossible to return back to the previous steps in case if an error is encountered. This helps greatly against brute force attacks

In this[19], for an 'n' dimensional lattice, embedded in 'd' dimensional space, plaintext space 'm', Ciphertext 'c' , error message 'e' & a Unimodular matrix 'U':

a) Public key= B' where B'=BU
b) Private key= B
c) Encryption process:
    c = (B' * m) + e
d) Decryption process:
    B^{-1} c which can be expanded as = B^{-1} (B'm + e) = B^{-1} (Bum + e) = B^{-1}Bum + B^{-1}e= Um + B^{-1}e
    Using Babai's algorithm we can remove B^{-1}e
    By computing U^{-1} to Um we can then arrive with result 'm'

With regards to real world viability: GGH was considered unusable as a real world protocol after the studies of Nguyen & Regev[8] 2009. But after few studies, it came to the conclusion that though its current form may not be viable, it has great potential to be a basis where new changes can be implemented, resulting in schemes which can be made viable. One good example would be the results of the Yoshino and Kunihiro[9] (2012) study, where they had proposed for the addition of a new parameter called ‘k’, having a new and high length parameter called perturbation factor represented as ‘r’ and giving further new conditions to the matrix, resulting in a schema better suited for cryptoanalysis but slow in decryption

- **N-th degree Truncated polynomial Ring Units (NTRU) Encryption**:
  This scheme works by using the Shortest vector problem (SVP) in a lattice. The SVP works on the difficulty of factoring few polynomials into 2 quotient polynomials in a truncated polynomial ring (ring of polynomial numbers formed from set of variables with coefficients). Found in 1996, this is the newest schema of the mentioned all

  In this[19], considering the main 3 integers ‘N’,’p’ & ‘q’ at degree ‘N-1’ in the truncated polynomial ring where N is prime, q>p and q & p are co-primes, the to be found polynomials as ‘f’ & ‘g’ where f must be such that $f*f_p=1$ and $f*f_q=1$, message ‘m’ , ciphertext ‘c’ and a random vector ‘r’:

  a) f, f_p & g are receiver’s private key
  b) Public key ‘h’ is calculated from: $h= p*f_q*g \pmod q$
  c) Encryption process:
  $c = m + (h*r)$ [mod q]
  d) Decryption process:
  Consider: $a= f*e$ [mod q] = $f*(r*h + m)$ [mod q] = $f*(r*pf_q*g + m)$ [mod q]= $pr*g + f*m$ [modq]
  Consider: $b= a$ [mod p]= $f*m$ [mod p]
  Now from Receiver’s side: $c= f_p*b= f_p*f*m$ [mod p]= m [mod p]
  from which Receiver can find the message ‘m’

  Looking at the analysis of Albrecht, Bai, & Ducas, 2016[10]; Kirchner & Fouque, 2016[11]; Singh & Padhye, 2017[12], NTRU schema is comparatively more sound in the mathematics part than other 2 schema but final result still depend on its proper implementation

RESULTS:

The best schema is one which has a good mathematical problem executed with perfect implementation. From the given results, we can see that currently NTRU Encryption schema is a leading candidate compared to the other two due to its soundness in mathematics, though all encryption schemes finally depend on implementation method. Since all 3 schemas were till now not been made to test on real environments which can practically execute them, not much solid evidence can be given right now on their implementation viabilities; except to analyse further on its theoretical possibilities by trying out different variations in the current algorithm & research further on developing quantum computers to test them on

CONCLUSION:

The realisation of quantum computing and quantum cryptology is currently farfetched, owing to the lack of resources required to sustain the system for longer periods of time and coming up with a cryptosystem strong enough against all factors and odds. As we have seen, even lattice cryptography and its schemes- dubbed as one of the main contenders for choosing to make cryptography schemas from- are still open to more research to become viable to the real world. Security though overlooked as secondary task by many still needs more focus and importance since once a quantum computer enters the game, it will be the saviour for a network & system dependent mankind

REFERENCES:

[1] Wikipedia: https://en.wikipedia.org/wiki/Scytale

[2] Forbes.com (https://www.forbes.com/sites/ibm/2020/01/16/the-quantum-computing-era-is-here-why-it-mattersand-how-it-may-change-our-world/)

[3] IBM Research (research.ibm.com)

[4] Oded Regev: Lattices in computer science (https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/index.html)

[5] Easttom II, W. C. (2018). *A Comparative Study of Lattice Based Algorithms for Post Quantum Computing* (Doctoral dissertation, Capitol Technology University).

[6] Crockett, E. (2017). *Simply safe lattice cryptography* (Doctoral dissertation, Georgia Institute of Technology)

[7] Fluhrer, S. R. (2016). Cryptanalysis of ring-LWE based key exchange with key share reuse. *IACR Cryptol. ePrint Arch.*, *2016*, 85.

[8] Nguyen, P. Q., & Regev, O. (2009). Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology*, *22*(2), 139-160.

[9] Yoshino, M., & Kunihiro, N. (2012, October). Improving GGH cryptosystem for large error vector. In *2012 International Symposium on Information Theory and its Applications* (pp. 416-420). IEEE.

[10] Albrecht, M., Bai, S., & Ducas, L. (2016, August). A subfield lattice attack on overstretched NTRU assumptions. In *Annual International Cryptology Conference* (pp. 153-178). Springer, Berlin, Heidelberg.

[11] Kirchner, P., & Fouque, P. A. (2016). Comparison between Subfield and Straightforward Attacks on NTRU. *IACR Cryptol. ePrint Arch.*, *2016*, 717.

[12] Singh, S., & Padhye, S. (2017). Cryptanalysis of NTRU with n Public Keys. In *2017 ISEA Asia Security and Privacy (ISEASP)* (pp. 1-6). IEEE.

[13] Preskill, John (2018-08-06). "Quantum Computing in the NISQ era and beyond". Quantum. 2: 79

[14] Harrow, Aram W.; Montanaro, Ashley (September 2017). "Quantum computational supremacy". Nature. 549 (7671): 203–209

[15] Daniel J. Bernstein (2009). "Introduction to post-quantum cryptography" (PDF).

[16] Nguyen, Phong Q. (1999). "Cryptanalysis of the Goldreich–Goldwasser–Halevi Cryptosystem from Crypto '97". CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag. pp. 288–304

[17] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. NTRU: A Ring Based Public Key Cryptosystem. In Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998

[18] Regev, Oded (2005-01-01). "On lattices, learning with errors, random linear codes, and cryptography". Proceedings of the thirty-seventh annual ACM symposium on Theory of computing - STOC '05. ACM. pp. 84–93

[19] Cordaro, J. A., Helinski, C. B., Marshall, N., & Torgerson, M. D. (2019). *Assessment of Post-Quantum Cryptographic Algorithms* (No. SAND2019-0111). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[20] Crockett, E., & Peikert, C. (2016). Challenges for Ring-LWE. *IACR Cryptol. ePrint Arch.*, *2016*, 782.