Survey of Lattice Based Post-Quantum Cryptography and its Applications

Aaron Weinberg
B.S. Candidate: Department of Electrical
Engineering and Computer Science
Case Western Reserve University
Cleveland, OH, USA
aaw66@case.edu

Colby Saxton
B.S. Candidate: Department of Electrical
Engineering and Computer Science
Case Western Reserve University
Cleveland, OH, USA
cas264@case.edu

Abstract

Lattice Based Encryption has emerged as the most popular encryption technique to handle encryption in a post-quantum world in the near future. In this paper, we hope to analyze all aspects of Lattice-Based Encryption. First we hope to detail its relevance and impact through a comparison to classical encryption techniques. Second we hope to describe what Lattice Encryption is in detail as well as describe NP-Hard problems commonly used in Lattice-Based Encryption models. Then we analyze Lattice-Based Schemas and detail how each works. Then we look at applications of Lattice-Based Encryption in various realms and highlight where further applications and work may be done to further progress the use of Lattice-Based Encryption.

Introduction

This is a survey of lattice-based cryptography and its applications. In this paper we will discuss weaknesses of classical encryption methods particularly in the post-quantum era, lattice encryption as a possible alternative and its comparison to classical encryption. We will discuss lattice problems as the mathematical basis to lattice encryption, and lattice encryption schemas. We will then conclude with a dive into the many current and future possible applications of lattice encryption.

Weakness of Classical Encryption

Classical computing is based on transistors and encoding bits to be a 1 or a 0. Quantum computing using qubits where a single bit can be used to encode more than two states. Quantum computers do exist already but only on small scales which have not yet reached quantums predicted possibilities. The challenge is building a quantum computer big enough in terms of qubit capacity to perform useful tasks better than classical computers and reducing the error in reading qubits.

Many parties are racing to do this and when quantum computers become powerful enough they pose a very real risk to our current classical encryption techniques. Companies, governments and academia around the world are all investing heavily in research into quantum computers and catching headlines about computing records being broken and further technology developments. While there is much hype, progress is still likely at least a couple years away from unlocking the theoretical potential of quantum computers and making them commercially available. Still quantum computers are coming and will be a breakthrough technology allowing us to solve many of the world's hardest problems;

however quantum computers also pose a risk to technology we depend on today.

With quantum computers it is possible to create algorithms that run orders of magnitude faster than on classical computers and break current encryption algorithms rendering their ability to secure information useless. Symmetric key algorithms like AES are thought to be safe with a sufficient enough key length, but current public key schemes like RSA which is very widely used, relies on factorization and would be rendered useless once more powerful quantum computers come to fruition. Quantum computers will make it possible to break nearly all practical applications of cryptography in use today, making things like secure digital communication, e-commerce, and other digital applications we rely on insecure and easily vulnerable to attack.

Lattice Encryption

Current post-quantum cryptography research is focused on many different approaches. Multivariate, hash-based, code-based, supersingular elliptic curve, and symmetric key quantum resistance and Lattice-based cryptography among others are the focus of research for post-quantum cryptography.

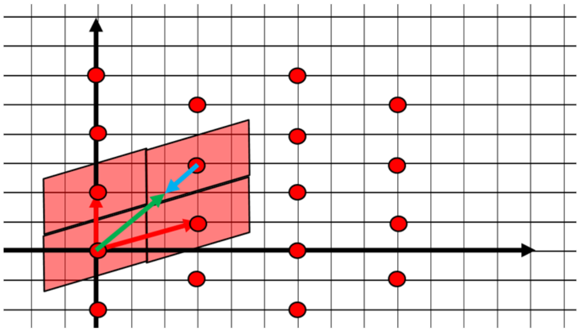
Of these, lattice-based cryptography is one of the leading candidate approaches for post-quantum cryptography. Lattice encryption is a cryptographic scheme that utilizes lattice problems to secure messages. The security of lattices is based on the hardness of these well-studied lattice problems which will be discussed later.

Unlike the widely used and well known public-key schemes, which are easily attacked by a quantum computer, many lattice-based cryptographic constructions are resistant to attack by both classical and quantum computers as there is no way to solve certain lattice problems efficiently even with quantum computers.

What is a Lattice?

A lattice is a mathematical construction made of a regularly spaced grid of points (vectors), stretching to infinity. A lattice can be highly dimensional, on the order of thousands or tens of thousands of coordinates for a cryptographic scheme. Figure 1 shows a simple two dimensional lattice with vectors.

Figure 1: Two dimensional lattice with vectors



Such a lattice spans the real vector space and can be represented by a finite object called the basis vector. A basis vector is a collection of vectors and any lattice can be represented by many different basis vectors. The whole lattice is formed by all linear combinations with integer coefficients of the basis vectors.

Lattice vs Classical Encryption

Classical Encryption

Classical Encryption like RSA, Diffie Hellman Key Exchange, SHA256, and Elliptic Curve usually have smaller key sizes. These schemas require relatively high computational processing and encryption is based on discrete mathematics and factorization problems which are computationally inefficient to solve in polynomial time with classical computing. However, classical encryption schemas can be solved in polynomial time with known algorithms running with a quantum computer.

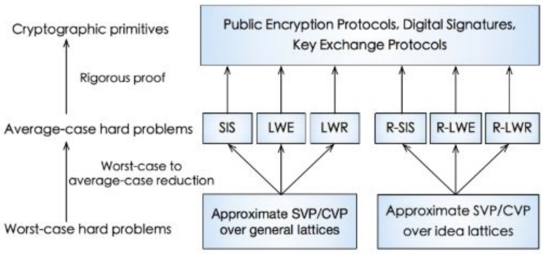
Factorization cryptographic schemes like RSA rely on integer factorization which is a worst-case problem meaning it is only secure for certain prime numbers keys and the such keys must be chosen very carefully.

Lattice-Based Encryption

Lattice-based encryption has larger key sizes but requires significantly less computational processing. Encryption schemas are based on lattice problems such as Shortest Vector Problem (SVP), Shortest Integer Solution (SIS) and Learning With Errors (LWE) problems which will be discussed in more detail in the next section. Importantly these lattice problems unlike classical public key encryption cannot be solved in polynomial time by classical or quantum computers.

Lattice based cryptography is based on average-case hard problems meaning for any average key the lattice problem will remain hard and therefore secure. Practically this means that the selection of keys can be done uniformly and randomly with proper parameter size to ensure security. Figure 2 below shows that the shortest vector problem is a worst-case hard problems but in lattice-based cryptography there are many average-case problems such as the short integer solution and learning with errors that enjoy a worst-case to average-case reduction allowing easy construction of cryptographic schemes and proofs of their security.

Figure 2: Worst-case to average-case reduction


Cryptographic primitives
Public Encryption Protocols, Digital Signatures, Key Exchange Protocols
Rigorous proof
Average-case hard problems
SIS
LWE
LWR
R-SIS
R-LWE
R-LWR
Worst-case to average-case reduction
Worst-case hard problems
Approximate SVP/CVP over general lattices
Approximate SVP/CVP over idea lattices

Lattice-based encryption allows for many practical applications as well. Lattice-based encryption allows for uses in Group Signatures, practical fully homomorphic encryption, IOT and connected devices, and oblivious transfer. Lattice-based encryption has possibilities in financial technology, cryptocurrencies, blockchain, and Electronic voting.

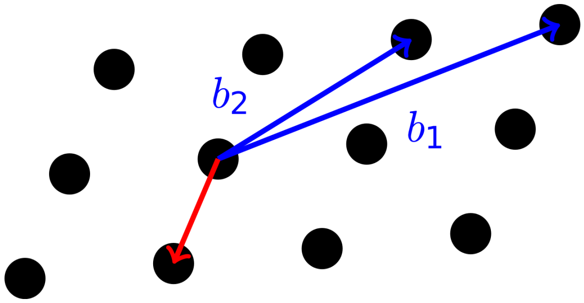
Lattice Problems

SVP - Shortest Vector Problem

Given long basis vectors of a lattice and a norm or function that calculates length, find the shortest non-zero vector in the lattice.

This may seem easy if already given short basis vectors. Figure 3, below, is an illustration to show the problem, basis vectors in blue and the shortest vector in red.

Figure 3: Example SVP Problem



This lattice problem turns out to be mathematically hard to solve in a high dimensional space with long basis vectors and requires exponential time. Currently we do not know of any algorithms that would solve this problem in polynomial time even with quantum computers. The hardness of solving this problem is what provides the security proof to many lattice-based encryption schemes [16].

SIS - Shortest Integer Solution

The Shortest Integer Solution is a mathematically hard problem commonly used in Lattice-based encryption schemes. What the problem is trying to solve is to find a nonzero integer vector, z that meets the condition of $Az = 0 \bmod q$. Solving this problem on average (with any noticeable probability) is at least as hard as approximating several lattice problems on n-dimensional lattices in the worst case to within poly(n) factors [16]. The SIS lattice enjoys a worst-case to average-case reduction from SVP.

LWE - Learning with Errors

Learning with errors is a machine learning problem that is mathematically hard to solve. An algorithm would solve the LWE problem if given samples to a linear function that deviate by a known noise model the algorithm can recreate the function or a close enough approximation of it. The Learning with errors problem is a versatile problem and is used in the creation of many lattice-based encryption schemas that have been shown to be post-quantum secure [17]. LWE also enjoys a worst-case to average-case hardness reduction.

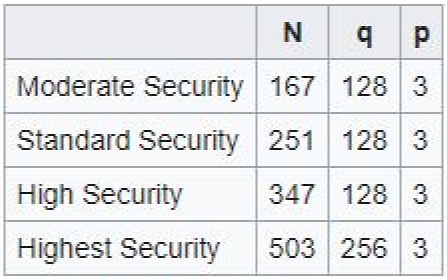
Encryption Schemas

Although numerous schemes for Lattice-based encryption we have decided to focus on NTRUEncrypt, BLISS, NewHope and DILITHIUM due to their popularity and importance as well as their use in the applications discussed in this paper.

NTRUEncrypt

NTRUEncrypt is a lattice-based encryption technique based off the Shortest Vector Problem (SVP). This encryption technique was first designed in 1996, however iterative improvements have been made over the past 20 years. Improvements has been mostly in the realm of performance increases, as well as the addition of a few security parameters. These changes have come in the form of adjusting the parameters of the secret key, ***N, q*** and ***p.*** Below, table 1, of the relative sizes of the input parameters and their levels of security.

Table 1: Parameters compared to Security Level



	N	q	p
Moderate Security	167	128	3
Standard Security	251	128	3
High Security	347	128	3
Highest Security	503	256	3

Overall, NTRUEncrypt is the most widely used lattice-based encryption technique due to its refined and fast performance as well as reliable security guarantees. Recently it has been accepted by the IEEE P1363.1 standard [15].

BLISS

BLISS is a lattice-based encryption scheme for digital signatures based on the Shortest Integer Solution(SIS) hard-problem and proposed in 2013. BLISS is widely known as the most unforgeable lattice-based encryption technique that is currently available. The reason for this heightened level of unforgeability is the way in which BLISS replaces discrete and uniform Gaussian sampling with Bimodal samples which reduces the rejection rate of this scheme [2]. BLISS claims to offer better computational efficiency and smaller signatures sizes with higher security however has yet to become standardized and is still being researched.

NewHope

NewHope is a lattice-based key-exchange encryption technique and is based on the Ring-Learning with Errors (R-LWE) hard problem proposed in 2017. NewHope follows a standard Key Exchange protocol with a few differences: a generalized reconciliation mechanism and a different error distribution model. Thus, this method utilizes a centered binomial distribution, ψ_k instead of a rounded Gaussian distribution without making a significant hit to the security. These key changes leads to parameters with a much smaller ***q*** modulus [2].

Recently google has selected NewHope for an experiment to reduce the impact of quantum computers. Google has integrated NewHope into an experimental web browser for use in HTTPs communications. NewHope has been submitted to NIST (National Institute of Standards and Technology) and is being evaluated to be standardized as a quantum robust key-exchange protocol.

DILITHIUM

DILITHIUM, one of the candidate algorithms submitted to the NIST post-quantum cryptography project is a lattice-based encryption scheme designed to prevent side channel attacks that other lattice-based encryption schemes may be susceptible to. Sampling in this scheme is uniform over some bounded domain, as well as the rejection sampling verifies that the coefficients are smaller than a certain bounded value. Additionally, the public key size is halved in comparison to other lattice based encryption techniques, making it a strong option for cryptocurrency applications [20].

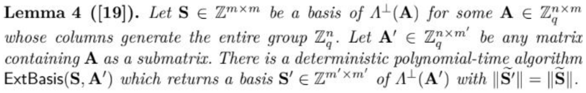
Applications

Group Signatures

Group Signatures allows a user within a group the ability to anonymously sign messages on behalf of the entire group. Additionally, group signatures include a mechanism to trace messages to a specific user within the group if the user is suspected on improper use. To reduce the risk of key exposure attacks of users within the group, a forward-secure group signature (FSGS) scheme is put in place to prevent potential attackers from forging group signatures from past events even if a new secret group key is released currently [6].

Current encryption schemes to enforce FSGS are based on number theoretical assumptions and utilize encryption schemes that are susceptible to quantum based computing attacks. To prevent this, San Ling, Khoah Nguyen, Huaxiong Wang, Yanhong Xu developed a new quantum prove implementation using lattice cryptography in their paper, *Forward-Secure Group Signatures from Lattices*. First of all, to achieve proper encryption techniques, this group utilizes the LWE hard problem to ensure the method is quantum proof. To ensure proper key distribution, the authors implemented a scalable key generating and distributing system that periodically updates all users secret keys. This structure is done through a Bonsai Tree Structure (Lemma 1) [6].

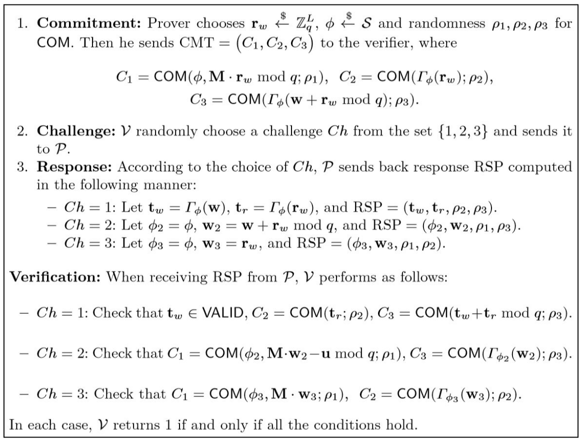
Lemma 1: Description of Bonsai Tree Structure



Lemma 4 ([19]). *Let* $\mathbf{S} \in \mathbb{Z}^{m \times m}$ *be a basis of* $\Lambda^{\perp}(\mathbf{A})$ *for some* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *whose columns generate the entire group* $\mathbb{Z}_q^n$. *Let* $\mathbf{A}' \in \mathbb{Z}_q^{n \times m'}$ *be any matrix containing* $\mathbf{A}$ *as a submatrix. There is a deterministic polynomial-time algorithm* $\mathsf{ExtBasis}(\mathbf{S}, \mathbf{A}')$ *which returns a basis* $\mathbf{S}' \in \mathbb{Z}^{m' \times m'}$ *of* $\Lambda^{\perp}(\mathbf{A}')$ *with* $\|\widetilde{\mathbf{S}'}\| = \|\widetilde{\mathbf{S}}\|$.

This Bonsai Tree Structure provides the option to either control how the group signature key scheme is released to individuals, or let the tree grow organically. This ultimately ensures that the signature scheme is existential unforgeable under attacks based on the SIS hard problem [6]. To ensure the validity of the generation and updating of secret keys, this implementation also uses a zero knowledge proof (Proof 1) to ensure its validity [6].

Proof 1: Zero Knowledge Proof Ensuring Proper Key Updating



1. **Commitment:** Prover chooses $\mathbf{r}_w \xleftarrow{\$} \mathbb{Z}_q^L$, $\phi \xleftarrow{\$} \mathcal{S}$ and randomness ρ_1, ρ_2, ρ_3 for COM. Then he sends $\mathrm{CMT} = \big(C_1, C_2, C_3\big)$ to the verifier, where

$$C_1 = \mathsf{COM}(\phi, \mathbf{M} \cdot \mathbf{r}_w \bmod q; \rho_1), \quad C_2 = \mathsf{COM}(\Gamma_\phi(\mathbf{r}_w); \rho_2),$$
$$C_3 = \mathsf{COM}(\Gamma_\phi(\mathbf{w} + \mathbf{r}_w \bmod q); \rho_3).$$

2. **Challenge:** $\mathcal{V}$ randomly choose a challenge Ch from the set $\{1, 2, 3\}$ and sends it to $\mathcal{P}$.
3. **Response:** According to the choice of Ch, $\mathcal{P}$ sends back response RSP computed in the following manner:
   - $Ch = 1$: Let $\mathbf{t}_w = \Gamma_\phi(\mathbf{w})$, $\mathbf{t}_r = \Gamma_\phi(\mathbf{r}_w)$, and $\mathrm{RSP} = (\mathbf{t}_w, \mathbf{t}_r, \rho_2, \rho_3)$.
   - $Ch = 2$: Let $\phi_2 = \phi$, $\mathbf{w}_2 = \mathbf{w} + \mathbf{r}_w \bmod q$, and $\mathrm{RSP} = (\phi_2, \mathbf{w}_2, \rho_1, \rho_3)$.
   - $Ch = 3$: Let $\phi_3 = \phi$, $\mathbf{w}_3 = \mathbf{r}_w$, and $\mathrm{RSP} = (\phi_3, \mathbf{w}_3, \rho_1, \rho_2)$.

Verification: When receiving RSP from $\mathcal{P}$, $\mathcal{V}$ performs as follows:

- $Ch = 1$: Check that $\mathbf{t}_w \in \mathsf{VALID}$, $C_2 = \mathsf{COM}(\mathbf{t}_r; \rho_2)$, $C_3 = \mathsf{COM}(\mathbf{t}_w + \mathbf{t}_r \bmod q; \rho_3)$.
- $Ch = 2$: Check that $C_1 = \mathsf{COM}(\phi_2, \mathbf{M} \cdot \mathbf{w}_2 - \mathbf{u} \bmod q; \rho_1)$, $C_3 = \mathsf{COM}(\Gamma_{\phi_2}(\mathbf{w}_2); \rho_3)$.
- $Ch = 3$: Check that $C_1 = \mathsf{COM}(\phi_3, \mathbf{M} \cdot \mathbf{w}_3; \rho_1)$, $C_2 = \mathsf{COM}(\Gamma_{\phi_3}(\mathbf{w}_3); \rho_2)$.

In each case, $\mathcal{V}$ returns 1 if and only if all the conditions hold.

After the implementation of these systems, the user can then achieve a full quantum proof forward-secure group signature scheme.

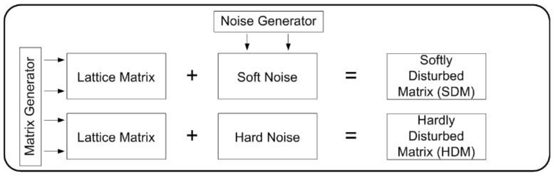
Homomorphic Encryption

Homomorphic Encryption is the ability to perform computations on ciphered data such that the operations would be the same had they be done on such deciphered data. Current encryption/signature scheme for homomorphic encryption are susceptible to attacks by quantum computers.

In a paper written by Carlos Aguilar Melchor, Guilhem Castagnos, Philippe Gaborit called *Lattice-based homomorphic encryption of vector spaces,* a new homomorphic encryption lattice-based technique is created. To achieve this, the authors described the technique in the following steps [4]:

First the user starts with a secret random N × 2N matrix M of rank N over a field Z/pZ and to hide the subspace it represents. This matrix is then used to produce a set of matrices which are then disturbed using a noise generator. Matrices can either be softly disturbed or hardly disturbed by the noise generator as seen in figure 5 [4].

Figure 5: Visualization of Creation of SDM and HDM



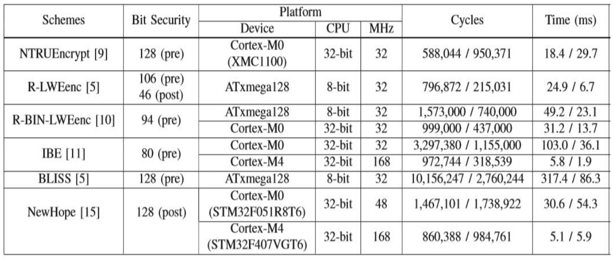
The public key is made up of one hardly disturbed matrix (HDM) and n, number of softly disturbed matrices (SDM). For the target matrix, it is encrypted by multiplying itself by the HDM. Then for each SDM in the public key, a vector is populated in the encrypted matrix using a set of small coordinates. Then using knowledge of the initially hidden subspace matrix and the position of unmodified columns of the HDM and SDMs, the noise of the encrypted matrix can be recovered [4].

The homomorphic properties of this scheme comes directly from the additive properties of the vectors within the encrypted matrix. For example, the addition of two encrypted messages is equivalent to the sum of two vectors of the hidden subspace plus two hard noises induced by the encrypted messages in addition to two small noises induced by the SDMs. By choosing ad hoc parameters, it can be ensured that the small noise parameters remains indistinguishable from the hard noise while still maintaining the proper homomorphic properties [4].

Internet of Things

Internet of Things is a network of internet connected devices beyond traditionally known computing devices. These devices are not designed with security in mind and are notoriously susceptible to malicious attacks such as Sybil and DDOS. Lattice encryption offers lightweight security guarantees with higher efficiency and lower latency for resource constrained devices. This is a large improvement over classical encryption which is typically too computationally expensive to implement on small processors in IoT devices.

Table 2: Implementation of Lattice Based Encryption Schemes on Lower Powered Controllers



Schemes	Bit Security	Platform			Cycles	Time (ms)
		Device	CPU	MHz		
NTRUEncrypt [9]	128 (pre)	Cortex-M0 (XMC1100)	32-bit	32	588,044 / 950,371	18.4 / 29.7
R-LWEenc [5]	106 (pre) 46 (post)	ATxmega128	8-bit	32	796,872 / 215,031	24.9 / 6.7
R-BIN-LWEenc [10]	94 (pre)	ATxmega128	8-bit	32	1,573,000 / 740,000	49.2 / 23.1
		Cortex-M0	32-bit	32	999,000 / 437,000	31.2 / 13.7
IBE [11]	80 (pre)	Cortex-M0	32-bit	32	3,297,380 / 1,155,000	103.0 / 36.1
		Cortex-M4	32-bit	168	972,744 / 318,539	5.8 / 1.9
BLISS [5]	128 (pre)	ATxmega128	8-bit	32	10,156,247 / 2,760,244	317.4 / 86.3
NewHope [15]	128 (post)	Cortex-M0 (STM32F051R8T6)	32-bit	48	1,467,101 / 1,738,922	30.6 / 54.3
		Cortex-M4 (STM32F407VGT6)	32-bit	168	860,388 / 984,761	5.1 / 5.9

In a paper titled, Lattice Encryption IoT by Rui Xu, Chi Cheng, Yue Qin and Tao Jiang, the above table 2 was created to investigate the application of various lattice-based encryption schemes applied in low-powered controllers for IoT use [5].

NTRUEncrypt, being the standard for Lattice Encryption currently, yields 128 bit security on 32 bit CPUs. It achieves this level of security with encryption and decryption times both under 30 ms. Other schemes yielding similar results on similar processors is the NewHope encryption scheme with yielded encryption and decryption times under 55 ms on a similar 128 bits of security on a 32 bit CPU. Schemes such as R-LWEenc and R-BIN-LWEenc were able to offer ~100 bit security on 8 bit processors in under 25 ms and 50 ms respectively [5].

In comparison with classical encryption schemes, the current state-of-art implementation of R-LWE based encryption on 8-bit AVR microcontroller can finish an encryption within 2 million cycles, while the RSA-1024 (has a lower level of security and no post-quantum security) implementations on comparable devices need more than 23 million cycles for the same task [5]. Overall, this table shows that for varying IoT processors, different schemes of Lattice-Encryption are lightweight and feasible security mechanisms that can prevent the threat of malicious attacks from quantum computers and run efficiently on IoT devices.

Oblivious Transfer

Oblivious transfer is a cryptographic primitive that encryption schemes are designed from. For example, authenticated key exchange and password-based authentication key exchange are based off Oblivious Transfer. Security in oblivious transfer revolves around preventing unauthorized access from illegitimate entities. To combat the threat of quantum computing on oblivious transfer, lattice-based encryption techniques have been implemented for the past twenty years. The first of such model was designed via dual mode encryption and has limited applications due to its inefficient encryption technique. A new model was proposed by Zengpeng Li, Can Xiang and Chengyu Wang in their paper titled, *Oblivious Transfer Via Lossy Encryption from Lattice-Based Cryptography* [1].

The main difference between the oblivious transfer application described in the paper and previous applications is dependant on their use of lossy encryption. In past methods, the ciphertext of a message is generated by encrypting the plaintext under an injective key. However, via lossy encryption, the ciphertext is completely isolated from the plaintext. The authors utilize lossy encryption by adapting a multiple bit GPV scheme to use within a LWE-based lossy encryption technique. From this new application of oblivious transfer, it can achieve multibit decryption, which reduces the time of performance requirements to perform this encryption technique, making it far more practical [1].

Genomic Susceptibility Testing

Genomic Susceptibility testing has become increasingly common to test patients for potential genetic diseases. Currently, many laboratories must outsource this data to third party sites for analyzation which presents large privacy risks for these patients’ genomic data. Juan Ramon Troncoso-Pastoriza, Alberto Pedrouzo-Ullao and Fernando Perez-Gonzalez recently submitted a new method of achieving quantum proof secure testing in their paper titled, *Secure Genomic Susceptibility Testing Based on Lattice Encryption* [3].

To achieve quantum proof encryption, this team utilized R-LWE as their cryptosystem. Areas of greater susceptibility within a patient's genomic data are called Single Nucleotide Polymorphisms (SNPs). SNPs are suitable for running disease susceptibility testing due to their high frequency of diseases being found within. The general layout of the schema can be seen in figure 6 [3].

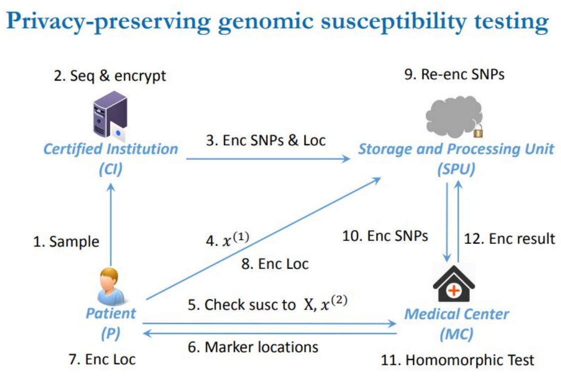


Figure 6: Secure Testing Protocol

The protocol goes as follows:

First the Certified analyzation institution will send their necessary keys to the Storage and Processing Unit. Second, after the patient sends their biological sample to the Certified Institution, the latter will sequence and analyze their SNPs whose locations are encrypted. These encrypted positions are then send to the Storage and Processing Unit. The medical center marks the locations of the SNPs [3]. It additionally sends the susceptibility of disease x whose identity is encrypted to the patient. Then the patient encrypts the location of diseases, x and sends it to the Storage and Processing Unit. Then the Storage and Processing Unit computes the susceptibility of the patient to disease x using homomorphism and then uses the relinearization matrix to switch the results to the Medical Center’s key and then sends it to the Medical Center. Then the Medical Center decrypts the results. Thus, this completes the secure genomic susceptibility testing using LWE-based encryption and homomorphism techniques [3].

Bitcoin - Blockchain

In blockchain based cryptosystems and signature schemes, the higher the memory usage(i.e. Block size) the more centralized the network becomes over time(assuming it is not already centralized by design, which most are). The primary centralized attack vector is the mining network involved in providing network consensus for transactions. The amount of data stored on the public ledger greatly affects the topology of the network(especially over time) and decreases the network's decentralization. The mining network becomes more centralized due to the fact that better hardware has more of an edge in mining bigger blocks, causing the mining industry to become more centralized and top heavy because it takes more computational power to remain profitable as a miner.

The second main attack vector via bigger blocks is due to the same supply and demand economic effects that occur amongst the mining network. Individual nodes who are downloading the entire blockchain and verifying that everyone on the network has the same copy of the same ledger also will need more computationally capable hardware to store the distributed ledger and thus will also become more centralized over time, allowing for bad actors to compromise the network and even possibly inflate the supply or double spend. In the context of blockchain, the most important parameters of a signature scheme are the signature and public key lengths which must be stored to fully verify transactions, as well as the timestamp to verify the signature [12]. With the sum of the signature and public key lengths in mind, hash and lattice based schemes are the only reasonable options for use in such networks.

Assuming the chosen hash function behaves like a random oracle, hash based schemes like XMSS have the advantage of having provable security [13]. Grover's algorithm is used for what is considered to be the generic attack against these schemes which means that their quantum security level is half of the classical security level. Current Classical Encryption Schemes can be contrasted in that the best known quantum attack against DILITHIUM at a 138 bit classical security level requires time 2^{125} [20]. Thus at the same level of quantum security, lattice based schemes have some advantage in signature plus public key length.

Although the lattice based scheme BLISS has the shortest sum of signature and public key lengths at 12kb(compared to DILITHIUM's 33.4kb) of all the quantum proof candidates, in practice there are reasons not to use it. The security of the BLISS relies on the hardness of the NTRU problem and the assumption that solving this problem is equivalent to finding a short vector in an NTRU lattice. It has been shown more recently that this assumption may not work, especially for data sets with large parameters. There is a history of attacks on previous NTRU-based signature schemes. The BLISS scheme's largest downside being that it is difficult to deploy the scheme to an application in a secure way without it being very susceptible to side channel attacks [13]. Thus, in the future it is necessary for the capitalization of the network and the network protocol itself to stay intact that these more blockchain oriented signature schemes are developed.

E-Voting

Advanced post quantum E-voting protocols have been developed and improved more and more over recent years. An E-voting cryptosystem has to have at least 3 main privacy requirements to be considered secure. One is vote-privacy, meaning the attacker cannot discern how a voter votes from any information that the voter may reveal for necessary purposes during the course of the election [14]. Another requirement is receipt-freeness, meaning the attacker cannot discern how a voter votes even if the voter voluntarily reveals additional information. The last one is coercion-resistance which is the strongest privacy requirement out of the three. Coercion-resistance is achieved if the attacker cannot discern how a voter votes even if the voter cooperates during the election process. Any of these requirements being met indicates that all previous requirements have been met, respectively [14].

Helios

Current encryption schemes exist which achieve the above attributes using classical encryption protocols. The most famous of which, being Helios which is widely deployed and used. This scheme uses a classical encryption protocol to provide encryption for the E-Voting system. Additionally it uses a Zero-Knowledge proof to verify the validity of the voter's identity. Once users have been properly verified, the user's name or an anonymous ID is placed on a publicly available ledger. Then the scheme randomizes the vote order and uses homomorphic encryption to count the votes [14].

Lattice E-voting

Lattice-based E-voting protocols have already started being developed and tested using security schemes based on classical Short Integer Solution(SIS) and Learning with Errors(LWE) assumptions.

One such scheme by Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, Malika Izabachène from their paper titled *A Homomorphic LWE Based E-voting Scheme* utilizes LWE hard problem for its encryption scheme. This paper proposes a new procedure to distribute the decryption task, where each trustee provides an independent proof of correct decryption in the form of a publicly verifiable ciphertext trapdoor. This scheme requires only two trustees, unlike classical E-voting proposals using threshold cryptosystems via Shamir's secret sharing. While Helios is broken by Schor's quantum algorithm, this new encryption technique cannot be broken by such quantum based algorithms. Additionally, Helios's additive homomorphism lacks expressiveness. This gets rid of the need in Helios for each voter to ensure that the plaintext encrypted in their ballot has a specific shape that is suitable for homomorphic additions. In addition, the lattice based encryption scheme shows that it can be distributed among t trustees, relying on a simple concatenated LWE scheme instead of using a threshold [14].

Another E-voting protocol proposed by researchers at IBM in 2017 is called EVOLVE and improves upon the previously mentioned scheme using SIS and LWE [14]. At its core EVOLVE is a homomorphic scheme involving a number of voting authorities. Privacy is maintained as long as at least is honest and the correctness of the results are guaranteed even if the authorities collude, and results can be independently computed by any observer. EVOLVE has been tested and shown to be both computationally, space efficient, and secure making it a great candidate to replace Helios as an e-voting scheme that is secure against quantum attacks.

Conclusion

Challenges

1. Provable security doesn't guarantee security in practice and might cause practical security to be overlooked.
2. Choosing appropriate parameters for lattice-based schemes is a challenge being addressed by ongoing research.
3. Need for a unified model of evaluating security of lattice-based cryptography. This is sited as a need by many papers and researches.
4. Quantum attacks can have quantum interaction with the cryptosystem. See quantum random oracle model in the literature [19].

Within this paper, we covered the following topics: First we detailed the relevance of Lattice-Based Encryption and its impact through a comparison to classical encryption techniques. Second we described what Lattice Encryption is in detail as well as describe NP-Hard problems commonly used in Lattice-Based Encryption models. Then we analyzed Lattice-Based Schemas and detail how each works. Then we look at applications of Lattice-Based Encryption in various realms and highlighted where further applications and work may be done to further progress the use of Lattice-Based Encryption. Overall, Lattice Encryption is a multi-faceted encryption technique that has the potential to be used in a wide array of applications in the near future due to the rising threat of quantum computing and its effect on current encryption protocols.

VI. References

[1] Z. Li, C. Xiang, and C. Wang, "Oblivious Transfer via Lossy Encryption from Lattice-Based Cryptography," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–11, 2018.

[2] N. Bindel, J. Buchmann, and S. Rieß, "Comparing apples with apples: performance analysis of lattice-based authenticated key exchange protocols," *International*

Journal of Information Security, vol. 17, no. 6, pp. 701–718, 2017.

[3] J. R. Troncoso-Pastoriza, A. Pedrouzo-Ulloa, and F. Perez-Gonzalez, “Secure genomic susceptibility testing based on lattice encryption,” *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017.

[4] C. A. Melchor, G. Castagnos, and P. Gaborit, “Lattice-based homomorphic encryption of vector spaces,” *2008 IEEE International Symposium on Information Theory*, 2008.

[5] R. Xu, C. Cheng, Y. Qin, and T. Jiang, “Lighting the Way to a Smart World: Lattice-Based Cryptography for Internet of Things,” *arXiv*, May 2018.

[6] S. Ling, K. Nguyen, H. Wang, and Y. Xu, “Forward-Secure Group Signatures from Lattices,” arXiv, Jan. 2019.

[7] Bindel, Nina, et al. “Comparing Apples with Apples: Performance Analysis of Lattice-Based Authenticated Key Exchange Protocols.” International Journal of Information Security, vol. 17, no. 6, Nov. 2018, pp. 701–718. EBSCOhost, doi:10.1007/s10207-017-0397-6.

[8] D. S. Gupta, G. P. Biswas, and R. Nandan, “Security weakness of a lattice-based key exchange protocol,” 2018 4th International Conference on Recent Advances in Information Technology (RAIT), 2018.

[9] Sepahi, Reza, et al. “Lattice-Based Certificateless Public-Key Encryption in the Standard Model.” International Journal of Information Security, vol. 13, no. 4, Aug. 2014, pp. 315–333. EBSCOhost, doi:10.1007/s10207-013-0215-8.

[10] Buchmann, Johannes, et al. “Post-Quantum Cryptography: Lattice Signatures.” Computing, vol. 85, no. 1/2, Aug. 2009, pp. 105–125. EBSCOhost, doi:10.1007/s00607-009-0042-y.

[11] Ikeda, K. qBitcoin: A peer-to-peer quantum cash system. arXiv preprint arXiv:1708.04955 (2017).

[12] Ali, A. (2015). Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network. *International Journal of Embedded Systems and Applications*, 5(2), pp.15-29.

[13] Alberto Torres W.A. et al. (2018) Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0). In: Susilo W., Yang G. (eds) Information Security and Privacy. ACISP 2018. Lecture Notes in Computer Science, vol 10946. Springer, Cham

[14] Chillotti I., Gama N., Georgieva M., Izabachène M. (2016) A Homomorphic LWE Based E-voting Scheme. In: Takagi T. (eds) Post-Quantum Cryptography. PQCrypto 2016. Lecture Notes in Computer Science, vol 9606. Springer, Cham

[15] S. Bu and H. Zhou, “A Secret Sharing Scheme Based on NTRU Algorithm,” 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009.

[16] D. J. Bernstein, J. Buchmann, and Dahmén Erik, Post-quantum cryptography. Berlin: Springer, 2009.

[17] R. Silva, A. C. D. A. Campello, and R. Dahab, “LWE-based identification schemes,” 2011 IEEE Information Theory Workshop, 2011.

[18] Pinom Lyubashevsky, Neven, Seiler, Practical Quantum-Safe Voting from Lattices, 2017.

[19] Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, Zhandry, Random Oracles in a Quantum World, *Lecture Notes in Computer Science Advances in Cryptology – ASIACRYPT,* 2011

[20] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle, “Dilithium: Digital Signatures from Module Lattices,” *CRYSTALS*.