An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitives

Chuck Easttom, D.Sc.
Capitol Technology University
Plano, TX
chuck@chuckeasttom.com

***Abstract*—Cryptographic primitives have been constructed on a wide range of mathematical basis. For asymmetric cryptography, those bases are problems in number theory. Lattice based mathematical problems provide a basis for cryptographic algorithms. Lattice-based cryptographic algorithms are believed to be resistant to quantum computing attacks. This makes research concerning these algorithms important. What is lacking in the current literature is a comparative study of existing cryptanalysis data for these algorithms. That data can be used to guide further research into lattice-based asymmetric cryptographic primitives. This current paper provides such a comparison.**

Keywords—mathematical lattices, lattice-based cryptography, post-quantum cryptography, asymmetric cryptography, NTRU, GGH, LWE Ring

I. INTRODUCTION

Asymmetric cryptographic primitives are based on some mathematical problem. The widely used RSA algorithm is based on the difficulty of factoring a large integer into its prime factors. Diffie-Hellman key exchange protocol is predicated on the difficulty of solving the discrete logarithm problem. Even elliptic curve cryptography is based on the difficulty of solving discrete logarithm problems of a random elliptic curve element with respect to a publicly known base point. Each of these algorithms is secure because it is difficult to solve the problems that form the basis for the algorithm. Put more precisely, there does not exist a classical computing algorithm that can solve these problems in polynomial time.

The advent of quantum computers undermines the security of these current widely used asymmetric algorithms. Shor's algorithm demonstrated that both factoring and discrete logarithm problems are solvable on a quantum computer. Peter Shor published his algorithm in 1994, and it demonstrated that on a quantum computer one could factor a given integer N into its prime factors in polynomial time [1] [2]. It is noteworthy that Shor's algorithm is probabilistic, rather than deterministic. This means a solution is not guaranteed. However, the fastest known classical computing algorithm for factoring is the general number field sieve. The number field sieve algorithm only works in sub-exponential time, making it somewhat inefficient.

The aforementioned asymmetric algorithms that are based on factoring or discrete logarithm problems are the most widely used asymmetric algorithms. There are, however, other cryptographic algorithms based on different mathematical problems. One area of cryptography that has been a focus for post-quantum computing research is lattice-based cryptography. The term "lattice-based cryptography" refers to any cryptographic algorithm based on lattices [3]. Lattice based cryptography is, in general, an improvement over classical number theoretic algorithms such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography [4] [5]. The reason for this advantage is because classical algorithms are based on average case problems, whereas lattice-based cryptography is based on worst case problems [6].

Average case problems are those which are difficult on average. For example, RSA is based on factoring, which is average case hard over a certain distribution [7]. Some numbers are not quite as difficult to factor, such as even numbers. Worst case problems are difficult to solve even in a worst-case scenario. This may appear to be an oversimplified explanation, but for the purposes of this paper it is adequate. It is also noteworthy that at least some lattice-based cryptographic systems are believed to be resistant to quantum-based attacks.

While the focus of this paper is to provide guidance for research into post-quantum cryptography using lattice-based algorithms, it must be noted that this is not the only application of this research. Many experts believe it will be at least a decade before quantum computers become a practical reality. A very small number of experts believe that we may never overcome the issues of decoherence and create practically usable quantum computers. Even if such dire predictions are accurate and quantum computing does not become a reality for many decades, or never, lattice-based algorithms present an alternative to current algorithms. RSA has long been known to be susceptible to many different attacks [8], [9], [10], [11]. The NSA formerly advocated the use of Elliptic Curve Cryptography over RSA but has since retracted that recommendation [12]. Clearly, there is a need for new more robust asymmetric algorithms, even in the absence of quantum cryptography.

The goal of this current study is to review existing literature regarding cryptanalysis of lattice-based algorithms. From that existing data, generalized information about lattice-based algorithms can be extracted. From that data, it is possible to extrapolate general guidelines for research into

978-1-7281-0554-3/19/$31.00©2019 IEEE

lattice-based algorithms. This goal of this paper is to provide such general guidelines.

II. Review of Literature

In this section an overview of current knowledge in this area is provided. That includes a review of essential mathematics, as well as a description of the algorithms in this study as well as the mathematical problems that provide the foundation for such algorithms. The basic review of lattices simply reviews fundamental mathematics required to understand the algorithms presented in this paper.

A. Lattices

Before discussing lattice based cryptographic algorithms, it is useful to briefly review the fundamentals of lattices. A lattice is a set of points in n-dimensional space with a periodic structure [13]. The basis vectors of the lattice are used to generate the lattice [14] [15]. A mathematical description of a lattice is provided in equation 1.

$$\mathcal{L}\ (b1, ...,bn) = \left\{ \sum_{l=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\} \quad (1)$$

Lattices use linearly independent vectors [16]. A set of vectors is said to be linearly dependent if one of the vectors in the set can be defined as a linear combination of the others; if no vector in the set can be written in this way, then the vectors are said to be linearly independent. These vectors form the basis for a lattice.

Another concept from linear algebra which is used frequently in lattice-based cryptography is orthogonality [17]. Two elements in a vector space (u and v) are said to be orthogonal if their dot product is zero. A dot product is the sum of the products of the corresponding elements of the two vertices [18]. Essentially, the dot product is used to produce a single number, a scaler, from two vertices or two matrices [19]. This is contrasted with the tensor product. In math, a tensor is an object with multiple indices, such as a vertex or array. The tensor product tensor product of two vector spaces, V and W, $V \otimes W$ is also a vector space [20].

Unimodular matrices are also used in some lattice-based algorithms. A unimodular matrix is a square matrix of integers with a determinant of +1 or -1. A determinant is a value which is computed from the elements of a square matrix.

B. Math problems in Lattices

As was previously stated, asymmetric cryptographic primitives are based on some mathematical problem. It must be a problem that is computationally hard to solve. This generally means that no solution can be found in polynomial time. Lattices provide several mathematical problems that can form the basis for cryptographic algorithms.

The first lattice based cryptographic system was created by Miklós Ajtai [21]. His system was based on a lattice problem known as the Short Integer Solution (SIS). The Short Integer Solution problem is summarized as follows: Given an m x n lattice A which is part of the set of integers, find an integer e satisfying $Ae = 0 \bmod \|e\|_2 < \alpha$. This problem forms the basis for Ajtai cryptographic primitive.

One of the most commonly used problems for lattice-based cryptography is the Shortest Vector Problem (SVP). Essentially this problem is that given a particular lattice, how do you find the shortest vector within the lattice. More specifically, the SVP problem involves finding the shortest non-zero vector in the vector space V, as measured by a *norm*, N. A *norm* is a function which assigns a strictly positive length or size to each vector in a vector space. The Shortest Vector Problem is presented more formally in figure 6.

Given a lattice basis A, find a non zero $v \in \mathcal{L}(A)$ such that $||v|| = \lambda_1(\mathcal{L}(A))$

Fig. 1. Shortest Vector Problem

Another such problem is the Learning With Errors (LWE) problem [22]. This is a problem from the field of machine learning. It has been proven this problem is as difficult to solve as several worst-case lattice problems. Algorithms are often measured by best-case, average-case, and worst-case solutions. Put simply, this means the LWE problem is very difficult to solve. As has already been stated in this paper, asymmetric cryptography is based on mathematical problems which are difficult to solve. In fact, the problems are so difficult to solve, no solution can be found within a practical period of time. The LWE problem has been expanded to use algebraic rings with Ring-LWE [23]. In abstract algebra a ring is an algebraic system consisting of a set, an identity element, two operations, and the inverse operation of the first operation.

In his doctoral dissertation, Eric Crockett examined lattice based cryptographic algorithms which are based on the Learning With Errors (LWE) problem [24]. The purpose of his study was to create a framework for the testing and study of these algorithms. The study postulated that almost all number theoretic cryptography applications can be constructed with lattices. This is important because lattice-based algorithms have been shown to be resistant to quantum computing based cryptanalysis attacks.

Pöppelmann and Güneysu [25], also studied lattice based cryptographic algorithms which are based on ring variations of the Learning With Errors (LWE) problem. Their study focused on those algorithms which are not patented, and thus open for anyone to use.

Particular issues of concern when implementing ring based LWE encryption are: efficient hardware implementation, efficient sampling, and reducing failures. This study used Ring-LWEEncrypt as the programming implementation of the algorithm. Pöppelmann and Güneysu made the source code they used as well as the test benches used available on their website. This is one reason this particular study is important when exploring lattice-based cryptography, the ready availability of the data, source code, and testing mechanisms utilized by the authors makes examining this algorithm easy.

Another mathematical problem which is used in lattice-based cryptography is the Closest Vector Problem (CVP).

This problem is summarized as: given a vector space V, and a metric M for a lattice L and a vector v which is in the vector space V, but not necessarily in the lattice L, find the vector in the lattice L which is closest to the vector v. This problem is related to the previously discussed SVP problem and is also difficult to solve.

These lattice-based mathematical problems are summarized in figure 4.

Problem	Basis	Relevant Algorithm
Shortest Vector Problem (SVP)	For a lattice L and one must find the shortest non-zero vector in V, as measured by a norm N, in L.	NTRUEncrypt
Closest Vector Problem (CVP)	For a given lattice L, as well as a vector v in V but not necessarily in L, find the vector in L closest to v (as measured by a metric M).	Goldreich–Goldwasser–Halevi (GGH)
Short Integer Solution (SIS)	For a given n x m matrix that consists of m uniformly random integer vectors, find a nonzero integer vector that is less than or equal to a given β. That value is usually $\sqrt{n}\log q$	Ajtai Algorithm
Learning With Errors (LWE)	This is a problem in machine learning that has been adapted to cryptography.	Piekert's Ring

Fig. 2. Summary of lattice based mathematical problems

The algorithms summarized in figure 4 are not the only mathematical problems based on lattices. However, they are the problems that have been most closely associated with cryptographic systems based on lattices.

C. *Specific Algorithms*

In this section, a general overview is provided of the algorithms identified in the previous section. This overview provides a basis for then comparing these algorithms. The goal of this section is not to provide a detailed study of each algorithm, but rather to provide a general overview. This will facilitate a better understanding of the cryptanalysis presented later in this paper. Various sources in the reference section provide more detail on the algorithms listed.

1) GGH

The GGH algorithm is a widely studied lattice-based cryptosystem. It was first published in 1997. Its name is derived from the surnames of its inventors: Glodreich, Goldwasser, and Halevi. It is an asymmetric algorithm which has been proven to be resistant to cryptanalysis. This algorithm is based on the difficulty of solving the closest vector problem (CVP).

The private key is a basis B of the lattice L. This basis vector has certain properties such as nearly orthogonal vectors and a unimodular matrix U. The public key is another basis of the same lattice of the form B' = UB. The message M is a message space which consists of the vector (m_1,..., m_n) in a range of $-M < m_i < M$. The message is encrypting by multiplying the message vector by the public key B'. This is shown mathematically in equation 1.

$$v = \sum m_i b'_i \tag{2}$$

The formula in figure 5 can be described also as

$v = m * B'$

Then the cipher text is simply:

$c = v + e$

Which is in turn equal to

$c = m * B' + ev$

The e is an error correcting vector, (1, -1). To decrypt the message the cipher text, c is multiplied by the inverse of B, B^{-1}. Put mathematically:

$M = c B^{-1}$.

Decrypting with GGH is a bit more complex and is not relevant to this current study. What is important is that it has been shown that GGH cannot be broken efficiently by current cryptanalysis techniques. This makes GGH a candidate for post-quantum cryptography. There is not a currently known quantum algorithm that can efficiently break GGH. However, as will be shown later in this paper, many implementations of GGH do have weaknesses.

2) NTRU

NTRU is another widely studied lattice-based algorithm. NTRU was invented by Jeffery Hoffstien, Jill Pipher and Joseph Silverman in 1996. This algorithm has been subjected to a substantial amount of cryptanalysis over several years. NTRU is a cryptosystem which provides both encryption and digital signatures. There have been several variations of this algorithm since its initial publication. It has been shown to be resistant to Shor's algorithm [26].

Nayak, Nanda, Awasthi, and Kumar [27] explored a very specific implementation of NTRU. In their study, they examined asymmetric cryptography using lattice-based cryptography, specifically the NTRU algorithm. What made this study unique, is Nayak, Nanda, Awasthi, and Kumar (2015) were able to associate multiple private keys with a single public key.

Different applications of multiple private keys were explored [28]. In one scenario all of the private keys were required to decrypt the message. This was done in case a private key become compromised, the messages which have been encrypted are still secure. Another application of this system was to have only one private key to decrypt a message, thus providing alternate keys, should one private key become corrupted or lost.

This study is relevant to the study of post quantum cryptography because it provided a novel application of lattice-based cryptography. Furthermore, Nayak, Nanda, Awasthi, and Kumar (2015) provided a general overview of NTRU cryptography. This paper contained a discussion of both NTRU encryption and decryption. This general overview

is helpful for the reader attempting to understand NTRU encryption.

NTRU operations are actually mathematically simple but are all based on objects in a truncated polynomial ring. This is shown in equation 3.

$$R = \mathbb{Z}[X]/(X^N - 1) \tag{3}$$

All polynomials in the ring have integer coefficients and degree at most N-1. Like all asymmetric algorithms, NTRU requires the generation of a public and private key pair. This process will involve several components, described here:
N - the polynomials in the ring R have degree N-1.
q - the large modulus to which each coefficient is reduced.
p - the small modulus to which each coefficient is reduced.
f - a polynomial which is the private key.
g - a polynomial which is used to generate the public key h from f
h - the public key, also a polynomial
r - the random "blinding" polynomial
d - coefficient

The key generation process begins with two polynomials f and g, with degree at most N-1. The polynomial f ∈ L must satisfy the additional requirement: the inverses modulo q and modulo p. Both f and f_p are the private key. The public key is generated via the formula $h = pf_q * g \pmod q$. The message m is encrypted into the ciphertext e by the formula $e = r * h + m \pmod q$. The ciphertext e is decrypted back to message m by the formula $m = f * e \pmod q$ [29].

3) LWE

Learning with errors with rings (sometimes called ring learning with errors or RLWE) was mentioned briefly previously. RLWE utilizes the learning with errors problem specialized with polynomial rings over a finite field. Learning with errors itself is a machine learning algorithm first proposed by Oded Regev in 2005. In 2018 Regev received the Gödel prize for this work on LWE. The RLWE problem can be reduced to the shortest vector problem (SVP) which is an NP hard problem.

As was mentioned previously, RLWE utilizes polynomials over a finite field. There are variations of this algorithm for key exchange, signature, and encryption. The focus in this paper will be on encryption. While not germane to this current study, it is noteworthy that RLWE is a homomorphic cryptosystem.

At its basis, the Learning With Errors problem involves the difficulty of solving
B = A * s + e
And B are both arrays (i.e. vectors). The person knows A and B, and the value of S becomes the private key.

This is a basic description of the simplest version of the LWE encryption scheme. The mathematics become more complex in various implementations.

4) The Status of Current Asymmetric Cryptography

The focus of this current study is on examining algorithms that have been posited as solutions for post-quantum cryptography. However, as was previously discussed in this paper, some experts believe it may be 10 years or more before practical, usable quantum computing is achieved. Still others believe it may be longer. This does not diminish the significance of this study and similar studies. There are already significant problems with RSA that lead to a need to find a replacement [34] [35] [36] [37].

III. Comparison of Lattice Based Algorithms

The question being addressed in this paper, is which of the three leading lattice-based algorithms discussed appears to be the most secure. Security is determined by a combination of reviewing current cryptanalysis literature for the algorithms in question and combining that data with randomness tests. Ideally a cryptographic primitive produces pseudorandom permutations. The degree of randomness in the output of an algorithm is one indicator of the efficacy of that algorithm. Current studies that focus on one of these algorithms can provide insight into the algorithm of focus. However, what is missing from the literature is a comparison of these algorithms. In this section a summary of the cryptanalysis of these algorithms is provided.

A. Cryptanalysis

The first part of this current study is to examine the literature regarding cryptanalysis studies of the three subject algorithms. Examining those published studies and extrapolating data regarding the algorithms will aid in evaluating the efficacy of the subject algorithms. Then cryptanalysis data from the studies are compared to provide an understanding of the efficacy of these algorithms.

1) GGH

Lee & Hahn [38] demonstrated that partial information of the plaintext can aid in decrypting the GGH algorithm ciphertext. While their method was applied against the highest dimension of GGH being proposed at the time, it also required coupling with Nguyen' attack [39]. The Lee & Han method also required some knowledge of the plaintext; thus, it can be argued that this cryptanalysis of GGH is intriguing, but unlikely to represent real-world cryptanalysis conditions. However, many sources considered GGH unusable after Nguyen's published flaws [40] [41]. Other researchers have shown that with minor modifications of GGH it is resistant to published attacks [42].

de Barros and Schechter [43] suggest enhancements to GGH. They began by describing GGH succinctly as follows "Its main idea is to encode a message into a lattice vector v, add some small perturbation r and generate the ciphertext c= v+r. The norm of the vector r must be sufficiently small, so that v is the lattice vector closest to c" They then describe the most direct way of attacking GGH is to reduce the public key in order to find a basis to apply Babai's algorithm. de Barros and Schechter further state that even if the private key cannot be derived, the message may be retrievable.

de Barro and Schechter then discuss modifications to GGH proposed by Yoshino and Kunihiro in 2012. Their variation depended on increasing the length of the perturbation vector r. This process involves adding a new parameter k to the algorithm. de Barro and Schechter further modify the GGH

system further. They accomplish the modification of GGH by adding additional conditions to the matrix. The details of their modification are not pertinent to this current paper and can be found in their paper. However, the result is relevant to this current study. The result was a variation of GGH must more resistant to cryptanalysis, but also slower in decryption. This tends to indicate that the underlying mathematics of GGH are suitable for cryptographic applications, but that at least the early implementations of GGH were flawed.

Zeroizing attacks have been successful against several variations of GGH. Brakerski et al., described these types of attacks as follows: "Roughly speaking, zeroizing attacks proceed by honestly computing many top-level encoding of zero, then using the prescribed zero-testing procedure to setup and solve a system of multilinear equations in the secret parameters of the scheme. These attacks rely crucially on the linearity of the zero-testing procedure, and so some attempts were made recently to devise alternative zero-testing procedures that are non-linear. " [44]

The data suggests that GGH as it was originally published may be susceptible to particular cryptanalysis attacks. However, the underlying mathematics can provide a basis for further research into modifications that might well be suitable.

2) LWE

Learning With Error's based algorithms have also been subjected to various cryptanalysis studies. Fluhrer [45] showed that key exchange protocols based on ring-LWE are susceptible to attack if the same key share is re-used. This does not indicate a fundamental problem with LWE, but rather a need to avoid key re-use.

Crockett and Peikert went further in their study [46]. They took a broad collection of Ring-LWE approaches and performed detailed analysis. Their study did not reveal any fundamental problems with the ring based LWE algorithms but did establish certain parameters that facilitate strong encryption based on ring based LWE. One such parameter is the quality of the lattice vectors. The authors defined that quality as measured by the Hermite factor. The Hermite factor is defined as follows: for a d-dimensional lattice £ vector v within the lattice £ (i.e. v $\in$ £) has a Hermite factor of:

$$\delta^d \text{ given by } \|\mathbf{v}\| = \delta^d \cdot \mathrm{vol}(\mathcal{L})^{1/d}; \quad (4)$$

The authors also found that block size had a significant impact on the difficulty of breaking the ring based LWE algorithm. Essentially Crockett and Peikert demonstrated that with the proper selection of variables, the ring based LWE algorithms were well suited for cryptographic uses, including post-quantum cryptographic applications. More importantly, Crockett and Peikert established a protocol for evaluating ring based LWE algorithms that can be applied to any such algorithm.

The attacks on LWE algorithms have all been predicated upon some error in the implementation. As an example, the aforementioned Fluhrer cryptanalysis study depended on re-using the same key share. This suggests that LWE can be a secure cryptographic scheme, provided it is implemented carefully

3) NTRU

There have been multiple studies of NTRU algorithms, including NTRU signature schemes [47], [48], [49]. However, all of these are predicated on attacks involving the implementation of NTRU. It should be noted that all cryptographic algorithms are predicated on correct implementation. Incorrect implementation can significantly degrade the performance of any cryptographic algorithm. Thus, the various published cryptanalysis studies of NTRU do not cast any doubt on the efficacy of NTRU when properly applied. This suggests that NTRU can be a secure cryptographic scheme, provided it is implemented carefully.

In addition to the cryptographic attacks that have been attempted on NTRU, the algorithm has also been analyzed via Shor's algorithm. It has been demonstrated that NTRU is not susceptible to Shor's algorithm [50] [51]. This is a significant advantage for any cryptographic primitive, as it was Shor's algorithm that proved quantum algorithms can break current widely used asymmetric algorithms.

B. Randomness tests

In addition to the comparative review of cryptanalysis studies for the lattice-based algorithm, each of the algorithms compared was subjected to randomness tests. Each algorithm was used to encrypt five texts and the resultant ciphertext was subjected to a suite of NIST randomness [52], and the randomness of the ciphertext measured. The text files where random text of sizes from 1 kilobyte to 1 megabyte.

The source code for implementing the algorithms was chosen to be implementations of the algorithms without any alterations. For NTRU cryptographic algorithm, the NTRUEncrypt algorithm code was used and for Learning with Errors the Compact LWE code was used. Both are submissions to the NIST Quantum Cryptography project. No publicly available source code for GGH was available. Each of these were coded using the C++ programming language. Each algorithm was coded following the originally published algorithms with no modifications.

Ideally a cryptographic algorithm should produce a pseudo random output with a high degree of randomness [53], [54], [55], [56]. Three randomness tests from the NIST suite of randomness where used to test to determine the degree to which outputs from a given algorithm achieved a random result. The results of those tests are provided in table 1.

TABLE I. RANDOMNESS TEST RESULTS

Specific Algorithm	Plaintext input	Results
CCG		
	1 kilobyte.	Frequency test results 7.586 Runs test results 2.853 Serial test results 1.256
	100 kilobytes.	Frequency test results 1.951 Runs test results 5.004 Serial test results 1.689
	250 kilobytes.	Frequency test results 2.354 Runs test results 5.993 Serial test results 2.01

	500 kilobytes.	Frequency test results 1.995 Runs test results 1.268 Serial test results 0.778
	1 megabyte.	Frequency test results 1.365 Runs test results 8.691 Serial test results 0.771
NTRU		
	1 kilobyte.	Frequency test results 0.644 Runs test results 1.225 Serial test results 0.354
	100 kilobytes.	Frequency test results 0.020 Runs test results 1.102 Serial test results 0.529
	250 kilobytes.	Frequency test results .132 Runs test results 1.037 Serial test results 0.937
	500 kilobytes.	Frequency test results 0.296 Runs test results 0.129 Serial test results 0.104
	1 megabyte.	Frequency test results 0.039 Runs test results 3.873 Serial test results 0.031
Learning With Error's		
	1 kilobyte.	Frequency test results 8.003 Runs test results 4.258 Serial test results 5.654
	100 kilobytes.	Frequency test results 2.565 Runs test results 5.908 Serial test results 1.985
	250 kilobytes.	Frequency test results 1.035 Runs test results 4.1283 Serial test results 2.368
	500 kilobytes.	Frequency test results 2.958 Runs test results 2.3658 Serial test results 1.759
	1 megabyte.	Frequency test results 2.687 Runs test results 5.755 Serial test results 1.658

The data from the randomness tests was then analyzed using t-test and p-values. There were three hypotheses tested:

1. Ciphertext produced by Learning With Error's is not statistically more random than GGH and NTRU.
2. Ciphertext produced by NTRU is not statistically more random than GGH and Learning With Error's.
3. Ciphertext produced by GGH is not statistically more random than Learning With Error's and NTRU.

TABLE II. INFERENTIAL STATISTICS

Algorithms Compared		t-test	p-value
GGH & NTRU	Frequency	2.454	.019844
	Test	2.30195	.025159
	Runs Test	3.08435	.007509
	Serial Test		
Learning With Error's & GGH	Frequency	-0.2422	.407361
	Test	-0.1943	.425391
	Runs Test	1.74873	.059231
	Serial Test		
Learning With Error's and NTRU	Frequency	2.70334	.013467
	Test	3.33774	.005133
	Runs Test	2.9802	.008798
	Serial Test		

In general, the larger the t value, the greater the evidence is against the null hypothesis value [55]. T-test values are included, however, p values are more informative in accepting or rejecting hypotheses. P values were calculated using Microsoft Excel with a confidence level of .05. A small p-value (typically ≤ 0.05) indicates strong evidence against the null hypothesis, so you reject the null hypothesis. Large p-value (> 0.05) indicates weak evidence against the null hypothesis leading to a failure to reject the null hypothesis.

Based on the p-values hypothesis 1 and 3 are accepted and hypothesis 2 is accepted. The data indicates NTRU produces a stronger pseudorandom permutation than either GGH or LWE. The results of the randomness testing by themselves would be inconclusive. However, they match the data derived from the review of cryptanalysis tests. This indicates that, of the three leading lattice-based algorithms tested, NTRU is the most secure.

IV. CONCLUSIONS

A review of current cryptanalysis literature leads to three conclusions. The first conclusion is that NTRU demonstrates improved security over GGH and LWE-Ring. This is based on the review of cryptanalysis studies, the performance of all three algorithms in testing the randomness of their outputs, and the fact that NTRU is already shown to be resistant to Shor's algorithm.

NTRU attacks have been, like the LWE attacks, predicated on inadequate implementations. NTRU, if properly implemented provides a valid choice for cryptographic solutions. Also, like LWE, NTRU modifications can and should be explored, but the existing NTRU algorithms are adequate. However, the culmination of all the data collected indicates NTRU is a more secure algorithm than GGH or LWE-Ring.

The second conclusion is that GGH algorithms have a sound mathematical foundation, however, many of the implementations have been insecure. Thus, GGH should be considered as a basis for further cryptological research, but current GGH algorithms may not be secure enough. Any research into GGH should be done in light of the existing cryptanalysis attacks. Building on modifications by Yoshino and Kunihiro as well as de Barro and Schechter is a recommended research strategy.

The third conclusion is that LWE algorithms seem to provide adequate security. Current cryptanalysis literature has only shown that poor implementations of LWE can be vulnerable to specific cryptanalysis attacks. This leads to the conclusion that LWE is a valid choice for cryptographic solutions. Certainly, modifications of LWE should also be explored, but current LWE implementations can be used.

Further research with all three of these lattice-based algorithms is indicated. However, any such further study must take into account the existing body of literature on cryptanalysis of lattice-based algorithms. One possible avenue for further research would be expanding the randomness test

to include more of the 15 tests in the NIST suite of tests is indicated. Further examination of the body of literature on cryptanalysis of these algorithms is also indicated.

Other additional studies are suggested from this current study. One such avenue for research would be to apply this same methodology to additional algorithms. This could include additional lattice-based algorithms, or other types of cryptographic algorithms such as multi-variate algorithms.

REFERENCES

[1] A. Johnston. " Shor's algorithm and factoring: don't throw away the odd orders." IACR Cryptology ePrint Archive, 2017, 83-90.

[2] D. Wang, C. Hill, & L. Hollenberg. " Simulations of Shor's algorithm using matrix product states." Quantum Information Processing, 2017 16(7), 176-183.

[3] D. Bernstein, J. Buckman, & E. Dahmen Bernstien "Post-quantum cryptography." New York City, New York: Springer.2017, 314.

[4] E. Crockett "Simply safe lattice cryptography (Doctoral dissertation)." 2017 Retrieved from The Georgia Institute of Technology, Georgia USA.

[5] L. Ducas, V. Lyubashevsky, & T. Brest. "Efficient identity-based encryption over NTRU lattices." In 2014 International Conference on the Theory and Application of Cryptology and Information Security. Melbourne, Australia: Springer.

[6] B. Applebaum "Cryptographic hardness of random local functions." Computational Complexity. 2017, 25(3), 667-722.

[7] J. Hoffstein, J. Pipher, J., & J. H. Silverman "An introduction to mathematical cryptography." 2014 New York City, New York: Springer.

[8] C. Easttom "The RSA Algorithm Explored." International Journal of Innovative Research in Information Security. (IJIRIS). 2017 4(1)

[9] C. Chen, T. "A new and extended fault analysis on RSA." ASIACCS '11 Proceedings of the 6th ACM Symposium on Information 2011, Computer and Communications Security, 466-470. doi:10.1145/1966913.1966980.

[10] M. Hinek & C. Lam " Common modulus attacks on small private exponent RSA and some fast variants (in practice)." Journal of Mathematical Cryptology, 2009 4 (1).

[11] M. Mimoso "NSA's Divorce from ECC Causing Crypto Hand-Wringing." Retrieved from https://threatpost.com/nsas-divorce-from-ecc-causing-crypto-hand-wringing/115150/ August 2018.

[12] A. Mohsen, A. Bahaa-Eldin, & M. Sobh, "Lattice-based cryptography." In Computer Engineering and Systems (ICCES), 2017 12th International Conference. Cairo, Egypt: IEEE.

[13] D. Micciancio "Lattice-based cryptography." In Encyclopedia of Cryptography and Security 2011 (pp. 713-715). Springer, Boston, MA.

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

[15] C. Peikert "A decade of lattice cryptography." Foundations and Trends in Theoretical Computer Science, 2016 10(4), 283-424.

[16] S. Friedberg & A. "Linear algebra." 2014. York City, New York: Pearson.

[17] S. Axler "Linear algebra done right." 2015. Berlin, Germany: Springer.

[18] J. Baik, P. Deift, T. Suidan "Combinatorics and Random Matrix Theory." 2016. Providence, Rhode Island: American Mathematical Society.

[19] D. Lay & S. Ray "Linear algebra and its applications." 2015. New York City, New York: Pearson.

[20] D. Chi, J. Choi, J. San Kim, & T. Kim "Lattice based cryptography for beginners." IACR Cryptology ePrint Archive, 2015, 938-1059.

[21] A. Bogdanov, S. Guo, D. Masny, S. Richelson, & A. Rosen "On the hardness of learning with rounding over small modulus." In 2016 Theory of Cryptography Conference. Beijing, CHina: Springer.

[22] J. Bootle, M. Tibouchi, & K. Xagawa "Cryptanalysis of Compact-LWE." In Cryptographers' Track at the 2018 RSA Conference. San Francisco, CA: Springer. doi: 10.1007/978-3-319-76953-0_5.

[23] E. Crockett "Simply safe lattice cryptography" (Doctoral dissertation). 2017. Retrieved from The Georgia Institute of Technology, Georgia USA.

[24] T. Pöppelmann & T. Güneysu, T. "Towards practical lattice-based public-key encryption on reconfigurable hardware." 2013 International Conference on Selected Areas in Cryptography. British Columbia, Canada: Springer.

[25] X. Lei & X. Liao "NTRU-KE: A Lattice-based Public Key Exchange Protocol." 2013 *IACR Cryptology ePrint Archive*, *2013*, 718.

[26] D. Nayak, A. Nanda, P. Awasthi, & L. Kumar (2015). Multiple private keys with NTRU cryptosystem. IJRCCT, 4(3), 250-255.

[27] J. Hoffstein, J. Pipher, & J. Silverman "NTRU: A ring-based public key cryptosystem." In 1998 International Algorithmic Number Theory Symposium (pp. 267-288). Springer, Berlin, Heidelberg.

[28] R. Monteiro "Post-quantum cryptography: lattice-based cryptography and analysis of NTRU public-key cryptosystem" (Doctoral dissertation). 2016. University of Lisbon, Portugal.

[29] A. Abubakar, S. Jabaka, B. Tijjani, A. Zeki, H. Chiroma, M. Usman, & M. Mahmud "Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: Issues and challenges." Journal of Theoretical & Applied Information Technology, 61(1), 2014.

[30] M. Bunder, A. Nitaj, W. Susilo, & J. Tonien "A generalized attack on RSA type cryptosystems." Theoretical Computer Science, 704, 74-81, 2017.

[31] Y. Yarom, D. Genkin, & N. Heninger "CacheBleed: a timing attack on OpenSSL constant-time RSA." Journal of Cryptographic Engineering, 7(2), 99-112, 2017.

[32] E. Vuicik, D. Šešok, & S. Ramanauskaitė "Efficiency of RSA key factorization by open-source libraries and distributed system architecture." Baltic Journal of Modern Computing, 5(3), 269-274, 2017.

[33] A. Abubakar, S. Jabaka, B. Tijjani, A. Zeki, H. Chiroma, M. Usma, & M. Mahmud "Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: Issues and challenges." Journal of Theoretical & Applied Information Technology, 61(1), 2014.

[34] M. Bunder, A. Nitaj, W. Susilo, & J. Tonien "A generalized attack on RSA type cryptosystems." Theoretical Computer Science, 704, 74-81, 2017

[35] S. Sarkar "Small secret exponent attack on RSA variant with modulus $ $ N= p^ rq $ $ N= p r q." Designs, Codes and Cryptography, 73(2), 383-392, 2014.

[36] Y. Yarom, D. Genkin, & N. Heninger "CacheBleed: a timing attack on OpenSSL constant-time RSA." Journal of Cryptographic Engineering, 7(2), 99-112, 2017.

[37] M. Lee S. & Hahn "Cryptanalysis of the GGH cryptosystem." Mathematics in Computer Science, 3(2), 201-208, 2010.

[38] P. Nguyen. "Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem" from crypto'97. In 2019 Annual International Cryptology Conference (pp. 288-304). Springer, Berlin, Heidelberg.

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

[40] B. Minaud & P. Fouque "Cryptanalysis of the New Multilinear Map over the Integers." *IACR Cryptology ePrint Archive*, *2015*, 941.

[41] C. Gu, Z. Yu, Z. Jing, P. Shi, & J. Qian "Improvement of GGH Multilinear Map." In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on (pp. 407-411). IEEE.

[42] C. de Barros & L. Schechter "GGH may not be dead after all." Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, 3(1), 2015.

[43] Z. Brakerski, C. Gentry, S. Halevi, T. Lepoint, A. Sahai, A., & M. Tibouchi "Cryptanalysis of the Quadratic Zero-Testing of GGH." IACR Cryptology ePrint Archive, 2015, 845.

[44] S. Fluhrer "Cryptanalysis of ring-LWE based key exchange with key share reuse." *IACR Cryptology ePrint Archive*, *2016*, 85.

[45] E. Crockett & C. Peikert "Challenges for Ring-LWE." *IACR Cryptology ePrint Archive*, *2016*, 782.

[46] C. Gentry & M. Szydlo "Cryptanalysis of the revised NTRU signature scheme." In 2002 International Conference on the Theory and Applications of Cryptographic Techniques (pp. 299-320). Springer, Berlin, Heidelberg,

[47] C. Gentry, J. Jonsson, J. Stern & M. Szydlo, M. "Cryptanalysis of the NTRU signature scheme (NSS)" from Eurocrypt 2001. In 2001 International Conference on the Theory and Application of Cryptology and Information Security (pp. 1-20). Springer, Berlin, Heidelberg.

[48] C. Gentry, C. "Key recovery and message attacks on NTRU-composite." In 2001 International Conference on the Theory and Applications of Cryptographic Techniques (pp. 182-194). Springer, Berlin, Heidelberg.

[49] S. Fluhrer "Quantum Cryptanalysis of NTRU." IACR Cryptology ePrint Archive, 2015, 676.

[50] R. Perlner & D. Cooper "Quantum resistant public key cryptography: a survey." In 2009 Proceedings of the 8th Symposium on Identity and Trust on the Internet (pp. 85-93). ACM.

[51] National Institute of Standards Statistical test suite for random and pseudorandom number generators for cryptographic applications NIST 800-22 rev 1a. Washington, DC: U.S. Government Printing Office.

[52] S. Pironio, A. Acín, S. Massar, A. de La Giroday, D. Matsukevich, P. Maunz, P., ... & C. Monroe, C. "Random numbers certified by Bell's theorem." Nature, 464(7291), 1021-1024, 2010.

[53] Simion, E. (2015). The relevance of statistical tests in cryptography. IEEE Security & Privacy, 13(1), 66-70.

[54] K. Tadaki & N. Doi, N. "Cryptography and algorithmic randomness." Theory of Computing Systems, 56(3), 544-580, 2015.

[55] C. Georgescu, A. Petrescu-Nita, E. Simion, & A. Toma "NIST Randomness Tests (in) dependence." IACR Cryptology ePrint Archive, 2017, 336.

[56] R. Peck, C. Olsen, & J. Devore, J. L. "Introduction to statistics and data analysis." Boston, Massachusetts: Cengage Learning, 2015.