Identification of Influential Parameters for NTRU Decryption Failure and Recommendation of Extended Parameter Selection Criteria for Elimination of Decryption Failure

Juliet Nyokabi Gaithuru, Mazleena Salleh, *Member, IAENG,* and Majid Bakhtiari

***Abstract*—NTRU is the leading alternative to ECC and RSA in the post-quantum era. However, it has a probability of decryption failure of 2^{-k} (with k being the security level) according to Philip S. Hirschhorn, Jeffrey Hoffstein, Nick Howgrave-Graham and William Whyte, 2009. This probability was provided for parameters selected using an algorithm which provides security against lattice reduction and MITM attacks, with particular emphasis on parameter size and coefficients of the private key. The recommendations for selection of polynomials in NTRU described by Hoffstein, Jeff Howgrave-Graham, Nick Pipher, Jill Whyte and William in 2010 prescribed that for polynomial f of binary form. In this paper, we re-evaluate the prescribed parameter selection criteria by rigorous testing of different polynomial combinations of f, g, m and φ as well as q for varied security levels. The testing experimentally verifies the influential parameters for NTRU operation whose results are used to propose an extended correlated parameter selection criteria for the private key, which ensures that a randomly selected polynomial f is invertible and that an accurate selection of the minimum size of q required for successful decryption is made.**

***Index Terms*—Cryptography, NTRU, decryption failure, lattices, private key, binary polynomials.**

I. Introduction

Lattice-based cryptosystems are resistant to quantum algorithm attacks [1], [2] thus providing assurance of security in the post-quantum era. The security of information, in terms of integrity and authenticity, is ensured through the use of encryption [3] which involves the application of a series of computations(employing confusion and diffusion attributes [4]) so as to encrypt the data [5] thereby safeguarding it. One such algorithm is the NTRU (Nth Degree Truncated Polynomial Ring) cryptosystem. It is an asymmetric key cryptosystem whose security is based on the difficulty in solving the approximate closest vector problem [6]. It has two varieties: NTRUEncrypt and NTRUSign. It is mostly implemented in the financial services industry and has been standardized by IEEE P1363.1, ANSI X9.98 [7], EESS1v2 [8] and EESS1v3 [9]. It has been projected as the leading contender for replacing ECC and RSA [10] in the post-quantum era because these algorithms are vulnerable to quantum algorithm attacks, specifically Shor's algorithm.

In comparison to ECC and RSA, NTRU has a small footprint of approximately 8kB, is faster and has a smaller key size than RSA [11]. NTRU has been improved progressively since its release in 1998 in terms of recommendation of parameter sets that can withstand various attacks such as the lattice reduction and Meet-in-the-middle(MITM) attacks and the recommendation of parameters that increase the combinational search space so as to enhance security. Research has also been conducted on variants of NTRU, in which the polynomial ring of integers is replaced with the Eisenstein integers [11], Gaussian ring of integers, integer matrices [12] as well as quarternion algebra which has a non-commutative structure thus making it more resistant to lattice-based attacks [13]. Despite NTRU's superior performance and security, it has one drawback in that, there is a probability of decryption failure which makes it impossible to recover the plain text from a validly created cipher text.

This study seeks to answer the following questions: does any randomly selected NTRU parameter from the range of all possible polynomial combinations of f,g,φ and m result in successful NTRU operation in terms of key generation, encryption and decryption and if not, which parameter(s) is most influential and what is the criteria for selecting this parameter(s), in addition to the published criteria, so as to ensure successful operation. In order to answer these questions, this study discusses an experimental study of the most influential parameters for NTRU operation and uses the derived nature of the NTRU parameters to propose an extended parameter selection criteria to ensure invertibility of a randomly selected private key and propose a correlated criteria for parameter selection. This extended criteria will help to further narrow down the range of acceptable parameters and thus reduce the number of errors occurring due to erroneous selection of non-invertible polynomial f and also providing a range for selection of the corresponding public parameter q that will further ensure there is a high probability of successful message decryption.

The paper is organized as follows: In Section II we introduce the basic structure and parameters of the NTRU public key cryptosystem. This is followed by a description of the previously recommended NTRU parameters in Section III. Section IV describes the methodology used in conduction this study along with a discussion of the test parameters used for experimentation. This is accompanied by a discussion of the test results obtained in the study. The Section VI describes the analysis conducted on the private key polynomial f as this was identified as a key determinant of decryption failure. An evaluation of the relationship between parameters is described along with the observations and conclusions drawn by progressive variation of parameters. Then

Manuscript received October 17, 2016; revised August 08, 2017.

J. Gaithuru is with the Faculty of Computing, Universiti Teknologi Malaysia, 81310, Skudai, Malaysia e-mail: julietgaithuru@yahoo.com.

M. Salleh and M. Bakhtiari are with Universiti Teknologi Malaysia.

an extended private key selection criteria is recommended in Section VII. Finally, a conclusion of the study is provided in Section VIII.

II. NTRU

NTRU is based on the polynomial convolution ring $R = \frac{Z[X]}{(X^N-1)}$ which implies that all computations are modulus $(X^N - 1)$ and that there are convolution multiplications. All polynomials in the ring have integer coefficients and a maximum degree of $(N-1)$. In the ring R, addition of two polynomials refers to the pairwise addition of coefficients of the same degree while multiplication is referred to as convolution multiplication. The parameters used in the NTRU cryptosystem are:

1) The parameter size N
2) A large modulus q
3) A small modulus p
4) Polynomial f which should be invertible modulus p and modulus q
5) A polynomial g which does not require to be invertible
6) A blinding value φ
7) Plain text message expressed as the polynomial m.

The parameter selection criteria for the NTRU parameters listed above is as described in the subsequent section as published in [14], [15].

A. Degree parameter N

The degree parameter N is a positive integer and specifies that the ring R consists of truncated polynomials of degree $(N-1)$ with integer coefficients $a = a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$. It determines the maximum degree $(N-1)$ for the polynomials f and g.

B. Parameters p and q

q is the large modulus while p is the small modulus, both of which should be relatively prime to each other. The polynomials in NTRU are either of binary, ternary or product form, depending on whether p is selected as 2, 3 or $2+x$ respectively. Binary polynomials allow for a small parameter q to be used [16]. Ternary polynomials provide a balance between security and efficiency in that there is an increased number of combinations and the size of q can be kept as small as possible while ensuring a low probability of decryption failure [14]. The use of product form polynomials originated from the need to provide efficiency [14] given that it eliminates the need to calculate the polynomial inverses. The corresponding values of q are: when $p = 2$ then q is selected as a prime number and when $p = 3$ or for $p = 2+x$ then q is selected as an integral power of 2 (that is 2^m where m is an integer).

C. Polynomials f and g

The small polynomials f and g are secret polynomials which are selected by uniform sampling from a set of binary or ternary polynomials whereby a predetermined number of -1 , 1 and 0 coefficients have been set [16]. For binary polynomials, the polynomial f has d_f of the coefficients equal to 1 while $(N - d_f)$ coefficients are 0. For ternary polynomials, the polynomial f has d_f of the coefficients equal to 1 while $(d_f - 1)$ coefficients are -1 and the rest are 0 coefficients. For ternary polynomials, $p = 3$, the polynomial g has d_g coefficients equal to 1, d_g coefficients equal to -1 and the rest of the coefficients are 0.

The slight difference between the polynomials f and g is because f has to be invertible while g does not need to be invertible. There is a greater probability of f having an inverse provided that the GCD of $f(1)$ with p and with q is 1 and the sum of the coefficients of f is 1 upon evaluation of $f(1)$.

D. L_f, L_g, L_m and L_φ

L_f and L_g represent private key spaces which are given by a set of small polynomials from which the private keys will be selected. The polynomials f and g are randomly generated in L_f and L_g respectively. L_m represents the plain text space, which is given by a set of polynomials which represent the encryptable message. L_φ represents a set of polynomials from which the blinding value will be selected [15].

E. Blinding value φ

φ is a blinding value (which is temporary), used to obscure or hide the message which is different for each transaction. It has d_φ coefficients equal to 1, d_φ coefficients equal to -1 and the rest of the coefficients are 0. The blinding polynomial is generated from the padded message using the standard polynomial convolution method or by the use of the optimized polynomial convolution method [9].

F. Plaintext message m

The message m is expressed in the form of a polynomial whose coefficients are modulo p so that its coefficients lie between $\frac{-p}{2}$ and $\frac{p}{2}$.

If a user desires a k-bit security level, then $2k$ bits of a message can be transported at a time. For example, for 112-bit security, then 224 bits of a message can be transported at a time thus the message has to be split into $2k$ bits blocks. The random padding length l should be such that $l \geq k$.

The value of N is set such that it is the first prime number that is greater than $3k$ [15], [17], for instance if desired security level k is 80-bits, then N can be selected as 243. If a message padding scheme is used, such as the SVES-3 padding scheme which utilizes 8 bits to encode the length of the transported message, the length of N should be at least $3k+8$ [18]. A smaller value of N implies that the bandwidth utilized will be lower and operations will be faster.

G. NTRU Operation

NTRU operation begins with the establishment of the integers N, p, q and the polynomials f, g, φ and m. The public and private keys are then generated by obtaining the multiplicative inverse of f mod p and f mod q such that:

$$F_q * f \equiv 1(mod\, q) \tag{1}$$

$$F_p * f \equiv 1(mod\, p) \tag{2}$$

The private key is given by f, F_p and the public key h is obtained by computing:

$$h = p\,F_q * g(mod\,q) \tag{3}$$

The message m is encrypted using the public key, h by computing:

$$e = \varphi * h + m(mod\,q) \tag{4}$$

The ciphertext is decrypted using the private key by computing:

$$a \equiv f * e(mod\,q) \tag{5}$$

After which adjustment is done by ensuring that the coefficients of a are in the range of $\frac{q}{2}$ and $\frac{-q}{2}$. This is then followed by retrieving the decrypted message by computing

$$C = F_p * a(mod\,p) \tag{6}$$

[21] provides a simplified implementation of NTRU in the form of mini-NTRU. Decryption is made possible because the polynomials p, φ, g and m are chosen to have small values in the polynomial convolution ring R thus ensuring the polynomial $p\varphi g + fm$ has a high probability of having width b (which represents $p\varphi g + fm$) less than q. In other words, the coefficients of these terms are selected in a way that ensures that they have an absolute value that does not exceed $\frac{q}{2}$ [22]. Therefore, the proof of decryption is as follows:

Since the ciphertext is obtained by computing $e \equiv \varphi * h + m(mod\,q)$ then

$$a \equiv f * e(mod\,q) = f * (\varphi * h + m) mod\,q \tag{7}$$

$$= (f * \varphi * h + f * m) mod\,q \tag{8}$$

Since $h \equiv p\,F_q * g(mod\,q)$ then

$$a\ = [(f * \varphi * (p * F_q * g)) + (f * m)]\,mod q \tag{9}$$

Since $F_q * f \equiv 1(mod\,q)$ then

$$a = [(p * \varphi * g) + (f * m)] mod\,q \tag{10}$$

This implies that since $C = F_p * a(mod\,p)$ then

$$C = F_p * a(mod\,p) = p * (F_p * \varphi * g) + F_p * f * m \tag{11}$$

$$= 0 + 1 * m = m\,mod\,p \tag{12}$$

The product $p * (F_p * \varphi * g)$ is a small value close to zero. In the real sense, it is observed that this product is a multiple of p thus reduction $mod\,p$ results in a zero. Thus retrieving the value of the plain text m.

In the case where the width of $(p * \varphi * g + f * m)$ is greater than or equal to q, then a gap failure occurs but if the range of of $(p * \varphi * g + f * m)$ is less than q but reduced into the wrong interval, then this is referred to as a wrap failure. A wrap failure can be adjusted by reducing a to the range $[A, A + q - 1]$ in which $A \neq \frac{-q}{2}$ and the mod q equality from the equation $a \equiv p * \varphi * g\,mod\,q$ is an exact equality in $Z[X]$ (meaning that the product is not greater than $\frac{q}{2}$ or less than $\frac{-q}{2}$) [23].

On the other hand, when a gap failure occurs, it will result in decryption failure since the range of a is exceeded thus resulting in the inability to correctly recover $(p*\varphi*g+f*m)$. The use of the range $[A.A + q - 1]$ serves as a partial solution to the problem of decryption failures. This process of increasing the chances of a correct decryption is called re-centering [24], [25].

III. Previous Recommended Parameters

Since the invention of NTRU in 1998, several parameter sets have been recommended and revised for binary, ternary and product-form polynomials. The Table I shows the some of the previously recommended parameter sets for $p = 2$ and $p = 3$, on which we base our study.

The parameter sets ees251ep4 and ees251ep5 use product form polynomial $(f = 1 + pF)$ because it results in an inverse of 1 therefore eliminating the need for calculating the inverse [8]. ees251ep4 stands for efficient embedded security encryption parameters with degree 251 set 4.

The parameter sets NTRU167.2, NTRU263.2 and NTRU503.3 were recommended following the establishment of the probability of wrap failure and gap failure in NTRU. These parameter sets were meant to provide a balance between security and decryption levels [20].

IV. Methodology

The methodology used in this study involved carrying out tests on NTRU parameters in order to answer the following questions: does any randomly selected NTRU parameter from the range of all possible polynomial combinations of f,g,φ and m result in successful NTRU operation in terms of key generation, encryption and decryption and if not, which parameter(s) is most influential and what is the criteria for selecting this parameter(s), in addition to the published criteria, so as to ensure successful operation. This was done by evaluating how varying any of the NTRU parameters affects its successful key generation, encryption and subsequently successful message decryption. This was followed by an analysis of the test results to identify the most influential parameters. The most influential parameters were then used to conduct further tests to identify a selection criteria that is bound to ensure a higher probability of successful operation and subsequently successful message decryption.

Previous research works on NTRU do not discuss the methodology used in deriving the recommended parameter sets and parameter selection criteria, including publications

TABLE I: Previously Recommended NTRU parameters for $p = 2$ and $p = 3$

Parameter set	Security level (k)	N	p	q	d_f	d_g	d_φ	Reference
ees251ep4	80	251	2	239	72	72	72	[8], [19]
ees251ep5	80	251	2	239	72	72	72	
NTRU167.2	Low	167	2	127	45	35	18	[20]
NTRU263.2	Moderate	263	2	127	35	35	22	
NTRU503.3	High	503	2	253	100	100	65	
NTRU 167	49	167	3	128	61	20	18	[6]
ees401ep1	112	401	3	2048	113	113	113	[7]

on variants of NTRU. This study delves into a description of the methodology used to arrive at an extended parameter selection criteria which further narrows down the margin for erroneous parameter selection in NTRU which will affect its successful operation and subsequent key generation, encryption and decryption.

A. Evaluating Effect of NTRU Parameter Variation

An experimental analysis of the NTRU parameters was done, beginning with low security levels to identify the most influential parameters in the occurrence of decryption failure. The results of the analysis at low security levels were then used to obtain the proportions for estimating sample sizes to be used for testing higher security levels. The testing began by varying each of the parameters f, g, φ and m one at a time for possible values of polynomials for $N = 11$. The proportions obtained for successful key generation, encryption and decryption from the analysis done at low security levels ($N = 11$ and $N = 53$) were used as input in determining appropriate sample sizes for testing higher security levels, including the previously proposed recommended NTRU parameters.

B. Uniform Sampling without Replacement

The sample sizes were obtained by using uniform random sampling where the samples were selected by using a random number generator without replacement. First, an initial sample size n_0 was obtained by computing:

$$n_0 = \frac{z^2 \times p\,(1-p)}{e^2} \tag{13}$$

where z is the critical value for the confidence level c, p is the proportion or distribution and e is the sampling error. Since n_0 is at least 5% of the population N and sampling is without replacement, the sample size is more accurately estimated by reducing the error in the previous computation of n_0 by applying the Finite Population Correction Factor (FPC). This was done by computing [26]–[29]:

$$n = \frac{n_0 \cdot N}{n_0 + (N-1)} \tag{14}$$

Uniform random sampling was used, with a 99% confidence interval and 5% margin of error. The proportion, p used is based on the results obtained from the test results for low security levels. The uniform sampling method is used in this study because it is the documented sampling method used to select secret polynomials f and g [14], [16], [18]. The method of sampling from a discrete Gaussian distribution as proposed by [30] in 2014 can also be used for selecting f and g. However, Gaussian sampling results in a large public key size of 378353 for $N = 256$, 1511821 for $N = 512$ for instance, in comparison to public key $q = 2048$ for uniform sampling [16]. For this reason, uniform sampling method was used in this study as opposed to sampling from a discrete Gaussian distribution.

C. Test Parameters

Tests were conducted for binary polynomials at $N = 11$, $N = 53$ and $N = 251$ for 3-bit, 16-bit and 80-bit security levels respectively. Testing at 32-bit security levels and beyond took a significant amount of time on the available processing resources owing to the sequential nature of the task execution for the tests in this study. Therefore, the obtained results for low security levels were used as input for proportions used for sampling to be used for high-security level testing. The test parameters used in this study are as shown in the Table II. The base test parameters used to conduct this study are appended in Appendix A. These base test parameters were selected following the existing parameter selection criteria.

The initial sample size tested for $N = 11$ was 2^8 out of the 2^{11} possible combinations for each of the polynomials f, g, φ and m. The value of parameter q was varied by testing the range of prime numbers starting from 1 to 203. Once proportions were obtained from the initial tests on $N = 11$, the sample sizes were computed after which the sample size of $N = 11$, eesTest1 was adjusted to the computed sample size (501 combinations) and more polynomial combinations tested as illustrated in the Table II. The proportions obtained from the initial tests were 0.4922:0.5078 which stand for the ratio of successful key generation to unsuccessful key generation. The sample sizes for eesTest1, eesTest2 and ees251ep4 were obtained by computation using the Equation 13 and Equation 14. The outcome of the tests is provided in Section V.

D. Testing Environment and Sequence

The testing sequence for this study was conducted as follows:

1) Input test parameters N, p, f, g, r, m for eesTest1.
2) Generate a range of prime numbers from 1 to a random large prime, for instance 700.
3) Vary q in the test parameter set using the generated primes in step 2.
4) Generate all possible polynomial combinations with maximum degree $N - 1$ (that is 2^N polynomial combinations).
5) Vary g by replacing it with the polynomial combinations generated in step 4, one at a time, and record the result.
6) Repeat step 5 for f, r and m.
7) In the case of non-invertible polynomial f, discard the polynomial and move onto the next polynomial in the sequence.
    a) If f is invertible and has successful message decryption, record the result.
    b) If f is invertible but has decryption failure, repeat steps 3 and 4 and record the result.
    c) If f is invertible but still has decryption failure after repeating steps 3 to 6, vary q by repeating step 3 and record the result. This is done to evaluate if the variation of parameters g, r and m could switch the result from 'decryption failure' to 'successful decryption'.
8) Repeat steps 1 to 7 for eesTest2, ees251ep4, NTRU167 and ees401ep1.

The results of the testing were used to identify the influential parameters which were then varied for $N = 53$ and the recommended parameter sets in the EESS1v2 [8]

TABLE II: Test parameters for binary and ternary NTRU polynomials

Parameter set	k	N	p	q	d_f	d_g	d_φ	d_m	Population	Sample size	Actual Sample Tested
eesTest1	3	11	2	37	4	5	4	6	2^{11}	501	1000
eesTest2	16	53	2	67	7	27	40	35	2^{53}	663	1000
eesTest3	3	11	3	32	4	5	4	6	3^{11}	501	1000
eesTest4	16	53	3	64	7	27	40	35	3^{53}	663	1000
ees251ep4 [8], [19]	80	251	2	239	72	72	72	35	3^{251}	663	1000
NTRU 167 [6]	49	167	3	128	61	20	18	70	3^{167}	663	1000
ees401ep1 [7]	112	401	3	2048	113	113	113	70	3^{401}	663	1000

for $N = 251$ for binary polynomials as well as product-form polynomials.

The testing was carried out on a Windows 8.1 64-bit operating system with Intel core i5 processor and 4GB RAM computer running the Magma computational algebra system. The Magma computational algebra system was used following precedence of other research studies conducted in the same environment, namely; the study conducted on speed records for NTRU when run on a graphical processing unit (GPU) by Hermans in 2010 [31] and in a cryptanalysis study on a revised NTRUSign scheme conducted by Geiler and Smart [32].

A discussion of the observations made from the test results for binary polynomials at various security levels is provided in the subsequent section.

V. Results-Identifying the Influential NTRU Parameters

The results of tests for the parameter sets with binary, product- form and ternary coefficients are described in the subsequent section.

A. Binary and Product-Form Polynomials

The results of varying NTRU binary and product form parameters is depicted in Table IV. The Table III shows the parameter being varied one at a time, in the left-most column, while all other parameters are kept constant. This is followed by the next three columns showing percentage variability for test parameters sets for 3-bit, 16-bit and 80-bit security respectively. The percentage variability stands for the number of polynomials which showed unsuccessful key generation. This occurs as a result of the selection of non-invertible polynomials of f which results in the key generation algorithm going into an infinite loop of trying to find the inverse and when no inverse is found then no key is generated.

TABLE III: Test Results for binary NTRU polynomials

Varying parameter	Percentage Variability		
	eesTest1	eesTest2	ees251ep4
q	Successful for large primes of q		
f	50.8982	50.3771	48.1146
product form ($f = 1 + pF$)	0	0	0
g	0	0	0
φ	0	0	0

The variation of polynomial q revealed that decryption was successful for large values of the prime q. Prime values greater than 29 resulted in successful decryption for eesTest1, while prime values greater than 101 resulted in successful decryption for eesTest2. This drew attention to the existence of a relationship between the value of prime q and the selected polynomial f.

The variation of polynomial g resulted in 100% successful decryption regardless of the binary polynomial of g chosen from the range of possible combinations of polynomials at the corresponding security levels.The variation of polynomial φ also resulted in 100% successful decryption regardless of the random polynomial of φ chosen.

The variation of polynomial f resulted in 50.8982% of the tested polynomial combinations having no multiplicative inverse mod p and mod q thus resulting in no key being generated and therefore no encryption and decryption for $N = 11$. For $N = 53$, 50.3771% of the polynomial combinations had no multiplicative inverse while 48.1146% had no multiplicative inverse for $N = 251$.

It was also observed from the results that the variation of the product form polynomial f also resulted in 100% successful key generation, and subsequent encryption and decryption regardless of the random polynomial of f chosen. This means that choosing the product form f means there is assurance of finding a multiplicative inverse mod p and mod q. These results point to the significance of the polynomial f chosen, on whether key generation is possible and subsequently on whether encryption and decryption is possible. This confirms the assertion that decryption failures are predominantly key-dependent [14].

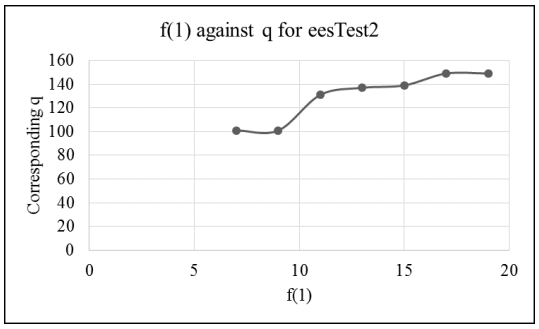
B. Ternary Polynomials

The results of varying NTRU ternary form parameters is depicted in Table IV.

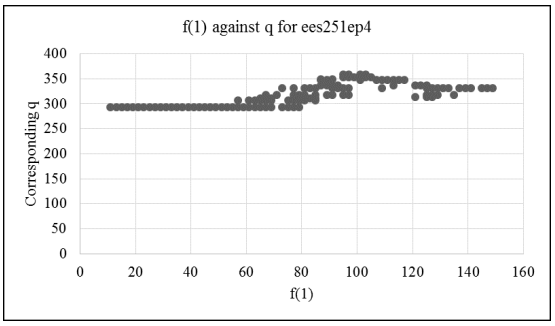
TABLE IV: Test Results for ternary NTRU polynomials

Varying parameter	Percentage Variability			
	eesTest3	eesTest4	NTRU 167	ees401ep1
q	Successful for large powers of 2 (large q)			
f	27.06	26.36	27.06	26.34
g	98.491	98.63	98.491	97.51
φ	97.577	97.010	98.491	97.872

For ternary polynomials, the variation of f, g, φ resulted in no key being generated in 72.94%, 1.509% and 2.423% of the instances for eesTest3. A similar general trend was also observed in test parameters eesTest3, eesTest4, NTRU 167 and ees401ep1. The variation of q revealed that there was



(a) Graph of $f(1)$ against q for eesTest2



(b) Graph of $f(1)$ against q for ees251ep4

Fig. 1: Evaluation of the relationship between $f(1)$ and q for NTRU binary polynomials

successful decryption for large powers of 2. The variation of f revealed that 72.94% of the polynomials tested for 8-bit ternary combinations have no multiplicative inverse $mod\, p$ and $mod\, q$ thus resulting in no key generation.

Further examination of the invertible polynomials of f revealed that the number of 1's were either one more than the number of -1 coefficients or one less than the number of 1 coefficients. This leads to the conclusion that in order to have a ternary polynomial of f that has an inverse $mod\, p$ and $mod\, q$ then the value of $f(1)$ when the sum of coefficients is computed should either be 1 or -1. This increases the range of possible polynomial combinations of f, since the previous parameter selection criteria prescribes that f should be selected such that $f(1) = 1$.

VI. Analysis of the relationship between f and q

This study revealed that some polynomials of f do not have a multiplicative inverse. Therefore, when these polynomials go through the process of finding a multiplicative inverse (which can be computed using the Extended Euclidean algorithm), the process results in an infinite loop which does not terminate and neither does it print out the inverse F_p and F_q thus no private key is generated thus resulting in an error.

Further evaluation of the invertible polynomials shows that $f(1)$ when the sum of coefficients was computed, is an odd number for all the invertible polynomials of f. In addition, it was observed that the value of $f(1)$ had a relationship with the size of q. For $N = 11$, the polynomial combinations that were invertible and had successful decryption had $q = 37$ and $f(1) = 3, 5$ and 7. For the higher security levels, some of the polynomial combinations with an odd value of $f(1)$ did not have successful decryption (due to the size of q upon evaluation) while others were successful for $N = 53$, $q = 37$ and $N = 251$, $q = 239$. The size of q was then varied upwards to a larger prime till decryption was successful and the corresponding values recorded.

In addition, it was observed that all the invertible polynomials of f have $GCD(f(1), p) = 1$ and $GCD(f(1), q) = 1$. This is in line with the recommended condition in [14] in the determination of whether a set of values have a multiplicative inverse such that $(a * b) mod\, n \equiv 1$.

A graphical representation of the relationship between $f(1)$ and q for eesTest2 is shown in the Figure 1a. The test results for eesTest2 show a correlation coefficient of 0.93109468 between the values of $f(1)$ and q and a corresponding equation of regression line was derived given by:

$$y = 72 + 4.429x \tag{15}$$

The results for ees251ep4 for binary form of f show a correlation coefficient of 0.7004 between the values of $f(1)$ and q and a corresponding equation of regression line was derived given by:

$$y = 281.586 + 0.442x \tag{16}$$

The graphical representation of this relationship is shown in the Figure 1b.

The NTRU parameter selection criteria recommended by [14], [15] for polynomial f ensured that there was a high probability of the polynomial having a multiplicative inverse therefore making it possible to generate a private key and eventually encrypt and decrypt messages correctly. Based on the results of this study, it has been established that the criteria set does not conclusively cover all possibilities for the selection of private keys that would result in successful decryption of messages encrypted using the NTRU cryptosystem.

A. Identification of the Selection Criteria for q for Elimination of Decryption Failure

The study proceeded to establish an additional selection criteria which will provide for the selection of the minimum size of q required for successful message decryption, as opposed to just selecting an upper limit. The existing recommended criteria on binary polynomials in [14], [22] is that in order to avoid decryption failure, the size of q should be large enough whereby c should be selected such that $3c + 1 > \frac{q}{2}$. The value of c is given by $c = \frac{q-2}{2p}$.

In order to establish the criteria that will ensure the selection of the minimum size of q required for successful decryption, an evaluation of the relationship between the previous criteria ($3c + 1 > q/2$) and the actual minimum size of q that resulted in successful message decryption was carried out in this study. The observed results are as illustrated in the Figure 2.

The Figure 2 points to the existence of a linear relationship between the previously published recommended criteria and the findings of this study for the minimum required size of q for successful message decryption. Therefore, this is beneficial in being able to accurately predict an exact size of q which will result in successful decryption as opposed to just selecting an upper limit.

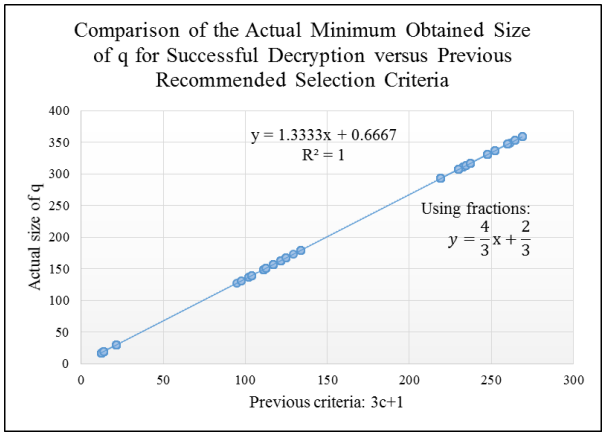


Fig. 2: Comparison of the previous selection criteria for size of q against the new recommended criteria and actual minimum size of q for successful decryption.

Expressing the relationship between the previous criteria $\frac{q}{2} = 3c + 1$ which translates to $q = 6c + 2$ and the observed sizes of q given by $y = 1.3333x + 0.6667$ in terms of fractions results in

$$y = \frac{4}{3}x + \frac{2}{3} \tag{17}$$

Replacing x with $3c + 1$ and y with q results in

$$q = \frac{4}{3}(3c + 1) + \frac{2}{3}$$
$$q = \frac{12c + 4}{3} + \frac{2}{3} = \frac{12c + 6}{3}$$
$$q = 4c + 2$$
$$\frac{q}{2} = 2c + 1$$

Therefore, this implies that in order to ensure successful message decryption at varied security levels, the size of public parameter q should be selected to be an appropriately large value which satisfies the condition that

$$q = 2c + 1 \text{ or } \frac{q}{2} = 2c + 1 \tag{18}$$

for binary polynomials.

In comparison to the existing published criteria, it is the observation of this study that the size of q required for successful message decryption is smaller than the previously published criteria, which gives an upper limit. A comparison of public parameter size q selected using the previous criteria compared to the newly recommended criteria as well as the actual size of q that results in successful decryption is as shown in the Figure 3.

It can be observed from the Figure 3 that the actual minimum size of q required for successful message decryption matches with the predicted size of q using the new recommended criteria $q = 4c + 2$. The predicted size of q using the previous criteria is much larger than the actual minimum size of q required for successful message decryption. The recommended criteria in this study results in a 33.050% reduction in the predicted size of q required for successful message decryption. This study proves that selecting the size of q such that $q = 4c + 2$ will result in a predicted size of q which exactly matches the actual minimum size of q required for successful message decryption.

This study has shown that the previous criteria set an upper limit for the size of q which would result in successful decryption. In the next section, we outline an extended parameter selection criteria which ensures successful message decryption.

VII. Recommended Extended Parameter Selection Criteria for the Private Key and Public Parameter q

The observations made in this study as described in the previous sections and the conclusions drawn led to the recommendation of an extended NTRU parameter selection criteria. The emphasis of this study is on the private key polynomial f and public parameter q (which directly affects the public key size) since it has been proven in Section V above, that these are the most influential parameters for successful NTRU operation. The polynomial f shows variability of 50.8982% in comparison to the 0% variability of polynomials m, g and φ.

The recommended general parameter selection algorithm which is a combination of previous work [14], [16], [22] and the findings of this study is as follows: i

1) Take $p = 2$.
2) Set N to be the first prime greater than $3k + 1$.
3) Select q to be a prime integer. Select q such that $q = 2c + 1$ where $c = \frac{q-2}{2p}$ in order to ensure successful decryption.
4) Select binary polynomials g,φ and m with d_g, d_φ, d_m number of 1's respectively. The number of coefficients d_g, d_φ, d_m lie in the range $1 \leq d_g, d_\varphi, d_m \geq N$.
5) Select binary polynomial f with d_f number of 1's where d_f is an odd integer so as to ensure it has a multiplicative inverse mod p and mod q. $GCD(f(1), p)$ and $GCD(f(1), q)$ should be 1.
6) Select ternary polynomial f with d_f number of 1's and $d_f - 1$ number of -1's (that is $f(1) = 1$) or $d_f - 1$ number of 1's and d_f number of -1's (that is $f(1) = -1$) so as to ensure it has a multiplicative inverse mod p and mod q

This extended parameter selection criteria ensures that the chosen polynomial of f is invertible modulus p and modulus q and that the exact size of q required for successful

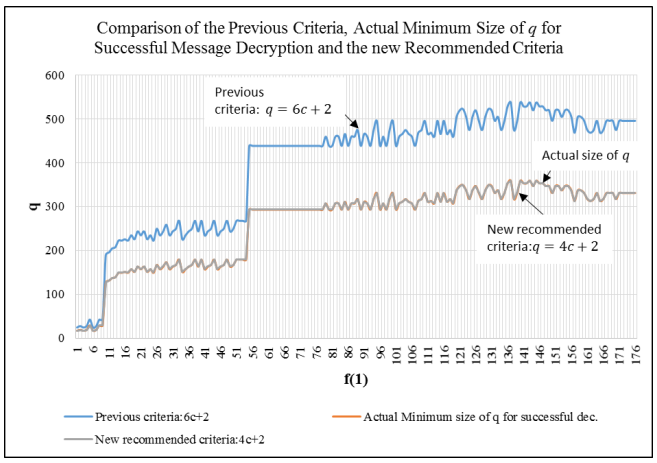


Fig. 3: Comparison of the previous criteria, actual minimum size of q for successful message decryption and the new recommended criteria.

decryption is selected so as to ensure there is no decryption failure. A tabular comparison of the extended parameter selection criteria in comparison to the existing selection criteria is depicted in Table V.

The Table VI provides a list of recommended parameter sets which ensure no decryption failure.

These parameters are derived from experimentation conducted in this study which follows the extended recommended parameter selection criteria proposed in this study. We leave to future work the evaluation of these recommended parameter sets against practical lattice reduction attacks. This will provide confirmation of these security levels in practical application where the parameters are prone to attacks.

VIII. Conclusion

The study shows that in order to ensure successful decryption and increase the range of polynomials of private key f which result in successful decryption, some additional parameter selection criteria should be included. The private key, for binary polynomials, should be selected such that in addition to having $GCD(f(1), p) = 1$ and $GCD(f(1), q) = 1$, the number of 1's in f (d_f) should be an odd integer which lies in the range $1 < d_f \leq N$, where N is the parameter size of the integer ring R. For ternary polynomials, the private key polynomial f should be selected such that the number of 1's in f are one more than -1's or the number of 1's are one less than the number of -1's ($f(1) = 1$ or -1) The use of this criteria ensures that the polynomial of f selected is invertible modulus p and modulus q and also increases the range of invertible polynomials of f.

In order to reduce the probability of decryption failure, the study revealed that it is imperative that parameters f and q are selected with consideration. This study revealed the existence of a high correlation between the size of $f(1)$ and q. The value of q should be selected to be appropriately large so as to ensure successful decryption.

This study provides a parameter selection criteria for the value of q which ensures no decryption failure at varied security levels. This can be achieved by selecting q such that $\frac{q}{2} = 2c + 1$. This extended parameter selection criteria helps to ensure no decryption failure in the NTRU cryptosystem thus providing a greater assurance of security.

The use of this recommended parameter selection criteria helps to accurately predict the public parameter q that ensures successful message decryption. This eliminates the need to select an upper limit of q, which provides efficiency in terms of memory requirements and thus subsequently reducing public key size. Therefore, there is memory efficiency and provision of assurance that the selected size of q will ensure successful message decryption.

Future work could be carried out to ascertain whether the recommended size of q selected using the criteria recommended in this study provides the same security level when the parameters are subjected to practical lattice reduction attacks.

Appendix
Base Test Parameters

$$N = 11$$
$$p = 2$$
$$q = 37$$
$$f = 1 + x^4 + x^7 + x^8 + x^9 \quad d_f = 5$$
$$g = 1 + x + x^4 + x^6 + x^{10} \quad d_g = 5$$
$$m = x + x^3 + x^5 + x^8 + x^9 + x^{10} \quad d_m = 6$$
$$\varphi = 1 + x^3 + x^4 + x^8 \quad d_\varphi = 4$$

TABLE V: Comparison of the previous and recommended extended parameter selection criteria

Coefficients	**previous selection criteria**	**proposed revised criteria**
Coefficients in binary f, d_f	-	odd integer
Coefficients in ternary f, d_f	f(1)=1	f(1)=1 or -1
$GCD(f(1), p)$	1	1
$GCD(f(1), q)$	1	1
Size of q	$(3c + 1) > \frac{q}{2}$	$2c + 1 = \frac{q}{2}$

TABLE VI: Recommended parameter sets

Parameter set	Security level (k)	N	p	q	d_f	d_g	d_φ	d_m
ees251epJ04	80	251	3	256	71	72	72	35
ees251epJ03	80	251	2	331	150	72	72	35
ees251epJ02	80	251	2	331	73	72	72	35
ees251epJ01	80	251	2	317	71	72	72	35
ees16epJ02	80	251	2	239	72	72	72	35
ees16epJ01	16	53	3	63	7	27	40	35
ees16epJ03	16	167	2	127	45	35	18	35
ees11epJ03	3	11	3	32	4	5	4	6
ees11epJ02	3	11	2	29	3	3	5	6
ees11epJ01	3	11	2	17	5	4	4	6

$$N = 53$$
$$p = 2$$
$$q = 67$$
$$f = x^{39} + x^{38} + x^{37} + x^{36} + x^{35} + x^{34} + x^{33}$$
$$+x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25}$$
$$+x^{24} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7$$
$$+x^6 + x^5 + x^4 + x$$
$$d_f = 27$$
$$g = x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21}$$
$$+x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12}$$
$$+x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x$$
$$d_g = 27$$
$$m = x^{37} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{29}$$
$$+x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} +$$
$$x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} +$$
$$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x$$
$$d_m = 35$$
$$\varphi = x^{42} + x^{41} + x^{40} + x^{39} + x^{38} + x^{37} + x^{36} + x^{35}$$
$$+x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26}$$
$$+x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17}$$
$$+x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8$$
$$+x^7 + x^6 + x^5 + x^4 + x$$
$$d_\varphi = 40$$

$$N = 251$$
$$p = 2$$
$$q = 239$$
$$f = x^{71} + x^{70} + x^{69} + x^{68} + x^{67} + x^{66} + x^{65} + x^{64}$$
$$+x^{63} + x^{62} + x^{61} + x^{60} + x^{59} + x^{58} + x^{57} + x^{56} + x^{55}$$
$$+x^{54} + x^{53} + x^{52} + x^{51} + x^{50} + x^{49} + x^{48} + x^{47} + x^{46}$$
$$+x^{45} + x^{44} + x^{43} + x^{42} + x^{41} + x^{40} + x^{39} + x^{38} + x^{37}$$
$$+x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{29} + x^{28}$$
$$+x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19}$$
$$+x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10}$$
$$+x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$d_f = 73$$
$$g = x^{71} + x^{70} + x^{69} + x^{68} + x^{67} + x^{66} + x^{65} + x^{64}$$
$$+x^{63} + x^{62} + x^{61} + x^{60} + x^{59} + x^{58} + x^{57} + x^{56} + x^{55}$$
$$+x^{54} + x^{53} + x^{52} + x^{51} + x^{50} + x^{49} + x^{48} + x^{47} + x^{46}$$
$$+x^{45} + x^{44} + x^{43} + x^{42} + x^{41} + x^{40} + x^{39} + x^{38} + x^{37}$$
$$+x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{29} + x^{28}$$
$$+x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19}$$
$$+x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10}$$
$$+x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$d_g = 72$$
$$m = x^{37} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30}$$
$$+x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21}$$
$$+x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12}$$
$$+x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x$$
$$d_m = 35$$
$$\varphi = x^{139} + x^{138} + x^{137} + x^{136} + x^{135} + x^{134} + x^{133}$$
$$+x^{132} + x^{131} + x^{130} + x^{129} + x^{128} + x^{127} + x^{126} + x^{125}$$
$$+x^{124} + x^{123} + x^{122} + x^{121} + x^{120} + x^{119} + x^{118} + x^{117}$$
$$+x^{116} + x^{115} + x^{114} + x^{113} + x^{112} + x^{111} + x^{110} + x^{109}$$
$$+x^{108} + x^{107} + x^{106} + x^{105} + x^{104} + x^{103} + x^{102} + x^{101}$$
$$+x^{100} + x^{99} + x^{98} + x^{97} + x^{96} + x^{95} + x^{94} + x^{93} + x^{92}$$
$$+x^{91} + x^{90} + x^{89} + x^{88} + x^{87} + x^{86} + x^{85} + x^{84} + x^{83}$$
$$+x^{82} + x^{81} + x^{80} + x^{79} + x^{78} + x^{77} + x^{76} + x^{75} + x^{74}$$
$$+x^{73} + x^{72} + x^{71} + x^{70} + x^{69} + x^{67}$$
$$d_\varphi = 72$$

REFERENCES

[1] R. Lai, H. Cheung, and S. Chow, "Trapdoors for ideal lattices with applications," in *Information Security and Cryptology*, ser. Lecture Notes in Computer Science, D. Lin, M. Yung, and J. Zhou, Eds. Springer International Publishing, 2015, vol. 8957, pp. 239–256. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-16745-9-14

[2] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. Bernstein, J. Buchmann, and E. Dahmen, Eds. Springer Berlin Heidelberg, 2009, pp. 147–191. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-88702-7-5

[3] N. Kishore and B. Kapoor, "Attacks on and advances in secure hash algorithms," *IAENG International Journal of Computer Science*, vol. 43, no. 3, pp. 326–335, 2016.

[4] R. E. Boriga, A. C. Dăscălescu, and A. V. Diaconu, "A new fast image encryption scheme based on 2d chaotic maps," *IAENG International Journal of Computer Science*, vol. 41, no. 4, pp. 249–258, 2014.

[5] H. Miyajima, N. Shigei, H. Miyajima, Y. Miyanishi, S. Kitagami, and N. Shiratori, "New privacy preserving back propagation learning for secure multiparty computation." *IAENG International Journal of Computer Science*, vol. 43, no. 3, pp. 270–276, 2016.

[6] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," in *Algorithmic number theory*. Springer, 1998, pp. 267–288.

[7] "Ieee standard specification for public key cryptographic techniques based on hard problems over lattices," *IEEE Std 1363.1-2008*, pp. C1–69, March 2009.

[8] EESS, "Efficient embedded security standards (eess)," 2003.

[9] W. Whyte, "Efficient embedded security standards (eess) 1: Implementation aspects of ntruencrypt," 2015.

[10] B.-Y. Yang, C.-M. Cheng, B.-R. Chen, and J.-M. Chen, "Implementing minimized multivariate pkc on low-resource embedded systems," in *Security in Pervasive Computing*, ser. Lecture Notes in Computer Science, J. Clark, R. Paige, F. Polack, and P. Brooke, Eds. Springer Berlin Heidelberg, 2006, vol. 3934, pp. 73–88. [Online]. Available: http://dx.doi.org/10.1007/11734666-7

[11] K. Jarvis and M. Nevins, "Etru: Ntru over the eisenstein integers," *Designs, Codes and Cryptography*, vol. 74, no. 1, pp. 219–242, 2015.

[12] M. Coglianese and B.-M. Goi, "Matru: A new ntru-based cryptosystem," in *Progress in Cryptology-INDOCRYPT 2005*. Springer, 2005, pp. 232–243.

[13] E. Malekian, A. Zakerolhosseini, and A. Mashatan, "Qtru: quaternionic version of the ntru public-key cryptosystems," *The ISC International Journal of Information Security*, vol. 3, no. 1, 2015.

[14] P. S. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, and W. Whyte, "Choosing ntruencrypt parameters in light of combined lattice reduction and mitm approaches," in *Applied Cryptography and Network Security*, ser. Lecture Notes in Computer Science, M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, Eds. Springer Berlin Heidelberg, 2009, vol. 5536, pp. 437–455. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-01957-9-27

[15] J. Hoffstein, N. Howgrave-Graham, J. Pipher, and W. Whyte, "Practical lattice-based cryptography: Ntruencrypt and ntrusign," in *The LLL Algorithm*, ser. Information Security and Cryptography, P. Q. Nguyen and B. Valle, Eds. Springer Berlin Heidelberg, 2010,

pp. 349–390. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-02295-1-11
[16] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for ntruencrypt," 2015. [Online]. Available: http://eprint.iacr.org/2015/708.pdf
[17] A. S. B. S. K. Ranjeet Ranjan, "Improvement of ntru cryptosystem," 2012.
[18] N. Howgrave-Graham, J. Silverman, and W. Whyte, "Choosing parameter sets for ntruencrypt with naep and sves-3," in *Topics in Cryptology CT-RSA 2005*, ser. Lecture Notes in Computer Science, A. Menezes, Ed. Springer Berlin Heidelberg, 2005, vol. 3376, pp. 118–135. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-30574-3-10
[19] J. Hoffstein, J. H. Silverman, and W. Whyte, "Ntru cryptosystems technical report# 012, version 2: Estimated breaking times for ntru lattices," *NTRU Cryptosystems, Inc*, 2003.
[20] J. H. Silverman, "Wraps, gaps, and lattice constants," *NTRU Report*, vol. 11, 2001.
[21] J. N. Gaithuru, M. Salleh, and I. Mohamad, "Mini n-th degree truncated polynomial ring (mini-ntru): A simplified implementation using binary polynomials," in *2016 IEEE 8th International Conference on Engineering Education (ICEED)*, Dec 2016, pp. 270–275.
[22] J. P. Jeffrey Hoffstein and W. Whyte, *More Efficient parameters, keys and encoding for hybrid-resistant NTRUEncrypt and NTRUSign*, 2009.
[23] J. Hoffstein, Silverman, and W. Whyte, "Ntru cryptosystems technical report# 018, version 1: Estimating decryption failures of ntruencrypt," *NTRU Cryptosystems, Inc*, 2003.
[24] N. Howgrave-Graham, P. Nguyen, D. Pointcheval, J. Proos, J. Silverman, A. Singer, and W. Whyte, "The impact of decryption failures on the security of ntru encryption," in *Advances in Cryptology - CRYPTO 2003*, ser. Lecture Notes in Computer Science, D. Boneh, Ed. Springer Berlin Heidelberg, 2003, vol. 2729, pp. 226–246. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-45146-4-14
[25] J. Scholten and F. Vercauteren, "An introduction to elliptic and hyperelliptic curve cryptography and the ntru cryptosystem," 2003.
[26] L. University. (2006) Sample size. [Online]. Available: http://library.lincoln.ac.nz/global/library/learning/maths and stats/qmet 103/sample-size.pdf
[27] M. Desu, *Sample size methodology*. Elsevier, 2012.
[28] P. J. Lavrakas, *Encyclopedia of survey research methods*. Sage Publications, 2008.
[29] P. S. Levy and S. Lemeshow, *Sampling of populations: methods and applications*. John Wiley and Sons, 2013.
[30] D. Cabarcas, P. Weiden, and J. Buchmann, "On the efficiency of provably secure ntru," in *Post-Quantum Cryptography*. Springer, 2014, pp. 22–39.
[31] J. Hermans, F. Vercauteren, and B. Preneel, "Speed records for ntru," in *Topics in Cryptology - CT-RSA 2010*, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed. Springer Berlin Heidelberg, 2010, vol. 5985, pp. 73–88. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-11925-5-6
[32] C. Gentry and M. Szydlo, "Cryptanalysis of the revised ntru signature scheme," in *Advances in Cryptology EUROCRYPT 2002*, ser. Lecture Notes in Computer Science, L. Knudsen, Ed. Springer Berlin Heidelberg, 2002, vol. 2332, pp. 299–320. [Online]. Available: http://dx.doi.org/10.1007/3-540-46035-7-20

Juliet N. Gaithuru was born in Thika, Kenya on the 15th of November 1985. This author attained a BSc. in Computer Information Systems from Kenya Methodist University in 2011. The author also holds a Master of Computer Science in Information Security from Universiti Teknologi Malaysia, 2013, where she carried out research on the S-Box in the Advanced Encryption Standard (AES) Algorithm. The author is currently pursuing a PhD degree in computer science specializing in the field of information security at Universiti Teknologi Malaysia. Her research interests are in the field of symmetric and asymmetric cryptography with particular interest in post-quantum cryptography.

Mazleena Salleh is an Associate Professor at the Faculty of Computing, Universiti Teknologi Malaysia. The author holds a PhD in Computer Science from Universiti Teknologi Malaysia. The author holds an MSc in Electrical Engineering from Virginia Polytechnic and State University in USA. The author attained a BSc in Electrical Engineering from University of Southern California, USA as well as a Diploma in Electrical Engineering from Universiti Teknologi Malaysia.

Majid M. Bakhtiari is a Senior Lecturer in the Faculty of Computing,Univesity Technology Malaysia (UTM). He holds a BSc in electronics, MSc in information security and PhD in computer science (cryptography). His research interests center around the area of cryptography and cryptanalysis.

He has over 30 years experience in the field of cryptography and cryptanalysis. He has designed, educated and installed three generations of data crypto-systems in the Ministry of Foreign Affairs of Isl. Rep. of Iran from 1985 to 2006. He has experience in algorithm breaking in the field of voice encryption and data encryption and is an expert in designing security systems for large organizations . His current research work concentrates on cryptography, cryptanalysis, security in cloud computing, steganography and watermarking.