ENHANCEMENT OF NTH DEGREE TRUNCATED POLYNOMIAL RING FOR IMPROVING DECRYPTION FAILURE

JULIET NYOKABI GAITHURU

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

FEBRUARY 2019

To my loving parents, Samuel Gaithuru and Esther Wairimu, brothers Robert Njeru and Robin Muigai for their unwavering love, support, prayers and words of encouragement.

ACKNOWLEDGEMENT

I thank God for bestowing upon me the strength, perseverance and determination to conduct this research. I would also like to express my special appreciation and gratitude to my core supervisor **Associate Prof. Dr. Mazleena Salleh** whose invaluable advice, insightful criticisms, and patient encouragement aided the writing of this thesis. The high standards set by her and the regular sessions that we had contributed greatly towards the remarkable quality of this work and helped to mould me into a better person. I would also like to appreciate the tremendous contribution of Dr. Majid Bakhtiari, Associate Prof. Dr. Ismail Mohamad and my co-supervisor Associate Prof. Dr. Nor Muhainiah in ironing out the mathematical concepts which were an essential part of his research study.

I am also grateful to Dr. William Whyte from Security Innovation, USA for his brilliant comments and suggestions in this research study. His ideas greatly contributed towards pointing me in the right direction during the course of this research.

I would also like to thank the staff at the Faculty of Computing for the facilities and opportunity to pursue this study. I thank the Malaysia Ministry of Higher Education for their financial support in the course of my research studies and without whom this accomplishment would not have been possible.

Special thanks go to my family for their love, unfettered support, patience, encouragement and whose prayers for me are what has sustained me thus far. Words cannot express how grateful I am to my mother and father for all of the sacrifices that they have made on my behalf.

ABSTRACT

N^{th} Degree Truncated Polynomial (NTRU) is a public key cryptosystem constructed in a polynomial ring with integer coefficients that is based on three main key integer parameters N, p and q. However, decryption failure of validly created ciphertexts may occur, at which point the encrypted message is discarded and the sender re-encrypts the messages using different parameters. This may leak information about the private key of the recipient thereby making it vulnerable to attacks. Due to this, the study focused on reduction or elimination of decryption failure through several solutions. The study began with an experimental evaluation of NTRU parameters and existing selection criteria by uniform quartile random sampling without replacement in order to identify the most influential parameter(s) for decryption failure, and thus developed a predictive parameter selection model with the aid of machine learning. Subsequently, an improved NTRU modular inverse algorithm was developed following an exploratory evaluation of alternative modular inverse algorithms in terms of probability of invertibility, speed of inversion and computational complexity. Finally, several alternative algebraic ring structures were evaluated in terms of simplification of multiplication, modular inversion, one-way function properties and security analysis for NTRU variant formulation. The study showed that the private key f and large prime q were the most influential parameters in decryption failure. Firstly, an extended parameter selection criteria specifying that the private polynomial f should be selected such that $f(1) = \pm 1$, number of 1 coefficients should be one more or one less than -1 coefficients, which doubles the range of invertible polynomials thereby doubling the presented key space. Furthermore, selecting $q \geq 2.5754 \times f(1) + 83.9038$ gave an appropriate size q with the least size required for successful message decryption, resulting in a 33.05% reduction of the public key size. Secondly, an improved modular inverse algorithm was developed using the least squares method of finding a generalized inverse applying homomorphism of ring R and an $(N \times N)$ circulant matrix with integer coefficients. This ensured inversion for selected polynomial f except for binary polynomial having all 1 coefficients. This resulted in an increase of 48% to 51% whereby the number of invertible polynomials enlarged the key space and consequently improved security. Finally, an NTRU variant based on the ring of integers, Integer TRUncated ring (ITRU) was developed to address the invertiblity problem of key generation which causes decryption failure. Based on this analysis, inversion is guaranteed, and less pre-computation is required. Besides, a lower key generation computational complexity of $O(N^2)$ compared to $O(N^2(log^2p + log^2q))$ for NTRU as well as a public key size that is 38% to 53% smaller, and a message expansion factor that is 2 to15 times larger than that of NTRU enhanced message security were obtained.

ABSTRAK

Darjah N Polinomial Terpangkas (NTRU) adalah kriptosistem kekunci awam yang dibina menggunakan polinomial gegelang dengan koefisien integer berdasarkan tiga parameter utama interger N, p dan q. Walau bagaimanapun, kegagalan penyahsulitan teks yang dijana mungkin berlaku di mana teks sifer tersebut perlu diabaikan dan penghantaran semula teks dilakukan menggunakan nilai parameter yang berbeza. Proses ini mungkin membawa kepada kebocoran kekunci peribadi yang menjadikannya terdedah kepada serangan. Di sebabkan ini, kajian ini memberi tumpuan kepada pengurangan atau penghapusan kegagalan penyahsulitan melalui beberapa penyelesaian. Kajian ini bermula dengan melaksanakan eksperimen untuk mengenal pasti parameter NTRU dan kriteria pemilihan yang sedia ada dengan melakukan persampelan rawak kuartil seragam tanpa penggantian untuk mengenal pasti parameter yang paling berpengaruh untuk menilai semula dan dengan demikian membangunkan satu model pemilihan parameter ramalan dengan mengaplikasikan pembelajaran mesin. Seterusnya, algoritma songsang modular NTRU yang lebih baik telah dibangunkan sebagai penilaian alternatif bagi algoritma songsang modular dari segi kebarangkalian boleh songsangan, kelajuan songsangan dan kekompleksan pengiraan. Akhirnya beberapa struktur gegelang algebra alternatif telah dinilai dari segi pendaraban mudah, songsangan modular, sifat berfungsi sehala dan keselamatan analisis untuk pembentukan variasi NTRU. Kajian menunjukkan bahawa kekunci persendirian f dan nilai perdana besar q adalah parameter yang paling berpengaruh dalam kegagalan penyahsulitan. Pertama, kriteria pemilihan parameter lanjutan menyatakan bahawa polinomial persendirian f dipilih sebagai $f(1) = \pm 1$, di mana bilangan koefisien 1 mesti lebih satu atau kurang satu dari koefisien -1 yang menggandakan julat songsangan polinomial dan ruang kekunci. Selain itu, pemilihan $q \geq 2.5754 \times f(1) + 83.9038$ memberikan saiz q yang bersesuaian, dengan saiz terkecil yang diperlukan untuk penyahsulitan mesej berjaya, menghasilkan pengurangan saiz kekunci awam sebanyak 33.05%. Kedua, algoritma songsang modular yang lebih baik telah dibangunkan dengan menggunakan kaedah kuasa dua terkecil untuk mencari songsangan umum dengan mengaplikasi gegelang homomorfisma bagi gegelang R dan matriks beredar $(N \times N)$ dengan koefisien integer. Kaedah ini memastikan adanya songsangan polinomial f kecuali apabila polinomial binari mempunyai kesemua koefisien 1. Ia telah menghasilkan peningkatan sebanyak 48% ke 51%, di mana bilangan polinominal meluaskan ruang kekunci serta meningkatkan keselamatan. Akhirnya, variasi NTRU berdasarkan gegelang integer, gegelang integer terpangkas (ITRU) dicadangkan untuk menyelesaikan masalah songsangan penjanaan kekunci yang menyebabkan kegagalan penyahsulitan. Berdasarkan analisis ini, nilai penyongsangan dijamin, dengan pra pengkomputeran yang rendah. Selain itu, kekompleksan pengiraan penjanaan kekunci yang rendah daripada $O(N^2)$ berbanding $O(N^2(log^2 p + log^2 q))$ untuk NTRU, saiz kekunci awam 38% hingga 53% lebih kecil dan faktor pengembangan mesej 2 hingga 15 kali lebih besar daripada NTRU yang mana dapat meningkatkan keselamatan mesej.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ASCII	-	American Standard Code for Information Interchange
appr-CVP	-	Approximate closest vector problem
BLISS	-	Bimodal Lattice Signature Scheme
CVP	-	Closest vector problem
DLP	-	Discrete logarithm problem
EESS	-	Efficient Embedded Security Standard
ECC	-	Elliptic Curve Cyptosystems
GCD	-	Greatest Common Divisor
IEEE	-	Institute of Electrical and Electronics Engineers
LWE	-	Learning with Errors
LCM	-	Least Common Multiple
LLL	-	Lenstra, Lenstra, and Lovász
NTRU	-	N^{th} Degree TRUncated Polynomial Ring
NTRUEncrypt	-	NTRU Encryption algorithm
NTRU-KE	-	NTRU Key Exchange protocol
NTRUSign	-	NTRU Signature scheme
RSA	-	Rivest, Shamir and Adleman
SVP	-	Shortest vector problem

LIST OF SYMBOLS

X_j	-	A coefficient of $(r * g + f * m)$
f_i	-	Coefficients of f
$Cov(X, Y)$	-	Covariance of two random variables
$erf(x)$	-	Complementary error function
$f * g$	-	Convolution multiplication of f and g
F	-	Circulant matrix of dimension $(N \times N)$ derived form f
N	-	Degree parameter or parameter size
$\|F\|$	-	Determinant of F
$f \times g$	-	Direct or cartesian product
$erfc(x)$	-	Error functions
$E(X)$	-	Expected value of a random variable X
$\in$	-	Element of
x	-	Indeterminate in a polynomial expression
∞	-	Infinity
R	-	Integer Ring
F^{-1}	-	Inverse matrix of F
$\acute{m}$	-	ITRU decimal representation of the message
$\acute{C}$	-	ITRU decrypted message
$\acute{a}$	-	ITRU intermediate decryption parameter
$\acute{q}$	-	ITRU large modulus
$\acute{f}$	-	ITRU private integer for private key generation
$\acute{g}$	-	ITRU private random integer for public key generation
$\acute{r}$	-	ITRU private random integer for obscuring the message
K_{pr}	-	ITRU private key pair ($\acute{f}$,$F_{\acute{p}}$)
K_{pb}	-	ITRU public key parameter $\acute{h}$
$\acute{p}$	-	ITRU small modulus

S_{key}	-	Key security
$\hat{x}$	-	Least squares solution of x
$S_{message}$	-	Message security
F_q	-	Modular inverse of $f\, mod\, q$
C	-	NTRU decrypted message
m	-	NTRU decimal representation of the message
a	-	NTRU intermediate decryption parameter
q	-	NTRU large modulus
f	-	NTRU private integer for private key generation
F_p	-	NTRU private key, modular inverse of $f\, mod\, p$
g	-	NTRU private random integer for public key generation
r	-	NTRU private random integer for obscuring the message
p	-	NTRU small modulus
$\#$	-	Number of
d_f	-	Number of the 1 coefficients in f
d_g	-	Number of the 1 coefficients in g
d_r	-	Number of the 1 coefficients in r
L_f	-	Private key spaces from which f is selected
L_g	-	Private key spaces from which g is selected
φ	-	Obscuring polynomial
L_r	-	Polynomial space from which blinding value is selected
P_{dec}	-	Probability of decryption failure
$R[x]$	-	Set of all polynomials in x over R
σ^2	-	Variance
$Var(X)$	-	Variance of a random variable X

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

The volume of online transactions has grown tremendously with the advent of the internet era; which poses a challenge in terms of maintaining the security of these large volumes of data. This makes cryptography a critical element of modern-day computer systems. Cryptography is a process that makes information indecipherable to unauthorized people thereby safeguarding the information for the authorized users (Patil *et al.*, 2016).

Presently, the most popular public key algorithms are RSA (Rivest, Shamir and Adleman) and Elliptic Curve Cyptosystems (ECC) (Sameer and Gazi, 2011), whose security is based on the difficulty in solving the discrete logarithm problem and the difficulty in factoring large primes respectively. Despite the advent of many new public key algorithms, RSA continues to have the highest popularity of implementation at 43% (Malhotra and Singh, 2013). Presently, longer key sizes are required to ensure security (at a key size of 4096 bits) which comes at the cost of slow performance in devices with limited memory and processing power, thereby necessitating the search for alternative public key algorithms. Both the integer factorization problem and discrete logarithm problems can be solved in an exponentially lower time when run on quantum mechanical systems in comparison to running them on classical computers (Nguyen, 2014).

Research by Shor (1994) demonstrated the importance of quantum computing on cryptography through the demonstration of quantum algorithms that could efficiently solve the discrete logarithm problem and factorization problems. This goes to show that the introduction of quantum computers would render widely used public key cryptosystems insecure. During the 2013 Blackhat Conference, researchers declared a possible impending 'cryptopolyse' with the world clamouring to find an alternative to the most popular encryption algorithms worldwide once quantum computers are introduced (Adams, 2013).

The N^{th} Degree Truncated Polynomial Ring (NTRU) public key cryptosystem is one such alternative, whose security is based on the difficulty in solving the closest vector problem thereby making it resistant to quantum algorithm attacks owing to its lattice structure. NTRU has faster encryption and decryption speeds coupled with a smaller key size compared to other practical cryptosystems. These properties make NTRU well suited for implementation in payment systems, secure messaging, mobile electronic commerce, vehicular systems, remote backup solutions and cloud data centres (Nguyen, 2014). NTRU is considered to be one of the strong candidates for post quantum cryptography which will safeguard information security and privacy in the post quantum era (Wong *et al.*, 2018).

In comparison to the more commonly used ECC and RSA asymmetric cryptosystems, the NTRU cryptosystem is significantly faster in terms of key generation, encryption, decryption (Nguyen, 2014). The NTRU encryption and decryption operations are roughly two orders of magnitude faster than ECC at comparable security levels. Furthermore, the NTRU keys are an order of magnitude larger than ECC key (Karu and Loikkanen, 2001). NTRU is a fast and low cost cryptosystem by virtue of its computation with small coefficient in the convolution product of polynomials (Alsaidi and Yassein, 2016).

Overall, NTRU stands out from the rest due to its resistance to quantum computing algorithms, which makes its security outstanding and future forward. NTRU is also well suited for implementation in embedded platforms which have limited resources, owing to its low power consumption and fast encryption speed (Wong *et al.*, 2018). It is currently implemented in the financial services industry (Fuller, 2011), in the Philips NXP's ARM7 LPC2000 and LPC3000 microcontrollers [1] (EETimes, 2008; Philips, 2015) as well as in the Cyph surveillance-free chat software (Lester, 2015). This research study specifically focuses on the NTRU public key cryptosystem.

[1] NXP Semiconductors and NTRU step up microcontroller security, Electronics World UK, http://www.electronicsworld.co.uk/news/archive/950-950.

1.2 Problem Background

The N^{th} Degree Truncate Polynomial (NTRU) cryptosystem was developed due to the need for a faster public key cryptosystem based on complex mathematical problems other than integer factoring and the discrete logarithm problem (Whyte and Hoffstein, 2011). NTRU is a proprietary algorithm which was invented by Hoffstein *et al.* (1998), patented by NTRU Cryptosystems Inc. and later acquired in 2009 by Security Innovations, a leading application security solutions provider (Kamat and Patel, 2010). Since then, it has been standardized as IEEE Std 1363.1-2008 and ASC X9.98 (Whyte *et al.*, 2008; Whyte and Hoffstein, 2011). In 2013 Security Innovation made the patent free to use in software licensed under the GPL free software licenses (Schanck, 2015).

This scheme is based on lattices and combines mixing and reduction modulo two prime numbers for the encryption process and uses unmixing for the decryption process, which uses the probability theory (Karu and Loikkanen, 2001). Its security is based on the use of polynomial mixing as well as the independence of the reduction modulo operation on the prime integers p and q. Security is also assured by the fact that it is difficult to find very short vectors in most of the lattices (Hoffstein *et al.*, 1998). The lattice structure in NTRU enables it to withstand quantum computing algorithm attacks thus is described as being a quantum-resistant cryptosystem (Jarvis and Nevins, 2013; Whyte and Hoffstein, 2011).

The four crucial problems pertaining to NTRU addressed in this study are described in the subsequent sections namely, the presence of decryption failure in NTRU, limited range of NTRU parameter sets, the difficulty in determining whether a polynomial is invetible and NTRU variant formulation. Countering these problems will foster security of information encrypted using the NTRU algorithm, which is a pertinent issue particularly once quantum computers are introduced, particularly since previous studies show that quantum algorithms can solve the integer factorization and discrete logarithm problems which are the security basis of the most popularly implemented algorithms presently.

1.2.1 Decryption Failure

Recent developments in quantum computing have created interest in post-quantum cryptography research thereby motivating NIST to organize a post-quantum cryptography standardization process, with the goal of standardizing one or more quantum-resistant public-key cryptographic primitives. NIST accepted submissions from various fields within post-quantum cryptography; lattice-based, code-based and multivariate cryptography. Research shows that numerous proposed key encapsulation mechanisms have a small probability of decryption failure for public key algorithms. This applies for majority of the schemes based on lattices, codes or primes. The probability of such failure varies with most of the failure probabilities lying around 2^{-128}. As this failure is dependent on the secret key, it might leak secret information to an adversary. However, as suggested by the wide range of failure probabilities in the NIST submissions, the implications of failures are still not well understood (D'Anvers *et al.*, 2018).

Given the trend towards quantum computing systems (Meyers, 2015), resistance to quantum algorithms is a fundamental property for cryptography algorithms which positions NTRU as the leading alternative for ECC and RSA in the post-quantum era. However, there is the possibility for the occurrence of decryption failure in NTRU. These decryption failures occur with a small probability over a range of random messages. This flaw can be exploited by an attacker who is able to decipher which messages induce failure thereby launch a successful cryptanalysis. The attacker uses this knowledge of the messages inducing decryption failure to extract knowledge about the private key. Thereby, optimal parameter selection in NTRUEncrypt is vital to upholding the cryptosystem's security (Hoffstein *et al.*, 2009).

However, as is the case with DES which were reported as being insecure thereby justifying the proposal of 3DES in a former NIST Challenge and AES which is reported as being broken at low rounds, these insecurities were highlighted in research findings but were not showcased in industrial implementations. The same case applies to NTRU which has been shown to have cases of decryption failure in previous related research work but no citations have been made pertaining to failure in its industrial implementation.

During the decryption process, there is possibility for the occurrence of either of these two types of failure; wrap failure and gap failure. When a wrap failure occurs, it can be adjusted but when a gap failure occurs, it is impossible to recover the original encrypted plaintext, thereby resulting in a decryption failure. Wrap failures occur more frequently in comparison to gap failures, thus 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 (Howgrave-Graham *et al.*, 2003a; Scholten and Vercauteren, 2003).

An attacker with access to timing information can be able to detect when a re-centering has been done thereby leaking information approximately once every million decryptions and even more often if some pre-computation has been done. For instance, for $N = 251$ a wrap failure will take place once in every 2^{21} messages while a gap failure will take place once in every 2^{43} messages (Howgrave-Graham *et al.*, 2003a).

Some countermeasures were proposed to overcome this weakness including: adding some check bits to the message block (Hoffstein and Silverman, 1998), use of a check-errors/re-encrypt protocol (Silverman, 2001; Yu *et al.*, 2005), use of a centering algorithm (Silverman and Whyte, 2003; Yu *et al.*, 2005),a compensating algorithm (Yu *et al.*, 2005) and the use of recommended parameters (Hoffstein *et al.*, 2010a; Hirschhorn *et al.*, 2009; Hoffstein *et al.*, 2015a; Security, 2015b). However, the use of centering algorithms and check-errors re-encrypt protocol were deemed to be inefficient leading to the development of a compensating algorithm (Yu *et al.*, 2005). The use of recommended parameters, which is the most recent countermeasure, provides a decryption failure of 2^{-k} with k being the security level in bits (Hirschhorn *et al.*, 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.

Howgrave-Graham *et al.* (2003b) made the assertion that decryption failure is largely key dependent. This is supported by initial findings in this study which show that during the key generation process whereby the randomly selected private polynomial is required to be invertible, in the event that a non-invertible private polynomial is selected, it goes into an inifinte loop of trying to find an inverse. This subsequently results in unsuccessful key generation, unsuccessful message encryption and consequently unsuccessful decryption. At this point, the random polynomial is discarded, an alternative one is selected and the process of finding an inverse is repeated. Decryption failure occurs when the adjustment or centering method fails (Hoffstein *et al.*, 2003b). The encryption process is probabilistic thus decryption errors can occur for some sets of parameters (Stehlé and Steinfeld, 2011). The guarantee of successful decryption means there is less re-generation of parameters and subsequently reduced likelihood of attacks. This calls attention to the possible of a relationship between decryption failure in NTRU and key generation, which is explored at length in this study.

1.2.2 Limited Range of NTRU Family of Parameters

The family of NTRU parameters provided in (Hirschhorn *et al.*, 2009) define a fixed value of $q = 2048$, on the basis that a smaller q would reduce the bandwidth and public key-size used in the cryptosystem. The authors go on to state that the inclusion of additional parameters would require that more lattice experiments be conducted at lower values of q while ensuring at the same time, that the decryption failure probability is still small enough.

The NTRU family of parameters published in previous works consists of parameter sets for binary variants of NTRU (Hoffstein *et al.*, 2003c; IEEE, 2003b) and ternary variants of NTRU (IEEE, 2009) with the most recent recommended parameter sets being for both product and non-product form of the private key polynomial f (Hoffstein *et al.*, 2015a; Security, 2015b). This existing family of NTRU parameters prescribe a fixed value of $q = 2048$. This serves as an indicator of the avenue for further research into expansion of the NTRU family of parameters for optimal security and performance. Enlargement of the NTRU family of parameters will enlarge the polynomial search space and subsequently enhance the security of the algorithm in the event of an attack.

1.2.3 Difficulty in Determining Whether a Polynomial is Invertible

The NTRU public key cryptosystem entails key generation by the computation of two modular polynomial inverses. However, previous studies point out the difficulty in determining whether a polynomial is invertible (Luo and Lin, 2011). To overcome this difficulty, Nayak *et al.* (2010) proposed a matrix solution to solve the problem. The study presented an approach involving the creation of one public key and two private keys. The authors proposed key generation using a non-commutative ring (matrix ring of polynomials) on condition that the determinant is one or negative one. However, the proposed solution resulted in a small selection range thereby making the cryptosystem more vulnerable to various attacks (Luo and Lin, 2011).

This was then improved by Luo and Lin (2011), who conducted a study which presented a new approach of finding the inverse modulo q with the selection of matrices with non-zero determinants. Given that there are many matrices with non-zero determinants in accordance with their approach, it was shown to be superior compared to the original matrix NTRU cryptosystem solution by (Nayak *et al.*, 2010) in terms of security. The improved solution was based on the concept that the inclusion of new conditions for key selection leads to an enlarged domain compared to previous studies and also improves the security against attacks. The approach was free of the restriction in the use of matrices with a zero determinant which imposes a restriction on the selection domain thereby providing the possibility of easily hacking the two private keys in the matrix NTRU. The approach used Gram Schmidt orthogonalization to find the orthogonal (perpendicular) basis which was then used in generating the inverse (Luo and Lin, 2011). The security of the approach against lattice attacks and its comparison with other NTRU variants still remains an open question for exploration.

Other previous studies that look into the NTRU inverse algorithm include the study by Banks and Shparlinski (2002), who presented a variant of NTRU using non-invertible polynomials. Zhao and Su (2011) presented an NTRU inverse algorithm which makes use of matrices in finding the modular polynomial inverse using the naïve method of matrix inversion. The proposed algorithm proved to be inefficient in terms of utilization of computational resources and thereby processing time. Moreover, a subsequent study by Wahab and Jaber (2015) presented a variant of NTRU using Chebyshev polynomials for the key generation process. This was motivated by the chaotic nature of Chebyshev polynomials. However, the study by Wahab and Jaber (2015) only applied the concept of Chebyshev polynomials in generating the polynomial coefficients of the private polynomial, while the process of finding an inverse remained unaffected, proceeding as in the classical NTRU. Therefore, the work by Wahab and Jaber (2015) does not have any effect on the chances of finding an inverse during key generation.

Despite efforts made by previous works to modify the key generation process by using matrices, limitations in finding an inverse are still present owing to the use of naïve matrix inversion which is computational resource intensive and which does not conclusively tackle the problem of predicting whether a polynomial is invertible and improving the probability of invertibility.

1.2.4 NTRU Variant Formulation

NTRU operates considerably faster than ECC and RSA (Coglianese and Goi, 2005a). However, its speed can be further improved by applying a different ring and choosing a more linear transformation; the encryption and decryption operations are akin to applying ring transformations to a ring element (Coglianese and Goi, 2005a; Hoffstein and Silverman, 2001).

Speed is the key property of the NTRU cryptosystem. The study of a new variant of NTRU is considered to be of great interest particularly if it enhances the speed along with security against lattice attacks (Luo and Lin, 2011). However, NTRU has the likelihood of the occurrence of decryption failure.

Previous research has been conducted on NTRU variants operating in different rings, in an effort to improve its performance. In Gaborit *et al.* (2002a), the authors presented a variant of NTRU whereby the ring of integers was replaced with the ring of polynomials in one variable over a finite field. Rourke and Sunar (2003) published a version of NTRU which uses Montgomery multiplication to speed up computation. Coglianese and Goi (2005b) proposed a variant of NTRU based on matrices. Nayak *et al.* (2008) presented a matrix formulation of NTRU, whereby matrices were used in place of integers. In this study, the matrix elements were computed modulus p as 3 and q as 32 while the parameters had values in the range [-1,1]. A critical evaluation of the work by Nayak *et al.* (2008) in the course of this research revealed the occurrence of decryption failure using the published parameters and published example. Jarvis and Nevins (2015) published a variant of NTRU with a structure based on Eisenstein integers, instead of the classical NTRU structure based on the polynomial ring of integers. The study by Tripathi and Thakur (2015) presented a variant of NTRU which uses logical XOR operations throughout the entire cryptosystem. A critical evaluation of the work by Tripathi and Thakur (2015) in the course of this research study revealed that the scheme was vulnerable because an attacker can easily obtain the ciphertext by reducing the ciphertext $mod\, p$ and furthermore, the private key is zero.

Previous works on variants of NTRU lay emphasis on improving its performance in terms of speed, however, none of the variants explored the formulation of a variant which addresses the problem of decryption failure and improvement of the probability of finding an inverse in NTRU.

1.3 Problem Statement

Cryptography ensures the security, secrecy and authenticity of information. With NTRU being the leading alternative for ECC and RSA in the post-quantum era, it has the weakness of decryption failure which is said to be largely key dependent. In order to keep the probability of decryption failure at a level of at most 2^{-k} (with k being the security level in bits), a list of recommended parameter sets were prescribed for binary polynomials. Binary polynomials were then replaced with the use of ternary and product-form polynomials in order to improve the combinatorial search space; both of which have prescribed lists of recommended parameter sets. However, these parameter sets are limited in range thereby creating a need to expand the size of the NTRU family of parameters. Given the lattice structure of NTRU which makes use of polynomial arithmetic, another inherent difficulty is determining whether a polynomial is invertible. This is of grave importance, as the key generation process in NTRU involves the computation of two modular polynomial inverses. In the event that a non-invertible private polynomial is selected, it goes into an infinite loop of trying to find an inverse thereby necessitating that the selected polynomial be discarded and another invertible one be selected in its place. This consequently results in unsuccessful key generation, encryption and thus unsuccessful message decryption.

There is therefore a need for research investigating the relationship between the NTRU parameters thereby stating with certainty which parameters have an effect on successful decryption. This will in turn be used to expand the size of the NTRU family of parameters by extending the parameter selection criteria. Subsequently, there is the need for the development of an improved NTRU inverse algorithm which improves the chances of generating a modular polynomial inverse.

Speed is the key property of NTRU cryptosystem along with its future forwardness with regards to quantum algorithm attacks. Thus, it is of valuable interest to study a new variant of NTRU which will not only provide a speed improvement along with lattice security, but will also improve the chances of finding a modular inverse and ensure improved probability of successful message decryption.

1.4 Research Questions

In order to address the issue of decryption failure, difficulty of determining polynomial invertibility and parameter selection criteria, the following list of research questions were singled out.

i. How can the existing NTRU recommended parameter sets be extended?

   (a) What are the NTRU parameters that have the greatest influence on the occurrence of decryption failure?

   (b) How can the NTRU parameters be selected in a manner that ensures successful message decryption?

   (c) What is the recommendation for selecting an appropriately large size of q for implementation over a range of security levels covering low, medium and high security levels?

ii. How can an NTRU inverse algorithm be developed which will always find an inverse and provide flexibility in polynomial selection?

   (a) Which algorithm will find an inverse for any random polynomial chosen by the user/recipient?

   (b) How can the parameters be selected in a way that improves the likelihood of finding modular polynomial inverses for private key generation.

iii. What variant of NTRU can be developed to overcome the problems of decryption failure and guarantee modular polynomial inversion when parameters are selected in accordance with a prescribed parameter selection criteria?

   (a) What manner can be used to select parameters so as to ensure that an inverse can be found and that decryption is successful?

   (b) How will the proposed variant withstand regular cryptanalysis attacks?

1.5 Research Objectives

NTRU is the top contender to replace ECC and RSA in the post-quantum era. However, previous studies by Luo and Lin (2011) point out the difficulty in determining whether a polynomial is invertible while Howgrave-Graham *et al.* (2003b) made the assertion that decryption failure present in NTRU, is largely key dependent.

In order to address these problems, this research works towards the aim of investigating decryption failure in NTRU so as to identify the key determinant of decryption failure, improve the probability of invertibility during NTRU key generation and formulate an NTRU variant with improved probability of successful message decryption and improved invertibility. In order to achieve the above stated aim, the objectives set out to be achieved in the course of this research study are:

i. To extend the NTRU parameter selection criteria for improved invertibility and successful message decryption.

   An investigation of NTRU parameters is conducted in an effort to identify the most influential parameters for decryption failure, considering both binary and ternary polynomial variants. The relationships between the parameters aid in identifying the influential parameters as well as recommend an extended parameter selection criteria which ensures invertibility and reduced probability of decryption failure coupled with an additional list of recommended parameter sets. The proposed extended parameter selection criteria is evaluated computationally to determine the probability of decryption failure in comparison to the published standard criteria.

ii. To improve the NTRU inverse algorithm for enhanced likelihood of modular polynomial inversion.

   Pursuant to identification of the most influential parameters of decryption failure, thereby the most pertinent section of the NTRU algorithm, the study works towards improving the NTRU inverse algorithm. Several alternative solutions are considered and compared in terms of performance efficiency and ultimately probability of decryption failure, so as to arrive at an optimal solution. The metrics used for measuring performance efficiency include the speed of inversion, correctness of the inverse result, provision for random polynomial selection and computational complexity.

iii. To provide an NTRU variant with improved modular polynomial inversion and successful message decryption.

The knowledge of influential parameters for decryption failure in NTRU coupled with the improved NTRU inverse algorithm are applied in formulating a variant of NTRU using an alternative ring. The performance of the formulated variant is evaluated in terms of security in bits, the algorithm's computational complexity, public key size, private key size, speed of inversion, encryption speed, decryption speed, key generation speed and message expansion factor. A list of recommended parameter sets for the variant along with the corresponding security strength are presented.

1.6 Scope

The scope of this study is limited to:

i. The study of decryption failure in binary and ternary variants of NTRU.

ii. The study of the key generation process in NTRUEncrypt, the encryption algorithm.

iii. Test parameters used in the experimentation are limited to the NTRU test vectors published in Angel (2014, 2016), recommended parameter sets published in Hoffstein *et al.* (2003c); EESS (2003b); Hoffstein *et al.* (1998); iee (2009) and examples published in related works.

1.7 Significance of the Study

This study provides an exploratory evaluation of the relationship between NTRU parameters; using this deduced relationship to provide an extended NTRU parameter selection criteria for improved invertibility. Furthermore, an improved NTRU inverse algorithm is presented which improves the likelihood of modular polynomial inversion. The aforementioned findings are integrated to formulate an NTRU variant which has improved invertibility and probability of successful message decryption. The outcome of this research study is beneficial to both the cryptography community and the common body of knowledge in the following aspects:

i. The insight gained in terms of the relationship between NTRU parameters plays an instrumental role in the concept behind NTRU parameter generation, the parameter selection criteria and subsequently the concept behind the approximation of the probability of decryption failure. Given that previous research work presents the probability of decryption failure without delving into the details of how these measures are derived, this study demystifies the approximation process right from the probability of selecting a certain polynomial coefficient up to the corresponding variance and probabilities of decryption failure as a power of the security level k and in bits.

ii. The study of the NTRU key generation process provided insight into the intricacies of polynomial inversion modulo an integer. This new insight is used to identify alternative modular polynomial inverse solutions and evaluate their pros and cons in terms of performance efficiency (speed of finding an inverse, accuracy of the result and the provision for totally random parameter selection). This equips the researcher with valuable input for the identification of an alternative modular inverse solution. The process can also be applied in other variants of NTRU.

iii. The evaluation of different algebraic ring structures in an effort to identify a suitable structure for the variant sheds light on the cryptographic properties of various algebraic structures. Furthermore, knowledge is obtained on cryptographic security analysis, basis and measurements which are applicable in the development of other NTRU variants as well as development of other cryptography algorithms.

This research will ultimately help to improve user confidence in the security of NTRU during implementation in the financial services industry, in the NXP Philips micro-controller as well as its implementation in surveillance-free chat applications.

1.8 Thesis Organization

NTRU is a public key cryptosystem that is paramount in ensuring the security of information, particularly in the financial services industry. Therefore, this requires that the cryptosystem be sound in terms of key generation which involves calculation of the modular polynomial inverse and successful message decryption. This thesis presents findings which will be beneficial in countering these challenges. This chapter provides insight into the research problem, the background of the challenges to be addressed and the approach to be applied in countering these highlighted challenges.

REFERENCES

(2006). *Sample Size*. URL http://library.lincoln.ac.nz/global/library/learning/mathsandstats/qmet103/sample-size.pdf.

(2008). IEEE Draft Standard Specification for Public- Key Cryptographic Techniques Based on Hard Problems Over Lattices. *IEEE Unapproved Draft Std P1363.1/D12, Oct 2008*, 1.

(2009). IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. *IEEE Std 1363.1-2008*, C1–69. doi: 10.1109/IEEESTD.2009.4800404.

Abuturab, M. R. (2014). Single-channel color information security system using LU decomposition in gyrator transform domains. *Optics Communications*. 323, 100 – 109. ISSN 0030-4018. doi: http://dx.doi.org/10.1016/j.optcom.2014.02.061. URL http://www.sciencedirect.com/science/article/pii/S0030401814002089.

Adams, E. (2013). *Researchers Predict "Cryptopolypse"*. URL http://blog.securityinnovation.com/blog/2013/11/researchers-predict-cryptopolypse.html.

Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M. and Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. *arXiv preprint arXiv:1003.4085*.

Albrecht, M. R., Curtis, B. R., Deo, A., Davidson, A., Player, R., Postlethwaite, E., Virdia, F. and Wunderer, T. (2018). *Estimate all the {LWE, NTRU} schemes!(2018)*. URL https://pure.royalholloway.ac.uk/portal/files/29876598/paper_11_.pdf.

Alsaidi, N. M. and Yassein, H. R. (2016). BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra. *International Journal of Advanced Computer Science & Applications*. 1(7), 1–6.

Amaral, J. N. (2011). About computing science research methodology. doi: 10.1.1.124.702. URL http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=A8A04BEAEB2D8DCC74156AB0ECFB7FF1?doi=10.1.1.124.702&rep=rep1&type=pdf.

American National Standards Institute, A. (2010). *ANSI X9.98-2010 Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry*.

Angel, Y. (2014). *NTRUEncrypt*. URL https://github.com/Yawning/ntru/tree/master/testvectors.

Angel, Y. (2016). *package ntru*. URL https://godoc.org/github.com/Yawning/ntru.

Ashok, K. N., Nayak, R. and Lalit, K. A. (2015). NTRU with Gaussian Integer Matrix.

Athreya, K. B. and Lahiri, S. N. (2006). *Measure Theory and Probability Theory*, New York, NY: Springer New York, chap. Central Limit Theorems. ISBN 978-0-387-35434-7, 343–382. doi: 10.1007/978-0-387-35434-7-12. URL http://dx.doi.org/10.1007/978-0-387-35434-7_12.

Atiyah, M. (2018). *Introduction to commutative algebra*. CRC Press.

Ayash, E. M. M. (2014). Research Methodologies in Computer Science and Information Systems. *Retrieved November*. 28, 2014.

Balle, S. M., Hansen, P. C. and Higham, N. (1994). A Strassen-type matrix inversion algorithm. *Advances in Parallel Algorithms*, 22–30.

Banks, W. D. and Shparlinski, I. E. (2002). A variant of NTRU with non-invertible polynomials. In *International Conference on Cryptology in India*. Springer, 62–70.

Baptista, M. (1998). Cryptography with chaos. *Physics Letters A*. 240(1), 50–54.

Ben-Israel, A. and Greville, T. N. (2003). *Generalized inverses: theory and applications*. vol. 15. Springer Science & Business Media.

Benhamouda, F., Krenn, S., Lyubashevsky, V. and Pietrzak, K. (2015). Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings. In Pernul, G., Y A Ryan, P. and Weippl, E. (Eds.) *Computer Security – ESORICS 2015*. Cham: Springer International Publishing. ISBN 978-3-319-24174-6, 305–325.

Bergamo, P., D'Arco, P., Santis, A. D. and Kocarev, L. (2005). Security of public-key cryptosystems based on Chebyshev polynomials. *IEEE Transactions on Circuits and Systems I: Regular Papers*. 52(7), 1382–1393. ISSN 1549-8328. doi: 10.1109/TCSI.2005.851701.

Bergou, J. A. and Hillery, M. (2013). *Introduction to the theory of quantum information processing*. Springer Science & Business Media.

Bi, J. and Cheng, Q. (2014). Lower bounds of shortest vector lengths in random NTRU lattices. *Theoretical Computer Science*. 560, 121 – 130. ISSN 0304-3975. doi: https://doi.org/10.1016/j.tcs.2014.10.011. URL http://www.sciencedirect.com/science/article/pii/S0304397514007737, networks, Algorithms and complexity: articles from the Turing centenary in Beijing, China.

Biehl, I., Meyer, B. and Müller, V. (2000). Differential fault attacks on elliptic curve cryptosystems. In *Advances in Cryptology—CRYPTO 2000*. Springer, 131–146.

Bourgeois, G. and Faugère, J.-C. (2009). Algebraic attack on NTRU using Witt vectors and Gröbner bases. *Journal of Mathematical Cryptology*. 3(3), 205–214.

Boyd, S. (2008). *Least Squares*. URL https://see.stanford.edu/materials/lsoeldsee263/05-ls.pdf.

Brand, K. (2013). *NTRU: A Lattice-Based Cryptosystem and Attacks Against It*.

Buchmann, J. A. (2004). *Congruences and Residue Class Rings*, New York, NY: Springer New York. ISBN 978-1-4419-9003-7, 29–70. doi: 10.1007/978-1-4419-9003-7_2. URL https://doi.org/10.1007/978-1-4419-9003-7_2.

Cabarcas, D., Weiden, P. and Buchmann, J. (2014). On the efficiency of provably secure NTRU. In *Post-Quantum Cryptography*. (pp. 22–39). Springer.

Challa, N. and Pradhan, J. (2007). Performance analysis of public key cryptographic systems RSA and NTRU. *International Journal of Computer Science and Network Security*. 7(8), 87–96.

Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016). *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology.

Chen, L., Jordan, S., Liu, Y.-k., Smith-Tone, D., Moody, D., Peralta, R. and Perlner, R. (2014). *A Quantum World and how NIST is Preparing for Future Crypto*. URL https://csrc.nist.gov/CSRC/media/Events/ISPAB-MARCH-2014-MEETING/documents/a_quantum_world_v1_ispab_march_2014.pdf.

Cheong, K. Y. and Koshiba, T. (2007). More on Security of Public-Key Cryptosystems Based on Chebyshev Polynomials. *IEEE Transactions on Circuits and Systems II: Express Briefs*. 54(9), 795–799. ISSN 1549-7747. doi: 10.1109/TCSII.2007.900875.

Chung, K., Lee, H.-S. and Lim, S. (2016). An efficient lattice reduction using reuse technique blockwisely on NTRU. *Discrete Applied Mathematics*. 214, 88 – 98. ISSN 0166-218X. doi: https://doi.org/10.1016/j.dam.2016.05.029. URL http://www.sciencedirect.com/science/article/pii/S0166218X16302542.

Coglianese, M. and Goi, B.-M. (2005a). *MaTRU: A New NTRU-Based Cryptosystem*, Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN 978-3-540-32278-8, 232–243. doi: 10.1007/11596219_19. URL http://dx.doi.org/10.1007/11596219_19.

Coglianese, M. and Goi, B.-M. (2005b). MaTRU: A new NTRU-based cryptosystem. In *Progress in Cryptology-INDOCRYPT 2005*. (pp. 232–243). Springer.

Committee, C. (July 2008). *IEEE P1363.1/D10 Draft Standard for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices*.

Contini, S., Kaya Koç, Ç. and Walter, C. D. (2011). *Modular Arithmetic*, Boston, MA: Springer US. ISBN 978-1-4419-5906-5, 795–798. doi: 10.1007/978-1-4419-5906-5_49. URL https://doi.org/10.1007/978-1-4419-5906-5_49.

Dai, W., Whyte, W. *et al.* (2018). Optimizing polynomial convolution for NTRUEncrypt. *IEEE Transactions on Computers*.

D'Anvers, J.-P., Vercauteren, F. and Verbauwhede, I. (2018). *On the impact of decryption failures on the security of LWE/LWR based schemes*. Cryptology ePrint Archive, Report 2018/1089. https://eprint.iacr.org/2018/1089.

Dattani, N. S. and Bryans, N. (2014). Quantum factorization of 56153 with only 4 qubits. *arXiv preprint arXiv:1411.6758*.

Davis, P. J. (2012). *Circulant matrices*. American Mathematical Soc. ISBN 0821891650.

Desu, M. (2012). *Sample size methodology*. Elsevier.

Ducas, L. and Lepoint, T. (2013). *BLISS: Bimodal Lattice Signature Schemes.(June 2013)*.

EESS (2003a). *Efficient Embedded Security Standard (EESS) #1: Version 2*.

EESS (2003b). *Efficient Embedded Security Standards (EESS)*.

EESS (2015). *Efficient Embedded Security Standard (EESS) #1: Version 3*.

EETimes (2008). *NXP, NTRU team for microcontroller security*. URL http://www.eetimes.com/document.asp?doc_id=1250186.

Eisenbud, D. (2013). *Commutative Algebra: with a view toward algebraic geometry*. vol. 150. Springer Science & Business Media.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *Information Theory, IEEE Transactions on*. 31(4), 469–472.

Etingof, P. I., Golberg, O., Hensel, S., Liu, T., Schwendner, A., Vaintrob, D. and Yudovina, E. (2011). *Introduction to representation theory*. vol. 59. American Mathematical Society Providence, RI.

Feng, X. and Zhang, Z. (2007). The rank of a random matrix. *Applied Mathematics and Computation*. 185(1), 689 – 694. ISSN 0096-3003. doi: https://doi.org/10.1016/j.amc.2006.07.076. URL http://www.sciencedirect.com/science/article/pii/S0096300306009040.

Fletcher, R. (1968). Generalized inverse methods for the best least squares solution of systems of non-linear equations. *The Computer Journal*. 10(4), 392–399.

Fluhrer, S. R. (2015). Quantum Cryptanalysis of NTRU. *IACR Cryptology ePrint Archive*. 2015, 676.

Fouhey, D. F., Him, M. H., Maturana, D., von Woofles, R. F. R. and Boy, G. (2015). Visually Identifying Rank.

Fuller, C. (2011). *Cryptographic Security for Financial Services*.

Gaborit, P., Ohler, J. and Solé, P. (2002a). *CTRU, a polynomial analogue of NTRU*. Ph.D. Thesis. INRIA.

Gaborit, P., Ohler, J. and Solé, P. (2002b). *CTRU, a polynomial analogue of NTRU*. Technical Report RR-4621. INRIA. URL https://hal.inria.fr/inria-00071964.

Gaithuru, J. and Salleh, M. (Under Review, submitted 11-10-2018c). *ITRU, Variant of NTRU Based on the Ring of Integers*.

Gaithuru, J. and Salleh, M. (Under Review, submitted 19-8-2018b). *Improved NTRU Inverse Algorithm using the Pseudo-Inverse in Least Squares Solution*.

Gaithuru, J. and Salleh, M. (Under Review, submitted 26-9-2018a). *Extended NTRU Parameter Selection Criteria Formulation for Improved Polynomial Inversion Using a Formal Test Procedure*.

Gaithuru, J. N. and Bakhtiari, M. (2014). Insight into the operation of NTRU and a comparative study of NTRU, RSA and ECC public key cryptosystems. In *2014 8th Malaysian Software Engineering Conference (MySEC)*. Sept. 273–278. doi: 10.1109/MySec.2014.6986028.

Gaithuru, J. N., Bakhtiari, M., Salleh, M. and Muteb, A. M. (2015). A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap. In *2015 9th Malaysian Software Engineering Conference (MySEC)*. Dec. 236–244. doi: 10.1109/MySEC.2015.7475227.

Gaithuru, J. N. and Salleh, M. (2017). ITRU: NTRU-Based Cryptosystem Using Ring of Integers. *International Journal of Innovative Computing*. 7(1).

Gaithuru, J. N., Salleh, M. and Bakhtiari, M. (2017a). Identification of Influential Parameters for NTRU Decryption Failure and Recommendation of Extended Parameter Selection Criteria for Elimination of Decryption Failure. *IAENG International Journal of Computer Science*. 44(3).

Gaithuru, J. N., Salleh, M. and Mohamad, I. (2016a). 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. 270–275. doi: 10.1109/ICEED.2016.7856086.

Gaithuru, J. N., Salleh, M. and Mohamad, I. (2017b). NTRU inverse polynomial algorithm based on the LU decomposition method of matrix inversion. In *2017 IEEE Conference on Application, Information and Network Security (AINS)*. Nov. 1–6. doi: 10.1109/AINS.2017.8270415.

Gaithuru, J. N., Salleh, M., Mohamad, I. and Adeyemi, I. R. (2016b). NTRU Binary Polynomials Parameters Selection for Reduction of Decryption Failure. In *International Conference on Computational Intelligence in Information System*. Springer, 175–187.

Gaithuru, J. N., Salleh, M. and Muhainiah (Under Review, submitted 14th March, 2018). Improved NTRU Inverse Algorithm using the Pseudo-Inverse in Least Squares Solution. *Malaysian Journal of Computer Science*.

Geißler, K. and Smart, N. (2003). Computing the M = UUt Integer Matrix Decomposition. In Paterson, K. (Ed.) *Cryptography and Coding*. (pp. 223–233). *Lecture Notes in Computer Science*, vol. 2898. Springer Berlin Heidelberg. ISBN 978-3-540-20663-7. doi: 10.1007/978-3-540-40974-8_18. URL http://dx.doi.org/10.1007/978-3-540-40974-8_18.

Gentry, C. and Szydlo, M. (2002). Cryptanalysis of the Revised NTRU Signature Scheme. In Knudsen, L. (Ed.) *Advances in Cryptology — EUROCRYPT 2002*. (pp. 299–320). *Lecture Notes in Computer Science*, vol. 2332. Springer Berlin Heidelberg. ISBN 978-3-540-43553-2. doi: 10.1007/3-540-46035-7-20. URL http://dx.doi.org/10.1007/3-540-46035-7-20.

Goldreich, O., Goldwasser, S. and Halevi, S. (1997). Public-key cryptosystems from lattice reduction problems. In *Annual International Cryptology Conference*. Springer, 112–131.

Grassl, M., Langenberg, B., Roetteler, M. and Steinwandt, R. (2016). Applying Grover's algorithm to AES: quantum resource estimates. In *International Workshop on Post-Quantum Cryptography*. Springer, 29–43.

Greuel, G.-M. and Pfister, G. (2012). *A Singular introduction to commutative algebra*. Springer Science & Business Media.

Group, M. (2015). *MAGMA Computational Algebra System. Version 2.21-2, Sydney*.

Hamasho, S., Murakami, Y. and Kasahara, M. (2012). A systematic encryption algorithm for knapsack scheme using random sequence. In *2012 7th International Conference on Computing and Convergence Technology (ICCCT)*. Dec. 514–517.

Hercigonja, Z. (2016). Comparative Analysis of Cryptographic Algorithms. *International Journal of Digital Technology & Economy*. 1(2), 127–134.

Hermans, J., Vercauteren, F. and Preneel, B. (2010). Speed Records for NTRU. In Pieprzyk, J. (Ed.) *Topics in Cryptology - CT-RSA 2010*. (pp. 73–88). *Lecture Notes in Computer Science*, vol. 5985. Springer Berlin Heidelberg. ISBN 978-3-642-11924-8. doi: 10.1007/978-3-642-11925-5-6. URL http://dx.doi.org/10.1007/978-3-642-11925-5-6.

Hillman, A. P. and Alexanderson, G. L. (1994). *Abstract algebra: A first undergraduate course*. PWS Publishing Company.

Hirschhorn, P. S., Hoffstein, J., Howgrave-Graham, N. and Whyte, W. (2009). Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches. In Abdalla, M., Pointcheval, D., Fouque, P.-A. and Vergnaud, D. (Eds.) *Applied Cryptography and Network Security*. (pp. 437–455). *Lecture Notes in Computer Science*, vol. 5536. Springer Berlin Heidelberg. ISBN 978-3-642-01956-2. doi: 10.1007/978-3-642-01957-9-27. URL http://dx.doi.org/10.1007/978-3-642-01957-9-27.

Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H. and Whyte, W. (2003a). NTRUSign: Digital Signatures Using the NTRU Lattice. In Joye, M. (Ed.) *Topics in Cryptology — CT-RSA 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN 978-3-540-36563-1, 122–140.

Hoffstein, J., Howgrave-Graham, N., Pipher, J. and Whyte, W. (2009). Practical lattice-based cryptography: NTRUEncrypt and NTRUSign. In *The LLL Algorithm*. (pp. 349–390). Springer.

Hoffstein, J., Howgrave-Graham, N., Pipher, J. and Whyte, W. (2010a). Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign. In Nguyen, P. Q. and Vallée, B. (Eds.) *The LLL Algorithm*. (pp. 349–390). Information Security and Cryptography. Springer Berlin Heidelberg. ISBN 978-3-642-02294-4. doi: 10.1007/978-3-642-02295-1-11. URL http://dx.doi.org/10.1007/978-3-642-02295-1-11.

Hoffstein, J., Howgrave-Graham, N., Pipher, J. and Whyte, W. (2010b). *Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign*, Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN 978-3-642-02295-1, 349–390. doi: 10.1007/978-3-642-02295-1_11. URL http://dx.doi.org/10.1007/978-3-642-02295-1_11.

Hoffstein, J., Pipher, J., Schanck, J. M., Silverman, J. H., Whyte, W. and Zhang, Z. (2015a). Choosing Parameters for NTRUEncrypt. URL http://eprint.iacr.org/2015/708.pdf.

Hoffstein, J., Pipher, J., Schanck, J. M., Silverman, J. H., Whyte, W. and Zhang, Z.

(2015b). *Choosing parameters for ntruencrypt*. Report. Cryptology ePrint Archive, Report 2015/708.

Hoffstein, J., Pipher, J. and Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In Buhler, J. P. (Ed.) *Algorithmic number theory*. (pp. 267–288). Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN 978-3-540-69113-6.

Hoffstein, J., Pipher, J., Silverman, J. H. and Silverman, J. H. (2008). *An introduction to mathematical cryptography*. vol. 1. Springer.

Hoffstein, J., Silverman and Whyte, W. (2003b). NTRU Cryptosystems Technical Report# 018, Version 1: Estimating decryption failures of NTRUEncrypt. *NTRU Cryptosystems, Inc*.

Hoffstein, J. and Silverman, J. (2001). Optimizations for NTRU. In *Public-Key Cryptography and Computational Number Theory: Proceedings of the International Conference organized by the Stefan Banach International Mathematical Center Warsaw, Poland, September 11-15, 2000*. Walter de Gruyter, 77.

Hoffstein, J. and Silverman, J. H. (1998). *Implementation Notes for NTRU PKCS Multiple Transmissions*. Technical report. Report.

Hoffstein, J., Silverman, J. H. and Whyte, W. (2003c). NTRU Cryptosystems Technical Report# 012, Version 2: Estimated Breaking Times for NTRU Lattices. *NTRU Cryptosystems, Inc*.

Hohn, F. E. (2013). *Elementary matrix algebra*. Courier Corporation.

Hornik, K., Buchta, C. and Zeileis, A. (2009). Open-source machine learning: R meets Weka. *Computational Statistics*. 24(2), 225–232.

Howgrave-Graham, N. (2007). A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In *Advances in Cryptology-CRYPTO 2007*. (pp. 150–169). Springer.

Howgrave-Graham, N., Nguyen, P., Pointcheval, D., Proos, J., Silverman, J., Singer, A. and Whyte, W. (2003a). The Impact of Decryption Failures on the Security of NTRU Encryption. In Boneh, D. (Ed.) *Advances in Cryptology - CRYPTO 2003*. (pp. 226–246). *Lecture Notes in Computer Science*, vol. 2729. Springer Berlin Heidelberg. ISBN 978-3-540-40674-7. doi: 10.1007/978-3-540-45146-4-14. URL http://dx.doi.org/10.1007/978-3-540-45146-4-14.

Howgrave-Graham, N., Silverman, J. and Whyte, W. (2005a). Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3. In Menezes, A. (Ed.) *Topics in Cryptology – CT-RSA 2005*. (pp. 118–135). *Lecture Notes in Computer Science*, vol. 3376. Springer Berlin Heidelberg. ISBN 978-3-540-24399-1. doi: 10.1007/

978-3-540-30574-3-10. URL http://dx.doi.org/10.1007/978-3-540-30574-3-10.

Howgrave-Graham, N., Silverman, J. H., Singer, A., Whyte, W. and Cryptosystems, N. (2003b). NAEP: Provable Security in the Presence of Decryption Failures. *IACR Cryptology ePrint Archive*. 2003, 172.

Howgrave-Graham, N., Silverman, J. H. and Whyte, W. (2003c). *A Meet-in-the-Middle Attack on an NTRU Private key*. Technical report. Technical report, NTRU Cryptosystems, June 2003. Report.

Howgrave-Graham, N., Silverman, J. H. and Whyte, W. (2005b). *Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3*, Springer. ISBN 3540243992, 118–135.

Howgrave-Graham, N., Silverman, J. H. and Whyte, W. (2005c). *Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3*, Springer. ISBN 3540243992, 118–135.

Hu, F., Hao, Q., Lukowiak, M., Sun, Q., Wilhelm, K., Radziszowski, S. and Wu, Y. (2010). Trustworthy Data Collection From Implantable Medical Devices Via High-Speed Security Implementation Based on IEEE 1363. *IEEE Transactions on Information Technology in Biomedicine*. 14(6), 1397–1404. ISSN 1089-7771. doi: 10.1109/TITB.2010.2049204.

IEEE (2003a). *Efficient Embedded Security Standards (EESS)*.

IEEE (2003b). *Efficient Embedded Security Standards (EESS), EESS 1: Implementation Aspects of NTRUEncrypt and NTRUSign, Version 2.0*.

IEEE (2008). IEEE Draft Standard Specification for Public- Key Cryptographic Techniques Based on Hard Problems Over Lattices. *IEEE Unapproved Draft Std P1363.1/D12, Oct 2008*.

IEEE (2009). IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. *IEEE Std 1363.1-2008*, C1–69. doi: 10.1109/IEEESTD.2009.4800404.

Iliev, A., Kyurkchiev, N. and Rahnev, A. (2018). A Note on Adaptation of the Knuth's Extended Euclidean Algorithm for Computing Multiplicative Inverse. *International Journal of Pure and Applied Mathematics*. 118, 281–290.

Irving, R. S. (2004). *Integers, Polynomials, and Rings: A Course in Algebra*. (1st ed.). Undergraduate Texts in Mathematics. Springer. ISBN 9780387218311,9780387403977,0387403973. URL http://gen.lib.rus.ec/book/index.php?md5=7A363582C4B9FEFDE4D1C32E5C2A8D36.

Ishii, M. (2008). Periodicity of Chebyshev polynomials over the residue ring of Z/2 r Z and an electronic signature. *Trans. of The Japan Society for Industrial and Applied Mathematics*. 18(2), 257–265.

James, G. and James, R. C. (1959). Mathematics dictionary. *Mathematics dictionary, by James, Glenn; James, Robert C. Princeton, NJ, Van Nostrand [1959].*

Jarvis, K. (2011). *NTRU over the Eisenstein integers*. Ph.D. Thesis. Université d'Ottawa/University of Ottawa.

Jarvis, K. and Nevins, M. (2013). ETRU: NTRU over the Eisenstein integers. *Designs, Codes and Cryptography*, 1–24.

Jarvis, K. and Nevins, M. (2015). ETRU: NTRU over the Eisenstein integers. *Designs, Codes and Cryptography*. 74(1), 219–242.

Jeeva, A., Palanisamy, D. V. and Kanagaram, K. (2012). Comparative analysis of performance efficiency and security measures of some encryption algorithms. *International Journal of Engineering Research and Applications (IJERA)*. 2(3), 3033–3037.

Jeffrey Hoffstein, J. P. and Whyte, W. (2009). *More Efficient parameters, keys and encoding for hybrid-resistant NTRUEncrypt and NTRUSign*.

Jeffrey Hoffstein, W. W., Jill Pipher (2009). *More Efficient Parameters Keys and Encoding for Hybrid Resistant NTRUEncrypt and NTRUSign*. Report. NTRU Cryptosystems Inc, Security Innovation.

Jenney, P. (2014). *NTRUOpenSourceProject/ntru-crypto*. URL https://raw.githubusercontent.com/NTRUOpenSourceProject/ntru-crypto/master/reference-code/Java/Encrypt/com/securityinnovation/testvectors/NtruEncryptTestVector.java.

Johnson, M. W., Amin, M. H., Gildert, S., Lanting, T., Hamze, F., Dickson, N., Harris, R., Berkley, A. J., Johansson, J., Bunyk, P. *et al.* (2011). Quantum annealing with manufactured spins. *Nature*. 473(7346), 194.

Jones, N. (2013a). *Computing: The Quantum Company*. URL https://www.nature.com/news/computing-the-quantum-company-1.13212.

Jones, N. (2013b). *Google and NASA snap up quantum computer*. URL https://www.nature.com/news/google-and-nasa-snap-up-quantum-computer-1.12999.

Kaliski, B. (2006). The Mathematics of the RSA Public-Key Cryptosystem. *RSA Laboratories*.

Kamat, P. and Patel, J. (2010). Design and validation of NTRU public-key cryptosystem.

Karu, P. and Loikkanen, J. (2001). Practical comparison of fast public-key cryptosystems. In *Telecommunications Software and Multimedia Lab. at Helsinki Univ. of Technology, Seminar on Network Security*. Citeseer.

Katz, J. (2010). Public-Key Cryptography. In *Handbook of Information and Communication Security*. (pp. 21–34). Springer.

Kay, S. M. (2006). *Expected Values for Discrete Random Variables*, Boston, MA: Springer US. ISBN 978-0-387-24158-6, 133–166. doi: 10.1007/0-387-24158-2_6. URL https://doi.org/10.1007/0-387-24158-2_6.

Kessler, G. C. (2012). Introduction to Cryptography. URL https://commons.erau.edu/cgi/viewcontent.cgi?article=1010&context=db-security-studies.

Khushboo Thakur, B. T. (2017). STRU: A Non Alternative and Multidimensional Public Key Cryptosystem.

Kocarev, L., Makraduli, J. and Amato, P. (2005). Public-Key Encryption Based on Chebyshev Polynomials. *Circuits, Systems and Signal Processing*. 24(5), 497–517. ISSN 1531-5878. doi: 10.1007/s00034-005-2403-x. URL http://dx.doi.org/10.1007/s00034-005-2403-x.

Kohavi, R. and Longbotham, R. (2017). *Online Controlled Experiments and A/B Testing*, Boston, MA: Springer US. ISBN 978-1-4899-7687-1, 922–929. doi: 10.1007/978-1-4899-7687-1_891. URL https://doi.org/10.1007/978-1-4899-7687-1_891.

Komargodski, I., Moran, T., Naor, M., Pass, R., Rosen, A. and Yogev, E. (2014). One-Way Functions and (Im)Perfect Obfuscation. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*. Oct. ISSN 0272-5428, 374–383. doi: 10.1109/FOCS.2014.47.

Kouzmenko, R. (2006). Generalizations of the NTRU cryptosystem. *Diploma Project, École Polytechnique Fédérale de Lausanne,(2005–2006)*.

Koyama, K., Maurer, U. M., Okamoto, T. and Vanstone, S. A. (1991). New public-key schemes based on elliptic curves over the ring Zn. In *Annual International Cryptology Conference*. Springer, 252–266.

Kra, I. and Simanca, S. R. (2012a). On circulant matrices. *Notices of the AMS*. 59(3), 368–377.

Kra, I. and Simanca, S. R. (2012b). On circulant matrices. *Notices of the AMS*. 59(3), 368–377.

Kumar, Y., Munjal, R. and Sharma, H. (2011). Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures.

International Journal of Computer Science and Management Studies. 11(03).

Lavrakas, P. J. (2008). *Encyclopedia of survey research methods*. Sage Publications.

Lei, X. and Liao, X. (2013). NTRU-KE: A Lattice-based Public Key Exchange Protocol. *IACR Cryptology ePrint Archive*. 2013, 718.

Leon, S. J., Björck, Å. and Gander, W. (2013). Gram-Schmidt orthogonalization: 100 years and more. *Numerical Linear Algebra with Applications*. 20(3), 492–532.

Lester, R. (2015). *Cyph chooses NTRU Crypto to power its secure chat communication platform*. URL https://www.cyph.com/blog/2015/09/29/ntru/.

Leung, H. (2016). A note on extended Euclid's algorithm. *arXiv preprint arXiv:1607.00106*.

Levy, P. S. and Lemeshow, S. (2013). *Sampling of populations: methods and applications*. John Wiley and Sons.

Lidl, R. and Pilz, G. (2012). *Applied abstract algebra*. Springer Science & Business Media.

Luo, X.-R. and Lin, C.-H. J. (2011). Discussion on Matrix NTRU. *International Journal of Computer Science and Network Security*. 11(1), 32–35.

Lyubashevsky, V. and Prest, T. (2015). Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices. In Oswald, E. and Fischlin, M. (Eds.) *Advances in Cryptology – EUROCRYPT 2015*. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN 978-3-662-46800-5, 789–815.

MacAusland, R. (2014). The Moore-Penrose Inverse and Least Squares. *Math 420: Advanced Topics in Linear Algebra*.

Malekian, E., Zakerolhosseini, A. and Mashatan, A. (2009). QTRU: A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra. *preprint, Available from the Cryptology ePrint Archive: http://eprint. iacr. org/2009/386. pdf*.

Malekian, E., Zakerolhosseini, A. and Mashatan, A. (2011). QTRU: quaternionic version of the NTRU public-key cryptosystems. *The ISC International Journal of Information Security*. 3(1), 29–42.

Malekian, E., Zakerolhosseini, A. and Mashatan, A. (2015). QTRU: quaternionic version of the NTRU public-key cryptosystems. *The ISC International Journal of Information Security*. 3(1).

Malhotra, M. and Singh, A. (2013). Study of Various Cryptographic Algorithms. 1(3), 77–78.

Maurich, v. I., Heberle, L. and Güneysu, T. (2016). IND-CCA secure hybrid encryption from QC-MDPC Niederreiter. In *International Workshop on Post-Quantum Cryptography*. Springer, 1–17.

McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. *DSN progress report*. 42(44), 114–116.

Melchor, C. A., Boyen, X., Deneuville, J.-C. and Gaborit, P. (2014). Sealing the Leak on Classical NTRU Signatures. In Mosca, M. (Ed.) *Post-Quantum Cryptography*. Cham: Springer International Publishing. ISBN 978-3-319-11659-4, 1–21.

Merali, Z. (2011). *First sale for quantum computing*. URL https://www.nature.com/news/2011/110531/full/474018a.html.

Merkle, R. and Hellman, M. E. (1978). Hiding information and signatures in trapdoor knapsacks. *Information Theory, IEEE Transactions on*. 24(5), 525–530.

Mersin, A. (2007). *The comparative performance analysis of lattice based NTRU cryptosystem with other asymmetrical cryptosystems*. Master's Thesis. İzmir Institute of Technology.

Meyers, R. E. (2015). Free-Space and Atmospheric Quantum Communications. In *Advanced Free Space Optics (FSO)*. (pp. 343–387). *Springer Series in Optical Sciences*, vol. 186. Springer New York. ISBN 978-1-4939-0917-9. doi: 10.1007/978-1-4939-0918-6_10. URL http://dx.doi.org/10.1007/978-1-4939-0918-6_10.

Micciancio, D. and Regev, O. (2009). Lattice-based Cryptography. In Bernstein, D., Buchmann, J. and Dahmen, E. (Eds.) *Post-Quantum Cryptography*. (pp. 147–191). Springer Berlin Heidelberg. ISBN 978-3-540-88701-0. doi: 10.1007/978-3-540-88702-7-5. URL http://dx.doi.org/10.1007/978-3-540-88702-7-5.

Miller, V. S. (1986). Use of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO'85 Proceedings*. Springer, 417–426.

Monteiro, R. T. (2016). *Post-quantum cryptography: lattice-based cryptography and analysis of NTRU public-key cryptosystem*. Faculdade de ciencias, departamento de matematica.

Naranjo, J., López-Ramos, J. and Casado, L. (2010). Applications of the extended Euclidean algorithm to privacy and secure communications. In *Proc. of 10th International Conference on Computational and Mathematical Methods in Science and Engineering*. 702–713.

Nayak, R., Sastry, C. and Pradhan, J. (2008). A matrix formulation for NTRU cryptosystem. In *Networks, 2008. ICON 2008. 16th IEEE International Conference on*. IEEE, 1–5.

Nayak, R., Sastry, C. and Pradhan, J. (2010). Algorithmic Comparison between Polynomial Base and Matrix Base NTRU Cryptosystem. *International Journal of Computer and Network Security (IJCNS) Vol.* 2.

Nelson, E. (2016). *Radically Elementary Probability Theory.(AM-117)*. vol. 117. Princeton University Press.

Nguyen, H. B. (2014). *An overview of the NTRU cryptographic system.* Ph.D. Thesis. San Diego State University.

NIST (2017). *Post-Quantum Cryptography*. URL https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

NIST (2018). *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program.*

Nitaj, A. (2017). Post Quantum Cryptography. *Moulay Ismaıl University Faculty of Sciences and Technology of Errachidia Department of Mathematics*, 7.

Nyamaa, N. (2009). *Partially Error-Tolerant NTRU Cryptosystem.*

Nyokabi, G. J., Salleh, M. and Mohamad, I. (2017). NTRU inverse polynomial algorithm based on circulant matrices using gauss-jordan elimination. In *2017 6th ICT International Student Project Conference (ICT-ISPC)*. May. IEEE. ISSN 978-1-5386-2996-3, 1–5. doi: 10.1109/ICT-ISPC.2017.8075326.

Ogawa, H. (1988). An operator pseudo-inversion lemma. *SIAM Journal on Applied Mathematics*. 48(6), 1527–1531.

Oldham, K. B., Myland, J. C. and Spanier, J. (2009a). *The Error Function erf(x) and Its Complement erfc(x)*, New York, NY: Springer US. ISBN 978-0-387-48807-3, 405–415. doi: 10.1007/978-0-387-48807-3_41. URL https://doi.org/10.1007/978-0-387-48807-3_41.

Oldham, K. B., Myland, J. C. and Spanier, J. (2009b). *The exp(x), erfc(Square root of x) and Related Functions*, New York, NY: Springer US. ISBN 978-0-387-48807-3, 417–426. doi: 10.1007/978-0-387-48807-3_42. URL https://doi.org/10.1007/978-0-387-48807-3_42.

Overbeck, R. (2008). Reducing Memory Requirements for Combinatorial Attacks on NTRU via Multiple Birthdays. In *International Conference on E-Business and Telecommunications*. Springer, 199–209.

Patil, P., Narayankar, P., D.G., N. and S.M., M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*. 78, 617–624. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2016.02.108. URL http://www.sciencedirect.com/science/article/pii/

S1877050916001101.

Petkovic, M. D. and Stanimirovic, P. S. (2009). Generalized matrix inversion is not harder than matrix multiplication. *Journal of Computational and Applied Mathematics*. 230(1), 270 – 282. ISSN 0377-0427. doi: http://dx.doi.org/10.1016/j.cam.2008.11.012. URL //www.sciencedirect.com/science/article/pii/S0377042708006237.

Philips (2015). *Training Module: NXP and NTRU Cryptography for ARM MCUs*. URL http://www.nxp.com/video/training-module-nxp-ntru-cryptography-for-arm-mcus:NTRU-CRYPTOGRAPHY-FOR-ARM-MCUS.

Pipher, J. (2002). *Lectures on the NTRU encryption algorithm and digital signature scheme: Grenoble, June 2002*. Report. Brown University, Providence RI 02912. URL http://www.math.brown.edu/~jpipher/grenoble.pdf.

Pollock, D. S. G. (2002). Circulant matrices and time-series analysis. *International Journal of Mathematical Education in Science and Technology*. 33(2), 213–230. ISSN 0020-739X.

Premnath, A. P., Jo, J.-Y. and Kim, Y. (2014). Application of NTRU Cryptographic Algorithm for SCADA Security. In *Information Technology: New Generations (ITNG), 2014 11th International Conference on*. IEEE, 341–346.

Rabin, M. O. (1980). Probabilistic algorithm for testing primality. *Journal of number theory*. 12(1), 128–138.

Ranjeet Ranjan, A. S. B. S. K. (2012). Improvement of NTRU Cryptosystem.

Rényi, A. (1963). On the central limit theorem for the sum of a random number of independent random variables. *Acta Mathematica Academiae Scientiarum Hungarica*. 11(1), 97–102. ISSN 1588-2632. doi: 10.1007/BF02020627. URL https://doi.org/10.1007/BF02020627.

Rivest, R. L., Shamir, A. and Adleman, L. (1983). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 26(1), 96–99.

Ross, S. M. (2014). *Introduction to probability models*. Academic press.

Rothe, J. (2005). Other Public-Key Cryptosystems and Protocols. *Complexity Theory and Cryptology: An Introduction to Cryptocomplexity*, 361–412.

Rourke, C. O. and Sunar, B. (2003). Achieving NTRU with Montgomery multiplication. *IEEE Transactions on Computers*. 52(4), 440–448. ISSN 0018-9340. doi: 10.1109/TC.2003.1190585.

Rutanen, K., Gómez-Herrero, G., Eriksson, S.-L. and Egiazarian, K. O. (2014). A general definition of the big oh notation for algorithm analysis.

Sachin Kumar, S. K. P., Shobha (2013). An Improved Post-Quantum Cryptographic Scheme Based on NTRU. *International Journal of Computer Applications Technology and Research*. 2(4), 499 – 503.

Sameer, H. A.-B. and Gazi, M. A. (2011). Securing peer-to-peer mobile communications using public key cryptography: New security strategy. *International Journal of Physical Sciences*. 6(4), 930–938.

Schanck, J. (2015). *Practical lattice cryptosystems: NTRUEncrypt and NTRUMLS*. Master's Thesis. University of Waterloo.

Scholten, J. and Vercauteren, F. (2003). *An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU Cryptosystem*.

Schroeppel, R., Orman, H., O'Malley, S. and Spatscheck, O. (1995). Fast key exchange with elliptic curve systems. In *Annual International Cryptology Conference*. Springer, 43–56.

Security, C. f. E. E. (2015a). *Efficient Embedded Security Standard (EESS) 1*. URL https://github.com/NTRUOpenSourceProject/ntru-crypto.

Security, C. f. E. E. (2015b). *Efficient Embedded Security Standard (EESS)1, Version 3.0*. URL https://github.com/NTRUOpenSourceProject/ntru-crypto.

Shen, X., Du, Z. and Chen, R. (2009). Research on NTRU algorithm for mobile java security. In *Scalable Computing and Communications; Eighth International Conference on Embedded Computing, 2009. SCALCOM-EMBEDDEDCOM'09. International Conference on*. IEEE, 366–369.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. IEEE, 124–134.

Silverman, J. H. (1999). Almost inverses and fast NTRU key creation. *NTRU Cryptosystems,(Technical Note# 014): http://www. ntru. com/cryptolab/pdf/NTRU Tech014. pdf*.

Silverman, J. H. (2001). Wraps, gaps, and lattice constants. *NTRU Report*. 11.

Silverman, J. H. and Whyte, W. (2003). Estimating decryption failure probabilities for NTRUEncrypt.

Stallings, W. (2014). *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*. vol. 5. Pearson Higher Ed. ISBN 0273793764.

Stamp, M. and Low, R. M. (2007). *Applied cryptanalysis: breaking ciphers in the real world*. John Wiley & Sons.

Stehlé, D. and Steinfeld, R. (2011). Making NTRU as secure as worst-case problems over ideal lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 27–47.

Stein, W. (2009). The Ring of Integers Modulo N. In *Elementary Number Theory: Primes, Congruences, and Secrets*. (pp. 1–27). Springer.

Sun, C.-a., Wang, Z. and Wang, G. (2014). A property-based testing framework for encryption programs. *Frontiers of Computer Science*. 8(3), 478–489. ISSN 2095-2236. doi: 10.1007/s11704-014-3040-y. URL https://doi.org/10.1007/s11704-014-3040-y.

Tata, P. G., Narumanchi, H. and Emmadi, N. (2014). Analytical study of implementation issues of NTRU. In *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. 700–707. doi: 10.1109/ICACCI.2014.6968468.

Thakur, K. and Tripathi, B. P. (2016). BTRU, A Rational Polynomial Analogue of NTRU Cryptosystem. *International Journal of Computer Applications*. 145(12), 22–24. ISSN 0975-8887. doi: 10.5120/ijca2016910769. URL http://www.ijcaonline.org/archives/volume145/number12/25330-2016910769.

Tripathi, B. P. and Thakur, K. (2015). A Logical XOR Operation for NTRU Cryptosystem. *International Journal of Computer Applications*. 126(2).

Tripathi, R. and Agrawal, S. (2014). Comparative study of symmetric and asymmetric cryptography techniques. *International Journal of Advance Foundation and Research in Computer (IJAFRC)*. 1(6), 68–76.

Truman, K. R. (2007). *Analysis and Extension of Non-commutative NTRU*. Ph.D. Thesis. University of Maryland.

Van Loan, C. (1992). *Computational Frameworks for the Fast Fourier Transform*. Society for Industrial and Applied Mathematics. doi: 10.1137/1.9781611970999. URL https://epubs.siam.org/doi/abs/10.1137/1.9781611970999.

Wahab, H. B. A. and Jaber, T. A. (2015). Improve NTRU algorithm based on Chebyshev polynomial. In *Information Technology and Computer Applications Congress (WCITCA), 2015 World Congress on*. June. 1–5. doi: 10.1109/WCITCA.2015.7442633.

Weil, A. (2013). *Basic number theory*. vol. 144. Springer Science & Business Media.

Whyte, W. (2005). *Ntru*, Boston, MA: Springer US. ISBN 978-0-387-23483-0, 427–430. doi: 10.1007/0-387-23483-7-279. URL http://dx.doi.org/10.1007/0-387-23483-7-279.

Whyte, W. (2015). *Efficient Embedded Security Standards (EESS) 1: Implementation Aspects of NTRUEncrypt*.

Whyte, W. and Hoffstein, J. (2011). Ntru. In *Encyclopedia of Cryptography and Security*. (pp. 858–861). Springer.

Whyte, W., Howgrave-Graham, N., Hoffstein, J., Pipher, J., Silverman, J. and Hirschhorn, P. (2008). *IEEE Std 1363.1-2008: Draft standard for public-key cryptographic techniques based on hard problems over lattices*. Technical report. Technical report, IEEE.

Wilf, H. S. (2002). *Algorithms and complexity*. AK Peters/CRC Press.

Wilmington, M. A. (2015). *Security Inovation Challenges the Crypto Community to defeat NTRU*. URL http://www.prweb.com/releases/2015/02/prweb12492128.htm.

Wong, X.-F., Goi, B.-M., Lee, W.-K. and Phan, R. C.-W. (2018). Performance Evaluation of RSA and NTRU over GPU with Maxwell and Pascal Architecture. *Software Networking*. 2018(1), 201–220.

Yao, J. and Zeng, G. (2006). Enhanced NTRU cryptosystem eliminating decryption failures. *Journal of Systems Engineering and Electronics*. 17(4), 890 – 895. ISSN 1004-4132. doi: http://dx.doi.org/10.1016/S1004-4132(07)60033-4. URL http://www.sciencedirect.com/science/article/pii/S1004413207600334.

Yasuda, T., Dahan, X. and Sakurai, K. (2015). Characterizing NTRU-Variants Using Group Ring and Evaluating their Lattice Security. *IACR Cryptology ePrint Archive*. 2015, 1170.

Yoshioka, D. and Dainobu, Y. (2015). Some properties of sequences generated by Chebyshev polynomials modulo 2k. In *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*. May. ISSN 0271-4302, 846–849. doi: 10.1109/ISCAS.2015.7168766.

Yu, W., He, D. and Zhu, S. (2005). Study on NTRU decryption failures. In *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*, vol. 2. July. IEEE, 454–459. doi: 10.1109/ICITA.2005.266.

Zendel, O., Murschitz, M., Humenberger, M. and Herzner, W. (2017). How Good Is My Test Data? Introducing Safety Analysis for Computer Vision. *International Journal of Computer Vision*. 125(1), 95–109. doi: 10.1007/s11263-017-1020-z. URL https://doi.org/10.1007/s11263-017-1020-z.

Zhao, N. and Su, S. (2011). An Improvement and a New Design of Algorithms for Seeking the Inverse of an NTRU Polynomial. In *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*. 891–895. doi: 10.1109/CIS.2011.201.