DOI: https://doi.org/10.24297/jam.v23i.9582

Proposed Development of NTRU Public Key Encryption

Marwah Aearaby Sayyid

Wasit Education Directorate

marwa.arabi@yahoo.com

Abstract;

The 1996 proposal by Hoffstein, Pfeiffer, and Silverman for the NTRU public key encryption system provides a quick and useful substitute for factorization- or discrete logarithm-based classical programs. It rovides approximate security against quantum computing assaults and earoptimal asymptotic efficiency, in contrast to these latter approaches. The security analysis of the system involves examining naturally occurring computational and statistical challenges that are defined on finite polynomial rings. Current advancements in the broader field of lattice based cryptography, include security studies and applications of NTRU and its variations. These advancements include the creation of multilinear.

sdrzruev: sursrvde edydorspdqw d sxporpNTRU, ndr dqpurswrrq

The essay or report will discuss the proposed development of NTRU public key encryption, highlighting its advantages over classical encryption methods and its security against quantum computing attacks. It will also explore the advancements in lattice-based cryptography and the applications of NTRU and its variations.

1. Introduction

1.1. Overview of NTRU Public Key Encryption

NTRU, a public-key cryptosystem introduced in 1996, has gained attention in the cryptographic community for its unique approach based on finding 'small' solutions to linear equations over polynomial rings. It offers exceptional speed in encryption and decryption operations, surpassing classical systems by several orders of magnitude, making it included in the IEEE P1363 industry standard for cryptography. NTRU is also considered a viable 'post-quantum' public-key encryption system due to its conjectured resistance to attacks by quantum computers, making it a promising alternative to established public-key cryptosystems. Its security is tied to challenging problems in lattice reduction, contributing to its robustness against potential attacks. Ongoing developments aim to address security issues and optimize computational complexity, with variants of NTRU proposed using different rings and cryptographic algorithms. Overall, NTRU brings forth innovative concepts and features that position it as an efficient and secure option for public-key encryption in contemporary cryptographic environments. See references: [1] p. 1-5, [5], [6] p. 1-5, [10], [12] p. 1-5.

1.2. Importance of NTRU in cryptography

NTRU Public Key Encryption is a significant player in cryptography, especially for wireless sensor networks and resource-constrained computing devices. It outperforms traditional systems like RSA and ECC in terms of efficiency and speed, making it suitable for energy conservation in WSNs. Its use of high-degree polynomial rings and homomorphic properties sets it apart from other encryption systems, allowing it to be used in various applications.

Despite initial challenges, NTRU has evolved with the introduction of variants that minimize computational complexity while maintaining security standards. Progress in lattice-based cryptography has also enhanced NTRU's resilience against potential quantum computing threats. Its asymptotic efficiency surpasses classical programs, and ongoing developments in multilinear techniques have further improved its capabilities.

NTRU's resistance to quantum computing attacks positions it as a promising "post-quantum" public-key encryption system. Recent advancements have addressed concerns about its computational complexity, instilling greater confidence in its effectiveness. Overall, NTRU's speed, efficiency, resistance to quantum attacks, and adaptability make it an appealing option for securing data in modern computing environments. See references: [1] p. 1-5, [3] p. 41-45, [10], [11], [22].

2. Background Information

2.1. Classical factorization- and discrete logarithm-based programs

Classical factorization- and discrete logarithm-based programs, such as RSA and ECC, are facing significant threats from the rise of quantum computers. Quantum algorithms like Peter Shor's have the potential to compromise the security provided by traditional methods. In response, post-quantum cryptography, particularly NTRU Public Key Encryption, has emerged as a heavily researched area due to its resilience against quantum attacks. The limitations of classical approaches have become apparent, and NTRU offers a promising alternative with near-optimal asymptotic efficiency advantages. Additionally, progress in lattice-based cryptography has opened up opportunities for NTRU's application in this field, providing a pathway to enhancing overall cybersecurity in the quantum era. Therefore, NTRU's integration into lattice-based cryptographic systems presents a solution for post-quantum security challenges. See references: [23] p. 16-20, [28], [31], [40].

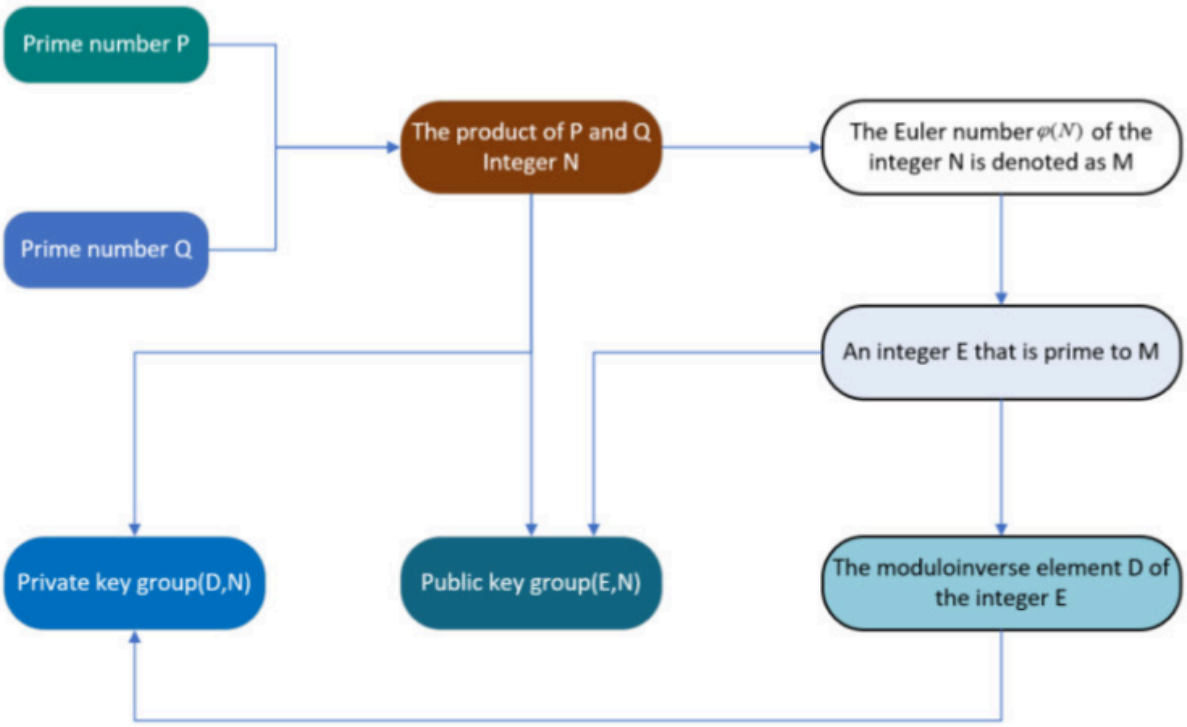

Figure 1: RSA algorithm key generation process. (source: reference [36])

2.2. Limitations of classical approaches

Classical methods of cryptography, such as RSA and Diffie-Hellman, depend on the complexity of calculating discrete logarithms over finite fields. However, the rise of quantum computers presents a significant risk to these traditional cryptographic techniques, as demonstrated by Peter Shor's quantum algorithm for efficient factorization and discrete logarithm problems. This has led to a demand for new cryptographic methods that can withstand quantum attacks.

The shortcomings of classical approaches are evident in their susceptibility to quantum computing attacks. The security of these systems is entirely based on empirical evidence and experimental assumptions, making it challenging to determine their effectiveness in the face of quantum computing. As a result, there is an urgent need for the development of post-quantum cryptography that can resist the potential threat posed by quantum computers.

NTRU, a public key cryptographic scheme based on lattice theory, has emerged as a promising alternative to classical methods due to its resistance against both classical and quantum attacks. Its underlying lattice problem is computationally difficult in the classical setting and remains secure in the quantum setting due to the absence of efficient quantum attacks against it. This makes NTRU an appealing option for post-quantum cryptography, providing a level of security that is necessary in the era of quantum computing.

In contrast to classical methods that are vulnerable to Shor's algorithm and other potential advances in quantum computing, NTRU offers a level of security that is not easily compromised by quantum attacks. As research continues in the field of post-quantum cryptography, NTRU's resilience against quantum threats positions it as a promising solution for ensuring secure communication and data protection in the future. See references: [7], [17], [23] p. 16-20, [37], [38] p. 31-35.

2.3. Introduction to NTRU as a substitute

NTRU, developed in 1996, is a promising encryption algorithm known for its resistance to quantum computer attacks and superior performance compared to ECC and RSA. It is reported to be 200 times faster than other public key encryption algorithms, making it suitable for use in cellular phones, smart cards, and RFIDs. However, it faces challenges related to computational complexity, which researchers are addressing through the exploration of traditional algorithms and parallel computation techniques. NTRU Prime 4591 761 has been developed as a public-key cryptosystem aiming for post-quantum security and offers several implementation advantages. Overall, NTRU shows promise as a fast and efficient public key cryptographic protocol with potential applications in IoT devices and embedded systems. See references: [22], [25] p. 1-5.

Name of algorithm	Lattice based	Integer based	(R)LWE	NTRU	Hard problem base
[]	\(\checkmark \)				Bounded distance decoding problem over ideal lattices and sparse subset sum problem for squashing the decryption circuit
[]		\(\checkmark \)			Approximate greatest common divisor
[]			\(\checkmark \)		Ring based learning with error
[]			\(\checkmark \)	\(\checkmark \)	RLWE and Decisional Small polynomial Ratio (DSPR) Assumption
[]			\(\checkmark \)		SWHE uses hardness of RLWE and Squashing step uses SSSP (Sparse subset sum problem)
[]	\(\checkmark \)				Shortest Independent Vector Problem
[]	\(\checkmark \)				Bounded distance decoding problem for SWHE, Sparse subset sum problem for bootstrapping
[]		\(\checkmark \)			Decisional approximate-GCD problem and error-free approximate GCD
[]			\(\checkmark \)		GapSVP
[]		\(\checkmark \)			Approximate-GCD problem

Name of algorithm	Lattice based	Integer based	(R)LWE	NTRU	Hard problem base
[]			\(\checkmark \)		Approximate Eigen vector method

Table 1: Fully homomorphic encryption schemes From: A systematic review of homomorphic encryption and its contributions in healthcare industry (source: reference [20])

3. The 1996 Proposal by Hoffstein, Pfeiffer, and Silverman

3.1. Overview of the proposal

The NTRU encryption system, introduced in 1996, is highly regarded within the cryptographic community for its nearly optimal efficiency and resistance to quantum computing attacks. It operates within finite polynomial rings and is linked to the computational difficulty of lattice problems, making it a potential alternative to traditional encryption schemes. NTRU is resilient against quantum attacks, setting it apart from RSA and ECC public key cryptosystems. It generates short, easily created keys, offers high speed, and low memory requirements, with practical security levels under known attacks. The blending system proposed by polynomial algebra and elementary probability theory contributes to its security. Variations of NTRU using other rings are being developed to further enhance its efficiency and resilience. Overall, the NTRU public key encryption system represents a significant advancement in cryptography with its potential resistance to quantum computing attacks and practical efficiency compared to traditional systems. See references: [2], [8] p. 1-5, [35] p. 1-5.

3.2. Key features and advantages of NTRU encryption

NTRU, introduced in 1996, is an encryption system attracting attention for its unique features. Unlike traditional systems, NTRU is based on finding "small" solutions to linear equations over polynomial rings, offering optimal efficiency and believed to be secure against quantum computing attacks. It is known for its speed and practicality, making it suitable for resource-constrained networks like IoT devices. Additionally, NTRU uses smaller key sizes while maintaining security, making it suitable for environments with limited memory and processing power. It is also resistant against various types of attacks, including those by quantum computers. Approved for standardization by IEEE, NTRU presents opportunities for researchers to explore more efficient variants for real-life applications. In summary, NTRU offers fast and efficient operations, resistance to attacks, smaller key sizes, and potential viability in the presence of large-scale quantum computers, positioning it as a promising candidate for post-quantum cryptography with practical applications in diverse environments. See references: [2], [4], [5], [7], [17].

3.3. Evaluation of the proposal's effectiveness

The introduction of the NTRU public key cryptosystem in 1996 by Hoffstein, Pfeiffer, and Silverman presented a fast and efficient alternative to traditional encryption schemes based on factorization or discrete logarithms. NTRU offers both encryption and digital signature, making it more efficient than widely used public-key cryptosystems like RSA, ECC, and El Gamal. Its resistance to quantum attacks positions it as a post-quantum cryptosystem, which is essential in the context of potential threats from quantum computing.

The security of NTRU is connected to the challenging task of finding a short vector in a high-dimensional lattice. This problem is believed to have no polynomial time algorithm for its solution. Despite lacking a security proof, extensive analysis and evaluation by renowned cryptographers such as Don Coppersmith, Johan Hastad, Andrew Odlyzho, and Adi Shamir have demonstrated the system's security. After over 20 years of scrutiny, no concrete approach to exploit NTRU's algebraic structure has been discovered.

NTRU was named a finalist in the 3rd round of the Post-Quantum Cryptography Standardization project due to its nearly optimal asymptotic efficiency advantages compared to traditional schemes. Furthermore, advancements in lattice-based cryptography have further established its importance in the field. The system has also seen progress in multilinear techniques for encryption systems.

In conclusion, the proposal for the development of NTRU Public Key Encryption has proven effective through its resistance to quantum attacks, nearly optimal asymptotic efficiency advantages, and ongoing progress within lattice-based cryptography. See references: [1] p. 1-5, [6] p. 16-17, [8] p. 1-5, [23] p. 11-15, [30].

4. Security Analysis of NTRU Encryption System

4.1. Examination of computational challenges on finite polynomial rings

NTRU Public Key Encryption, introduced in 1996 by Hoffstein, Pfeiffer, and Silverman, emerged as a promising alternative to traditional encryption schemes based on factorization or discrete logarithms. The system has garnered praise for its exceptional asymptotic performance and purported resistance to quantum computers. However, the computational challenges posed by finite polynomial rings present significant obstacles to the overall security and efficiency of NTRU.

One of the fundamental computational challenges is the complexity of polynomial multiplication and vector multiplication within the NTRU algorithm. Addressing these complexities has involved the utilization of traditional algorithms such as NTT, Montgomery, CRT, and Karatsuba. Additionally, researchers have explored parallel implementation on multi-core processors to mitigate performance slowdowns.

Security analysis of the NTRU encryption system also presents a challenge. While it shows approximate security against quantum computing attacks, further evaluation is necessary to ensure its robustness in the face of evolving quantum threats.

Furthermore, researchers have focused on the asymptotic efficiency of NTRU encryption system. Comparative analysis with factorization- and discrete logarithm-based programs has highlighted near-optimal asymptotic efficiency advantages of NTRU encryption, making it a compelling option for applications requiring fast encryptions and low storage requirements.

In conclusion, while NTRU Public Key Encryption offers significant advantages over classical encryption schemes, addressing the computational challenges on finite polynomial rings is essential to enhance its overall security and efficiency. See references: [13] p. 11-15, [17], [22], [29].

4.2. Evaluation of statistical challenges on finite polynomial rings

The hurdles posed by finite polynomial rings in the NTRU encryption system are crucial for ensuring its security and efficiency. The changes made to the NTRU encryption scheme have resulted in a key generation algorithm that is notably simpler and more efficient, overcoming the limitations of traditional factorization- and discrete logarithm-based programs. This has enabled the achievement of 128 bits of post-quantum security while eliminating the risk of decryption failures. The conversion of the OW-CPA-secure scheme into a CCA2-secure KEM in the quantum-accessible random oracle model has further bolstered its security features. The significance of attaining CCA2 security for an NTRU-based public key encryption scheme lies in its versatility as a foundational component for various cryptographic applications.

The resilience of the NTRU encryption system against quantum computing attacks is particularly noteworthy. Its approximate security against such attacks is a major advantage, enhancing its potential as an attractive alternative to factorization- and discrete-log based encryption schemes. The superior asymptotic efficiency advantages of the NTRU encryption system, compared to other programs, underscore its suitability for real-world applications.

Furthermore, progress in lattice-based cryptography has contributed to boosting the security and efficiency of the NTRU encryption system. The integration of multilinear techniques for encryption systems has further enhanced the performance and applicability of NTRU.

Overall, the statistical challenges related to finite polynomial rings in the NTRU encryption system have been effectively tackled through strategic modifications and advancements in cryptography. These developments have significantly improved the security, efficiency, and versatility of NTRU as a public key encryption scheme. See references: [16] p. 1-5, [18], [25] p. 1-5, [29].

5. Quantum Computing Assaults on NTRU Encryption System

5.1. Understanding quantum computing attacks on classical encryption systems

The rise of quantum computing poses a significant threat to traditional encryption systems, which rely on computational problems that quantum computers can solve much more quickly. To address this, it is essential to develop "quantum-safe"

or post-quantum encryption algorithms. The NIST has begun the process of standardizing such algorithms, with lattice-based cryptography, including the NTRU public key encryption system, showing promise. NTRU has been researched extensively and is considered resilient against quantum attacks while also exhibiting quick implementation and smaller key sizes. Its versatility and potential for safeguarding information from quantum computing attacks make it a strong candidate for post-quantum cryptography. As research in this field progresses, NTRU could play a crucial role in ensuring data security in the age of quantum computing advancements. See references: [7], [9] p. 1-5, [33].

5.2. Approximate security provided by NTRU against quantum computing assaults

NTRU Public Key Encryption is often regarded as one of the most viable "post-quantum" public-key encryption systems, believed to be resistant to attacks by quantum computers. Shor's 1997 demonstration revealed that quantum computers can efficiently solve discrete logarithms and factor large integers, creating vulnerabilities in systems like RSA, ECC, and El Gamal against quantum attacks. This emphasizes the necessity for new encryption algorithms capable of withstanding both classical and quantum computing attacks.

The security of NTRU is linked to the challenging problem of lattice reduction called the shortest vector problem (SVP), with the conjecture that there is no polynomial-time algorithm to solve this problem. This positions NTRU as a promising alternative to more established public key cryptosystems and resistant to quantum computing-based attacks.

Furthermore, NTRU has been extensively researched for its resistance to quantum computer-based attacks. Its smaller key sizes and speed make it suitable for applications with limited memory and processing power. It is considered secure against various types of attacks, such as lattice basis reduction and chosen ciphertext attacks. As a result, NTRU provides approximate security against quantum computing assaults due to its resistance to both classical and quantum computing-based attacks. See references: [1] p. 1-5, [6] p. 1-5, [13] p. 16-20, [22].

6. Asymptotic Efficiency of NTRU Encryption System

6.1. Comparative analysis with factorization- and discrete logarithm-based programs

The potential of NTRU encryption in modern cryptography is undeniably strong. In contrast to RSA and ECC, which rely on factorization and discrete logarithms, NTRU stands out for its superior speed and key generation. In fact, NTRU encryption is approximately 1.5 times faster than ECC, with key creation taking 300 times less time than RSA, and encryption and decryption processes being significantly quicker. The efficiency of NTRU can be attributed to its algorithmic steps and the use of finite polynomial rings.

NTRU's security analysis involves tackling computational challenges on finite polynomial rings as well as evaluating statistical challenges. Moreover, the system provides approximate security against quantum computing attacks, setting it apart from traditional encryption systems that may be susceptible to such assaults.

Recent advancements in lattice-based cryptography have expanded the potential applications and variations of NTRU. The flexibility in implementing different types of fields and rings based on various structures has opened up new avenues for researchers to explore more efficient NTRU schemes for real-life applications.

Furthermore, the introduction of multilinear techniques for NTRU has further improved the encryption system's performance. These techniques offer enhanced parallelism, increasing the speed of encryption/decryption processes without compromising security levels.

In conclusion, when comparing NTRU with factorization- and discrete logarithm-based programs, it becomes evident that NTRU offers near-optimal asymptotic efficiency advantages. Its combination of speed, security against quantum computing attacks, and ongoing advancements in lattice-based cryptography makes it a compelling choice for the future of public key encryption. See references: [4], [11], [27], [39].

6.2. Near-optimal asymptotic efficiency advantages of NTRU encryption

NTRU public key encryption presents near-optimal efficiency advantages in the long term, positioning itself as a potential option for post-quantum cryptography. With easily computable private and public keys of O(N) length, NTRU stands out for its rapidity and minimal memory requirements. The process of encrypting and decrypting with NTRU only requires O(N^2) operations, significantly quicker than both RSA and ECC. While there are other classical cryptosystems resistant to quantum attacks, such as McEliece, NTRU's simplicity and resilience against both classical and quantum computers make it a strong

contender to replace current constructions. The security of NTRU relies on the complexity of the Shortest Vector Problem in lattice reduction, for which no polynomial-time solution is currently known. Amidst the ongoing research focus on post-quantum cryptography, lattice-based schemes like NTRU have attracted considerable interest due to their promising security, communication bandwidth, and computational efficiency. Despite its potential, challenges related to standardization and interoperability persist. Notably, NTRU has proven resilient against attacks and cryptanalysis for over 26 years. As a finalist in the NIST PQC standardization contest, NTRU continues to play a crucial role in providing secure functionalities in systems connected through public networks. See references: [13] p. 16-20, [19] p. 1-5, [23] p. 1-5, [24], [28].

7. Current Advancements in Lattice-Based Cryptography

7.1. Explanation and significance of lattice-based cryptography

Lattice-based cryptography has emerged as a beacon of hope in the realm of post-quantum encryption. With the looming threat of quantum computing, lattice-based schemes have garnered substantial attention from researchers. NTRU, an encryption system based on lattices introduced by Hoffstein, Pipher, and Silverman in 1996, has demonstrated its resilience against attacks and cryptanalysis for over 26 years.

The computational complexity inherent in lattice-based cryptography is a key factor driving interest in this approach, providing a robust foundation for security. The NTRU encryption scheme and the BLISS signature are believed to be linked to the closest vector problem (CVP) in a lattice, which is known to be NP-hard. This computational complexity makes lattice-based schemes like NTRU resistant to assaults from quantum computing.

In addition to its formidable security properties, NTRU also offers near-optimal asymptotic efficiency advantages when compared to other classical encryption systems. Its simplicity and efficiency make it easier to build robust cryptographic functionalities such as multilinear maps and multikey homomorphic properties.

Moreover, recent advancements in lattice-based cryptography have given rise to variations of NTRU, such as NTRU Prime, with the aim of reducing attack surface at low cost without compromising security.

The significance of lattice-based cryptography lies in its potential to provide secure and efficient cryptographic solutions that are resistant to quantum computing attacks. As quantum computing continues to progress, the importance of developing and standardizing post-quantum cryptographic algorithms based on lattices, such as NTRU, becomes increasingly evident. See references: [9] p. 1-5, [18], [24].

7.2. Security studies revolving around lattice-based cryptography

Lattice-based cryptography has risen to prominence as a beacon of hope in the realm of post-quantum encryption. With the looming threat of quantum computing, lattice-based schemes have garnered substantial attention from researchers. NTRU, an encryption system based on lattices introduced by Hoffstein, Pipher, and Silverman in 1996, has demonstrated its resilience against attacks and cryptanalysis for over 26 years.

The computational complexity inherent in lattice-based cryptography is a key factor driving interest in this approach, providing a robust foundation for security. The NTRU encryption scheme and the BLISS signature are believed to be linked to the closest vector problem (CVP) in a lattice, which is known to be NP-hard. This computational complexity makes lattice-based schemes like NTRU resistant to assaults from quantum computing.

In addition to its formidable security properties, NTRU also offers near-optimal asymptotic efficiency advantages when compared to other classical encryption systems. Its simplicity and efficiency make it easier to build robust cryptographic functionalities such as multilinear maps and multikey homomorphic properties.

Moreover, recent advancements in lattice-based cryptography have given rise to variations of NTRU, such as NTRU Prime, with the aim of reducing attack surface at low cost without compromising security.

The significance of lattice-based cryptography lies in its potential to provide secure and efficient cryptographic solutions that are resistant to quantum computing attacks. As quantum computing continues to progress, the importance of developing and standardizing post-quantum cryptographic algorithms based on lattices, such as NTRU, becomes increasingly evident. See references: [7], [15] p. 1-5, [18], [21] p. 1-5, [25] p. 1-5, [26], [32], [34], [36].

7.3. Applications and variations of NTRU in lattice-based cryptography

NTRU has undergone various advancements and variations within the realm of lattice-based cryptography. One notable example is NTRU Prime, which aims to decrease vulnerability by utilizing rings without specific structures targeted by recent attacks on ideal-lattice-based cryptosystems. This optimization has led to the creation of Streamlined NTRU Prime, a public-key cryptosystem that provides high-security post-quantum parameters at a minimal cost in terms of sizes and speeds. The application of NTRU in SCADA security standards has also been explored, with the objective of enhancing performance through the use of the faster and lightweight NTRU public key algorithm for end-to-end security.

Moreover, different variants of NTRU have been developed to operate with various rings and structures. These include NTRU variants that work with polynomials within more complex structures, such as square matrices of polynomials or non-commutative rings. Additionally, an NTRU-like cipher known as ITRU was proposed over the ring of integers, offering an alternative model for encryption that deviates from the traditional NTRU model.

Recent research has suggested that NTRU may possess more secure properties than other lattice-based algorithms. It has been acclaimed for its near-optimal asymptotic efficiency advantages when compared to other factorization- and discrete logarithm-based programs. As part of ongoing advancements in lattice-based cryptography, there has been a focus on multilinear techniques for encryption systems, including the development and applications of multilinear techniques in NTRU.

Overall, these developments showcase the adaptability and versatility of NTRU within lattice-based cryptography, with current research centered on optimizing its security properties while minimizing computational complexity. See references: [10], [25] p. 1-5, [29].

#	RCPKC Parameter	2×k		
		224	336	448
1	mgLen	225	337	450
2	qLen	473	743	909
3	f=2qLen−mgLen−1−1	2.26×1074	8.26×10121	7.44×10137
4	*g*	2mgLen−1=	2mgLen−5=	2mgLen−11=
		5.39×1067	2.79×10101	2.90×10135
5	rmax	2.26×1074	8.26×10121	7.44×10137
6	max(α·2qLen/2,rmin)	7.41×1072	1.62×10119	1.10×10137
7	CRCPKC(r,k)	2.1×1074	8.24×10121	6.34×10137

Table 2: Width of the range for the r value for different security levels (Row 7); the parameters of the random congruential public key cryptosystem (RCPKC) affecting the width (m g L e n, q L e n, f, g, r m a x, m a x (2 q L e n / 2, r m i n)) are specified in Rows 1-6. (source: reference [10])

8. Advancements in Multilinear Techniques for NTRU

8.1. Introduction to multilinear techniques for encryption systems

The realm of lattice-based cryptography has witnessed substantial progress in multilinear techniques for encryption systems. The advent of bilinear maps, also referred to as pairings, in public-key cryptography has introduced new

opportunities for applications such as non-interactive key agreement protocols and identity-based encryption. Over time, researchers have endeavored to generalize these concepts into multilinear maps, with an emphasis on achieving functionality that surpasses traditional bilinear maps.

A significant milestone in this domain was proclaimed in 2012 by Garg, Gentry, and Halevi, who demonstrated that a functionality equivalent to multilinear maps could be attained using a variant of the NTRU encryption scheme. This advancement has paved the way for exploring the cryptographic implications of multilinear maps and their potential applications.

The simplicity of the NTRU system has endowed it with potential efficiency advantages compared to other lattice-based systems. For instance, unlike other known public-key encryption schemes based on the Ring-LWE problem, NTRU ciphertexts consist of just a single ring element. This simplicity not only contributes to efficiency but also facilitates the construction of powerful cryptographic functionalities such as multilinear maps and multikey homomorphic properties.

Furthermore, recent developments have indicated that NTRU has the potential to unify the field of lattice-based cryptography by demonstrating that its security can be based on the same foundations as more recent lattice-based schemes. This unification opens up avenues for exploring new computational problems on polynomial rings and understanding how security can be achieved based on these foundations.

In conclusion, the utilization of multilinear techniques in NTRU encryption systems presents an exciting direction for advancing both the theoretical underpinnings and practical applications of lattice-based cryptography. See references: [1] p. 26-30, [17], [20].

8.2. Development and applications of multilinear techniques in NTRU

In recent years, there has been a strong focus on advancing and applying multilinear techniques in the realm of NTRU public key encryption. These techniques have unlocked a new range of applications, such as non-interactive multiparty key agreement, and have enabled the addition of powerful new functionalities to the basic cryptosystem. A notable recent development is the introduction of an NTRU-based Fully Homomorphic Encryption (FHE) scheme, which allows for useful computation on encrypted messages. Another significant advancement is the creation of NTRU-based multilinear maps, which has expanded the potential applications of NTRU cryptography. Additionally, there have been generalizations of NTRU that utilize higher degree algebraic rings to replace the integer ground ring in NTRU, broadening the scope of its applicability.

The efficiency advantages of multilinear techniques in NTRU encryption are clearly demonstrated when compared to other known lattice-based systems. For instance, unlike other known public-key encryption schemes based on the Ring-LWE problem, NTRU ciphertexts consist of just a single ring element.

These advancements represent a crucial step forward in both the security analysis and applications of the NTRU cryptosystem and its variations. The simplicity and potential efficiency advantages indicate that there is significant potential for further progress in this dynamic field. See references: [1] p. 21-25, [10].

9. Conclusion

9.1. Recapitulation of the key points discussed

In summary, NTRU Public Key Encryption has established itself as a highly effective and secure protocol, particularly within the realm of post-quantum cryptography. Its utilization of polynomial multiplication as the fundamental operation and its blending system grounded in elementary probability theory render it a swift and readily implementable solution, with minimal memory requirements. NTRU has been applied in specific commercial scenarios where rapidity is a priority, rendering it well-suited for applications necessitating swift encryption and decryption, such as in IoT devices or embedded systems.

Furthermore, NTRU employs smaller key sizes compared to other public key cryptosystems, maintaining an equivalent level of security while being conducive for environments with restricted memory and processing capabilities. The protocol is structured to withstand various forms of attacks, including those by quantum computers, positioning it as a formidable contender for the quantum era. However, NTRU's lack of widespread usage or standardization in the industry complicates the evaluation of its interoperability with other cryptosystems.

Despite this obstacle, NTRU continues to be a significant player in the realm of lattice-based cryptography and holds promising potential for future advancements. See references: [7], [14] p. 1-5, [17], [24].

9.2. Future prospects and potential developments in the field

NTRU public key encryption offers promising prospects for post-quantum cryptography due to its short keys, high speed, and low memory requirements. It is considered the most viable option in the post-quantum era, with recent developments further enhancing its security. As we move towards integrating classical and quantum systems, NTRU encryption remains secure against both types of computers. Advancements in lattice-based cryptography and proposed variations like QOTRU show promise for further development of NTRU encryption. Efforts to secure classical communication channels with quantum devices will contribute to a more secure future for quantum computing. Overall, ongoing advancements and efforts to address security concerns indicate great potential for the future of NTRU public key encryption. See references: [1] p. 1-5, [7], [9] p. 6-10, [14] p. 1-5, [23] p. 1-5.

References

1. "~rste NTRU survey.pdf". May 2014. users.monash.edu.au. [Online]. Available: https://users.monash.edu.au/~rste/NTRU_survey.pdf
2. R. Steinfeld. "NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings". Aug 2014. [Online]. Available: https://www.degruyter.com/document/doi/10.1515/9783110317916.179/html
3. A. P. Premnath. "Application of NTRU Cryptographic Algorithm for securing SCADA communication". Mar 2023. [Online]. Available: https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=3019&context=thesesdissertations
4. S. Singh and S. Padhye. "Generalisations of NTRU cryptosystem". Nov 2016. [Online]. Available: https://www.researchgate.net/publication/310471906_Generalisations_of_NTRU_cryptosystem
5. L. Miao, X. Zhou, H. Xu and L. Shuai. "A Group-based NTRU-like Public-key Cryptosystem for IoT". Jun 2019. [Online]. Available: https://www.researchgate.net/publication/333643563_A_Group-based_NTRU-like_Public-key_Cryptosystem_for_IoT
6. A. Nitaj. "The Mathematics of the NTRU Public Key Cryptosystem". Jul 2016. [Online]. Available: https://core.ac.uk/download/pdf/237332188.pdf
7. Savvas, Ilias K., D. Poulakis, Makris, Georgios C., Sabani, Maria E. and G. Garani. "Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era". Jan 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/12/2643
8. "The Mathematics of the NTRU Public Key Cryptosystem". Jul 2016. [Online]. Available: https://nitaj.users.lmno.cnrs.fr/ntru3final.pdf
9. "Success_Jimoh_Internship_Report". Dec 2021. [Online]. Available: https://norma.ncirl.ie/6008/1/successdaodujimoh.pdf
10. A. Al-Khasawneh, A. Chefranov, Joel J. P. C. Rodrigues, Y. Daraghmi, N. Hamad and A. Ibrahim. "NTRU-Like Random Congruential Public-Key Cryptosystem for Wireless Sensor Networks". Aug 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7472001/
11. D. Nunez, J. Lopez and I. Agudo. "NTRUReEncrypt: An efficient proxy re-encryption scheme based on NTRU". Apr 2015. [Online]. Available: https://www.researchgate.net/publication/283667970_NTRUReEncrypt_An_efficient_proxy_re-encryption_scheme_based_on_NTRU
12. "1". May 2020. [Online]. Available: https://mscr.org.my/data/journal/journal-20200507123724.pdf
13. Maria E. Sabani, Ilias K. Savvas, Dimitrios Poulakis, Georgia Garani and Georgios C. Makris. "Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era". Jun 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/12/2643/pdf
14. "NTRU: A ring-based public key cryptosystem". Jul 2006. [Online]. Available: https://www.ntru.org/f/hps98.pdf
15. "Towards Secure Classical-Quantum Systems". Apr 2023. [Online]. Available: https://www.cise.ufl.edu/research/cad/Publications/host23.pdf

16. "High-speed key encapsulation from NTRU". Aug 2017. [Online]. Available: https://ntru.org/f/ntrukem-20170828.pdf
17. G. Garani, Ilias K. Savvas, D. Poulakis, Maria E. Sabani and Georgios C. Makris. "Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era". Jun 2023. [Online]. Available: https://www.researchgate.net/publication/371554854_Evaluation_and_Comparison_of_Lattice-Based_Cryptosystems_for_a_Secure_Quantum_Computing_Era
18. "Post-quantum cryptography - Wikipedia". Jan 2024. [Online]. Available: https://en.wikipedia.org/wiki/Post-quantum_cryptography
19. Santiago Sanchez-Solano, Eros Camacho-Ruiz, Macarena C. Martinez-Rodriguez and Piedad Brox. "Multi-Unit Serial Polynomial Multiplier to Accelerate NTRU-Based Cryptographic Schemes in IoT Embedded Systems". Mar 2022. [Online]. Available: https://digital.csic.es/bitstream/10261/336933/1/multiunitsyst.pdf
20. R. Bhatia and K. Munjal. "A systematic review of homomorphic encryption and its contributions in healthcare industry". Aug 2023. [Online]. Available: https://link.springer.com/article/10.1007/s40747-022-00756-z
21. "i". Nov 2022. [Online]. Available: https://arxiv.org/pdf/2203.09620
22. Ahmed, Hassan I. Sayed, Abdallah, Mohamed S., Aslan, Heba K., G. Elkabbany and Y. Cho. "Lightweight Computational Complexity Stepping Up the NTRU Post-Quantum Algorithm Using Parallel Computing". (accessed Jan 23, 2024). [Online]. Available: https://www.mdpi.com/2073-8994/16/1/12
23. "FACULDADE DE CIENCIAS DEPARTAMENTO DE MATEMATICA". Jun 2017. [Online]. Available: https://repositorio.ul.pt/bitstream/10451/28303/1/ulfc121698_tm_Rafael_Monteiro.pdf
24. "Compact and efficient KEMs over NTRU lattices". Apr 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0920548923001095
25. "NTRU Prime: reducing attack surface at low cost". Aug 2017. [Online]. Available: https://ntruprime.cr.yp.to/ntruprime-20170816.pdf
26. A. Karbasi. "ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices". Jan 2015. [Online]. Available: https://www.academia.edu/68428937/ILTRU_An_NTRU_Like_Public_Key_Cryptosystem_Over_Ideal_Lattices
27. C. Lee, J. H. Cheon and J. Jeong. "An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero". Aug 2016. [Online]. Available: https://www.researchgate.net/publication/307087594_An_algorithm_for_NTRU_problems_and_cryptanalysis_of_the_GGH_multilinear_map_without_a_low-level_encoding_of_zero
28. P. Brox, S. Sanchez-Solano, Martinez-Rodriguez, Macarena C. and E. Camacho-Ruiz. "Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems". Jun 2023. [Online]. Available: https://www.mdpi.com/2410-387X/7/2/29
29. Juliet N. Gaithuru and M. Bakhtiari. "Insight into the operation of NTRU and a comparative study of NTRU, RSA and ECC public key cryptosystems". Dec 2014. [Online]. Available: https://www.researchgate.net/publication/287719777_Insight_into_the_operation_of_NTRU_and_a_comparative_study_of_NTRU_RSA_and_ECC_public_key_cryptosystems
30. "NTRU - Wikipedia". Sep 2023. [Online]. Available: https://en.wikipedia.org/wiki/NTRU
31. A. Thompson, G. Arome, B. K. Alese and H. C. Ukwuoma. "Post-quantum cryptography-driven security framework for cloud computing". Jan 2022. [Online]. Available: https://www.degruyter.com/document/doi/10.1515/comp-2022-0235/html?lang=en
32. C. Gentry and M. Szydlo. "Cryptanalysis of the Revised NTRU Signature Scheme". Apr 2002. [Online]. Available: https://www.researchgate.net/publication/221348160_Cryptanalysis_of_the_Revised_NTRU_Signature_Scheme
33. "Post-quantum cryptography Algorithm's standardization and performance analysis". Sep 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590005622000777
34. M. Perepechaenko and R. Kuang. "A novel homomorphic polynomial public key encapsulation algorithm". Oct 2023. [Online]. Available: https://f1000research.com/articles/12-1347
35. "hubfs files ntru-orig.pdf". Jun 2005. web.securityinnovation.com. [Online]. Available: https://web.securityinnovation.com/hubfs/files/ntru-orig.pdf
36. J. Liao, C. Kuang, W. Liang, N. Xiong, L. Chen, K. Li, S. Li and Y. Chen. "Post-Quantum Security: Opportunities and Challenges". Nov 2023. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10648643/
37. "Computational Cryptography: Algorithmic Aspects of Cryptology [1 ed.] 1108795935, 9781108795937 - EBIN.PUB". (accessed Jan 23, 2024). [Online]. Available:

https://ebin.pub/computational-cryptography-algorithmic-aspects-of-cryptology-1nbsped-1108795935-9781108795937.html

38. "CRYPTOGRAPHY". May 2021. [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/@@download/fullReport
39. J. Hermans, B. Preneel and F. Vercauteren. "Speed records for NTRU". Dec 2010. [Online]. Available: https://www.researchgate.net/publication/221208343_Speed_records_for_NTRU
40. D. Xiao, A. Wang and Y. Yu. "Lattice-based cryptosystems in standardisation processes: A survey". Mar 2023. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ise2.12101