International Journal of Advanced Research in Engineering Technology & Science ISSN: 2349-2819
Email: editor@ijarets.org Volume-10 Issue-1 January-2023 www.ijarets.org

A PUBLIC KEY CRYPTOSYSTEM USING NUMBER-THEORETIC TRANSFORMS FOR SECURE COMMUNICATION

Md Jabir Hussain
Ph.D. Scholar
Department of Mathematics
Malwanchal University Indore, (M.P.).

Dr. Kulbir Singh
Supervisor
Department of Mathematics
Malwanchal University Indore, (M.P.).

ABSTRACT

Public key cryptosystems are fundamental to secure digital communication, but traditional models like RSA and ECC face limitations in efficiency and resistance to emerging cryptographic threats. This study proposes a novel public key cryptosystem leveraging number-theoretic transforms (NTT) to enhance security and computational efficiency in secure communication. The research explores the mathematical foundations of NTT and integrates them into encryption and decryption processes to strengthen resistance against factorization-based and quantum attacks. A comparative analysis with RSA and ECC demonstrates improved encryption speed, reduced computational overhead, and enhanced security. The proposed system is evaluated in both end-to-end and group communication scenarios, ensuring its robustness against key recovery attacks and cryptanalysis. Security validation through reduction techniques and mathematical proof further establishes its reliability. The findings contribute to the advancement of cryptographic security by introducing an efficient and scalable alternative to traditional public key systems. The study also discusses practical applications in secure digital transactions, enterprise security, and government communications. Future research directions include optimizing the scheme for post-quantum security and real-world implementation. The proposed cryptosystem offers a promising solution for modern cryptographic challenges, ensuring long-term data protection in an evolving digital landscape.

Keywords: *Public Key Cryptosystem, Number-Theoretic Transforms (NTT) etc.*

INTRODUCTION

Cryptography has existed since ancient times, where simple encryption methods were used to hide messages. The Caesar cipher, used by Julius Caesar, is the first known cipher that shifted letters to aid in secrecy. As time passed, cryptographic techniques evolved, leading to more complex systems like polyalphabetic ciphers and digital encryption methods developed in the 20th and 21st centuries. With computers, encryption grew more complicated, utilizing asymmetric techniques, hash functions, and quantum-resistant encryption. Number theory, the mathematical study of integers, is vital for many cryptographic algorithms and helps maintain the security of these systems by relying on difficult number-theoretic problems, such as integer factorization and the discrete logarithm problem. Key number theory concepts in cryptography include prime numbers, modular arithmetic, the greatest common divisor (GCD), and the Chinese Remainder Theorem. Prime numbers are crucial due to their properties and difficulty in factorization, as seen in the RSA algorithm, which creates a public key from two large prime numbers. Various modern cryptographic algorithms depend on these number-theoretic principles, including RSA,

Diffie-Hellman Key Exchange, and Elliptic Curve Cryptography. These algorithms are used across many fields, such as secure communication (like HTTPS), data integrity with digital signatures, blockchain technologies, password protection, and ongoing efforts for quantum-resistant cryptography.

Research Aim

To develop a public key cryptosystem based on number-theoretic transforms (NTT) that ensures robust security for end-to-end and group communication while maintaining computational efficiency.

Research Objectives

- To establish security requirements for end-to-end and group communication in cryptographic systems.
- To design a public key cryptosystem using number-theoretic transforms for improved security and efficiency.

Research Questions

1. What are the essential cryptographic principles that must be satisfied to ensure secure end-to-end and group communication?
2. How can number-theoretic transforms be leveraged to develop a more secure and efficient public key cryptosystem?
3. What mathematical techniques can be used to validate the robustness of the proposed cryptosystem against cryptographic attacks?
4. How does the proposed cryptosystem perform in comparison to conventional encryption schemes such as RSA and ECC in terms of computational efficiency and security?

Research Gap

While existing public key cryptosystems such as RSA and ECC provide secure encryption, they face challenges related to computational efficiency, scalability, and vulnerability to emerging cryptographic attacks, including post-quantum threats. Most traditional cryptosystems rely on factorization or discrete logarithm problems, which are becoming increasingly susceptible to advanced computational techniques. The integration of number-theoretic transforms (NTT) in cryptographic security has been explored in limited contexts, but its full potential in public key cryptosystems remains under-researched. There is a lack of comprehensive studies that evaluate the security, efficiency, and real-world applicability of NTT-based cryptosystems in secure communication. This research aims to bridge this gap by developing and analyzing a novel NTT-based cryptographic model for enhanced security.

LITERATURE REVIEW

Md. Helal Ahmed (2021) Among the most important goals in assessing ICT are maintaining user privacy and the system's integrity. We present an arithmetic method for developing asymmetric key cryptography

in this chapter. Foundational to our approach is the construction of cyclotomic matrices that map to a diophantine system. A one-way function design method used in cyclotomic matrices. While the output of a one-way function may be efficiently computed, processing its inverse might be challenging without knowing privileged knowledge about the hidden input. In addition, we prove that the asymptotic complexity of Oe2.373 is sufficient for efficient encryption and decryption. As a last step, we analyse the cryptosystem's mathematical complexity.

Michel Waldschmidt (2008) On the one hand, the linkages between classical arithmetic and modern ways for achieving a greater security of data transmission are among the surprising elements of recent breakthroughs in technology. On the other hand, these connections are among the technologies that have been overlooked. In order to highlight this particular facet of the topic, we shall demonstrate how contemporary cryptography is connected to our own understanding of certain characteristics of natural numbers. As an example, we show how prime numbers play a significant role in the procedure which enables you to withdraw safely from your bank account using ATM (Automated Teller Machines) with your private PIN (Personal Identification Number) code.

Wayne Patterson (2007) Divisibility, multiplicative functions, congruences, residues, prime numbers, Diophantine equations, and elliptic curves are some of the fundamental subjects that are covered in this article, which provides an introduction to number theory from a computational point of view. This paper investigates the crucial function that number theory plays in cryptographic systems, despite the fact that it has historically been considered a pure area of mathematics. Number theory has found important applications in technologically advanced computer security. The Data Encryption Standard (DES), public-key cryptosystems, and the Rivest–Shamir–Adleman (RSA) cryptosystem are some of the examples of the practical implementations of number-theoretic concepts in encryption and security protocols that are discussed in this work.

Draft Copy (2003) Cryptography is a specialized branch of applied mathematics focused on developing schemes and formulas to enhance the privacy, security, and integrity of communications through the use of codes. It enables users, including governments, military organizations, businesses, and individuals, to protect sensitive information from unauthorized access, ensuring confidentiality in data exchange. The primary objective of any cryptographic scheme is to be resistant to cracking, meaning only authorized recipients should be able to decode and interpret the encrypted information. Beyond confidentiality, cryptography also plays a crucial role in preserving data integrity, preventing unauthorized alterations, and safeguarding information from tampering or malicious modifications.

Alessandro Languasco (2003) The editors, or the publishing house, translated from the Italian this paper in an amateurish way; for example they inserted several mathematical typos: on p.3 the limit for pi(x) over x/log x is 1, the definition of the Riemann zeta function as a series holds for Re(s)>1; the same for Euler's product on p.4. I inserted more corrections as annotations. This translation was published without the final authors' approval] On the one hand, the study of numbers – and especially of prime numbers – has fascinated mathematicians since ancient times; on the other hand, humans have always felt the need for security in the transmission of information.

RESEARCH METHODOLOGY

A well-structured research design is essential in cryptographic studies, particularly when evaluating algorithmic security, computational efficiency, and mathematical robustness. The nature of cryptographic research demands a methodology that ensures rigorous empirical testing, algorithmic validation, and security proofing. This study adopts an experimental research design, as it provides a framework for systematically investigating the performance, computational complexity, and security strength of cryptographic algorithms.

Cryptographic algorithms are built upon well-established mathematical principles, requiring precise validation through controlled experiments rather than exploratory analysis. While exploratory research is useful in theoretical studies, it lacks the empirical depth necessary for cryptographic evaluation. The experimental research design, in contrast, allows for the quantitative measurement of algorithmic performance, security resilience, and computational efficiency, making it the most suitable approach for this study. By leveraging mathematical modeling, algorithm benchmarking, and formal security proofs, this research aims to demonstrate the robustness and real-world applicability of the proposed cryptographic schemes.

A fundamental requirement for modern cryptographic protocols is provable security, which ensures that an algorithm's security properties are formally verifiable through mathematical proofs. This study employs reductionist security proofs, indistinguishability-based arguments, and game-theoretic models to validate the robustness of the proposed cryptographic algorithms.

Reductionist security proofs involve demonstrating that breaking the cryptographic scheme is equivalent to solving a well-known computationally hard problem. For example, the security of the proposed elliptic curve signature scheme is proven by reducing the ability to forge a valid signature to solving the elliptic curve discrete logarithm problem (ECDLP). By establishing these security reductions, this research ensures that the proposed cryptographic schemes are as secure as the underlying number-theoretic problems they rely on.

In addition to formal mathematical reductions, this study employs indistinguishability-based security models to evaluate the resistance of cryptographic protocols against attacks. Indistinguishability ensures that an adversary cannot distinguish between encrypted messages under chosen-plaintext attack (CPA) and chosen-ciphertext attack (CCA) scenarios. The security proofs in this study incorporate game-based models, where adversaries interact with the cryptographic system under predefined constraints, allowing for a structured evaluation of cryptographic strength.

Finally, the cryptographic schemes are evaluated against common cryptanalytic attacks, including side-channel attacks, lattice-based attacks, and quantum adversarial models. This ensures that the proposed algorithms remain secure in both classical and post-quantum computing environments. By integrating provable security methodologies, this research provides rigorous mathematical justifications for the security guarantees offered by the proposed cryptographic schemes.

The research approach adopted in this study is deeply rooted in mathematical and algorithmic principles, ensuring that the proposed cryptographic schemes achieve strong security guarantees, computational efficiency, and resistance to adversarial attacks. By leveraging number-theoretic foundations such as the

Chinese Remainder Theorem, primitive root exponentiation, and elliptic curve cryptography, this study constructs cryptographic protocols that are both secure and computationally optimized

Through computational complexity analysis, the study evaluates the difficulty of breaking the proposed algorithms, ensuring that their security is grounded in integer factorization and discrete logarithm problems. Furthermore, provable security methods are employed to formally validate the security properties of the cryptographic schemes, using reductionist techniques, indistinguishability arguments, and game-based security models.

By integrating mathematical rigor, algorithmic efficiency, and formal security proofs, this research establishes a comprehensive framework for designing and evaluating cryptographic algorithms, ensuring that they meet the highest standards of security, performance, and practical applicability.

DATA ANALYSIS

Cryptography has long relied on foundational algorithms like RSA and the Merkle-Hellman Knapsack cryptosystem. While these methods were pioneering in their time, the evolution of computational power and cryptanalysis techniques has necessitated the development of more robust cryptographic models. The performance and security limitations inherent in these traditional schemes have become increasingly evident, particularly with the rise of quantum computing and advanced factorization techniques.

To address these challenges, our proposed cryptographic model introduces innovations in mathematical transformations, optimized key generation, and computational efficiency. A crucial part of this research is the comparative evaluation of these models against existing cryptographic standards, focusing on both performance and security aspects. The primary goal is to demonstrate how our approach improves efficiency while maintaining or enhancing security levels, making it a viable alternative to RSA and Merkle-Hellman.

Performance Benchmarking Before and After Implementing New Models

The performance of a cryptographic system is a fundamental measure of its feasibility for practical applications. Traditional algorithms like RSA have been widely used due to their theoretical security, but they exhibit significant inefficiencies when deployed in real-world scenarios. Key generation in RSA requires the selection of two large prime numbers and the computation of their product, a process that becomes increasingly time-consuming as key sizes grow. Encryption and decryption operations are also computationally expensive, relying on modular exponentiation, which is inherently slow when performed sequentially.

Similarly, the Merkle-Hellman Knapsack cryptosystem was initially developed as an efficient alternative to RSA, utilizing a subset sum approach for encryption and decryption. However, it was later found to be vulnerable to lattice-based cryptanalysis, significantly undermining its practical security. While its encryption process remains computationally efficient, the reliance on superincreasing sequences and modular transformations limits its adaptability to modern security requirements.

In contrast, our proposed cryptographic model integrates a division-based DM addition chain, fuzzy modular arithmetic, and parallel computational techniques to optimize key generation, encryption, and

decryption processes. This approach significantly reduces computational overhead, allowing for faster cryptographic operations without compromising security. Parallelized processing enables multiple calculations to be executed simultaneously, improving efficiency beyond what is achievable with traditional RSA implementations. Additionally, the division-based DM addition chain streamlines modular exponentiation, eliminating redundant calculations and accelerating encryption speed.

Security Assessment of RSA Using Parallelism and Fuzzy Modular Arithmetic

While RSA remains a cornerstone of public-key cryptography, its security has been increasingly scrutinized due to emerging attack vectors. One of its primary vulnerabilities lies in its dependence on the integer factorization problem. As computational power continues to grow, the feasibility of factoring large RSA keys increases, particularly with advancements in quantum computing. Shor's algorithm, for example, has demonstrated that a sufficiently powerful quantum computer could factor RSA's modulus in polynomial time, effectively rendering the encryption useless.

Moreover, RSA's security is heavily reliant on key size. To maintain resistance against brute-force attacks, RSA keys must be expanded beyond 2048 or even 4096 bits. However, increasing key sizes leads to performance degradation, making encryption and decryption prohibitively slow for large-scale applications. Additionally, RSA implementations are susceptible to various side-channel attacks, where adversaries exploit physical characteristics of computation—such as execution time variations—to extract cryptographic keys.

To mitigate these risks, our proposed cryptographic model incorporates parallelism, which distributes computational tasks across multiple processing units, thereby reducing execution time while maintaining the mathematical strength of cryptographic functions. Unlike conventional RSA, where encryption and decryption rely on sequential exponentiation, our model leverages multi-threaded architectures to accelerate calculations, making cryptographic operations more efficient without sacrificing security.

A key innovation in our approach is the integration of fuzzy modular arithmetic. Traditional modular arithmetic in cryptography follows deterministic rules, allowing attackers to exploit predictable patterns for cryptanalysis. Fuzzy modular arithmetic introduces controlled randomness into modular operations, disrupting predictable structures and making it significantly harder for adversaries to perform cryptographic attacks. This added layer of complexity enhances RSA's resistance to both classical and quantum attacks, ensuring that even if the integer factorization problem is partially solved, the unpredictability introduced by fuzzy modular arithmetic adds another level of security.

Beyond theoretical improvements, these optimizations also address real-world cryptographic concerns. Timing attacks, which exploit variations in execution time to infer private keys, become substantially more difficult when fuzzy modular arithmetic is implemented. Since calculations are no longer strictly deterministic, attackers cannot reliably predict how a cryptographic function will behave in different scenarios. This strengthens RSA against modern cryptanalysis techniques, preserving its viability in high-security applications.

DISCUSSION

The research yielded several pivotal findings that reinforce the efficiency, security, and applicability of the proposed cryptographic framework. One of the most significant outcomes was the successful integration of number-theoretic transforms (NTT) to enhance encryption and decryption processes, leading to improved computational efficiency without compromising security. The development of a public key cryptosystem based on modular arithmetic and probability theory demonstrated resilience against traditional cryptographic attacks while maintaining feasibility in both end-to-end and group communication scenarios. Furthermore, the study introduced a novel signature scheme, leveraging elliptic curves and symmetric functions to ensure data integrity in group-oriented communications. This scheme was rigorously tested against conventional methods such as DSA and ECDSA, revealing superior performance in terms of speed, security, and computational efficiency. Another crucial finding was the successful application of cryptographic protocols in securing electronic voting systems, where elliptic curves played a pivotal role in enhancing security and ensuring voter anonymity. The research also led to the development of an optimized deterministic factorization algorithm, which proved to be computationally efficient in breaking and securing cryptographic keys.

Beyond algorithmic innovations, the study provided an interdisciplinary perspective by integrating number theory and probability theory to model cryptographic security. These mathematical foundations reinforced the theoretical soundness of the developed cryptosystem while enabling a deeper understanding of security guarantees in encryption schemes. Additionally, extensive benchmarking of cryptographic performance highlighted the efficiency of the proposed models in terms of key generation time, encryption time, decryption speed, and computational overhead reduction.

Each of the research findings aligns with the predefined objectives, demonstrating how the proposed methodologies address fundamental cryptographic challenges:

Development of a Public Key Cryptosystem: The study successfully formulated a public key encryption scheme utilizing number-theoretic transforms, ensuring robust security in both end-to-end and group communication. The cryptosystem was rigorously tested against traditional public key methods like RSA and Merkle-Hellman Knapsack, validating its improved efficiency and attack resistance.

Signature Schemes for Data Integrity: The research introduced a signature scheme based on elliptic curves and symmetric functions, addressing data integrity concerns in multi-user environments. This innovation ensures non-repudiation, authentication, and resistance to forgery attacks in group-oriented communication.

Interdisciplinary Use of Mathematical Foundations: A novel interdisciplinary approach was employed, incorporating number theory and probability theory to mathematically validate the cryptographic models. These theories played a crucial role in enhancing key security, optimizing encryption complexity, and strengthening randomness in cryptographic operations. Application in Electronic Voting Systems: The research extended its practical applicability by demonstrating the feasibility of elliptic curve-based encryption in securing electronic voting systems. This implementation ensures voter privacy, vote integrity, and resistance against tampering, making it a viable alternative to conventional e-voting security frameworks.\

Development of an Efficient Factorization Algorithm: A special-purpose deterministic factorization algorithm was designed to optimize key management and enhance cryptographic security. The algorithm was benchmarked against traditional factorization techniques, showing significant improvements in efficiency and computational feasibility.

The study makes significant contributions to the field of cryptographic research by addressing computational inefficiencies and security limitations in existing encryption methodologies. Unlike RSA and other conventional cryptosystems, which suffer from scalability issues and susceptibility to quantum attacks, the proposed models introduce mathematically optimized encryption schemes that enhance both security and computational speed. The signature scheme presented in this research also contributes to the domain of secure multi-party communication, an area of growing importance in finance, healthcare, and governmental security infrastructures.

CONCLUSION

This study addressed the need for robust cryptographic solutions by overcoming the limitations of traditional models like RSA and ECC in terms of efficiency, attack resistance, and scalability. By leveraging number-theoretic transforms (NTT), the research developed a secure public key cryptosystem for end-to-end and group communication while integrating elliptic curve cryptography (ECC) with symmetric techniques to design an advanced digital signature scheme ensuring data integrity and computational efficiency. Through rigorous mathematical validation using modular arithmetic, probability theory, and computational complexity analysis, the study established a strong theoretical foundation for assessing cryptographic security. The findings highlight the significance of structured mathematical approaches in enhancing encryption and authentication mechanisms, contributing to scalable, attack-resistant, and efficient cryptographic solutions for modern digital communication networks.

REFERENCES

1. Ahmed, Md & Tanti, Jagmohan & Pushp, Sumant. (2021). A Public Key Cryptosystem Using Cyclotomic Matrices. 10.5772/intechopen.101105.

2. Sykt, A., Azad, M. S., Tanha, W. R., Morshed, B. M., Shubha, S. E. U., & Mahdy, M. R. C. (2025). Multi-layered security system: Integrating quantum key distribution with classical cryptography to enhance steganographic security. Alexandria Engineering Journal, 121, 167-182.

3. Subramani, S., & Svn, S. K. (2023). Review of security methods based on classical cryptography and quantum cryptography. Cybernetics and Systems, 1-19.

4. Sundaram, Divya. (2015). Number Theory Research Unit - A New Security Strategy for Peer-To-Peer Mobile Communication.

5. Soleymani, Ali, et al. A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map.‖ The Scientific World Journal, vol. 2014, Hindawi, 2014.

6. Tropea, M., Spina, M. G., De Rango, F., & Gentile, A. F. (2022). Security in wireless sensor networks: A cryptography performance analysis at mac layer. Future Internet, 14(5), 145.

7. Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.

8. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177-28193.

9. Thomé, Emmanuel. (2012). Algorithmic Number Theory and Applications to the Cryptanalysis of Cryptographical Primitives.

10. Theory, Based & Bleichenbacher, Daniel & Inform, Dipl. (2002). Efficiency and Security of Cryptosystems based on Number Theory.

11. Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. Alexandria Engineering Journal, 72, 37-50.

12. Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Materials Today: Proceedings, 37, 2653-2659.