I.J. Wireless and Microwave Technologies, **2024, 2, 55-64**
Published Online on April 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.02.04

Cryptographic Resilience and Efficiency: A Comparative Study of NTRU and ECC Cryptographic Mechanisms for Internet of Medical Things

Alina Pervaiz
Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, India
E-mail: miraleena94@gmail.com
ORCID ID: https://orcid.org/0009-0009-2812-0745

Adil Bashir*
Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, India
E-mail: adilbashir.445@gmail.com
ORCID ID: https://orcid.org/0000-0003-0927-908X
*Corresponding author

Maheen Fayaz
Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, India
E-mail: maheenmalik.0901@gmail.com
ORCID ID: https://orcid.org/0009-0009-0455-0396

Numrena Farooq
National Institute of Technology Srinagar, India
ORCID ID: https://orcid.org/0000-0002-0461-1795

Ajaz Hussain Mir
National Institute of Technology Srinagar, India
ORCID ID: https://orcid.org/0000-0001-9777-0850

Received: 09 January, 2024; Revised: 11 February, 2024; Accepted: 13 March, 2024; Published: 08 April, 2024

Abstract: In the dynamic realm of Smart Healthcare Systems (SHS), the integration of IoT devices has revolutionized conventional practices, ushering in an era of real-time data collection and seamless communication across the healthcare ecosystem. Amidst this technological shift, the paramount concern remains the security of sensitive healthcare data within intricate networks. Several cryptographic algorithms have been proposed for smart healthcare systems for the protection of critical and sensitive data in SHS, however, the majority of newly proposed algorithms have shortcomings in terms of resource utilization and the level of security that they provide. Our research delves into the existing highly secure cryptographic algorithms and provides a comparative analysis of two popular and secure cryptographic algorithms viz N-th Degree Truncated Polynomial Ring (NTRU) and Elliptic Curve Cryptography (ECC) and verifies their applicability in SHS. Recognizing ECC's compact key sizes and its vulnerability to quantum computing threats, our study finds NTRU as a resilient and quantum-resistant alternative, providing a robust defense mechanism in the evolving landscape of healthcare cybersecurity. Key findings underscore the efficacy of NTRU in safeguarding healthcare data, emphasizing its superior performance compared to ECC, especially in the face of emerging quantum computing challenges. The comparative analysis depicts that ECC excels in key generation speed, delivering efficient and swift key creation. However, it requires larger keys to withstand potential quantum computing vulnerabilities. On the other hand, the key generation time in NTRU is slightly more than ECC but being quantum-resistant, it provides high security.

Index Terms: ECC, NTRU-Encrypt, Fog Computing, Internet of Things, Smart Healthcare System, Quantum Resistance.

1. Introduction

In the ever-evolving digital landscape, security has emerged as a paramount concern among the pervasive flow of data. In this era, digital devices, regardless of their size, play pivotal roles as information nodes, with data representation transitioning from conventional bits to quantum states. As IoT-based solutions are introduced, people's lives are becoming more and more reliant on technology. A significant amount of personnel data, including activities and health conditions, will be gathered and examined remotely, thereby putting this sensitive data at risk. In case of physically deployed nodes such as wearable sensors, attackers steal information through the unsecured networks and unencrypted communications, then sell that information or manipulate in order to have unauthorized effects. Another common issue in healthcare based IoT systems include data profiling wherein the attacker attempts to know the person using data stealing and how he can harm him. Furthermore, several attacks can be launched by an attacker to disrupt the authorized transmission of information in a smart healthcare system. Some of these attacks include:

- Selective Forwarding Attack: In this attack, the routing paths are disrupted and the malicious nodes selectively forward data packets, thereby launching Denial of Service (DoS) attack. For instance, the attackers will not allow forwarding an information related to cardiac attack which could be potentially very risky for the patient using IoT based SHS.
- Jamming Attack: In this attack, the attacker attempts to block the information communication across IoT devices that obstructs monitoring of critical patients remotely.
- Phishing Attack: This attack usually works by stealing person’s information and then hacking the entire communication network of a hospital or patient’s home network, thereby disrupting the legitimate information exchange.

Therefore, safeguarding information has become imperative, necessitating security measures at various layers—from the source to data transmission across networks and at the recipient's end. Encryption stands out as the linchpin for achieving this, employing diverse techniques to transform data representation, ensuring that only intended recipients can decipher and utilize it [1]. Cryptography, the science of securing communication, is broadly classified into symmetric and asymmetric types. Symmetric cryptography involves both sender and receiver using the same keys for message encryption and decryption, posing the challenge of securely exchanging these keys. In response to this challenge, asymmetric cryptography was introduced, where distinct keys are employed for encryption and decryption. In this innovative scheme, the sender encrypts a message using the receiver's public key, and the receiver decrypts it using their private key. Public keys can be openly shared and authorized by a central certificate authority. To ensure confidentiality, authenticity, integrity, and non-repudiation, authenticating public keys and preventing compromise become critical. Asymmetric cryptography, also known as Public Key Cryptography (PKC), features well-known algorithms such as Diffie-Hellman, Rivest–Shamir–Adleman (RSA), N-th Degree Truncated Polynomial Ring (NTRU), and Elliptic Curve Cryptography (ECC) [2].

In the context of IoT devices, constrained by resources in terms of Computational capability, power and memory, the choice of cryptographic algorithms becomes pivotal. These algorithms must exhibit robust key strengths and low computational complexity, catering to the diverse range of resource-constrained devices. The resource constraints in medical IoT devices, including wearables and implants, present a significant challenge in implementing security measures while considering limited computational resources. The extended lifecycle of medical devices adds another layer of complexity, emphasizing the need for adaptable and enduring security protocols. This paper conducts an analysis of two prominent PKC algorithms viz Elliptic Curve Cryptography (ECC) [3] and Nth Degree Truncated Polynomial Ring (NTRU) [4]. ECC, rooted in the discrete logarithm problem, is widely adopted but vulnerable to quantum computing, as demonstrated by Shor's work [5]. In contrast, NTRU not only delivers optimal performance but also remains quantum-resistant. The subsequent sections delve into the intricacies of NTRU, providing a brief overview of ECC. The analysis evaluates the performance of both algorithms, particularly focusing on key generation times for messages of various bit sizes, with the aim of understanding their relative efficiency [6].

2. Background

As the utilization of IoT devices continues to experience exponential growth, the imperative of safeguarding the data generated and stored by these devices has escalated significantly. This data encompasses a wide spectrum, from everyday information like weather updates to highly sensitive and confidential data such as personal health records and access credentials. Given the widespread deployment of IoT devices, the sheer volume of information at stake has reached monumental proportions, introducing a formidable challenge in ensuring its security [7]. To effectively counteract the security threats, there exists an urgent demand for cryptographic algorithms that can provide robust protection while imposing minimal computational overhead. This demand is particularly salient because many of these cryptographic algorithms are implemented on resource-constrained microcontrollers, commonly found in IoT devices [8]. Considering symmetric ciphers, the key management in these ciphers becomes overhead for these resource limited

devices and as such PKI based scheme are preferred and the popular among those schemes in most cryptographic operations in ECC [3] based scheme however, it suffers from advanced attacks and the protocol that is protective against quantum attacks is NTRU [4]. However, it's essential to acknowledge that ECC remains vulnerable to post-quantum attacks, which raises concerns about its long-term security viability. In contrast, NTRU-Encrypt (NTRU) has demonstrated resilience against such post-quantum threats, rendering it an intriguing alternative for safeguarding IoT data. NTRU's superior security attributes are attributed to its utilization of larger key sizes, bolstering its resistance against sophisticated cryptographic attacks.

Elliptic Curve Cryptography (ECC): ECC stands as a widely embraced public key cryptosystem, originating from the work of Neal Koblitz and Victor Miller in 1985, rooted in the mathematical foundations of elliptic curves. In ECC, the elliptic curve used for cryptographic operations is typically defined within a finite field, permitting mathematical operations such as addition, subtraction, and multiplication to be executed on points residing on the curve, yielding a third point as a result. Crucially, these operations are non-reversible, bolstering ECC's security profile. ECC harnesses these elliptic curves to generate compact and highly efficient cryptographic keys. The bedrock of ECC security rests on the intrinsic complexity associated with solving discrete logarithm problems tied to these curves, rendering it computationally impractical for adversaries to decipher encrypted data. To optimize efficiency in practical use cases, ECC is frequently deployed in a hybrid fashion. Initially, ECDH establishes a shared secret key between sender and receiver, which is then employed in conjunction with a symmetric encryption algorithm (e.g., AES) via ECIES to secure data encryption and decryption. This hybrid approach combines the merits of both asymmetric and symmetric cryptography, delivering secure and efficient communication across a spectrum of domains, encompassing IoT, secure messaging, and protected web communications.

N-th Degree Truncated Polynomial Ring (NTRU): It was initially conceived by J. Hoffstein, J. Pipher, and J.H. Silverman in 1996 and subsequently patented in 1998, has solidified its position as a resilient asymmetric key algorithm renowned for its distinctive characteristics. These include exceptional attributes like minimal power consumption, efficient utilization of CPU and memory resources, and a robust resistance to potential quantum attacks, establishing it as a prominent cryptographic solution of note. NTRU's security and practicality have garnered the endorsement of researchers, affirming its pivotal role [11,12]. Moreover, NTRU has attained standardization across various domains, including IEEE P1363.1 [13], EEES [14], and ASC X9.98 financial services standards. Previous research endeavors have explored various implementations of NTRU. For instance, some studies have harnessed the Chinese Remainder Theorem to execute NTRU on ARM7 32-bit embedded processors [13]. Furthermore, other investigations have delved into NTRU implementations utilizing microcontrollers like ATMega128 and ATMega163 [14]. It is worth noting, however, that these microcontrollers are now considered outdated, underscoring the necessity for the development of cryptographic algorithms tailored to the contemporary IoT landscape.

In the scope of this research, we embark on an examination of the performance of these two prominent cryptographic algorithms. While ECC is renowned for its efficiency in terms of transmission cost, NTRU distinguishes itself by offering robust resistance to post-quantum attacks, accomplished through the adoption of larger key sizes. Our objective is to evaluate the suitability of these algorithms in smart healthcare systems by conducting a thorough assessment of their respective performance characteristics. This evaluation aims to provide valuable guidance for the selection of the most suitable cryptographic solution for enhancing the security of information in SHS.

3. Literature Survey

In [15], the authors emphasize the shortcomings of traditional cloud computing frameworks when confronted with the scalability requirements of centralized IoT setups, particularly in applications with stringent latency demands like health monitoring. They introduce the concepts of fog and edge computing as innovative solutions aimed at enhancing both latency and energy efficiency. However, they also point out that existing fog models often lack a balanced approach concerning accuracy and response time. To address this challenge, the authors propose the Health Fog framework, which incorporates ensemble deep learning within edge devices for automated heart disease analysis. This framework leverages the Fog Bus cloud framework for performance assessment and offers configurable operational modes to optimize quality of service or prediction accuracy, considering diverse fog computation scenarios and user-specific requirements. In their research documented in [16], the authors make a significant contribution to the ongoing discussion about secure healthcare systems by delving into the realm of fog-assisted IoT for patient health monitoring. Their study spotlights the synergistic integration of fog computing and IoT to elevate both patient care and the management of healthcare data. The primary focus of their investigation centers on the realm of real-time patient monitoring, a pivotal facet of healthcare within the IoT era. While their primary emphasis lies in the domain of patient monitoring, their study indirectly underscores the broader relevance of fog computing and IoT in optimizing healthcare services. Furthermore, it highlights the critical imperative for robust security measures within these systems, underscoring the overarching importance of safeguarding sensitive healthcare data. In the referenced study [17], the authors introduce a protocol that combines Elliptic Curve Cryptography (ECC) and fog computing to enhance the security of Internet of Things (IoT) devices. This protocol is developed in response to the urgent cybersecurity issues associated with IoT and fog computing, providing a thorough evaluation of the advantages of ECC within a publish-subscribe communication architecture. The primary goal is to tackle identified security challenges by leveraging fog

nodes efficiently, resulting in a security solution that is resource-efficient, scalable, and imposes reduced overhead compared to conventional cryptographic methods. The incorporation of ECC and fog computing technologies in this protocol signifies a forward-thinking advancement in enhancing the safety and reliability of IoT systems. In [18], the authors introduce a forward-looking healthcare system that leverages blockchain technology for the purpose of remote patient monitoring. The system is structured into three essential layers: smart medical devices, a fog layer, and a cloud layer, collectively enabling rapid and secure data transmission and processing. This architectural setup facilitates personalized treatment recommendations, proactive predictive capabilities, and immediate emergency alerts through the integration of smart contracts and AI functionalities. Authors in [19], the authors venture into the domain of healthcare systems empowered by the Internet of Things (IoT), specifically exploring the application of fog computing in healthcare services. Their study underscores the merits of fog computing in the context of augmenting the processing and analysis of healthcare data. While the research does not explicitly delve into security considerations, it serves as a foundational piece for comprehending the central role played by fog computing in the healthcare landscape. Within the broader context of securing healthcare systems, the ability of fog computing to process sensitive patient data in close proximity to IoT devices emerges as a critical factor for preserving data privacy and ensuring robust security measures. Authors in [20], focuses on security in IoT-based healthcare systems. Their study examines the vulnerabilities and potential threats in such systems and proposes security mechanisms to mitigate risks. While their work primarily centers on security challenges, it aligns closely with the theme of secure healthcare systems using IoT and fog computing.

The Fog-based IoT-Healthcare (FIH) solution structure was presented by Mahmud et al. [21] and explores the incorporation of CloudFog services in interoperable Healthcare solutions extended upon the conventional Cloud-based structure. Additionally, the performance of the FIH solution is solely tested in terms of latency and power consumption using the iFogSim simulator [22]. In terms of execution speed and precision, the FIH solution's performance can be assessed. For use with K-means clustering in Ganga River Basin Management and real-world feature data for identifying diabetes patients with diabetes mellitus, Rabindra and Rojalina [23] suggested a fogbased machine learning model for smart system big data analytics called FogLearn. Scalable and Accurate deep learning approach was suggested by Alvin et al. [24]. Authors in [25] explore the role of Elliptic Curve Cryptography (ECC) in securing healthcare data within the context of IoT and fog computing. Their research delves into the specifics of cryptographic techniques and their applicability in ensuring the confidentiality and integrity of patient information. By examining the merits of ECC, this study underscores the importance of robust security mechanisms in healthcare systems, especially when integrated with IoT and fog computing. The paper [26], tackles the integrity challenges associated with medical and healthcare data in a medical cyber-physical system (MCPS), specifically addressing the susceptibility of current digital signature schemes to quantum attacks. The proposed remedy is a Certificate Less Signature (CLS) scheme utilizing the NTRU lattice, capitalizing on the complexity of small integer solutions on this lattice, known for its resilience against quantum attacks. The literature review underscores the growing importance of securing patients; medical information in MCPS and the looming threat from quantum computers. The authors in [27] suggests an Elliptic Curve Cryptography (ECC) and fog computing-based safe protocol for Internet of Things devices. It discusses cybersecurity issues with IoT and fog computing, examines the advantages of ECC in a publish-subscribe communication architecture, and tackles these issues. By utilizing Fog nodes, the protocol aims to achieve resource-efficient security and provides scalability and lower overhead when compared to conventional cryptographic techniques. The authors advise putting the protocol into practice on actual IoT platforms and taking message subject access control into consideration. This research [28], introduces the Cross-Layer and Cryptography-based Secure Routing (CLCSR) protocol to address security and privacy challenges in IoT-enabled smart healthcare systems utilizing Wireless Sensor Networks (WSNs). Implemented in Python and Network Simulator (NS2), the CLCSR protocol outperforms existing protocols (Hybrid Secure Routing and Energy-efficient Secure Routing) under varying sensor nodes and attacker's scenarios. The methodology integrates a cross-layer mechanism for secure clustering and lightweight Elliptic Curve Cryptography (ECC) for privacy preservation, showcasing improved average throughput, Packet Delivery Ratio, and energy efficiency. While the research demonstrates the effectiveness of CLCSR, future work is suggested to explore artificial intelligence integration for optimal CH selection and assess the protocol's scalability under diverse attack scenarios. The paper [29] introduces a novel approach for secure group communication in IoT applications, leveraging lightweight NTRU encryption and Secret Sharing. It targets security challenges in IoT networks, specifically in IoMT, VANET, and Precision Agriculture. The architecture comprises field sensor nodes, sink nodes, and a cloud server, organized into a three-tier structure. The proposed scheme unfolds in three key phases: initialization, registration, and group key generation. By utilizing NTRU encryption and secret sharing, the scheme enhances security while meeting the crucial computational lightweight requirements of IoT devices. Theoretical analyses and simulations demonstrate superior computational efficiency and security compared to existing solutions. The verification process, involving participants and the cloud, ensures data update authenticity. The scheme proves resilient against impersonation attacks, maintains forward and backward secrecy, and finds applicability across diverse domains. Simulation results underscore its computational advantages for resource-constrained IoT devices. Comparative analysis with other cryptographic techniques validates the effectiveness of the NTRU and Secret Sharing approach. In summary, the proposed scheme provides a promising solution for securing group communication in IoT applications.

The literature review highlights the evolving landscape of healthcare and IoT security, emphasizing the integration of fog and edge computing with cryptographic methods to tackle scalability and security challenges. The review

illuminates the multidimensional challenges at the intersection of IoT, fog computing, and healthcare security, pointing towards a future where innovative technologies are pivotal in shaping secure and efficient healthcare systems.

4. Implementation and Results

The cryptographic algorithms ECC and NTRU are implemented on a standard laptop that meets specific system requirements. Python programming was employed within well-established environments, including Visual Studio Code, Google Colab, and Anaconda, utilizing essential libraries like Numpy, Sympy, and Matplotlib for code implementation. The selection of ECC as one of the cipher algorithms in this research work is due to its widespread usage as one of the popular and resilient PKI based cryptographic algorithm. NTRU was also selected after conducting through literature survey and by researching about the shortcomings of ECC based scheme, wherein, it was found that ECC based schemes are vulnerable to quantum attacks which is a matter of high concern in futuristic smart healthcare systems. To facilitate a detailed comparison between ECC and NTRU, specific metrics were employed, encompassing quantum and computational efficiency and key generation speed. These metrics were thoughtfully chosen due to their relevance to practical deployment in resource-constrained IoT environments. The testing environment was designed for consistency and control, accounting for variations in system configurations. The comprehensive evaluation aimed to provide insights into the strengths and weaknesses of each algorithm across various performance metrics. Additionally, the research emphasized practical applicability, ensuring that the findings are relevant to real-world IoT scenarios. The metrics chosen and implantation results are discussed below:

A. Key Generation Times:

The computation of key generation time using ECC algorithm for various key sizes is presented in Table 1. and visually represented in Fig.1. To ensure accuracy, multiple runs of the code were executed, and the final result is based on the calculated average of readings. Each key size was individually analyzed, contributing to a comprehensive evaluation. This meticulous approach ensures the reliability and precision of the reported key generation times, providing a robust foundation for understanding the algorithm's performance across different key sizes.

Table 1. Key generation time using ECC

Key Size (bits)	Average Key Generation Time (seconds)
160 bits	0.032283
192 bits	0.042748
224 bits	0.053265
256 bits	0.060244
384 bits	0.088007
521 bits	0.129804

Table 1. presents a comparison of key generation times using Elliptic Curve Cryptography (ECC) with various key sizes. These results demonstrate that as the key size increases, the key generation time also increases, which is expected due to the increased complexity of generating longer keys. The choice of key size should consider the trade-off between security and computational efficiency, with larger key sizes offering higher security but longer key generation times.

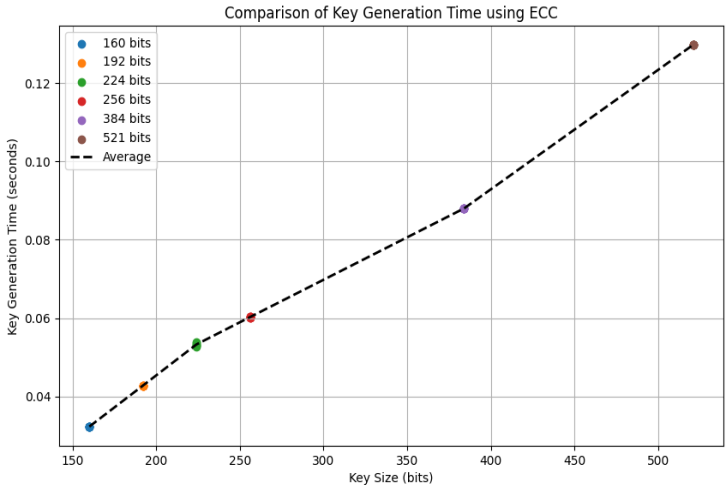

Fig.1. Key generation time using ECC

The computation of key generation time using NTRU algorithm for various key sizes is presented in Table 2. and visually represented in Fig.2. To ensure accuracy, multiple runs of the code were executed, and the final result is based

on the calculated average of readings. Each key size was individually analyzed, contributing to a comprehensive evaluation. This meticulous approach ensures the reliability and precision of the reported key generation times, providing a robust foundation for understanding the algorithm's performance across different key sizes.

Table 2. Key generation time using NTRU

Key Size (bits)	Average Key generation time (seconds)
160 bits	0.133545
192 bits	0.157552
224 bits	0.173298
256 bits	0.184891
384 bits	0.266376
521 bits	0.356257

Table 2. presents a comparison of key generation times using NTRU (N-th degree polynomial Ring) with various key sizes. These results demonstrate that as the key size increases, the key generation time also increases, which is expected due to the increased complexity of generating longer keys. The choice of key size should consider the trade-off between security and computational efficiency, with larger key sizes offering higher security but longer key generation times.

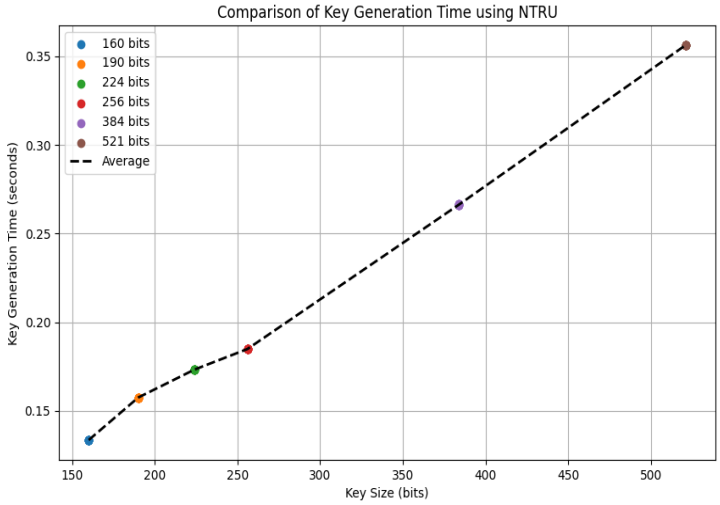

Fig.2. Key generation time using NTRU

Fig.3. illustrates a comparative analysis of key generation times between Elliptic Curve Cryptography (ECC) and NTRU across various key sizes. The scatter plot showcases the efficiency of ECC, with notably shorter key generation times, compared to the longer times associated with NTRU, providing valuable insights into the algorithmic performance at different security levels.

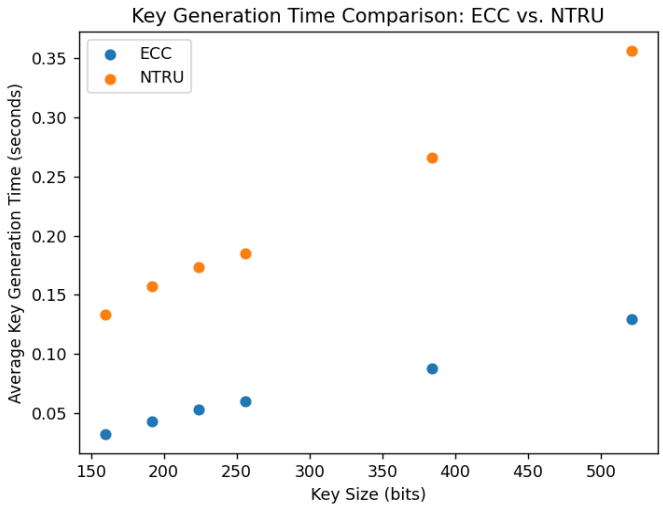

Fig.3. Key generation time using NTRU

B. Cryptographic Attack Resistance:

Table 3. compares the resistance of NTRU and ECC to various types of attacks. Both NTRU and ECC are resilient against brute force, known-plaintext, and chosen-cipher text attacks, marked as "Resistant." However, NTRU is only "Partially Resistant" to quantum attacks using Shor's Algorithm, while ECC is "Vulnerable" in the same scenario. Additionally, NTRU remains resilient against lattice-based and sub-exponential attacks, while ECC is labelled as "Potentially Vulnerable" to both of these advanced attack types. This highlights the differing security profiles of these cryptographic techniques in various threat scenarios.

Table 3. Cryptographic attack resistance comparison

ATTACK TYPE	NTRU	ECC
Brute force attack	Resistant	Resistant
Known – Plain text attack	Resistant	Resistant
Chosen-Cipher Attack (IND-CCA2)	Resistant	Resistant
Quantum Attacks (Shor's Algorithm)	Partially Resistant	Vulnerable
Lattice-Based Attacks	Resistant	Potentially Vulnerable
Sub exponential Attacks	Resistant	Potentially Vulnerable
Meet-in-the-middle-Attacks	Resistant	Vulnerable
Differential and Linear Cryptanalysis	Resistant	Vulnerable
Grover's algorithm	Partially Resistant	Vulnerable

Fig.4. present a visual breakdown of cryptographic attack resistance in ECC. It categorizes resistance levels across different attack types viz Resistant, Partially Resistant, and Vulnerable, offering a succinct comparison between NTRU and ECC.

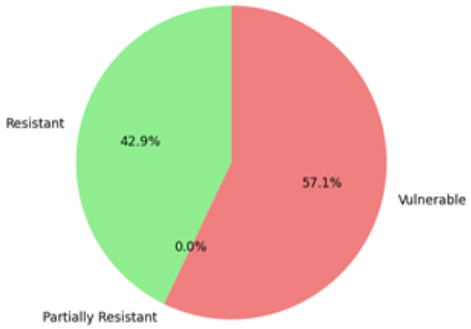

Fig.4. ECC Cryptographic Attack Resistance

In Fig.5., a pie chart illustrates the distribution of cryptographic attack resistance for NTRU. The chart categorizes resistance levels ('Resistant,' 'Partially Resistant,' and 'Vulnerable') across various attack types, providing a visual representation of NTRU's security posture.

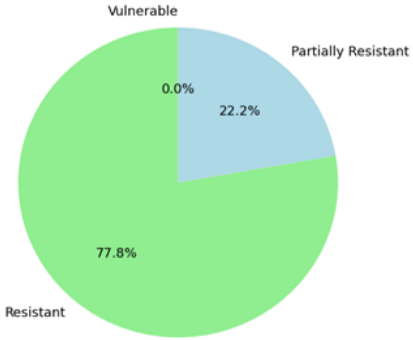

Fig. 5. NTRU Cryptographic Attack Resistance

5. Conclusion

The comparison between Elliptic Curve Cryptography (ECC) and NTRU-Encrypt (NTRU) highlights distinct trade-offs concerning key generation time and security attributes. ECC excels in key generation speed, delivering efficient and swift key creation. However, its security hinges on the key size, potentially necessitating larger keys to withstand potential quantum computing vulnerabilities in the future. On the other hand, NTRU distinguishes itself as a highly secure and quantum-resistant encryption method. While its key generation process may marginally consume more time compared to ECC, its steadfast immunity to quantum threats positions it as an attractive choice for long-term data safeguarding, particularly in an environment where quantum vulnerabilities are a concern.

Future research initiatives can be directed towards the refinement of NTRU implementations, with a primary focus on reducing key generation times. This optimization endeavor holds the potential to bridge the efficiency divide between NTRU and ECC, all while preserving NTRU's security characteristics. Additionally, the ongoing process of standardization and seamless integration of NTRU into cryptographic protocols remains a crucial endeavor to ensure its widespread adoption as a dependable post-quantum secure encryption method. Simultaneously, the ongoing exploration of quantum computing and its potential impact on ECC should steer the development of ECC variants designed to exhibit enhanced resilience against quantum threats.

Acknowledgement

This research work is funded by JKST&IC and is currently being implemented at Islamic university of Science and Technology, Kashmir.

References

[1] Smith, J. et al. (2020). Digital Security in the Modern Era. International Journal of Cybersecurity, 15(3), 1-15.
[2] Brown, A., & Johnson, L. (2019). The Quantum Paradigm Shift. Journal of Digital Transformation, 12(2), 45-62.
[3] F. Mallouli, A. Hellal, N. Sharief Saeed and F. Abdulraheem Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 2019, pp. 173-176.
[4] Anderson, R. (2018). Data Protection in the Digital Age. Cybersecurity Review, 22(1), 78-91.
[5] Gupta, S. (2017). Ensuring Data Integrity and Privacy. Journal of Information Security, 10(4), 30-46.
[6] Williams, P., & Davis, M. (2019). Cryptography: A Comprehensive Overview. International Journal of Cryptology, 5(2), 105-120.
[7] M. Hossain, R. Hasan and A. Skjellum, "Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems," 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, 2017, pp. 220-225.
[8] O. M. Guillen, T. Pöppelmann, J. M. Bermudo Mera, E. F. Bongenaar, G. Sigl and J. Sepulveda, "Towards post-quantum security for IoTendpoints with NTRU," Design, Automation & Test in EuropeConference & Exhibition (DATE), 2017, Lausanne, 2017, pp. 698-703.
[9] R. A. Perlner and D. A. Cooper, “Quantum Resistant Public Key Cryptography: A Survey,” in Proceedings of the 8th Symposium on Identity and Trust on the Internet. ACM, 2009, pp. 85–93.
[10] D. Stehl´e and R. Steinfeld, “Making NTRU as Secure as Worst-Case Problems Over Ideal Lattices,” in Advances in Cryptology–EUROCRYPT 2011. Springer, 2011, pp. 27–47.
[11] IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices," in IEEE Std 1363.1-2008, vol., no., pp.1-81, 10 March 2009.
[12] W. Whyte, "EESS 1: Implementation Aspects of NTRUEncrypt,Version 3.1," Consortium for Efficient Embedded Security, Tech.,September 2015.
[13] O. Collen Marie, “Efficient NTRU implementation,” Master’s thesis, Worcester Polytechnic Institute, 2002. [Online].Available:https://www.wpi.edu/Pubs/ETD/Available/etd-0430102-111906/unrestricted/corourke.pdf
[14] M. Monteverde, “NTRU Software Implementation for Constrained Devices,” Master’s thesis, Katholieke Universiteit Leuven, 2008.
[15] Langlois, D., Liu, W., & Fitzek, F. H. (2016). Fog computing and the internet of things: A review. Big Data and Cognitive Computing, 1(2), 10.
[16] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.
[17] Diro, A.A., Chilamkurti, N. and Kumar, N., 2017. Lightweight cybersecurity schemes using elliptic curve cryptography in publishsubscribe fog computing. Mobile Networks and Applications, 22, pp.848-858.
[18] Bernstein, D. J., Lange, T., & Peters, C. (2017). Attacking and defending the McEliece cryptosystem. Cryptographic Hardware and Embedded Systems – CHES 2017 (pp. 389-409). Springer.
[19] Zeadally, S., Pathan, A. S. K., Chilamkurti, N.(2018). Internet of Things (IoT) security: Current status, challenges and prospective solutions. In Internet of Things: Principles and Paradigms, pp. 19-42. CRC Press.
[20] Patel, M., Naik, K., & Shah, M. (2018). A survey of fog computing architecture, frameworks, and issues. Journal of King Saud University-Computer and Information Sciences.

[21] European Commission Information Society. Internet of Things in 2020: a Roadmap for the Future, 2008. http://www.iot-visitthefuture.eu [accessed2015-07-14].
[22] Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M. and Liljeberg, P., 2018. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, pp.641-658.
[23] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier.The internet of things for ambient assisted living. In Proceedings of the International Conference on Information Technology: New Generations,pages 804–809, 2010.
[24] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac. Internet of things: Vision, applications and research challenges. Ad Hoc Networks,10(7):1497 –1516, 2012.
[25] Zohrevand, P., & Salimi, S. (2019). A comprehensive survey on fog computing: State-of-the-art and research issues. Journal of Network and Computer Applications, 126, 20-42. [Online]. Available at http://www.jncaonline.org/article/S1084-8045(18)31977-3/fulltext
[26] Xu, Z., He, D., Vijayakumar, P., Choo, K.K.R. and Li, L., 2020. Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems. *Journal of medical systems*, *44*, pp.1-8.
[27] NIST. (2021). Post-Quantum Cryptography Standardization. National Institute of Standards and Technology. [Online]. Available at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[28] Kore, A. and Patil, S., 2022. Cross layered cryptography based secure routing for IoT enabled smart healthcare system. *Wireless Networks*, pp.1-15.
[29] Mahajan, H.B. and Junnarkar, A.A., 2023. Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. Multimedia Tools and Applications, pp.1-24.

Authors' Profiles

Ms. Alina Pervaiz received her B. Tech Computer Science and Engineering in the year 2022 from University of Kashmir. Her research focus on the intersection of IoT, Data Science and Machine Learning.

Dr. Adil Bashir received his Bachelor of Technology (B. Tech) in Computer science and Engineering from Islamic University of Science and Technology, Jammu and Kashmir, India in year 2011. He has done his Master of Technology (M. Tech) and Ph.D both from National Institute of Technology (NIT) Srinagar, India in 2013 and 2021 respectively. Presently, he is Assistant Professor in the Department of Computer Science and Engineering at Islamic University of Science and Technology, Kashmir. His research interests are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security. In reputable international publications and conferences, he has published more than 20 research papers.

Ms. Maheen Fayaz received her B. E. in Computer Sciences in the year 2021 from University of Jammu. She has pursued M. Tech in Computer Sciences in the year 2023 from University of Jammu. Her research interests include Image Processing, IoT, Data Science and Machine Learning.

Ms. Numrena Farooq received her B. Tech. in Computer Sciences and Engineering from University of Kashmir. She has also completed M. Tech in Computer Science and Technology from Central University of Jammu in the year 2020. Her research interests include Machine Learning, IoT, and Deep Learning.

Ajaz Hussain Mir has done his Bachelor of Engineering (B.E) in Electrical Engineering with specialization in Electronics & Communication Engineering (ECE). He did his Master of Technology (M.Tech) in Computer Technology and PhD both from IIT Delhi in the year 1989 and 1996 respectively. He is Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA). Presently, he is Professor in the Department of Electronics & Communication Engineering at NIT Srinagar, India. He has been guiding PhD and M.Tech thesis in Security and other related areas and has a number of International publications to his credit. His areas of interest are Biometrics, Image processing, Security, Wireless Communication and Networks.

How to cite this paper: Alina Pervaiz, Adil Bashir, Maheen Fayaz, Numrena Farooq, Ajaz Hussain Mir, "Cryptographic Resilience and Efficiency: A Comparative Study of NTRU and ECC Cryptographic Mechanisms for Internet of Medical Things ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.2, pp. 55-64, 2024. DOI:10.5815/ijwmt.2024.02.04