Journal of Theoretical and Applied Information Technology

15th December 2023. Vol.101. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NOVEL SIGNATURE SCHEMES FOR MULTI-MESSAGE SIGNING WITH A SINGLE PUBLIC KEY USING POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS IN MANET

[1]R.PRIYAVANI, [2]DR.N.KOWSALYA,

[1]Research Scholar, Sri Vijay Vidyalaya College of Arts & Science (Affiliated to Periyar University), Dharmapuri, Tamilnadu, India.
[2] Assistant Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science (Affiliated to Periyar University), Dharmapuri, Tamilnadu, India.

E-mail: [1]rpriyavanimsc@gmail.com, [2]kowsisara2003@gmail.com

ABSTRACT

Mobile Ad hoc Networks (MANETs) are decentralized networks that organize themselves, forming multi-hop connections through an ever-changing and unpredictable topology. In this context, any node can function as a sender, receiver, or router, facilitating peer-to-peer communication without relying on centralized infrastructure. Given the reliance on battery power for mobile nodes, the instantaneous connectivity of diverse devices within this network can sometimes result in instances of non-acknowledgement behavior, potentially causing network performance deterioration. To mitigate this performance degradation, we propose an innovative approach using Post-Quantum Cryptography (PQC) tailored to handle non-acknowledgement data in MANETs. Specifically, our method incorporates a customizable hash function called "Everything tweak able hash function" to establish a reliable end-to-end solution. This solution introduces location-aware post-quantum encryption, effectively countering non-acknowledgement data behavior within a bi-directional multi-hop relay setup. Our novel Post-Quantum Cryptography (NPQC) algorithm not only focuses on addressing non-acknowledgement data concerns but also seeks to comprehensively assess the implications of this issue. By evaluating key metrics such as key generation time, encryption/decryption time, security level, execution time, and memory consumption, our aim is to achieve notable enhancements in execution time and overall security within the dynamic environment of an MANET.

Keywords: *Post Quantum Cryptography, Multivariate Cryptography, Hash Based Signature, Tweakable Hash Function, MANET*

1. INTRODUCTION

A mobile ad-hoc network embodies decentralization as its core principle. Communication within this network can take the form of direct or indirect connections. When nodes are within close proximity, direct communication is established. Conversely, if nodes are distant, they facilitate communication through intermediary nodes—this is termed indirect communication. The applications of MANET are diverse, ranging from military operations to healthcare systems. In MANET, nodes possess the autonomy to join or exit the network at will. Upon joining, nodes can function as both sources and destinations of communication.

In the realm of wireless networks, bandwidth plays a pivotal role due to its diminished capacity in comparison to wired links. This factor significantly influences network performance.

Post-quantum cryptography, often referred to as quantum-safe or quantum-resistant cryptography, involves the utilization of cryptographic systems that are presumed to withstand the computational power of quantum computers. The security of prevailing public key cryptosystems hinges on problems rooted in number theory that are believed to be difficult to solve using classical computers [1]. These predicaments include

prime number factorization of large integers and the computation of discrete logarithms, challenges that have been extensively studied over a prolonged period. Cryptographic systems built upon RSA, DSA, and ECDSA all hinge on the complexity of two mathematical dilemmas: prime number factorization and the computation of discrete logarithms. These challenges are vulnerable to attacks orchestrated by quantum computers. A case in point is the 1994 Shor algorithm [2], which illustrates that quantum computers can solve these problems in polynomial time relative to input size. Mere escalation of key sizes doesn't offer a remedy, as this exponential acceleration in contrast to classical computers would inevitably render RSA, DSA, and ECDSA vulnerable in real-world scenarios.

While quantum computers with such attack capabilities aren't yet operational, there is a rapid advancement underway [3]. The duration of energy storage for quantum switches is undergoing significant expansion [4], paralleled by the prolongation of quantum bit storage time [5]. Even if we take an optimistic stance assuming that progress will eventually decelerate and quantum computer realization remains distant, a judicious approach to risk management necessitates the establishment of post-quantum security infrastructures. This is especially relevant in the case of post-quantum digital signature schemes, which should be broadly adopted as a precautionary measure.

The realization of a quantum computer capable of executing Shor's algorithm for relevant cryptographic inputs remains an unmet challenge, leaving uncertainty about the timing and feasibility of such an achievement. Despite this uncertainty, the cryptographic community remains on edge, fully aware that developing and implementing new cryptographic schemes and protocols is a formidable undertaking. Cryptography that maintains its security even when confronted by adversaries wielding quantum computers is referred to as post-quantum cryptography. The pivotal distinction between post-quantum cryptography and traditional cryptography lies in the foundational problems upon which they rely. The focus of this research centers on a specific category of post-quantum digital signature algorithms: multivariate cryptography (specifically the Rainbow signature scheme) and hash-based signature algorithms (notably SPHINCS+).

Multivariate Public Key Cryptosystems (MPKCs) stand as post-quantum cryptography candidates, hinging their security on the intricate challenge of solving systems of multivariable quadratic equations. Rainbow, an MPKC signature scheme [6], exhibits efficient signature generation and verification. However, Rainbow, like other MPKCs, presents challenges in terms of substantial public and secret key sizes. The size of public keys in Rainbow is notably larger in the context of MANETs, and its performance, while comparable to current algorithms, falls short of requirements. An optimized version of Rainbow with reduced public key size exists, yet this comes at the expense of heightened computational demands. Notably, potential adoption of Rainbow may be hindered by royalty considerations.

Although multivariate public key cryptography (MPKC) schemes generally outperform RSA in computation, they encounter two significant hindrances. The first challenge pertains to the large sizes of their keys, while the second centers on their security reliance on both the multivariate quadratic (MQ) problem and the Isomorphism of Polynomials (IP) problem, rendering them susceptible to not only direct but also structural attacks.

Hash-based signature algorithms, exemplified by SPHINCS, derive their security from the underlying basic signing schemes. For SPHINCS+, a hyper-tree construction utilizing WOTS, a 7-bit reduction in expected security was reported [7]. Although SPHINCS+ is stateless, the degradation of security in relation to the number of generated signatures can pose challenges, particularly in distributed signing scenarios.

In response to these challenges, this research introduces a novel post-quantum cryptography algorithm aimed at achieving secure transmission and optimal execution time. The algorithm employs tweakable function sets tailored to diverse software signing use-cases across two post-quantum security levels. The results demonstrate the feasibility of this novel algorithm, showcasing minimal impact on key generation, encryption and decryption times, and

memory consumption, all while achieving superior outcomes.

2. MULTIVARIATE CRYPTOGRAPHY

Multivariate cryptography represents a distinctive paradigm within the realm of modern cryptography, characterized by its innovative reliance on multivariate polynomial equations to safeguard digital communication and protect sensitive information. In contrast to classical cryptographic approaches that draw from number theory or discrete logarithm problems, multivariate cryptography harnesses the complexity of polynomial equations to provide a robust foundation for encryption, decryption, and digital signatures.

The significance of multivariate cryptography is magnified in the context of modern security landscapes, which are increasingly exposed to the potential threats posed by quantum computers. While conventional cryptographic methods, such as RSA or ECC, face vulnerability to quantum attacks due to advancements in quantum computing, multivariate cryptography emerges as a promising contender for ensuring security in the post-quantum era. Its reliance on distinct mathematical problems positions it as a candidate for withstanding quantum-based attacks, potentially providing a robust alternative to traditional cryptographic systems.

The secret key, denoted as F = (M1, M2, ..., Mn), pairs with the public key F' = (M'1, M'2, ..., M'n) where M'i = ST * M'i * S. For generating a signature, the message m is hashed into h = hash(m), and the signature s is computed as s = F'^(-1)(h). During verification, given signature s for message m and h = hash(m), the equation F'(s) = h is checked, essentially inverting F' as part of the signing process. The underlying hard problems involve distinguishing F' from a random system of quadratic equations and the challenge of inverting a system of random quadratic equations (MQ). It's important to note that the difficulty of the first problem is influenced by how F' is generated.

Multivariate cryptography offers advantages like efficient secret key operations, compact signatures/ciphertexts, and cost-effective encryption. However, it exhibits larger public key sizes (up to 1 Mb) due to the public key F'. Its security relies on heuristic methods, and confidence in its security level is not yet high. Multivariate cryptography was somewhat dormant until the emergence of post-quantum cryptography, which has spurred efforts to enhance its security credibility.

2.1. Rainbow Signature scheme cryptography(RSSC)

The Rainbow signature scheme involves a series of polynomial operations and mathematical equations. Here's a high-level overview of the algorithm along with some simplified formulas to give you a sense of the process. Please note that these formulas are simplified for illustrative purposes and may not accurately represent the full complexity of the Rainbow scheme.

1. Key Generation:

Parameters: Choose parameters for the scheme, such as the number of layers (L), the number of polynomials per layer (n), and the sizes of the polynomials.

Central Map Generation: Create a central map that establishes the relationship between layers. This map helps generate the private and public keys.

Random Quadratic Polynomial Generation: Generate random quadratic polynomials for each layer. For each layer i, generate a set of quadratic polynomials:

$$Polynomial\ Q_i(x) = A_i x^2 + B_i x + C_i$$

Private Key Generation: Solve a system of multivariate quadratic equations to obtain the private key coefficients. This involves solving equations of the form:

$$Q_1(x_1) = 0$$

$$Q_2(x_2) = 0$$
$$\ldots$$
$$\ldots$$
$$Q_L(x_L) = 0$$

Public Key Derivation: Derive the public key from the private key using the central map.

2. Signature Generation:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Hashing: Hash the message M to be signed to obtain a digest D.

Equation Generation: Use the private key to generate a set of equations for the layers. For each layer i, generate an equation using the corresponding polynomial:

$Q_l(x_l) = D_i$

Solution: Solve the system of equations to obtain solutions for \(x_1, x_2, \ldots, x_L\). These solutions form the signature.

3.Signature Verification:

Hashing: Hash the received message M to obtain a digest D.

Equation Generation: Use the public key to generate a set of equations for the layers. For each layer i, generate an equation using the corresponding polynomial:

$$Q_l(x_l) = D_i$$

Combining Equations: Combine the results of the equations from each layer to verify the signature. If the equations hold, the signature is valid.

Limitations of the Rainbow Signature Scheme:

Efficiency and Key Size: Rainbow signatures can have relatively large key sizes compared to some other signature schemes, which can impact efficiency, especially in resource-constrained environments.

Key Generation and Management: The key generation process for Rainbow can be computationally intensive, and managing the large number of parameters and coefficients can be complex.

Cryptanalysis: As with any cryptographic scheme, the security of Rainbow relies on the difficulty of certain mathematical problems. If advances in cryptanalysis reveal weaknesses, the security of the scheme could be compromised.

Not Widely Adopted: Rainbow is not as widely adopted as some other signature schemes like RSA or ECDSA. This could lead to limited support in software libraries and applications.

3. HASH BASED SIGNATURE

Hash-based signature schemes possess the advantageous characteristic of not being bound to a specific hash function [10]. This attribute grants flexibility, allowing the hash function to be modified for reasons of enhanced efficiency or heightened security. Given that hash functions are subject to a finite operational lifespan, the ability to substitute one function for another while preserving the foundational structure significantly contributes to the longevity of hash-based signature schemes. In the context of signing, the utilization of a hash function is imperative. It is assumed that this hash function exhibits resistance to inversion, ensuring its preimage resistance. Remarkably, this single property serves as a foundational cornerstone for constructing a comprehensive signature scheme. Key aspects of hash-based signature schemes include:

Minimalist Assumption: The scheme is built upon a minimalist assumption, requiring only a one-way function to establish its foundations.

High Confidence in Security: Hash-based schemes instill a high level of confidence in their security due to the robustness of the underlying cryptographic properties.

Challenge and Construction: The primary challenge lies in creating a signature scheme based on the properties of a given one-way function.

Message Independence: Notably, the message is chosen after the signature key has been made public, enhancing the versatility and applicability of the scheme.

The adaptable nature, strong security assurances, and foundational attributes of hash-based signature schemes position them as a resilient and versatile option in modern cryptographic landscapes.

3.1. SPHINCS+

The SPHINCS+ algorithm involves a complex combination of cryptographic primitives, including tree-based hashing, WOTS (Winternitz

One-Time Signature), and FORS (Forsyth-Ors Signatures). Below, I'll provide a high-level overview of the SPHINCS+ algorithm along with simplified formulas to give you an idea of its structure. Please note that these formulas are highly simplified and may not capture all the details of the actual algorithm.

1. Key Generation:

Parameters: Choose security parameters, such as the desired level of security and hash functions.

Secret and Public Key Generation: Generate a secret key SK and compute the corresponding public key PK by hashing the secret key.

2. Tree-Based Hashing:

Merkle Tree Construction: Divide the message into blocks m_1, m_2, …, m_n), and compute the hash of each block:

$$H_1 = H(m_1)$$
$$H_2 = H(m_2)$$
...
...
...
$$H_n = H(m_n)$$

Build a binary Merkle tree by hashing adjacent nodes together:

$$T_1 = H(H_1, H_2),$$
$$T_2 = H(H_3, H_4),$$
...
...
...
$$T_{n/2} = H(H_{n-1}, H_n).$$

3. WOTS (Winternitz One-Time Signature):

Signature Generation: For each leaf node in the Merkle tree, generate a WOTS signature:

$$W_1 = WOTS_{SK}(H_1),$$
$$W_2 = WOTS_{SK}(H_2),$$
...
...
$$W_{n/2} = WOTS_{SK}(H_{n/2}).$$

These signatures become part of the SPHINCS+ signature.

4. FORS (Forsyth-Ors Signatures):

Signature Generation: Generate a short-term key pair SK', PK' and a FORS signature:

$$S_{FORS} = FORS_{SK'}(H(T_1, T_2, ..., T_{n/2})).$$

Include the FORS signature in the SPHINCS+ signature.

5. Final Signature Generation: Combine the WOTS and FORS components to form the final SPHINCS+ signature:

$$SPHINCS{+}SK_m = W_1, W_2, ..., W_{n/2}, S_{FORS}.$$

6. Signature Verification: To verify the SPHINCS+ signature, the verifier repeats the steps of tree-based hashing, computes the WOTS signature verification, and verifies the FORS signature.

Limitations of the SPHINCS+ Algorithm:

Signature Size: SPHINCS+ signatures can be relatively large, which may impact transmission and storage efficiency.

Key Generation Complexity: Key generation in SPHINCS+ can be computationally expensive due to the need to generate various short-term key pairs and signatures.

Verification Complexity: Verifying SPHINCS+ signatures requires significant computational effort, which can impact performance, especially in resource-constrained devices.

Dependency on Hash Functions: The security of SPHINCS+ relies on the collision resistance and preimage resistance of the chosen hash functions. If these assumptions are violated, the security of the scheme could be compromised.

Limited Real-World Deployment: SPHINCS+ and other post-quantum cryptographic schemes are still being researched and developed. Their real-world deployment and integration into existing systems may face challenges and require careful consideration.

Dynamic Environments: While SPHINCS+ is designed to be secure in a post-quantum world, its performance and security in dynamic and rapidly changing network environments like MANETs need to be thoroughly evaluated.

5. PROPOSED NOVEL POST QUANTUM CRYPTOGRAPHY DIGITAL SIGNATURE:

In a Mobile Ad hoc Network (MANET), nodes communicate directly, bypassing centralized resources and established infrastructure. Given that mobile nodes operate on battery power, the instantaneous connectivity in this environment may lead to non-acknowledgement behavior in

network-enabled heterogeneous devices, potentially causing network degradation. To counter this performance decline, we propose an Incentive technique based on Post-Quantum principles for addressing non-acknowledgement data in MANETs. This technique employs an Everything tweakable hash function to establish an end-to-end reliable solution, integrating location-aware post-quantum encryption into the network while mitigating the non-acknowledgement issue.

Post-quantum computing, capable of nearly instantaneous resolution of complex mathematical problems, stands in stark contrast to the billions of years required by traditional computing machines. This research advocates for the inclusion of data encryption in the post-quantum era. Notably, Rainbow and hash-based signatures are employed within post-quantum cryptography, providing unique solutions. These algorithms share a fundamental component—the use of a One-Time Signature (OTS) scheme. The utilization of multiple OTS key pairs is consolidated through a Merkle Tree, facilitated by a hash tree structure. Numerous enhancements to the Merkle construction have vastly improved its efficiency.

A challenge inherent to hash tree signatures is the issue of a forger generating multiple instances of their own WOTS+ public key/private key pairs in an attempt to replace a validated WOTS+ key in the upper tree. This forger could use the same hash function as the upper tree's leaves to match and switch out keys. This vulnerability is exacerbated when multiple legitimate signers use the same hash function, potentially leading to a detect-one-of-many (DOOM) scenario. To counter this, SPHINCS+ employs a family of closely related hash functions, with the selection known as the "tweak." By allowing the tweak to vary based on user-specific parameters, input size, or leaf index, SPHINCS+ thwarts various attack vectors, such as multi-targeting and length extension attacks.

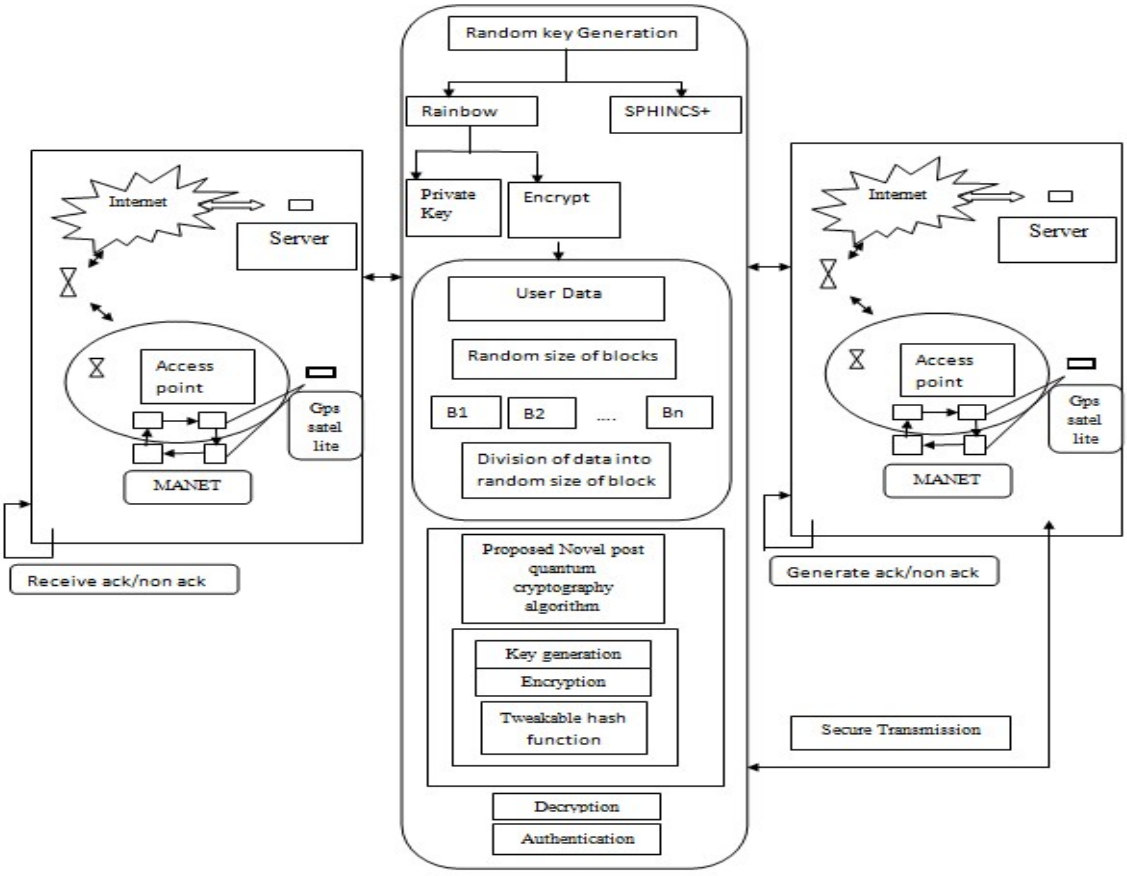


Figure 5: Proposed Framework

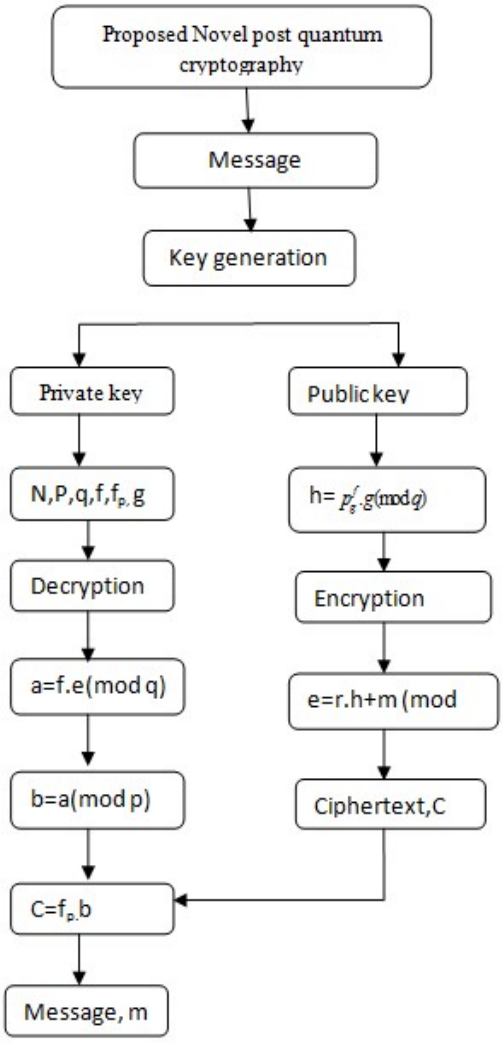
SPHINCS+ boasts several attributes that position it at the forefront of the post-quantum landscape. These include resilience against quantum attacks, robust concurrent performance, parallelism, security based on intractability assumptions, and solutions to longstanding cryptographic challenges. While these attributes demonstrate potential security benefits for classical cryptographic systems in theory and experimentation, implementing them in energy-constrained MANETs requires a streamlined post-quantum algorithm tailored for MANETs. This is where the Everything tweakable hash function shines, providing an end-to-end reliable solution. By incorporating location-aware post-quantum encryption and decryption, the algorithm addresses non-acknowledgement behavior within a bi-directional MANET environment. The proposed algorithm also seeks to assess the impact of non-acknowledgement data through novel post-quantum cryptography techniques.

The primary objective of this research was to leverage post-quantum cryptography to secure data transmission within MANET networks. By utilizing the unique attributes of SPHINCS+ and the Everything tweakable hash function, the study aimed to enhance the security and reliability of data communication in the challenging and dynamic context of MANETs.

Proposed Novel post quantum cryptography Digital signature Algorithm:

Definition of variables

N – the polynomials in the ring R with degree N − 1. p and q – are small and large modulus respectively, which are used for the reduction in coefficients in the encryption/decryption of data. f and g – polynomials used to process the public key h, r – a random blinding polynomial used to distort data, m–is the message to be encrypted/decrypted represented in polynomial form.



Upon access to the manet, users are given the opportunity to either edit already uploaded data or upload fresh data, these data are secured using the proposed novel post quantum cryptography. NPQC algorithms consists of three algorithms: key generation algorithm, which produces a public and a private key, an encryption algorithm, and a decryption algorithm.

Key generation

The sender computes f·fp = 1(mod p) and f·fq = 1(mod q) and then processes the public key h using:

$$h = pfq \cdot g(\text{mod } q). \quad (6)$$

Encryption

To encrypt a message, the following is processed:

$$e = r \cdot h + m(\text{mod } q). \quad (7)$$

Decryption
The following is computed to decrypt the message

$$a = f \cdot e(\text{mod } q), \quad (8)$$
$$b = a(\text{mod } p), \quad (9)$$
$$C = fp \cdot b, \quad (10)$$

Below are the algorithms for processes of the proposed novel post quantum cryptography

Algorithm: Proposed novel post quantum cryptography -key generation
Input: parameters for encryption (p, f, g, q)
Output: Keys (h)
Begin
i. Compute $f \cdot fp = 1(\text{mod } p)$ and
ii. $f \cdot fq = 1(\text{mod } q)$
iii. $h = p \cdot fq \cdot g \ (\text{mod } q)$
iv. Return (h)
End
Algorithm 5: Proposed novel post quantum cryptography -encryption
Input: Parameters for encryption (m, r, h, q)
Output: Cipher text (e)
Begin
i. Compute $e = r \cdot h + m \ (\text{mod } q)$
ii. Return (e)
End
Algorithm 6: Proposed novel post quantum cryptography -decryption
Input: Parameters for encryption (e, f, p, q)
Output: Plain text (c)
Begin
i. Compute a = f·e(mod q)
ii. Compute b = a(mod p)
iii. C = fp· b
iv. Return (c)
End

6. EXPERIMENTAL RESULTS

In this section, we delve into the setup and software implementation nuances, as well as the challenges faced, when deploying Post-Quantum Cryptography (PQC) cryptosystems on 32-bit CPU single-board devices and mobile devices. The construction of PQC schemes can be undertaken from the ground up, following the blueprints detailed in research papers and employing a variety of programming languages like C/C++, JAVA, Python, among others. However, such endeavors necessitate the creation and integration of numerous mathematical, cryptographic, and arithmetic modules—examples include Gaussian samplers and matrix/polynomial multiplication. This "from-scratch" approach may inadvertently introduce security vulnerabilities and performance bottlenecks.

To counteract these challenges, open source initiatives and libraries have emerged, streamlining the implementation of PQC schemes and associated mathematical functions. Notable examples encompass projects like Codecrypt (the post-quantum cryptography tool), Java Library (jLBC), libPQP (Python post-quantum library), and liboqs library (the Open Quantum Safe project, Stebila and Mosca, 2016). By harnessing these libraries housing PQC primitives, developers can achieve greater efficiency and stability, mitigating potential security concerns and enhancing overall performance.

Key Generation Time : A key pair is generated for each user, resulting in distinct private and public keys. Despite the key length being consistent, the time required for key generation varies.

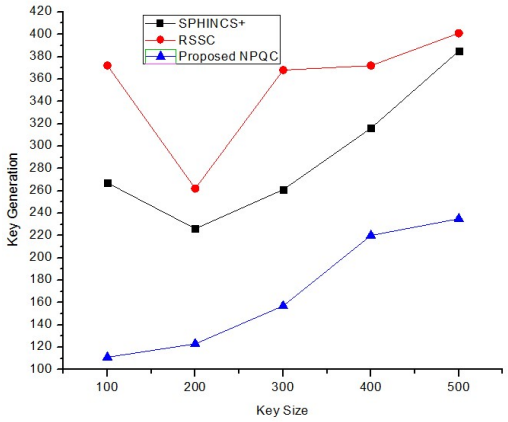


Figure 6: Key Generation Time

Smaller key sizes exhibit quicker generation times. Figure 6 depicts the comparison between the NPQC cryptosystem and the RSSC, SPHINCS+ cryptography algorithms in relation to key size and key generation. The visual representation highlights that the proposed NPQC outperforms RSSC and SPHINCS+ in terms of key generation within the realm of post-quantum cryptography.

Encryption / Decryption Time : The measured runtime is expressed in milliseconds. Figure 7

illustrates the graphical representation of encryption runtime, while Figure 8 depicts decryption runtime. Encryption time signifies the duration taken by the data owner to convert original data into encrypted form, while decryption time refers to the time taken for the data owner to decrypt encrypted data into its original state. Both figures highlight the encryption and decryption time patterns of the proposed algorithm in relation to varying data sizes.

Encryption Time: This parameter gauges the speed of the proposed system's operation within the context of MANET, as it pertains to different input sizes.

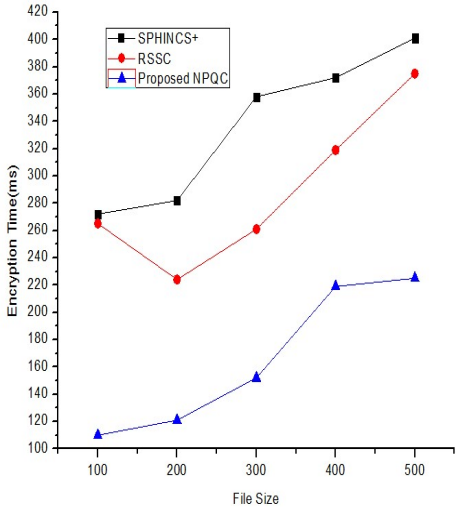


Figure 7: Encryption Time

It quantifies the time taken by an algorithm to transform plaintext into ciphertext. To assess the efficiency of the proposed NPQC algorithm in comparison to RSSC and SPHINCS+, we analyze their respective encryption times. The ensuing graph exhibits the performance of RSSC, SPHINCS+, and the proposed NPQC algorithm in terms of encryption time. Based on the findings, it is evident that the proposed algorithm outperforms the others.

Decryption Time : Decryption time denotes the duration required for an algorithm to transform ciphertext into plaintext. In this context, we conduct a comparative analysis of the decryption times associated with the RSSC, SPHINCS+, and the proposed NPQC algorithm. The performance of these algorithms in terms of decryption time is presented through both a graph and a table. The observed outcomes affirm the superior performance of the proposed algorithm compared to the others.

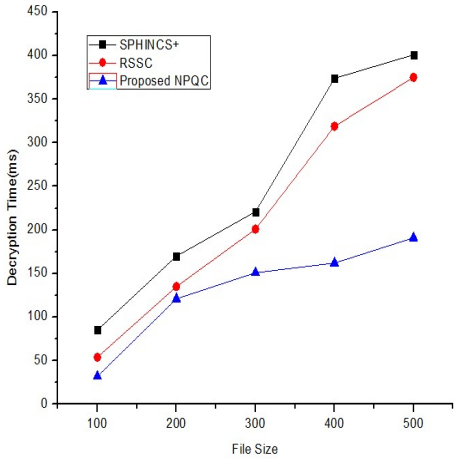


Figure 8: Decryption Time

Security level: The analysis of security encompasses the RSSC, SPHINCS+, and the proposed NPQC algorithms, a critical concern within the context of MANET. The significance of security within MANET is paramount. Figure 9 offers a comparative view, centering on the security levels, between the proposed NPQC algorithm and its counterparts. The security level is modulated based on the quantity of records.

In instances where the record count reaches 3000, the security level of the proposed NPQC algorithm stands at 17. In contrast, the RSSC and SPHINCS+ algorithms exhibit lower security levels of 12 and 6, respectively. This discrepancy underscores the heightened security of the proposed NPQC algorithm. Across all record quantities, the proposed NPQC algorithm consistently demonstrates superior security levels compared to the other alternatives.Hence, drawing from the insights presented in the graph and description, it is unequivocally evident that the proposed NPQC algorithm surpasses the security capabilities of the RSSC and SPHINCS+ algorithms.

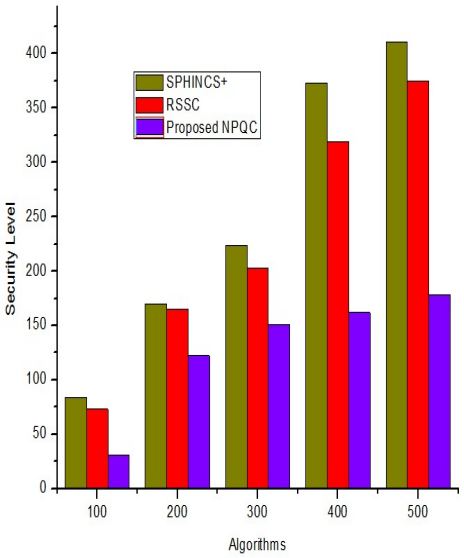


Figure 9: Security Level

Execution Time(s): The execution time stands as a pivotal performance parameter that significantly influences the overall efficacy of the Novel Post Quantum Cryptography (NPQC) algorithm. In this context, the evaluation of encryption and decryption execution times is conducted with considerations of message size (k), public key, and illustrated through Figure 5. Surprisingly, the execution time exhibits improvement as plaintext size increases, while maintaining a constant public key size.

This observation, although seemingly counterintuitive to the conventional understanding that time should elongate with larger message bit sizes, is reconciled by a constraint that leads to decreased time with expanding plaintext size. As the plaintext size expands, the polynomial degree (t) diminishes, reinforcing the trend toward enhanced execution time. Figure 10 accentuates the variation in execution times for encryption and decryption, separately juxtaposing the RSSC, SPHINCS+, and the proposed NPQC algorithms. Notably, the proposed NPQC algorithm outperforms the others in terms of execution time.

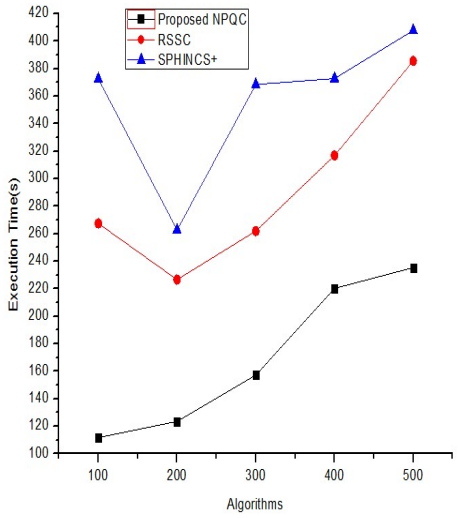


Figure 10: Execution Time

Memory consumption (mega bytes): Memory consumption pertains to the volume of memory utilized within a MANET, signifying the occupied capacity of the CPU. Within the proposed algorithm, a tweakable hash function is employed, converting messages into memory-efficient bit structures. This technique, coupled with the encryption process, reduces the size of both messages and keys, thereby conserving memory storage. When scrutinizing digital signature submissions, the RSSC, SPHINCS+, and NPQC algorithms stand out for their minimal memory usage across various security levels. Figure 1 visually presents the memory consumption levels associated with key generation, signing, and verification processes. While other competitive schemes are explored in subsequent sections, it is evident that the RSSC, SPHINCS+, and NPQC algorithms outperform their counterparts in terms of memory conservation.

The results illuminate a pattern where an increase in the number of nodes corresponds to heightened memory consumption at each node, particularly for session sizes spanning up to 300 units to transmit 1000 characters. Remarkably, the proposed NPQC algorithm stands out with the lowest memory consumption in comparison to the other algorithms.

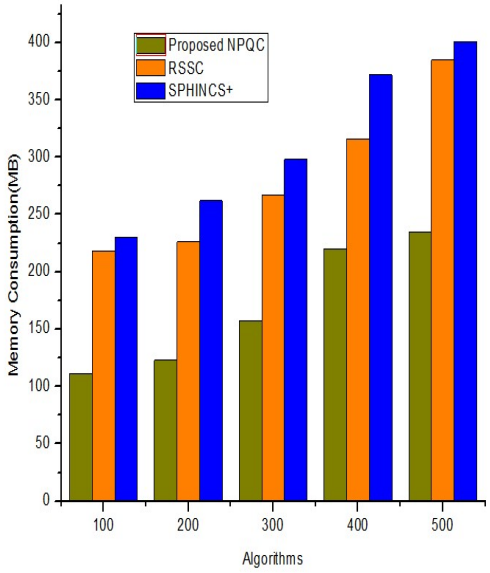


Figure11: Memory Consumption

7.CONCLUSION

In this study, we introduce a novel post-quantum cryptographic system designed to operate seamlessly within the MANET environment, ensuring data confidentiality and relieving users of the responsibility of self-securing their data. Our approach involves the proposal of three distinct algorithms. Prior to data encryption, a dual-phase key encryption is employed. Initially, the Rainbow algorithm encrypts the keys, storing them securely in a private database for subsequent decryption of the original data. Subsequently, the sphnics+ algorithm encrypts the keys utilized in the encryption of the original data by the NPQC algorithms.

To assess the efficacy of our proposed methodologies, a comparative analysis is conducted against alternative post-quantum cryptographic algorithms. This evaluation encompasses various parameters, including key generation time, encryption/decryption time, security level, execution time, and memory consumption. Our experimental findings unequivocally demonstrate that our proposed approach boasts a robust security framework, streamlined execution, and minimal memory usage. In contrast, competing algorithms, often entailing encryption and decryption processes for each data block, result in substantial time expenditure.

REFERENCES:

[1]. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26(5), 1484–1509 (1997)

[2]. DeAngelis, S.F.: Closing In On Quantum Computing. Wired (2014)

[3]. Pop, I.M., Geerlings, K., Catelani, G., Schoelkopf, R.J., Glazman, L.I., Devoret, M.H.: Coherent suppression of electromagnetic dissipation due to superconducting quasiparticles. Nature 508(7496), 369–372 (2014)

[4]. Saeedi, K. et al: Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28. Science 342(6160), 830–833 (2013)

[5]. Rich, S., Gellman, B.: NSA seeks to build quantum computer that could crack most types of encryption. The Washington Post (2014)

[6]. Ding, J. and Schmidt, D., "Rainbow, a New Multivariable Polynomial Signature Scheme", ACNS'05, Springer LNCS vol. 3531, pp. 164–175, 2005.

[7]. Aumasson, J.-P., and Endignoux, G. Clarifying the subset-resilience problem. IACR Cryptology ePrint Archive (2017), 909.

[8]. A. Kipnis, J. Patarin, L. Goubin: Unbalanced Oil and Vinegar schemes. EUROCRYPT 1999, LNCS vol. 1592, pp. 206 - 222. Springer, 1999.

[9]. Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, Applied Cryptography and Network Security, pages 164–175, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg

[10]. Denis Butin, Stefan-Lukas Gazdag, and Johannes Buchmann. Real-world postquantum digital signatures. In Cyber Security and Privacy Forum, pages 41–52. Springer, 2015.

[11]. Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. "The SPHINCS+ signature framework." In: Conference on Computer and Communications Security – CCS '19. Ed. by XiaoFeng Wang and Jonathan Katz. To appear. ACM, 2019. url:

https://eprint.iacr.org/2019/1086 (cit. on pp. 17, 43, 92, 102–104, 106, 111, 146, 215, 259).

[12]. Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas H ulsing, and Markus Ruckert. On the security of the Winternitz one-time signature scheme. In A. Nitaj and D. Pointcheval, editors, Africacrypt 2011, volume 6737 of Lecture Notes in Computer Science, pages 363{378. Springer Berlin / Heidelberg, 2011

[13]. Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. XMSS — A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In Bo-Yin Yang, editor, *Post-Quantum Cryptography 2011*, volume 7071 of *Lecture Notes in Computer Science*, pages 117–129. Springer Berlin / Heidelberg, 2011.

[14]. Johannes Buchmann, Erik Dahmen, and Michael Schneider. Merkle tree traversal revisited. In Johannes Buchmann and Jintai Ding, editors, *Post-Quantum Cryptography*, volume 5299 of *Lecture Notes in Computer Science*, pages 63–78. Springer Berlin / Heidelberg, 2008.

[15]. Lamport, L.: Constructing Digital Signatures from a One Way Function. Tech. rep., SRI International Computer Science Laboratory (1979)

[16]. Dods, C., Smart, N., Stam, M.: Hash Based Digital Signature Schemes. In: Cryptography and Coding, Lecture Notes in Computer Science, vol. 3796, pp. 96–115. Springer (2005)

[17]. Hülsing, A.: W-OTS+ — Shorter Signatures for Hash-Based Signature Schemes. In: AFRICACRYPT. Lecture Notes in Computer Science, vol. 7918, pp. 173–188. Springer (2013)

[18]. Merkle, R.C.: A Certified Digital Signature. In: CRYPTO. Lecture Notes in Computer Science, vol. 435, pp. 218–238. Springer (1989)

[19]. Merkle, R. C. (1987, August). A digital signature based on a conventional encryption function. In Conference on the theory and application of cryptographic techniques (pp. 369-378). Springer, Berlin, Heidelberg.

[20]. Denis Butin, Andreas Hülsing, Aziz Mohaisen, and Stefan-Lukas Gazdag. XMSS: Extended Hash-Based Signatures. Internet-Draft draft-irtf-cfrg-xmss-hash-basedsignatures- 09, Internet Engineering Task Force, March 2017. URL https://datatracker.ietf.org/doc/html/draft-irtf-cfrg xmss-hash-basedsignatures- 09. Work in Progress.