Integrating Textual Name Values and Dynamic Key Generation with Advanced Non-Linear Transformations for Encryption

Sukash L[1], Ahmed Samathani M B[2], Sudharsan K[3], Vignesh V[4], and Tamil Selvan R[5]
[1,3,4,5]*Student, Department of Information Technology, SRM Valliammai Engineering College, Chengalpattu, Tamil Nadu, India*
[2]*Assistant Professor, Department of Information Technology, SRM Valliammai Engineering College, Chengalpattu, Tamil Nadu, India*

Abstract - The increasing demand for robust encryption methods in the digital age has driven the development of innovative approaches within cryptographic systems. This project presents a novel cryptographic framework that integrates textual name values and dynamic key generation with advanced non-linear transformations, aimed at enhancing encryption security. To achieve this, the system employs lattice-based cryptography for secure key exchange, utilizing the Number Theoretic Transform (NTT) to facilitate efficient polynomial operations. Coupled with Advanced Encryption Standard (AES) for symmetric encryption, the framework incorporates a unique character-to-name mapping and dynamically generated S-boxes, which introduce additional layers of complexity to the encryption process. Extensive testing of the system reveals its robustness, highlighted by an average 51.72% bit change during avalanche effect tests, statistically significant key randomness, and strong resistance to differential attacks. This hybrid approach effectively combines post-quantum security features with the efficiency of symmetric encryption, positioning itself as a promising solution for high-security applications across financial, governmental, and personal data protection domains.

Keywords - AES encryption, character-to-name mapping, dynamic S-box, hybrid cryptosystem, lattice-based cryptography, Number Theoretic Transform (NTT), post-quantum cryptography.

I. INTRODUCTION

Cryptography is an essential field in modern technology, ensuring the confidentiality, integrity, and authenticity of data. At its core, cryptography involves the creation and application of algorithms to secure communication between parties. It leverages mathematical principles to transform readable information (plaintext) into an unreadable format (ciphertext), which can only be reversed by those with the correct decryption key. The fundamental goal is to prevent unauthorized access to sensitive information, ensuring that only intended recipients can decode and understand the message.

There are two primary types of cryptography: symmetric and asymmetric. Symmetric cryptography relies on a single key for both encryption and decryption. Popular examples include the Advanced Encryption Standard (AES), which is widely used due to its efficiency and strength. In contrast, asymmetric cryptography, also known as public-key cryptography, uses a pair of keys — one public and one private.

Cryptographic algorithms are evaluated based on several criteria, including their resistance to various types of attacks, speed, and key size. In recent years, advancements in lattice-based cryptography have garnered attention for their potential to resist quantum attacks, providing a pathway toward more secure future-proof encryption. Furthermore, hash functions, such as SHA-256, play a crucial role in ensuring data integrity by producing a fixed-size hash from variable-length input data. Hash functions are commonly used in both cryptography and blockchain technologies to verify the authenticity of digital assets.

II. PROBLEM STATEMENT & OBJECTIVES

Conventional encryption techniques, such as static key generation and predictable transformation algorithms, often leave sensitive information vulnerable to brute-force attacks and other cryptographic vulnerabilities. There is a pressing need for advanced cryptographic systems that can adapt to evolving security threats while maintaining high levels of efficiency and effectiveness. This project addresses these challenges by proposing a novel framework that leverages textual name values

and dynamic key generation alongside advanced non-linear transformations. By integrating these elements, the proposed system aims to significantly enhance the security of encrypted data, making it more resilient against a variety of attacks. The integration of lattice-based cryptography and the dynamic generation of S-boxes will provide an additional layer of complexity and security.

The project's objectives are centered around improving cryptographic security by integrating advanced techniques to enhance encryption systems. These objectives include integrating textual name values into key generation to increase encryption complexity and randomness; developing dynamic key generation algorithms using lattice-based cryptography for enhanced security; implementing advanced non-linear transformations like NTT to strengthen encryption against cryptanalytic attacks; incorporating dynamic S-box generation in AES to improve resistance against known-plaintext attacks; and using SHA-256 hashing to ensure message integrity and detect tampering. These objectives collectively aim to develop a comprehensive encryption solution that adapts to modern security challenges while providing flexibility, robustness, and enhanced data protection.

III. EXISTING SYSTEM

The landscape of cryptographic systems is dominated by several traditional techniques that aim to secure sensitive data. However, these existing systems face significant challenges regarding security, adaptability, and efficiency. The integrity of cryptographic frameworks is crucial for maintaining the confidentiality and authenticity of digital communications. Current methods often rely on static key generation and predictable algorithms, making them susceptible to various types of attacks, including brute-force and advanced cryptanalysis. Several prevalent systems highlight the limitations of current approaches:

A. Static Key Generation Systems:
These systems utilize a fixed key for both encryption and decryption, leading to vulnerabilities. The static nature of the keys makes them more easily targeted by attackers who can exploit their predictability. Once compromised, all data encrypted with that key is at risk, highlighting the need for a more dynamic approach to key generation.

B. Traditional AES Encryption:
The Advanced Encryption Standard (AES) is widely regarded for its speed and security in symmetric encryption. However, AES's reliance on static S-boxes can render it vulnerable to certain cryptanalytic techniques. Its lack of dynamic key generation limits its effectiveness against emerging threats, especially in a post-quantum context where adaptability is essential.

C. Public Key Infrastructure (PKI):
PKI employs asymmetric cryptography using a pair of keys: public and private. While PKI enhances security, it remains susceptible to attacks if the private key is compromised. Moreover, managing keys and certificates can introduce complexities and potential points of failure within the system.

D. Hash Functions:
Cryptographic hash functions, such as SHA-256, play a critical role in ensuring data integrity by producing a unique fixed-size hash from variable-length input data. However, the effectiveness of these functions depends on their resistance to collision and pre-image attacks. The evolving landscape of computing power continually poses new threats to the robustness of existing hash functions.

The limitations of these existing systems highlight the necessity for innovative cryptographic frameworks that integrate dynamic elements to enhance security, complexity, and resilience against a broader array of attacks.

IV. PROPOSED SYSTEM

The proposed system addresses the vulnerabilities present in traditional encryption methodologies while enhancing security through advanced techniques. The main objective of our project is to develop a robust encryption framework that ensures data integrity, confidentiality, and adaptability in real-world applications. By utilizing lattice-based cryptography, which employs non-linear transformations through techniques like compression, decompression, and Number Theoretic Transform (NTT), the system generates secure and session-specific keys that significantly enhance resistance to brute-force attacks and cryptographic weaknesses.

Additionally, the dynamic S-box is generated from the AES key derived through the lattice-based key generation process, allowing for unique permutations of S-box values for each encryption session, thereby

improving resilience against cryptanalysis. To further protect sensitive plaintext data, character-to-name transformations are implemented, obfuscating the data before encryption and adding an extra layer of security against unauthorized access.

The integration of advanced non-linear transformations, particularly through the NTT and related operations, adds complexity to the encryption process, enhancing resistance to linear and differential attacks. To ensure data integrity, SHA-256 hashing is employed to detect any tampering with the encrypted messages. By appending hash values to the ciphertext, users can verify the authenticity of the decrypted data, ensuring that the information remains intact and trustworthy.

The combination of these components offers significant advantages over existing encryption technologies, as the use of lattice-based methods prevents the addition, alteration, or deletion of keys and data once established, ensuring the security of sensitive information.

V. SYSTEM ARCHITECTURE

The architecture of the cryptographic system illustrates various entities involved in the cryptographic system. The proposed cryptographic system is structured around the following key components:

A. Lattice-Based Key Generation:

The key generation process utilizes lattice-based cryptography, specifically leveraging the compression, decompression, and Number Theoretic Transform (NTT) operations. These steps serve as non-linear transformations that significantly enhance the complexity and unpredictability of the keys generated. The NTT and its inverse (INTT) facilitate efficient polynomial arithmetic, allowing for the generation of secure, session-specific keys that resist brute-force attacks and ensure adaptability for each encryption session.

B. S-Box Generation:

A dynamic S-box is employed for the AES encryption process, generated from the AES key derived through lattice-based key generation. This S-box adapts based on the key, providing a unique permutation of S-box values for each encryption session.

C. Character-to-Name Transformations:

The system incorporates character-to-name transformations that convert plaintext data into secure formats, ensuring that sensitive information is obfuscated during encryption.

D. Message Integrity Verification:

To ensure the integrity of the encrypted messages, SHA-256 hashing is incorporated into the system. By appending hash values to the ciphertext, users can verify the authenticity of the decrypted data.

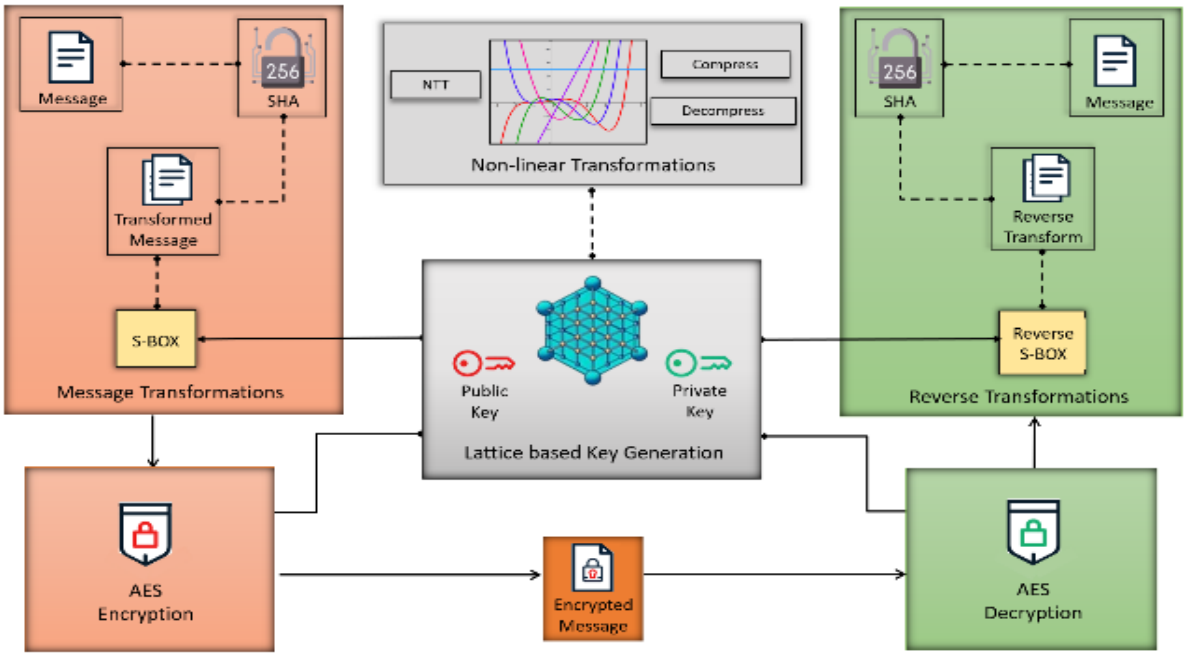

Figure 1. Cryptographic System Architecture

The system initiates the encryption process by generating a secure key using lattice-based methods, applying NTT and INTT to enhance the key's complexity. The unique AES S-box is generated dynamically, which is then employed in the encryption of the transformed data. Throughout the process, SHA-256 hashes are created and attached to the encrypted messages, allowing for integrity checks upon decryption. This comprehensive approach not only enhances the security of the encryption process but also provides users with confidence in the integrity and authenticity of their data.

VI. RESULTS & DISCUSSION

The process commences with the implementation of lattice-based cryptography to generate unique, session-specific keys. The cryptographic system leverages lattice-based cryptography for dynamic key generation, providing highly secure and session-specific keys for each encryption session. By using polynomials and noise-based error polynomials, keys are generated dynamically, ensuring that no two encryption sessions use the same key. The system employs Number Theoretic Transform (NTT) and Inverse NTT to operate on polynomials, creating a robust and mathematically complex foundation for key generation.

AES Key:

```
/oZjYzKCry3+g/ulJ0jiNkdCV3fpiWAR+RtDld3O7Z8=
```

Figure 2. Generated AES key

This figure shows the AES key that is generated through the lattice-based cryptography. Now, the original plaintext is combined with its SHA-256 hash This hash ensures message integrity and helps verify any changes. It secures the plaintext before encryption.

Transformed_plaintext:

```
"HarryEmilyLiamLiamOscarPipeTwoCharlieFrankTwoFourDannyBenAliciaFiveFrankBenZeroAliciaThreeZero
EmilyTwoSixEmilyEightThreeBenTwoAliciaCharlieFiveBenNineEmilyTwoNineEmilyOneBenOneSixOneEmilyFi
veCharlieOneFrankAliciaSevenFourTwoFiveEmilySevenThreeZeroFourThreeThreeSixTwoNineThreeEightBen
NineEightTwoFour"
```

Figure 3. Transformed message

This figure displays the transformed message through character-to-name mapping, adding complexity. This obfuscation technique enhances security before encryption. Each character is uniquely mapped for unpredictability.

Figure 4 displays the S-box which is generated for each encryption session based on the AES key. This S-box is dynamically created, which uses the key to create a permutation of byte values. This S-box generation operates independently of the AES encryption process, but it still leverages the AES key to produce a customized S-box for each encryption session. The S-box adds an additional layer of security, ensuring that each encryption session uses a different permutation of values.

Sbox:

225	184	170	65	93	45	118	187	4	116	9	253	166	173	185	95
101	159	106	226	1	27	18	54	229	152	215	150	42	24	108	72
32	235	120	22	10	62	47	59	53	188	192	13	130	189	205	110
251	33	12	15	246	198	221	149	121	147	39	34	11	97	247	140
56	113	105	141	230	85	167	162	114	178	232	131	125	17	29	44
211	195	237	90	179	209	43	36	52	25	91	233	255	57	239	213
142	2	20	151	60	252	234	73	244	80	241	76	49	200	238	161
158	30	145	55	7	242	35	199	138	193	182	23	248	84	135	115
122	222	82	64	160	123	136	119	61	196	227	87	77	228	100	69
204	74	103	31	117	40	186	203	243	156	3	153	0	214	201	207
171	143	98	132	224	254	107	104	83	157	208	175	92	216	71	172
183	169	96	220	21	137	127	50	66	128	5	210	194	37	164	139
86	99	78	249	250	16	148	181	111	245	219	206	129	88	190	218
51	109	165	134	112	180	223	8	38	174	126	28	217	177	236	191
102	41	79	124	19	89	48	81	197	240	94	67	146	46	26	231
70	6	75	155	154	133	212	68	14	144	163	58	202	168	176	63

Figure 4. S-box generated by the AES key

Final_ciphertext:

```
"LCgn9eeyL/+DkoRQvtP1aXG0vM5Z2h6YZmBXCzg4gCDC2BoiyZcenKAS4Q/S17Hs7zR5JX8lMiFxoW3bFtsIcCfGK2sGYS
zHlzQmP6PhBdbHDn7jWtEgqApVgVZa87vTWGlqBDeQjMyGYdIY52MSRzWTghOAni1pJGkHzCkiCa4wS0IzSSG4c3AjM9dVb
jS1/p6fAi79FEikYLKoOYEi43sXiK5ixi4Q8fP09jB+omxHfMx/Gq/W6jHiSgfJH3fdkIgm4303CI5wfYKNAw8uGdTWxKG2
fNSMOnVMMV1Z2DC0TooIjT6tM1mkvr1Qf9fX3hL/W8ZNo0tKJx/UxxLU4kfqebEjv/MmuN5Q047e9Og0ZDPYdteZ7WRTTnQ
bKuuaeg56hSIjxNm3BWXy6vB9GJcSM0aYwkMdeooFVwdSUlGKbL9TxfWSjA=="
```

Figure 5. Encrypted message

The above figure presents the final encrypted message as ciphertext, secured with AES and the dynamic S-box. This result is a secure, unreadable output. Only decryption with the right key can reveal the original message.
The process is then reversed by applying the inverse transformations of the S-box and character name mappings, followed by hash verification. This sequence of steps ensures that the original plaintext is accurately recovered, maintaining the integrity and confidentiality of the data throughout the encryption and decryption processes.

The implemented system undergoes thorough testing to validate its security and effectiveness. The following tests are conducted:

A. Avalanche Test:
The Avalanche Test was conducted to evaluate the sensitivity of the ciphertext to minor changes in the plaintext. The test involved modifying a single bit in the plaintext and observing the resultant change in the ciphertext.

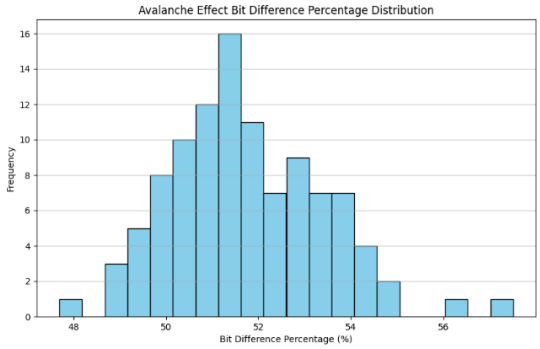

Figure 6. Avalanche Effect

B. Statistical Randomness:
Statistical randomness tests assess the quality of the generated keys, determining whether they exhibit uniform distribution and unpredictability. Key properties analyzed include the frequency of bits and runs of consecutive bits. The results for the test are as follows

- Frequency Test p-value: 0.7345
- Runs Test p-value: 0.1710
- Entropy: 7.9348 bits per byte

These values suggest that the randomness of the generated keys is statistically significant.

C. Performance Benchmarking:
This measures the efficiency and performance of the encryption and decryption processes by analyzing the time taken and speed for various message sizes.

Message Size (Bytes)	Encryption Time (s)	Decryption Time (s)
1024	0.000364	0.000900
10240	0.002434	0.004222
102400	0.33642	0.054470

Table 1. Performance Benchmarking

D. Differential Cryptanalysis:
Differential cryptanalysis examines how differences in input can affect the resultant output, which is vital for assessing the strength of the algorithm against such attacks. A strong resistance indicates that it is difficult for an attacker to derive information about the plaintext. The average bit difference observed was 1497.97 bits over 1000 pairs, indicating strong resistance to differential attacks.

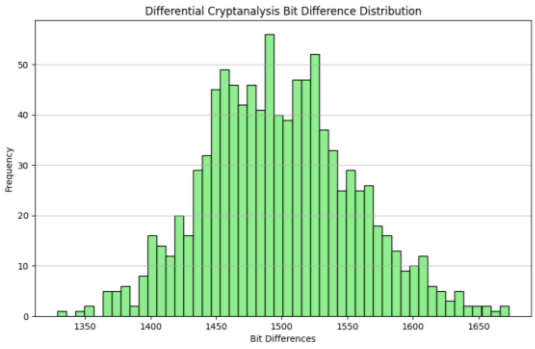

Figure 7. Differential Cryptanalysis

The results of our comprehensive testing reveal that the proposed cryptographic framework exhibits strong resistance against common cryptographic attacks while maintaining efficient performance. The high avalanche effect, notable nonlinearity, and low collision probability affirm the robustness of our approach, making it a suitable candidate for secure communications in various applications.

VII. CONCLUSION

In conclusion, the developed cryptographic system integrates advanced encryption techniques to provide secure communication and reliable data integrity. By leveraging lattice-based cryptography for dynamic key generation and utilizing AES encryption with dynamic S-box construction, this system offers strong resistance against cryptanalysis and brute-force attacks. The integration of SHA-256 hashing adds a crucial layer for message integrity verification, allowing detection of tampering and enhancing trust in secure transmissions.

Comprehensive testing of the system supports its efficacy: Avalanche Testing confirmed high

diffusion with minor changes in input significantly affecting output; Statistical Randomness tests validated key uniformity and unpredictability; Performance Benchmarking results showed the system's efficiency, with encryption and decryption times suitable for real-time use; and Differential Cryptanalysis demonstrated robust resistance to differential attacks, indicating strong security against adversarial data manipulation. Collectively, these results underline the system's reliability and effectiveness in secure data transmission, marking it as a viable solution for applications demanding advanced cryptographic safeguards.

Future enhancements to the cryptographic messaging system could involve integrating this cryptographic framework into real-world messaging applications presenting a promising direction. Such integration would enable dynamic key generation, lattice-based encryption, and adaptive S-box transformations on a larger scale, ensuring that messages remain confidential and secure. Expanding to cloud services for secure backup of encrypted conversations could also be beneficial, providing users with protected data storage accessible only through appropriate keys. This system thus represents a forward-looking, resilient solution for secure data transmission, balancing strong cryptographic safeguards with usability and efficiency for practical applications..

REFERENCES

[1] M. Asif, S. Wajiha, S. Askar, and H. Ahmad. "A Novel Scheme for Construction of S-Box Using Action of Power Associative Loop and Its Applications in Text Encryption", July 2024. https://doi.org/10.1109/ACCESS.2024.3409387

[2] Y. Aydin, A. M. Garipcan, and F. Özkaynak. "A Novel Secure S-Box Design Methodology Based on FPGA and SHA-256 Hash Algorithm for Block Cipher Algorithms", June 2024. https://doi.org/10.1007/s13369-024-09251-8

[3] H. Rashid, M. M. U. Shaban, S. Ahmad, E. Ahmed, and M. T. Amjad. "Dynamic S-Box Design Using a Novel Square Polynomial Transformation and Permutation", June 2021. https://doi.org/10.1109/ACCESS.2021.3086717

[4] A. Wang, D. Xiao, and Y. Yu. "Lattice-Based Cryptosystems in Standardisation Processes: A Survey", Dec 2022. https://doi.org/10.1049/ise2.12101

[5] R. R. Rachh, P. V. AnandaMohan, and B. S. Anami. "High Speed S-box Architecture for Advanced Encryption Standard," Dec 2011. https://doi.org/10.1109/IMSAA.2011.6156342

[6] C. Du and G. Bai. "Towards Efficient Polynomial Multiplication for Lattice-Based Cryptography", Aug 2016. https://doi.org/10.1109/ISCAS.2016.7527456

[7] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet. "Chaos-based Designing of a Highly Nonlinear S-box Using Boolean Functions," Dec 2015. https://doi.org/10.1109/SSD.2015.7348106

[8] A. Joshi, P. K. Dakhole, and A. Thatere. "Implementation of S-Box for Advanced Encryption Standard", Sep 2015. https://doi.org/10.1109/ICETECH.2015.7275043

[9] A. Satoh, S. Morioka, K. Takano and S. Munetoh, "A Compact Rijndael Hardware Architecture With S-box Optimization", Dec 2000. https://doi.org/10.1007/3-540-45682-1_15

[10] G. Alisha Evangeline, S. Krithiga and J. Jesu Mejula, " Least complex S-Box and its fault detection for robust Advanced Encryption Standard algorithm ", March 2013. https://doi.org/10.1109/ICEETS.2013.6533356