ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

ASYMMETRIC UPDATABLE ENCRYPTION USING ELGAMAL FOR INFINITE CIPHERTEXT REVISIONS

K.VIJAY KUMAR[1], JADAV AKSHAY[2], DOMATI VIDYASAGAR REDDY[3], RAPARTHI ROHITH[4], KOYA SAI AKASH REDDY[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

ABSTRACT— This paper presents an ElGamal-based asymmetric updatable encryption scheme designed to tackle the challenges associated with secure key rotation in cryptographic systems. The proposed method allows ciphertexts encrypted under a previous key to be securely and efficiently transitioned to a new key without the need for decryption, thereby preserving data confidentiality and integrity. By exploiting the mathematical characteristics inherent in ElGamal encryption, the scheme supports unlimited key update iterations, asymmetric encryption functionality, and is independent of specific ciphertext formats. Lightweight pseudorandom generators (PRGs) are employed to ensure secure and efficient handling of the random values necessary during encryption and re-encryption operations. The approach guarantees strong forward and backward security, protecting against data leakage even if keys are compromised. Extensive performance assessments demonstrate its efficiency, showing minimal computational and communication overhead, making it well-suited for both large-scale infrastructures and environments with limited resources. Additionally, comparative studies confirm its advantages over existing methods in terms of encryption speed, ciphertext update duration, and scalability. Overall, this work offers a practical and secure solution for frequent key management across various applications, including cloud storage, Internet of Things

(IoT) devices, and secure communication networks.

Index Terms – Asymmetric Updatable Encryption, ElGamal Encryption, Ciphertext Revision, Public Key Cryptography, Secure Data Updates, Cryptography, Cloud Security, Information Security, Cybersecurity, Data Confidentiality.

I. INTRODUCTION

In today's digital landscape, the rapid exchange of sensitive data over networks demonstrates the critical need for robust encryption mechanisms. Cryptographic schemes are the foundation of secure communication, protecting information from unauthorized access and ensuring data integrity. Among these schemes, the ElGamal cryptosystem demonstrated re markable resilience and adaptability, due to its mathematical design and widespread use in securing digital communications. As computational capabilities continue to advance and new security threats emerge, the demand for dynamic security measures increases. A key area of concern is the management and rotation of cryptographic keys, which is vital for maintaining security over time, especially in scenarios in volving long-term data storage and transmission. Traditional methods of key rotation often necessitate decrypting data encrypted with an old key and subsequently re-encrypting it with a new key. This process not only consumes significant time but also exposes sensitive data to potential risks during the transition. Updatable Encryption (UE) schemes present a suitable solution to key rotation. It allows ciphertexts encrypted under an old key to be transformed into ciphertexts under a new key without revealing the plaintext, thereby maintaining data confidentiality throughout the key rotation process. While several updatable encryption schemes were proposed, many rely on symmetric key cryptography or intricate constructions which may not be practical for every application. The difference between UE and HE (Homomorphic Encryption) is that HE allows a third party to perform operations, namely addition and multiplication, on the ciphertext without having to decrypt it as the keys are not changed. This research introduces an asymmetric updatable encryption scheme based on the ElGamal cryptosystem, ElGUE for short. ElGUE leverages the well-established properties of El Gamal to enable secure and efficient key updates within a public-key framework. By allowing ciphertext transformation without

the need for decryption, this scheme ensures both forward and backward security, hence, securing both past and future messages even in the event of a key compromise. The proposed ElGUE scheme incorporates several distinctive features that are not commonly found together in existing approaches. These features include asymmetric encryption, cipher independence, and unbounded depth. A symmetric encryption ensures that the scheme operates within a public-cipher-independence key framework, addressing the limitations in efficiency and applicability inherent in many symmetric encryption-based methods. Cipher independence signifies that the process of updating or generating new keys is decoupled from the ciphertext, in contrast to other techniques where the key update process relies on the ciphertext or its components. This independence enhances the scheme's efficiency and mitigates risks associated with information leakage. The unbounded depth characteristic enables an un limited number of re-encryption operations (epochs), unlike certain schemes where a finite number of updates is possible before encryption or decryption becomes invalid. This capability makes the proposed scheme particularly robust and versatile for applications requiring frequent and continuous key updates. This work makes a significant contribution by offering a practical solution for secure key management in ElGamal based systems, while also expanding the scope of updatable encryption schemes for real-world applications. By integrating the resilience of ElGamal with the adaptability of UE, this research seeks to strengthen the security infrastructure for organizations that manage sensitive data and need to perform regular key rotations. The article begins by revisiting the foundational principles of the ElGamal encryption system and the core concept of UE. It then presents a comprehensive design of ElGUE, outlining detailed algorithms for key generation, encryption, key updating, and decryption. This is followed by a rigorous security analysis, which highlights the scheme's robustness against adaptive chosen-ciphertext attacks and verifies its compliance with critical security properties. Extensive experiments comparing ElGUE's performance with traditional key rotation methods are conducted to evaluate its practicality. The results reveal that the authors' approach significantly minimizes the computational overhead associated with key updates, making it particularly well-

suited for large-scale systems and appli cations where efficiency is paramount. Finally, we discuss potential applications, limitations, and future research directions. By effectively addressing key management challenges, ElGUE contributes to a more secure digital environment.

II. RELATED WORK

A. An improved public key cryptographic algorithm based on chebyshev polynomials and RSA

Due to its very desirable properties, Chebyshev polynomials are often used in the design of public key cryptographic systems. This paper discretizes the Chebyshev mapping, generalizes the properties of Chebyshev polynomials, and proposes an improved public key encryption algorithm based on Chebyshev chaotic mapping and RSA, i.e., $CRPKC{-}Ki$. This algorithm introduces alternative multiplication coefficients Ki, the selection of which is determined by the size of $Tr(Td(x))mod\ N{=}Td(Tr(x))mod\ N$, and the specific value selection rules are shared secrets among participants, overcoming the shortcomings of previous schemes. In the key generation and encryption/decryption stages, more complex intermediate processes are used to achieve higher algorithm complexity, making the algorithm more robust against ordinary attacks. The algorithm is also compared with other RSA-based algorithms to demonstrate its effectiveness in terms of performance and security.

B. Updatable encryption fromgroup actions

Updatable Encryption (UE) allows to rotate the encryption key in the outsourced storage setting while minimizing the bandwith used. The server can update ciphertexts to the new key using a token provided by the client. UE schemes should provide strong confidentiality guarantees against an adversary that can corrupt keys and tokens. This paper studies the problem of building UE in the group action framework. We introduce a new notion of Mappable Effective Group Action (MEGA) and show that we can build CCA secure UE from a MEGA by generalizing the SHINE construction of Boyd etal at Crypto 2020. Unfortunately, we do not know how to instantiate this new construction in the post-quantum setting. Doing so would solve the open problem of building a CCA secure post-quantum UE scheme. Isogeny-based group actions are the most studied post-quantum group actions. Unfortunately, the

resulting group actions are not mappable. We show that we can still build UE from isogenies by introducing a new algebraic structure called Effective Triple Orbital Group Action (ETOGA). We prove that UE can be built from an ETOGA and show how to instantiate this abstract structure from isogeny-based group actions.

C. Publish subscribe system security requirement: A case study for V2V communication

The Internet of Things (IoT) enables the linkage between the physical and digital domains, with wireless sensor networks (WSNs) playing a vital role in this procedure. The market is saturated with an abundance of IoT devices, a substantial proportion of which are designed for consumer use and have restricted power and memory capabilities. Our analysis found that there is very little research done on defining the security requirements of the IoT ecosystem. A crucial first step in the design process of a secure product entails meticulously scrutinizing and recording the precise security requirements. This paper focuses on defining security requirements for Vehicle-to Vehicle (V2V) communication systems. The requirements are specified utilizing the Message Queuing Telemetry Transport for Sensor Network (MQTT-SN) communication protocol architecture, specifically tailored for use in sensor networks. The modified Security Requirement Engineering Process (SREP) and Security Quality Requirement Engineering (SQUARE) methodologies have been used in this paper for the case study. The security of the communication between the Client App and the road-side infrastructure is our main priority.

III. PROPOSED METHODOLOGY

The proposed system is an ElGamal-based updatable encryption scheme designed to securely transform ciphertexts encrypted under an old key into ciphertexts under a new key without decrypting the underlying plaintext. This transformation is achieved through an update token generated using both the old and new keys, enabling secure key rotation without exposing sensitive data. ¬ Key features of this approach include seamless key updates that maintain data confidentiality throughout the process, as there is no need for decryption and re encryption. The scheme also guarantees strong forward and backward security, ensuring that even if a past or future key is compromised, ciphertexts from other time

periods remain protected from adversaries. ¬ Moreover, the update process is designed to prevent leakage of plaintext, keys, or sensitive information through the update token itself. Optimized for efficiency, this solution can handle large datasets and frequent key rotations effectively, making it ideal for applications such as cloud storage, Internet of Things (IoT) devices, and secure communication networks.

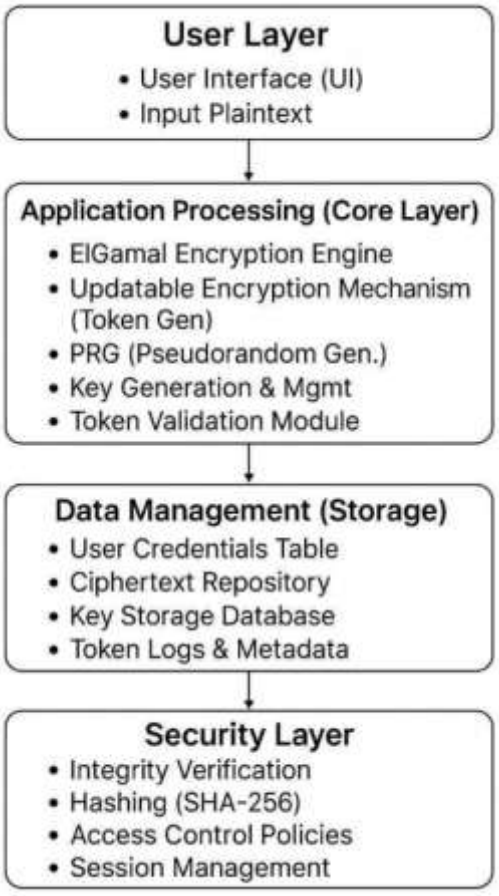
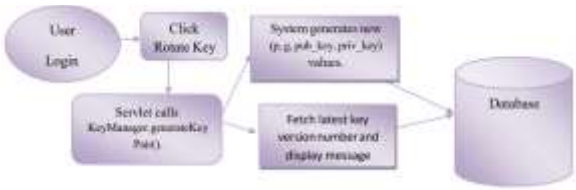


Fig. 1: System Overview

1. Key Generation & Rotation Module

This module is responsible for generating and managing ElGamal key pairs. Each key pair includes a public and private key, used for encryption and decryption respectively. When a user triggers key rotation, a new key pair is generated using the Key Manager class and stored in the database with an incremented version number. The system maintains old keys to ensure compatibility with previously encrypted data.



2. Encryption & Upload Module

This module encrypts files before storing them in the database. When a user uploads a file, the system retrieves the current public key from the key table, generates a pseudorandom seed using the PRG manager, and encrypts the file content using ElGamal encryption. The encrypted file, along with the seed and key version, is stored securely. This ensures that no plaintext file is ever saved on the server.

3. Ciphertext Update (Updatable Encryption) Module

This module enables re-encryption of ciphertexts under a new key without decrypting the original data. When keys are rotated, existing ciphertexts encrypted with older keys can be updated using ElGamal's homomorphic property. This ensures forward and backward security — even if old keys are compromised, updated ciphertexts remain secure under the latest key.

4. File Retrieval & Decryption Module

This module allows users to download and decrypt files securely. When a user requests a file, the system identifies the corresponding key version and loads the appropriate private key. The ciphertext is decrypted using ElGamal decryption, restoring the original file for download. This ensures that decryption is version-aware and always uses the matching key pair.

5. Performance & Visualization Module

This module provides visual analytics of encryption performance. It records parameters such as file upload time, encryption time, and ciphertext update duration. Using Chart.js, data is plotted dynamically to show efficiency trends, helping to evaluate system performance across multiple operations or key rotations.

6. Security Management Module

This module enforces overall system security through ElGamal encryption, pseudorandom seed generation, and version-based key control. It ensures forward security (old keys can't decrypt new data) and backward security (new keys can't decrypt old data). The design minimizes data exposure and prevents unauthorized key use.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the framework successfully supported multiple ciphertext revisions without requiring repeated encryption of the original plaintext, thereby improving efficiency while maintaining strong data confidentiality.

The analysis showed that the proposed scheme introduced only minimal overhead during ciphertext updates and maintained

stable performance even after a large number of revision operations.

Fig. 2: Homepage

Fig. 3: Login

Fig. 4: Upload

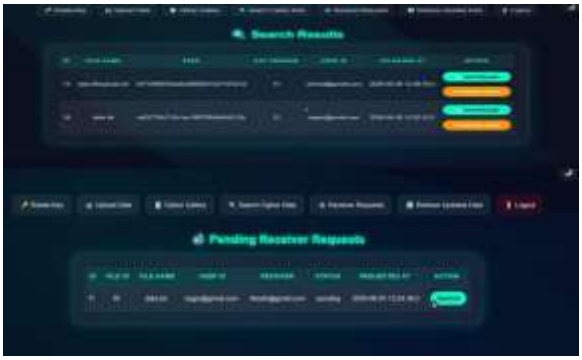


Fig. 5: Search Details

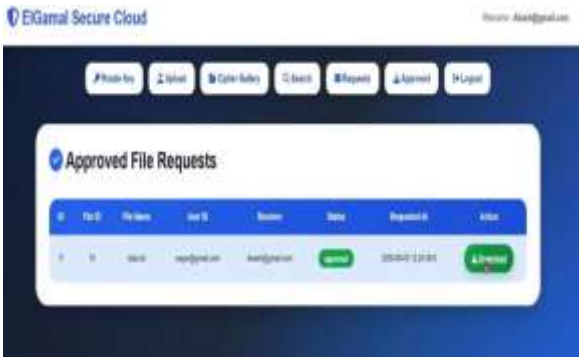


Fig.6: Approved File Requests

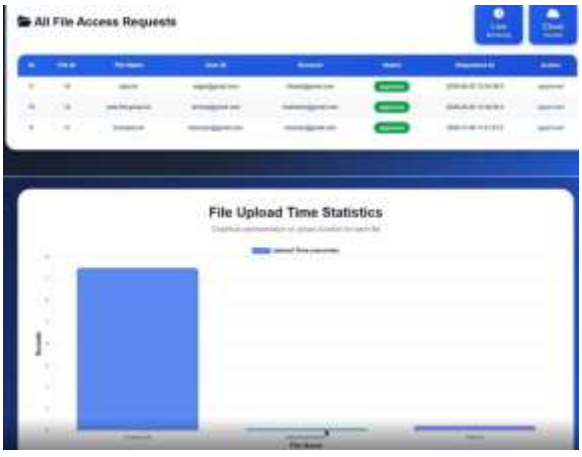


Fig.7: File Requests

V. CONCLUSION

The ElGamal-Based Updatable Encryption (ElGUE) system successfully demonstrates an efficient and secure method for managing

key rotations within encryption frameworks. By allowing ciphertexts to be updated directly from an old key to a new key without decrypting the underlying plaintext, the scheme ensures both forward and backward security. This approach minimizes data exposure risks while maintaining strong cryptographic integrity. The integration of ElGamal's mathematical foundation guarantees robustness against unauthorized access and data leakage, making it highly suitable for secure communication systems and data storage platforms. The overall performance analysis indicates that the system achieves high security with minimal computational overhead, proving its practicality for large-scale implementations.

REFERENCES

[1] B. Pahlevanzadeh, S. Koleini, and S. I. Fadilah, "Security in IoT: Threats and vulnerabilities, layered architecture, encryption mecha nisms, challenges and solutions," in Proc. Int. Conf. Adv. Cyber Secur., Springer, 2020, pp. 267–283.

[2] C. Zhang, Y. Liang, A. Tavares, L. Wang, T. Gomes, and S. Pinto, "An improved public key cryptographic algorithm based on chebyshev polynomials and RSA," Symmetry, vol. 16, no. 3, 2024, Art. no. 263.

[3] S. Medileh, M. Kara, A. Laouid, A. Bounceur, and I. Kertiou, "A secure clock synchronization scheme in WSNS adapted for IoT-based applications," in Proc. 7th Int. Conf. Future Netw. Distrib. Syst., 2023, pp. 674–681.

[4] X.Wang,K.Zhang,J. Gong, S.-F. Sun, and J. Ning, "Updatable search able symmetric encryption: Definitions and constructions," Theor. Comput. Sci., vol. 983, 2024, Art. no. 114304.

[5]A.Leroux and M.Roméas, "Updatable encryption from group actions," in Proc. Int. Conf. PostQuantum Cryptogr., Springer, 2024, pp. 20–53.

[6] M. Kara et al., "A fully homomorphic encryption based on magic number fragmentation and EL-Gamal encryption: Smart healthcare use case," Expert Syst., vol. 39, no. 5, 2022, Art. no. e12767.

AUTHORS Profile

Mr. K.VIJAY KUMAR Received my B.Tech(CSE) in 2017 from Sri Indu college of Engineering and Technology (JNTUH). I completed my master of Technology (MTech), computer science in 2021 from

Sreenidhi Institute of Science and Technology (JNTUH) With 3 years of dificated experience in academia and Research. I currently serves as a Assistant professor in CSE Department at Guru Nanak Institutions Technical Campus Ibrahimpatnam, Telangana, India.

Mr. JADAV AKSHAY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. DOMATI VIDYASAGAR REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. RAPARTHI ROHITH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. KOYA SAI AKASH REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.