Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2581

Digital signature scheme and a modified ElGamal Elliptic curve cryptosystem using polynomials over matrix ring

R. Yuvasri †
A. Manimaran *
Department of Mathematics
School of Advanced Sciences
Vellore Institute of Technology
Vellore 632014
Tamil Nadu
India

Abstract

Digital signatures, a crucial component of electronic communications, are enhanced by encryption, ensuring the integrity, validity, and non-repudiation of digital signatures. This paper explores a digital signature scheme based on a new mathematical problem which is a combination of Factor Problem, Discrete Logarithm Problem, and Conjugacy Search Problem, using polynomial over matrix ring. Additionally, a hybrid cryptosystem by combining Elliptic Curve and ElGamal cryptosystem is proposed. The security of the scheme is also analyzed.

Subject Classification: *11T71, 94A60, 94A62.*

Keywords: *Diffie-hellman, ElGamal cryptosystem, Elliptic curve cryptography, Digital signature, Ring.*

1. Introduction

ElGamal and Elliptic curve cryptography (ECC) are popular cryptosystems for encryption, addressing discrete logarithm problem (DLP) and providing unique signature schemes. These systems enhance encryption schemes, making them more resilient to cryptanalytic attacks and increasing operational effectiveness in limited resources. Sensitive health information (SHI) is a popular model in healthcare for centralized patient records, allowing patients to control

† *ORCID-ID:* **0009-0007-1552-7189**
* *ORCID-ID:* **0000-0001-6717-1152**

† *E-mail:* **beviramesh@gmail.com**
* *E-mail:* **marans2011@gmail.com (Corresponding Author)**

© Taru Publications

their personal health information. But privacy and security issues can hinder its widespread adoption.

An efficient new form of the ECC with faster computations to generate keys is proposed in [1]. [2] proposed a cryptosystem and a digital signature scheme based on ECC and ElGamal. In [3], ECC is implemented and demistified along with ElGamal cryptosystem. [4] successfully developed and examined a novel biometric security approach using ECC integrated along with modified session keys. [5] Cryptanalyzed ECC algebrically using Grobner bases and suggested a strategy to strengthen its security. In [6], a message sharing mechanism with unity properties over a ring that utilizes finite associative-commutative rings is introduced. Using non-commutative structures, ([7]-[9]) introduced digital signature schemes. In ([10]-[18]), the authors used matrices and some hard problems and proposed key exchange protocols and cryptosystems. Some cryptographic schemes are also suggested for healthcare systems ([19]-[21]).

In this study, the DLP, Conjugacy Search Problem (CSP), and Factorization Search Problem (FP) ideas are extended over a non-commutative semi group $M_{n\times n}(Z_n)$ by the addition of secret parameters, which becomes the Factorization Discrete Logarithm Conjugacy Search Problem ($FDLCSP$). The proposed digital signature scheme relies on the difficulty of calculating discrete logarithms in a large prime modulus and combines the exponentiation with the conjugacy search problem and factorization problem. We focus on conjugacy relations and factoring, making the key generation step more efficient. The proposed cryptosystem is a combination of ElGamal and ECC, which depends on the key generation phase of digital signature scheme. Paper organization: In Section 2, the required basic definitions are given along with the system's background. In Section 3, the proposed digital signature scheme is provided. In Section 4, to secure the SHI a cryptosystem based on the Elliptic Curve and the ElGamal cryptosystem. In Section 5, the security is analyzed. Finally, in Section 6, the conclusion is given.

2. Preliminaries

The basic definitions required are given along with the system's background in this section.

Definition 2.1: [15] The Discrete Logarithm Problem (DLP): Let q be a prime and given an element $\gamma \in F_q^*$ where F_q^* is a cyclic group of order $q-1$ generated by ω, find an integer d, $0 \le d \le q-1 \ni \omega^d \equiv \gamma \mod q$.

Definition 2.2: [15] The Factorization search problem is defined as finding two elements $a' \in A'$ and $b' \in B' \ni a'.b' = x$ where x is an element in the group G and A', B' are subgroups of G.

Definition 2.3: [22] The Conjugacy search problem (CSP) is defined as finding an element x in a group G, given an element $z \in G$ such that $y = xzx^{-1}$ where $y \in G$.

Definition 2.4: Let G be a non-abelian semi-group and H be a subsemi-group of G. Let $g \in G$ such that $g = xy_1^i y_2^i x^{-1}$ where $y_1, y_2 \in G$, $x \in H$ and $i \in F_q^*$. Here, finding x and i is the Factorization Discrete Logarithm Conjugacy Search problem (FDLCSP).

Definition 2.5: [22] Let $k \in G$ and the set of elements that commute with k, that is, $C(k) = a \in G : ka = ak$. The centralizer of k in G is denoted as $C(k)$.

Definition 2.6: [23] A hash function is a function $h: G_1 \rightarrow G_2$, where G_1 and G_2 are arbitrary groups. It accepts a variable length block of data M as input and produces a fixed-size hash value $h = H(M)$. Inputs to hash functions are called messages and outputs are called hash value (digests).

2.1 *System structure*

The structure of the healthcare system is shown in Figure 1. It is classified as subsequent.

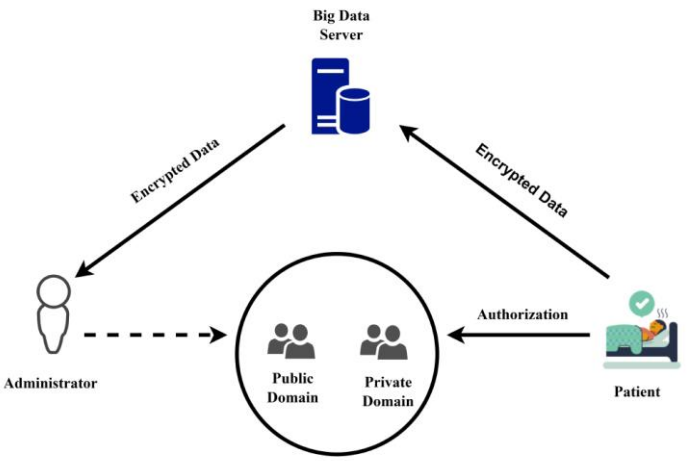


Figure 1
HS6 The structure of the healthcare system

(i) Patient (P_a) i.e., the data owner: Name, date of birth, gender, residence, phone number, illness, and other information about P_a are all recorded in the system. It is also recorded in S. (ii) Personal Domain (P_eD): The people who are dear to P_a are reflected in the domain i.e., friends and family members. According to the necessary requirements, P_a grants them access permissions. (iii) Public Domain (P_uD): Parties like insurance corporations, hospitals elsewhere, etc. are covered in the domain. Until P_a grants authorization, the parties are unable to access the SHI. (iv) Administrator (A_d): Initially, P_a is requested to provide their profile information and register when they arrive at the

hospital. A_d gives P_a an enrollment ID and private key (which is updated upon each use). (v) Server (S): This is where P_a's SHI is stored. Massive data processing, analysis, and storage are made easy using S.

2.2 *Architecture of the proposed protocol*

The roles designated for managing SHI are as follows. The treatment records of P_a may be added, edited, or removed by a doctor. The complete medical data of the P_a is assigned to them and are made available to him or her. Although they have limited rights, nurses may still access and manage P_a health information. Specifically, a nurse has the ability to add details to a P_a's medical care record. However, they are not permitted to view any specific medical records like doctors assigned to a P_a, since they have restricted access to the visit history of that person. The staff member, who is the third role owner, has access to the P_a's fundamental data, such as his identification, visit history as well as fees. The staff records how long patients wait and assigns the P_a to a qualified and reachable doctor. Defining duties, allocating individuals to these positions, and managing role granting and revocation of employees fall within the responsibility of the A_d. The following is a description of the suggested protocol's process. The first time a P_a goes to the hospital, the SHI is created along with list of authorized users with access privileges defined by P_a. It is first encrypted and then A_d uploads it in S. Upon the request of SHI by the P_a or the authorized user, they can decrypt and access it according to the wish of P_a.

2.3 *Potential challenges*

In order to prevent the privacy of P_a and data leakage, the internal and external threats should be effectively neutralized. The technical issues that would occur need to be solved as quickly and efficiently as possible. The cost of hiring the specialists is quite high. The medical and expert workers who have adequate knowledge of this scheme are less which makes it difficult to provide adequate care, particularly in remote locations. To remain ahead of emerging risks, it is essential to perform regular security assessments and upgrades. Also, it is necessary to update the user demands that arise in the future. Effective implementation of this scheme requires sufficient financing.

3. The Proposed Digital Signature Scheme

The proposed digital signature scheme is as follows:

System Initialization phase: The user (P_a/authorized user from P_uD, P_eD) does the following procedure before communicating with A_d: Let p_1 and p_2 be two large primes chosen randomly and $A = M_{n\times n}(Z_n)$ be a matrix ring. Choose α, β from A. Calculate $N = p_1p_2$. Choose a positive integral coefficient polynomial, $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in Z_{>0}[x]$. Calculate $y_1 = p(\alpha) \bmod N$ and $y_2 = p(\beta) \bmod N$. User calculates $P = y_1^i y_2^j$ where i, j are big positive integers. The centralizers of y_1 is $C_A(y_1)$. The public parameters are A, y_1 and P.

Key generation phase: First, the user and A_d exchanges the common secret key.

Phase 1: User computes $C_1 = x_1^{-1}Px_1$ where the secret parameter x_1 is chosen from $B_1 \backslash C_A(y_1)$. User sends C_1 to A_d. Note that, $x_1P \neq Px_1$.

Phase 2: A_d computes $C_2 = x_2^{-1}Px_2$ where the secret parameter x_2 is chosen from $B_2 \backslash C_A(y_1)$. Note that, $x_2P \neq Px_2$. A_d sends C_2 to user.

Phase 3: User conjugates the value of C_2 by x_1 and calculates her secret key $K_1 = x_1^{-1}x_2^{-1}Px_2x_1$. Similarly, A_d conjugates the value of C_1 by x_2 and calculates his secret key $K_2 = x_2^{-1}x_1^{-1}Px_1x_2$. The exchanged secret key is

$$K_1 = x_1^{-1}x_2^{-1}Px_2x_1 = x_2^{-1}x_1^{-1}Px_1x_2 = K_2.$$

Signature generation phase: Suppose the user wants to send the original plaintext message $o_m \in A$ to A_d, he/she creates the signature on o_m as follows: User calculates hash of the original plaintext message $H(o_m)$, $S_1 = x_1^{-1}H(o_m)K_1x_1$, $S_2 = x_1^{-1}S_1Px_1$, $S_3 = x_1^{-1}S_1H(o_m)x_1$, $S_4 = x_1^{-1}H(o_m)x_1$. User's signature on o_m is (S_2, S_3, S_4) and she sends it to A_d for verification.

Verification phase: A_d first computes $S = K_2^{-1}x_2^{-1}S_4$ and $S' = x_2^{-1}S_2^{-1}S_3$. He verifies $S = S'$ and accepts it only if the equality holds.

Verification of Correctness:

$$\begin{aligned} K_2^{-1}x_2^{-1}S_4 &= x_2^{-1}S_2^{-1}S_3 \\ (x_2^{-1}x_1^{-1}Px_1x_2)^{-1}x_2^{-1}x_1^{-1}H(o_m)x_1 &= x_2^{-1}(x_1^{-1}S_1Px_1)^{-1}x_1^{-1}S_1H(o_m)x_1 \\ x_2^{-1}x_1^{-1}P^{-1}x_1x_2x_2^{-1}x_1^{-1}H(o_m)x_1 &= x_2^{-1}x_1^{-1}P^{-1}S_1^{-1}x_1x_1^{-1}S_1H(o_m)x_1 \\ x_2^{-1}x_1^{-1}P^{-1}H(o_m)x_1 &= x_2^{-1}x_1^{-1}P^{-1}H(o_m)x_1 \end{aligned}$$

4. Proposed Cryptosystem

Following the proposed digital signature scheme in Section 3, this section proposes a hybrid cryptosystem that combines two potent cryptographic approaches the Elliptic Curve and the ElGamal Cryptosystem. By using the advantages of both systems, it provides faster calculations due to smaller key sizes than more conventional cryptosystems like RSA. Strong security based on the difficulty of the elliptic curve discrete logarithm problem and by fusing the advantages of ElGamal with ECC, making it appropriate for both digital signatures as well as encryption.

Let $y^2 = x^3 + ax + b \bmod p_3$ be the elliptic curve defined over F_{p_3} where p_3 is a prime number. The order of the elliptic curve is r. Let G be the generator point of the elliptic curve. A_d chooses $d_1 \in [1, p_3 - 1]$ and calculates $E_1 = P^{d_1} \bmod p_3$ and sends E_1 to user.

Key generation: User calculates her secret key, $S_A = K_{1_{1,1}}G \bmod p_3$ where $K_{1_{1,1}}$ is the first entry of K_1. Similarly, A_d calculates his secret key $S_B = K_{2_{1,1}}G \bmod p_3$ where $K_{2_{1,1}}$ is the first entry of K_2. Since $K_1 = K_2$, the value of $S_A = S_B = (S_A(1), S_A(2))$.

Encryption: User chooses $d_2 \in [1, p_3 - 1]$ and encrypts the original plaintext message o_m by calculating $E_2 = P^{d_2} \bmod p_3$, $E_3 = E_1^{d_2} \bmod p_3$ and $E_4 = S_A(1) o_m E_3 \bmod p_3$. User sends the ciphertext (E_2, E_4) to A_d.

Decryption: A_d decrypts the ciphertext by calculating $D_1 = E_2^{d_1} \bmod p_3$ and $o_m = S_A(1)^{-1} E_4 D_1^{-1} \bmod p_3$. Proof of correctness is as follows.

$$\begin{aligned} o_m &= S_A(1)^{-1} E_4 D_1^{-1} \\ &= S_A(1)^{-1} S_A(1) o_m E_3 (E_2^{d_1})^{-1} \\ &= o_m E_3 (E_2^{d_1})^{-1} \\ &= o_m E_1^{d_2} ((P^{d_2})^{d_1})^{-1} \\ &= o_m (P^{d_1})^{d_2} (P^{d_2 d_1})^{-1} \\ &= o_m P^{d_1 d_2} (P^{d_1 d_2})^{-1} \\ &= o_m. \end{aligned}$$

5. Security Analysis

In this section, we evaluate the proposed method through a variety of attacks to ensure its security.

Data Forgery: Assume that the adversary substitutes the original message o_m with a forged message o'_m. A_d is given the signature (S'_2, S'_3, S'_4). Using the fabricated information, determine the value of $H(o'_m)$ and subsequently verify the equation. Due to the full incorporation of $H(o'_m)$ in the signature generation process but not in the verification process, $S = S'$ is not feasible. Therefore, the equation $K_2^{-1} x_2^{-1} S_4 = x_2^{-1} S_2^{-1} S_3$ is valid only for the original message. It is not feasible to engage in data forgery without retrieving the signature. Another approach is to seek the value of o'_m that satisfies the condition for a valid $H(o_m)$. However, this is not feasible, as we made the assumption that the hash function H is cryptographically secure. Therefore, it is not possible to sign the incorrect data with a valid signature.

Signature Repudiation: Suppose user desires to reject the acknowledgment of her signature on certain valid message. It follows that the adversary has forged the signature. But during the verification process, A_d checks $S = S'$ and detects the forgery.

Existential forgery: Suppose the adversary signs a forged message o'_m and generates the signature (S'_2, S'_3, S'_4). Without the knowledge of the private key and secret parameters it is impossible to find a valid signature for o'_m.

Total Break: A signature system is safe if the task of finding the secret key from the public parameters is resolved. The verification data is not available to the public. Today, everyone makes use of this property. The unsolvable nature of some group theory or number theory-related computing issues dictates it. In this algorithm, we made use of an intractable problem like the CSP. The enemy is unable to discover the secret key as a result.

The security of the proposed cryptosystem is dependent on various aspects, including the value of N, the choice of polynomial, the order of the matrix, and the matrix discrete logarithm problem. Matrix cryptography provides equivalent

security for smaller bit sizes, but the level of complexity escalates when using larger order matrices and selecting polynomials. As the dimensions of the base matrix increase and the modulo N becomes larger, the task of determining inverses becomes increasingly challenging.

6. Conclusion

In this paper, we first introduce a digital signature scheme and perform a verification of its correctness. The main idea is that the probability of accurately tracing the private key is extremely low due to the system's reliance on the difficulty of solving the underlying problem. Then, we propose a cryptosystem that is a combination of the elliptic curve and the ElGamal cryptosystem and is based on polynomials over non-commutative rings. Matrix cryptography's computational benefits lie in utilizing the shortest key length, resulting in reduced calculations for secure systems. Since the complexity of matrix operations increases with matrix size enlargement, we can assert that our proposed approach provides us with reliable indicators of safety.

References

[1] R. Aljamaly, Karrar Taher and K. Ruma Kareem Ajeena, "The kr-elliptic curve public key cryptosystem", *Journal of Physics: Conference Series,* IOP Publishing, vol. 3, no. 1879 (2021).

[2] K. Rabah, "Elliptic curve elgamal encryption and signature schemes", *Information Technology Journal*, vol. 4, no. 3, pp. 299-306 (2005).

[3] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks", *Journal of Interdisciplinary Mathematics,* vol. 23, no. 2, pp. 463-470 (2020).

[4] V. D.Gowda, P. Gite, M. Rahman, and K. R. Kadam, "Novel approaches to biometric security using enhanced session keys and elliptic curve cryptography", *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 477-488 (2024).

[5] Madan Mohan Tito Ayyalasomayajula, M. A. Hayder Ghanimi, M. Manimaran, Vijaya Krishna Sonthi, Abrar Ahmed Katiyan, Sudhakar Sengan and Pankaj Dadheech, "Enhanced network security through algebraic cryptanalysis of elliptic curve cryptography", *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 7, pp. 2219-2230 (2024).

[6] S. L. Kryvyi, V. N. Opanasenko, E. A. Grinenko, Y. A. Nortman, "Symmetric Information Exchange System Based on Ring Isomorphism", *Cybernetics and Systems Analysis*, pp. 1-12 (2022).

[7] S. C. Gupta, M. Sanghi, "On an efficient RSA public key encryption scheme", *Malaya J Matematik*, vol. 8, no. 3, pp. 1138-1141 (2020).

[8] V. Jalaja, G. S. G. N. Anjaneyulu, and L. Narendra Mohan, "New digital signature scheme on non-commutative rings using double conjugacy", *Journal of Integrated Science and Technology*, vol. 11, no. 2, pp. 471-471 (2023).

[9] V.Jalaja, P. Vijaykumar, R. Elumalai, and G. S. G. N. Anjaneyulu, "Differential polynomials on Non-Commutative Rings in Digital Signature scheme" *Journal of Integrated Science and Technology,* vol. 11, no. 3, pp. 526-526 (2023).

[10] M. Eftekhari, "A diffie-hellman key exchange protocol using matrices over noncommutative rings", *Groups Complexity Cryptology,* (2012).

[11] J. Pan, C. Qian and M. Ringerud, "Signed (Group) Diffie-Hellman Key Exchange with Tight Security", *Journal of Cryptology*, vol. 35, no. 4, pp. 26 (2022).

[12] V. Roman'kov, "An improvement of the Diffie-Hellman noncommutative protocol", *Designs, Codes and Cryptography*, vol. 90, no. 1, pp. 139-153 (2022).

[13] L. A. Lizama-Perez, "Non-invertible key exchange protocol", *SN Applied Sciences,* vol. 2, no. 6, pp. 1083 (2020).

[14] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using matrices over group rings", *Groups-Complexity-Cryptology,* vol. 5, no. 1, pp. 97-115 (2013).

[15] I. Gupta, A. Pandey, and M. K. Dubey, "A key exchange protocol using matrices over group ring", *Asian-European Journal of Mathematics,* vol. 12, no. 05, pp. 1950075 (2019).

[16] A. Pandey, I. Gupta, D. K. Singh, "On the security of DLCSP over GL_n (F_q [S_r])", *Applicable Algebra in Engineering, Communication and Computing*, pp. 1-10 (2021).

[17] R. Yuvasri, A. Manimaran, "A Secure Key Exchange Protocol and a Public Key Cryptosystem for Healthcare Systems", *Contemporary Mathematics*, pp. 2491-2507 (2024).

[18] R. Yuvasri, A. Manimaran, "A key exchange protocol and a cryptosystem based on the generalized decomposition problem", *International Journal of Computer Mathematics: Computer Systems Theory,* pp. 139-154 (2024).

[19] R. Boussada, M. E. Elhdhili,L. A. Saidane, , "Toward privacy preserving in IoT e-health systems: A key escrow identity-based encryption scheme", In *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-7 (2018).

[20] M. K. Misra, A. Chaturvedi, S. P. Tripathi, and V. Shukla, " A unique key sharing protocol among three users using non-commutative group for electronic health record system", *Journal of discrete mathematical sciences and cryptography,* vol. 22, no. 8, pp. 1435-1451 (2019).

[21] K. Sharma, A. Agrawal, D. Pandey, R. A. Khan, and S. K. Dinkar, " RSA based encryption approach for preserving confidentiality of big data", *Journal of King Saud University-Computer and Information Sciences*, (2019).

[22] D. Ezhilmaran and V. Muthukumaran, "Key exchange protocol using decomposition problem in near-ring", *Gazi University Journal of Science,* vol. 29, no. 1, pp. 123-127 (2016).

[23] J. H. Silverman, J. Pipher, and J. Hoffstein, "An introduction to mathematical cryptography", Springer New York, vol. 1 (2008).

Received March, 2025