Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 3, pp. 973–979
DOI : 10.47974/JDMSC-2239

Design of public key cryptosystem based on the underlying mathematical complexity

Jincy Pauly *
M. I. Saju †
Renjith Varghese §
E. F. Antony John ‡
Department of Mathematics
St. Thomas College (Autonomous)
Affiliated to University of Calicut
Thrissur 680001
Kerala
India

Abstract

This study aims to present a new cryptographic system based on the principles of the Discrete Logarithm Problem (DLP) applied to automorphisms and the non-commutative nature of rectangular matrices. The suggested system undergoes significant adjustments in encryption, decryption, and key generation algorithms to ensure its strength and effectiveness. Empirical results indicate the system's ability to function within a non-abelian group, thus strengthening it to resist various attacks. Additionally, the integration of a private matrix key adds an extra layer of complexity. Overall, the proposed cryptosystem demonstrates commendable functionality and provides reasonable security.

Subject Classification: *08A35, 94A60, 15A09.*

Keywords: *Automorphism, DLP, Public key cryptography, Rectangular matrix.*

* *ORCID-ID:* **0000-0003-1647-1029**

* *E-mail:* **jincy.pauly@gmail.com (Corresponding Author)**
† *E-mail:* **sajumambilly@gmail.com**
§ *E-mail:* **renjithvarghese8@gmail.com**
‡ *E-mail:* **antonyjohnef@gmail.com**

1. Introduction

In the modern world, data security is absolutely essential. Every syllable spoken is being monitored by someone. Therefore, covert contact is very challenging. This is where encryption plays a key role. There are many cryptosystems currently accessible. One of the better modes of communication that provides more protection for data is the "public key cryptosystem" (PKC). PKC primarily relies on the challenging mathematical problems like the DLP, Integer Factorization Problem (IFP), Knapsack problem and Elliptic Curve Discrete Logarithm Problem (ECDLP). The first public key systems were RSA [1] and ElGamal [2]. RSA is based on the IFP, while ElGamal and its under lying key agreement protocol by Diffie Hellman [3] are based on the DLP. Many updated versions of RSA and ElGamal are accessible [4–7].

There is a great deal of variants in the ElGamal system. The ElGamal system works on abelian groups of integers as an asymmetric cryptosystem. Saju et al. [8] used the DLP's difficulty on a finite extension field to create a PKC that is more secure than ElGamal. Mahalobious [9] looked into the effects of DLP on automorphism on the security of ElGamal.

On the ElGmal key agreement procedure, Irawadi et al. [10] used the square matrix for better resistance. Assault using over defined systems of multivariate polynomial equations, the benefits of using a rectangular matrix for the Hill cipher was examined by Maxrizal [11]. The non-commutativity of the rectangular matrix gives the Hill cipher an asymmetric visage. Also the traditional Hill cipher is expanded by Sundarayya et al.[12] using rectangular matrices, its pseudo inverse and modular operations over prime fields, which guarantees the security. This encourages authors to develop systems featuring non-commutative structures.

Smaller key sizes, faster operations, and stronger security per bit make ECDLP stand out. It's also tiny enough for IoT devices. In ECDLP, there are numerous works. Tahat et al.[13] created a self-certified multi-proxy signature system that guarantees efficiency, security, data integrity, and authentication. It is based on the ECDLP.

The current study aims to develop new public key cryptography based on both DLP on automorphism and non-commutativity of the rectangular matrix. To ensure proper operation of the suggested system, modifications are made to the encryption, description, and key pair generation algorithm. Moreover, the attempt to brute force attack will be difficult since the usage of private matrix key.

2. Perliminaries

2.1 *Frobenius Automorphism* [14]

Let p the prime number and n is a positive integer then $\mathbb{F}_q$ will be a finite field with $q = p^n$ elements. The Frobenius automorphism, represented by σ , is characterized as the function from$\mathbb{F}_q$ to itself, where each element of $\mathbb{F}_q$ is raised to the power of p. Mathematically, for any α in $\mathbb{F}_q$, the Frobenius σ can be expressed as: $\sigma(\alpha) = \alpha^p$.

2.2 *Cyclic Group Generated by Frobenius Automorphism*

Cyclic group for a frobenius automorphism over the finite field $\mathbb{F}_q$, is $< \sigma > = \{\sigma^i : \sigma^i(\alpha) = \alpha^{p^i}, \mathrm{Gcd}(i,n) = 1\}$. In which all elements are again automorphisms. So there exist $\varphi(n)$ such automorphisms.

2.3 *Matrix multiplication* [15]

For two matrices $A_{m\times n} = [x^{a_{ij}}]$, $B_{n\times k} = \left[x^{b_{jl}}\right]$ be in $\mathbb{F}_q{}^*$, the product of matrices defined as $A * B = C_{m\times k} = [\prod_{t=1}^{k}(x^{a_{it}})^{b_{tl}}]$. Satisfies all matrix multiplication axioms.

3. Creation of public and private keys

It is expected of Legastin, the user, to produce a public and private key by carrying out the below actions:

- Choose a prime p
- To create the extension field $\mathbb{F}_q$, where $q = p^n$, choose a primitive polynomial $f(x)$ with a sufficiently high degree n over $\mathbb{F}_p$.
- Choose $K_{1\times m}$, with values that come from $\mathbb{F}_q{}^*$.
- Pick an element $a \in \mathbb{F}_q{}^*$
- Choose an automorphism $\phi_L \in < \sigma >$ randomly and compute $\phi_L(a)$.

With T being the right inverse of K over$\mathbb{F}_q{}^*$, Legastin's secret key is(T, ϕ_L), and his public key is $(p, f(x), K, a, \phi_L(a))$. The alternatives for T are $(p^n - 1)^m$.

4. Encryption

Let's say Merin, a different person, wishes to contact Legastin using Legastin's public key. Merin must then take the following actions:

- Represent the message as elements of $\mathbb{F}_q{}^*$, then make each m block message to matrix $M_{m\times 1}$.
- Choose a random automorphism $\phi_M \in < \sigma >$ and compute $c_1 = \phi_M(\phi_L(a))$.
- Represent $C_1 = binary\ (c_1)$
- Compute $\phi_M^{-1}(a)$.
- Compute $c_2 = \phi_M^{-1}(a)MK$.
- Represent $C_2 = binary\ (c_2)$

Merin then sends a secret note $C = (C_1, C_2)$ to Legastin.

5. Decryption

The procedures below should be taken by Legastin in order to decode the message $C = (C_1, C_2)$:

1. Find c_1, c_2 , then compute $\phi_M(a) = \phi_L^{-1}(c_1)$.
2. Compute $MK = (\phi_M^{-1}(a))^{-1}c_1$.
3. Find $M = MKT$.

6. Proof of validity

From the relation $c_1 = \phi_M(\phi_L(a))$ it is clear that $\phi_L^{-1}(c_1) = \phi_L^{-1}(\phi_M(\phi_L(a))) = \phi_M(a)$. In the relation $C_2 = \phi_M^{-1}(a)MK$ apply $(\phi_M^{-1}(a))^{-1}$ on left side, leads to $(\phi_M^{-1}(a))^{-1}c_1 = MK$. Apply T on right side reveals $MKT = M$.

7. Illustration

Legastin publish public key as

$(2,\ x^8 + x^6 + x^5 + x + 1,\ [1 + x^4 + x^6 \quad x + x^4 + x^6 + x^7$
$1 + x^3 + x^7 1 + x + x^2 + x^3 + x^5], 1 + x^2 + x^7, x^2 + x^4 + x^5 + x^6)$

Kept

$([x + x^2 + x^3;\ x + x^2 + x^7;\ x^2 + x^3 + x^5;$
$1 + x + x^2 + x^3 + x^4 + x^6 + x^7]\ , \sigma^3)$ as secret.

Let "HOPE" is the message Merin wants to send. Since Legastin's public key K has order 1×4 and message has length 4, so here we have only one block exist.

Merin convert the message into

$M = [1 + x + x^5 + x^6\ ;\ x^3 + x^6 + x^7\ ;\ 1 + x + x^4 + x^5 + x^6 + x^7\ ;\ x^5]$

and selects $\phi_M = \sigma^2$, then calculate $C_1 = binary(1 + x^2 + x^4 + x^5 + x^6) = (01110101)$.

And

$c_2 = [1 + x + x^2 + x^3 + x^7 \quad 1 + x + x^4 + x^5 \quad 1 + x^3 + x^5 + x^6 \quad x + x^2 + x^3 + x^5\ ;\ 1 + x + x^2 + x^3 + x^4 + x^5 \quad 1 + x^3 + x^4 + x^5 + x^6 + x^7 \quad x + x^3 + x^4\ ;\ 1 + x^2 + x^3 + x^4 + x^6 \quad x^2 + x^4 + x^7 \quad 1 + x + x^3 + x^4 + x^5 + x^6 + x^7 \quad x^3 + x^5\ ;\ 1 + x + x^3 + x^6 + x^7 \quad 1 + x + x^2 + x^3 + x^4 + x^5 \quad x + x^2 + x^3 + x^7 \quad x + x^4 + x^5]$

$C_2 = 10001111001100110110100100101110001111111$
$11100100011010010111011001010011111011001010$
$00110010110011111110001110001100 10$

Then send $C = (C_1, C_2)$ to Legastin.

To decode the message $C = (C_1, C_2)$ Legastin compute $\phi_M(a) = x^2 + x^7$

Then $(\phi_M^{-1}(a))^{-1} = x + x^5 + x^6 + x^7$

$M = (\phi_M^{-1}(a))^{-1}c_1^T = [1 + x + x^5 + x^6\ ;\ x^3 + x^6 + x^7\ ;$
$1 + x + x^4 + x^5 + x^6 + x^7\ ;\ x^5]$

And read it as "HOPE"

8. Security

The security of the proposed system relies on the Discrete Logarithm Problem (DLP) and the computational complexity involved in determining the correct inverse of a row matrix.

When employing an integer-based cryptosystem (such Elgamal, RSA, or ECC), the algorithm's resilience against 2357 brute force assaults is maximized. Additionally, for a 4x4 matrix, the system described in paper [10] strength is found in $\prod_{k=0}^{3}(2357^4 - 2357^k)$. Nevertheless, the brute force attack in this approach can reach as high as $(p^n - 1)^m(p^n - p^{n-1}) = (2357^8 - 1)^4(2357^8 - 2357^7)$ when using a 1×4 matrix and primitive polynomial of degree 8. This suggests that systems get more robust as the prime and degree of primitive polynomial increase, and that it will take a long time for hackers to figure out the right inverse of K.

Even if one or more simple texts are found or inferred, the private key matrix T remains elusive. Consequently, employing the proposed method will make it harder to overcome the chosen plain text attack.

Moreover, a single letter alteration results in a 32-bit variation in the cipher text, demonstrates strong diffusion property of system. And also the system's security against side channel assaults is strengthened by these ϕ_L and ϕ_M since decisions are made arbitrarily.

9. Conclusion

In summary, this study introduces an innovative approach to public key cryptography, utilizing DLP in conjunction with automorphisms and the unique characteristics of rectangular matrices. The proposed system has undergone extensive refinement across its encryption, decryption, and key generation mechanisms to ensure its resilience and effectiveness. Empirical data affirm its capacity to operate efficiently within a non-abelian group, thereby strengthening its defense against attacking algorithms. Again the incorporation of a private matrix key adds an additional layer of complexity, enhancing the system's ability to withstand brute force attacks. Overall, this cryptographic system demonstrates impressive functionality and offers reasonable security. These advancements mark significant progress in cryptographic methodologies

Acknowledgment

The corresponding author extends her gratitude to the Department of Collegiate Education, Government of Kerala, and for supporting this work under the ASPIRE Scholarship scheme. And acknowledges Department of Science & Technology, Government of India for financial support under ‘WISE Fellowship for Ph.D.’ programme to carry out this work".

References

[1] R. Rivest, “RSA (cryptosystem),” *Arithmetic Algorithms and Applications* (1977).

[2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469–472 (1985).

[3] W. Diffie, "Diffie-Hellman Key Exchange," (1976).

[4] P. K. Panda and S. Chattopadhyay, "A hybrid security algorithm for RSA cryptosystem," in 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1–6, IEEE (2017).

[5] B. P. U. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on 'n' prime numbers," *International Journal of Engineering And Computer Science*, vol. 1, pp. 63–66 (2012).

[6] T. Takagi, "Fast RSA-type cryptosystem modulo pkq," in Advances in Cryptology—CRYPTO'98: 18th Annual International Cryptology Conference Santa Barbara, California, USA August 23–27, 1998 Proceedings, pp. 318–326, Springer (1998).

[7] S. Aikins-Bekoe and J. B. Hayfron-Acquah, "Elliptic curve diffie-hellman (ECDH) analogy for secured wireless sensor networks," *International Journal of Computer Applications*, vol. 176, pp. 1–8 (2020).

[8] S. M. I., R. Varghese, and E. F. A. John, "A design of public key Cryptosystem in an algebraic extension field over a finite field using the difficulty of solving DLP," *Malaya Journal of Matematik* (MJM), vol. 8, pp. 459–463 (2020), doi: 10.26637/MJM0802/0022.

[9] A. Mahalanobis, "Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups," Florida Atlantic University (2005).

[10] S. Irawadi, "Discrete Logarithmic Improvement for ElGamal Cryptosystem Using Matrix Concepts," in 2020 8th International Conference on Cyber and IT Service Management (CITSM), pp. 1–5, IEEE (2020).

[11] M. Maxrizal and B. D. A. Prayanti, "A New Method of Hill Cipher: The Rectangular Matrix As The Private Key," in 2nd International Conference on Science and Technology for Sustainability Proceeding, p. 81 (2016).

[12] P. Sundarayya and G. Vara Prasad, "A public key cryptosystem using Affine Hill Cipher under modulation of prime number," *Journal of Information and Optimization Sciences*, vol. 40, no. 4, pp. 919–930 (2019), doi: 10.1080/02522667.2018.1470751.

[13] N. Tahat, A. K. Alomari, O. M. Al-Hazaimeh, and M. F. Al-Jamal, "An efficient self-certified multi-proxy signature scheme based on ellip-

tic curve discrete logarithm problem," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 4, pp. 935–948 (2020), doi: 10.1080/09720529.2020.1734293.

[14] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, Cambridge (1996).

[15] S. M. I., J. Pauly, R. Varghese, and A. John E. F., "Primitive-Polynomial-Based Secure Cryptosystem Under the Difficulty of DLP," *Bulletin of the Calcutta Mathematical Society*, vol. 116, no. 3, pp. 333-340 (2024).

Received July, 2024