IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

A Right Duo Seminearring based Key Exchange Technique

Senthil S[1], Perumal R[2], and Babu M[3]
Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India[1,3]
Department of Mathematics, College of Engineering and Technology,
SRM Institute of Science and Technology, Kattankulathur, Tamilnadu, India[2]
senthilsports@yahoo.co.in, perumalr@srmist.edu.in, mbabu5689@gmail.com

Abstract: *In this paper, we present a novel symmetric key exchange protocol based on Right duo seminearring. The proposed protocol leverages the unique algebraic properties of Right duo seminearrings to ensure secure key exchange. We provide detailed examples to illustrate the protocol's functionality and practical applicability. The algorithm's structure is elaborated, and its time complexity is analyzed to demonstrate computational efficiency. Furthermore, a comprehensive security analysis is conducted, highlighting the protocol's resilience against common cryptographic attacks. The proposed cryptosystem offers a secure and efficient approach to symmetric key exchange, contributing to the advancement of algebra-based cryptographic protocols.*

Keywords: Key exchange, Semirings, Cryptography 2000 Mathematics subject classification: 16Y60, 94A60, 14G50, 11K70, 11T71

I. INTRODUCTION

Cryptography is the art and science of protecting communication and data. Cryptography plays an important role in securing our digital data [1]. Important data like personal informations, financial transactions, medical informations could be easily intercepted and seen by unauthorized individuals. The need for cryptography rises from the necessity to keep our sensitive information confidential, ensure data integrity, authenticate the persons involved in communication, and ensure the secure communication over an insecure network [2]. Strong cryptographic methods are becoming important as technology continues to change our society. The use of right duo seminearring in cryptography is one such novel strategy. By using characteristics of right duo seminearrings, it gives a novel impact on resolving cryptographic problems. Understanding the implications of integrating this mathematical framework into cryptography is crucial for advancing the field and ensuring the security of our digital communications and transactions [3]. Symmetric encryption and asymmetric encryption are two fundamental cryptographic techniques used to secure data and communications. They differ in their approach to encryption, key management, and use cases [4]. Symmetric encryption, alternatively referred to as secret-key or private-key encryption, relies on a single shared secret key for both the encryption and decryption processes. One of the central hurdles in symmetric encryption lies in the secure distribution of this secret key [5]. When two parties seek to communicate securely, it becomes imperative for them to exchange the secret key in a manner that ensures confidentiality and integrity [6]. Symmetric encryption is notably recognized for its speed and efficiency, making it well-suited for encrypting substantial amounts of data, such as files and data streams.. Symmetric encryption is commonly used for data encryption at rest (e.g., encrypting files or databases), in transport layer security (e.g., SSL (Secure Sockets Layer)/TLS (Transport Layer Security) for securing web traffic), and for securing communications within closed systems where the key exchange problem is manageable [7]. The introduction of public-key cryptography by Whitfield Diffie and Martin Hellman in 1976 revolutionized the field, as did the RSA (Rivest-Shamir-Adleman) cryptosystem, presented in their 1978 paper. The RSA cryptosystem is a widely used and robust method of public-key encryption [8]. RSA encryption relies on the mathematical complexity of factoring large integers, which is believed to be a computationally infeasible task for sufficiently large numbers. In the RSA encryption algorithm, a key pair is generated, comprising a public key used for encryption and a private key used for decryption.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

The public key is freely shareable, enabling anyone to encrypt messages intended for the owner of the corresponding private key [9]. However, only the individual possessing the private key has the capability to decrypt these messages. The security of RSA hinges on the computational complexity of factoring the product of two large prime numbers, providing a robust and widely trusted encryption method. This characteristic makes RSA a key player in securing sensitive information and facilitating secure online communications. The symmetric key cryptosystem is faster and more efficient than the asymmetric cryptosystem, but when exchanging keys over the unsecured networks, it lacks security [10]. Symmetric encryption is much faster and computationally efficient than asymmetric encryption [11]. This makes it ideal for encrypting and decrypting large volumes of data, such as files or data streams, without significant performance overhead. Symmetric encryption algorithms are generally easier to implement and understand, which makes them a preferred choice in situations where simplicity and performance are critical. Symmetric encryption requires less computational power, making it suitable for resource-constrained devices and systems, such as embedded devices, IoT devices [12], and mobile devices. Symmetric encryption is commonly used to protect data at rest, such as files, databases, and storage devices. It prevents unauthorized access to the data even if physical storage media are compromised. Many researchers had studied public key cryptosystem over a variety of algebraic structure. This creates interest to study the symmetric key cryptosystem over seminearring structure R. In this paper, the symmetric-key cryptosystem based on non commutative matrices over right duo seminearring R is introduced. We focus on the application of right duo seminearring in cryptography.

II. THE PROPOSED RIGHT DUO SEMINEARRING

1. Let S = {1, 2, 3} and Z be a set of all integers.
2. The operations on the set S are defined as follows,

$\oplus$	1	2	3
1	1	1	1
2	2	2	2
3	3	3	3

$\odot$	1	2	3
1	1	1	1
2	1	2	2
3	1	2	2

3. The binary operation on the set Z is the classical addition and classical multiplication of integers.
4. Consider the set R = S × Z which is a cartesian product of the set S and Z.
5. The structure R is a right duo seminearring under the following binary operations,

(a) (s1, z1) + (s2, z2) = (s1 $\oplus$ s2, z1 + z2)

(b) (s1, z1) • (s2, z2) = (s1 $\odot$ s2, z1 • z2)" ,

where s1, s2 $\in$ S, z1, z2 $\in$ Z, (s1, z1), (s2, z2) $\in$ R,

6. The set of n × n matrices over the set R is denoted by Mn(R).

III. STICKEL'S KEY EXCHANGE SCHEME

The following key exchange approach is proposed by Stickel in 2005 [13].

Let G be a non-commutative group. Let x, y $\in$ G be two public elements such that xy$\neq$ yx. Let Alice and Bob be the two people who want to communicate in a public network. Now,

1. Alice selects two random natural numbers i and j and computes P = xi · yj and sends it to Bob.
2. Bob selects two random natural numbers k and l and computes Q = xk · yl and sends it to Alice.
3. Alice computes $\text{Key(A)}=x^i \cdot Q \cdot y^j = x^i \cdot (x^k \cdot y^l) \cdot y^j = x^{i+k} \cdot y^{j+l}$
4. Bob computes $\text{Key(B)}=x^k \cdot P \cdot y^l = x^k \cdot (x^i \cdot y^j) \cdot y^l = x^{k+i} \cdot y^{l+j}$

Thus, Alice and Bob gets the same key which can be used as a shared secret key.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

IV. PROPOSED KEY EXCHANGE PROTOCOL

We propose the following key exchange protocol using our right duo seminearring.

Let A, B ∈ Mn(R) be two public matrices such that AB≠ BA. Let Alice and Bob are the two people who want to communicate in a public network. Now,

1. Alice selects two random natural numbers x and y and computes $U = A^x \cdot B^y$ and sends it to Bob
2. Bob selects two random natural numbers m and n and computes $V = A^m \cdot B^n$ and sends it to Alice
3. Alice computes $\text{Key(A)}=A^x \cdot V \cdot B^y = A^x \cdot (A^m \cdot B^n) \cdot B^y = A^{x+m} \cdot B^{n+y}$
4. Bob computes $\text{Key(B)}=B^m \cdot U \cdot B^n = A^m \cdot (A^x \cdot B^y) \cdot B^n = A^{m+x} \cdot B^{y+n}$

Thus, Alice and Bob gets the same key which can be used as a shared secret key.

4.1 Parameters

To achieve an efficient security, we propose the following parameters.

1. The size of the matrix n must be 10.
2. The integers taken from Z must be chosen randomly from [−1000, 1000].
3. The private parameters must be chosen in a range of [103, 105].

4.2 Example of the protocol

We illustrate our key exchange scheme with the following example.

$$\text{For instance, } A = \begin{pmatrix} (2, 44) & (3, -16) \\ (1, -25) & (1, -3) \end{pmatrix} \quad \begin{pmatrix} (1, 32) & (3, 16) \\ (1, 18) & (3, 18) \end{pmatrix}$$

1. Alice selects two natural numbers 5 and 3 and computes A5 and B3.

$$A^5 = \begin{pmatrix} (1, 314707024) & (1, -92666576) \\ (1, -144791525) & (1, 42498957) \end{pmatrix}$$

$$B^3 = \begin{pmatrix} (1, 14054828451200) & (1, 8782897297792) \\ (1, -6471786873688) & (1, -4044308161688) \end{pmatrix}$$

2. Now Alice computes U = A5 · B3 and sends it to Bob.

$$U = \begin{pmatrix} (1, 314707024) & (1, -92666576) \\ (1, -144791525) & (1, 42498957) \end{pmatrix} \begin{pmatrix} (1, 56384) & (2, 35392) \\ (1, 39816) & (2, 25416) \end{pmatrix}$$

$$U = \begin{pmatrix} (1, 14054828451200) & (1, 8782897297792) \\ (1, -6471786873688) & (1, -4044308161688) \end{pmatrix}$$

3. Bob selects two natural numbers 8 and 6 and computes A8 and B6.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

$$A^8 = \begin{matrix} (1,\ 42634820265616) & (1,\ -12549176263440) \\ (1,\ -19608087911625) & (1,\ 5771614991761) \end{matrix}$$

$$B^6 = \begin{matrix} (1,\ 4588323328) & (2,\ 2895065600) \\ (1,\ 3256948800) & (2,\ 2055140928) \end{matrix}$$

4. Now Bob computes V = A8 · B6 and sends it to Alice.

$$V = \begin{matrix} (1,\ 42634820265616) & (1,\ -12549176263440) \\ (1,\ -19608087911625) & (1,\ 5771614991761) \end{matrix} \cdot \begin{matrix} (1,\ 4588323328) & (2,\ 2895065600) \\ (1,\ 3256948800) & (2,\ 2055140928) \end{matrix}$$

$$V = \begin{matrix} (1,\ 154750315837613657218048) & (1,\ 976402757614860903372 80) \\ (1,\ -711703926609057910512 00) & (1,\ -449052186044949637057 92) \end{matrix}$$

5. Alice computes Key(A)=A5 · V · B3

$$Key(A) = \begin{matrix} (1,\ 450696898734567582543913904500699 1360) & (1,\ 284378684336837029526911489183254 9376) \\ (1,\ -207279680363499646029265538413172 0704) & (1,\ -130788392281012031541888839122885 9904) \end{matrix} \quad (1,$$

6. Bob computes Key(B)=A8 · U · B6

7. Thus, Key(A) = Key(B)

$$Key(B) = \begin{matrix} (1,\ 450696898734567582543913904500699 1360) & (1,\ 284378684336837029526911489183254 9376) \\ (1,\ -207279680363499646029265538413172 0704) & (1,\ -130788392281012031541888839122885 9904) \end{matrix}$$

8. The shared secret keys are equal.

V. EXPERIMENTAL ANALYSIS

We used Python 3.10 to implement our key exchange protocol to verify the efficiency of our key exchange scheme. The average time taken to generate the secret key is given in Table 1. The data in Table 1 is then plotted in Fig 1 for visual representation.

Key size (bits)	Time taken (s)
8	0.1523
12	0.1701
14	0.2119
16	0.2611
24	0.2798
32	0.3080
36	0.3811

Table 1: Key generation time

5.1 Time complexity

The term time complexity refers to the duration an algorithm requires to run, expressed as a function of the length of the input. In our protocol, the addition and multiplication of the right duo seminearing and the set Z are defined independently. This makes the time complexity of our protocol equivalent to the classical multiplication of matrices. Thus the time complexity of our proposed protocol is O(n2), where n denotes the size of the matrix.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

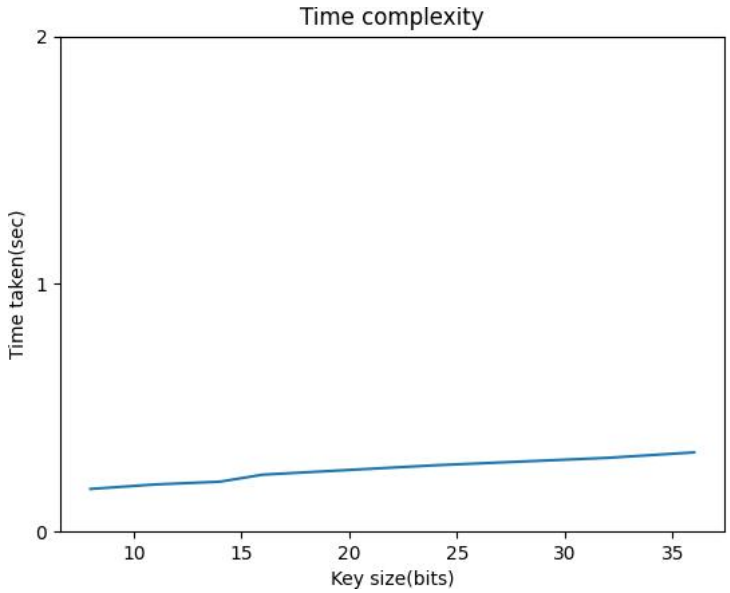

Figure 1: Time taken

VI. SECURITY ANALYSIS

Key exchange schemes are fundamental in ensuring the confidentiality and integrity of sensitive information during communication. A thorough security analysis helps identify vulnerabilities and weaknesses in the scheme, ensuring that adversaries cannot easily intercept or tamper with the exchanged keys. Security analysis helps in preventing unauthorized access to encrypted data. A robust key exchange scheme ensures that only authorized parties can derive the shared secret key, protecting against eavesdroppers and unauthorized users. An attacker may try to use the algebraic properties of the proposed

6.1 Known data attack

The Known data attack is an attacking technique where the adversary uses the known public information to extract the shared secret key. In our case with the knowledge of the matrices A, B, U and V the attacker may try to find the secret key. But to find the private parameters the attacker has to find the values of x, y, m and n from

$U = Ax \cdot By$ (1)

$V = Am \cdot Bn$ (2)

where, A, B, U and V are known matrices.

But solving the Equations 1 and 2 requires solving a system of non linear equations. It is well known that solving a system of non linear equations is very hard. Thus our protocol is secure from Known data attacks.

6.2 Brute force attack

A brute force attack is a systematic method employed by attackers to gain unauthorized access to a system or decrypt the encrypted data. In this type of cryptographic attack, the assailant methodically tries every possible combination within the key or password space until the correct one is found. The success of a brute force attack depends on the size of the key or password space, which, in turn, is influenced by factors such as the length and complexity of the key or password. The time required for a successful brute force attack is influenced by the computational power available to the attacker and the complexity of the secret key.

In our protocol, we used an infinite right duo seminearring. Therefore the cardinality of our set is infinite. Thus the key space of our key exchange protocol ensures the security against Brute force attack. Thus the selection of right duo seminearring makes our key exchange scheme resilient against Brute force attack.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

VII. CONCLUSION

Strong cryptographic methods are becoming important as technology continues to change our society. The use of right duo seminearring in cryptography is one such novel strategy. By using characteristics of right duo seminearrings, it gives a novel impact on resolving cryptographic problems. Understanding the implications of integrating this mathematical framework into cryptography is crucial for advancing the field and ensuring the security of our digital communications and transactions. In this paper, symmetric-key cryptosystem based on non commutative matrices over right duo seminearring R is introduced. This paper is focused on the application of right duo seminearring in cryptography. We define non commutative matrices over the right duo seminearring. We construct such a non commutative matrices by using an infinite right duo seminearring which is not a left duo seminearring. The classical Stickel key exchange protocol is explained, and our new protocol is introduced over the right duo seminearring and demonstrating its implementation using Python 3.10. The efficiency of the proposed key exchange scheme is substantiated through a detailed analysis, presenting average time data in Table 1 and visualizing the results in Figure 1. The strength of our security measures comes from using our right duo seminearrings in a cryptography framework. These seminearrings does not have the invertibility property. This is crucial for making sure our cryptographic systems are strong and reliable. It's really important for us to understand and recognize how this mathematical foundation helps us in cryptography.

Statements and Declarations

Data deposition information

All data generated or analysed during this study are included in this article.

Conflict of interest

The authors have no competing interests to declare that are relevant to the content of this article.

REFERENCES

[1] Diffie W and Hellman M E, New directions in cryptography, IEEE Transactions on Information Theory, vol. IT-22, no 6 (1976), pp. 644-654. https://doi.org/10.1145/3549993.3550007.

[2] Jackson, J., and R. Perumal. "An Algebraic Attack on the Key Exchange Protocol based upon a Modified Tropical Structure." Information and Computation (2024): 105259.

[3] Grigoriev D, Ponomarenko I. Constructions in public-key cryptography over matrix groups. arXiv preprint math/0506180. 2005 Jun 10. https://doi.org/10.48550/arXiv.math/0506180.

[4] Amutha, B., and R. Perumal. "Public key exchange protocols based on tropical lower circulant and anti circulant matrices." AIMS Mathematics 8.7 (2023): 17307-17334.

[5] Grigoriev D, Shpilrain V. Tropical cryptography. Communications in Algebra. 2014 Jun 3;42(6):2624-32. https://doi.org/10.1080/00927872.2013.766827.

[6] A, P., & R, P. (2023). Toeplitz matrices based key exchange protocol for the internet of things. International Journal of Information Technology. https://doi.org/10.1007/s41870-023-01608-w.

[7] Grigoriev D and V. Shpilrain. 2019. Tropical cryptography II: extensions by homomorphisms. Communications in Algebra 47 (10):4224–9. doi:10.1080/00927872.2019.1581213.

[8] Fiat, Amos. "Batch rsa." In Advances in Cryptology—CRYPTO'89 Proceedings 9, pp. 175-185. Springer New York, 1990.

[9] Jackson, J., Perumal, R. A tropical algebraic collatz conjecture based key exchange protocol for IoT environment. Int. j. inf. tecnol. (2024). https://doi.org/10.1007/s41870-024-02295-x.

[10] Jackson, J., & Perumal, R. (2023). Another Cryptanalysis of a Tropical Key Exchange Protocol. IAENG International Journal of Computer Science, 50(4), 1330-1336.

[11] Jackson, J., Perumal, R. A secure key exchange protocol for Industrial Internet of Things based on tropical triad matrix semiring. Int. j. inf. tecnol. (2024). https://doi.org/10.1007/s41870-024-02276-0.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, May 2025
Impact Factor: 7.67

[12] Ponmaheshkumar, A., and R. Perumal. "Enhancing vehicle IoT security through matrix power functions in supertropical semiring." Mathematics in Engineering, Science & Aerospace (MESA) 15, no. 1 (2024).

[13] Stickel E. A new method for exchanging secret keys. InThird International Conference on Information Technology and Applications (ICITA'05) 2005 Jul 4 (Vol. 2, pp. 426-430). IEEE. https://doi.org/10.1109/ICITA.2005.33