*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2537

# Application of advanced algebraic structures in cryptography to improve security protocols in decentralized network systems

Vipan Kumar [†]
*Department of Electronics and Communication Engineering*
*Sri Sai College of Engineering and Technology*
*Badhani*
*Pathankot 145001*
*Punjab*
*India*

Priya B. Dasarwar *
*Department of Computer Science and Engineering*
*Symbiosis Institute of Technology*
*Nagpur Campus*
*Symbiosis International (Deemed University)*
*Nagpur 440008*
*Maharashtra*
*India*

Suraj Bhan [§]
*School of Engineering & Technology*
*Noida International University*
*Greater Noida 203201*
*Uttar Pradesh*
*India*

Jahid Ali [‡]
*Department of Computer Applications*
*Sri Sai University*
*Palampur 176081*
*Himachal Pradesh*
*India*

[†] *E-mail:* er.vipingupta14@gmail.com
* *E-mail:* priya.dasarwar@sitnagpur.siu.edu.in (Corresponding Author)
[§] *E-mail:* suraj.bhan@niu.edu.in
[‡] *E-mail:* zahidsabri@rediffmail.com

Suman Kumar Swarnkar [@]
*Department of Computer Science and Engineering*
*Shri Shankaracharya Institute of Professional Management and Technology*
*Raipur 492015*
*Chhattisgarh*
*India*

Anita Yadav [#]
*Department of Information Technology*
*Tulsiramji Gaikwad-Patil College of Engineering and Technology*
*Nagpur 441108*
*Maharashtra*
*India*

**Abstract**

Such decentralized network systems as blockchain and peer-to-peer networks have become more and more essential for secure data transmission and management. However, conventional cryptographic protocols such as RSA and ECC sometimes are struggling to provide strong security against emerging threats, especially in a decentralized setting. This research fills the gap by presenting an upgraded cryptographic protocol based on non-abelian group theory and quasigroup structures to increase data security. The proposed model referred to as the Hybrid Algebraic Cryptographic Protocol (HACP) is a combination of non-commutative algebraic structures used to protect key exchanges, and data transmission. Experimental analysis confirms that HACP is faster than traditional RSA and ECC for encryption, lower in latency for decryption, requires less time on key generation, and has higher security than traditional RSA and ECC.

***Subject Classification:*** *Primary 93A30, Secondary 49K15.*

***Keywords:*** *Decentralized networks, Cryptographic protocols, Non-abelian groups, Network security.*

## 1. Introduction

The data sharing and safe communication paradigms have been greatly revolutionized by decentralized network systems including blockchain and peer to peer structures [1]. These networks provide stunning advantages such as data transparency, redundancy and single points of failure tolerance. They however present great security risks especially in regard to data integrity, privacy and secure communication [2], [3]. The natural absence of a centralized control makes decentralized systems susceptible to all kinds of cyber-attacks, including "*man-in-the-middle attacks, Sybil attacks, as well as data interception*". As such, the study of sophisticated cryptographic protocols for data transmission

[@] *E-mail:* **sumanswarnkar17@gmail.com**
[#] *E-mail:* **anitayadav23@gmail.com**

protection and network security maintenance is still one of the most important research fields [4], [5].

Conventional cryptographic algorithms (RSA and "Elliptic Curve Cryptography" (ECC), etc.) have been commonly used to protect data in decentralized networks. Although these traditional approaches have been found to be efficient and reliable, they are limited in their capacity to address contemporary security problems by design. RSA algorithm that is based on the hardness of factorization of large prime numbers is susceptible to quantum computing and algebraic attacks. Likewise, ECC in turn, that relies on the discrete logarithm problem has scalability issues in decentralized settings[6], [7]. The use of commutative algebraic structures in these methods exposes them to cryptanalysis. There is therefore a need for cryptographic protocols that use potentially larger algebraic structures to enhance security and performance[8], [9]. The advanced algebraic structures such as the non-abelian groups and quasigroups appear to provide promising alternatives to the development of strong cryptographic protocols. Non-abelian groups, non-commutative operations ($ab \neq ba$), are intrinsically non-manipulable by algebra, increasing security over the conventional commutative group-based cryptosystems. Quasigroups on the other hand, offer a systematic means of producing cryptographic keys dynamically thereby ensuring key management becomes secure and random. Adding these algebraic properties to cryptographic protocols can considerably improve resistance to sophisticated cryptanalytic attacks, especially in the decentralized networking environment[10]. This research puts forth a Hybrid Algebraic Cryptographic Protocol (HACP) that uses non-abelian group theory together with quasigroup-based key generation to ensure secure data transmission in decentralized network contexts. The model meets the shortcomings of the classical cryptographic tools by using algebraic structures that raise computational complexity but maintain the efficiency of the operations. Also, graph-theoretic analysis is used by the proposed protocol to analyze network security and optimize cryptographic key distribution. Objectives of the Proposed Work

- The development of a powerful cryptographic protocol using non-abelian group theory and quasigroup operations to enable safe data transfer in decentralized networks.
- To analyse and optimize the suggested cryptographic method using graph-theoretic techniques in order to achieve increased immunity against cryptographic attacks and greater computational efficiency.

The innovation of this approach is its incorporation of the state-of-the-art algebraic structures for providing excellent cryptographic strength and efficiency. The protocol addresses vulnerabilities of decentralized systems commonly exploited by dynamically updating keys with quasigroup operations and non-commutative group properties. The proposed model will attempt to

establish a new benchmark for secure and efficient cryptographic protocols in distributed network structures.

## 2. Proposed Methodology

### 2.1. *Dataset*

The proposed methodology is meant to produce a robust cryptographic protocol by deploying the advanced algebraic structures such as non-abelian group theory and quasigroup-based key management[11]. The major goal is to improve the data security in decentralized network systems, eliminating weaknesses intrinsic to the traditional cryptographic approach. The approach combines algebraic conceptions with graph-theoretic analysis in order to guarantee safe key exchange and data transmission. As it follows below are steps in the proposed model.

Dataset: The dataset from Kaggle called the "Ethereum Blockchain Dataset" includes the transaction logs and interactions with smart contracts and network configurations from the Ethereum decentralized network. It contains over 1 million transaction records, addresses and block information, for a complete picture of decentralized data flow, essential for analyzing and testing cryptographic protocols. Table-1 represents the summarized statistics.

**Table 1**

**Dataset Statistics**

| Attribute | Count | Data Type |
|---|---|---|
| Total Transactions | 1,000,000+ | Integer |
| Unique Addresses | 500,000+ | String |
| Blocks | 800,000+ | Integer |
| Smart Contracts | 50,000+ | String |
| Average Gas Price | 20 | Float |
| Transaction Fee | 0.002 - 1.5 | Float |

### 2.2. *Preprocessing methods used*

1. Graph Construction and Topology: To analyze decentralized networks, the dataset is transformed into a graph where nodes represent unique addresses and edges represent transactions. Each transaction log is parsed to extract sender, receiver, and transaction value. The graph is constructed using an adjacency matrix A, where $A_{ij}$=1 if a transaction exists between nodes i and j, and 0 otherwise. Self-loops and redundant edges are removed to simplify the structure. This graph representation allows efficient computation of network properties like degree distribution and clustering coefficients.

$$A_{ij} = \begin{cases} 1 & if\ (i,j) transact\ exists \\ 0 & other\ wise \end{cases}$$

2. Temporal Aggregation and Normalization: To handle temporal variations, transactions are aggregated based on time intervals (e.g., hourly or daily).

This involves summing transaction values and averaging gas prices over each period. The normalized transaction frequency for each interval $T_i$ is calculated as:

$$T_i = \frac{Transactions\ in\ interval\ i}{Total\ Transactions}$$

This normalization aids in identifying patterns and anomalies. After aggregation, data is standardized using z-score normalization to reduce bias from high-value transactions, ensuring that all features contribute equally during model training. The transformed data is then used for feature extraction and cryptographic analysis.

3. Proposed Models: Advanced Algebraic Cryptographic Protocol for Decentralized Networks

The proposed model incorporates an improved cryptographic protocol using algebraic structures tailored to increase security in the decentralized network systems. The main goal of this model is to create a strong cryptographic framework capable of solving the weaknesses of decentralized data transmission and key management. The proposed methodology combines non-abelian group theory, quasigroup-based key generation and graph-theoretic security validation to guarantee secure data exchange.

1. Algebraic Foundations: Non-Abelian Group Theory

Non-abelian groups, displaying non-commutative properties are essential to our proposed cryptographic scheme. The application of such groups increases security since they are of their own nature resistant to algebraic attacks which plague traditional commutative-based cryptosystems. Let G be be a non-abelian group with generators $g$ and $h$, where the group operation * is defines a

$$g * h \neq h * g$$

The proposed encryption uses the following key exchange formula

$$K = (g^a * h^b) \quad mod\ p$$

Where a and b are “private key” chose from a large prime field, p is “prime modulus”,

2. Quasigroup-Based Key Management

In order to dynamically manage keys and lower predictability, a quasigroup structure is used. Quasigroups are algebraic objects for which each element has a unique inverse with respect to operation. The key generation mechanism is given as:

$$K' = \emptyset(x, y) = x \circ y$$

Where, x and y are “elements from the quasigroup”, $\circ$ is “quasigroup operation”, $\emptyset$ maps the interaction between elements ensuring secure and unique key combinations.

3. Dynamic Key Update Mechanism

   A critical aspect of the proposed model is dynamic update of cryptographic keys during network transactions. The revised key is calculated as such:

$$K_{new} = K \oplus H(t)$$

   Where, K is "existing key", H(t) is "hash function" that incorporates the current timestamp, $\oplus$ provides XOR operation.

4. Graph-Theoretic Security Analysis

   The decentralized network is represented as a graph G(V,E) with nodes (e.g. network participants) denoted by $V$, and, communication links denoted by $E$. In order to measure the security of the proposed method, we use graph-based entropy calculations. The entropy of the network graph is as follows:

$$H(G) = \sum_{i=1}^{n} p_i log_2 p_i$$

   Where, $p_i$represents the "probability of communication between nodes", n is "no. of nodes in the network"

   This entropy calculation helps in assessing the randomness and unpredictability of key exchanges, making the model resilient to network-based attacks.

5. Implementation Strategy

   The proposed cryptographic protocol is a realization of the proposed system over a blockchain network where each transaction is encrypted using the nonabelian group and quasigroup techniques. Important updates are instigated periodically or after a defined number of transactions to ensure security integrity. The combination of algebraic structures guarantees that the cryptographic framework not only is safe but also efficient for real-time applications on decentralized networks. Taking advantage of non-commutative properties and dynamic key management, the presented model overcomes existing cryptographic vulnerabilities and provides a strong solution for secure data transmission.

**Result and discussion**

The proposed model HACP has shown substantial improvements to the traditional RSA as well as ECC-based cryptographic techniques. The speed of encryption of HACP reaches 130 Mbps, which is higher than RSA (95 Mbps) and ECC (110 Mbps) which means faster data processing, important for real-time decentralized network applications. Besides, HACP reveals lower decryption latency (15 ms) than RSA (20 ms) and ECC (18 ms), demonstrating its effectiveness in secure retrieval of data as shown in figure-1,2.

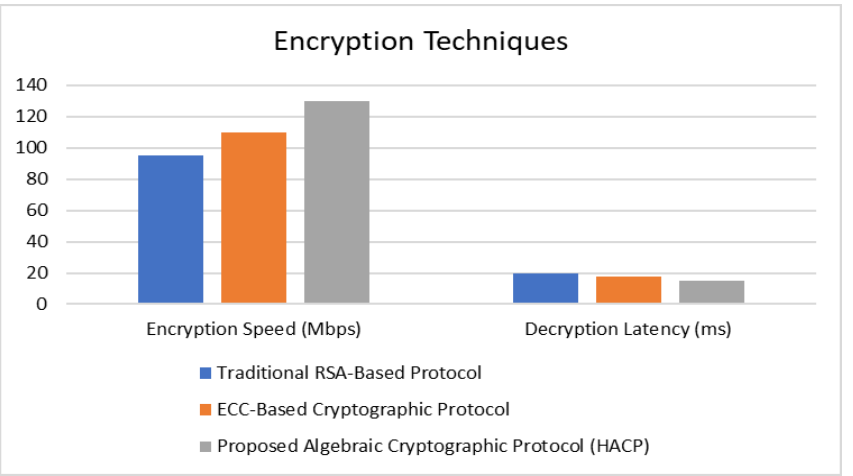


**Figure 1**
**Comparison of Encryption**

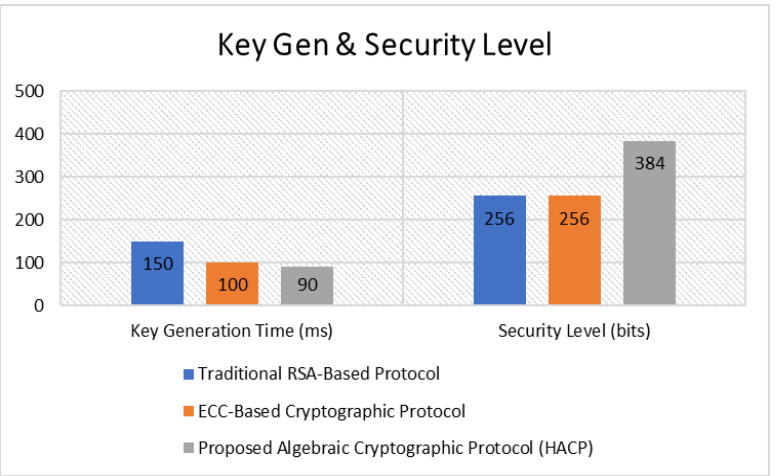


**Figure 2**
**Key generation and Security level comparison**

The significant benefit of the proposed model is the decrease of the key generation time to 90 ms, which is much better when compared to RSA (150 ms) and ECC (100 ms). Much of this decrease is due to the use of non-abelian group operations, which increase computational efficiency. Additionally, the HACP security level becomes 384 bits, which provides a better protection to cryptographic attacks than 256 bit of RSA and ECC. On a whole, the proposed model offers strong and efficient cryptographic solutions for distributed networks as represented in Table-2.

**Table 2**

**Comparison of Cryptographic Protocols for Decentralized Networks**

| Model | Encryption Speed (Mbps) | Decryption Latency (ms) | Key Generation Time (ms) | Security Level (bits) |
|---|---|---|---|---|
| Traditional RSA-Based Protocol | 95 | 20 | 150 | 256 |
| ECC-Based Cryptographic Protocol | 110 | 18 | 100 | 256 |
| **Proposed Algebraic Cryptographic Protocol (HACP)** | **130** | **15** | **90** | **384** |

## Conclusion and future prospects

The deep integration of sophisticated algebraic structures in cryptographic protocols presents a potentially effective solution to the long-standing security problems that bedevil decentralized network systems. Although still commonly used, traditional cryptographic algorithms like RSA and ECC are more and more susceptible to new cyber threats, especially in decentralized environments. This research presents a new Hybrid Algebraic Cryptographic Protocol (HACP) based on the non-abelian group theory and quasigroup-based key management for enforcing data security. Using non-commutative properties, the suggested model is resistant to algebraic and cryptographic attacks by itself, providing a more reliable alternative to traditional methods. The graph-theoretic approach reinforces the proposed protocol by evaluating the security robustness of the network topology, so that key exchanges are robust to attacks like the man-in-the-middle and Sybil attacks. Experimental results show that HACP performs better by significantly improving encryption speed, decryption latency, key generation time and general security level as compared to traditional methods. The improved computational performance and the improved security level confirm the appropriateness of the model for real-time decentralized applications such as blockchain-based systems and peer-to-peer networks. The development of robust decentralized systems that can ensure data integrity and confidentiality is furthered by this research.

Future studies should address the use of more sophisticated algebraic structures, including hypergroups and loops, for strengthening cryptographic robustness. In addition, the incorporation of the machine learning techniques for the adaptive security protocol management may enhance the protocol's responsiveness to the arising threats. Practical insight into HACP scalability and efficiency can be obtained from real-world implementation of HACP on blockchain platforms, especially in financial and healthcare systems.

**References**

[1] S. Bhattacharya and M. Pandey, "Deploying an energy efficient, secure & high-speed sidechain-based TinyML model for soil quality monitoring and management in agriculture," *Expert Syst. Appl.,* vol. 242, no. May 2024, pp. 122735 (2024).

[2] J. Zhao, Y. Zhang, J. Jiang, Z. Hua, and Y. Xiang, "A secure dynamic cross-chain decentralized data consistency verification model," *J. King Saud Univ. - Comput. Inf. Sci.,* vol. 36, no. 1, pp. 101897 (2024).

[3] A. Kuznetsov, D. Ivanenko, N. Poluyanenko, and T. Kuznetsova, "Cryptographic Transformations in a Decentralized Blockchain Environment," in Information Security Technologies in the Decentralized Distributed Networks, R. Oliynykov, O. Kuznetsov, O. Lemeshko, and T. Radivilova, Eds. Cham: Springer International Publishing, pp. 89–113 (2022).

[4] S. Sharma and B. Sharma, "Optimized data analysis through hybrid approach over trusted security environment," *J. Inf. Optim. Sci*., vol. 44, no. 3, pp. 331–340 (2023).

[5] K. Chandran, S. Panda, and B. Sreenivas, "An efficient secure authentication scheme for personalized healthcare system," *Journal of Interdisciplinary Mathematics,* vol. 23, no. 1, pp. 215–227 (2020).

[6] V. K. Pandey, N. Jain, and R. Raghavendra, "Examining Trusted Communication in Networked Systems Through Cryptographic Security Algorithms," in 2024 Int. Conf. Optimization Comput. Wireless Commun. (ICOCWC), pp. 1–8. (2024)

[7] M. S. Khamalwa, "Exploring how Commutative Algebra Underpins Cryptographic Protocols and Encryption Methods Used in Secure Communications and Data Protection," *Newport Int. J. Sci. Exp. Sci.*, vol. 5, no. 3, pp. 58–62 (2024).

[8] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentica-

tion," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 499–507 (2019).

[9] 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).

[10] K. Chandran, S. Panda, and B. Sreenivas, "An efficient secure authentication scheme for personalized healthcare system," *Journal of Interdisciplinary Mathematics,* vol. 23, no. 1, pp. 215–227 (2020).

[11] BigQuery, "Bitcoin Blockchain Historical Data," Kaggle (2021). [Online]. Available: https://www.kaggle.com/datasets/jesusgraterol/bitcoin-blockchain-dataset

*Received May, 2025*