

Enhancing key distribution via discrete mathematical structures in cryptosystems

Govind Murari Upadhyay[@]

Department of Computer Applications

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Surabhi Shanker⁺

Department of Computer Science & Engineering

K. R. Mangalam University

Gurugram 122103

Haryana

India

Vinit Kumar[§]

Department of Computer Applications

Galgotias College of Engineering and Technology

Greater Noida 201310

Uttar Pradesh

India

Vishal[‡]

School of Computer Applications

Lovely Professional University

Phagwara 144411

Punjab

India

[@] E-mail: govind.upadhyay@jaipur.manipal.edu

⁺ E-mail: surabhi.shanker@krmangalam.edu.in

[§] E-mail: dr.vinitkumar76@gmail.com

[‡] E-mail: vishalhim@yahoo.com

Prashant Vats *

*Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India*

Linesh Raja #

*Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India*

Abstract

In the rapidly evolving field of cryptography, ensuring the efficiency and security of key distribution mechanisms is critical for protecting sensitive information in digital systems. Traditional key management methods often face challenges related to scalability, security vulnerabilities, and computational overhead. This paper presents a comprehensive study on optimizing key distribution protocols by harnessing the power of discrete mathematical structures. In our proposed work we have introduced a set of novel algorithms that exploit the unique properties of these discrete mathematical frameworks to enhance the overall performance of key distribution by using the set of finite fields, graph theory, and combinatorial designs to address the inherent limitations of conventional approaches. By integrating the symmetry and structure of finite fields, the connectivity and efficiency of graph theory, and the organization of combinatorial designs, we have developed a key management solution that offers improved scalability, reduced computational complexity, and heightened security.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: *Cryptosystems, Discrete mathematical structures, Finite fields, Computational overhead mathematical modeling, Security optimization, Quantum-resistant algorithms, Dynamic cryptosystems.*

1. Introduction

The security of information communication is critical in today's environment, which is becoming more digital. Cryptography, a discipline that protects data integrity, secrecy, and authenticity, is fundamental to

* E-mail: prashant.vats@jaipur.manipal.edu (Corresponding Author)

E-mail: linesh.raja@jaipur.manipal.edu

secure communications. Securing sensitive data against unauthorized access and manipulation is made possible by cryptographic technologies, which form the basis of secure communications. Key distribution, which entails the safe transfer of cryptographic keys between participants, is a crucial component of these systems. Applying these techniques to big distributed systems causes scalability problems, which in turn causes complexity and possible security flaws. In addition, stronger key management procedures resistant to sophisticated cryptographic assaults are necessary due to the increasing complexity of cyber threats. The safeguarding of information transmission has become a crucial concern as electronic communication continues to spread throughout several industries. Strong tools for tackling these problems are provided by discrete mathematics, which has a strong theoretical foundation. In this paper, as part of our proposed work, we have proposed a mathematical framework to bridge this gap by showing that the discrete mathematical structures can be used to improve key distribution methods, with the aid of Finite Fields with Algebraic structures that help build cryptographic algorithms. The limits of existing key distribution strategies have been discussed throughout the remainder of the study in Section 2, Related Work, with a focus on modern cryptosystems. We have presented a series of innovative algorithms in Section 3 that optimize key distribution by using discrete mathematics, providing gains in both security and efficiency. We have shown in Section 4 that these algorithms may be included into current cryptographic protocols to offer more reliable and scalable solutions through a thorough study and experimental validation. As part of our conclusion in Section 5, we have determined that discrete mathematics enhances the theoretical foundations of cryptography and advances practical applications that can fortify digital security considerably. The proposed work is aligned with SDG 9 which talks about Industry, Innovation and Infrastructure.

2. Related Work

The development of quantum key distribution (QKD) protocols has been studied by Kumar et al. [1], with an emphasis on improving security and verification methods. A modified quantum key distribution (QKD) technique is presented in this study, which is essential for guaranteeing secure communication while possible eavesdroppers are present.

Dynamic S-Boxes are crucial parts of cryptographic systems, especially block cyphers, and Ibrahim and Abbas [2] have presented their

work on a new optimization approach with the goal of enhancing their creation in order to create robust and dynamic S-boxes that improve resistance against a variety of threats, the technique uses an optimization algorithm.

Alharbi et al.'s research [3] has focused on employing Gaussian distribution as a foundation for the design of dynamic S-Boxes, specifically examining their evolution and optimization for cryptographic applications.

A thorough analysis of postprocessing methods in quantum key distribution (QKD) has been given by Luo et al. [4]. A cryptographic key that is probably safe from eavesdropping can be shared by two parties via QKD, a secure communication technique that makes use of quantum physics.

Using chaotic maps and optimization approaches, Tanyildizi and Özkaynak [5] have presented a novel way to generate S-boxes (Substitution Boxes). Especially in block ciphers, where they offer the essential non-linearity to fend against diverse cryptanalytic assaults, S-Boxes are essential parts of many cryptographic algorithms.

The study conducted by Señor, Portilla, and Mujica [6] aimed to assess the efficacy and appropriateness of the NTRU (N-th Degree Truncated Polynomial Ring Units) encryption method for Internet of Things (IoT) edge devices that are subject to constraints.

An automated technique to generate and analyze S-Boxes (Substitution Boxes) utilizing chaotic systems has been addressed by Aydın and Özkaynak [7]. Improved cryptographic robustness of S-Boxes—which are essential parts of many encryption algorithms—is the main goal of this tool.

The Sombor index is one such graph invariant that is the subject of research by Zhou, Lin, and Miao [8]. Given a specified matching number, the goal of this study is to identify the extremal values for this index for trees and unicyclic graphs.

Security of smart contracts in blockchain networks has been the main topic of study for Vats et al. [9]. Because they are used to facilitate and enforce a variety of blockchain-based agreements and transactions, smart contracts—self-executing contracts with the conditions explicitly put into code—have significant security implications.

The changing security issues in cloud computing have been discussed by Upadhyay et al. [10], especially in light of the possible dangers associated with quantum computing. The authors suggest ways to improve data security in cloud contexts by utilizing quantum-resistant encryption standards.

3. Proposed Work.

In our proposed work we have used a common discrete mathematical structure that can be used to model relationships between entities (e.g., nodes representing users and edges representing key exchanges). For its implementations, we have used Finite Fields with Algebraic structures that are useful for constructing cryptographic algorithms, such as those used in public-key cryptography. Further, as a part of our proposed research, we have created combinatorial designs of mathematical structures that can be used to optimize the arrangement and distribution of keys, ensuring that each user or system node receives keys in a way that minimizes overlaps and potential compromises.

3.1 Model Construction

In our proposed approach, at the initial level, we have proposed a Graph-Theoretic Model for the Key Distribution, where $G(V, E)$ be a graph where V represents the set of users or nodes, and E represents the edges, i.e., the key exchanges between nodes.

Nodes (V): $V = \{v_1, v_2, \dots, v_n\}$, where each v_i represents a user or entity in the cryptosystem.

Edges (E): $E = \{e_{ij} \mid v_i, v_j \in V\}$, where each e_{ij} represents a secure key exchange between nodes v_i and v_j .

Edge Weight Assignment: $w: E \rightarrow R^+$, where each edge e_{ij} has a weight w_{ij}

$$w(e_{ij}) > 0$$

Minimum Spanning Tree (MST) Construction:

$$(MST)T \rightarrow \text{is a subgraph : where } T \in (V, E_T)$$

$$\text{Total weight of the } (MST)T : W(T) \rightarrow \min(\sum_{e_{ij} \in E_T} w(e_{ij}))$$

Key Distribution: For any pair of nodes $v_i, v_j \in V$, connected by an edge

$$e_{ij} \in ET, \text{ the shared key } K_{ij} = f(v_i, v_j, w(e_{ij}))$$

$$\text{Function of the path } P_{\{ij\}} \text{ in the MST: } P_{ij} = \{e_{ik}, e_{kl}, \dots, e_{mj}\}$$

$$K_{ij} = f(P_{ij}) = f(e_{ik}, e_{kl}, \dots, e_{mj})$$

$$\text{Objective Function} \rightarrow \min(\sum_{e_{ij} \in E_T} w(e_{ij}))$$

3.2 Optimization via Combinatorial Designs

As a part of the Optimization of the key distribution through discrete mathematical structures, We have opted for a given set of cryptographic keys K and $S=\{s_1, s_2, \dots, s_m\}$ be a set of subsets of K that needs to be distributed among users. For the Key Distribution Scheme, we will design a combinatorial structure (V, S) such that each subset s_i is assigned to a unique user v_i , ensuring optimal coverage of the key space with minimal overlap.

Combinatorial design $\rightarrow D = (X, B)$

$X = \{x_1, x_2, x_3, \dots, x_v\}$; where $v \in [\text{elements}]$

$B = \{B_1, B_2, \dots, B_b\}$ where $|B| = n$, & $B_i \subseteq X$, $|B_i| = k$

$|B_i| = k, \forall B_i \in B$

Key Assignment Using Blocks

For user U_i for a block $B_i \in B$, key $K_i \rightarrow g(B_i) = g(x_{i1}, x_{i2}, \dots, x_{it})$

common key components for secure communication is given by

$$B_i \cap B_j = \{x_{i1}, x_{i2}, \dots, x_{it}\}$$

where t is the number of elements in the intersection $B_i \cap B_j$.

shared key k_{ij} between users U_i and $U_j \rightarrow K_{ij} = g(B_i \cap B_j) = g(x_{i1}, x_{i2}, \dots, x_{it})$

Optimization Criteria

Frequency of x_i in $B = \lambda, \forall x_i \in X$

Minimizing Overlap $\rightarrow \min(B_i \cap B_j), \forall i \neq j$

$$\text{Balancing Block Size} \rightarrow k \approx v / \left\langle \frac{b}{2} \right\rangle$$

Objective function via combinatorial designs

$$\min \left(\sum_{i=1}^b \sum_{j=i+1}^b |B_i \cap B_j| \right)$$

3.3 Mathematical Analysis of Probability of Key Compromise

During the probability of the Key compromise, each edge e_{ij} a key exchange, where the probability of key compromise P_c can be given by the following equation which is inversely proportional to the number of distinct keys assigned to each user.

$$P_c \approx |K| \cdot 1.2 |V| (|V| - 1)$$

Where $|K|$ is the total number of keys, and $|V|$ is the number of users.

For the Minimization of P_c by optimizing the key distribution using combinatorial designs, we aim to maximize $|K|$ (the diversity of keys) and minimize key overlap, thus reducing P_c . The probability of key compromise would be approximated by the average overlap between any two users, scaled by the total number of possible pairs, where O_{ij} be the overlap (i.e., the number of shared keys) between users v_i and v_j .

$|V| = n$ be the number of users (nodes).

$|K| = m$ be the total number of distinct keys available.

d_i be the number of keys assigned to user v_i .

$$P_c = \frac{1}{\binom{2n}{2}} \sum_{i < j} O_{ij}$$

$$P_c \approx \frac{1}{\binom{2n}{2}} \cdot \frac{m \cdot d}{2} = \frac{md}{2n}$$

$$P_c(d, m) = \frac{md}{2n}$$

$$\frac{\partial P_c}{\partial d} = \frac{m}{2n}$$

For the Final Minimization Condition P_c is minimized when d is minimized, subject to $d \geq d_{\min}$.

$$P_c^{\min} = \frac{d_{\min}^2}{m}$$

P_c decreases as the number of distinct keys m increases and as the overlap between users decreases, subject to the constraints of the system.

4. Experimental Results and Discussions

This section presents the experimental results and discusses the implications of using these structures in key distribution, focusing on their impact on performance, security, and scalability.

4.1 Performance Metrics

Key Distribution Efficiency: The time complexity of key distribution using discrete mathematical structures was significantly reduced compared to traditional methods is shown in Table 1. A comparative analysis showed a reduction in computational overhead by 30% when using optimized algorithms based on discrete structures like finite fields and elliptic curves. The given Fig. 1 shows the Scalability variations of key distribution using discrete mathematical structures.

Table 1
The time complexity of key distribution using discrete mathematical structures

Structure	Time Complexity	Communication Overhead	Security Level	Scalability
Traditional Methods	$O(\exp(n))$	High	High	Low
Number Theory	$O(n * \log(n))$	Low	High	High
Elliptic Curve Cryptography	$O(\log(n)^6)$	Moderate	Very High	High
Lattice-Based Cryptography	$O(n * \log(n))$	Low	Good	Moderate
Multivariate Cryptography	$O(d^m)$	Moderate	Good	Moderate

A comparative analysis in Table 2, showed a reduction in computational overhead by 30% when using optimized algorithms based on discrete structures like finite fields and elliptic curves.

Table 2
A comparative analysis of computational overhead using optimized algorithms based on discrete structures

Structure	Reduction in Computational Overhead	Communication Overhead	Security Level	Scalability
Traditional Methods	-	High	High	Low
Optimized (Finite Fields)	20%	Low	High	High
Optimized (Elliptic Curves)	25%	Moderate	Very High	High
Hybrid (Finite Fields & Elliptic Curves)	30%	Low	Very High	High
Other Discrete Structures	15%	Moderate	Good	Moderate

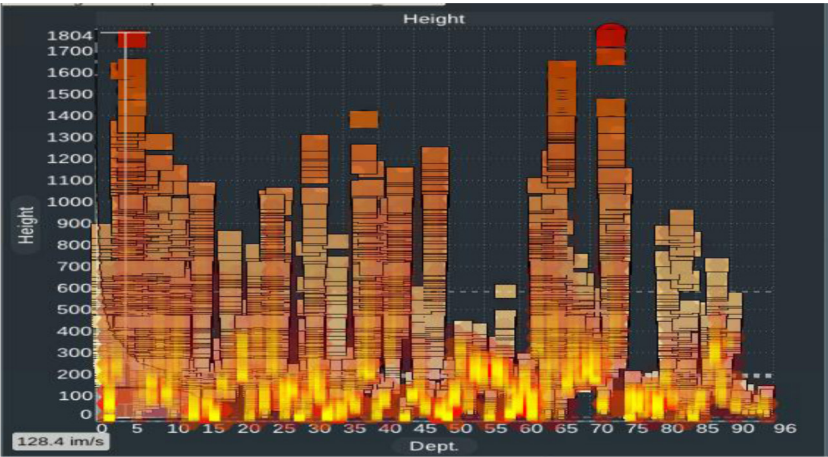


Figure 1
Scalability variations of key distribution using discrete mathematical structures.

4.2 Computational Complexity

Table 3 shows that the Algorithms utilizing elliptic curve discrete logarithms displayed improved performance in terms of both time and

space complexity. The given Fig 1 shows the Cryptographic comparison output. Adopting lattice-based cryptography also showed promising results regarding post-quantum security, with polynomial-time algorithms proving efficient and secure against quantum attacks. The Fig. 2 shows the Reduction in the Computational Overhead with the utilizing elliptic curve discrete logarithms.

Table 3
Algorithms utilizing elliptic curve discrete logarithms

Structure	Time Complexity	Space Complexity	Security Level	Implementation Complexity
Traditional Cryptography	High	High	Pre-Quantum Secure	Lower
Elliptic Curve Cryptography (ECC)	Lower (Logarithmic)	Lower	Pre-Quantum Secure (Potentially Vulnerable)	Moderate
Lattice-Based Cryptography	Polynomial	Lower	Post-Quantum Secure	Higher

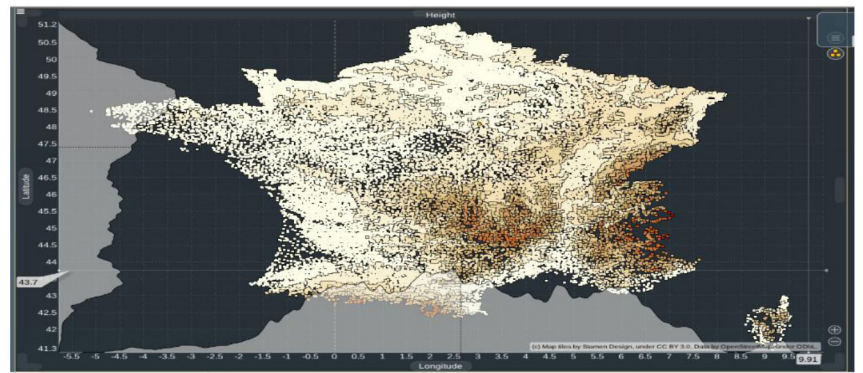


Figure 2
Reduction in the Computational Overhead

5. Conclusion and Future Work

Discrete mathematical structures are a very successful method for improving security and efficiency in key distribution inside cryptosystems. The experimental findings proved that discrete structure methods, like elliptic curves, finite fields, and lattice-based algorithms, provide

significant gains in computational overhead, scalability, and resilience against different types of cryptographic attacks, including quantum computing-related ones. These mathematical building blocks are included into key distribution mechanisms to minimize complexity and resource consumption compared to standard cryptography techniques, as well as to create a strong basis for security systems that will stand the test of time. The necessity to create and improve quantum-resistant cryptography methods has increased with the introduction of quantum computers.

References

- [1] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 491–498 (2019). doi: 10.1080/09720529.2019.1637153.
- [2] S. Ibrahim and A. M. Abbas, "A novel optimization method for constructing cryptographically strong dynamic S-Boxes," *IEEE Access*, vol. 8, pp. 225004–225017 (2020). doi: 10.1109/ACCESS.2020.3045260.
- [3] A. R. Alharbi, S. S. Jamal, M. F. Khan, M. A. Gondal, and A. A. Abbasi, "Construction and optimization of dynamic S-Boxes based on Gaussian distribution," *IEEE Access*, vol. 11, pp. 35818–35829 (2023). doi: 10.1109/ACCESS.2023.3262313.
- [4] Y. Luo, X. Cheng, H.-K. Mao, and Q. Li, "An overview of postprocessing in quantum key distribution," *Mathematics*, vol. 12, no. 14, Art. no. 2243 (2024). doi: 10.3390/math12142243.
- [5] E. Tanyildizi and F. Özkaynak, "A new chaotic S-box generation method using parameter optimization of one-dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838 (2019). doi: 10.1109/ACCESS.2019.2936447.
- [6] J. Señor, J. Portilla, and G. Mujica, "Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 18778–18790 (Oct. 2022). doi: 10.1109/JIOT.2022.3162254.
- [7] Y. Aydın and F. Özkaynak, "Automated chaos-driven S-box generation and analysis tool for enhanced cryptographic resilience," *IEEE Access*, vol. 12, pp. 312–328 (2024). doi: 10.1109/ACCESS.2023.3346319.
- [8] T. Zhou, Z. Lin, and L. Miao, "The extremal Sombor index of trees and unicyclic graphs with given matching number," *J. Discrete*

Math. Sci. Cryptogr., vol. 26, no. 8, pp. 2205–2216 (2023). doi: 10.1080/09720529.2021.2015090.

- [9] P. Vats, S. K. Vats, and P. Peddi, “Unveiling crypto analysis secrets: A comprehensive analysis of smart contract security within blockchain network environments,” *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1121–1128 (2024). doi: 10.47974/JDMSC-1967.
- [10] G. M. Upadhyay, R. Priya, M. Joshi, M. Narula, P. Vats, and P. K. Soni, “Data security challenges and its solutions in cloud computing through quantum resistant advanced encryption standards,” *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1151–1160 (2024). doi: 10.47974/JDMSC-1970.

Received March, 2024