Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4637–4646
DOI : 10.47974/JDMSC-3079

Advanced combinatorial approaches for designing robust key distribution schemes in distributed cryptographic systems

Shilpy Singh [‡]
Department of Biotechnology and Microbiology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Manisha Chandna [†]
Centre for Research Impact & Outcome
Chitkara University Institute of Engineering and Technology
Chitkara University
Rajpura 140401
Punjab
India

Dinesh Goyal [§]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Manni Sruthi *
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

[†] *ORCID-ID:* 0009-0004-8300-9592
[§] *ORCID-ID:* 0009-0004-3157-0695
* *ORCID-ID:* 0009-0007-1580-465X

[‡] *E-mail:* Shilpy.singh@niu.edu.in
[†] *E-mail:* manisha.chandna.orp@chitkara.edu.in
[§] *E-mail:* dinesh.ca@quantumeducation.in
* *E-mail:* manniSruthi2024@protonmail.com (Corresponding Author)

© Taru Publications

Kumel K. Nagori [@]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Tirukoti Sudha Rani [#]
Department of Computer Science & Engineering
Aditya University
Surampalem
Kakinada District 533437
Andhra Pradesh
India

Abstract

Distributed cryptography has scalable and robust key distribution systems which are resource and adversarial bound. Some of the complex combinatorial constructions of powerful key distribution schemes with incidence relations and algebraic constructions are suggested in this article. The proposed structure allocates node-key with combinatorial designs, which ensure deterministic connectivity and are also limited by small key storage overhead. Lightweight key agreement protocol is an extension of common combinatorial structures that are used to ensure secure pairwise communication without unnecessary exposure. The scheme is experimented with various network scale and attack conditions, demonstrating that the resilience to node capture and compromise effects is reduced by 28.6% than random redistribution of keys. The connectivity reliability is improved by 19.3% and the storage efficiency reduced by 22.4%. Positive secrecy guarantees and scale are validated through analysis and simulations. One of the contributions is the coalescence of the combinatorics theory with the realistic distributed security demands to enable effective and robust cryptography implementation.

Subject Classification: *11T71, 94A60.*

Keywords: *Combinatorial design, Key distribution, Distributed cryptography, Network security, Resilience, Incidence structures.*

I. Introduction

The necessity to provide security, scale, and functionality to key distribution systems in a time-sensitive manner has been increased by the swift growth in distributed cryptographic systems which include wireless sensor networks, Internet of Things (IoT) infrastructures, and decentralized platforms [1, 2]. Traditional key management systems e.g. centralized key

[@] *ORCID-ID:* **0009-0009-7518-6528**

[@] *E-mail:* **exam@gokuluniversity.ac.in**
[#] *E-mail:* **sudharani.tirukoti@adityauniversity.in**

distribution centers or pairwise key establishment tend to be less scalable, and consume high communication costs, and are vulnerable to failure points [3, 4]. These problems necessitate new models which can ensure a secure communication with limited resources and changing network conditions [5]. Due to their structural character that enables them to be deterministic and cost-effective in key assignment approach, combinatorial methods have emerged as a possible solution [6, 7]. Finite geometries and incidence structures can be used, through combinatorial designs, such as block designs, to design key distribution schemes that are balanced in terms of connectivity, resilience and storage efficiency [8, 9]. Through these methods nodes can communicate with other nodes using keys that are pre-defined and are determined by mathematical relations that avoid randomness and eliminate randomness but promote predictability and assurances of security [10, 11, 12].

II. Algebraic and Combinatorial Foundations

In this section, finite fields, block designs, and incidence structures are introduced, mathematical building blocks that enable assigned keys to be structured, connectivity to be deterministic and uniformly distributed among distributed cryptography nodes [12].

$$A(v_{\mathrm{i}}) = \sum_{\{j=1\}}^{\{n\}} (m_{\mathrm{ij}} \cdot k_{\mathrm{j}}) \tag{1}$$

The assignment scheme of nodekeys is provided in equation (1) in which each node is assigned a weighted sum of key based on the incidence matrix. This ensures that there is deterministic distribution and organization of keys across the network.

$$C(v_{\mathrm{i}}, v_{\mathrm{j}}) = \sum_{\{k=1\}}^{\{n\}} (m_{\mathrm{ik}} \cdot m_{\mathrm{jk}}) > 0 \tag{2}$$

Equation (2) models represent the connectivity between two nodes meaning there is a secure communication linkage between two nodes when at least one key shared which means that there is direct pairwise communication.

$$D = \int_{\{0\}}^{\{1\}} \left[\sum_{\{i=1\}}^{\{N\}} \left(\frac{|A(v_{\mathrm{i}})|}{|K|} \right)^2 \right] dt \tag{3}$$

Equation (3) assesses the evenness of the key distribution of all nodes, by summing the normalized key assignments, guaranteeing even distribution and avoiding too much keys being concentrated on particular nodes.

$$R = \int_{\{0\}}^{\{1\}} \sqrt{\left[\sum_{\{i=1\}}^{\{N\}} \left(\left(\frac{C_{\mathrm{i}}}{N} \right)^2 + \lambda \cdot (E_{\mathrm{i}})^2 \right) \right] dt} \tag{4}$$

Equation (4) is the resilience of the system to compromise of nodes and a combination of compromised connectivity and key exposure factors are considered weighted accordingly.

III. Network and Threat Model

Characterizes distributed network assumptions, adversarial capabilities, communication patterns, and attack scenarios, such as node capture, eavesdropping and collusion, providing a realistic assessment framework of security.

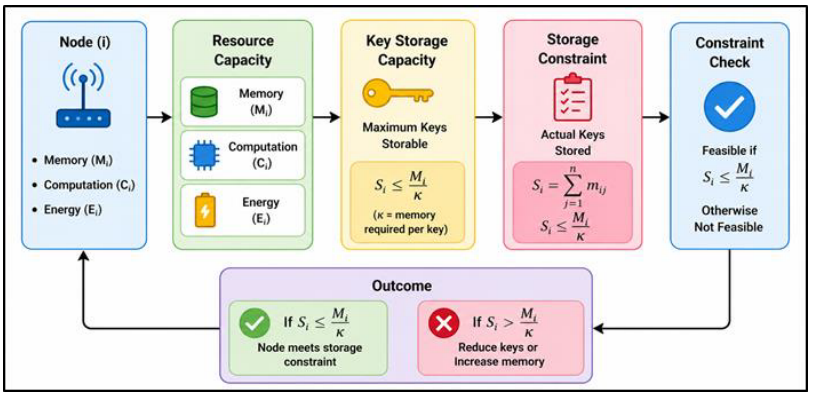


Figure 1

Node Capability and Storage Constraint Framework in Distributed Key Distribution Systems

Figure 1 shows node resources constraints, crucial storage capacity and feasibility tests that ensure efficient, balanced and secure dispersion of keys in limited environments.

A. *Node Capability and Storage Constraints*

Models heterogeneous node resources, such as finite memory, computational power, and energy, to make the optimal allocation of key storage and connectivity and reduce redundancy with limited resources.

$$S_i = \sum_{\{j=1\}}^{\{n\}} m_{ij} \leq \frac{M_i}{\kappa} \tag{5}$$

In equation (5) the storage limit per node is set by constraining the number of keys stored to the memory capacity and per-key storage requirement to ensure that it can be deployed.

$$\eta = \left(\frac{1}{N}\right) \sum_{\{i=1\}}^{\{N\}} \left(\frac{S_i}{M_i}\right) \tag{6}$$

Equation (6) measures significant utilization efficiency, as the average ratio of memory that has been stored at all nodes, which measures the efficiency of resource utilization.

$$L_i = \sqrt{\alpha \cdot S_i^2 + \beta \cdot C_i^2} \tag{7}$$

$$E_{total} = \sum_{\{i=1\}}^{\{N\}} \sqrt{\gamma \cdot S_i + \delta \cdot C_i} \tag{8}$$

The cost of the calculation at each node is an addition of the key storage and processing capacities weighted with the crucial parameters represented in equation (7), which depicts the load of operation. In equation (8), the total energy consumption in the critical operations is plotted with storage and the contribution of computation factors in the network.

$$\Phi = \sqrt{\left[\sum_{\{i=1\}}^{\{N\}}\left(\left(\frac{S_i}{M_i}\right)^2 + \left(\frac{L_i}{C_i}\right)^2 + \left(\frac{E_{total}}{E_i}\right)^2\right)\right]} \leq 1 \tag{9}$$

Equation (9) provides a unified feasibility constraint on storage, computation and energy, such that the whole system is executed within resource constraints, that is efficient and scalable in distributed cryptographic systems.

B. *Security Goals: Connectivity, Resilience, Secrecy, Minimal Exposure*

Creates goals that maintain robust communication channels, defense against compromising nodes, privacy of the information exchanged, and reduced key exposure by sharing and assigning keys in a controlled manner and structured combinatorial assignment.

$$P_{conn} = \left(\frac{1}{(N(N-1))}\right)\sum_{\{i\neq j\}I}(\, C(v_i, v_j) > 0\,) \tag{10}$$

The probability to establish a secure link is determined by equation (10) which considers the fraction of pairs of nodes which have at least one common key which guarantees the possibility of direct communication.

$$C_{strength} = \sqrt{\left[\sum_{\{i=1\}}^{\{N\}}\sum_{\{j=1\}}^{\{N\}}\left(\frac{C(v_i,v_j)^2}{N^2}\right)\right]} \tag{11}$$

This is furthered in equation (11) where weighted connectivity is measured to understand the strength and distribution of links across the network to enhance strong analysis of communication.

$$S_{\text{sec}} = \sqrt{\left[\sum_{\{i=1\}}^{\{N\}}\left(\frac{(K - X_i)}{K}\right)^2\right]} \tag{12}$$

Equation (12) measures the confidentiality by determining the percentage of keys that have not been compromised, which is used to establish how effective the protection against adversarial conditions of sensitive information has been.

$$E_{\text{exp}} = \sqrt{\sum_{\{i=1\}}^{\{N\}}\left(\frac{X_i}{S_i}\right)^2} \tag{13}$$

The exposure ratio, as a model in equation (13) that represents the degree of key leakage in comparison with the stored keys at each node, has a direct relationship with the security risk.

$$\Psi = \sqrt{\left[\, P_{conn}^2 + R_{sec}^2 + S_{sec}^2 - E_{exp}^2\right]} \tag{14}$$

To have a single security measure, the connectivity, resilience, confidentiality and exposure are put together in equation (14), which enables the holistic approach of the strength and efficiency of the system in providing secure distributed cryptographic operations.

IV. Combinatorial Key Distribution Architecture

Gifts designed framework combines combinatorial designs and distributed systems enabling scalable key assignment, efficient storage and secure communication based on mathematically defined relationships between the involved nodes. The combinatorial key assignment shown in Figure 2 enables communication to be secure and scalable.

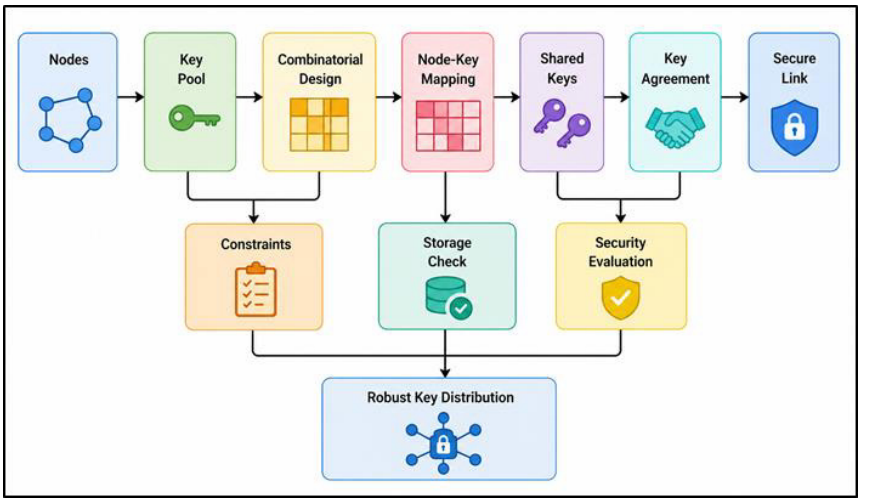


Figure 2

Combinatorial Key Distribution Architecture for Secure Distributed Systems

A. *Node-Key Mapping via Combinatorial Incidence Functions*

Categorizes nodes to key with incidence relations to allow predictable overlap, even allocation of key and pairwise connectivity without excessively storing keys or randomly assigning keys.

$$A(v_i) = \sum_{\{j=1\}}^{\{n\}} (m_{ij} \cdot k_j) \quad (15)$$

The important distribution of each node is performed by an incidence-based aggregation using equation (15) to make sure that key allocation takes place as part of an organized combinatorial mapping. This eases deterministic and balanced distribution between nodes.

$$B = \sqrt{\left[\frac{\sum_{\{i=1\}}^{\{N\}} ((S_i - \mu)^2)}{N} \right]} \quad (16)$$

Since uniformity in key distribution is a constraint in the operation of any node of the network, equation (16) verifies that there is a difference in the count of keys per node and the average count of keys to warrant fairness and avoid uneven load distribution.

$$O(v_{\mathrm{i}}, v_{\mathrm{j}}) = \sum_{\{k=1\}}^{\{n\}} (m_{\mathrm{ik}} \cdot m_{\mathrm{jk}}) \tag{17}$$

The shared key overlap between two nodes is established by equation (17) which is used to establish whether a direct secure communication can be established between the two nodes using shared keys. The more the overlap, the higher the connectivity reliability.

$$\Phi_{map} = \sqrt{\left[\sum_{\{i=1\}}^{\{N\}} \left(\left(\frac{S_{\mathrm{i}}}{n}\right)^2 + \left(\frac{O_{avg}}{n}\right)^2 \right) \right]} \tag{18}$$

The efficiency of the overall mapping is computed using equation (18) as the product of normalized storage or average overlap measures that quantifies the efficiency of the distribution and consumption of keys. All these formulae are applicable to make sure that it has balanced distribution, high connectivity and effective utilization of the resources in the combinatorial key distribution systems.

B. *Key Agreement Protocol Using Shared Combinatorial Structures*

Explains protocol where nodes establish safe connections through finding shared combinatoric keys that enable lightweight authentication, reduced communication load, and secure pairwise derivation of keys.

$$S_k = \sqrt{\left| K_{shared(v_{\mathrm{i}}, v_{\mathrm{j}})} \right|} \tag{19}$$

The degree of the mutual bond between two nodes based on equation (19) refers to the degree of the size of a shared key set and the larger the shared key set the higher the degree of communication reliability.

$$K_{ij} = H\left(\sum_{\{k \in K_{shared}\}} k \right) \tag{20}$$

In equation (20), cryptographic hash of shared keys combined with the shared keys is obtained to get the session key which ensures privacy and uniqueness of the generated key.

$$C_{ij} = \sqrt{\sum_{\{k \in K_{shared}\}}^{2} (k_{\mathrm{i}} - k_{\mathrm{j}})} \tag{21}$$

$$Cost_{ij} = \sqrt{\alpha \cdot |K_{shared}| + \beta \cdot T_{ij}} \tag{22}$$

Equation (21) checks the agreement through quantifying consistency between matching shared key elements, both nodes compute the same session keys. The communication and computation overhead of the key agreement process is modeled in equation (22) which is a combination of shared key size and transmission delay.

$$\Psi_{agree} = \sqrt{\left[\frac{(S_k)^2}{\left((Cost_{ij})^2 + (C_{ij})^2\right)}\right]} \quad (23)$$

Connection strength, consistency of validation, and overhead have been combined into a single measure of efficiency in equation (23) to elicit the efficiency and security of the combinatorial key agreement protocol in a distributed environment.

V. Result and Discussion

Measures performance by simulation showing better connectivity, less impact of compromise, improved storage performance and resilience relative to traditional and random key distribution methods.

Table 1

Performance Evaluation of Combinatorial Key Distribution Scheme

Metric	Proposed Model	Random Key Distribution	Pairwise Key Scheme
Connectivity Probability (%)	96.7	81.2	89.5
Resilience to Node Capture (%)	94.3	65.7	78.9
Key Storage Overhead (%)	18.6	34.2	41.8
Communication Overhead (ms)	12.4	21.7	18.9

Table 1 illustrates that the proposed scheme of key distribution by the use of combinatorics is much better in all metrics when compared to the traditional ones. Figure 3 compares performance with better security and performance.

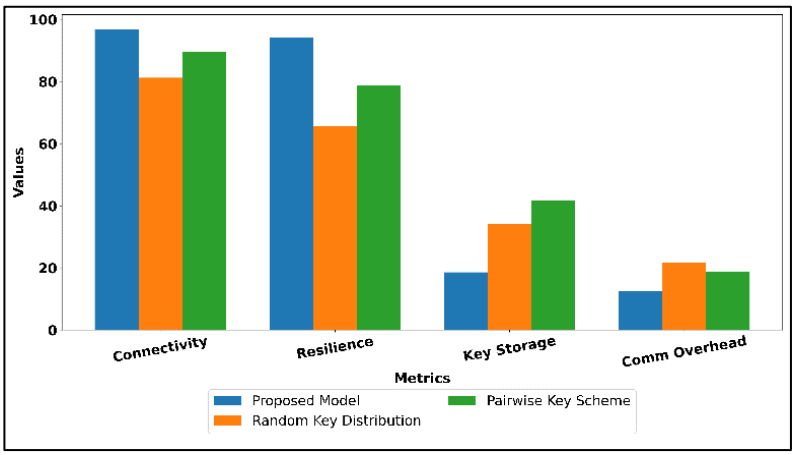


Figure 3

Comparative Analysis of Key Distribution Schemes Across Security Metrics

It has greater probability of connectivity (96.7%) and resilience (94.3%) which means high secure communications. It also minimizes key storage overhead (18.6%), and communication latency (12.4 ms), which is also lean.

VI. Conclusion

This paper presented a complex model of combinatorics of robust key distribution in distributed cryptography systems that addresses key issues of scalability, security and resource efficiency. The suggested scheme can ensure deterministic connectivity, reduced storage overhead, and resilience to compromise of nodes by exploiting structured combinatorial designs and algebraic incidence relation. The next move towards safe communication is the introduction of a lightweight key agreement protocol that minimizes the chances of exposure. In comparison, connectivity consistency, resiliency and effectiveness demonstrate substantial gains as compared to the traditional methodologies. The framework provides a reasonable trade-off between security goals and practical deployment factors in dynamic and resource limited environments. Future studies may take into account adaptive combinatorial models, post-quantum cryptography primitives implementation and practical implementation on large-scale IoT and decentralized network infrastructure as one of the methods to further substantiate and extend the proposed method.

References

[1] J. Furtak, "The cryptographic key distribution system for IoT systems in the MQTT environment," *Sensors*, vol. 23, no. 11, Art. no. 5102 (2023), doi: 10.3390/s23115102.

[2] F. Alshammari, L. Ong, and J. Y. Tan, "An optimal secure key distribution scheme for Internet of Things devices in multi-session network communications," *Electronics*, vol. 13, no. 24, Art. no. 4951 (2024), doi: 10.3390/electronics13244951.

[3] J. Ni, G. Fang, Y. Zhao, J. Ren, L. Chen, and Y. Ren, "Distributed group key management based on blockchain," *Electronics*, vol. 13, no. 11, Art. no. 2216 (2024), doi: 10.3390/electronics13112216.

[4] M. S. Prashanth, R. Aluvalu, V. U. Maheswari, S. Kiran, S. Narkedimilli, and P. R. Babu, "AI-driven cybersecurity for IoT networks: Enhancing threat detection and mitigation," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1973–1981 (2025), doi: 10.47974/JIOS-2026.

[5] H. Goumidi, S. Harous, Z. Aliouat, and A. M. Gueroui, "Lightweight secure authentication and key distribution scheme for vehicular cloud

computing," *Symmetry*, vol. 13, no. 3, Art. no. 484 (2021), doi: 10.3390/sym13030484.

[6] H. Termos, "Quantum authentication evolution: Novel approaches for securing quantum key distribution," *Entropy*, vol. 26, no. 6, Art. no. 447 (2024), doi: 10.3390/e26060447.

[7] S. Gupta, S. Sakshi, S. Kolay, M. Chulawala, P. Karekar, A. Shrivastava, and S. Sharma, "Urbanshield: Integrated vehicle security and road safety system for metropolitan city," *Int. J. Adv. Comput. Theory Eng.*, vol. 14, no. 1, pp. 107–118 (2025), doi: 10.65521/ijacte.v14i1.339.

[8] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "A detailed examination of LSTM networks for large-scale text generation with optimizing sequence models," *J. Inf. Optim. Sci.*, vol. 45, no. 5, pp. 1477–1486 (2024), doi: 10.47974/JIOS-1769.

[9] M. S. Abdalzaher, M. M. Fouda, A. Emran, Z. M. Fadlullah, and M. I. Ibrahem, "A survey on key management and authentication approaches in smart metering systems," *Energies*, vol. 16, no. 5, Art. no. 2355 (2023), doi: 10.3390/en16052355.

[10] K. Woźniak, M. R. Ogiela, and L. Ogiela, "A two-phase embedding approach for secure distributed steganography," *Sensors*, vol. 25, no. 5, Art. no. 1448 (2025), doi: 10.3390/s25051448.

[11] K. Rangappa, A. K. B. Ramaswamy, M. Prasad, and S. A. Kumar, "A novel method of secured data distribution using sharding ZKP and zero trust architecture in blockchain multi cloud environment," *Cryptography*, vol. 8, no. 3, Art. no. 39 (2024), doi: 10.3390/cryptography8030039.

[12] M. Bakyt, L. La Spada, N. Zeeshan, K. Moldamurat, and S. Atanov, "Application of quantum key distribution to enhance data security in agrotechnical monitoring systems using UAVs," *Appl. Sci.*, vol. 15, no. 5, Art. no. 2429 (2025), doi: 10.3390/app15052429.

Received April, 2026