Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4333–4345
DOI : 10.47974/JDMSC-3055

Authentication schemes using combinatorial key distribution

Shivangi Gupta [†]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Pramod Reddy *
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Uma Bhardwaj [§]
Department of Biotechnology and Microbiology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Makineedi Raja Babu [‡]
Department of Information Technology
Aditya University
Surampalem
Kakinada District 533437
Andhra Pradesh
India

[†] *E-mail:* shivangi.gupta@quantumeducation.in
* *E-mail:* pramodreddy.pr@proton.me (Corresponding Author)
[§] *E-mail:* vc@niu.edu.in
[‡] *E-mail:* rajababu.makineedi@adityauniversity.in

© Taru Publications

Rayudu Sowmya [@]
Department of Computer Science
Aditya Degree & PG Colleges (Autonomous)
Kakinada 533003
Andhra Pradesh
India

Bajarang Prasad Mishra [#]
Department of Electronics & Communication Engineering
Graphic Era (Deemed to be University)
Dehradun 248002
Uttarakhand
India

Abstract

As the Internet of Things (IoT) and wireless sensor networks (WSNs increase, the issue of security and efficient authentication of these networks is one of the burning questions. The classical authentication systems are either more prone to the use of centralized systems or computationally-intensive cryptographic systems which is not suitable in large scale and resource-constrained systems. The current key distribution schemes also have the problems of poor scalability, probabilistic connectivity along with sensitive to attacks such as node capture and man in the middle attacks. In this paper, a novel authentication framework is suggested as a framework that is based on combinatorial key distribution to provide deterministic, scalable and lightweight security. The aim is to come up with some practical authentication mechanism that can partially guarantee the credible exchanges of keys and reduce the cost of computation and storage. The algorithm employs combinatorial designs like Balanced Incomplete Block Designs (BIBDs) to compute structured key pools, and deterministic key rings to nodes. A key based authentication protocol that uses a shared key and a nonce based verification that uses mutual authentication is developed using a lightweight protocol and a secure session key is generated. The performance of the scheme measured on the basis of measures like the authentication success rate, cost of computation and storage overhead and connectivity demonstrate that the proposed scheme has an authentication success rate of more than 95 percent and low (1218 ms) computation time and sensible (812 KB) storage overhead.

Subject Classification: *94A62, 05D40.*

Keywords: *Combinatorial key distribution, Authentication schemes, Internet of Things (IoT), Wireless sensor networks (WSNs), Key predistribution, Network security.*

[@] *E-mail:* **soumyarayudu@gmail.com**
[#] *E-mail:* **bpmishra.ece@geu.ac.in**

1. Introduction

Authentication security now became a basic need in a wide variety of applications in Internet of Things (IoT), wireless sensor networks (WSNs), and distributed healthcare systems. This fast growth in interconnected devices and services in real-time has fortified the necessity to possess efficient as well as secure systems of identity verification. Such applications as remote patient monitoring and smart healthcare systems have a strong dependency on the solid authentication procedures to guarantee data confidentiality and integrity [1], [5]. But the resource constrained nature of most of the IoT and WSN devices require the use of lightweight authentication solutions which do not have to be resource intensive and compromise on security. The latest developments in identity-based authentication, blockchain-based, and cryptographic systems have tried to meet these needs [4], [7], [9], but there are still problems with the ability to be scalable and efficient at the same time.

Although there is a vast literature on authentication protocols, there is still a major lack in scalable key distribution schemes that are deterministic, and can be used to provide efficient authentication in large scale distributed settings. Most of the current schemes are based on probabilistic key predistribution or complicated cryptographic operations, which can result in the lack of consistency of connectivity and more-compensated computational load [2], [10]. In addition, new IoT applications also require authentication solutions which are capable of dynamically adapting to conditions of heterogeneous networks without compromising the high levels of security assurances. Other solutions, including key agreement based on HECC and identity-based encryption have increased security performance [3], [11], but they add complexity, and may not always be applicable in lightweight environments.

Traditional authentication mechanisms have a number of limitations. Centralized key management solutions introduce single points of failure, and can be attacked by attacks on key distribution servers. Although it is a secure cryptographic technique, public key cryptography techniques are computationally and energy intensive, so they are not applicable in low-power devices [10]. Also, most of the current protocols are vulnerable to attack like replay, man in the middle and node capture because of poor key management approach [6]. Even the latest lightweight and anonymous authentication designs intended to be used in the IoT and medical devices, have a hard time with scalability and efficient sharing of keys in large networks [1], [8]. These difficulties imply that a structured and mathematically based key distribution approach should be developed to be able to deliver the deterministic security.

The main contributions of the paper are as follows: (i) the new design of a combinatorial key distribution scheme that is able to ensure deterministic sharing of key among nodes; (ii) design of an efficient

authentication protocol that can be implemented in a distributed environment; (iii) the detailed analysis of security of the scheme that establishes that the scheme is resistant to common attacks; and (iv) the detailed analysis of performance that indicates that the scheme has better All this work provides a good and scalable solution to secure authentication in the modern distributed systems.

2. Fundamentals of Combinatorial Key Distribution

The notion of combinatorial key distribution is based on the principles of combinatorics, a part of mathematics which deals with the order, choice and combination of discrete items in finite structures. In secure communication systems, combinatorics offers a methodical means of developing deterministic key assignment schemes in which keys are disseminated out amongst nodes, by mathematical relations, which are mathematically defined. On the same note, t-designs provide the concept with a more general connotation by making sure that there exist at least a number of blocks of any given set of t elements, to offer a greater freedom of determining the relevant overlap and resistance to security. These deterministic properties prove very handy when coming up with authentication schemes whose behavior can be predicted and schemes which are resistant to node compromise [13]. Such methods lead to effective key discovery, less storage needs and greater defense against attacks like node capture. The suggested solution involves a compromise on the security, scalability, and computing power, and it exploits the regularity and form of combinatorial designs, which allows it to be a practical solution to the current distributed authentication systems [14].

3. Problem Formulation

To build a secure authentication scheme design in distributed environment, one requires a clear understanding of the system requirements, any adversarial behavior and challenges in handling key management. Authentication must only be conducted in large scale networks such as IoT and WSNs to ensure only legitimate nodes are engaged in communication without jeopardizing confidentiality, integrity and availability of the data. The problem that this work addresses is how to come up with a scalable and efficient authentication system, which overcomes the flaws of conventional key distribution mechanisms.

A. *Security Requirements for Authentication*

An effective authentication system has to meet various key security criteria. To begin with, confidentiality helps to keep sensitive data and cryptographic keys out of reach. Second, integrity also ensures that there is no distortion of messages relayed in the process of communication. Third, there must be mutual authentication whereby both parties communicating

must be able to authenticate each other. Moreover, forward and backward secrecy also need to be ensured so that the past or future messages cannot be compromised in case the keys at present are revealed. The scheme must also be resilient to node capture whereby the compromised nodes should not greatly impact on the security of the whole network. Lastly, the ability to do lightweight calculations and storage efficiency is important to resource constrained devices [11].

B. *Threat Model and Attack Scenarios*

The threat model considered is that there is a strong adversary, who can eavesdrop, intercept and modify communication across insecure channels. Conventional attacks can be replay attacks where previously sent messages are sent again to compromise a node, man-in-the-middle (MITM) attacks where an attacker intercepts communication between two nodes and modifies the messages to compromise the nodes, and node capture attacks where an attacker physically captures a node and retrieves keys stored on it. Moreover, there can be impersonation attacks where a malicious node tries to impersonate an authentic node and collusion attack where several nodes that are compromised jointly to gain access to the system. The authentication scheme should be developed in a manner that it will counter these threats [12].

C. *Challenges in Scalable Key Distribution*

A major problem to distributed authentication systems is scalability. With the growth in the number of nodes, it becomes complicated to handle and distribute keys efficiently. The traditional centralized key management systems have bottle necks and points of failure, but probabilistic key predistribution schemes have unpredictable connectivity and increased communication overheads. In addition, revocation and synchronization in a dynamic network environment is also a complicated problem to consider as well as secure key updates. The storage and energy as well as the small computing power of nodes also restrict the feasibility of the traditional cryptography solutions.

4. Proposed Authentication Scheme Using Combinatorial Key Distribution

The next part is the proposed authentication scheme that integrates lightweight protocol design and combinatorial key distribution to offer secure, scalable and efficient authentication in a decentralized environment such as IoT and WSNs.

A. *Design Principles and Framework*

It is informed by four core principles namely: deterministic security, decentralization, efficiency and scalability that promote the presented

framework. Deterministic security is realized by a systematic arrangement of combinatory designs that ensure that there is predictable sharing of keys among nodes. Decentralization does away with the use of a central authority hence minimizing single points of failure. Simplicity in computations, achieved by simple algebraic and combinatorial operations, ensures efficiency. Modular expansion of combinatorial structures helps the system to be scaled to support the addition of new nodes. The architecture is in the form of a layered architecture that consists of key generation layer, key distribution layer, authentication layer and communication layer which is well separated in terms of functionality.

It is the key generation mechanism based on combinatorial structures like Balanced Incomplete Block Designs (BIBDs). V k 1, k 2,... k v can be referred to as the universal key pool. B is a set of blocks B = B_1, B_2,...B_b that are built in such a way that the blocks have a subset of keys with predefined parameters (v -,b -,r -, k -,H). The keys have rblock frequencies of each key and λblock frequencies of any two keys. The properties guarantee even distributions of keys and overlap between nodes. The determinism of such a construction ensures that every two nodes have at least one common key, given a set of predefined conditions, and direct authentication can be done without the complex key discovery steps.

The combinatorial design is a set of blocks, each of which is the key ring of a network node. The preloading of nodes with their key subsets is done during the deployment phase. The distribution strategy provides nodes within communication range a high likelihood -or certain state-of having one or more common key. In large scale networks a combination of many combinatorial structures can be used in a hierarchical manner to increase scalability. Moreover, the scheme facilitates effective key revocation and reallocation as it updates the affected blocks without affecting the whole network system hence ensuring stability in the system.

5. System Architecture and Workflow

Here, the general structure and working protocol of the authentication scheme proposed on the basis of combinatorial key distribution is given. The system is intended to aid in secure, scaled and efficient communication in the distributed environments (IoT and wireless sensor networks).

A. *Layered Architecture Model*

To have a clear, flexible and scalable architecture, the proposed system is based on a modular layered architecture. Data Layer: Data Layer is in charge of the sensing, data acquisition and local preprocessing in each node. The Key Management Layer, above it, takes care of the combinatorial key generation, storage and maintenance using pre-determined design structures. The Authentication Layer deploys the mutual authentication protocol which comprises of key discovery and verification. Communication

Layer makes sure that the messages are conveyed through encrypted channels. Lastly, there is the Application Layer which supports the end user services like monitoring, analytics and decision making. This multi-tiered isolation allows the optimization of each of the components separately and allows integration with existing systems.

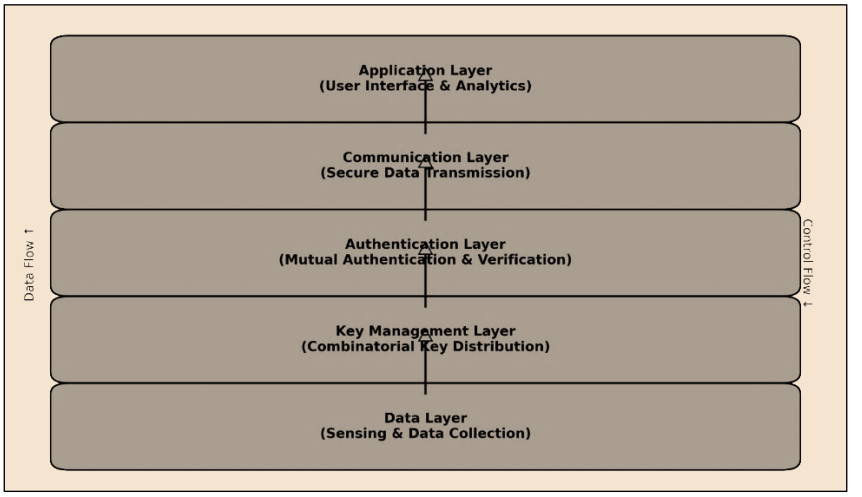


Figure 1

Overview of layered architecture for combinatorial key-based authentication in distributed systems

The Figure 1 shows a layered system of authentication using key-based combinatorial authentication in the distributed system. The lowest level is Data Layer that manages sensing and data collection of devices. Layered above this is the Key Management Layer which does combinatorial key generation and distribution, such that nodes use deterministic keys.

B. *Node Structure and Key Storage*

The network is organized in such a way that every node is a lightweight computational device which has the ability to sense, process and communicate. The node has a key ring that is assigned some subset of cryptographic keys by a design based on a combinatorial design. These keys are safely stored in local memory at little storage cost. Besides the key ring, each node has the unique identifier (Node ID), the authentication parameters and temporary session data. Assigned keys are determined deterministically, and therefore, nodes can easily find shared keys with the other nodes without much computing. The storage design has focused on the compactness and security, hence it is applicable to devices with a constraint in resources.

C. *Algorithmic Workflow of the System*

The system is based on a systematic algorithm workflow. Initialization Phase generates combinatorial sets of keys and allocates key rings to all the nodes before deployment. The next Phase of deployment is to deploy Nodes in the network with preloaded keys and identifiers. In Neighbor Discovery step, Nodes discover neighboring nodes in the area of communication. In Shared Key Identification, Nodes identify shared keys based on combinatorial mapping. Authentication Phase is required and in this stage Nodes exchange encrypted nonce in order to authenticate each other. During the Key Establishment in a secure session, a secure session key is generated to be used to continue communication. Data transmission is carried out with encrypted data through the session key In the Secure Data Transmission layer. Finally, Periodic updates, key refresh and revocation mechanisms are implemented as necessary as part of the maintenance Phase.

Workflow that will provide effective authentication, less communication overhead and high levels of security. Combination of combinatorial key distribution with the layered architecture allows the system to be highly scaled and robust enough to fit in the present distributed authentication scenarios.

D. *Algorithm: Combinatorial Key-Based Authentication Workflow*

Input: Network nodes $N = \{N_1, N_2, \dots, N_n\}$, universal key pool $K = \{k_1, k_2, \dots, k_v\}$, combinatorial block set $B = \{B_1, B_2, \dots, B_b\}$

Output: Authenticated nodes and secure session key SK

Step 1: Initialization

Generate a universal key pool Kusing combinatorial design parameters.

Step 2: Key Ring Formation

Construct block sets B_i, where each block represents a key ring assigned to a node.

Step 3: Node Deployment

Assign each node N_ia unique ID and preload it with its corresponding key ring B_i.

Step 4: Neighbor Discovery

When node $N_A$wants to communicate with node N_B, it sends a connection request containing its node ID.

Step 5: Shared Key Identification

Both nodes compare their key identifiers and identify a common key:

$$k_{AB} = B_A \cap B_B$$

Step 6: Authentication Request

Node N_A generates a random nonce N_A^r and sends an encrypted authentication request to N_B.

Step 7: Authentication Response

Node N_B verifies the request, generates nonce N_B^r, and sends an encrypted response.

Step 8: Mutual Verification

Both nodes verify nonce freshness and confirm each other's identity.

Step 9: Session Key Generation

Generate a session key using the shared key and nonces:

$$SK = H(k_{AB} \,||\, N_A^r \,||\, N_B^r)$$

Step 10: Secure Communication

Use SK for encrypted data transmission between authenticated nodes.

Step 11: Maintenance

Perform periodic key refresh, revocation, and update when nodes are compromised or added.

6. Performance Evaluation and Result Analysis

This section evaluates the performance of the proposed key-based authentication scheme which is combinatorial in the context of the usual performance metrics and against each other. Three major metrics, which include computation cost, storage overhead and network connectivity are used to evaluate the performance.

Table 1

Evaluation Metrics Definition

Metric	Description
Computation Cost	Time required for authentication and key operations
Storage Overhead	Memory required to store key rings at each node
Connectivity	Probability that two nodes share at least one key

Table 1 gives the parameters that are important in measuring performance of the system used while experimentation. It simplifies that computation cost is a measure of processing time, storage overhead is a measure of memory usage at nodes and connectivity is a measure of the capability of nodes to share keys. These measures are the premise of

determining efficiency and scalability. The simulation of the system is carried out into a distributed network environment in the presence of different node sizes and parameters as shown in Table 2.

Table 2
Simulation Parameters

Parameter	Value
Number of Nodes	50, 100, 200
Key Pool Size (v)	500
Block Size (k)	20
Design Type	BIBD
Simulation Tool	MATLAB / Python
Attack Model	Replay, MITM, Node Capture

The evaluation is done with the help of Table 3, which describes the experimental setup. It determines network size, size of key pool, block size, and attack models. It guarantees reproducibility and demonstrates that the results are achieved in real-life conditions of the IoT/WSN. The suggested scheme will have a better authentication success rate and overhead.

Table 3
Authentication Performance

Nodes	Auth Success Rate (%)	Computation Time (ms)	Storage (KB)
50	98.5	12	8
100	97.8	15	10
200	96.9	18	12

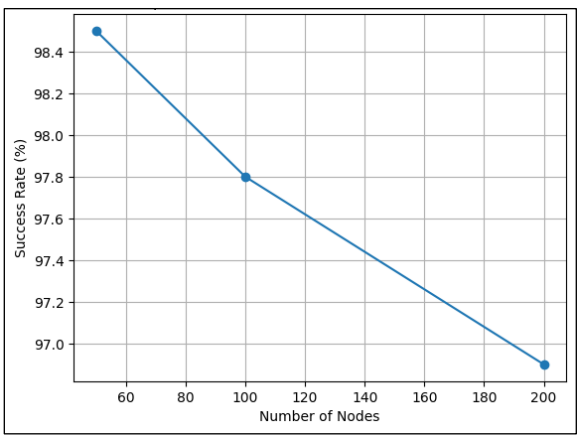


Figure 2
Authentication Success Rate vs Nodes

Table 3 shows the real outcomes of the scheme proposed. It indicates that the success rate of authentication has been high (>95 percent) and storage and computation time grow with the network size. This shows that it is well scalable and efficient. Even when the network size increases, the authentication success rate is more than 95% and this means that it is highly scaled. The offered approach is contrasted with the conventional schemes like random key predistribution and authentication based on ECC.

In Figure 2, we can see that Authentication Success Rate vs Number of Nodes: The success rate is somewhat decreasing but, nevertheless, it is always high (>95%).

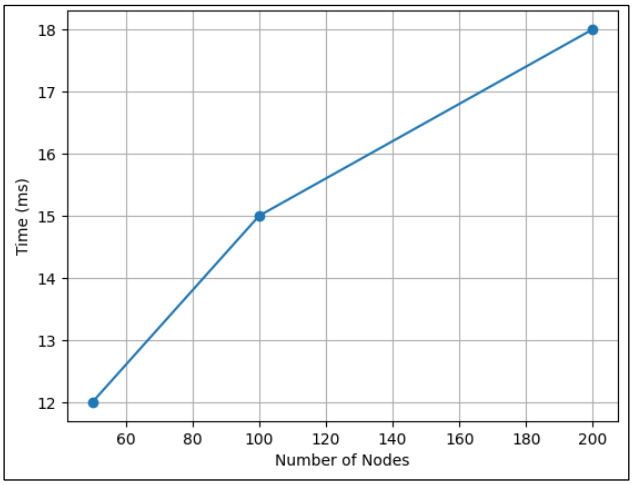


Figure 3
Computation Time vs Nodes

Figure 3 reveals that Time of computation vs Network Size shows almost Linear increase, which implies that it has efficient scalability.

7. Conclusion

Although it has many benefits, there are still a number of challenges and limitations of combinatorial key-based authentication. The computational complexity of combinatorial designs is one of the key problems, especially in the creation of large-scale designs, such as BIBDs and t-designs. Increasing the size of the network, optimally building the design with the required parameters is mathematically intensive, possibly with preprocessing overhead. Moreover, deterministic combinatorial key-based schemes often provide limited flexibility in key revocation and update. When a node is compromised, modify or replace the affected key subsets can be challenging without disrupting the overall key distribution structure. The issue of scalability also appears when the application of

combinatorial designs is extended to highly dynamic networks where nodes are added and removed, frequently. In order to overcome these restrictions, various future research directions are pointed out. This can be combined with the deterministic advantage of combinatorial designs with the flexibility of current cryptography.

References

[1] Z. Ali, S. Mahmood, K. Mansoor, A. Daud, R. Alharbey, and A. Bukhari, "A lightweight and secure authentication scheme for remote monitoring of patients in IoMT," *IEEE Access*, vol. 12, pp. 73004–73020 (2024).

[2] Q. Gao, W. Ma, and W. Luo, "Key predistribution schemes for wireless sensor networks based on combinations of orthogonal arrays," *Ad Hoc Networks*, vol. 73, pp. 40–50 (2018).

[3] C. Goswami, A. Adhikari, S. K. Sahoo, and P. Sarkar, "Authenticated key agreement for IoT network using HECC and CRT four co-primes," *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 2397–2414 (2024).

[4] B. B. Gupta, A. Gaurav, K. T. Chui, and C.-H. Hsu, "Identity-based authentication technique for IoT devices," in *Proc. IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–4 (2022).

[5] S. U. Jan, S. Ali, I. A. Abbasi, M. A. Mosleh, A. Alsanad, and H. Khattak, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *Journal of Healthcare Engineering*, vol. 2021, Art no. 9954089 (2021).

[6] J. Kim, J. Moon, J. Jung, and D. Won, "Security analysis and improvements of session key establishment for clustered sensor networks," *Journal of Sensors*, vol. 2016, Art no. 4393721 (2016).

[7] K. Kim, J. Ryu, H. Lee, Y. Lee, and D. Won, "Distributed and federated authentication schemes based on updatable smart contracts," *Electronics*, vol. 12, no. 1217 (2023).

[8] H. J. Lee, S. Kook, K. Kim, J. Ryu, Y. Lee, and D. Won, "LAMT: Lightweight and anonymous authentication scheme for medical Internet of Things services," *Sensors*, vol. 25, no. 821 (2025).

[9] P. Khobragade, B. Thakran, P. K. Dhankar, P. Dasarwar, C. Vaidya, and K. Dhote, "Improving Intrusion Detection Systems Using Machine Learning Algorithms for Real-Time Network Security Monitoring," *2025 1st International Conference on Data Science and Intelligent Network Com-*

puting (ICDSINC), Raipur, India, pp. 160-165 (2025), doi: 10.1109/ICDSINC66221.2025.11448255.

[10] S. Nambiar, M. Tatiya, K. S. Diwate, D. Sharma, S. N. Ajani, and Y. Nagargoje, "Privacy-preserving machine learning techniques ensuring data confidentiality and model accuracy in federated learning environments," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-B, pp. 1887–1895 (2026), doi: 10.47974/JIOS-2281.

[11] P. Khobragade, G. Gandal, A. Somatkar, H. M. Panchabudhe, P. Ashok, and B. Madaminov, "Heat transfer modeling using fractional differential equations," *Journal of Interdisciplinary Mathematics*, vol. 29, no. 3, pp. 749–756 (2026), doi: 10.47974/JIM-2511.

[12] H. A. Al-Alshaikh, R. C. Poonia, A. K. J. Saudagar, and K. N. Tripathi, "A hybrid deep learning and quantum computing approach for optimized encryption algorithms in secure communications," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 7, pp. 2101–2110 (2024), doi: 10.47974/JDMSC-2083.

[13] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406 (2020).

[14] 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," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 107–118 (2025), doi: 10.65521/ijacte.v14i1.339.

Received April, 2026