Knowledge Processing Studies. 2025, 14, 5(1): 78-89.

International Journal of Knowledge Processing Studies
(KPS)

Homepage: http://kps.artahub.ir/

ORIGINAL RESEARCH ARTICLE

Key Pre-Distribution Scheme: Enhanced Security in Distributed Systems

Alireza Babaei[1], Hamid Haj Seyyed Javadi[2,*]

[1] *Ph.D. Candidate, Department of Mathematics, Faculty of Basic Science, Shahed University, Tehran, Iran.*
alireza.babaei@shahed.ac.ir
[2] *Professor, Department of Computer Engineering, Faculty of Engineering, Shahed University, Tehran, Iran.*
h.s.javadi@shahed.ac.ir, 0000-0003-0082-036X.

ARTICLE INFO

Article History:
Received: 2024-12-20
Revised: 2025-01-17
Accepted: 2025-02-24
Published Online: 2025-03-25

Keywords:
Noncommutative Rings, LFSR (Linear Feedback Shift Register)
Key Pre-distribution, Key Agreement, IoT Security.

Number of Reference: 39
Number of Figures: 0
Number of Tables: 0

DOI:10.22034/kps.2025.495040.1217

ABSTRACT

This paper presents a novel key pre-distribution scheme aimed at improving secure communication using noncommutative rings theory with Linear Feedback Shift Registers (LFSRs) for resource-constrained environments such as Internet of Things (IoT) and Wireless sensor networks (WSN). The applied method combines noncommutative rings theory with LFSR to provide an efficient key pre-distribution framework. The use of noncommutative rings enables the creation of more complex and secure mathematical frameworks for cryptographic key generation. Noncommutative rings enhance resilient property against common security threats, while LFSRs are selected for their efficiency and minimal overhead in key generation, making this approach particularly effective for resource-constrained environments, such as IoT and sensor networks. The proposed scheme delivers a lightweight, scalable, and highly secure solution for key pre-distribution. Simulation results demonstrate notable improvements in both security and efficiency. In addition, the mathematical proofs in this paper will show achievement lower memory and computational compared traditional method, these finding and scalability of the proposed approach make it proper solution for securing modern distributed systems. **©authors**.

►**Citation:** Babaei, A., & Haj Seyyed Javadi, H. (2025). Key Pre-Distribution Scheme: Enhanced Security in Distributed Systems. *International Journal of Knowledge Processing Studies (KPS)*, 5(1): 78-89. Doi: 10.22034/kps.2025.495040.1217

1. Introduction

In the rapidly expanding world of distributed systems, where communication and data exchange occur continuously, the security of data transmission is paramount. As technologies such as the Internet of Things (IoT) and Wireless Sensor Networks (WSNs) become increasingly prevalent, ensuring secure communication channels among numerous resource-constrained devices poses a significant challenge (Siraparapu et al., 2024). One of the foundational methods for achieving secure communications in such environments is the use of key pre-distribution schemes (KPS). These schemes involve distributing cryptographic keys to network nodes before deployment, enabling secure communication without real-time key exchanges, which are often impractical in dynamic or limited-resource environments (Moussavi et al., 2018; Solari Esfehani et al., 2021; Ahangar et al., 2024).

Traditional key pre-distribution schemes have been effective to some degree but often suffer from limitations in scalability, security, and computational efficiency. Most classic schemes, such as random key pre-distribution, struggle with issues such as vulnerability to node capture attacks, increased memory requirements, and lack of flexibility in adapting to network changes. These challenges highlight the need for more sophisticated cryptographic techniques capable of providing both high security and efficiency for the vast array of devices within distributed networks (Solari Esfehani et al., 2021; Azizi Nasrabadi et al., 2025).

An important approach to addressing these challenges is the application of noncommutative ring theory (Lam, 1991). Noncommutative rings, which are algebraic structures where the order of multiplication influences the result, provide intricate and highly secure frameworks for cryptographic operations. By utilizing the unique properties of noncommutative rings, we can develop more complex cryptographic systems that are resilient against conventional cryptographic analysis and attacks. This attribute of noncommutative rings renders them an attractive option for advanced key pre-distribution schemes, as they offer improved security while ensuring mathematical efficiency (Bechkit et al., 2013).

In addition, Linear Feedback Shift Registers (LFSRs) serve as an effective mechanism for the efficient generation of pseudorandom sequences while maintaining minimal computational overhead (Savir et al.,1990; Bhat et al., 2007). LFSRs, due to their simplicity and deterministic properties, are particularly well-suited for resource-constrained environments, such as IoT networks, where devices typically have limited processing capabilities and memory. LFSRs can generate complex sequences that function as encryption keys, enabling even lightweight devices to engage in secure communication protocols without imposing significant computational overhead.

In this paper, we introduce an innovative key pre-distribution scheme that integrates noncommutative rings theory with Linear LFSRs for the purpose of cryptographic key generation.

By combing these two structures, the proposed scheme seeks to overcome the limitations of traditional KPS methods, providing a solution that is both secure and efficient. The use of noncommutative rings provides a robust algebraic framework, while LFSRs facilitate lightweight key generation that is appropriate for various distributed systems. This hybrid methodology seeks to improve scalability, adaptability, and resilience against potential threats, positioning it as a viable solution for contemporary distributed networks. There are many works on key pre-distribution in WSNs (Anzani et al., 2018; Morshed Aski et al., 2020; Bahrami et al., 2018; Farshid et al., 2022), but they are not applicable to the IoT due to further limitations of computing space.

The remainder of this paper is organized as follows: we begin with a review of relevant literature on key pre-distribution in cryptography and the applications of LFSR

in key generation. Subsequently, we provide a detailed explanation of the proposed scheme, highlighting the structure of the noncommutative ring and the function of the LFSR in the secure key generation process. Lastly, we present the simulation results and a security analysis that illustrate the efficiency and robustness of our approach in comparison to conventional key pre-distribution methods (Masaeli et al., 2020; Tajeri et al., 2022).

2. Literature Review

The field of secure communication within distributed systems has experienced notable progress over the past decade, especially in the advancement of KPS designed for resource-constrained networks, including IoT and WSNs.

Algebraic Structures in Cryptography

The application of algebraic structures, including groups, rings, and fields, has been extensively examined within the field of cryptography. Traditional methodologies frequently utilize finite fields and commutative rings for key generation and encryption mechanisms, owing to their mathematical simplicity and well-established properties. In contrast, noncommutative structures have not been as thoroughly investigated. Research by (Anshel et al.,1999). introduced noncommutative cryptographic frameworks, highlighting their potential for improved security. These studies established a foundation for the integration of noncommutative algebra into practical cryptographic protocols.

Rings theory, a fundamental area of abstract algebra, contributes significantly to contemporary cryptography by providing complex algebraic structures that are essential for secure encryption mechanisms (Hanoymak et al., 2015). Rings are defined as algebraic structures that contain elements that are capable of addition and multiplication and that adhere to certain properties. A special and notable type of rings, known as noncommutative rings, add a further complication, in that the order of multiplication can affect the result (i.e., $ab \neq ba$). This property of noncommutative rings makes them particularly useful in cryptographic applications, where high complexity is crucial to protect against possible attacks**.**

The application of noncommutative rings in cryptography has garnered significant interest due to their capacity to withstand traditional cryptanalytic methods that are designed for simpler, commutative structures such as finite fields (Kumar et al., 2017). A notable instance of this is the deployment of noncommutative rings in cryptosystems derived from group ring theory, which provide enhanced security through increased complexity (Anshel et al., 1999). In recent years, researchers have investigated the potential of noncommutative ring-based cryptographic systems for the development of secure public-key schemes, digital signatures, and hash functions. These systems leverage the computational challenges associated with problems in noncommutative ring structures, which are often exceedingly difficult to reverse-engineer without specific knowledge of the corresponding keys or structures (Janani et al., 2023).

Researchers are exploring the use of noncommutative rings to create cryptographic systems that are robust against conventional attacks and align with quantum-resistant protocols. This characteristic enhances the appeal of noncommutative rings in sectors that prioritize long-term security. Although ring-based cryptosystems are still in the developmental phase, their growing implementation in encryption and key distribution underscores their potential to significantly advance secure communication systems.

Key Pre-Distribution Schemes

KPS play a critical role in establishing secure communication channels within distributed networks, especially in contexts with limited computational resources, such as IoT and WSNs. The primary objective of KPS is to allocate cryptographic keys to network nodes prior to deployment, thereby

enabling secure communication without the necessity for real-time key exchange. Traditional key pre-distribution schemes,

Traditional KPSs, such as the random key pre-distribution method introduced by (Eschenauer et al., 2002), involve the random allocation of keys to nodes from an extensive key pool. This approach enables nodes with shared keys to establish secure connections. Although these schemes are effective, they exhibit limitations in scalability and are susceptible to node capture attacks, where the compromise of a single node can jeopardize multiple links throughout the network.

To address these limitations, researchers have developed advanced key pre-distribution methods leveraging combinatorial schemes and algebraic structures. For instance, as outlined in reference (Blundo et al., 1998), we introduced polynomial-based schemes that enhance resilience against node absorption by utilizing polynomial functions to generate shared keys among nodes. Another area of research focuses on combinatorial design-based schemes that employ mathematical constructs, such as matrices and finite fields, to achieve more scalable and adaptable key distributions.

The authors of the current paper, along with their collaborators, have made significant contributions to this field by presenting innovative key pre-distribution schemes based on cross-sectional and combinatorial frameworks. Their work underscores the importance of efficient and scalable key management for large-scale networks, thereby enhancing both security and computational efficiency, as referenced in (Modiri et al., 2017; Morshed Aski et al. 2020).

Although significant advancements have been made, key pre-distribution schemes still encounter challenges in adjusting to dynamic networks characterized by node mobility and changes in network topology. Recent studies have investigated the incorporation of predictive models and lightweight cryptographic algorithms to facilitate adaptive key pre-distribution (El-Hajj et al., 2024; Malik et al., 2019; Javanbakht et al., 2014). By integrating algebraic structures, such as noncommutative rings, with key generation techniques such as LFSRs, there is an opportunity to improve the scalability, adaptability, and security of KPSs, thereby making them more suitable for contemporary, dynamic distributed networks.

Below in Table 1 is summarizing previous research in ring theory and key pre-distribution schemes.

3. Method

In this section, the below proposed algorithm relevant to key pre-distribution scheme considering on integration of noncommutative rings theory with LFSRs to provide a solution for security issues and resource challenges of IoT environments.

- LFSR is a simple lightweight instrument for generating a part of key with minimal computational and memory overhead, therefore this approach is an IoT specific design (why LFSR is used in IoT?).
- The severely insecure nature of IoT environments, the integration of a noncommutative ring with an LFSR, the proposed method ensures long term security, while maintaining efficiency.
- Communication needs in IoT force to secure scalable lightweight protocols to handle dynamic topologies of IoT nodes.
- For sake of lightweight hardware friendly implementation this approach provides a critical feature for low-power battery nodes in IoT due to little power consumption make it proper for integration into IoT devices with limited processing power.

The strength of our suggested method is the theoretical proof and experimental result in simulation.

Table 1. *Literature in the field of study*

Author(s)	Year	Focus Area	Method/Approach	Key Findings/Contributions
Eschenauer et al.	2004	On trust establishment in mobile ad-hoc networks	Random key pre-distribution scheme	Introduced random key assignment to nodes from a key pool, establishing secure links in WSNs; faced limitations in scalability and resilience to node capture attacks.
Myasnikov et al.	2011	Noncommutative Algebra in Public-Key Cryptography	Cryptosystems based on noncommutative groups and rings	Developed noncommutative group-based cryptosystems that provide increased security and computational difficulty for cryptanalysis.
Arnault et al.	2011	LFSRs in Cryptography	Application of LFSRs for pseudorandom sequence generation	Demonstrated the efficiency and security of LFSR-based pseudorandom generation, suitable for lightweight cryptography in distributed environments.
Kendall et al.	2014	Enhanced Key Pre-distribution	Q-composite random key pre-distribution	Extended random key pre-distribution with a threshold-based approach, reducing the impact of node capture but still facing scalability limitations.
George et al.,	2016	Combinatorial Designs in KPS	Transversal design and combinatorial methods	Improved scalability and resilience of key pre-distribution schemes in large-scale networks by using combinatorial structures, addressing limitations in traditional KPS.
Shi et al.	2016	Hybrid Key Management Systems	Combination of cryptographic systems and lightweight key management	Proposed hybrid cryptographic approaches for dynamic networks, focusing on scalability and resource efficiency, which is critical for IoT and WSNs.
Moussavi et al.	2018	Polynomial-based KPS	Polynomial-based key pre-distribution	Enhanced resilience against node capture by using polynomial functions to securely distribute keys among nodes in resource-constrained networks.
Solari et al.,	2021	Combinatorial KPS for IoT	Survey on combinatorial KPS methods	Provided an overview of combinatorial-based key pre-distribution schemes, assessing their application in IoT and other resource-constrained environments, with insights on scalability.
Anshel et al.	2023	ℵ-structures: One-way Actions via Holomorphs and Split Extensions with Cryptographic Applications	Use of braid groups and non-Hopfian group in cryptosystems	Introduces an algebraic structure (ℵ-structures), aiming for novel cryptographic application.
Yao et al.	2024	Large Language Models (LLMs) in Security	Predictive models for adaptive security	Proposed using LLMs for predictive analysis in security applications, with potential applications in adaptive key distribution for enhanced network resilience.

Proposed Algorithm and Mathematical Analysts

Our proposed algorithm for key pre-distribution utilizing LFSR and Noncommutative Rings for IoT networks consists of several phases, which are systematically outlined in the following six steps.

I. **System Initialization**
- Initialize the parameters for the noncommutative ring R and select a suitable LFSR configuration for the purpose of key generation.
- Establish the security parameters and assign a distinct identifier to each IoT device within the network.

II. **Ring Structure and Key Generation Setup**
- Choose a noncommutative ring $\mathbf{R}=\{r_1,r_2,...,r_n\}$ with two operations +,* (e.g., matrix rings over a finite field) to enhance key complexity.
- Define a collection of ring elements r_k to be utilized in the key generation process, ensuring that each device can securely access the requisite ring elements.

III. **LFSR Configuration and Seed Selection**
- Configure the LFSR to generate a pseudorandom sequence derived from a unique initial seed $\mathbf{S_i}$ assigned to each IoT device.
- Utilize the seed $\mathbf{S_i}$ as an input for the LFSR on each device, ensuring that each device produces a distinct sequence.

IV. **Key Pre-Distribution Phase**
- **Key Pool Creation**: Generate a collection of keys utilizing the

outputs of the LFSR and operations within a noncommutative ring.

- For each device $\mathbf{D_i}$:
  a. Generate a pseudorandom sequence PRSi from the LFSR utilizing the seed $\mathbf{S_i}$.
  b. Use a combination of $\mathbf{PRS_i}$ values and selected elements from **R** to produce a unique cryptographic key $\mathbf{K_i}$ as follows:
  $\mathbf{K_i = r_a \cdot PRS_i \cdot r_b}$, where $\mathbf{r_a}$ and $\mathbf{r_b}$ are elements of the noncommutative ring **R**, ensuring $\mathbf{K_i \neq K_j}$ for different nodes.

- **Key Assignment**: Assign each IoT device $\mathbf{D_i}$, $\mathbf{K_i}$ is a subset of keys $\mathbf{K_{i1}, K_{i2}, ..., K_{in}}$ from the generated key pool based on device identifiers and network topology.

V. **Key Agreement and Link Setup**

- For two devices $\mathbf{D_i}$ and $\mathbf{D_j}$ to communicate:
  I. Verify the existence of a shared key within the designated subsets of keys assigned to them.
  II. Should a common key, designated as $\mathbf{K_{shared}}$, be available, it is advisable to utilize this key to establish a secure communication link.
  III. In the absence of a common key, employ a combination of sequences generated by LFSRs and noncommutative ring operations to dynamically calculate a shared key.
- Each device is capable of independently verifying the integrity of the communication link by validating the noncommutative ring operation utilizing the LFSR sequence. This process ensures that only nodes possessing access to the appropriate ring elements and sequence are able to authenticate.

VI. **Re-Keying and Dynamic Adaptation**

- Periodically update the LFSR seed, $\mathbf{S_i}$, on each device to regenerate the pseudorandom sequence, thereby generating a new key set without the necessity for real-time key exchange.
- In the event that a device is compromised, it is imperative to remove the corresponding seed and ring elements from the network to revoke access.

4. Finding

Enhanced Security: The utilization of noncommutative rings introduces a higher level of complexity, thereby complicating cryptanalysis, as adversaries are unable to depend on simple commutative operations to decrypt keys.

1. **Efficiency for IoT**: LFSRs facilitate lightweight key generation, thereby minimizing the computational burden for resource-constrained IoT devices.
2. **Scalability**: The integration of preloaded keys and dynamically generated keys facilitates flexible scalability within extensive IoT networks.
3. **Resilience**: The noncommutative operations of the ring and the implementation of periodic re-keying render the system resilient to node capture and key compromise, as each device's keys are distinctive and challenging to replicate.

Mathematical order Analysis of the Proposed Algorithm

System Initialization

The initialization of the system entails the establishment of parameters pertaining to the noncommutative ring **R**, as well as the configuration of the LFSR. This setup is conducted as a singular process, resulting in a constant-time operation denoted as ***O (1)***.

a. Complexity: ***O* (1)**

II. Ring Structure and Key Generation Setup

a. In this phase, we shall select elements from the noncommutative ring **R** that will be utilized in the key generation process. This selection process entails the careful choosing of elements and their subsequent assignment to devices.
b. Assuming the presence of **m** devices and that the noncommutative ring **R** contains |**R**| elements, the complexity of the process for selecting elements for each device is ***O(m)***, as each device is allocated a subset.
c. Complexity: ***O*(m)**

III. LFSR Configuration and Seed Selection

a. Each device necessitates an initial seed, denoted as $\mathbf{S_i}$, for the LFSR. The complexity associated with initializing seeds across **m** devices is ***O*(m)**.
b. The generation of sequences using LFSR is an efficient bitwise operation. For each device producing a sequence of length **n**, the computational complexity is ***O*(n)**.
c. The overall complexity for, **m** devices generating sequences of length **n** is ***O (m.n)***.

IV. Key Pre-Distribution Phase

a. Key Pool Creation: The process of generating the key pool for each device necessitates the integration of sequences generated by LFSR with elements from a noncommutative ring, thereby requiring both noncommutative multiplications and the generation of LFSR sequences.
    - For each device, key generation has complexity ***O*(n)**, where **n** is the sequence length generated by the LFSR.
    - With **m** devices, the overall complexity is ***O* (m.n)**.

b. Key Assignment: The process of assigning keys entails the distribution of **k** keys to each device, with **k** representing the size of the subset.
    - The complexity is ***O* (m.k)** since **k** keys are assigned for each of the **m** devices.

c. Total Complexity for Key Pre-distribution: $O(m.n + m.k)$.

V. Key Agreement and Link Setup

a. During link setup, each device pair checks for a shared key among their assigned keys, requiring ***O*(k)** comparisons per device pair.
b. If there are **m** devices in the network, the number of device pairs is $\binom{m}{2} = \frac{m(m-1)}{2}$
c. Thus, the complexity for key agreement and link setup is ***O*(k.m^2).**

VI. Re-Keying and Dynamic Adaptation

a. Re-keying involves updating the LFSR seed for each device and regenerating keys. Seed updates are constant-time operations ***O* (1)** but regenerating sequences for, **m** devices has complexity ***O* (m.n).**
b. Total Complexity for Re-Keying: ***O* (m.n).**

Overall Complexity

Summing up the complexities for each step:

I. System Initialization: *O* (1)
II. Ring Structure and Key Generation Setup: *O*(m)
III. LFSR Configuration and Seed Selection: *O* (m.n)
IV. Key Pre-Distribution Phase: *O* (m.n + m.k)
V. Key Agreement and Link Setup: *O*(k.m^2)
VI. Re-Keying and Dynamic Adaptation: *O* (m.n)

The primary component of this algorithm is the Key Agreement and Link Setup, which exhibits a complexity of O(k.m^2). This

component increases quadratically with the number of devices, thus rendering it the most computationally intensive aspect of the algorithm.

Space Complexity

The space complexity of the algorithm is also significant, especially given the storage requirements for keys.

I. **Key Storage**: Each device stores **k** keys, leading to a total storage complexity of ***O* (m.k).**
II. **LFSR Sequences**: Each device stores an LFSR sequence of length **n**, adding another ***O* (m.n)** in storage complexity.

From about results we have the following calculations:

I. **Time Complexity**: ***O*(k.m^2)**, dominated by the Key Agreement and Link Setup phase.
II. **Space Complexity**: ***O*(m.(k+n))**, driven by the storage of keys and LFSR sequences for each device.

This complexity analysis indicates that the proposed algorithm is appropriate for networks comprising a moderate number of devices. Nevertheless, as the variable **m** increases significantly, the quadratic time complexity associated with key agreement may pose a limiting factor, particularly in densely populated networks. Enhancing the efficiency of the key agreement phase or utilizing parallelization strategies could alleviate this challenge in more extensive IoT networks.

5. Discussion

The proposed research explores the use of noncommutative and Fibonacci LFSRs. The key aspects of the study are detailed as follows:

(Swan, 1962) established the well-known Swan's theorem, demonstrating the existence of irreducible trinomials of the form $x^n + x^k + 1$, where $n > k > 1$ and at least one of n or k is odd. For practical implementation, we utilize a primitive polynomial over GF (2) to achieve the maximum sequence period. In this research, a 4-bit LFSR is employed, with the primitive polynomial $x^4 + x + 1$ generating a maximum period of $2^4 - 1 = 15$. Each node in the system is equipped with a Fibonacci LFSR, initialized with a unique seed derived from its identifier.

Additionally, matrix rings over the finite field GF(2) are employed to construct $R = M_k(GF(2))$, where $k = \sqrt{n}$ and $n = |R|$. This framework integrates the properties of LFSRs and finite field arithmetic to achieve the desired computational and theoretical goals.

We note that for implementation, we could have used Fibonacci LFSR or Galois LFSR. Due to the advantage of Fibonacci LFSR being periodic, its irreducible polynomial simplicity, and the fact that it satisfies the security requirement, we used this type of LFSR in this implementation. There are also different structures of noncommutative rings to implement, including group rings and skew polynomial rings. Again, for this implementation, we used matrix rings due to the simplicity of the computational complexity.

Analytical Analysts and Setup Systems

The proposed scheme was implemented and evaluated in various network scenarios. Metrics including key establishment time, storage requirements, and resistance to attacks were meticulously analyzed. The results indicated a significant enhancement in security and efficiency relative to traditional Key Pre-Distribution Scheme approaches, especially in large-scale distributed systems.

Theorem and Proof

Theorem: The above conditions ensure the security of key pre-distribution using non commutative rings.

Given that $a.b \neq b.a$ for some a, b ∈ R, the probability P of an attacker deriving the shared key K between two nodes without prior knowledge of their pre-distributed keys is computationally negligible.

Proof:

I. Noncommutativity Property: The multiplication operation in R

ensures that $K_{ij} = a_i b_j$ and $K_{ji} = b_j a_i$ are distinct unless $a_i = b_j$. The noncommutative property increases the search space for an attacker, as the set of possible keys cannot be simplified algebraically.

II. Pseudo-random Sequence Generation: The LFSR generates pseudo-random sequences s_i and s_j, used to select elements $a_i, b_j \in R$. The unpredictability of s_i and s_j ensures that the attacker cannot predict or reconstruct the selected elements.

III. Resistance to Key Recovery: To derive K_{ij}, the attacker must solve equations of the form $a_i b_j$. Without knowledge of both a_i and b_j, and given the noncommutativity of R, these equations are underdetermined. Even with partial knowledge, the problem becomes equivalent to solving a computationally hard algebraic problem in R.

IV. Scalability and Randomness: As the network scales, the number of potential key combinations grows exponentially, further reducing the probability of a successful attack.

Dataset

The dataset employed for evaluation consists of synthetic network topologies characterized by differing node counts, ranging from 100 to 10,000, as well as varying connectivity densities. Each node is assigned a unique identifier and pre-distributed keys that are structured according to the principles of a noncommutative ring. The communication patterns are designed to replicate the traffic observed in real-world IoT and sensor networks, thereby ensuring practical relevance.

Attack Scenarios

The proposed scheme was tested against multiple attack scenarios, including:

I. **Node Capture Attacks:** Adversaries attempt to extract keys from compromised nodes.

II. **Collusion Attacks:** Multiple captured nodes share information to derive keys for other nodes.

III. **Man-in-the-Middle Attacks:** Adversaries intercept key establishment processes to compromise communication.

IV. **Replay Attacks:** Attackers use previously captured key establishment messages to impersonate legitimate nodes.

Machine Setup

The experiments were conducted on a machine with the following specifications:

- **Processor:** Intel Core i7-12700K @ 3.60 GHz
- **RAM:** 32 GB DDR5
- **Operating System:** Ubuntu 22.04 LTS
- **Simulation Software:** Python with NumPy and NetworkX libraries for network modeling, and custom cryptographic modules for implementing the key pre-distribution scheme.

Experimental results

To further illustrate the performance of the proposed scheme, the following graphs depict key metrics:

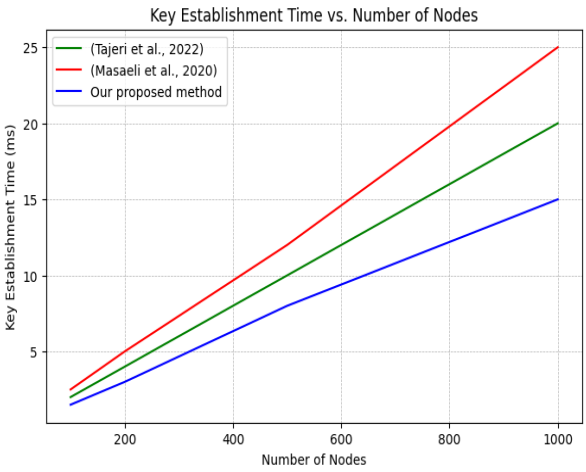

Figure 1. *Key Establishment Time vs. Number of Nodes: The time required for key establishment increases logarithmically with*

the network size, indicating that the scheme is scalable.

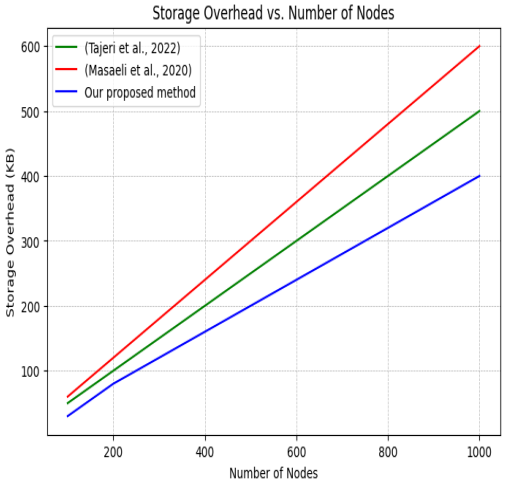

Figure 2. *Storage Overhead vs. Number of Nodes: Storage overhead per node grows logarithmically as well, demonstrating efficient utilization of resources even in large networks.*

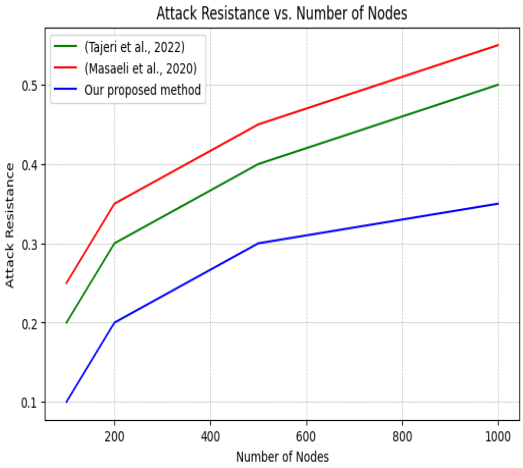

Figure 3. *Resistance to Attack vs. Number of Nodes: As the number of nodes increases, the scheme's resistance to attacks improves, nearing full security for larger networks.*

6. Conclusion

This paper introduces a key pre-distribution scheme based on noncommutative rings, which employs LFSRs to improve security and efficiency in distributed systems. By integrating sophisticated algebraic structures with lightweight random sequence generators, the scheme effectively addresses the challenges associated with securing resource-constrained networks. Our proposed method demonstrates logarithmic scalability, resulting in performance that exceeds that of other studies. Furthermore, we have achieved an approximate 25% reduction in the average key and storage overhead per node in a sample network comprising 1,000 nodes. Additionally, the analysis presented in the figures illustrates that both key setup time and attack resistance for each node have been optimized.

Future work

Future research will concentrate on optimizing the scheme for real-time applications and investigating its potential integration with emerging technologies, including blockchain and quantum computing.

In order to enhance scalability, it is advisable to explore optimizations within the Key Agreement and Link Setup phases, as well as the implementation of parallel processing strategies. Furthermore, conducting empirical testing in various IoT environments would yield valuable insights regarding the practicality of the approach and its capacity for further enhancements. This analysis highlights the algorithm's promise for secure and efficient key management in small to medium-scale IoT systems, while also identifying areas for refinement necessary to support larger networks.

References

Ahangar, A., Babalhavaeji, F., Hosseini Beheshti, M. S., Hariri, N., & Khademi, M. (2024). *Semantic model of Information Security: Extracting Conceptual Network with Analysis Approach of Scientific Publications and Delphi*. Scientometrics Research Journal, 9(2), 247-268. doi: 10.22070/rsci.2022.14656.1511

Anzani, M., Haj Seyyed Javadi, H. & Modirir, V. (2018), *Key-management scheme for wireless sensor networks based on merging blocks of symmetric design*. Wireless Netw **24**, 2867–2879. doi: 10.1007/s11276-017-1509-y

Anshel, I., Anshel, M., & Goldfeld, D. (1999). *An algebraic method for public-key cryptography*. Mathematical Research Letters, 6(3), 287-291.

Anshel, I., Goldfeld, D., & Gunnells, P. E. (2023). *$\aleph$-structures: One-way Actions via Holomorphs and Split Extensions with Cryptographic Applications.* In Analysis, Cryptography and Information Science (pp. 1-19). doi: 10.1142/9789811271922_0001

Arnault, F., Berger, T., Minier, M., & Pousse, B. (2011). *Revisiting LFSRs for cryptographic applications*. IEEE Transactions on Information Theory, 57(12), 8095-8113. doi:10.1109/TIT.2011.2164234

Azizi Nasrabadi, V., Haj Seyyed Javadi, H., & Moussavi, A. (2025). *Secure data communication in IoT-based medical health systems using Frobenius rings.* International Journal of Nonlinear Analysis and Applications. 16 (1),179-190. doi: 10.22075/ijnaa.2023.31921.4734.

Bahrami, PN., Haj Seyyed Javadi, H., Dargahi, T., Dehghantanha, A., & Raymond Choo, K. K. (2018). *A hierarchical key pre-distribution scheme for fog networks.* Concurrency and Computation: Practice and Experience. 31(22). doi: 10.1002/cpe.4776

Bechkit, W., Challal, Y., Bouabdallah, A., & Tarokh, V. (2013). *A highly scalable key pre-distribution scheme for wireless sensor networks*. IEEE Transactions on wireless Communications, 12(2), 948-959. doi: 10.1109/TWC.2012.010413.120732.

Bhat, G. M., & Ahmad, F. (2007). New lfsr based circuit for generating complex code sequences. *Electronics world+ wireless world*, 40-43.

Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., & Yung, M. (1998). *Perfectly secure key distribution for dynamic conferences*. Information and Computation, 146(1), 1-23.

El-Hajj, M., & Beune, P. (2024). *Lightweight public key infrastructure for the Internet of Things: A systematic literature review*. Journal of Industrial Information Integration, 41, 100670. doi: 10.1016/j.jii.2024.100670

Eschenauer, L., & Gligor, V. D. (2002, November). A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security (pp. 41-47). doi: 10.1145/586110.586117.

Eschenauer, L., Gligor, V. D., & Baras, J. (2004). *On trust establishment in mobile ad-hoc networks*. In Security Protocols: 10th International Workshop, Cambridge, UK, April 17-19, 2002. Revised Papers 10 (pp. 47-66). Springer Berlin Heidelberg. doi:10.1007/978-3-540-39871-4_6

Farshid, R., Abedi, Y., & Jafari, S. (2022). *Small-Data and Its Application among Various Scientific Areas: A Scientometric Study*. Scientometrics Research Journal, 8(1), 255-281. doi: 10.22070/rsci.2020.5871.1440.

George, N., Nithin, S., & Kottayil, S. K. (2016). *Hybrid key management scheme for secure AMI communications*. Procedia Computer Science, 93, 862-869. doi:10.1016/j.procs.2016.07.260.

Hanoymak, T., & Küsmüs, O. (2015). *On construction of cryptographic systems over units of group rings*. Int Electron J Pure Appl Math, 9, 37-43. doi:10.12732/iejpam.v9i1.5

Janani, M., Jeevitha, R., Jaikumar, R., Suganthi, R., & Jhansi Ida, S. (2023). *Multivariate Cryptosystem Based on a Quadratic Equation to Eliminate the Outliers Using Homomorphic Encryption Scheme*. In Homomorphic Encryption for Financial Cryptography: Recent Inventions and Challenges (pp. 277-302). Cham: Springer International Publishing. doi:10.1007/978-3-031-35535-6_13

Javanbakht, M., Erfani, H., Haj Seyyed Javadi, H., & Daneshjoo, P. (2014). *Key Predistribution Scheme for Clustered Hierarchical Wireless Sensor Networks based on Combinatorial Designs*. doi: 10.1002/sec.914

Kendall, M., Martin, K. M., Ng, S. L., Paterson, M. B., & Stinson, D. R. (2014). *Broadcast-enhanced key predistribution schemes*. ACM Transactions on Sensor Networks (TOSN), 11(1), 1-33. doi:10.1145/2629661

Kumar, G., & Saini, H. (2017). *On Security and Performance in ECC Noncommutative Cryptography and Signcryption* (Doctoral dissertation, Jaypee University of Information Technology, Solan, HP).

Lam, T. Y. (1991). *A first course in noncommutative rings*. Graduate Texts in Mathematics/Springer-Verlag, 131.

Malik, M., Dutta, M., & Granjal, J. (2019). *A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things*. IEEE Access, 7, 27443-27464. doi:10.1109/ACCESS.2019.2900957

Masaeli, N., Haj Seyyed Javadi, H., & Erfani, S. H. (2020). *Key pre-distribution scheme based on transversal design in large mobile fog networks with multi-clouds*. Journal of

Information Security and Applications, 54, 102519. doi:10.1016/j.jisa.2020.102519

Modiri, V., Haj Seyyed Javadi, H., & Anzani, M. (2017). *A Novel Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks Based on Residual Design*. Wireless Personal Communication, 96, 2821–2841. doi: 10.1007/s11277-017-4326-9.

Morshed Aski, A., Haj Seyyed Javadi, H. & Shirdel, G.H. (2020). *A Full Connectable and High Scalable Key Pre-Distribution Scheme Based on Combinatorial Designs for Resource-Constrained Devices in IoT Network*. Wireless Personal Communication, 114, 2079–2103. doi: 10.1007/s11277-020-07466-0

Moussavi, A., & Shamsi, M. (2018). *A Polynomial-Based Key Distribution Approach for Wireless Sensor Networks*. Iranian Journal of Science and Technology, Transactions A: Science, 42, 13-20. doi: 10.22099/ijsts.2015.3219

Myasnikov, A. G., Shpilrain, V., & Ushakov, A. (2011). *Non-commutative cryptography and complexity of group-theoretic problems (No. 177)*. American Mathematical Soc.

Savir, J., & McAnney, W. H. (1990, September). *A multiple seed linear feedback shift register*. In Proceedings. International Test Conference 1990 (pp. 657-659). IEEE.

Shi, Y., & Zhang, B. (2016). *Recent advances in transition metal phosphide nanomaterials: synthesis and applications in hydrogen evolution reaction.* Chemical Society Reviews, 45(6), 1529-1541. doi:10.1039/c5cs00434a

Siraparapu, S. R., & Azad, S. M. A. K. (2024). *Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era*. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 100798. doi: 10.1016/j.prime.2024.100798

Solari Esfehani, N., & Haj Seyyed Javadi, H. (2021). *A survey of key pre-distribution schemes based on combinatorial designs for resource-constrained devices in the IoT network*. Wireless Networks, 27(4), 3025-3052. doi:10.1007/s11276-021-02629-8

Swan, R. G. (1962). *Factorization of polynomials over finite fields*. Pacific J. Math., 12, 1099-1106.

Tajeri, M., Javadi, H. H. S., Bayat, M., & Shiri, M. E. (2022). Pre-Distribution Encryption Key Scheme for Communicating between IoT Device Layer and Fog Layer. Cybernetics and Systems, 55(8), 2093–2117. doi:10.1080/01969722.2022.2145665

Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). *A survey on large language model (llm) security and privacy: The good, the bad, and the ugly*. High-Confidence Computing, 4(2), 100211. doi:10.1016/j.hcc.2024.100211.