

An Efficient and Privacy Preserved Session Sharing for Unmanned Aerial Vehicle Communication Using Lattice Based Ring Signature Scheme

¹Hemalatha S, ²Sugirtha Thayalan, ³Sudha P, ⁴Medikonda Swapna and ⁵Tamilarasi Rajamani

¹School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, Tamil Nadu, India.

²Department of Computer Science and Engineering, Indian Institute of Information Technology (IIIT), Tiruchirappalli, Tamil Nadu, India.

³Presidency School of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India.

⁴Department of Computer Science of Engineering, Nitte Meenakshi Institute of Technology (NMIT), Nitte (Deemed to be University), Yelahanka, Bangalore, Karnataka, India.

⁵School Computer Science, Villa College, Male, Maldives.

¹lshemalatha@gmail.com, ²sugirthat@iiit.ac.in, ³sudha.p@presidencyuniversity.in, ⁴m.swapna@nmit.ac.in,

⁵tamilarasi.rajamani@villacollege.edu.mv

Correspondence should be addressed to Hemalatha S : lshemalatha@gmail.com

Article Info

Journal of Machine and Computing (<https://anapub.co.ke/journals/jmc/jmc.html>)

Doi : <https://doi.org/10.53759/7669/jmc202606017>

Received 19 May 2025; Revised from 18 September 2025; Accepted 13 October 2025.

Available online 21 October 2025.

©2026 The Authors. Published by AnaPub Publications.

This is an open access article under the CC BY-NC-ND license. (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

Abstract – Unmanned Aerial Vehicle (UAV) is playing an important role in various and diverse applications. UAV networks are designed with the support of efficient communication, secure, and privacy-preserved data exchange particularly for sensitive and mission-critical applications, like defensive surveillance, disaster response, civilian support, and smart city infrastructure. This paper presents an efficient and novel approach for establishing a secure session sharing in UAV networks through a Lattice-based Ring Signature Scheme (LRS). This paper presents a secure and privacy-preserved authentication scheme for large-scale UAV connection network using an Lattice-based Ring Signature Scheme. This technique offers a scalable and efficient solution for drone communication network. The proposed architecture incorporates a layered approach for establishing a strong connection between UAV devices and ground stations for ensuring streamlined data collection and processing. The proposed method has been designed with a strong ring signature scheme based on lattice cryptography. This technique is guaranty to achieve anonymity and authenticity by enabling any drone to sign data without exposing the signer's identity, thereby protecting device privacy. Ground controlling station and UAV operators can verified by using these signatures. The security analysis for the proposed ring signature scheme has been conducted through formal security analysis and this security analysis shows that the proposed scheme resilient to various attacks. The formal security analysis has been conducted by using formal security analysis with the help of game theory concepts by using correctness analysis, unforgeability, and unconditional anonymity. Performance analysis for the proposed technique has been conducted by using execution time analysis making it well-suited for resource-constrained devices, like UAV or Drones, supporting both scalability and security in real-world healthcare scenarios.

Keywords – Unmanned Aerial Vehicles, Session Sharing, Lattice, Ring Signature Scheme, Random Oracle Model, Cyber Defensive System.

I. INTRODUCTION

Accommodating Unmanned Aerial Vehicles (UAV) for various and diverse applications is increasing in a faster way. These applications are various from defensive border security system, civilian logistics, environmental monitoring, and disaster management. These applications are prompted with significant interest in the development of secure and reliable communication between drones. UAV devices are operated autonomously or in making coordination with ground control stations and nearby moving drones for exchanging of sensitive data over wireless channels. UAV networks are exposing

various array of cyber threats, which includes eavesdropping, spoofing, data manipulation, denial of service, and unauthorized access. Authentication techniques are taking important role for ensuring the integrity, confidentiality, and correctness of communication in entire UAV network. Authentication achieves secure and trusted communication between communicating parties by verifying the UAV identities. Traditional authentication methods are designed by using symmetric and public key infrastructure are providing efficient solution for many conventional networks. These techniques are suitable for UAV environments due to the limited on-board processing power. Moreover, UAVs often operated in an infrastructure less environments and providing a centralized authentication approaches is impractical. To address these challenges, researchers are proposing a variety of lightweight authentication techniques for UAV network, which includes identity-based authentication, challenge and response model, and certificate less digital sign verification model. Ring signature-based authentication technique has emerged as an efficient and robust solution for UAV network to achieve security and confidentiality. Ring signatures have been designed to allow a member of a group to sign a message on behalf of the group without revealing the actual identity of participating device in the signing process and this will achieve device or user anonymity.

This feature is particularly valuable in military or intelligence missions, where the concealment of a UAV's identity is crucial for operational security. When integrated with Lattice Based Cryptography (LBC), which offers high security with small key sizes and low computational requirements, ring signature schemes become especially well-suited for resource-constrained UAV platforms. Secure ring signature authentication techniques provide several advantages: they ensure message authenticity and integrity, protect the identity of the sender, and resist various attacks such as replay attacks, impersonation, and man-in-the-middle attacks. Moreover, these techniques support scalable and decentralized authentication, which is ideal for dynamic UAV swarms and networks with rapidly changing topologies. The ability of a UAV to authenticate itself anonymously while still maintaining traceability under certain conditions (e.g., via a trusted authority in case of misuse) offers a balanced trade-off between privacy and accountability. In recent implementations, ring signature schemes have also been enhanced with session key agreement mechanisms, enabling secure and private session sharing among UAVs without recurring to resource-intensive re-authentication processes. This is vital for mission continuity and real-time communication. Furthermore, these schemes often include features like forward secrecy, ensuring that the compromise of one session key does not affect the security of past or future communications. The increasing threat landscape faced by UAV networks, combined with the need for high-assurance, low-latency security protocols, makes the study and application of ring signature-based authentication techniques not only relevant but essential. This section provides a detailed introduction about the comprehensive understanding of specialized authentication in UAV networks and how secures ring signature schemes especially those based on lattice cryptography. Lattice based signature scheme represents a powerful and efficient tool for achieving robust, privacy-preserving authentication in various application. As UAV networks continue to scale and evolve, adopting such advanced cryptographic techniques will be key to ensuring secure autonomous operation, trustworthiness, and resilience against adversarial threats.

Research Objective

The primary objective of this the primary objective of this research is to develop an efficient and privacy-preserving session-sharing framework for Unmanned Aerial Vehicle (UAV) communication using a lattice-based ring signature scheme. The proposed system focused on to address the challenges of current session sharing methods particularly against quantum computing threats. This research is focusing on to design a lightweight lattice-based ring signature technique for ensuring indemnity anonymity, data integrity, and un-link ability among UAV sessions sharing. The proposed technique minimizes computational complexity and makes this is suitable for resource constrained UAV environment. Performance analysis for the proposed technique has been conducted in terms of computational complexity and execution time analysis with related ring signature technique.

Organization

The raining section of paper has been organized as follows, Section 2 provides a detailed review about lattice-based ring signature schemes with detailed comparison table by covering objective, key features, and limitations. A detailed working principle and system for the proposed lattice-based ring signature has been given in section 3. Section 4 provides a detailed formal security analysis for the proposed lattice-based ring signature technique with other related techniques is given in section 4. The computational complexity and execution time analysis for proposed signature technique with other signature techniques is given in section 5 with detailed evaluation. Conclusion with remarks and future direction for the secure session sharing in the UAV environment has been given in section 6.

II. RELATED WORK

Liu et al. [1] introduced an extended property known as link ability to the traditional ring signature scheme, resulting in the creation of linkable ring signature (LRS). This method retains the core attributes of standard ring signatures, such as correctness, unforgeability, and anonymity. However, LRS includes an additional feature that allows one to determine if two distinct signatures were generated by the same signer, enabling link ability. LRS proves valuable in scenarios demanding both anonymity and non-repeatability. For instance, within blockchain systems [2], if a user attempts to sign the same transaction twice, LRS helps the verifier detect this and reject the second signature, preventing the double-spending issue. In smart grid systems [3], where user electricity consumption data is automatically gathered via smart

meters, attackers could potentially infer the user's habits from this information. LRS can obscure the specific identity of the meter user while filtering redundant data, providing the system with the capability to monitor and track abnormal user behavior effectively

Liu et al. [4] developed an unconditional anonymous linkable ring signature (UALRS) scheme, which resolved the challenge that ring signatures (RS) could not simultaneously support both link ability and strong anonymity, thereby enhancing its security. RS schemes provide two forms of anonymity: computational and unconditional. Computational anonymity protects the signer's identity based on the difficulty of certain number-theoretic problems, meaning an adversary can compromise the anonymity if they solve the underlying problem. In contrast, unconditional anonymity ensures that even with unlimited computing power and time, an adversary has no better chance of identifying the actual signer than by random guessing. Specifically, if there are l participants in the RS scheme, the likelihood that an adversary correctly identifies the public key of the actual signer remains no greater than $\frac{1}{l}$, even with infinite computational resources

It is relatively straightforward to design a Ring Signature (RS) scheme that provides unconditional anonymity, as most conventional RS schemes can meet these requirements. However, constructing an Unconditional Anonymous Linkable Ring Signature (UALRS) scheme is considerably more challenging. The difficulty arises from two primary factors. First, in a Computational Anonymous Linkable Ring Signature (CALRS) scheme, the linking tag is often derived from a pseudorandom function tied to the signer's private key and based on a mathematical problem. However, unconditional anonymity assumes that an adversary has unlimited computational power, enabling them to solve any NP-hard problem, such as NTRU-SIS, integer factorization, discrete logarithms, or finding the preimage of a hash function. Therefore, relying solely on mathematical problems for the linking tag is insufficient, necessitating more sophisticated techniques.

Second, ensuring unconditional anonymity often complicates the generation and verification processes of the linking tag, potentially increasing the size of the public and private keys as well as the signatures, thereby reducing the scheme's computational efficiency. Notably, between 2004 and 2013, the only LRS scheme achieving unconditional anonymity was the one proposed by Liu et al. [4]

The aforementioned schemes are based on classical number theory problems, such as the discrete logarithm and large integer factorization challenges. However, the advent of quantum computing presents significant threats to cryptosystems relying on these classical problems. The operation of unmanned aerial vehicles within ad hoc networks and the cooperative interactions among vehicles in VANETs are extensively analyzed, with an emphasis on routing protocols and the detection of malicious vehicles [5]. Rezazadeh et al. [6] introduce a novel framework aimed at facilitating the reliable classification of verification schemes, grounded on seven distinct criteria. Zhang et al. [8] present a decentralized group authentication technique that operates without relying on a centralized certificate authority. In 1994, Shor [7] introduced a quantum algorithm capable of solving the large integer factorization problem in polynomial time under quantum computing, rendering many existing public key cryptosystems vulnerable to quantum attacks. Qin et al. [19] proposed a practical ring signature method of constant size, emphasizing its claims of unforgeability and user anonymity. However, Zhang et al. [8] demonstrated that Qin et al.'s scheme [19] is vulnerable to attacks compromising both unforgeability and user anonymity. Duong et al. [9] introduced a post-quantum blind ring signature approach, which is built on multivariate public key cryptography. In response, the study of post-quantum cryptography has gained traction within the cryptographic community. Among the potential alternatives, lattice-based cryptography has garnered considerable attention due to its efficiency, simplicity, parallelizability, and strong provable security features. In 2016, In 2017, Yang et al. [15] introduced a lattice-based LRS scheme employing weak pseudorandom functions, accumulators, and zero-knowledge proofs. In 2018, Baum et al. [10] and Alberto Torres et al. [11] proposed one-time LRS schemes based on the module-SIS and ring-SIS problems, respectively. Building on this, Zhang et al. [12] presented an LRS scheme over ideal lattices using homomorphic commitment and Σ -protocols, followed by Liu et al. [13] in 2019, who introduced a scheme supporting stealth addresses. In 2020, Beullens et al. [14] created a logarithmically scaling LRS scheme based on isogeny and lattice assumptions.

III. PROPOSED MODEL

This section discussed about the proposed lattice-based ring signature technique and this section contains four phases, like system initialization, key generation, signature generation, and verification phase. The system initialization phase is an initial stage for all the participating entities in the UAV device management. This phase has been initiated by the Center for Service Authority (CSA).

System Initialization

The participating UAV entities have to register with the any one of the ground control stations (GCS) with following basic attributes. The following security attributes are taking main role for constricting Lattice based ring signature. The following algorithm 1 provides a discussion about the steps involved in the system initialization phase based on the Assumption 1, *Assumption 1*: Let us assume that n number of entities are participating in the UAV devices management system, q is a larger prime number, and the positive integer m has been orient with $m \geq 7 \cdot n \cdot \log q$, $L = O(\sqrt{n \cdot \log q})$, and $\sigma = L \cdot \omega(\sqrt{\log n})$.

Algorithm 1: System Initialization

The center of CSA derives an approximate random distribution matrix $\mathbb{K} = A \in \mathbb{Z}_q^{n \times m}$ and this will be the master public key.

Select a basic key parameter $key \in \mathbb{Z}_q^{n \times m}$ from the known matrix A and this will satisfied condition of $\|key'\| \leq L$, given in the assumption 1

Two secure hash functions are selected over $\mathbb{Z}_q^{n \times m}$, these secure hash one way functions are defined as follows,

$$\mathcal{H}_1(\cdot) \rightarrow \{0,1\}^* \in \mathbb{Z}_q^{n \times m} \rightarrow (1)$$

$$\mathcal{H}_2: \mathbb{Z}_q \times M \times \mathbb{Z}_q^{n \times m} \rightarrow \mathbb{Z}_p^* \rightarrow (2)$$

Assign $\mathbb{M} = key \in \mathbb{Z}_q^{n \times m}$

Share the public attributes $\{A \in \mathbb{Z}_q^{n \times m}, \mathcal{H}_1, \mathcal{H}_2\}$

Key Generation

Each participating entity PE_i in UAV device management network has to generate unique and secure key pair $(S_{Key}^{K_i}, P_{Key}^{K_i})$ has been computed and agreed with center of CSA by using Algorithm 2. The steps involved in the key generation phase.

Algorithm 2: Key Generation

Select a random number $r_1 \in \mathbb{Z}_q$

The center of CSA computes $H_1^{D_i} = \mathcal{H}_1(r_1 || D_i) \in \mathbb{Z}_q^{n \times m}$

Compute the private key

$$S_{Key}^{K_i} = \text{Samplerpre}(A, key, H_1^{D_i}, \sigma) \in \mathbb{Z}_q^m \rightarrow (3)$$

Here $\sigma \geq \|key'\| \omega(\sqrt{\log m}, H_1^{D_i} \bmod q = A \cdot S_{Key}^{K_i}$, and $\|S_{Key}^{K_i}\| \leq \sigma \cdot \sqrt{m}$

The public key has been assigned with $P_{Key}^{K_i} = H_1^{D_i}$ for each participating entity

Signature Generation

Each communication between entities in the device network has been recorded by the Blockchain as signed message. The message $\mathcal{M}$ has been signed by using the private key of individual entity in the device network as follows.

Algorithm 3: Signature Generation

The signing entity selects a random number $m_1 \in \mathbb{D}_q^m$

Compute has value of $X = \mathcal{H}_2(A \cdot m_1, \mathcal{M})$

Compute $Y = S_{Key}^{K_i} \cdot X + m_1$

Check the probability of

$$\text{Min} \left(\frac{\mathfrak{D}_\sigma^m(X)}{\mathfrak{D}_{\mathcal{M}\sigma}^m(\mathbb{Z}_q^m)}, 1 \right) \rightarrow (4)$$

If it satisfies then the signed message is $\langle X, Y \rangle$, otherwise repeat from step 1.

Verification

The smart contract nodes and other participating entities are verifying the signed message as follows with the public attributes of $\{\mathcal{M}, A \in \mathbb{Z}_q^{n \times m}, \mathcal{H}_1, \mathcal{H}_2, \langle X, Y \rangle\}$ and public key $P_{Key}^{K_i}$. The signed message $\langle X, Y \rangle$ has been verified accordance with $\mathcal{M}$.

Algorithm 4: Verification

Check $\|X\| > L$, then reject the signature

Check $\|X\|_\infty > \frac{q}{4}$, then reject the signature

If $X = \mathcal{H}_2 \left((A \cdot Y - H_1^{D_i} \cdot X) \bmod q, \mathcal{M} \right)$, then accept the signature

Otherwise, reject the message

The proposed technique is more suitable for verification, authenticating, and traceability over the shared sensitive information.

Proposed Signature Verifications System Model

The signature verification model has been constructed with four fundamental algorithms with probabilistic polynomial time. This section discussed about the model setup for the proposed ring signature verification technique. This model has been designed with the assumption of Center for Service Authority (CSA) for key distribution Initial Setup, Initial security parameters for lattice based cryptographic defined by the CSA. Key Exchange Generate public and private key pairs for each participating user in the participation group signing process. Signature, the signer generates a signature $\mathcal{S}$ from the known private key and message $\mathcal{M}$. Verifier, the verification phase receives and verifies the signature generated by the signer and this will return either Accept or Reject. The working principle of the proposed secure and reliable framework for data sharing among the UAV devices has been illustrated as follows in **Fig 1**.

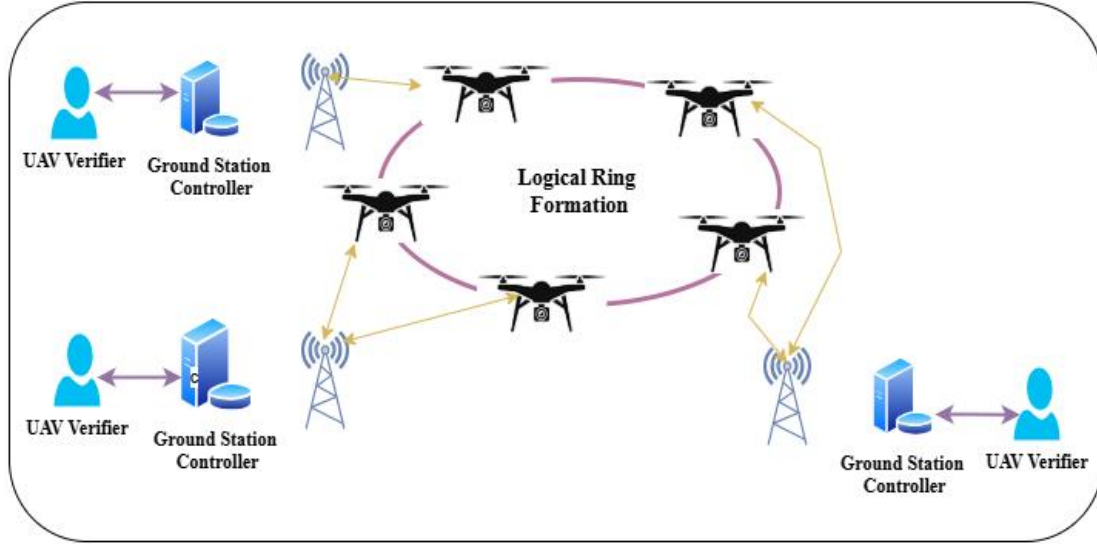


Fig 1. Logical Ring Formation by Connecting UAV Devices.

IV. SECURITY ANALYSIS

This section provides a detailed formal security analysis conducted for the proposed lattice-based ring signature method aimed at establishing a secure and reliable UAV device management over communication entities. The security analysis includes an examination of lattice-based ring signature properties such as correctness analysis, unforgeability analysis, and unconditional anonymity. This analysis has been conducted based on the game and verified model for ensuring the security and reliability.

Correctness Analysis

The integrity of the UAV related information shared between the communicating entities in a same transaction from each entity ED_i has to be checked by the verifier (algorithm 4). The following security analysis shows that the correctness for verifying the signature is upheld by the proposed ring signature method,

Verifier receives $\mathcal{S}_{ED_i} = \langle X_i, Y_i \rangle$ for $\forall i \in [1, \dots, n]$ and verifies as follows, according to the verification algorithm,

When the signature satisfies then conditions given in the algorithm 4, if the following verification holds (equation 10).

$$\mathcal{H}_2 \left((A \cdot Y - H_1^{D_i} \cdot X) \bmod q, \mathcal{M} \right) = Y = S_{Key}^{K_i} \cdot X + m_1 \quad (5)$$

According to the above given equation (11) has to prove,

$$A \cdot Y - H_1^{D_i} \cdot X \bmod q = A \cdot m_1 \bmod q \quad (6)$$

$$A \cdot Y - H_1^{D_i} \cdot X \bmod q = A \cdot (S_{Key}^{K_i} \cdot X + m_1) - H_1^{D_i} \cdot X \bmod q \quad (7)$$

$$\left. \begin{aligned} &A \cdot S_{Key}^{K_i} \cdot X + A \cdot m_1 - H_1^{D_i} \cdot X \bmod q \\ &H_1^{D_i} \cdot X + A \cdot m_1 - H_1^{D_i} \cdot X \bmod q \\ &(A \cdot m_1) \bmod q \end{aligned} \right\} \quad (8)$$

Substitute $H_1^{D_i} \cdot X + A \cdot m_1 - H_1^{D_i} \cdot X \bmod q$ and we can proof that $\forall i \in [1, \dots, n] \mathcal{H}_2 \left((A \cdot Y_i - H_1^{D_i} \cdot X_i) \bmod q, \mathcal{M} \right) = \mathcal{H}_2(A \cdot m_1, \mathcal{M})$

Unforgeability Analysis

Theorem 1: With the assumption of formal oracle model, the adversary $\mathcal{Adv}_{\mathcal{T}}$ choose a message $\mathcal{M}^*$ in game II to perform a forgery attack against entity ED_i . If there exists an efficient algorithm for computing Short Integer Solution (SIS) in polynomial time $\mathcal{T}$, then it shows that SIS hard problem can be broken with non-negligible amount of wining probability $\mathcal{P}_w^{\mathcal{T}}$. The proposed signature technique cannot be forged under the hardness of SIS problem.

Proof: The role of simulator $\mathcal{Q}_{\mathcal{S}}$ over an adversary model $\mathcal{Adv}_{\mathcal{T}}$ is defined as, to compute forged signature from the captured particular signature instance $\mathbb{S}_{ED_i} = \langle X_i, Y_i \rangle$. The adversary node tries to create a forged signature from the available information as follows,

Adversary utilizes received information $\mathbb{S}_{ED_i} = \langle X_i, Y_i \rangle$ for generating a valid signature $\mathbb{S}_{ED_i} = \langle X'_i, Y'_i \rangle$ for targeting entity of ED_i . The adversary node generates other valid signature $\mathbb{S}_{ED_i} = \langle X'_i, Y'_i \rangle$ for entity ED_i with the message of $\mathcal{M}'$. Here adversary entity utilizes the same selected $m_1 \in \mathcal{D}_q^m$. This has been computed as follows,

$$X'_i = \mathcal{H}_2 \left((A \cdot Y'_i - H_1^{D_i} \cdot X'_i) \bmod q, \mathcal{M}' \right) = \mathcal{H}_2 \left((A \cdot Y'_i - H_1^{D_i} \cdot X'_i) \bmod q, \mathcal{M}' \right) \quad (9)$$

This has been computed by using $\mathcal{H}_2(\cdot)$ and message $\mathcal{M}'$,

$$(A \cdot Y'_i - H_1^{D_i} \cdot X'_i) \bmod q = (A \cdot Y'_i - H_1^{D_i} \cdot X'_i) \bmod q \quad (10)$$

$$A \cdot (Y'_i - Y_i) = H_1^{D_i} \cdot (X'_i + X_i) \equiv 0 \bmod q \quad (11)$$

According to the assumption, $\|Y'_i\|$ and $\|Y''_i\| \leq \frac{q}{4}$ and $\|Y'_i - Y''_i\| \leq \frac{q}{2}$. It can derive a solution $\|Y'_i - Y''_i\| \leq \beta$ for all the instance of $\mathbb{Z} - \text{SIS}_{q,n,m,\beta}$ shown as follows,

$$A \cdot (Y'_i - Y_i) \equiv 0 \bmod q \quad (12)$$

According to the lattice assumptions mentioned in the derivations could not solve with current computing facilities and this shows that the hypothesis of the adversary is invalid. This proof shows that; an adversary entity can create forged valid signature with the probability of $\frac{1}{q \cdot \mathcal{H}_1 + q \cdot \mathcal{H}_2 + q \cdot p + q \cdot S}$. This probability value is very negligible. Hence, this proof shows that the proposed lattice-based ring signature technique can resist forgery attack for the illegal entities in UAV device management network.

Unconditional Anonymity

Theorem 2: In the proposed lattice-based ring signature method, the signer has to satisfy the unconditional anonymity. For any efficient polynomial time computing algorithm $\mathcal{O}$ for participant from $ED_{\tau}, \tau \in [1, \dots, n]$ and $P_{Key}^{\mathcal{D}_{\tau}} \in P_{List}$, has the wining probability of $\Pr \left[P_{Key}^{\mathcal{D}_{\tau}} = P_{Key}^{\mathcal{D}_{\tau}^*} \right]$ is always $\frac{1}{2} = 0.5$, from the signature $\mathbb{S}_{ED_{\tau}} = \langle X_{\tau}, Y_{\tau} \rangle i \in [1, \dots, n]$ created by the participating entity D_{τ} .

Proof: The signature generated by the signing entity ED_{τ} cannot be viewed by any other third party until the verifier has opened all the information. In the proposed lattice-based ring signature method, $\mathbb{S}_{D_{\tau}}$ is computed by the entity ED_{τ} through randomly selected $m_1 \in \mathcal{D}_q^m$. Therefore, the signature $\mathbb{S}_{D_{\tau}}$ is uniformly distributed in $\mathcal{D}_q^m$. The probability of winning chance for the success in guessing of real signer is at most of $\frac{1}{((n \times m) + 1)} \cong 0$ for non-member from the lattice-based ring signature group. The probability of success in guessing of real signer is at most $\frac{1}{(n \times m)}$ for member from the ring signature group. With this negligible probability, the proposed lattice-based ring signature scheme satisfies unconditional anonymity.

Traceability

The digital signature technique is playing an important role for protecting IoT based network applications to achieve secure and reliable data sharing among communicating IoT devices. This section discussed about the success of achieving traceability in data sharing process in UAV device management network.

In a common scenario, traceability can identify the unauthorized entry in signature verification mechanism guarantees the traceability of UAV collected information sharing with other coordination entities. The unauthorized opening the

corresponding signature when some security incident occurs will be traced. The Blockchain technology ensures an immutable public ledger for the records of UAV related data storage and operational processes, which ensures traceability of data sharing in different UAV device networks. Any dispute occurs, it can be easily identified by the record verifiers

V. EFFICIENCY ANALYSIS

This section presents a comprehensive comparison of the proposed lattice-based signature technique against other related signature schemes. The subsequent section offers an in-depth analysis of both computational and communication costs. For implementation, basic functions were developed using the Java Pairing-Based Cryptography (JPBC) library, with experiments conducted on a 14th Gen Intel® Core™ i5-13400 CPU and 32GB RAM. **Fig 2** shows execution time analysis with 128 lattice key size.

The following **Table 1** summarizes the computational complexity of the proposed lattice-based ring signature in comparison to other signature schemes, considering varying ring and lattice sizes. Complexity measurements are expressed using Big-O notation. All analysed schemes assume linear complexity in both signing and verification operations relative to the ring size, which is standard for lattice-based ring signature schemes (RSS). Notably, Peng et al. Approach minimizes key generation costs by eliminating the need for trapdoors, while Wang et al. [20] scheme incurs additional computational overhead due to the inclusion of both encryption and decryption steps required for the sign crypton process. Liu et al. [18] method introduces lightweight stealth address processing, and Yang et al. scheme achieves the lowest overall costs by adaptively tuning parameters based on vehicular speed requirements. Deng et al. [16] solution incorporates traceability features while maintaining minimal complexity overhead.

Table 1. Time Complexity Analysis for the Lattice Based Ring Signature Scheme

Ring Signature Technique	Key Generation	Signing	Verification
Liu et al. (2019) [13]	$O(n.d)$	$O(n.d)$	$O(n.d)$
Deng et al. (2024) [16]	$O(d.\log q)$	$O(n.d)$	$O(n.d)$
Peng et al. (2022)	$O(d)$	$O(n.d)$	$O(n.d)$
Wang et al. (2023) [20]	$O(d)$	$O(n.d) + C_{Encry}$	$O(n.d) + C_{Decry}$
Yang et al. (2022)	$O(d)$	$O(n.d)$	$O(n.d)$
Jiang et al. (2024) [18]	$O(d)$	$O(n.d)$	$O(n.d)$
Proposed scheme	$O(d)$	$O(n.d)$	$O(n.d)$

Table 2. Execution Time Analysis With 128 Bits Key Size

Lattice based RSS	Key Generation (Msec)	Signing (Msec)	Verification (Msec)	Total Cost
Liu et al. [13]	≈ 236	≈ 214	≈ 189	≈ 403
Peng et al.	≈ 215	≈ 255	≈ 221	≈ 476
Wang et al. [20]	≈ 286	≈ 333	≈ 239	≈ 572
Yang et al.	≈ 207	≈ 275	≈ 211	≈ 486
Deng et al. [16]	≈ 216	≈ 221	≈ 209	≈ 403
Jiang et al. [18]	≈ 198	≈ 231	≈ 204	≈ 486
Proposed scheme	≈ 168	≈ 202	≈ 197	≈ 397

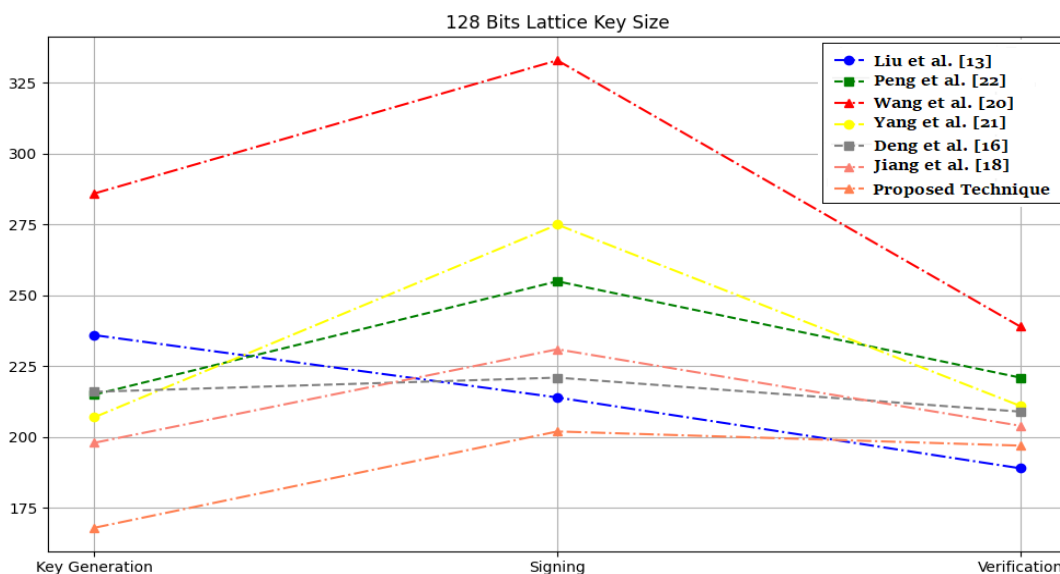


Fig 2. Execution Time Analysis with 128 Lattice Key Size.

Table 2 shows the execution time analysis with 128 bits for the lattice-based ring signature schemes with proposed lattice-based RSS technique. The above result shows that the Wang et al. incur more computational power due to the involvement of encryption process for achieving message integrity. Remaining schemes are nearly close to each other schemes for taking execution time to complete signing and verification process. Following **Table 3** and **4** shows the result analysis with different key size from 256 bits and 512 bits. **Fig 3** shows execution time analysis with 256 lattice key size. **Fig 4** represents execution time analysis with 512 lattice key size.

Table 3. Execution time Analysis with 256 bits key size

Lattice based RSS	Key Generation (Msec)	Signing (Msec)	Verification (Msec)	Total Cost
Liu et al. [13]	≈ 321	≈ 311	≈ 257	≈ 568
Peng et al. [17]	≈ 300	≈ 352	≈ 289	≈ 541
Wang et al. [20]	≈ 371	≈ 430	≈ 307	≈ 737
Yang et al.	≈ 292	≈ 372	≈ 279	≈ 651
Deng et al. [16]	≈ 301	≈ 318	≈ 277	≈ 595
Jiang et al. [18]	≈ 283	≈ 328	≈ 272	≈ 600
Proposed scheme	≈ 253	≈ 299	≈ 265	≈ 564

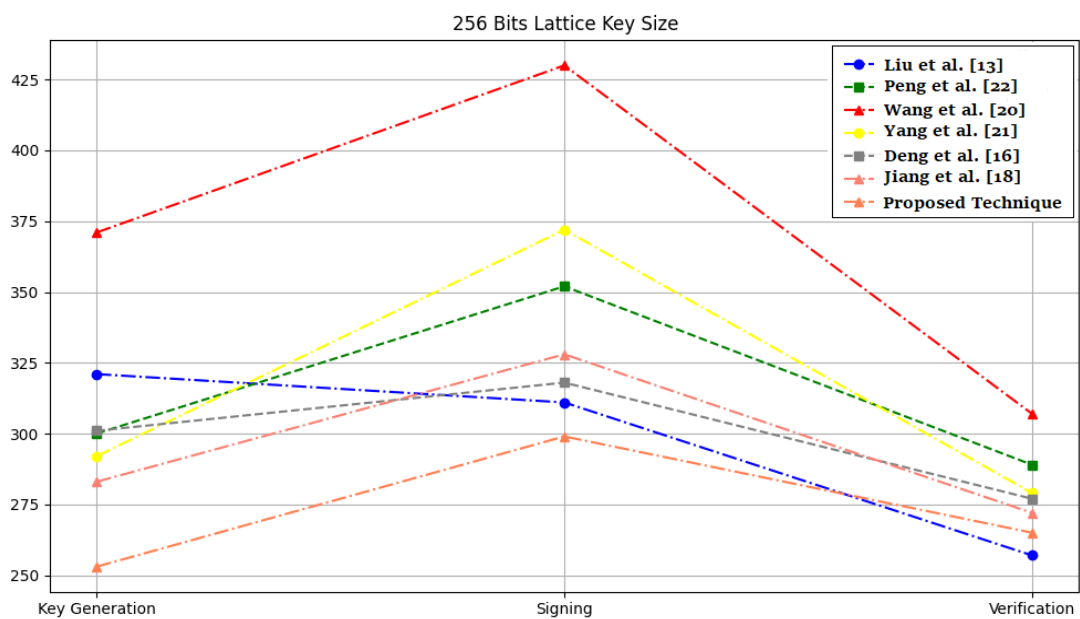


Fig 3. Execution Time Analysis with 256 Lattice Key Size.

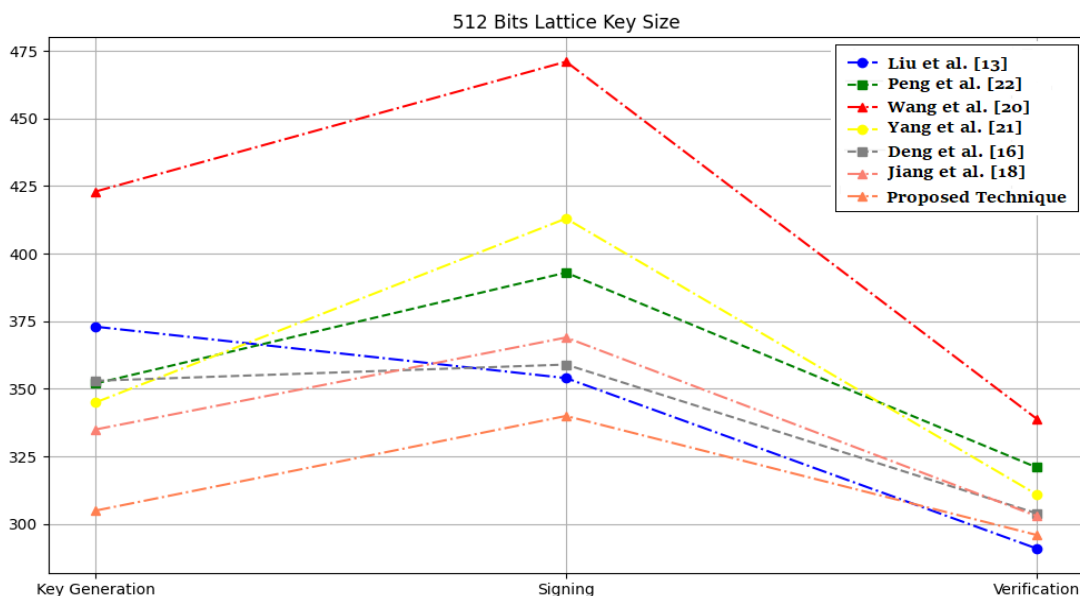


Fig 4. Execution Time Analysis with 512 Lattice Key Size.

Table 4. Execution Time Analysis With 512 Bits Key Size

Lattice based RSS	Key Generation (Msec)	Signing (Msec)	Verification (Msec)	Total Cost
Liu et al. [13]	≈ 373	≈ 354	≈ 291	≈ 645
Peng et al.	≈ 352	≈ 393	≈ 321	≈ 714
Wang et al. [20]	≈ 423	≈ 471	≈ 339	≈ 810
Yang et al.	≈ 345	≈ 413	≈ 311	≈ 724
Deng et al. [16]	≈ 353	≈ 359	≈ 304	≈ 663
Jiang et al. [18]	≈ 335	≈ 369	≈ 303	≈ 672
Proposed scheme	≈ 305	≈ 340	≈ 296	≈ 636

VI. CONCLUSION

Lattice based signature scheme can protect the communication link and commands in the UAV networks. UAV networks are supporting for establishing efficient communication, secure, and privacy-preserved data exchange particularly for sensitive and mission-critical applications. This paper presents an efficient and novel approach for establishing a secure session sharing in UAV networks through a Lattice-based Ring Signature Scheme (LRS). This paper presents a secure and privacy-preserved authentication scheme for large-scale UAV connection network using Lattice-based Ring Signature Scheme. Formal security analysis shows that the proposed technique achieves anonymity and un-link ability among the devices in UAV network. The proposed technique requires minimum computational complexity and reduces 47 % of execution time compare to other lattice-based ring signature techniques, which is more suitable for light weight device like UAV.

Future direction for this research is to focus on to reduce the computation complexity further in UAV network, by introducing decentralization mechanism for authentication verification through ground control station. An efficient abstract based proxy signature technique can be designed for maintaining anonymity with minimum computational cot. The proposed technique has been evaluated through simulated environment and this can be extended to real-time environment for taking execution tie evaluation in the future research.

CRedit Author Statement

The authors confirm contribution to the paper as follows:

Conceptualization: Hemalatha S, Sugirtha Thayalan, Sudha P, Medikonda Swapna and Tamilarasi Rajamani;

Methodology: Hemalatha S, Sugirtha Thayalan and Sudha P; **Software:** Medikonda Swapna and Tamilarasi Rajamani;

Data Curation: Hemalatha S, Sugirtha Thayalan and Sudha P; **Writing-Original Draft Preparation:** Hemalatha S,

Sugirtha Thayalan, Sudha P, Medikonda Swapna and Tamilarasi Rajamani; **Visualization:** Hemalatha S, Sugirtha

Thayalan and Sudha P; **Investigation:** Medikonda Swapna and Tamilarasi Rajamani; **Supervision:** Hemalatha S, Sugirtha

Thayalan and Sudha P; **Validation:** Medikonda Swapna and Tamilarasi Rajamani; **Writing- Reviewing and Editing:**

Hemalatha S, Sugirtha Thayalan, Sudha P, Medikonda Swapna and Tamilarasi Rajamani; All authors reviewed the results and approved the final version of the manuscript.

Data Availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Conflicts of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests

The authors declare no conflict of interest.

Reference

- [1]. J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups," *Information Security and Privacy*, pp. 325–335, 2004, doi: 10.1007/978-3-540-27800-9_28.
- [2]. X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A Blockchain Privacy Protection Scheme Based on Ring Signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020, doi: 10.1109/access.2020.2987831.
- [3]. F. Tang, J. Pang, K. Cheng, and Q. Gong, "Multiauthority Traceable Ring Signature Scheme for Smart Grid Based on Blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/5566430.
- [4]. J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable Ring Signature with Unconditional Anonymity," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 1, pp. 157–165, Jan. 2014, doi: 10.1109/tkde.2013.17.
- [5]. T. Ta et al., "Efficient Unique Ring Signature for Blockchain Privacy Protection," *Information Security and Privacy*, pp. 391–407, 2021, doi: 10.1007/978-3-030-90567-5_20.
- [6]. M. A. Rezazadeh Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, "Authentication strategies in vehicular communications: a taxonomy and framework," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, May 2021, doi: 10.1186/s13638-021-01968-6.

- [7]. P. W. Shor, “Polynomial time algorithms for discrete logarithms and factoring on a quantum computer,” *Algorithmic Number Theory*, pp. 289–289, 1994, doi: 10.1007/3-540-58691-1_68.
- [8]. Zhang, J., Bai, W., & Jiang, Z. (2020). On the security of a practical constant-size ring signature scheme. *International Journal of Network Security*, 22(3), 394–398.
- [9]. D. Hoang Duong, W. Susilo, and H. T. N. Tran, “A Multivariate Blind Ring Signature Scheme,” *The Computer Journal*, vol. 63, no. 8, pp. 1194–1202, Nov. 2019, doi: 10.1093/comjnl/bxz128.
- [10]. C. Baum, H. Lin, and S. Oechsner, “Towards Practical Lattice-Based One-Time Linkable Ring Signatures,” *Information and Communications Security*, pp. 303–322, 2018, doi: 10.1007/978-3-030-01950-1_18.
- [11]. W. A. Alberto Torres et al., “Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0),” *Information Security and Privacy*, pp. 558–576, 2018, doi: 10.1007/978-3-319-93638-3_32.
- [12]. H. Zhang, F. Zhang, H. Tian, and M. H. Au, “Anonymous Post-Quantum Cryptocash,” *Financial Cryptography and Data Security*, pp. 461–479, 2018, doi: 10.1007/978-3-662-58387-6_25.
- [13]. Z. Liu, K. Nguyen, G. Yang, H. Wang, and D. S. Wong, “A Lattice-Based Linkable Ring Signature Supporting Stealth Addresses,” *Computer Security – ESORICS 2019*, pp. 726–746, 2019, doi: 10.1007/978-3-030-29959-0_35.
- [14]. W. Beullens, S. Katsumata, and F. Pintore, “Calamari and Falafel: Logarithmic (Linkable) Ring Signatures from Isogenies and Lattices,” *Advances in Cryptology – ASIACRYPT 2020*, pp. 464–492, 2020, doi: 10.1007/978-3-030-64834-3_16.
- [15]. S. Bouakkaz and F. Semchedine, “A certificateless ring signature scheme with batch verification for applications in VANET,” *Journal of Information Security and Applications*, vol. 55, p. 102669, Dec. 2020, doi: 10.1016/j.jisa.2020.102669.
- [16]. J. Liang, J. Huang, Q. Huang, L. Lan, and M. H. A. Au, “A Lattice-Based Certificateless Traceable Ring Signature Scheme,” *Information*, vol. 14, no. 3, p. 160, Mar. 2023, doi: 10.3390/info14030160.
- [17]. Z. Zhao, C. Hsu, L. Harn, Z. Xia, X. Jiang, and L. Liu, “Lightweight ring-neighbor-based user authentication and group-key agreement for internet of drones,” *Cybersecurity*, vol. 7, no. 1, Aug. 2024, doi: 10.1186/s42400-024-00247-3.
- [18]. H. Yu and Z. Lv, “Lattice-based ring signcryption for consortium blockchain,” *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, p. 101602, Jul. 2023, doi: 10.1016/j.jksuci.2023.101602.
- [19]. Yang, G., Liu, Z., Wong, D. S., Wang, H., & Zhang, F. (2022). Anti-quantum lattice-based ring signature scheme and applications in VANETs. *Cluster Computing*, 25, 2177–2191. <https://doi.org/10.1007/s10586-021-03529-4>
- [20]. Peng, X., Guo, Y., & Wang, Z. (2022). Efficient lattice-based ring signature scheme without trapdoors for machine learning. *Journal of Low Power Electronics and Applications*, 12(3), Article 61. <https://doi.org/10.3390/jlpea12030061>

Publisher’s note: The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The content is solely the responsibility of the authors and does not necessarily reflect the views of the publisher.