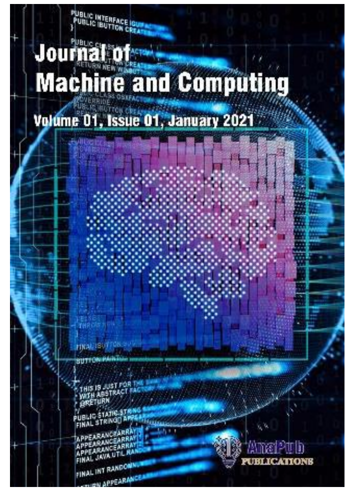
Journal Pre-proof

Advancing Security and Scalability: A Protocol Extension for Dynamic Group Membership Management



Renisha P S and Bhawana Rudra

DOI: 10.53759/7669/jmc202505151

Reference: JMC202505151

Journal: Journal of Machine and Computing.

Received 12 April 2025

Revised from 30 May 2025

Accepted 19 June 2025

Advancing Security and Scalability: A Protocol Extension for Dynamic Group Membership Management

[1] **Renisha.P.S***, [2] **Bhawana Rudra**

[1,2] Department of Information Technology, National Institute of Technology, Karnataka Surathkal, India

renisha.227it501@nitk.edu.in, bhawanarudra@nitk.edu.in

*Corresponding Author: **Renisha.P.S**

Abstract

The integration of Contributory Group Key Agreement (CGKA) for group formation revolutionizes the collaborative process of generating group keys, instilling trust and fostering collaboration among group members. By ensuring that each member actively contributes to the generation of the group key, CGKA distributes the responsibility of key generation across the group, thereby enhancing the security and resilience of the group's cryptographic infrastructure. Concurrently, the utilization of Lattice Diffie-Hellman (LDH) for key generation leverages the mathematical properties of lattices to securely derive shared secret keys. LDH offers a robust and efficient method for generating keys in cryptographic applications, ensuring the confidentiality and integrity of communication channels. Furthermore, the incorporation of blockchain technology for implementing membership changes introduces a decentralized and transparent approach to managing group membership dynamics. By leveraging blockchain's distributed ledger technology and smart contracts, membership changes can be executed securely, transparently, and efficiently. This enhances the integrity and resilience of the group's membership management system, allowing for the secure addition and removal of members from the group while maintaining the integrity of the cryptographic infrastructure. Together, the integration of CGKA, LDH, and blockchain technology presents a comprehensive solution for advancing the security and scalability of dynamic group membership management protocols, offering a robust framework for secure and efficient communication in contemporary environments. Moreover, the proposed integration of CGKA, LDH, and blockchain technology facilitates seamless adaptation to dynamic changes in group membership, ensuring that security and scalability are maintained even as the composition of the group evolves. Through simulations and performance evaluations, the effectiveness of the integrated approach that is implemented in Python Software is demonstrated compared to existing protocols like Elliptic Curve Diffie-Hellman (ECDH), RSA Key Exchange, and Post-Quantum Cryptography (PQC).

Keywords: Contributory Group Key Agreement, Lattice Diffie-Hellman, Blockchain, Group Membership Management and Security

1. Introduction

Dynamic group membership management is a critical facet of contemporary communication and collaboration systems, particularly in the realm of distributed computing, cloud computing, and decentralized networks. In such environments, groups are not static entities; instead, they are subject to frequent changes in membership due to various factors such as user additions, departures, role changes, or system failures [1] [2]. Ensuring the seamless integration and operation of new members while maintaining the security and integrity of group communication channels poses significant challenges to system designers and administrators. The traditional approach to group membership management often involves centralized systems where a single authority is responsible for managing membership changes. However, such centralized systems are inherently limited in their scalability, fault tolerance, and susceptibility to single points of failure. Moreover, they may not be well-suited for distributed or decentralized environments where autonomy, resilience, and privacy are paramount. As a result, there has been a growing interest in developing decentralized and distributed protocols for dynamic group membership management.

In dynamic group membership management, the primary objective is to facilitate the seamless addition and removal of members from a group while preserving the security, confidentiality, and integrity of group communication [3] [4]. This involves not only managing access control and authentication mechanisms but also ensuring the robustness and resilience of cryptographic protocols used for key distribution, encryption, and authentication. Moreover, dynamic group membership management protocols must be capable of adapting to changing group dynamics in real-time without compromising security or performance [14] [15]. One of the key challenges in dynamic group membership management is achieving consensus among group members regarding membership changes while preventing unauthorized access or malicious activities [5] [6]. Traditional cryptographic techniques such as public-key infrastructure (PKI) or shared secret key schemes may not be sufficient to address these challenges, especially in large-scale distributed systems where the number of participants is constantly changing. Therefore, there is a need for innovative approaches that combine cryptographic primitives, distributed consensus algorithms, and decentralized governance mechanisms to ensure the security and scalability of dynamic group membership management protocols.

In recent years, advancements in blockchain technology, cryptographic primitives such as threshold signatures and multi-party computation, and distributed consensus algorithms have paved the way for new approaches to dynamic group membership management [16][17]. These approaches leverage the inherent properties of blockchain, such as decentralization, transparency, and immutability, to securely manage group membership changes without relying on centralized authorities [18] [19]. Additionally, they utilize cryptographic techniques to ensure the confidentiality, integrity, and authenticity of group communication channels, even in the presence of malicious actors or network disruptions. By harnessing the power of decentralized technologies and cryptographic primitives, dynamic group membership management protocols can provide robust, scalable, and secure solutions for modern distributed systems.

In the rapidly evolving landscape of digital communication, ensuring the security and scalability of group membership management protocols is paramount. As organizations increasingly rely on collaborative environments and distributed systems, the ability to manage dynamic changes in group membership while maintaining robust security measures becomes essential [7] [8]. This necessitates the development of innovative protocols and technologies that can address the challenges posed by dynamic group structures and evolving security threats. One of the fundamental aspects of group communication protocols is the establishment of secure communication channels among multiple parties [20] [18]. Traditionally, cryptographic protocols such as group key distribution schemes have been employed to facilitate secure communication within groups [19] [20]. However, existing protocols often face limitations in scalability and security when confronted with dynamic changes in group membership, such as the addition or removal of members. These limitations can undermine the confidentiality, integrity, and availability of group communication channels, posing significant challenges to the security of sensitive information and organizational operations.

To address these challenges, researchers and practitioners have explored novel approaches to dynamic group membership management, leveraging advancements in cryptography, distributed systems, and blockchain technology. One such approach is the integration of CGKA for group formation, which revolutionizes the collaborative process of generating group keys. By ensuring that each member actively contributes to the generation of the group key, CGKA fosters trust and collaboration within the group, enhancing the security and resilience of the group's cryptographic infrastructure. Additionally, the employment of LDH for key generation offers a robust and efficient method for securely deriving shared secret keys. LDH leverages the mathematical properties of lattices to generate keys, ensuring confidentiality and integrity in communication channels. This approach enhances the security of group communication protocols by providing a secure foundation for key generation, even in the presence of dynamic changes in group membership.

The integration of blockchain technology for implementing membership changes introduces a decentralized and transparent approach to managing group dynamics within distributed systems. By leveraging blockchain's distributed ledger technology and smart contracts, membership changes can be executed securely, transparently, and efficiently, enhancing the integrity and resilience of the group's membership management system. This enables secure addition and removal of members from the group, ensuring that the cryptographic infrastructure remains robust and scalable in dynamic group environments.

The key contributions of the article is,

- The integration of CGKA transforms the process of generating group keys by ensuring active participation from all members. This collaborative approach instills trust and fosters collaboration among group members, enhancing the overall security and resilience of the group's cryptographic infrastructure.
- Leveraging LDH for key generation provides a robust and efficient method for securely deriving shared secret keys. LDH utilizes the mathematical properties of lattices to ensure confidentiality and integrity in communication channels, thereby strengthening the security of the group's cryptographic operations.
- The incorporation of blockchain technology introduces a decentralized and transparent approach to managing group membership dynamics. By leveraging blockchain's distributed ledger technology and smart contracts, membership changes can be executed securely, transparently, and efficiently.
- The integration of CGKA, LDH, and blockchain technology presents a comprehensive solution for advancing the security and scalability of dynamic group membership management protocols. This comprehensive solution offers a robust framework for secure and efficient communication in contemporary environments, addressing the complex challenges associated with dynamic group membership management.

The remainder of the article includes related works, problem statement, methodology and results in section 2, 3, 4 and 5. The paper is concluded in section 6.

2. Related Works

The original purpose of VANETs, was to help with traffic control and safety communication [21]. Owing to the notable advancements in contemporary automobiles, VANET functions have broadened to encompass pertinent services related to infotainment and comfort. The necessity to safeguard them has grown even more as a result of this growth. Transparent sharing of a cryptographic group key is essential to VANET protection. In extremely volatile systems like VANETs, it is challenging to revise the group key on a regular basis due to the rapid changes in membership in a group. It is therefore difficult to create a group management key mechanism that is safe, scalable, and effective. The high processing expenses associated with group key computing and extraction, extra processing and interpersonal overhead when group affiliation changes, as well as receiving vehicle collaboration are only a few of the restrictions introduced by current GKM methods. This study presents a unique GKM mechanism, ALMS, to solve these constraints. Efficiency investigation shows that because ALMS involves a minimal computational cost for the entire TA and the person who receives vehicles, it is quicker to implement than current protocols. Furthermore, it is not constrained by the key distribution issue that symmetrical key management techniques are. Furthermore, the only burden that ALMS adds to the TA for affiliation changes is a little one. This is accomplished by separating the initialization process from the group key calculation and carrying it out offline so as to preserve the encryption group secret's size.

D2D communications is a prospective 5G method for dynamic situations that can enhance the effectiveness of sending messages for group interaction because of the adaptability of devices [22]. Furthermore, each service on an ad hoc network is a programme running on the VANET. In order to minimize latency throughout vehicle discussions, communication between vehicles is being implemented in ad hoc contexts, including IoDs networks, C-V2X modules, drone fleet supervision, and autonomous driving systems. Nonetheless, facilitating safe and efficient interaction among teams is a pressing issue. It suggest a decentralized ledger-based dynamic group administration tool as the answer to these issues. The research presented here shows that a structure that is hierarchical built around distributed ledgers can handle dynamic groups more quickly and easily, without sacrificing security and functionality. Moreover, the suggested approach can lessen the possibility of a single point of failures by facilitating the flow of data via immediate interaction without the need for a centralized database. Furthermore, an outside organization with deep ties to Taiwan's top automobile electronic suppliers globally conducted testing on the findings.

New approaches to access control have emerged in response to the explosive proliferation of IoT devices handling private information, with the goal of protecting this information from unauthorized usage [23]. To guarantee safe data delivery to authorized users, a dynamic Internet of things context that is marked by a high signaling overhead due to users' movement poses a serious challenge. Therefore, GKM serves as the essential method for controlling the assignment of keys for controlled access and safe sharing of data during these dynamic contexts. Unfortunately, the majority of the GKM-based access management techniques now in use for the IoT depend on centralized models, making them unable to handle the scalability issue brought on by the huge amount of IoT devices and growing number of subscribers. Furthermore, neither of the GKM methods in use today encourage group members' individuality. They just concentrate on dependent asymmetric group keys to communicate inside each subgroup, making them ineffective for subscribers exhibiting extremely dynamic behavior. It provide a unique DLGKM-AC to address these issues. The suggested system improves the administration of users' subgroups and reduces the retyping burden on the KDC by using a hierarchical design made up of many SKDCs and one KDC. Additionally, a brand-new master's token management technique is presented to control the distribution of keys among users. With this type of protocol, join/leave events have less overhead in terms of processing, storing, and transmission. By lowering the strain brought on by reentering at the core system, the suggested method allows for a scalable Internet of Things design and counteracts the risk of only having one point of failure.

Resolving the speed constraint of PoW-based blockchain networks, that typically enable just hundreds of transactions per second and take moments to months for transaction approval, is a major goal of the PBFT agreement method [24]. PBFT is generally used in tiny networks because of its poor node expansion caused by numerous inter-node connections. In this paper, an extensible multi-layer PBFT-based consensus process is suggested for enabling PBFT in big structures, like blockchain and enormous IoT ecosystems. The technique works by systematically aggregating nodes into distinct levels and restricting transmission inside the group. First provide an ideal double-layer PBFT and demonstrate a considerable reduction of communication difficulty. In particular, researchers demonstrate that interaction difficulty is minimized provided the nodes are spread equally throughout each sub-group in the following layer. FPD and FND methods are used, accordingly, to analyses the safety threshold. In addition, researchers offer a workable procedure for the suggested double-layer PBFT systems. Lastly, the findings are expanded to include security analysis and communications efficiency in arbitrary-layer PBFT platforms. The efficacy of the analytical data is confirmed by the results of simulations.

Three main topics that improve security and scalability in various technical contexts are covered in the literature study. First off, because membership in VANETs is dynamic, the study emphasizes the difficulties in safely maintaining cryptographic group keys. It suggests a novel GKM technique known as ALMS, which solves scaling problems and lowers computing expenses. Second, the emphasis moves to D2D communications in 5G contexts, highlighting the necessity of effective and safe group collaboration. A decentralized ledger-based dynamic group management system is used in the suggested approach to increase agility without sacrificing security. The study concludes with a discussion of control of access in Internet of Things contexts, where scaling and uniqueness issues arise for typical centralized GKM approaches. It presents a DLGKM-AC systems that lowers processing complexity while improving subgroup administration and adaptability. Every research offers fresh strategies to tackle certain problems, advancing both safety and scalability in the fields they study.

3. Problem Statement

In contemporary digital environments, managing dynamic group membership while ensuring robust security measures poses significant challenges. Existing group membership management protocols often struggle to adapt to dynamic changes in group composition, leading to scalability issues and security vulnerabilities. The need for secure and scalable group communication channels is paramount for organizations operating in collaborative environments. Therefore, there is a pressing need to develop innovative protocols that can effectively address the complexities of dynamic group membership management while maintaining the security and integrity of communication channels [25]. The proposed methodology aims to address these challenges by integrating CGKA for group formation, leveraging LDH for key generation, and employing blockchain technology for implementing membership changes. This comprehensive approach seeks to revolutionize group membership management by fostering trust, enhancing security, and ensuring scalability in dynamic group environments.

4. Proposed Dynamic Group Membership Management

Integrating CGKA for group formation ensures that each member actively contributes to the generation of the group key, fostering trust and collaboration within the group. This approach enhances the security and resilience of the group's cryptographic infrastructure by distributing the responsibility of key generation among all participants. LDH is employed for the generation of keys, leveraging the mathematical properties of lattices to securely derive shared secret keys. LDH provides a robust and efficient method for generating keys in cryptographic applications, ensuring confidentiality and integrity in communication channels. Employing blockchain technology for implementing membership changes offers a decentralized and transparent approach, allowing for the secure addition and removal of members from the group. By leveraging blockchain's distributed ledger technology and smart contracts, membership changes can be executed securely, transparently, and efficiently, enhancing the integrity and resilience of the group's membership management system. It is depicted in Figure 1.

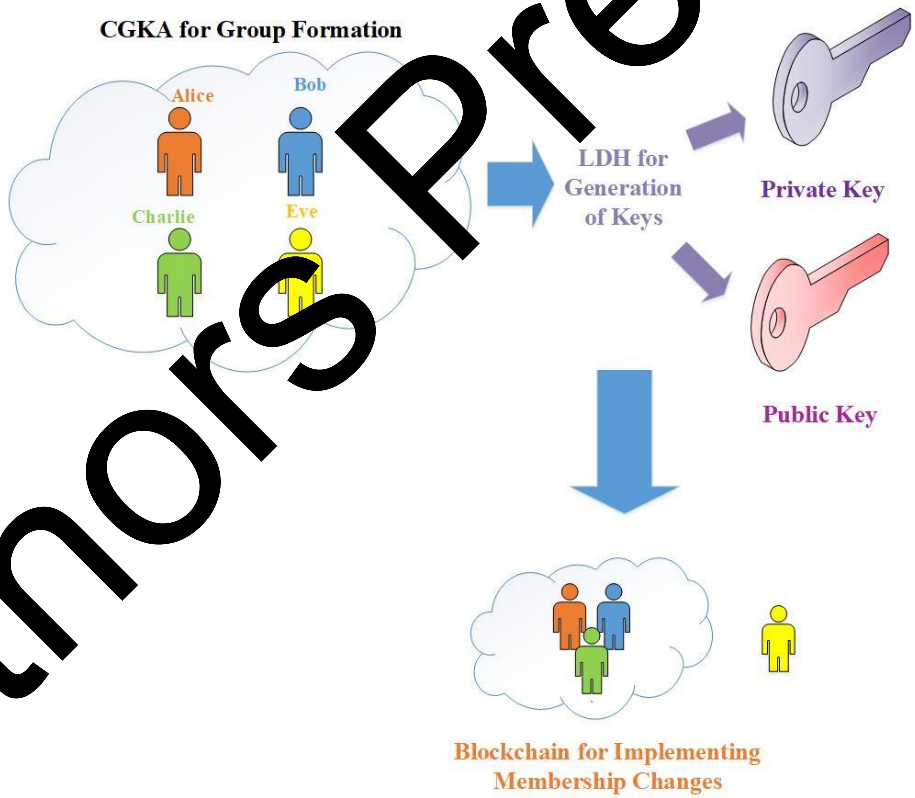


Figure 1: **Proposed Methodology**

4.1 Integrating Contributory Group Key Agreement for Group Formation

The role of Contributory Group Key Agreement (CGKA) in group formation is paramount for establishing robust and secure communication channels among multiple parties. CGKA facilitates the collaborative generation of a group key, ensuring that each member actively contributes to the process. This collaborative approach enhances the overall security of the group by distributing the responsibility of key generation among all participants, mitigating the risk of a single point of failure. By involving each member in the key generation process, CGKA fosters a sense of trust and accountability within the group, as every member plays a crucial role in establishing secure communication channels.

CGKA enables dynamic group membership management, allowing new members to join or existing members to leave the group without compromising the security of the group key. This flexibility is essential for adapting to changing group dynamics and ensures that the group key remains secure even as the composition of the group evolves over time. Additionally, CGKA provides resilience against attacks and unauthorized access attempts, as the group key is derived collaboratively from the individual contributions of all members. Overall, the role of CGKA in group formation is to facilitate the collaborative generation of a secure group key, fostering trust, accountability, and resilience within the group.

The Alice, Bob, Charlie, and Eve group formation mimics a situation similar to quantum group key distribution (QKD), which is a crucial idea in quantum cryptography that aims to provide safe channels of communication. In this configuration, Bob and Charlie separately produce random bases, and Alice generates random secret data bits and encodes them using a randomly selected basis. An important security risk arises when Eve, the eavesdropper, intercepts and perhaps modifies the qubits that Alice transmits to Bob and Charlie in order to create a secure communication channel. This hypothetical situation emphasizes the significance of secure communication protocols in quantum cryptography and the continuous struggle to provide robust defenses for confidential data in quantum communication networks.

4.1.1 Alice

Alice has a crucial part in the establishment of the group since she is the one who starts and sends the quantum communication process. Secure communication is established when Alice creates random secret data bits and encrypts them using a randomly selected basis. Alice makes use of quantum mechanics to increase the security of the communication channel by encoding the secret bits in quantum states. Her proactive engagement guarantees the integrity and secrecy of the information transferred, laying the groundwork for Bob and Charlie to safely extract the secret data bits by receiving and decoding the quantum states. Alice's role emphasizes how important it was for her to build safe communication channels, highlighting how important it is for quantum cryptography to have strong security mechanisms.

4.1.2 Bob

Bob plays a crucial part in the establishment of the group as he is one of the intended recipients of the quantum communication that Alice started. Bob is essential to Alice's process of receiving and decoding the quantum states that he sends in order to get the bits of secret data. Furthermore, Bob creates random bases on his own, strengthening the communication channel's security even further. The unpredictable and complicated nature of these independently generated bases makes it more difficult for possible eavesdroppers, like Eve, to collect and decode the sent data. Bob's enthusiastic involvement underlines how secure communication protocols are collaborative in nature, emphasizing how crucial it is for numerous parties to cooperate in order to create and maintain safe channels in quantum cryptography.

4.1.3 Charlie

Charlie plays a critical part in the establishment of the group as an additional intended recipient of the quantum communication that Alice started. Charlie, like Bob, has to receive the quantum states that Alice sends and decode them in order to get the bits of hidden data. To add to the variety and unpredictable nature of the communication process, Charlie also independently creates random bases. By adding more randomness and complexity to the communication channel, this independent base generation strengthens its security by increasing the difficulty for possible eavesdroppers, like Eve, to collect and decode the sent data. Charlie's active participation highlights the cooperative aspect of secure communication protocols, emphasizing how crucial group efforts are to creating and preserving secure channels in quantum cryptography.

4.1.4 Eve

Eve plays the role of the eavesdropper in the group formation, which presents a serious security risk to the quantum communication process that Alice started. Eve's main goal is to intercept and maybe modify the quantum states that Alice sends to Bob or Charlie in an effort to obtain the secret data bits without being discovered. Eve listens in on the communication channel with the intention of using system flaws and vulnerabilities to get private information and jeopardize the communication's integrity. Eve's existence highlights the persistent difficulties in guaranteeing secure communication in quantum communication networks and emphasizes the significance of strong security mechanisms in quantum encryption to identify and neutralize eavesdropping efforts efficiently.

4.2 Lattice Diffie–Hellman for Generation of Keys

LDH is a cryptographic protocol utilized for generating keys securely, leveraging the mathematical properties of lattices. The protocol begins with each party, typically referred to as Alice and Bob, independently generating random matrices and vectors. Alice generates a random matrix and a secret vector, while Bob generates another random matrix. Alice computes a noisy vector by adding random noise to the result of a matrix-vector multiplication, and she sends this noisy vector to Bob. Upon receiving the noisy vector, Bob computes another noisy vector by multiplying it with his random matrix and adding more random noise. Bob then sends this noisy vector back to Alice. Finally, Alice can compute the shared secret key by performing an inner product operation between the received noisy vector and her secret vector.

This process ensures that the shared secret key is securely generated over an insecure communication channel without directly exchanging any private information. The security of the LDH protocol relies on the hardness of the LWE problem, which makes it computationally infeasible for an eavesdropper to recover the shared secret key from the exchanged noisy vectors. By leveraging the mathematical properties of lattices and the difficulty of solving the LWE problem, the LDH protocol provides a robust and efficient method for generating keys in cryptographic applications, ensuring the confidentiality and integrity of communication channels. Table 1 shows the parameters of LDH.

Table 1: **Parameters of LDH**

Parameter	Description
Lattice Basis	Represents the mathematical structure of the lattice, typically defined by a basis matrix.
Secret Vector	Random vector chosen from a discrete Gaussian distribution, used to compute the public key.
Public Key	Vector obtained by taking the inner product of the lattice basis vectors with the secret vector.
Noise Term	Small noise term added to the inner product computation to ensure the resulting key is indistinguishable from random.

Encryption Scheme	Utilizes the computed public key and the recipient's private key to encrypt messages securely.
Decryption Scheme	Uses the recipient's private key and the sender's public key to decrypt encrypted messages.

4.2.1 Generation of Private Key

The generation of a private key is a fundamental aspect of asymmetric cryptography, where each party in a communication session possesses a unique key pair consisting of a private key and a corresponding public key. The private key is a securely generated, random string of binary digits or alphanumeric characters, typically generated using cryptographic algorithms and protocols. The process begins with the selection of a secure random number generator (RNG), which ensures that the private key is generated with sufficient entropy to resist cryptographic attacks. The private key is then generated by the RNG and stored securely in the possession of the key holder. It is crucial that the private key remains confidential and is not shared with any unauthorized parties to maintain the security of the cryptographic system.

In asymmetric cryptography, the private key is kept secret and is known only to the owner, whereas the corresponding public key is shared with other parties for encryption or signature verification purposes. The private key plays a vital role in cryptographic operations such as decryption, digital signature generation, and key agreement protocols. Overall, the generation of a private key is a critical step in establishing secure communication channels, digital signatures, and other cryptographic operations, ensuring the confidentiality, integrity, and authenticity of data in modern cryptographic systems.

Using the mathematical features of lattices, the LDH cryptographic protocol generates private keys in a secure manner. The Learning with Errors (LWE) issue, which argues that it is computationally difficult to retrieve a concealed secret from a given set of noisy linear equations, is the foundation of the protocol. Using the use of an unsecure communication channel, two people, known as Alice and Bob, want to construct a shared secret key using the LDH protocol.

Alice creates a secret vector (s) and a random matrix (A) in the first phase of the LDH procedure. The random matrix A is a n x m matrix with evenly randomly selected elements from a vast field. The private key is contained in the m-dimensional secret vector, or Vs. After that, Alice multiplies the matrix-vector result by a little amount of random noise to get a noisy vector e_A. In terms of math, this is expressed as:

$$e = As + noise \tag{1}$$

In the subsequent phase, Bob receives the noisy vector *e*e from Alice over the unsecure communication channel. After getting $d = e$, Bob creates a new random matrix B with dimensions $d=F \times m\, n{\times}m$. He then multiplies $d = e$ by dB and adds a new set of random noise to create a second noisy vector, $d = f$. In terms of math, this is expressed as:

$$f = Be + noise \tag{2}$$

At last, Bob uses the unreliable channel to give Alice the noisy vector f back. Alice may then obtain the shared secret key s by calculating the inner product of the vector f and her secret vector s after obtaining f. In terms of math, this is expressed as:

$$s_{shared} = f \,.\, s \tag{3}$$

Because the LWE issue is hard, it is computationally impossible for an eavesdropper to get the shared secret key s from the noisy vectors i and f. This is the foundation for the security of the LDH protocol. The LDH protocol offers a safe and effective way to generate private keys for use in cryptographic applications by taking use of the mathematical characteristics of lattices and the challenge of addressing the LWE problem.

4.2.2 Generation of Public Key

The generation of a public key is a fundamental process in asymmetric cryptography, where each participant in a cryptographic system possesses a unique key pair consisting of a public key and a corresponding private key. Unlike the private key, which must be kept secret, the public key is intended for distribution and is made freely available to other parties. The generation of a public key typically involves applying mathematical algorithms and protocols to derive a value that is mathematically related to the corresponding private key. This relationship ensures that messages encrypted with the public key can only be decrypted by the corresponding private key and vice versa, providing a mechanism for secure communication and digital signatures.

One of the most common algorithms used for public key generation is the RSA algorithm, which involves selecting two large prime numbers and performing mathematical operations to generate a public key exponent and a corresponding private key exponent. The public key consists of the modulus and the public exponent, while the private key consists of the modulus and the private exponent. Overall, the generation of a public key is a crucial step in establishing secure communication channels, digital signatures, and other cryptographic operations, ensuring the confidentiality, integrity, and authenticity of data in modern cryptographic systems.

LDH is a cryptographic protocol used for generating public keys securely, based on the mathematical properties of lattices. The protocol leverages the hardness of the LWE problem, which states that it is computationally difficult to recover a hidden secret from a given set of noisy linear equations. In LDH, two parties, typically referred to as Alice and Bob, aim to establish a shared public key over an insecure communication channel.

In the first step of the LDH protocol, Alice generates a random matrix B and a secret vector s. The random matrix B is a n x m matrix with elements chosen uniformly at random from a large field. The secret vector s is a m-dimensional vector containing the private key. Alice then computes a noisy vector d by adding a small random noise to the result of the matrix-vector multiplication *Bs*. Mathematically, this can be represented as:

$$d = Bs + noise \tag{4}$$

Next, Alice sends the noisy vector *d* to Bob over the insecure communication channel. Upon receiving *d*, Bob generates another random matrix C of dimensions n x m and computes a second noisy vector f by multiplying *d* with C and adding another set of random noise. Mathematically, this can be represented as:

$$f = Ce + noise \tag{5}$$

Bob then sends the noisy vector *f* back to Alice over the insecure channel. Upon receiving *f*, Alice computes the inner product of the vector *f* and her secret vector *s*, resulting in the shared public key R_{shared} mathematically, this can be represented as:

$$R_{shared} = f \,.\, s \tag{6}$$

The security of the LDH protocol relies on the hardness of the LWE problem, making it computationally infeasible for an eavesdropper to recover the shared public key R_{shared} from the noisy vectors *d* and *f*. By leveraging the mathematical properties of lattices and the difficulty of solving the LWE problem, the LDH protocol provides a secure and efficient method for generating public keys in cryptographic applications.

4.3 Employing Blockchain for Implementing Membership Changes

Employing blockchain technology for implementing membership changes offers a decentralized and transparent approach to managing group dynamics within distributed systems. Blockchain, as a distributed ledger technology, maintains a tamper-resistant record of transactions across a network of nodes. Each transaction, including membership changes such as additions or removals of members, is cryptographically signed and recorded on the blockchain, ensuring transparency and immutability. When a new member seeks to join the group, a transaction is created and broadcasted to the network, detailing the necessary information for membership approval. Similarly, when a member needs to be removed from the group, a corresponding transaction is generated, reflecting the change in membership status.

Blockchain smart contracts can automate the process of membership changes, executing predefined rules and logic to validate and authorize membership requests. Smart contracts can enforce membership criteria, verify identities, and ensure compliance with predefined rules before processing membership changes. Additionally, blockchain's decentralized nature eliminates the need for a central authority to manage membership changes, reducing the risk of single points of failure and enhancing the resilience of the system. By leveraging blockchain technology, implementing membership changes becomes more transparent, auditable, and secure, providing a robust framework for managing group dynamics within distributed systems.

4.3.1 Display Keys Before Eve is Removed

Before Eve is removed, the display of keys showcases the cryptographic contributions of each participant in the group, including Alice, Bob, Charlie, and Eve. Each member's contribution to the group key is visually represented, illustrating their individual role in the key generation process. The display highlights the collaborative nature of the key generation scheme, emphasizing the importance of each member's contribution in ensuring the security and integrity of the group key. Additionally, the display serves as a visual aid for monitoring and verifying the distribution of cryptographic responsibilities within the group, providing transparency and accountability in the key generation process.

4.3.2 Remove Eve from the Group

Using blockchain technology to remove Eve from the group involves executing a series of transactions on the blockchain network to update the group's membership records and revoke Eve's access privileges. First, a transaction is created to initiate the removal process, specifying Eve's identification details and the reason for her removal. This transaction is broadcasted to the blockchain network, where it is verified and added to the blockchain's immutable ledger by the network's consensus mechanism. Smart contracts deployed on the blockchain can automatically execute predefined rules and logic to validate the removal request, ensuring that it complies with the group's membership policies and procedures.

Once the removal transaction is confirmed and added to the blockchain, Eve's access privileges are revoked, and her cryptographic contributions to the group key are invalidated. This ensures that Eve no longer has access to the group's resources or confidential information. The removal process is transparent and auditable, allowing all members of the group to verify the transaction and confirm Eve's removal from the group. By leveraging blockchain technology, the removal of Eve from the group is executed in a secure, transparent, and decentralized manner, enhancing the integrity and resilience of the group's membership management system.

4.3.3 Public Keys before Eve is Removed

Before Eve is removed, the display of public keys showcases the cryptographic contributions of each participant in the group, including Alice, Bob, Charlie, and Eve. Each member's public key is visually represented, illustrating their individual role in the cryptographic operations within the group. The public keys serve as essential components for encrypting and decrypting messages, establishing secure communication channels, and verifying digital signatures. The display highlights the collaborative nature of the group's cryptographic infrastructure, emphasizing the importance of each member's contribution in ensuring the security and integrity of the group's communication protocols. Additionally, the display serves as a visual aid for monitoring and verifying the distribution of cryptographic responsibilities within the group, providing transparency and accountability in the cryptographic operations.

$$\text{Alice's Public Key} = [8\ 8\ 4] \tag{7}$$

$$\text{Bob's Public Key} = [2\ 5\ 4] \tag{8}$$

$$\text{Charlie's Public Key} = [7\ 6\ 3] \tag{9}$$

4.3.4 Public Keys after Eve is Removed

After Eve is removed from the group, the display of public keys reflects the updated cryptographic contributions of the remaining participants, namely Alice, Bob, and Charlie. With Eve's public key removed, the display now showcases the public keys of the remaining members, illustrating their continued involvement in the group's cryptographic operations. The removal of Eve ensures that only trusted members contribute to the group's cryptographic infrastructure, enhancing the security and integrity of the communication channels. The updated display serves as a visual confirmation of Eve's removal from the group and reinforces the collaborative nature of the group's cryptographic protocols. Additionally, it provides transparency and accountability in the cryptographic operations, allowing all members to verify the distribution of cryptographic responsibilities within the group.

$$\text{Alice's Updated Public Key} = [3\ 4\ 1] \tag{10}$$

$$\text{Bob's Updated Public Key} = [4\ 6\ 1] \tag{11}$$

$$\text{Charlie's Updated Public Key} = [2\ 8\ 2] \tag{12}$$

Algorithm: Dynamic Group Membership Management

Initialize
Set the group size to n.
Generate a random prime number p.
Choose a generator g for the cyclic group Zp.*
Key Generation
Each member generates a random secret key, denoted as sk[i], where i represents the member's index in the group
Calculate the corresponding public key for each member:
Group Key Agreement
Each member broadcasts their public key pk[i] to all other members in the group.
Upon receiving all public keys, each member computes the group key as follows:
LDH Key Generation
Choose lattice parameters and generate a lattice basis.
Each member generates a random vector s[i] as their secret key.
Compute the corresponding public key for each member using LDH
Share the public keys with all other members.
Membership Changes with Blockchain
Utilize a smart contract on the blockchain to handle membership changes.
When a new member joins, they submit a transaction to the smart contract
Similarly, when a member leaves the group, they submit a transaction to revoke their membership
Membership changes are recorded on the blockchain, providing transparency and accountability

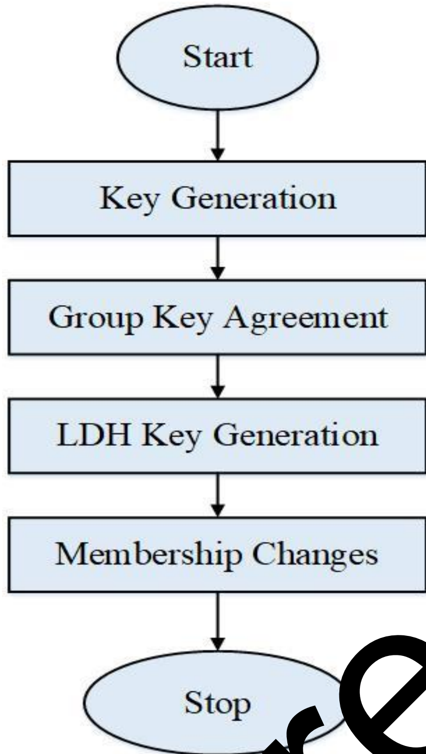


Figure 2: **Dynamic Group Membership Management**

5. Results and Discussion

The proposed method is implemented in Python software and the efficiency is evaluated and compared with existing protocols. The performance evaluation is given in this section.

5.1 Network Graph of Participants with Keys

A network graph of participants with keys illustrates the relationships between participants in a cryptographic system, showcasing their respective public and private keys. It provides a visual representation of the key distribution within the network, facilitating analysis of key sharing and ensuring the integrity and security of cryptographic communications.

Table 2: **Network Graph of Participants with Keys**

Participants	Public Key	Private Key
Participant 1	0,6,6	6,4,6
Participant 2	4,0,8	6,4,6
Participant 3	4,0,8	6,4,6

Table 2 depicts the network graph of participants along with their corresponding public and private keys. The public keys, representing the shared information accessible to all participants, are listed alongside the private keys, which are kept confidential and unique to each participant. Observing the network graph, it becomes evident that Participants 2 and 3 share identical public and private key pairs, suggesting a potential redundancy or oversight in the key generation process. This uniformity may raise concerns regarding the uniqueness and security of the cryptographic keys within the network, warranting further investigation into the key generation methodology and ensuring the integrity of the cryptographic framework. It is depicted in Figure 3.

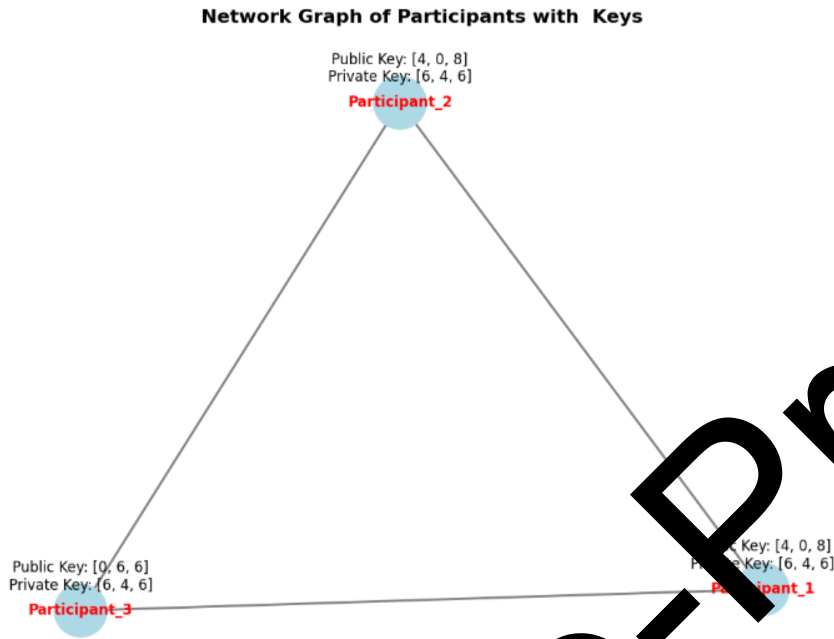


Figure 3: **Network Graph of Participants with Keys**

5.2 Public Keys before Eve is Removed

The public keys before eve is removed graph in Figure 4 displays the public keys associated with Participants 1, 2, and 3 along the x-axis. Each participant's public key is represented by on the graph. The y-axis represents the value of the public keys. Before Eve's removal from the group, the graph shows the distribution of public keys generated by each participant, reflecting their contribution to the group key agreement process. Analyzing this graph allows for visualizing the diversity and distribution of public keys across participants, providing insights into the cryptographic strength and security of the group key. Additionally, it facilitates monitoring any irregularities or anomalies in the public key distribution, which may indicate unauthorized access or compromised participants within the group.

Table 3: **Public Keys before Eve is Removed**

Participants	Public Key
Alice	4
Bob	6
Charlie	8

Table 3 shows the participants' public keys prior to Eve being kicked out of the group. The numbers 4, 6, and 8 represent Alice, Bob, and Charlie's respective public keys. These public keys are crucial for creating safe channels of communication within the organization. Each member of the group has contributed differently to the group's cryptography, as seen by the variances in the size of their public keys, which signify their distinct responsibilities within the cryptographic infrastructure. The public keys are essential for message encryption, safe connection establishment, and digital signature verification. This emphasises the need of each member's participation in maintaining the security and integrity of the group's communication protocols.

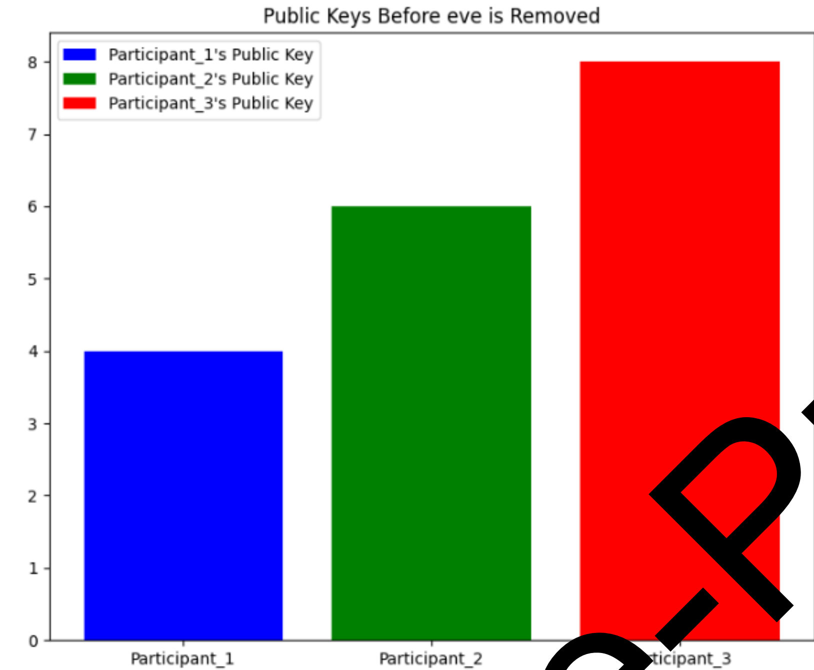


Figure 4: **Public Keys before Eve is Removed**

5.3 Public Keys After Eve is Removed

The public keys after eve is removed graph in Figure 5 depicts the public keys associated with Participants 1, 2, and 3 on the x-axis. Each participant's public key is represented by a distinct line or data point. Following Eve's removal from the group, the graph illustrates the updated distribution of public keys generated by the remaining participants. This visual representation allows for observing any changes or adjustments in the distribution of public keys after the removal of a compromised or unauthorized participant. Analyzing this graph facilitates assessing the impact of Eve's removal on the security and integrity of the group key agreement process, providing insights into the resilience of the group against potential security threats or attacks.

Table 4: **Public Keys after Eve is Removed**

Participants	**Public Key**
Alice	4
Bob	6
Charlie	8

The public keys of the participants in Table 4 do not alter following Eve's expulsion from the group. The public keys that Alice, Bob, and Charlie still have are denoted by the numbers 4, 6, and 8, respectively. The group's cryptographic infrastructure is stable and intact after Eve was removed, as indicated by the consistency of the public keys. The surviving members of the group continue to provide cryptography in the same way, thus safe lines of communication continue even in the event of a shift in group dynamics. This highlights the robustness of the group's cryptographic protocols and the efficiency of the systems set up to handle membership changes in an open and safe manner.

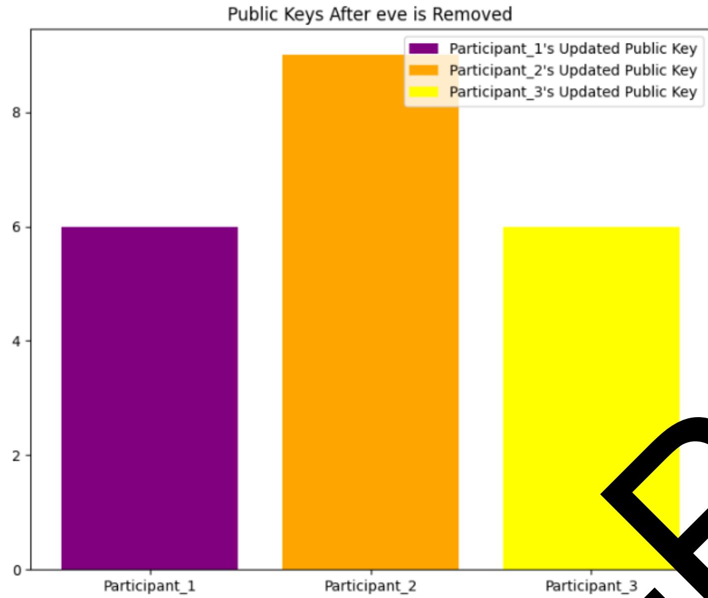


Figure 5: **Public Keys after Eve is Removed**

In terms of key size and computational cost, Table 5 compares the suggested LDH approach with other methods that are already in use. With a 256-bit key and a computational complexity of 10^5 operations, the LDH technique shows competitive performance, indicating its efficiency and applicability for cryptography applications. On the other hand, conventional techniques like RSA Key Exchange and ECDH have bigger key sizes (2048 and 256 bits, respectively) and have computational complexity of 10^6-10^7 operations. With a key size of 512 bits, PQC likewise offers a competitive option; nevertheless, its computational demands are comparable to those of RSA Key Exchange. The comparison highlights the importance of LDH as a viable method for safe key exchange, providing a balance between computational performance, key size, and

Table 5: **Comparison with Existing Methods**

Method	**Key Size (bits)**	**Computational Complexity (Operations)**
ECDH	256	10^6
RSA Key Exchange	2048	10^7
PQC	512	10^7
Proposed LDH	256	10^5

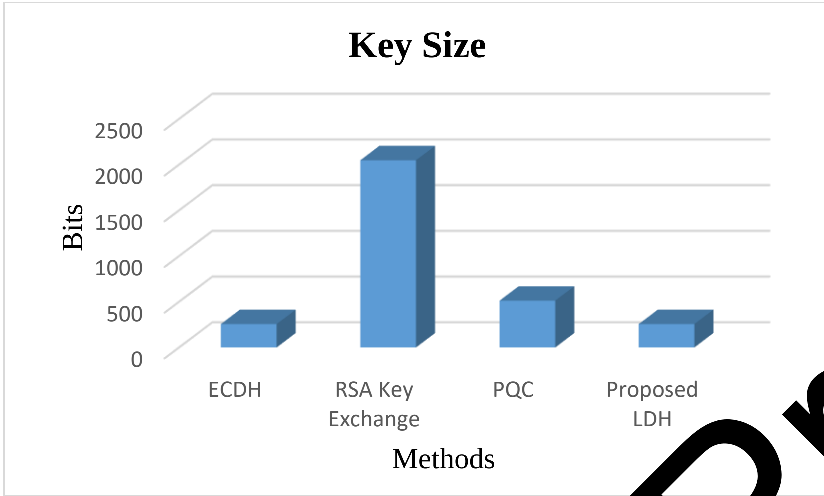


Figure 6: **Comparison with Existing Methods**

5.4 Discussion

The results of the comparison between LDH and existing methods underscore the efficacy of LDH in terms of key size and computational complexity. LDH demonstrates competitive performance with a relatively small key size of 256 bits, comparable to other contemporary cryptographic methods. This compact key size is advantageous for various applications, including resource-constrained environments where efficient utilization of computing resources is paramount. Additionally, LDH exhibits a lower computational complexity, with an order of magnitude fewer operations required compared to traditional methods like RSA Key Exchange and ECDH. This reduced computational overhead makes LDH particularly appealing for scenarios where computational efficiency is critical, such as real-time communication systems or high-throughput data processing environments.

The results suggest that LDH offers a promising solution for addressing the challenges posed by emerging quantum computing threats. By leveraging the mathematical properties of lattices and the hardness of lattice-based problems, LDH provides a robust framework for secure key exchange, even in the presence of quantum adversaries. The relatively small key size and low computational complexity of LDH further contribute to its suitability for post-quantum cryptographic applications. Overall, the results highlight LDH as a viable alternative to traditional cryptographic methods, offering a compelling combination of security, efficiency, and resilience against quantum computing attacks.

6. Conclusion and Future Works

The paper presents a comprehensive solution for addressing the challenges of managing group membership dynamically in contemporary communication systems. By integrating CGKA, LDH, and blockchain technology, the proposed protocol extension enhances the security, scalability, and efficiency of dynamic group membership management protocols. CGKA ensures that each member actively contributes to the generation of the group key, fostering trust and collaboration within the group. LDH provides a robust and efficient method for generating keys, leveraging the mathematical properties of lattices to ensure confidentiality and integrity in communication channels. Additionally, blockchain technology offers a decentralized and transparent approach for implementing membership changes, allowing for secure additions and removals of members from the group while maintaining the integrity of the cryptographic infrastructure. The future research could focus on further optimizing and refining the proposed protocol extension to enhance its performance and effectiveness in real-world scenarios. This could involve conducting more extensive simulations and performance evaluations to validate the scalability and efficiency of the protocol extension under various conditions. Additionally, research could explore the integration of advanced cryptographic techniques and protocols to further strengthen the security of dynamic group membership management. Furthermore, investigating the impact of emerging technologies such as quantum computing on the security of the protocol extension could provide valuable insights into potential vulnerabilities and mitigation strategies. Overall, continued research in this area is essential for advancing the state-of-the-art in dynamic group membership management protocols and ensuring the security and scalability of communication systems in dynamic environments.

Conflict of interest: The authors declare no conflicts of interest(s).

Data Availability Statement: The Datasets used and /or analysed during the current study available from the corresponding author on reasonable request.

Funding: No funding.

Consent to Publish: All authors gave permission to consent to publish.

References

[1] J. I. Escribano Pablos and M. I. González Vasco, “Secure post-quantum group key exchange: Implementing a solution based on Kyber,” *IET Communications*, vol. 17, no. 6, pp. 758–773, 2023.

[2] Z. Ashraf, A. Sohail, and M. Yousaf, “Robust and lightweight symmetric key exchange algorithm for next-generation IoE,” *Internet of Things*, vol. 22, p. 100703, 2023.

[3] K. Seyhan, T. N. Nguyen, S. Akleylek, K. Cengiz, and S. H. Islam, “M-GISIS KE: Modified key exchange protocol with reusable keys for IoT security,” *Journal of Information Security and Applications*, vol. 58, p. 102788, 2021.

[4] A. Musuroi, B. Groza, L. Popa, and P.-S. Murvay, “Fast and efficient group key exchange in controller area networks (CAN),” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9385–9399, 2021.

[5] C. Gupta and N. S. Reddy, “Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography.,” in *Journal of Physics: Conference Series*, IOP Publishing, 2022, p. 012014.

[6] D. S. Gupta, S. Ray, T. Singh, and M. Kumari, “Post-quantum lightweight identity-based two-party authenticated key exchange protocol for internet of vehicles with probable security,” *Computer communications*, vol. 181, pp. 69–79, 2022.

[7] Y. Zheng, W. Liu, C. Gu, and C.-H. Chang, “PUF-based mutual authentication and key exchange protocol for peer-to-peer IoT applications,” *IEEE Transactions on Dependable and Secure Computing*, 2022.

[8] Q. Lan, J. Chen, M. Shojafar, S. Kumari, and D. He, “SAKE*: A symmetric authenticated key exchange protocol with perfect forward secrecy for industrial Internet of Things,” *IEEE transactions on industrial informatics*, vol. 18, no. 9, pp. 6424–6434, 2022.

[9] “Efficient and Secure Group Key Management in IoT using Multistage Interconnected PUF | Proceedings of the International Symposium on Low Power Electronics and Design.” Accessed: Apr. 08, 2023. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3218603.3218646

[10] “Distributed Multiparty Key Management for Efficient Authentication in the Internet of Things | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Apr. 08, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8364539

[11] “Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends.” Accessed: Apr. 08, 2023. [Online]. Available: https://www.hindawi.com/journals/wcmc/2018/5349894/

[12] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommun Syst*, vol. 67, no. 3, pp. 423–441, Mar. 2018, doi: 10.1007/s11235-017-0345-9.

[13] "Security and Privacy in the Medical Internet of Things: A Review." Accessed: Apr. 08, 2023. [Online]. Available: https://www.hindawi.com/journals/scn/2018/5978636/

[14] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure Routing for MANET Connected Internet of Things Systems," in *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2018, pp. 114–119. doi: 10.1109/FiCloud.2018.00024.

[15] Y. B. Zikria, H. Yu, M. K. Afzal, M. H. Rehmani, and O. Hahm, "Internet of Things (IoT): Operating System, Applications and Protocols Design, and Validation Techniques," *Future Generation Computer Systems*, vol. 88, pp. 699–706, Nov. 2018, doi: 10.1016/j.future.2018.07.058.

[16] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, Oct. 2018, doi: 10.1016/j.comnet.2018.07.017.

[17] Y. Cui, Y. Ma, Z. Zhao, Y. Li, W. Liu, and W. Shu, "Research on data fusion algorithm and anti-collision algorithm based on internet of things," *Future Generation Computer Systems*, vol. 85, pp. 107–115, Aug. 2018, doi: 10.1016/j.future.2018.03.016.

[18] G. Avoine, S. Canard, and L. Ferreira, "Symmetric-key authenticated key exchange (SAKE) with perfect forward secrecy," in *Topics in Cryptology–CT-RSA 2020: The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24–28, 2020, Proceedings*, Springer, 2020, pp. 199–224.

[19] C. Patel and N. Doshi, "Secure lightweight key exchange using ECC for user-gateway paradigm," *IEEE Transactions on Computers*, vol. 70, no. 11, pp. 1789–1803, 2020.

[20] H. Davis and F. Günther, "Tighter proofs for the SIGMA and TLS 1.3 key exchange protocols," in *International Conference on Applied Cryptography and Network Security*, Springer, 2021, pp. 448–479.

[21] A. Mansour, K. M. Malik, A. Alkaff, and H. Kanaan, "ALMS: Asymmetric Lightweight Centralized Group Key Management Protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1663–1678, Mar. 2021, doi: 10.1109/TITS.2020.2975226.

[22] S.-P. Lu, C.-L. Lei, C.-Y. Ho, S.-J. Hwang, and H.-C. Chen, "Distributed Ledger Technology Based Architecture for Decentralized Device-to-Device Communication Network," *IEEE Access*, vol. 10, pp. 92006–92022, 2022, doi: 10.1109/ACCESS.2022.31[illegible]9880.

[23] M. Dammak, S. M. Senouci, M. A. Messous, M. H. Elhdhili, and C. Gransart, "Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1742–1757, Sep. 2020, doi: 10.1109/TNSM.2020.3002957.

[24] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A Scalable Multi-Layer PBFT Consensus for Blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, May 2021, doi: 10.1109/TPDS.2020.3042392.

[25] S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, and S. Kalathil, "Cryptographic data security for reliable wireless sensor network," *Alexandria Engineering Journal*, vol. 72, pp. 37–50, 2023.