Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 28 No. 7s (2025)

# Secure and Efficient Lightweight Key Distribution Protocol (LKDP) for IoT Networks.

**Kamakshi Gupta, Syed Afzal Murtaza Rizvi**

Jamia Millia Islamia, New Delhi, India

***Article History:***

**Received: 15-12-2024**

**Revised: 23-1-2025**

**Accepted: 3-2-2025**

**Abstract:**

The Internet of Things (IoT) plays a crucial role in ensuring secure device-to- device (D2D) interactions due to its ability to interconnect vast numbers of smart devices in real-time. In IoT ecosystems, devices often communicate directly without human intervention, creating opportunities for malicious activities like unauthorized access, data tampering, or eavesdropping. However, the restricted compute, memory, and energy capacities of devices provide a number of difficulties for key distribution in lightweight cryptography for the Internet of Things and other resource-constrained situations. The paper therefore proposes a novel dimension to key distribution, the Lightweight Key Distribution Protocol for IoT devices. The protocol presented is not only secure against many attack instances but also efficiently scalable to adaptable IoT networks, it also complies with current and future standards. In this paper, LKDP-IoT demonstrated that, via the complementation of theory and practical test deployment, it is a novel but significantly superior solution when securing communication, over IoT in comparison to other existing solutions. It could be considered that the arrival of LKDP-IoT is a move forward in providing reliable and secure solutions for Internet of Things.

**Keywords** - Key Distribution・Lightweight Cryptography・Authentication・Session Key Management・Authentication

## Introduction

The Lightweight Key Distribution Protocol (LKDP) specialized in establishing a shared secret between IoT devices to distribute cryptographic keys. The idea is to use lightweight cryptographic primitives instead, allowing LKDP to exchange secure keys with reduced processing overhead and making it more suitable for resource- limited environments. Those solutions of protocol provide not only a trusting channel and as well as robust, resilient defence against many cyberattacks: plaintext attack, man-in-the-middle attacks, replay attacks and impersonation etc. The protocol is additionally scalable for the increasing number of things and dynamic, as IoT ecosystems tend to regularly add new devices such as IP-cameras or voice-control speakers.

One of the major obstacles that IoT has in implementing secure communication is the development of a reliable and effective key distribution mechanism. Due to their high complexity, the resultant key distribution protocols that were initially designed for computer environments that have enhanced capacity become unfit to handle IoT devices. To eliminate these drawbacks, other lightweight cryptographic techniques that can meet the special needs required to facilitate IoT are employed. In this work, we propose a novel secure Lightweight Key Distribution Protocol for IoT Devices (LKDP-IoT) to tackle the problem of security and other relevant requirements for contemporary IoT systems. The suggested protocol is more appropriate with regards to its implementation in resource constrained Internet of Things because the proposed protocol aligns itself with the principles of low computing complexity, low energy and a reliable security system. In the first instance, the primary concern has been to reduce the protocol's overhead by using low resource demands for cryptographic functions in order to achieve secure key distribution. LKDP-IoT represents a new step forward in the construction of stable and effective key distribution approaches in the constantly evolving IoT context.

## Motivation

At present, the developers actively use the concept of the Internet of Things (IoT) that denotes a significant number of devices connected across the world, including sensors and actors, household appliances, and control systems of industrial facilities. These devices usually work in restricted circumstances that involve restricted computation power, storage space, and energy bank. Still, they are expected to secure communication thus being prone to a myriad of cyber threats. The conventional key distribution schemes, which are fine for more secure computational systems, fail to fit well the requirements of IoT objects. However, the computational and energy cost of these protocols becomes a significant burden for resource-scarce devices, which can lead to issues and even breaches. Furthermore, the IoT networks are very large and heterogeneous in nature, making these challenges more acute and requiring a protocol that is secure and at the same time, light on the network. This compelling requirement for a solution gives rise to a Lightweight Key Distribution Protocol for IoT Devices (LKDP-IoT). The main idea of LKDP-IoT is to establish a protocol which addresses the strict security demands together with the working difficulties of IoT gadgets. As a remedial to the weaknesses of existing protocols, LKDP-IoT's design tries to achieve secure distribution of keys in the various IoT settings in order to enhance IoT central security and reliability.

## Organisation

This paper is organized as follows. Section 1 presents an overview of the problem and importance of key distribution in the context of the IoT, and an appeal for the development of effective light-weight cryptography in the IoT environment. Section 2 emphasises on the motivation in the dynamic nature of the internet of things (IoT) leading to risk and threats in security architectures. Section 3 organises the paper. Section 4 presents the Related Work and Reviews of the existing key distribution protocols and cryptographic techniques used in IoT to date, their inefficiencies in the constrained environment. This section also provides a brief about the security requirements and constraints for the IoT networks. Section 5 presents a new designed and developed protocol known as the Lightweight Key Distribution Protocol for the Internet of Things (LKDP-IoT) together with details of the design, architectural framework and working process of the proposed protocol. The section also elaborates how LKDP-IoT solves the challenges as well as limitations of the current protocols. Section 6 contains performance analysis of the proposed protocol against existing key distribution schemes in terms of computational complexity, energy consumption and scalability. Section 7 describes future research directions and possible future improvements to LKDP-IoT, synergies with other security frameworks, and other possible kinds of IoT scenarios. Section 8 restate the contributions of the research with emphasis on the need to come up with a lightweight key distribution protocol in order to enhance secure communication in the IoT networks. This section also discusses the possible implication of LKDP-IoT with the future of IoT security.

## Review of Literature

Lightweight cryptography was utilized by Ma et al. [8] in form of communication authentication protocol which was developed using quantum key distribution with decoy-state technique with a view of tackling the issue of unauthorized control in the fixed RFID systems. A new RFID system was established with the weakly coherent photons transmitted through the optical fibre with which quantum keys were disseminated to RFID tags, readers, and EPC information servers. The paper also presented a security analysis that shows how the protocol is secure against several types of attacks and it also provides a comprehensive description of how the system works which includes system initialization, quantum key transmission and reception, as well as the process of the authentication.

The Internet of Things (IoT) faced significant security challenges due to continuous data transfer, which were addressed using cryptography and steganography techniques to ensure authentication and privacy. As per the study by Khari et al. [54] introduced the Elliptic Galois Cryptography Protocol to encrypt sensitive medical data and employed a Matrix XOR encoding steganography method to embed the encrypted data into low-complexity images. The Adaptive Firefly algorithm optimized cover block selection. Results showed effective data recovery and decryption, with improved security parameters compared to existing methods, highlighting the approach's efficiency.

Ostad-Sharif et al. [9] proposed a security model for WSNs and specifically for IoT settings, where the used model will consist of an authentication service and a key agreement protocol. As for previous protocols, [9,13,20,28,45] it was noted that the recent protocols suffered from the replay attacks or the absence of perfect forward secrecy. As solutions for these problems, the study provides a new secure and lightweight protocol and provides AVISPA analysis to prove it outperforms other protocols in security and performance.

A novel data encryption technique for IoT applications utilized by Saračević et al. [55] Catalan objects as cryptographic keys, leveraging combinatorial structures for secure encryption. Experimental analysis showed the Catalan method was harder to decipher than DES, with key quality verified through NIST tests and complexity analysis. Applications included e-Health IoT and smart city data processing. The Elliptic Galois Cryptography (EGC) protocol enhanced security using ECC over Galois fields, achieving 86% steganography embedding efficiency in MATLAB simulations. Performance evaluations highlighted its effectiveness compared to existing methods like OMME, FMO, and LSB.

Amin et al. [13] provided solution to the security challenges of data produced from the IoT devices by adopting Cloud Computing (CC) technique for the handling of the large database systems. It highlighted vulnerabilities in the multi-server cloud environments of existing protocols by Xue et al. and Chuang et al. The researchers proposed a new architecture and authentication protocol using smartcards, ensuring secure access to private information from distributed cloud servers. The protocol's robustness was verified using the AVISPA tool and BAN logic model, with performance analysis demonstrating its superiority over existing protocols.

Tight security proofs contributed to shorter security parameters and improved efficiency. A new signature scheme, SSSTR, was introduced by Chen et al. [52] demonstrating strong existential unforgeability under adaptively chosen message attacks. The security of this scheme was tightly linked to the Strong Diffie–Hellman assumption in the standard model. Additionally, two identity-based signature schemes were presented, which were proven to be existentially unforgeable under adaptively chosen message and identity attacks, with their security also tightly related to the Strong Diffie–Hellman assumption in the standard model.

Chen et al. [14] gave the energy limitations of most IoT devices, many manufacturers developed IoT applications based on group communication. Secure and effective authenticated group secret keys were essential for these applications, but existing protocols with centralized architectures were prone to single points of failure. In order to link IoT devices with blockchain networks, this study presented a blockchain-based authenticated group key agreement protocol. It also had a kind of device manager as well. A security study showed the protocol to be resilient against a number of attack vectors and simulations verified that the execution durations for the protocol were suitable for Internet of Things scenarios.

Secure and private computations on random access machines (RAM) were deemed more efficient than circuit or Turing machine computations, particularly for preventing information leakage on computers or cloud platforms. A novel scheme by Dolev [53] evaluated RAM programs while concealing program details, data, and results, using Shamir Secret Sharing and private string matching for instruction accuracy. This approach achieved information-theoretical security without computational hardness assumptions. Additionally, a model for outsourcing computations ensured confidentiality, integrity, and verifiability, keeping client programs and data hidden while directly handling secrets. This model proved ideal for securely outsourcing computations while safeguarding programs.

The networks of the future wireless sensor could offer IP connectivity to all nodes, with communication on IPv6 addresses down to IEEE 802.15.4 using 6LoWPAN. For the applications of e-health monitoring security should be achieved, but this adds an extra burden on top of its already high resource consumption and for many nodes with both energy memory and processing limitations security is truly a necessity. Lavanya et al. [20] proposed a light-weight key agreement and authentication protocol for end-to-end security. The protocol was then implemented on top of NS-2 and performance comparison with the current IKEv2 protocol was conducted.

Conventional cryptographic methods like AES, SHA-256, and RSA/Elliptic Curve were effective for systems with sufficient processing power and memory but were unsuitable for embedded systems and sensor networks. Lightweight cryptography emerged as a solution to address constraints such as physical size, processing requirements, memory limitations, and energy consumption. The study by Buchanan et al. [58] reviewed popular lightweight cryptography methods, including PRESENT, CLEFIA, LED, and KANTAN, analyzing their strengths and limitations. It also highlighted ultra-lightweight cryptography for resource-constrained IoT devices like sensors and RFID, outlining trends in designing lightweight algorithms for such applications.

Seyhan et al. [31] introduced a novel pair-wise key pre distribution protocol called Bilateral Generalization Inhomogeneous Short Integer Solution (Bi-GISIS). in 2021. To allow key reusing and reduce the time for key generation for Internet of Things (IoT) devices, this protocol uses bilateral pasteurization modified into random oracle model. Reusable keys were shown to be beneficial over key management in D2D-assisted fog computing scenarios, which is also fits the quantum-secure key exchange. This allowed for efficient use where resources were scarce (such as in IoT).

Random numbers played a crucial role in various fields of computer science. However, generating high-quality random numbers using only basic arithmetic operations posed a significant challenge, particularly for devices with limited hardware capabilities, such as Internet of Things (IoT) devices. To address this, a novel pseudorandom number generator called the Simple Chain Automaton Random Number Generator (SCARNG) was introduced, by Dömösi et al. [51] leveraging compositions of abstract automata. The primary advantage of this algorithm lay in its simple structure, which allowed easy implementation on low-computing-capacity IoT systems, FPGAs, or GPU hardware. The random numbers produced by SCARNG exhibited promising statistical behaviour and successfully met the NIST statistical suite requirements, demonstrating its potential for practical applications.

One aspect of distributed IoT applications is the possibility of utilizing Wireless Sensor Networks (WSNs) for which end-to-end security with reliable authentications are needed because of the limitations as well as the variability of the nodes. Further, it was realised that conventional systems were not of any help when it came to these uses. Porambage et al. [22] proposed P Auth Key, a new implicit certificate-based authentication and keying approach for WSNs providing application level end-to-end security. By performance assessment and security analysis, the study explained the behaviour of the protocol and it also provided that P Auth Key may be employed in the resource-limited WSNs.

A study by Khan et al. [56] surveyed key IoT security issues, categorizing them based on IoT's layered architecture and protocols for networking, communication, and management. It outlined security requirements, highlighted existing threats, and mapped them to state-of-the-art solutions. The analysis included a parametric evaluation of attacks and their corresponding solutions. Additionally, the study explored blockchain's potential as a solution to critical IoT security challenges and identified open research problems and future directions for reliable and scalable IoT security frameworks.

To cope with the constantly increasing threats in the field of IoT, Saied et al. [23] highlighted challenges that arose due to the dissimilar power capabilities of IoT entities and diverse IoT messaging. Thus, it was concluded that the legacy key exchange protocols could be infeasible for resource-constrained devices due to their extensive use of cryptographically complex operations. Realizing this, to have restricted devices transfer the cryptographic responsibilities to the neighbours with fewer restrictions this study examined current security standards and proposed new collaborative key establishment schemes. Performance investigation concluded that the said approach could potentially reduce energy consumption by as much as 80% when compared to traditional key installation techniques.

Applications that rely on point-to-multipoint or multipoint-to-point communication paradigms in many ad hoc networks can encrypt communication between many endpoints by using a single group key. Thus, Veltri et al.
[42] designed a unique centralized strategy to effectively distribute and maintain a group key in generic ad hoc networks The suggested protocol was used for secure data aggregation in IoT and Vehicle-to-Vehicle (V2V) communications in Vehicular Ad hoc Networks (VANETs). It handled

user joins and departs using two leave strategies: pre-determined or random periods.

IoT's growth has introduced significant security challenges, as cyberattacks exploiting IoT vulnerabilities have led to physical, economic, and health damages. Despite these risks, manufacturers often struggle to ensure robust IoT security. A study by Schiller et al [57] reviewed the IoT security landscape, identifying key challenges, defining major security objectives, introducing a threat taxonomy to highlight prevalent gaps, and summarizing countermeasures available in current IoT security technologies.

Sensors integrated into regular home appliances, offices, cars, streets and other buildings together with cars and other vehicles is called IoT for Internet of Things, where VANETs for vehicular ad-hoc networks play an important role in secure vehicle operations. Vijayakumar et al. [43] presented a new method in 2017 to improve the authentication support in VANETs with an anonymous authentication method that can improve the privacy of the messages while at the same time providing a secure and reliable method of authenticating messages exchanged in the network. The proposed framework reduced the computation costs and time of existing schemes as it also facilitated the affirmation of vehicles much faster. Besides, a novel anonymous group key distribution scheme has also been proposed for secure V2V and V2I communication and it has been implemented that exhibits better performance in terms of signature verification delay and computation overheads than earlier protocols.

The IoT helps the genuine consumers to safely gather data from industrial sensors with the help of AKA protocols. Nevertheless, it is crucial to understand that the agreement of a powerful session key in secure communication in industrial IOT (IIoT) particularly industrial IoT is a highly challenging and an even very costly affair. In this research, the author proposed a computationally efficient key agreement protocol that can replace the old ones. The proposed protocol as follows the adoption of the hybrid approach: First step to compute mutual secret key using Elliptic Curve Cryptography ECC shared by two users and a gateway node (GWN). With this key, GWN initiates a session key agreement involving the GWN and sensors in order to establish a secure communication link. Vinoth et al. [49] showed that through these simulations there was a great decrease in computational and communicational complexities as compared to previous protocols.

**Table 1. Summarizing previous protocol**.

| **Protocol** | **Key Security Features** | **Strengths** | **Weaknesses** | **Typical Attacks Mitigated** |
|---|---|---|---|---|
| **QKD with Decoy- State Method** | Quantum Key Distribution, weakly coherent photons | Very High Security (quantum-level protection), strong against eavesdropping | High computational and communication costs, limited scalability | Eavesdropping, man-in-the- middle, and other quantum attacks |
| **Lightweight** | Lightweight cryptographic | High security with | May lack perfect forward secrecy, | Replay attacks, brute |

| | | | | |
|---|---|---|---|---|
| **Cryptography for WSNs** | primitives, AVISPA validation | efficient resource usage | potential vulnerabilities in lightweight schemes | force attacks, unauthorized access |
| **Cloud Computing and Smartcards** | Smartcards, cloud- based authentication | Robust against various server-side attacks, strong access controls | Relies on the security of cloud and smartcard systems, can be complex | Data breaches, unauthorized access, multi- server attacks |
| **Blockchain-Based Group Key Management** | Decentralized trust model, blockchain technology | High security due to decentralization and immutability | Potential scalability issues, high energy consumption | Man-in-the-middle, data tampering, unauthorized group access |
| **Enhanced Authentication Protocol for WSNs** | Secure against replay and denial of service attacks | Comprehensive security for WSNs, addresses previous protocol flaws | May still be vulnerable to advanced attacks or implementation flaws | Replay attacks, denial of service, impersonation attacks |
| **Lightweight Pseudonym Identity-Based Authentication** | Pseudonym-based, implicit certificates | Efficient for smart city environments, improves over previous protocols | Security depends on smartcard management and pseudonym implementation | Privacy breaches, impersonation, unauthorized access |
| **Lo WPAN for IP Connectivity** | IP connectivity, lightweight protocol | Good for constrained devices, scalable | Security depends on additional layers, may not handle all attack vectors | Eavesdropping, packet injection, denial of service |
| **Public Key Cryptography with ECC and NTRU** | Optimized asymmetric cryptography, ECC/NTRU | Strong security with lower computational costs compared to traditional PKC | Complexity of key management, requires optimized implementations | Man-in-the-middle, data breaches, eavesdropping |
| **P Auth Key Protocol** | Implicit certificates, lightweight authentication | End-to-end security, efficient for WSNs | Security depends on certificate management and implementation | Unauthorized access, data tampering, man-in-the- middle |
| **Collaborative Key Establishment** | Offloading cryptographic tasks, collaborative approach | Reduces energy consumption, efficient in resource-constrained environments | Potential vulnerabilities in collaborative nodes, key management | Energy exhaustion, unauthorized access, eavesdropping |

| | | | | |
|---|---|---|---|---|
| | | | complexity | |
| **Bi-GISIS-Based Key Exchange Protocol** | Reusable keys, post- quantum security | Suitable for post-quantum environments, efficient key management | Complexity in key management, moderate scalability | Quantum attacks, unauthorized access, key compromise |

| **Protocol** | **Key Security Features** | **Strengths** | **Weaknesses** | **Typical Attacks Mitigated** |
|---|---|---|---|---|
| **Centralized Group Key Distribution** | Centralized key management, leave strategies | Efficient for managing group keys, robust security with centralized control | Centralized approach can be a single point of failure | Single point of failure, unauthorized access, data tampering |
| **Anonymous Authentication for VANETs** | Anonymous authentication, group key distribution | Enhances privacy, reduces computation costs | Relies on the strength of anonymous schemes, may have latency issues | Privacy breaches, unauthorized access, eavesdropping |
| **Hybrid Key Agreement Protocol** | ECC for key generation, hybrid approach | Efficient and scalable, reduces computational and communication costs | Complexity of hybrid approach, security depends on ECC implementation | Unauthorized access, eavesdropping, man-in-the- middle |

## 5. Proposed Protocol

The Lightweight Key Distribution Protocol (LKDP) works by establishing secure communication between IoT devices through efficient key distribution.

### 5.1 Assumptions

1. Pre-shared Secret key: Every device holds the key to a unique pre-shared secret key with the Trusted Authority (TA).

2. Symmetric Encryption and HMAC: They both use what is referred to as symmetric encryption for instance the Advanced Encryption Standard (AES) or the HMAC as the method of authentication.

3. Random Nonce Generation: The devices may possess ability to produce random nonce for ensuring the freshness of a communication.

### 5.1.1 Protocol details

To build a new efficient key distribution scheme for providing lightweight cryptographic components for secure messaging in IoT devices, we will devise the essence of the protocol i.e. ***Lightweight Key Distribution Protocol for IoT Devices (LKDP-IoT)*** with the requirements of constrained platforms of the IoT system. The protocol is resistant to common security threats like replay attacks, man-in-the-middle attacks, and impersonation, ensuring robust security in IoT environments.

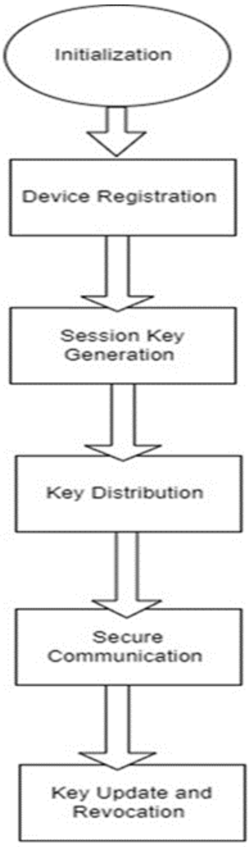

**Figure 1: Lightweight Key Distribution Algorithm**

### 1. Initialization Phase

#### A. Trusted Authority Setup:

The trusted authority (TA) generating a symmetric master key $KTA$ typically involves the use of a secure pseudorandom number generator (PRNG) or a key derivation function (KDF) to ensure randomness and security.

A mathematical representation for generating $KTA$ could be as follows:

**$KTA$=PRNG (S, length)**

Where:

PRNG is a pseudorandom number generator function.

S is the seed or entropy source used to initialize the PRNG. length specifies the desired bit length of the symmetric key $K_{TA}$

Alternatively, if using a cryptographic hash-based KDF, the formula could be:

$\boldsymbol{K_{TA}}$ **=KDF (S||info, length)**

Where:

KDF is a key derivation function (e.g., HMAC-based KDF).

S is the seed or master secret

info represents additional context information. length specifies the desired key length for $K_{TA}$.

2. **Device Registration Phase**:

A. **Inputs for Identifier Generation**:

Let $P_{D_i}$ represent the unique properties of device $D_i$ (e.g., MAC address, serial number, or a combination of both).

B. **Device Identifier Generation using Hashing**:

Each device $D_i$ generates a unique device identifier $I_{D_i}$A secure cryptographic hash function H (·) is applied to the unique properties to generate the device identifier $I_{D_i}$.

$\boldsymbol{I_{D_i}}$ **=H (** $\boldsymbol{P_{D_i}}$**)**

where:

$I_{D_i}$ is the unique device identifier for device $D_i$ .

$P_{D_i}$ is the unique property or combination of properties of $D_i$ .

H (·) is a secure hash function like SHA-256 or SHA-3.

This method makes sure that $I_{D_i}$ is unique and derived from the specific characteristics of the device
$D_i$ .The use of a cryptographic hash function also ensures that the identifier is difficult to reverse and provides integrity. TA stores the unique key $K_i$ and identifier $I_{D_i}$ for each device.

C. **Device Information**:

For each device Di, the TA generates the following:

- A unique symmetric key $K_i$
- A unique device identifier $I_{D_i}$

### D. TA Storage Mechanism:

The TA stores this information in a secure database or data structure, which could be a table, a key-value store or a list. The storage is represented by storing the device identifier $ID_i$ as the primary key and the symmetric key $K_i$ as the value associated with that identifier.

The mathematical representation of the storage can be expressed as:

**TA Database: S= {$(ID_1, K_1)$, $(ID_2, K_2)$, …. $(ID_n, K_n)$}**

where:
S specifies the storage of all devices.

$ID_i$is the unique identifier for device $D_i$ .

$K_i$ is the unique symmetric key for device $D_i$ . n is the total number of devices.
Alternatively, this can be thought of as:

**TA stores $(ID_i, K_i)$ for each device $D_i$, i =1,2…n**

This structure ensures that the TA can reference any device $D_i$ . by its unique identifier $ID_i$ and retrieve the corresponding symmetric key $K_i$ whenever necessary. The security of the storage relies on keeping the database confidential and protected against unauthorized access.

### 3. Session Key Generation Phase

The communication between Device $D_A$ and Device $D_B$ can be expressed mathematically as a secure exchange of messages, where a session key $K_{Session}$ is generated and used for encryption and authentication during communication. This is a detailed explanation of how to mathematically represent the communication:

### A. Session Initiation:

Device $D_A$ initiates communication with Device $D_B$ by generating a random nonce $N_A$, which acts as a challenge to ensure freshness.

$$D_A \xrightarrow{IDA, NA} D_B$$

$D_A$ sends its identifier $ID_A$ and the nonce $N_A$ to $D_B$.

### B. Session Key Generation:

Device DB verifies the identity $I_{DA}$ with the trusted authority (TA) and generates its own random nonce
$N_B$.Both devices $D_A$ and $D_B$ compute a session key $K_{Session}$ , which is derived using a key

derivation function based on their pre-shared symmetric keys $K_A$, $K_B$, and the nonces $N_A$ and $N_B$. The expression for generating the session key is:

$$\boldsymbol{K_{Session}} = \textbf{HMAC}\ (\boldsymbol{K_A, K_B} \parallel \boldsymbol{N_A} \parallel \boldsymbol{N_B})$$

where:

$K_A$ is the symmetric key of Device $D_A$.

$K_B$ is the symmetric key of Device $D_B$.

$N_A$ and $N_B$ are the random nonces generated by $D_A$ and $D_B$, respectively.

|| denotes concatenation.

### C. Session Key Distribution:

$D_B$ encrypts its nonce $N_B$ using the symmetric key $K_A$and $K_B$ sends it to $D_A$ :

$$\boldsymbol{EKA}(\boldsymbol{NB})$$
$$\boldsymbol{D_A} \longleftarrow\!\!-\!-\!-\!-\!- \boldsymbol{D_B}$$

where:

$E_{KA}(N_B)$ specifies the encryption of $N_B$ using $K_A$

### D. Session Key Verification:

Device $D_A$ decrypts the message using its key $K_A$ to retrieve $N_B$:

$$\boldsymbol{N_B} = \boldsymbol{D_{K_A}}\ (\boldsymbol{E_{K_A}}\ (\boldsymbol{N_B}))$$

Both $D_A$ and $D_B$ verify the nonces $N_A$ and $N_B$ to ensure the integrity and freshness of the session key exchange.

## 4. Key Distribution Phase

### A. Distributing Unique Symmetric Key:

The Trusted Authority (TA) distributes a unique symmetric key $K_i$ to each device $D_i$ securely using the master key $K_{TA}$.

### B. Encryption for Secure Distribution:

The TA encrypts the unique key $K_i$ using the master key $K_{TA}$, ensuring secure transmission of the key to the device. The encrypted key can be represented as:

$$\textbf{Ci}=\boldsymbol{E_{K_{TA}}}\ (\ \boldsymbol{K_i} \parallel \boldsymbol{ID_i}\ )$$

where:

$C_i$is the ciphertext (the encrypted form of $K_i$).

$K_{TA}$ is the symmetric master key for encryption.

$K_i$ is the unique symmetric key generated for device Di.

$ID_i$ is the identifier of device $D_i$, concatenated with $K_i$(denoted by ∥) for added integrity in distribution.

$E_{KTA}(\cdot)$ represents the encryption of the message using the key $KTA$.

### C. Decryption at the Device:

Device $D_i$ receives $C_i$ and decrypts it using the master key $K_{TA}$ to retrieve $K_i$.

$$\boldsymbol{K_i \parallel ID_i = E_{KTA}(Ci)}$$

where:

$D_{KTA}(Ci)$ is the decryption of the ciphertext using the master key $KTA$. The device checks $ID_i$ to verify its identity before using $K_i$.

This ensures the secure distribution of the symmetric key $K_i$ to each device $D_i$.

**Table 2: List of notations used in proposed LKDP Protocol.**

| **Abbreviation** | **Description** |
|---|---|
| TA | Trusted Authority |
| $KTA$ | Symmetric Master Key of Trusted Authority |
| $Ki$ | Unique Symmetric Key of Device Di |
| $Di$ | IoT Device i |
| $I_{DA}$ | Identifier of Device DA |
| $N_A$ | Random Nonce Generated by Device DA |
| $N_B$ | Random Nonce Generated by Device DB |
| $EK_A(N_B)$ | Encrypted Nonce NB with device DA's Symmetric Key KA. |
| $K_{Session}$ | Session Key |
| HMAC | Hash Based Message Authentication Code |
| $K_A$ | Symmetric Key of Device DA |
| $K_B$ | Symmetric Key of Device DB |
| KDF | Key Derivation Function |

## 5. Secure Communication Phase:

Once the session key $K_{Session}$ is established, both devices use it to encrypt and authenticate their communication. The message M sent by $D_A$ to $D_B$ can be represented as:

$$\boldsymbol{D_A \xrightarrow{E_{KSession}(M)} D_B}$$

where:

M is the message

$E_{KSession}$ (M) represents the encryption of message M using the session key $K_{Session}$. Similarly, DB can respond securely using the same session key $K_{Session}$ :

$\boldsymbol{E_{K_{Session}}(M')}$

$D_A \leftarrow---------- D_B$

This ensures confidentiality, integrity, and authenticity in communication between DA and DB

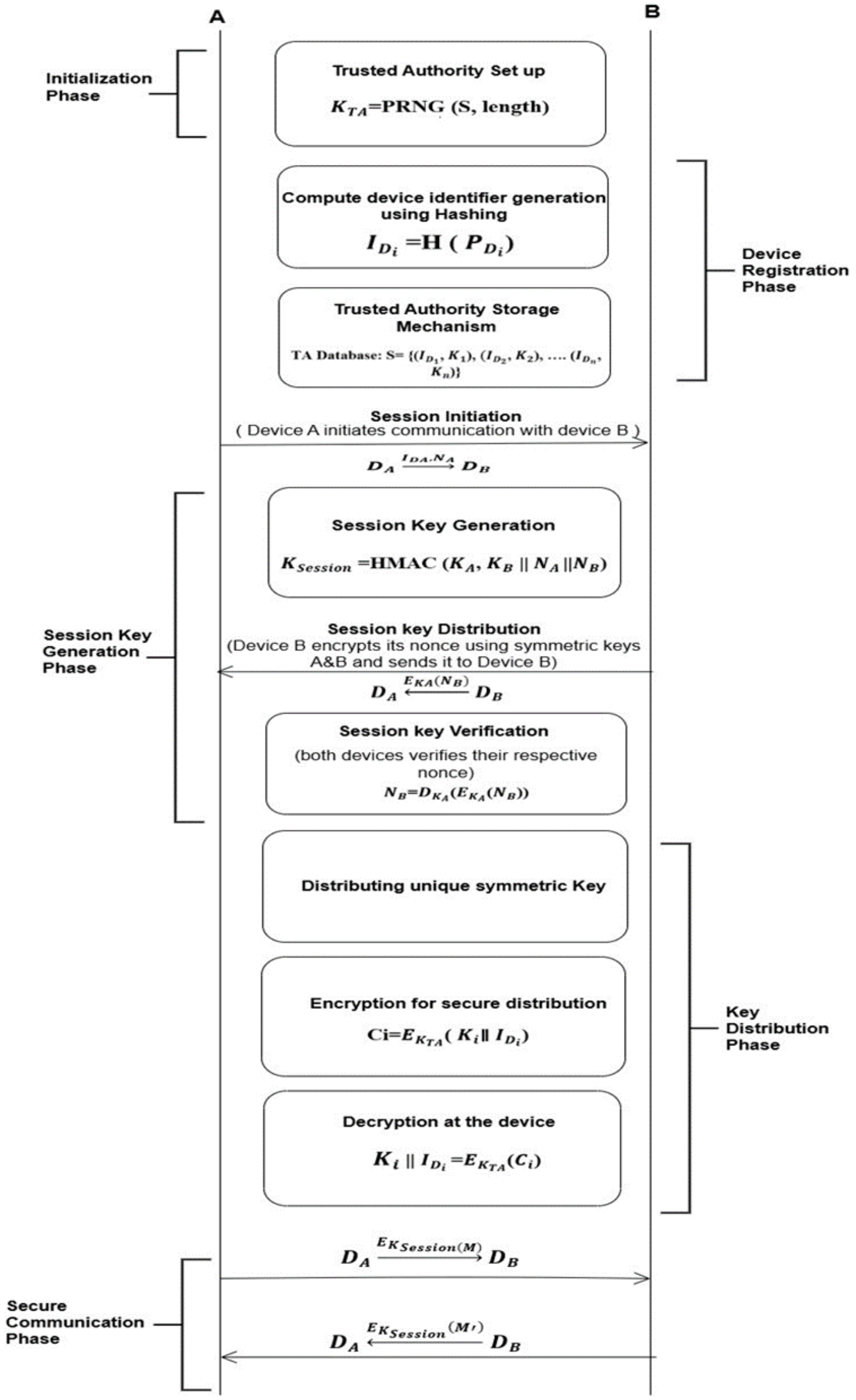
A
B
Initialization Phase
Trusted Authority Set up
$K_{TA}$=PRNG (S, length)
Compute device identifier generation using Hashing
$I_{D_i}$ =H ( $P_{D_i}$)
Trusted Authority Storage Mechanism
TA Database: S= {($I_{D_1}$, $K_1$), ($I_{D_2}$, $K_2$), .... ($I_{D_n}$, $K_n$)}
Device Registration Phase
Session Initiation
( Device A initiates communication with device B )
$D_A \xrightarrow{I_{DA}, N_A} D_B$
Session Key Generation
$K_{Session}$ =HMAC ($K_A$, $K_B$ || $N_A$ ||$N_B$)
Session Key Generation Phase
Session key Distribution
(Device B encrypts its nonce using symmetric keys A&B and sends it to Device B)
$D_A \xleftarrow{E_{KA}(N_B)} D_B$
Session key Verification
(both devices verifies their respective nonce)
$N_B$=$D_{K_A}(E_{K_A}(N_B))$
Distributing unique symmetric Key
Encryption for secure distribution
Ci=$E_{K_{TA}}$( $K_i$|| $I_{D_i}$)
Decryption at the device
$K_i$ || $I_{D_i}$ =$E_{K_{TA}}(C_i)$
Key Distribution Phase
$D_A \xrightarrow{E_{K_{Session}(M)}} D_B$
Secure Communication Phase
$D_A \xleftarrow{E_{K_{Session}}(M')} D_B$

**Figure 2: Detailed steps of Proposed Lightweight Key Distribution Protocol.**

## 5.2 Key Features of LKDP-IoT

Features of the proposed Lightweight Key Distribution Protocol for IoT Devices (LKDP-IoT) will cover many aspects owing to unique characteristics and necessities associated with the suitable operation in an environment like that which is we see in most IOT. Highlights of LKDP-IoT.

### 1. Efficiency

- **Lightweight Cryptographic Primitives**: Uses symmetric key cryptography and lightweight algorithms to ensure minimal computational overhead, making it suitable for resource-constrained IoT devices.
- **Low Power Consumption**: Designed to conserve battery life by minimizing energy-intensive operations.

### 2. Scalability

- **Support for Large Networks**: Can handle a large number of devices without significant performance degradation, ensuring scalability in diverse IoT deployments.
- **Dynamic Device Management**: Efficiently manages the addition and removal of devices from the network.

### 3. Security

- **Strong Key Management**: Securely handles key generation, distribution, update, and revocation to protect against various security threats.
- **Mutual Authentication**: Ensures both devices in communication authenticate each other using certificates and pre-shared keys.
- **Resistance to Attacks**: Includes mechanisms to prevent common attacks such as man-in-the-middle, replay, and physical attacks.
- **Periodic Key Updates**: Regularly updates keys to ensure ongoing security and mitigate the impact of compromised keys.

### 4. Interoperability

- **Interactivity**: Compatible with different existing IoT standards and protocols, meaning it can work with many devices as well as communication frameworks. It is flexible supporting IoT devices of all kinds and communication protocols.

### 5. Usability

- **Simplified Deployment**- End-users do not need to perform much configuration of gewa 21. The initial key distribution and configuration are handled by a trusted authority (TA).

### 5.2.1 LKDP Addressing Challenges

Designing a new lightweight key distribution protocol for IoT devices can help address the challenges listed in various ways. Here's how the proposed protocol can mitigate these challenges:

#### 1. Resource Constraints

•Limited Processing Power and Memory: The protocol makes use of symmetric key cryptography because this is quite easier in terms of computational complexity than asymmetric cryptography. It is therefore necessary to incur less resource usage and this is achieved by using lightweight cryptographic algorithms.

•Battery Life: Besides, low power cryptographic operations and proper handling of keys do help in saving battery life.

#### 2. Scalability

•Number of Devices: The symmetric keys and secure key exchanging procedure makes the given protocol scalable to a number devices addition to the marginal overhead.

•Dynamic Network: It can also easily add and remove devices due to effective key update and revocation mechanisms provided in the protocol.

#### 3. Security Threats

•Man-in-the-Middle Attacks: It is safeguarded against interception by mechanisms such as the pre-shared keys and the lightweight versions of Diffie-Hellman.

• Replay Attacks**:** This is done by ensuring that the messages exchanged in the keys include nonces as well as timestamps to counter any replay attacks.

• Physical Attacks: Key storage security and frequent key change are some of the features incorporated in the protocol to slightly reduce the effects of the physical attacks.

#### 4. Key Management

• Initial Key Distribution: This ensures that the TA is the only person to deal with the initial distribution of the keys in a secure manner. Devices are programmed with keys during making of devices or at the time of deployment of devices.

•Key Update and Revocation: The key update mechanisms also facilitate the possibility of updating the keys frequently and do not affect the network. TA provides and regularly updates revocation lists in order to make sure that keys which are compromised are no longer utilized.

#### 5. Interoperability

• Diverse Devices: The IoT device that is intended to implement this protocol is assumed to have variables capabilities, and may possess different communication protocols as well.

•Protocol Compatibility: The protocol can be easily implemented in line with different IoT interfaces and other protocols used in communication.

### 6. Latency and Real-Time Constraints

- Communication Delays: ‘Small’ cryptographic operations consume less computational resources and time so as to maintain the real-time communication.
- Synchronization: This means that devices will be able to securely communicate with each other even if connectivity between them is at times interrupted and sporadic.

### 7. Usability and Management

- Ease of Deployment: The operation of the protocol is such that it is easy to deploy with no much system configuration to be done by the end-users. As seen in the earlier sections, the TA is responsible for managing several critical key-related operations.

- User Management: Authorization and effective control mechanisms for multiple users are coordinates brought in the model.

### 8. Regulatory and Compliance Issues

- Data Privacy: The protocol also adheres to the key management policies by protecting participant’s information and encrypting it to prevent data protection acts violation.

- Industry Standards: The protocol is highly compatible with the existing standards of IoT.

### 9. Cost

- Low implementation Cost: As the usage of symmetric key encryption and light weight algorithm keep cost down in terms of implementing this protocol.

### 10. Environmental Factors

•Harsh environment: A significant factor for key management in harsh condition and the protocol even offers excellent secure storage systems.

## 6. Comparison Analysis

Assessment of LKDP-IoT decision-making process against existing key distribution protocols requires due consideration of efficiency, security and applicability. The following matrix reveals the advantages of LKDP-IoT.

**Table 3. Comparison Analysis of LKDP protocol with existing protocols.**

| **Feature** | **LKDP-IoT** | **Existing Protocols** |
|---|---|---|
| **Cryptographic Primitives** | Lightweight symmetric key algorithms | Often use a mix of symmetric and asymmetric algorithms. [4] |
| **Efficiency** | Optimized for low computational and energy usage | May involve more resource-intensive operations. [25] |
| **Scalability** | Designed to support a large number of devices with minimal performance degradation | Scalability may be limited by resource constraints and protocol design [22] |

| | | |
|---|---|---|
| **Key Management** | Secure key generation, distribution, update, and revocation | Varies; some protocols may have less efficient key management. [25] |
| **Authentication** | Mutual authentication using certificates and pre-shared keys | Typically involves more complex authentication mechanisms. [16] |
| **Resistance to Attacks** | Protection against common attacks (e.g., man-in-the-middle, replay) | some protocols may be vulnerable to specific attacks [13] |
| **Latency** | Low latency for real-time communication | Latency can be higher depending on the complexity of the protocol. [21] |
| **Usability** | Simple deployment with minimal configuration | Some protocols may be complex to deploy and manage. [2] |
| **Interoperability** | Complies with existing IoT standards and supports various devices | Varies; some may not be compatible with all IoT devices. [24] |
| **Cost** | Cost-effective in terms of implementation and maintenance | Costs can vary; some protocols may be more expensive to implement. [4] |
| **Regulatory Compliance** | Ensures data privacy and adheres to industry standards | Compliance may vary depending on the protocol. [49] |
| **Environmental Sustainability** | Energy-efficient operations | Energy efficiency may vary; some protocols may be more resource-intensive. [14] |

## 7. Future Work

There are several possible directions for further advance in the proposed Lightweight Key Distribution Protocol for IoT Devices (-IoT). Here are some key areas for exploration and enhancement:

### 1. Integration with Emerging LKDP Technologies

- Quantum-Resistant Cryptography: Investigate integrating quantum-resistant cryptographic algorithms to ensure long-term security against future quantum computing threats.
- Blockchain-Based Key Management: Explore the use of blockchain technology for decentralized and immutable key management and distribution.

### 2. Enhanced Security Features

- Advanced Threat Detection: Develop mechanisms for detecting and mitigating advanced threats such as side channel attacks and physical tampering.
- Adaptive Security Measures: Implement adaptive security features that can dynamically adjust based on detected threats or changes in the device environment.

### 3. Performance Optimization

- Protocol Efficiency: Optimize the protocol for even lower latency and reduced computational overhead, especially for ultra-low-power devices.

- Scalability Improvements: Enhance scalability to support larger networks and more dynamic environments, with improvements in handling high device churn rates.

### 4. Interoperability and Standardization

•IoT Standards Alignment: Work towards aligning LKDP-IoT with emerging IoT standards and frameworks to improve interoperability with other systems and devices.

•Cross-Protocol Compatibility: Develop methods to ensure compatibility with existing key distribution and cryptographic protocols to facilitate integration in diverse environments.

### 5. Usability and Deployment

•Automated Key Management: Implement automated systems for key generation, distribution, and renewal to simplify deployment and management.

•User-Friendly Interfaces: Develop user-friendly interfaces and tools for easier configuration and management of the protocol in various IoT ecosystems.

### 6. Real world tests and validation

- Field Trials: Invest heavily in consequent field trials that would prove, how well the indicated protocol performs and resists real IoT conditions.

- Case Studies: Based on industry-specific real-life applications (like smart home, industrial IoT), it is easier to grasp about problems and needs.

### 7. Energy Efficiency

- Even more improve the efficiency of the protocol regarding the energy use focusing specifically on the battery powered devices that have limited power supply capacity.
- Energy Harvesting Integration: Investigate integration with energy harvesting technologies to extend the operational lifespan of IoT devices.

### 6. Regulatory Compliance and Privacy

•Compliance with Regulations: Make certain, that Data protection regulations in the region change for the organization’s compliance. mating to legal requirements of the modern indemnity such as GDPR and CCPA.

- Privacy-Enhancing Features: Integrate components that would ensure its user’s privacy through the use of anonymization and data minimization measures.

### 7. Dynamic Adaptability

•Context-Aware Security: Agree Implement security solutions that relate to the context of the specific device and its context of operation within the network.

- Self-Healing Mechanisms: The system should be enabled to automatically rectify problems in key management that may happen due to mishandling of equipment or security compromise**.**

## 8. Adaptive capability with Machine Learning

•Anomaly Detection: Combine resources to apply machine learning algorithms to identify unusual occurrence regarding key distribution and communications.

- Predictive Maintenance: Use of predictive maintenance for timely check and update of the formulated protocol to reflect data and developments observed.

Future work on LKDP-IoT should focus on enhancing its security features, optimizing performance, improving interoperability, and adapting to emerging technologies and real-world conditions. Addressing these areas will help ensure that the protocol remains relevant, secure, and efficient as the IoT landscape evolves.

## 8. Conclusion

In this paper, therefore, we presented the Lightweight Key Distribution Protocol for IoT Devices (LKDP-IoT) as one that is suitable to provide for every unique feature of IoT networks. The proposed protocol effectively utilizes simple cryptographic techniques that do not put a strain on resource limitations by requiring a heavy weight computation, makes use of key distributing just to secure communication between two devices and ensures that the two communicating devices can securely exchange keys and set up an encrypted channel. Even though, the proposed protocol can be considered as the significant development in the area of IoT security, several directions for the further investigations have been identified, which are the protocol fine tuning for specific IoT structures and the protocol incorporation with other security approaches. Altogether, LKDP-IoT is a valuable contribution to the continuous process of IoT network protection that determines further development of more secure IoT systems.

**Author Contributions** All authors contributed equally.

### Declarations

**Conflict of Interest** The authors declare that there is no conflict of interest.

## References

[1] Hamalainen, Panu, et al. "Design and implementation of low-area and low-power AES encryption hardware core." 9th EUROMICRO conference on digital system design (DSD'06). IEEE, 2006.

[2] Zhao, Wenfeng, Yajun Ha, and Massimo Alioto. "AES architectures for minimum-energy operation and silicon demonstration in 65nm with lowest energy per encryption." 2015 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2015.

[3] Dao, Van-Lan, et al. "A compact, low power AES core on 180nm CMOS process." 2016 International Conference on IC Design and Technology (ICICDT). IEEE, 2016.

[4] Bogdanov, Andrey, et al. "PRESENT: An ultra-lightweight block cipher." Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. Springer Berlin Heidelberg, 2007.

[5] Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers." *Proceedings of the 52nd annual design automation conference*. 2015.

[6] Stern, Jacques, et al. "Flaws in applying proof methodologies to signature schemes." *Annual International Cryptology Conference*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002.

[7] Kunz, T., S. Okunick, and U. Pordesch. *Data structure for the security suitability of cryptographic algorithms (DSSC)*. No. rfc5698. 2009.

[8] Ma, Hongyang, and Bingquan Chen. "An authentication protocol based on quantum key distribution using decoy-state method for heterogeneous IoT." *Wireless Personal Communications* 91 (2016): 1335-1344.

[9] Ostad-Sharif, Arezou, et al. "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme." *Future Generation Computer Systems* 100 (2019): 882-892.

[10] Henson, Michael, and Stephen Taylor. "Memory encryption: A survey of existing techniques." ACM Computing Surveys (CSUR) 46.4 (2014): 1-26.

[11] Tang, Bowen, et al. "Eternal War in Software Security: A Survey of Control Flow Protection." 2016 7th International Conference on Education, Management, Computer and Medicine (EMCM 2016). Atlantis Press, 2017.

[12] Agrawal, Sarita, Manik Lal Das, and Javier Lopez. "Detection of node capture attack in wireless sensor networks." IEEE Systems Journal 13.1 (2018): 238-247.

[13] Amin, Ruhul, et al. "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment." *Future Generation Computer Systems* 78 (2018): 1005-1019.

[14] Chen, Chien-Ming, et al. "A secure blockchain-based group key agreement protocol for IoT." *The Journal of Supercomputing* 77 (2021): 9046-9068.

[15] Harbi, Yasmine, et al. "Enhanced authentication and key management scheme for securing data transmission in the internet of things." *Ad Hoc Networks* 94 (2019): 101948.

[16] Huang, Huihui, et al. "An efficient authentication and key agreement protocol for IoT-enabled devices in distributed cloud computing architecture." *EURASIP Journal on Wireless Communications and Networking* 2021.1 (2021): 150.

[17] Liu, An, and Peng Ning. "Tiny ECC: A configurable library for elliptic curve cryptography in wireless sensor networks." 2008 International Conference on Information Processing in Sensor Networks (ipsn 2008). IEEE, 2008.

[18] Omar, Sami, Raouf Ouni, and Saber Bouanani. "Hashing with elliptic curve L-functions."

Arithmetic of Finite Fields: 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings 4. Springer Berlin Heidelberg, 2012.

[19] Fazio, Nelly, and Antonio Nicolosi. "Cryptographic accumulators: Definitions, constructions and applications." Paper written for course at New York University: www. cs. nyu. edu/nicolosi/papers/accumulators. pdf 24 (2002).

[20] Lavanya, M., and V. Natarajan. "Lightweight key agreement protocol for IoT based on IKEv2." *Computers & Electrical Engineering* 64 (2017): 580-594.

[21] Nguyen, Kim Thuat, Maryline Laurent, and Nouha Oualha. "Survey on secure communication protocols for the Internet of Things." *Ad Hoc Networks* 32 (2015): 17-31.

[22] Porambage, Pawani, et al. "PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications." *International Journal of Distributed Sensor Networks* 10.7 (2014): 357430.

[23] Saied, Yosra Ben, et al. "Lightweight collaborative key establishment scheme for the Internet of Things." *Computer Networks* 64 (2014): 273-295.

[24] Ferrag, Mohamed Amine, et al. "Authentication protocols for internet of things: a comprehensive survey." Security and Communication Networks 2017 (2017).

[25] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.

[26] Sakiyama, Kazuo, et al. "Superscalar coprocessor for high-speed curve-based cryptography." International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[27] Von Maurich, Ingo, and Tim Güneysu. "Towards side-channel resistant implementations of QC-MDPC McEliece encryption on constrained devices." Post-Quantum Cryptography: 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings 6. Springer International Publishing,
2014.

[28] Wang, King-Hang, et al. "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags." *The Journal of Supercomputing* 74 (2018): 65-70.

[29] Chatterjee, Urbi, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. "A PUF-based secure communication protocol for IoT." ACM Transactions on Embedded Computing Systems (TECS) 16.3 (2017): 1- 25.

[30] Zhou, Lu, Chunhua Su, and Kuo-Hui Yeh. "A lightweight cryptographic protocol with certificateless signature for the Internet of Things." *ACM Transactions on Embedded Computing Systems (TECS)* 18.3 (2019): 1-10.

[31] Seyhan, Kübra, et al. "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security." *Journal of Information Security and Applications* 58 (2021): 102788.

[32] Chikouche, Noureddine, et al. "A privacy-preserving code-based authentication protocol for Internet of Things." The Journal of Supercomputing 75 (2019): 8231-8261.

[33] Al-Husainy, Mohammed Abbas Fadhil, Bassam Al-Shargabi, and Shadi Aljawarneh. "Lightweight cryptography system for IoT devices using DNA." Computers and Electrical Engineering 95 (2021): 107418.

[34] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey." Ad Hoc Networks 24 (2015): 264-287.

[35] Yan, Wei, et al. "PCB Chain: Lightweight reconfigurable blockchain primitives for secure IoT applications." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 28.10 (2020): 2196-2209.

[36] Mundhenk, Philipp, et al. "Security in automotive networks: Lightweight authentication and authorization." ACM Transactions on Design Automation of Electronic Systems (TODAES) 22.2 (2017): 1-27.

[37] Kamil, Ismaila, Oladayo Olakanmi, and Sunday Oyinlola Ogundoyin. "A secure and privacy-preserving lightweight authentication protocol for wireless communications." Information Security Journal: A Global Perspective 26.6 (2017): 287-304.

[38] Rao, Vidya, and K. V. Prema. "Light-weight hashing method for user authentication in Internet-of-Things." Ad Hoc Networks 89 (2019): 97-106.

[39] Santos, Maria LBA, et al. "FLAT: Federated lightweight authentication for the Internet of Things." Ad Hoc 1Networks 107 (2020): 102253.

[40] Cho, Jung-Sik, Young-Sik Jeong, and Sang Oh Park. "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol." Computers & Mathematics with Applications 69.1 (2015): 58-65.

[41] Das, Ashok Kumar, Sherali Zeadally, and Mohammad Wazid. "Lightweight authentication protocols for wearable devices." *Computers & Electrical Engineering* 63 (2017): 196-208.

[42] Veltri, Luca, et al. "A novel batch-based group key management protocol applied to the Internet of Things." *Ad Hoc Networks* 11.8 (2013): 2724-2737.

[43] Vijayakumar, Pandi, et al. "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks." *cluster computing* 20 (2017): 2439-2450.

[44] Abbasinezhad -sMood, Dariush, and Morteza Nikooghadam. "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications." Future Generation Computer Systems 84 (2018): 47-57.

[45] Liang, Wei, et al. "A double PUF-based RFID identity authentication protocol in service-centric internet of things environments." *Information Sciences* 503 (2019): 129-147.

[46] Salem, Fatty M., and Ruhul Amin. "A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS." Information sciences 527 (2020): 382-393.

[47] Siddhartha, Valmiki, Gurjot Singh Gaba, and Lavish Kansal. "A lightweight authentication protocol using implicit certificates for securing iot systems." Procedia Computer Science 167 (2020): 85-96.

[48] Sadhukhan, Dipanwita, et al. "A secure and privacy preserving lightweight authentication scheme for smart- grid communication using elliptic curve cryptography." Journal of Systems Architecture 114 (2021): 101938.

[49] Vinoth, R., and Lazarus Jegatha Deborah. "An efficient key agreement and authentication protocol for secure communication in industrial IoT applications." *Journal of Ambient Intelligence and Humanized Computing* 14.3 (2023): 1431-1443.

[50] Gu, Ke, et al. "Efficient and secure attribute-based signature for monotone predicates." Acta Informatica 54 (2017): 521-541.

[51] Dömösi, Pál, Géza Horváth, and Norbert Tihanyi. "Simple chain automaton random number generator for IoT devices." Acta Informatica 60.3 (2023): 317-329.

[52] Chen, Huiyan, and Chenchen Zhang. "Identity-based signatures in standard model." *Acta Informatica* 56.6 (2019): 471-486.

[53] Dolev, Shlomi, and Yin Li. "Secret-shared RAM indefinite private and secure RAM execution of perfectly unrevealed programs." *Acta Informatica* 60.1 (2023): 59-78.

[54] Khari, Manju, et al. "Securing data in Internet of Things (IoT) using cryptography and steganography techniques." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50.1 (2019): 73-80.

[55] Saračević, Muzafer H., et al. "Data encryption for internet of things applications based on catalan objects and two combinatorial structures." *IEEE Transactions on Reliability* 70.2 (2020): 819-830.

[56] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future generation computer systems* 82 (2018): 395-411.

[57] Schiller, Eryk, et al. "Landscape of IoT security." *Computer Science Review* 44 (2022): 100467.

[58] Buchanan, William J., Shancang Li, and Rameez Asif. "Lightweight cryptography methods." *Journal of Cyber Security Technology* 1.3-4 (2017): 187-201.

[59] Gupta, Shubham, and Sandeep Saxena. "Lightweight Cryptographic Techniques and Protocols for IoT." *Internet of Things: Security and Privacy in Cyberspace*. Singapore: Springer Nature Singapore, 2022. 55- 77.