A Comprehensive Review of Lightweight Key Exchange Protocols for Secure Internet of Things (IoT) Applications

Prachi Patel[1], Pooja Verma[2]

Dr. A.P.J. Abdul Kalam University, Indore

ABSTRACT

The rapid proliferation of the Internet of Things (IoT), Industrial Internet of Things (IIoT), edge computing, and next-generation communication networks has significantly increased the demand for secure and efficient key exchange mechanisms. Resource-constrained devices deployed in these environments possess limited computational capability, memory, bandwidth, and battery power, making conventional cryptographic algorithms such as RSA and traditional Diffie–Hellman unsuitable for practical implementation. Consequently, lightweight authentication and key agreement protocols have emerged as an active research area to provide secure communication while minimizing computational and communication overhead. This review presents a comprehensive analysis of the evolution of key exchange protocols, ranging from classical public-key cryptography to modern lightweight cryptographic techniques based on Elliptic Curve Cryptography (ECC), hash functions, Physical Unclonable Functions (PUFs), identity-based cryptography, blockchain, and edge-assisted authentication frameworks. The paper critically reviews recent authentication and key agreement protocols proposed for IoT, smart grids, wireless sensor networks, and edge computing environments, with emphasis on their security properties, computational complexity, communication cost, energy efficiency, scalability, and resistance against common cyberattacks including replay, impersonation, man-in-the-middle, insider, and session key disclosure attacks. Furthermore, a comparative analysis of existing protocols is presented to identify their strengths and limitations. Based on the findings, several open research challenges are highlighted, including lightweight post-quantum security, dynamic key management, privacy preservation, interoperability, and secure Integration with 5G/6G-enabled IoT ecosystems. Finally, future research directions are discussed to support the development of adaptive, scalable, and quantum-resilient lightweight key exchange protocols capable of meeting the security and performance requirements of next-generation resource-constrained networks.

INDEX TERMS

Internet of Things (IoT); Lightweight Cryptography; Key Exchange Protocol; Authenticated Key Agreement; Elliptic Curve Cryptography (ECC); Resource-Constrained Devices; Internet of Medical Things (IoMT); Smart Grid; Edge Computing; 5G/6G Networks; Mutual Authentication; Cyber security.

I. INTRODUCTION

A. 1. Introduction

The Internet of Things (IoT) has become one of the most influential technologies of the digital era, connecting billions of devices that continuously collect, process, and exchange data. Today, IoT applications are widely used in smart homes, healthcare, industrial automation, transportation, agriculture, and smart grid systems. The integration of edge computing and 5G/6G communication technologies has further expanded the capabilities of IoT by enabling faster data processing, lower latency, and real-time decision-making. While these advancements have improved the efficiency and intelligence of connected systems, they have also introduced significant security challenges.

One of the primary requirements for secure communication in IoT networks is the ability to establish a secret key between communicating devices. A key exchange protocol enables two legitimate entities to generate a common secret key over an insecure communication channel without exposing sensitive information to potential attackers. Once established, the shared key is used

to protect data confidentiality, ensure message integrity, and authenticate communicating devices. Therefore, the security of the entire communication process largely depends on the effectiveness of the key exchange mechanism.

Traditional public-key cryptographic algorithms, such as RSA and the Diffie–Hellman (DH) key exchange protocol, have been widely used to secure digital communications for decades. Although these techniques provide strong cryptographic security, they require considerable computational power, memory, and energy. Such requirements are often beyond the capabilities of IoT devices, which are typically designed with limited processing resources, restricted memory, and battery constraints. As the number of connected devices continues to increase, the need for lightweight security mechanisms has become more critical.

To overcome these limitations, researchers have proposed a variety of lightweight authentication and key exchange protocols that aim to reduce computational complexity while maintaining a high level of security. Among these, Elliptic Curve Cryptography (ECC) has emerged as one of the most promising approaches because it offers equivalent security with much smaller key sizes compared to traditional public-key algorithms. Other techniques, including hash-based authentication, identity-based cryptography, Physical Unclonable Functions (PUFs), blockchain-assisted security, and edge-assisted authentication frameworks, have also been investigated to address the unique requirements of resource-constrained environments.

Despite the considerable progress made in this area, designing an efficient and secure lightweight key exchange protocol remains a challenging task. Many existing schemes achieve lower computational costs but compromise on scalability, privacy, or resistance to sophisticated attacks. Furthermore, the emergence of heterogeneous IoT environments, edge computing, and quantum computing has introduced new security requirements that many current protocols are not fully equipped to address.

This review paper provides a comprehensive overview of lightweight key exchange protocols designed for resource-constrained IoT and next-generation communication networks. It examines the evolution of key exchange mechanisms, reviews recent authentication and key agreement protocols, and compares them based on security features, computational complexity, communication overhead, energy efficiency, and scalability. The paper also identifies key research gaps and discusses future directions for developing secure, lightweight, and adaptable key exchange solutions capable of supporting emerging technologies such as edge computing and 5G/6G networks.

A. 2. Background and Evolution of Key Exchange Protocols

The ability to exchange information securely has always been a fundamental requirement in computer networks. As communication technologies have evolved—from traditional wired networks to wireless systems, cloud computing, and the Internet of Things (IoT)—the need for efficient and reliable key exchange mechanisms has become increasingly important. Before any confidential information can be transmitted, the communicating parties must establish a shared secret key that can be used for encryption and authentication. This process is known as key exchange and forms the foundation of secure communication.

In the early years of cryptography, secure communication relied primarily on symmetric-key algorithms. These algorithms are computationally efficient because the same secret key is used for both encryption and decryption. However, their effectiveness depends on the secure distribution of the secret key before communication begins. As networks expanded and the number of connected users increased, securely managing and distributing secret keys became a major challenge,

particularly in large-scale and distributed environments.

A significant breakthrough came in 1976 when Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography. Their key exchange protocol demonstrated that two parties could establish a shared secret over an insecure communication channel without exchanging the secret key itself. This revolutionary idea solved one of the biggest challenges in cryptography and laid the foundation for modern secure communication systems. It also inspired the development of several public-key algorithms, including RSA and later Elliptic Curve Cryptography (ECC).

Although these public-key techniques provide strong security, they are computationally demanding. Algorithms such as RSA and the classical Diffie–Hellman protocol require large key sizes and complex mathematical operations, resulting in higher processing time, greater memory usage, and increased energy consumption. While these limitations are acceptable for desktop computers and servers, they present significant challenges for IoT devices, wireless sensor networks, and embedded systems, where processing power, storage capacity, and battery life are often limited.

To address these challenges, researchers introduced Elliptic Curve Cryptography (ECC), which provides the same level of security as traditional public-key algorithms while using much smaller key sizes. The reduced computational and communication overhead makes ECC particularly suitable for resource-constrained devices. As a result, ECC has become one of the most widely adopted cryptographic techniques for lightweight authentication and key agreement protocols.

In recent years, the rapid growth of IoT, Industrial IoT (IIoT), edge computing, smart grids, and 5G/6G communication networks has accelerated research into lightweight cryptography. Modern key exchange protocols no longer rely on a single cryptographic technique. Instead, they combine ECC with hash functions, identity-based cryptography, Physical Unclonable Functions (PUFs), blockchain technology, and edge-assisted authentication to provide stronger security while maintaining low computational and communication costs. These approaches are designed to meet the unique requirements of resource-constrained environments by offering efficient mutual authentication, secure session key establishment, user privacy, and resistance to common cyberattacks.

Understanding how key exchange protocols have evolved provides valuable insight into the strengths and limitations of existing approaches. It also highlights why lightweight cryptographic solutions have become essential for securing modern IoT and next-generation communication networks. The following sections discuss the major key exchange techniques, beginning with classical cryptographic protocols and progressing toward contemporary lightweight authentication mechanisms.

1) 2.1 Classical Key Exchange Protocols

The development of secure key exchange protocols marks one of the most significant milestones in the history of modern cryptography. Before the introduction of public-key cryptography, secure communication relied almost entirely on symmetric-key algorithms, where both communicating parties shared the same secret key for encryption and decryption. Although symmetric encryption algorithms are fast and computationally efficient, they require the secret key to be exchanged securely before communication begins. In small networks this approach is manageable, but as the number of users and connected devices increases, secure key distribution becomes increasingly complex.

The introduction of the Diffie–Hellman (DH) key exchange protocol in 1976 fundamentally changed the field of cryptography. For the first time, two communicating parties could establish a shared secret over an insecure communication channel without transmitting the secret key itself. The protocol is based on the computational difficulty of

solving the discrete logarithm problem, making it computationally infeasible for an attacker to derive the shared secret from publicly exchanged information. This breakthrough became the foundation of modern public-key cryptography and remains one of the most influential contributions to secure communications.

Following the success of Diffie–Hellman, the RSA algorithm was introduced as another landmark public-key cryptographic technique. Unlike Diffie–Hellman, which focuses on key establishment, RSA supports both encryption and digital signatures, making it suitable for authentication as well as secure communication. Its security relies on the computational difficulty of factoring large prime numbers. Because of its robustness and widespread standardization, RSA has been extensively used in secure web communications, digital certificates, email security, and Public Key Infrastructure (PKI).

Despite their strong security guarantees, both Diffie–Hellman and RSA present practical limitations when deployed in resource-constrained environments. Their security depends on large key sizes and computationally intensive arithmetic operations, which increase processing time, memory usage, communication overhead, and energy consumption. These characteristics make them less suitable for devices such as wireless sensors, RFID tags, wearable devices, and IoT nodes that operate with limited hardware resources and battery capacity.

As IoT applications expanded and billions of low-power devices became interconnected, researchers recognized the need for more efficient cryptographic solutions. The challenge was to preserve the security advantages of public-key cryptography while reducing computational and communication costs. This requirement led to the development of Elliptic Curve Cryptography (ECC), which achieves comparable security with significantly smaller key sizes and lower computational overhead. Consequently, ECC has become the preferred public-key technique for many lightweight authentication and key agreement protocols designed for modern IoT and next-generation communication networks.

Although classical key exchange protocols continue to play an essential role in cybersecurity, they also provide an important benchmark for evaluating newer lightweight approaches. Understanding their design principles, advantages, and limitations helps explain the evolution of secure communication mechanisms and highlights the motivation for developing lightweight cryptographic protocols tailored to resource-constrained environments.

1) 2.2 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) was introduced to overcome the limitations of traditional public-key cryptographic algorithms, particularly in environments where computing resources are limited. As the number of connected devices increased and applications expanded to wireless sensor networks, IoT, and embedded systems, it became evident that conventional algorithms such as RSA and Diffie–Hellman required more computational power, memory, and energy than many devices could provide. ECC emerged as an efficient alternative by offering the same level of security while using significantly smaller key sizes.

The security of ECC is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is considered computationally infeasible to solve using current classical computing techniques. Instead of relying on large integer factorization or discrete logarithms in finite fields, ECC performs cryptographic operations on points defined over an elliptic curve. This mathematical foundation allows ECC to achieve strong security with much shorter keys. For example, a 256-bit ECC key provides a security level comparable to a 3072-bit RSA key. Smaller key sizes reduce storage requirements, communication overhead, and computational complexity, making ECC particularly suitable for resource-constrained devices.

One of the main advantages of ECC is its efficiency. Shorter keys require less memory for storage and fewer bits for transmission, resulting in lower communication costs. In addition, ECC operations consume less processing time and energy compared to traditional public-key algorithms. These characteristics are especially valuable for battery-powered devices such as wireless sensors, wearable devices, RFID tags, and smart meters, where energy conservation directly affects device lifetime.

Because of these advantages, ECC has become one of the most widely adopted cryptographic techniques for authentication and key agreement in IoT environments. Many lightweight security protocols combine ECC with cryptographic hash functions and symmetric encryption to provide mutual authentication, secure session key establishment, and data confidentiality while maintaining low computational overhead. Recent studies have also integrated ECC with identity-based cryptography, blockchain technology, edge computing, and Physical Unclonable Functions (PUFs) to enhance security and improve system scalability.

Despite its advantages, ECC is not without challenges. Operations such as scalar multiplication remain computationally intensive for extremely constrained devices. In addition, implementing ECC securely requires protection against side-channel attacks, including timing, power analysis, and fault injection attacks. Selecting appropriate elliptic curve parameters and ensuring secure implementation are therefore essential for maintaining the expected level of security.

Overall, ECC represents a major advancement in public-key cryptography and has become the foundation of many modern lightweight authentication and key exchange protocols. Its ability to balance strong security with computational efficiency makes it particularly well suited for emerging applications such as IoT, Industrial IoT (IIoT), smart grids, edge computing, and next-generation 5G/6G communication networks. Consequently, most recent lightweight key exchange protocols reviewed in this paper are either directly based on ECC or incorporate ECC as a core component of their security framework.

1) 2.3 Lightweight Cryptography

The rapid expansion of the Internet of Things (IoT) has brought millions of low-power devices into everyday applications, ranging from smart homes and healthcare systems to industrial automation and intelligent transportation. Unlike traditional computers and servers, these devices operate with limited processing power, memory, battery capacity, and communication bandwidth. As a result, implementing conventional cryptographic algorithms on such devices often leads to higher computational delays, increased energy consumption, and reduced system performance. These limitations have driven the development of lightweight cryptography, which aims to provide strong security while making efficient use of available resources.

Lightweight cryptography focuses on designing cryptographic algorithms and protocols that require less computation, smaller memory, and lower communication overhead without compromising essential security requirements. Rather than replacing conventional cryptographic techniques,

lightweight cryptography complements them by addressing the unique needs of resource-constrained environments. The primary objective is to achieve an appropriate balance between security, efficiency, and implementation cost.

An effective lightweight cryptographic solution is expected to possess several key characteristics. First, it should have low computational complexity so that encryption, decryption, and authentication operations can be completed quickly even on low-end processors. Second, it should require minimal memory, allowing the algorithm to run efficiently on devices with limited RAM and storage. Third, energy efficiency is essential because many IoT devices operate on batteries or energy-harvesting mechanisms and are expected to function for extended periods without frequent maintenance. Finally, lightweight protocols should minimize communication overhead by reducing the amount of data exchanged during authentication and key establishment, thereby conserving both bandwidth and power.

Lightweight cryptography can be broadly classified into two categories: lightweight symmetric cryptography and lightweight public-key cryptography. Symmetric cryptographic algorithms are generally faster and consume fewer computational resources because the same secret key is used for both encryption and decryption. Lightweight block ciphers such as PRESENT, GIFT, LED, SIMON, SPECK, and PRINCE have been specifically developed for constrained devices. Similarly, lightweight hash functions including SPONGENT, PHOTON, and QUARK provide efficient mechanisms for ensuring data integrity and authentication while requiring minimal hardware resources.

Although symmetric cryptography is highly efficient, it introduces the challenge of secure key distribution. This limitation has encouraged researchers to develop lightweight public-key cryptographic techniques that simplify key management while maintaining acceptable performance. Among these approaches, Elliptic Curve Cryptography (ECC) has emerged as the most widely adopted solution because it provides strong security with relatively small key sizes. Recent protocols also combine ECC with identity-based cryptography, Physical Unclonable Functions (PUFs), blockchain technology, and edge computing to further improve authentication efficiency and strengthen resistance against evolving cyber threats.

Despite the significant progress achieved in lightweight cryptography, designing secure and efficient protocols remains a challenging task. Reducing computational complexity often requires trade-offs that may affect security, scalability, or interoperability. Moreover, lightweight protocols must remain resilient against attacks such as replay attacks, impersonation attacks, man-in-the-middle attacks, side-channel attacks, and session key compromise while operating within strict resource constraints. Achieving this balance between efficiency and robust security continues to be one of the most important research challenges in modern cryptography.

As IoT ecosystems continue to grow and support increasingly diverse applications, lightweight cryptography has become a fundamental building block for secure communication. Its ability to deliver strong security with minimal resource consumption has made it indispensable for IoT, wireless sensor networks, smart grids, healthcare systems, edge computing, and emerging 5G/6G communication environments. Consequently, most recent authentication and key exchange protocols are built upon lightweight cryptographic principles to meet the demanding requirements of next-generation networks.

1) 2.4 Requirements of Lightweight Key Exchange Protocols

The increasing adoption of IoT devices and next-generation communication technologies has made the design of lightweight key exchange protocols more important than ever. Unlike conventional computer systems, IoT devices

operate under strict resource constraints while often communicating over open and potentially insecure networks. As a result, an effective key exchange protocol must not only establish a secure session key but also ensure that this is achieved with minimal computational and communication overhead. Designing such protocols requires balancing strong security with the limited capabilities of resource-constrained devices.

One of the most important requirements of any key exchange protocol is mutual authentication. Before exchanging sensitive information, both communicating entities must verify each other's identity to ensure that they are communicating with legitimate devices. Mutual authentication helps prevent unauthorized access and protects the network from impersonation attacks, where an attacker pretends to be a trusted device.

Another essential requirement is confidentiality, which ensures that sensitive information remains inaccessible to unauthorized users. During the key exchange process, secret keys and authentication messages must be protected from eavesdroppers. Once a secure session key has been established, all subsequent communication should remain encrypted to prevent data leakage.

Maintaining data integrity is equally important. Devices should be able to verify that transmitted messages have not been altered during communication. Even a small modification to authentication data or exchanged keys can compromise the entire communication process. Therefore, lightweight protocols commonly employ cryptographic hash functions and message authentication techniques to detect any unauthorized modifications.

Modern key exchange protocols are also expected to provide forward secrecy. This property ensures that the compromise of a long-term private key does not expose previously established session keys. Even if an attacker gains access to a device's secret key at a later stage, earlier communication sessions should remain protected. Forward secrecy has become a standard security requirement for modern authentication protocols, particularly in applications involving sensitive personal or industrial data.

Privacy protection has emerged as another important consideration in IoT environments. Many smart devices continuously exchange personal or location-based information, making users vulnerable to tracking and profiling. To address this issue, lightweight authentication protocols should preserve user anonymity and device privacy by concealing permanent identities during communication. Temporary identities or pseudonyms are commonly used to reduce the risk of user tracking while maintaining secure authentication.

Because IoT deployments often consist of thousands or even millions of connected devices, scalability is another critical design requirement. A lightweight key exchange protocol should continue to operate efficiently as the network grows without causing excessive delays or increasing communication costs. Similarly, low computational complexity and minimal memory requirements are essential for devices with limited processing capability and storage. Efficient algorithms extend battery life and improve the overall performance of constrained devices.

In addition to these functional requirements, modern protocols must demonstrate resilience against a wide range of cyberattacks. They should be capable of resisting replay attacks, man-in-the-middle attacks, impersonation attacks, session key disclosure attacks, password guessing attacks, insider attacks, and denial-of-service attacks. Formal security verification and performance evaluation are therefore important components of protocol design, providing confidence that the proposed scheme satisfies both security and efficiency requirements.

Overall, the effectiveness of a lightweight key exchange protocol depends on its ability to provide strong security while consuming minimal

computational resources. Achieving this balance remains one of the primary research challenges in IoT security. The following section reviews existing lightweight authentication and key exchange protocols proposed in the literature and compares their strengths, limitations, and suitability for resource-constrained environments.

A. 3. Review of Lightweight Key Exchange Protocols

The growing adoption of IoT and resource-constrained devices has led to the development of numerous lightweight authentication and key exchange protocols over the past two decades. These protocols differ in their cryptographic techniques, security objectives, and performance characteristics. While some approaches focus on minimizing computational cost, others prioritize stronger security, user privacy, or scalability. As a result, no single protocol is suitable for every application, and selecting an appropriate solution depends largely on the requirements of the target environment.

Researchers have proposed a variety of lightweight key exchange mechanisms to address the challenges associated with limited computational resources, memory constraints, and energy consumption. Early studies mainly concentrated on reducing the complexity of traditional public-key cryptography, whereas more recent research has explored hybrid approaches that combine multiple cryptographic techniques to achieve improved security and efficiency. These developments reflect the growing demand for secure communication in emerging applications such as smart healthcare, intelligent transportation, industrial automation, smart grids, and edge computing.

Based on the underlying cryptographic techniques, existing lightweight key exchange protocols can be broadly classified into several categories. The most common approaches include Elliptic Curve Cryptography (ECC)-based protocols, hash-based authentication schemes, identity-based cryptographic protocols, Physical Unclonable Function (PUF)-based authentication mechanisms, blockchain-assisted key management schemes, and hybrid authentication frameworks. Each category offers distinct advantages while also presenting specific challenges related to computational complexity, communication overhead, implementation cost, and resistance to security attacks.

Among these approaches, ECC-based protocols have received considerable attention because they provide strong security using relatively small key sizes. Their ability to reduce computation time and communication overhead makes them particularly suitable for IoT devices with limited processing capabilities. Consequently, many recent authentication protocols incorporate ECC as the primary mechanism for secure key establishment while integrating lightweight hash functions and symmetric encryption to improve overall efficiency.

At the same time, researchers have recognized that security alone is not sufficient for modern IoT environments. Contemporary protocols are increasingly designed to satisfy additional requirements such as user anonymity, forward secrecy, resistance to replay and impersonation attacks, and secure operation in heterogeneous networks. Some studies have also incorporated edge computing, blockchain technology, and machine learning to enhance authentication efficiency, reduce latency, and improve trust management in distributed environments.

Although substantial progress has been achieved, several limitations remain. Many existing protocols perform well under specific conditions but experience challenges when deployed in large-scale IoT systems. Issues such as high communication overhead, limited scalability, increased authentication delay, and vulnerability to emerging cyber threats continue to motivate further research. These limitations highlight the need for lightweight key exchange protocols that can simultaneously provide strong security, efficient performance, and adaptability to next-generation communication networks.

The following subsections present a detailed review of the major categories of lightweight key exchange protocols. Each category is discussed in terms of its working principles, recent developments, strengths, limitations, and suitability for different IoT applications.

1) 3.1 ECC-Based Lightweight Key Exchange Protocols

Elliptic Curve Cryptography (ECC) has become the preferred public-key cryptographic technique for lightweight authentication and key exchange in resource-constrained environments. Its widespread adoption is largely due to its ability to provide strong security using much smaller key sizes than conventional algorithms such as RSA. This makes ECC particularly attractive for IoT devices, where processing power, memory, and battery life are often limited. By reducing both computational and communication costs, ECC enables secure communication without placing excessive demands on device resources.

The introduction of ECC marked an important milestone in the development of efficient public-key cryptography. Early research demonstrated that ECC could achieve security comparable to traditional public-key algorithms while requiring significantly shorter keys. This improvement encouraged researchers to explore its use in applications where conventional cryptographic methods were considered too resource-intensive. As IoT technologies evolved, ECC quickly became a core component of lightweight authentication and key agreement protocols.

Over the years, numerous ECC-based protocols have been proposed to address the diverse security requirements of IoT applications. Many of these protocols combine ECC with lightweight cryptographic techniques such as hash functions and symmetric encryption to improve efficiency while maintaining a high level of security. These hybrid designs reduce the number of computationally expensive elliptic curve operations, resulting in faster authentication, lower communication overhead, and reduced energy consumption. Such improvements are particularly valuable for battery-powered devices that must operate continuously for long periods.

The flexibility of ECC has also allowed it to be adapted to a wide range of application domains. In smart healthcare, it helps protect sensitive patient information during communication between medical devices and healthcare providers. In smart grids, ECC-based protocols secure data exchange between smart meters and utility control centres. Similarly, in edge computing environments, lightweight ECC schemes enable rapid authentication between edge servers and connected devices while minimizing communication delays. These applications demonstrate the versatility of ECC in meeting the security demands of different IoT ecosystems.

Despite its many advantages, ECC is not a complete solution to every security challenge. The scalar multiplication operation, which forms the basis of ECC computations, can still be computationally demanding for extremely low-power devices. In addition, secure implementation is just as important as the underlying mathematical algorithm. Poor implementation practices may expose systems to side-channel attacks, including timing attacks, power analysis, and fault injection attacks. Researchers have therefore focused not only on improving the efficiency of ECC-based protocols but also on strengthening their practical security against implementation-level threats.

Another important direction in recent research has been the integration of ECC with emerging technologies such as blockchain, Physical Unclonable Functions (PUFs), identity-based cryptography, and edge computing. These hybrid approaches aim to enhance privacy, simplify key management, and improve scalability while preserving the lightweight characteristics required for IoT devices. As IoT networks continue to expand, such combinations are expected to play an

increasingly important role in developing secure and efficient authentication mechanisms.

Overall, the existing literature clearly indicates that ECC provides an effective balance between security and efficiency, making it the foundation of many modern lightweight key exchange protocols. Although current ECC-based schemes have achieved significant progress, challenges related to scalability, implementation security, and support for future technologies such as quantum computing remain active areas of research. Addressing these challenges will be essential for developing the next generation of lightweight authentication protocols capable of securing increasingly complex IoT environments.

Table 1. Summary of Representative ECC-Based Lightweight Key Exchange Protocols

Authors	Year	Application	Key Technique	Major Strength	Limitation
Miller	1985	Public-Key Cryptography	ECC	Introduced ECC	Mathematical framework only
Liu & Ning	2008	Wireless Sensor Networks	Tiny ECC	Low memory implementation	Limited scalability
Lee & Lee	2020	IoT	ECC and Hash	Efficient mutual authentication	Communication overhead in large networks
Chen et al.	2023	Smart Grid	ECC and Lightweight Auth	Strong security with low	Limited real-world validation
			entication	computation	
Wang et al.	2023	Edge Computing	ECC and Anonymous Authentication	Privacy preservation and low latency	Higher protocol complexity

1) 3.2 Hash-Based Authentication Protocols

Hash-based authentication protocols have emerged as an effective solution for securing communication in resource-constrained environments where computational efficiency is a primary concern. Unlike public-key cryptographic algorithms, cryptographic hash functions require significantly less processing power and memory, making them well suited for IoT devices, wireless sensor networks, RFID systems, and other low-power applications. Their simplicity and speed have made them an important component of many modern lightweight authentication schemes.

A cryptographic hash function transforms an input message of any length into a fixed-length output, commonly referred to as a hash value or message digest. An ideal hash function is computationally efficient while exhibiting properties such as one-way computation, collision resistance, and resistance to preimage attacks. These characteristics enable hash functions to verify data integrity and authenticate messages without revealing sensitive information.

Many lightweight authentication protocols rely on hash functions to reduce computational overhead during the authentication process. Instead of performing expensive public-key operations repeatedly, devices generate and verify hash values to authenticate each other and establish secure communication. This significantly decreases processing time, communication delay, and energy consumption, making hash-based schemes

particularly suitable for battery-powered devices that operate continuously in dynamic environments.

Over the past decade, researchers have proposed several hash-based authentication protocols for IoT applications. These protocols are commonly designed to provide mutual authentication, secure session key establishment, and message integrity while minimizing resource consumption. Many schemes also combine hash functions with symmetric encryption or Elliptic Curve Cryptography (ECC) to strengthen security without introducing substantial computational overhead. Such hybrid approaches have shown improved efficiency while maintaining resistance to common security threats.

One of the major strengths of hash-based authentication is its ability to deliver fast authentication with minimal computational cost. Since hash functions require relatively simple mathematical operations, they are considerably more energy efficient than traditional public-key algorithms. This advantage makes them particularly useful for applications where devices have limited battery capacity or where frequent authentication is required. In addition, the reduced communication overhead contributes to faster response times and improved network performance.

Despite these advantages, hash-based authentication protocols also have certain limitations. Because hash functions alone cannot perform secure key exchange, many protocols depend on additional cryptographic mechanisms to establish shared session keys. Furthermore, if protocol design is inadequate, systems may remain vulnerable to replay attacks, impersonation attacks, and offline password guessing attacks. Consequently, recent research has focused on combining hash functions with complementary security techniques to improve both efficiency and resilience against sophisticated cyber threats.

Overall, hash-based authentication has become an essential component of lightweight security solutions for IoT environments. Its low computational requirements, fast execution, and efficient use of system resources make it an attractive choice for resource-constrained devices. However, achieving an effective balance between simplicity, strong security, and scalability remains an active area of research. As IoT networks continue to expand, future authentication protocols are expected to integrate hash functions with advanced cryptographic techniques to provide more secure, flexible, and efficient key exchange mechanisms.

1) 3.3 Identity-Based Authentication Protocols

As IoT networks continue to expand, managing cryptographic keys and digital certificates has become increasingly challenging. In large-scale environments consisting of thousands or even millions of interconnected devices, traditional Public Key Infrastructure (PKI) can introduce significant communication overhead, complex certificate management, and higher deployment costs. To address these challenges, researchers have explored identity-based cryptography as an alternative approach that simplifies authentication while maintaining a high level of security.

The concept of identity-based cryptography allows a user's unique identity, such as an email address, device identifier, or network address, to serve as the public key. This eliminates the need for digital certificates, reducing the complexity associated with certificate generation, storage, verification, and revocation. As a result, identity-based authentication protocols are particularly attractive for IoT environments where devices have limited computational resources and network connectivity.

In recent years, numerous identity-based authentication and key agreement protocols have been proposed for IoT applications. These protocols are designed to provide secure mutual authentication while reducing computational complexity and communication overhead. Many schemes combine identity-based cryptography with

lightweight techniques such as cryptographic hash functions and Elliptic Curve Cryptography (ECC) to achieve both efficiency and strong security. This combination enables devices to establish secure session keys with fewer computational steps than conventional certificate-based systems.

One of the key advantages of identity-based authentication is its simplified key management. Since public keys are directly derived from device identities, there is no need to distribute or validate certificates during the authentication process. This reduces communication delays and makes the authentication procedure more efficient, especially in dynamic IoT environments where devices frequently join or leave the network. The simplified architecture also lowers implementation costs and improves scalability.

Another important benefit is the flexibility of identity-based protocols across different application domains. They have been successfully applied in smart healthcare, industrial IoT, intelligent transportation systems, cloud-assisted IoT, and smart grid networks. In these applications, identity-based authentication supports secure communication while minimizing the processing burden on constrained devices. Many recent protocols also incorporate anonymous identities or pseudonyms to enhance user privacy and prevent device tracking.

Despite these advantages, identity-based authentication schemes are not without limitations. Most protocols rely on a trusted authority, commonly referred to as the Private Key Generator (PKG), which is responsible for generating users' private keys. This creates a key escrow problem because the trusted authority has knowledge of every user's private key. If the PKG is compromised, the security of the entire system may be affected. Researchers have proposed certificateless and distributed identity-based cryptographic approaches to reduce this dependency and improve overall system security.

Recent research has focused on strengthening identity-based authentication by integrating it with emerging technologies such as blockchain, edge computing, and Physical Unclonable Functions (PUFs). These hybrid approaches aim to improve privacy, reduce trust dependency, and enhance resistance against attacks such as impersonation, replay, and man-in-the-middle attacks. As IoT ecosystems continue to evolve, identity-based authentication remains an active area of research because of its ability to simplify key management while providing efficient and secure communication.

Overall, identity-based authentication protocols offer an attractive balance between security, efficiency, and ease of deployment. Their reduced certificate management overhead makes them well suited for large-scale IoT environments, although challenges related to key escrow and trusted authority management still require further investigation. Ongoing research is expected to address these issues and develop more scalable and privacy-preserving authentication mechanisms for future IoT applications.

1) 3.6 AI-Enabled and Hybrid Authentication Protocols

The rapid evolution of IoT, edge computing, and next-generation communication networks has introduced new security challenges that cannot always be addressed by conventional authentication techniques alone. As IoT ecosystems become larger and more dynamic, researchers have started combining multiple security technologies to develop authentication protocols that are not only secure but also adaptive and intelligent. This has led to the emergence of AI-enabled and hybrid authentication protocols, which integrate cryptographic methods with artificial intelligence, machine learning, blockchain, edge computing, and other advanced technologies.

Unlike traditional authentication schemes that rely on predefined rules, AI-based approaches can analyse network behaviour, identify unusual

activities, and detect potential attacks in real time. Machine learning algorithms are increasingly being used to recognize abnormal communication patterns, detect compromised devices, and improve intrusion detection systems. By learning from historical data, these models can identify threats that may not be detected through conventional rule-based security mechanisms. This ability makes AI particularly valuable in large-scale IoT environments where manual monitoring is impractical.

In addition to artificial intelligence, many researchers have proposed hybrid authentication frameworks that combine multiple cryptographic techniques to achieve better security and performance. For example, Elliptic Curve Cryptography (ECC) is frequently integrated with lightweight hash functions, blockchain, Physical Unclonable Functions (PUFs), or identity-based cryptography. Such combinations leverage the strengths of different techniques while compensating for their individual limitations. As a result, hybrid protocols often provide stronger authentication, improved privacy protection, and more efficient key management than approaches based on a single cryptographic method.

Edge computing has also become an important component of modern authentication frameworks. Instead of sending every authentication request to a central cloud server, edge devices perform security operations closer to the data source. This reduces communication latency, decreases network congestion, and enables faster authentication decisions. Combining edge computing with lightweight cryptographic techniques allows IoT devices to maintain secure communication while meeting the real-time requirements of applications such as autonomous vehicles, industrial automation, and smart healthcare.

Although AI-enabled and hybrid authentication protocols offer several advantages, they also present new challenges. Artificial intelligence models require high-quality training data and sufficient computational resources, which may not always be available in constrained IoT environments. Similarly, integrating multiple security technologies can increase implementation complexity and make protocols more difficult to deploy and maintain. Ensuring interoperability among devices from different manufacturers and protecting AI models from adversarial attacks remain important areas of ongoing research.

Despite these challenges, current research indicates that hybrid approaches represent a promising direction for future IoT security. Rather than relying on a single authentication mechanism, they combine complementary technologies to provide stronger security, improved scalability, and greater resilience against evolving cyber threats. As IoT networks continue to expand and support increasingly complex applications, AI-enabled and hybrid authentication protocols are expected to play a key role in securing next-generation communication systems.

The review of existing literature demonstrates that each category of lightweight key exchange protocol offers distinct advantages while addressing specific security requirements. However, no single approach fully satisfies all the demands of modern IoT environments. This observation highlights the importance of identifying the strengths and limitations of current solutions, which forms the basis for the comparative analysis presented in the next section.

A. 4. Comparative Analysis of Existing Lightweight Key Exchange Protocols

Over the past two decades, researchers have proposed numerous lightweight authentication and key exchange protocols to address the security challenges of resource-constrained environments. Although these protocols share the common objective of establishing secure communication with minimal resource consumption, they differ considerably in their design, security features, and overall performance. Some prioritize computational efficiency, while others focus on enhancing privacy, reducing communication overhead, or improving resistance to cyberattacks.

As a result, evaluating these protocols from multiple perspectives is essential for understanding their practical suitability for different IoT applications.

A comparative analysis provides a clearer picture of how existing protocols have evolved and where they stand in terms of security and efficiency. Instead of examining each protocol individually, it enables researchers to identify common design patterns, assess their strengths and limitations, and recognize the trade-offs involved in different cryptographic approaches. Such an analysis also helps determine which techniques are most appropriate for specific application domains, including wireless sensor networks, smart healthcare, industrial IoT, smart grids, and edge computing.

One of the most significant observations from the existing literature is the growing preference for Elliptic Curve Cryptography (ECC). Because ECC offers strong security with relatively small key sizes, many recent protocols use it as the foundation for secure key establishment. These protocols are often combined with lightweight hash functions, symmetric encryption, or identity-based cryptography to further reduce computational complexity and communication costs. More recent studies have also integrated blockchain technology, Physical Unclonable Functions (PUFs), and edge computing to improve trust management, privacy, and scalability.

While security remains the primary objective of any authentication protocol, performance has become equally important in resource-constrained environments. IoT devices often operate with limited battery capacity, processing power, memory, and communication bandwidth. Consequently, modern lightweight protocols are expected to achieve strong security without introducing excessive computational delay or energy consumption. Researchers therefore evaluate protocols using both security-related metrics, such as resistance to replay attacks, impersonation attacks, man-in-the-middle attacks, and forward secrecy, and performance-related metrics, including computation time, communication overhead, memory requirements, and energy efficiency.

The comparative analysis presented in this review is based on representative lightweight key exchange protocols reported in recent literature. Each protocol is evaluated using a common set of security and performance criteria to provide a balanced assessment of its capabilities. This structured comparison not only highlights the progress achieved in lightweight cryptography but also identifies the challenges that continue to influence protocol design.

The findings indicate that no single protocol satisfies all security and performance requirements simultaneously. Protocols offering stronger security often require additional computation or communication, whereas highly efficient schemes may provide fewer security features or rely on stronger assumptions. These trade-offs demonstrate that protocol selection depends on the intended application and its specific operational requirements. The following tables summarize the characteristics of representative lightweight key exchange protocols and provide a detailed comparison of their security properties and performance.

A. 5. Research Gaps and Future Research Directions

The comparative analysis of existing lightweight key exchange protocols reveals that significant progress has been made in developing secure and efficient authentication mechanisms for IoT and other resource-constrained environments. Modern protocols provide stronger security, lower computational overhead, and better energy efficiency than traditional cryptographic approaches. Nevertheless, the rapid evolution of IoT ecosystems, edge computing, and next-generation communication networks continues to introduce new challenges that existing solutions do not fully address.

One of the most noticeable research gaps is the lack of a protocol that can simultaneously achieve high security, low computational complexity, and strong scalability. Many protocols are designed for specific applications or network architectures and perform well under controlled conditions. However, when deployed in large-scale IoT environments with thousands of interconnected devices, issues such as communication delays, increased authentication overhead, and key management complexity become more evident. Developing protocols that remain efficient as network size grows is therefore an important research priority.

Privacy protection also remains an active area of research. Although many recent authentication schemes support anonymous communication through temporary identities or pseudonyms, protecting user privacy in highly dynamic IoT environments is still challenging. Location tracking, identity disclosure, and traffic analysis continue to threaten user confidentiality, particularly in applications such as smart healthcare and intelligent transportation systems. Future authentication protocols should strengthen privacy-preserving mechanisms while maintaining lightweight operation.

Another important challenge is preparing lightweight cryptographic systems for the emergence of quantum computing. Most existing protocols rely on mathematical problems such as integer factorization or the elliptic curve discrete logarithm problem, which could become vulnerable to sufficiently powerful quantum computers. Although practical quantum attacks are not yet a reality for most IoT systems, researchers have already begun investigating lightweight post-quantum cryptographic techniques. Designing quantum-resistant key exchange protocols that remain suitable for resource-constrained devices represents one of the most promising directions for future research.

Interoperability is another issue that deserves greater attention. IoT ecosystems typically consist of devices from different manufacturers that use diverse communication standards and hardware platforms. Ensuring that lightweight authentication protocols operate efficiently across heterogeneous environments without compromising security remains a significant challenge. Future research should focus on developing standardized and interoperable authentication frameworks capable of supporting seamless communication among diverse IoT devices.

The increasing adoption of edge computing and artificial intelligence also presents new opportunities for improving authentication mechanisms. Edge-assisted security architectures can reduce authentication latency by processing requests closer to the source of data, while artificial intelligence can help detect abnormal behaviour, identify compromised devices, and respond to evolving cyber threats. Integrating these technologies with lightweight cryptographic techniques may lead to authentication systems that are both adaptive and computationally efficient.

Another promising research direction involves hybrid security frameworks that combine multiple technologies rather than relying on a single cryptographic approach. Recent studies have shown that integrating Elliptic Curve Cryptography (ECC), Physical Unclonable Functions (PUFs), blockchain, identity-based cryptography, and lightweight hash functions can improve both security and efficiency. However, balancing the benefits of these technologies while avoiding unnecessary computational overhead remains an open research challenge.

Overall, the literature suggests that future lightweight key exchange protocols should not only focus on reducing computational cost but also address emerging requirements such as quantum resistance, privacy preservation, scalability, interoperability, and intelligent threat detection. Achieving this balance will be essential for securing future IoT, Industrial IoT, edge computing, and 6G communication networks. Continued research in these areas will contribute to

the development of authentication protocols that are secure, efficient, scalable, and capable of meeting the evolving demands of next-generation digital infrastructures.

References

1. W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.
2. V. S. Miller, "Use of Elliptic Curves in Cryptography," in Advances in Cryptology—CRYPTO '85, Lecture Notes in Computer Science, vol. 218, Springer, 1986, pp. 417–426.
3. N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, Jan. 1987.
4. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
5. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.
6. A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," in Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN), 2008, pp. 245–256.
7. D. J. Bernstein and T. Lange, "Faster Addition and Doubling on Elliptic Curves," in Advances in Cryptology—ASIACRYPT, Springer, 2007.
8. D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York, NY, USA: Springer, 2004.
9. W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2020.
10. M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Cengage Learning, 2022. M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," in Advances in Cryptology—CRYPTO '93, Springer, 1994, pp. 232–249.
11. C. Boyd and A. Mathuria, Protocols for Authentication and Key Establishment. Springer, 2003.
12. J. Katz and Y. Lindell, Introduction to Modern Cryptography, 3rd ed. CRC Press, 2020.
13. S. A. Camtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 8, no. 4, pp. 2–13, 2006.
14. D. He, N. Kumar, M. K. Khan, and J. H. Lee, "Lightweight Anonymous Authentication Protocol for Mobile Pay-TV Systems," IEEE Transactions on Consumer Electronics, vol. 60, no. 4, pp. 665–671, 2014.
15. X. Li, J. Niu, M. K. Khan, and J. Liao, "An Enhanced Smart Card-Based Remote User Password Authentication Scheme," Journal of Network and Computer Applications, vol. 36, no. 5, pp. 1365–1371, 2013.
16. H. Lee and K. Lee, "A Lightweight Authentication and Key Agreement Scheme for IoT Environments," IEEE Access, vol. 8, pp. 119213–119226, 2020.
17. S. Ali, M. Irshad, M. S. Obaidat, and S. Kumari, "Energy-Efficient Authentication Protocol for Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9354–9365, 2020.
18. Y. Chen, Z. Wang, and X. Li, "ECC-Based Lightweight Authentication Scheme for Internet of Things," IEEE Access, vol. 10, pp. 57284–57298, 2022.
19. L. Chen, H. Zhao, and X. Wang, "Lightweight Authentication and Key Agreement Protocol for IoT-Enabled Smart Grid," IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6843–6858, 2023.
20. H. Wang, Y. Zhang, and J. Liu, "A Lightweight IoT Security Framework for Secure Authentication and Key Management," Future Generation Computer Systems, vol. 145, pp. 155–170, 2023.

21. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8084, 2019.
22. M. Rostami, F. Koushanfar, and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," Proceedings of the IEEE, vol. 102, no. 8, pp. 1283–1295, 2014.
23. C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," Proceedings of the IEEE, vol. 102, no. 8, pp. 1126–1141, 2014.
24. NIST, "Recommendation for Key Management—Part 1: General," NIST Special Publication 800-57, Rev. 5, 2020.
25. NIST, "Lightweight Cryptography Standardization Process," National Institute of Standards and Technology, 2023.
26. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996. Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Communications, vol. 30, no. 11–12, pp. 2314–2341, 2007.
27. Data Protection in the Cloud: A Backup and Recovery Approach by H. NAGA CHANDRIKA1 and DR. PRAMOD PANDURANG JADHAV, Journal of Innovative Engineering and Research (JIER) Vol. - 6, Issue -2, October, 2023, pp. 6-10.
28. Extreme Programming in Software Development Dr. Sanjay Singh Bhadoriya1 and Saurabh Parikh, Journal of Innovative Engineering and Research (JIER) Vol.- 6, Issue -2, October 2023, pp. 16-19
29. A Review on Security of Wireless Sensor Networks using Cryptographic Techniques DINESH KUMAR GUPTA1, DR. DEEPIKA PATHAK2, Journal of Innovative Engineering and Research (JIER) Vol.- 5, Issue -2, October 2022, pp. 17-20 .
30. A Security-focused Review on Virtual Machines MAYANK YADAV, Journal of Innovative Engineering and Research (JIER) Vol.- 5, Issue -1, April 2022, pp. 5- 10.
31. A Performance Comparison of Edge Cover Graph Coloring Approach for Resource Allocation in Cloud Computing Environment NEELEMA RAI, DR. DEEPIKA PATHAK, Journal of Innovative Engineering and Research (JIER) Vol.- 3,Issue - 2,October 2020, pp. 24-29.
32. Design of Chatting Application Based on Android Bluetooth with Hotspot Feature APARNA KHARE1, AKSHAY GUPTA, Journal of Innovative Engineering and Research (JIER) Vol.- 3,Issue - 1, April 2020, pp. 5-6
33. A Novel Technology to Improve Grid Frequency Response on Electrical Power System with High Level of Renewable Generation Penetration VINAY KUMAR, SUNIL BHATT, Journal of Innovative Engineering and Research (JIER) Vol.- 2,Issue - 2, October 2019, pp. 1-4
34. Security Enhancement of Networked Building Automation System in Airports NIKHIL RATHORE, SANTOSH PAWAR, Journal of Innovative Engineering and Research (JIER) Vol.- 2,Issue - 2, October 2019, pp. 16-21.
35. A Study on College Students: Stress Management for Enhanced Academic Performance SHUBHA R. SINGH1* and VIKASH PATIDAR, Journal of Innovative Engineering and Research (JIER) Vol.- 1, Issue - 2, October 2018, pp. 6-10.