International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V73I3P108

Volume 73 Issue 3, 104-119, March 2025
© 2025 Seventh Sense Research Group®

*Review Article*

# Lightweight Authentication Protocols in Internet of Things - A Review

Nusrat Hamid Shah[1], Saiful Adli Ismail[2], Azizul Azizan[3], Anne Anoop[4], Durdana Taranum Khan[5], Saahira banu Ahamed[6]

[1,2,3]*Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia.*
[1,4,5,6]*Department of Computer Science, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia.*

[1]*Corresponding Author : nusrat@graduate.utm.my*

Received: 10 October 2024 Revised: 08 January 2025 Accepted: 13 February 2025 Published: 28 March 2025

***Abstract*** *- One possible explanation for the increasing fascination with the Internet of Things (IoT) is the breadth of its possible applications in smart homes, healthcare, transportation, and industrial automation. Data is collected from physical environments and sent across connected networks. From coordinating the usage of small sensors to maintaining server infrastructure, various obstacles exist to overcome when putting IoT into effect. However, a secure and safe data transmission strategy must be implemented due to the enormous volume of data generated and sent by the IoT. Traditional cryptographic methods are often inefficient for such applications. Addressing security issues in the IoT Lightweight Cryptography (LWC) schemes is essential. This study reviews Elliptic Curve Cryptography (ECC), a security method well-matched for IoT environments. The ECC model employs the procedure for creating Private Keys (PRIKs) to encode the elliptic curve. The research found that ECC is often used in IoT-based systems or has gotten more attention than other cryptographic algorithms. With its short key sizes and high degree of security, elliptic curve Encryption (ENC) has become one of the best prominent asymmetric ENC algorithms today. A more robust ECC-based algorithm is required to address the IoT's secrecy and security concerns and ensure efficient operation. The review highlights the growing use of ECC in IoT systems and its advantages, focusing on the security and efficiency of modern IoT applications.*

***Keywords*** *- Lightweight Cryptography, ECC, IoT, Data security, Network security.*

## 1. Introduction

### *1.1. IoT Overview*

Owing to its extensive range of possible usages in fields as diverse as agriculture, logistics, smart transportation, smart homes, cities, the environment, Industry 4.0, healthcare infrastructure, and countless added, the IoT has recently increased a portion of academic responsiveness. The devices themselves are at the center of any IoT solution. In order to detect, gather, transmit, analyze, and act upon data, IoT devices include processors, actuators, and sensors. They make data-driven control and automation possible by establishing connections to various devices, networks, and services. A wide range of businesses and requests may profit from this data in terms of increased efficiency and production. Various IoT devices can share data and information via communication with one another and with other computer devices. Logistics, transportation, energy management, and production processes are just a few areas that may benefit from this data's ability to be tracked, controlled, and optimized. IoT devices may boost efficiency and production in several sectors by collecting data from various sources and enabling automated decision-making [1].

#### *1.1.1. IoT Components*

There are four main components of the IoT [5]: 1. Sensors and other devices: they aid in the pre-defined collection of data from the environment. 2. Connectivity: Wired or wireless connectivity enables the communication of stored data to a cloud infrastructure. 3. Data Processing: The management system processes collected data after data collection and availability on the cloud. 4. User interface: end-users may access the data [3].

#### *1.1.2. IoT Infrastructure and Cloud Storage*

The concept of Cloud Computing (CC) agrees to deliver services and applications via the internet. On a "pay as per requirement" basis, cloud services may provide users with computing, networking, and storage according to their demand. IoT-enabled technologies include CC. Using the cloud, IoT devices can store their big data. The IoT and CC are, hence, connected technologies. Cloud storage is necessary to store the huge amounts of data caused by IoT network sensor devices. Data analysis may be performed on the cloud, and actuators will get instructions to carry out the work grounded on the results.

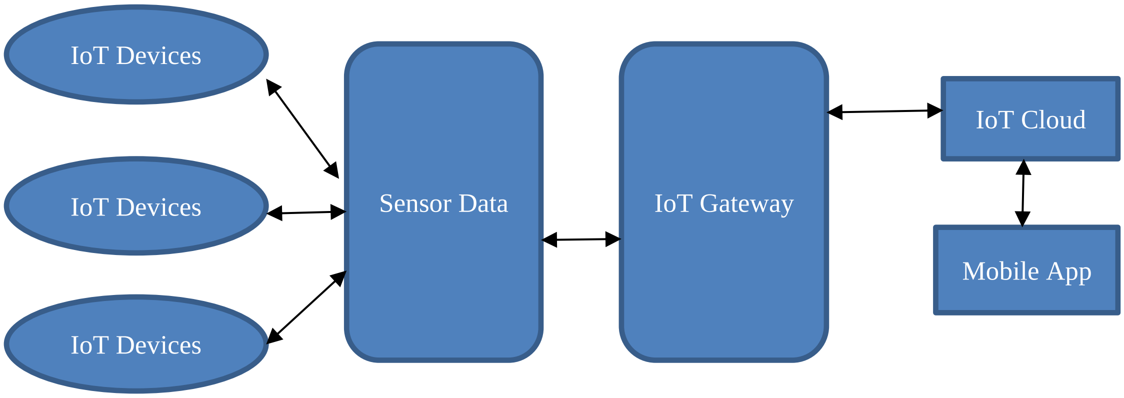

**Fig. 1 Cloud IoT architecture**

The majority of IoT applications need a cloud-based IoT infrastructure. Figure 1 depicts the cloud-based IoT architecture. IoT devices (smart sensors) gather data from the physical environment and send it over a network. This data is transferred to the cloud via the IoT gateway for processing and analysis. Then, IoT storage is done for the massive amounts of data produced by IoT devices. Decisions may be made by means of processed information from data processing. The mobile app, in the IoT architecture, allows users to manage devices remotely. However, various attacks, such as data interception during wireless transmission, can compromise the system as the data moves to and from the cloud [2].

### *1.1.3. IoT Security*

IoT security has become crucial since IoT devices have steadily improved over the last period, and security is the biggest obstacle to IoT adoption. Here are some of the most pressing security concerns:

- *Confidentiality:* Ensuring the data is secure prevents unauthorized persons from gaining access.
- *Heterogeneity:* The IoT is taking an active role in developing goods and devices for a wide variety of industries all over the globe. The lack of standardization leads to varying device setups and the creation of new protocols and operating systems; this requires consistency and standardisation.
- *Data Integrity:* Accuracy and extensiveness are essential to data integrity. Due to attenuation, distortion, or noise, messages may get corrupted during wireless IoT transmission when data is sent among devices created on wireless or wired networks.
- *Availability:* Despite being susceptible to large-scale cyberattacks, availability is a key component in the development and enhancement of the IoT based on hardware or networks [5].

### *1.1.4. IoT Challenges*

Despite the well-known economic benefits of the IoT, it also faces numerous obstacles. To accommodate the one trillion IoT devices, it overcomes some of the following challenges: Most IoT devices lack fundamental security measures. There is a lack of visibility into security problems due to the huge diversity of IoT devices and hardware profiles, which reduces the possibility of having uniform ENC procedures and protocols. The result is a lack of openness on issues of privacy and security. Due to expanded communication protocols, values, and device abilities, which all create concerns, increase complexity, and cause security blind spots, IoT network security faces greater hurdles than conventional network security.

In contrast to business networks, where authentication procedures often require a person to input a credential, the majority of IoT authentication situations are machine-to-machine-oriented and do not include any human involvement at all. ECC currently handles integrity, authentication, and key exchange, while AES handles confidentiality and integrity in the IoT. Even though it has a huge policy space and is inherently vulnerable to SCA, AES is the finest option since it is a lightweight block cipher. Investigating the IoT architecture in further detail reveals security flaws at each layer. The IoT relies on the following three major architectural layers: The perception layer receives the data. Subsequently, the perception network and the perception node receive the data. In this case, the perception network layer gives commands for control while the perception node acquires and controls data.

Data security and network transmission are both handled by the network layer. It provides the perception layer with an environment that is accessible from anywhere. The application layer details all IoT-using or deployed apps [12]. Many security and privacy concerns surround the IoT, which is a big worry since these systems are typically linked to vital organizations and may be hijacked to cause attacks [6, 7]. For data security, cryptography is the best option [8, 9]. IoT-based systems hold great promise for protecting privacy and the security of client data; hence, cryptographic approaches for data integration are crucial. In order to keep sensitive data from prying eyes, ENC is a great tool to use. It helps with concealment, data integrity, and with authentication. Future IoT systems will likely use ENC on sensor devices located with many restrictions that traditional systems have never employed. Researchers are investigating and developing LWC as a potential solution for devices with incomplete processing power and resources. The records used in ENC algorithms are MD5, RSA, 3DES, SHA, AES, and ECC; these algorithms are computationally demanding. Because IoT devices have minimal resource constraints, ECC is the lightest cryptographic technique among the common public-key cryptography algorithms. The technique ensures authenticity and data security by using two keys-one publicly and one privately-to represent the user's personal information. To setup as an asymmetric and Public Key (PUBK) algorithm [10].

El-Gamal and Diffie-Hellman's key algorithms should be able to secure IoT systems. Compared to ECC, AES is 100-1000 times faster on 8-bit microcontrollers. However, ECC has recently surpassed all others as the go-to security mechanism for IoT networks. In 1976, Whitfield Diffie and Martin Hellman (DH) wanted to solve the key management problem; therefore, they invented public-key cryptography [11]. The two parties are believed to have exchanged two sets of keys, a "PUBK" and a "PRIK". There is a mathematical link between these two keys. With DH, have a conversation in both ways. However, it struggles when group members come and go at a regular pace.

### *1.2. LWC*

There are two kinds of IoT devices: 1. Plentiful in resources, including smartphones, tablets, and PCs. 2. Limited Resources: This includes actuators, RFID tags, sensors, and other resource-constrained devices. Because so many applications require these resource-constrained devices, their popularity is growing [2]. LWC, which is widely utilized in Internet security protocols to offer sufficient security, is one such cutting-edge technique. ECC is more appropriate for resource-constrained devices because it is lightweight compared to other cryptographic techniques. Stream, block, hash, and authenticated ciphers are the four categories into which lightweight symmetric cryptographic methods fall.

An LWC scheme is one of the best crucial methods to address resource difficulties in IoT devices because traditional cryptography schemes are ineffective for IoT applications due to resource constraints. The greatest option for low power consumption and high security is ECC. As an alternative to conventional, computationally costly cryptography methods, LWC aims to provide an appropriate degree of security in resource-constrained contexts via rapid development and efficient cryptographic algorithms. Lightweight solutions aim to be smaller regarding key size, memory needs, and execution time. The objective of lightweight algorithm design is to minimise the algorithm's impact on system resources while simultaneously improving its performance and cryptographic robustness [12].There are two cryptographic algorithms: symmetric key ciphers and asymmetric key ciphers. Symmetric ENC uses a single key to encrypt and decrypt data instead of asymmetric ENC, which employs two keys. As a kind of secure along with relatively quick ENC, symmetric key cryptography's only drawback is that it requires the communicating parties to share the key without leaking it. However, this might be circumvented if the key was pre-shared via a reliable third party. In addition, it uses authentication ENC mode (AEAD) to guarantee data confidentiality, integrity, and authentication. Hash functions along with MACs like Marvin along with Quark, as well as block/streaming cyphers like PRESENT and SPONGENT, have recently been formed for IoT lightweight symmetric cryptography. Asymmetric Cryptography (AC) applies to the IoT, including post-quantum lattices, codes, and number-theoretic cryptography. Existing lightweight solutions like Chaskey, SPARX, FLY, LEA, etc., have excellent assessment results. This is because software speed is critical for LWC, especially because maximum IoT devices are operating in multitask mode. The IoT necessitates thinking about things like cypher kinds, block sizes, key sizes, applicable attacks, etc. Table 1 shows the LWC algorithms review.

### *1.3. Asymmetric-Key*

Many forms of AC, including post-quantum lattices and codes, number-theoretic cryptography (e.g., ECC), and others, have applications in the IoT. The asymmetric-key method of ENC and DEC are based on public-key cryptography, which employs a PUBK and a secret key, respectively. AC includes the RSA, Diffie-Hellman, and elliptic curve algorithms. Two sets of private and PUBKs are used in AC. The sender's PRIK (functioning as a digital signature) is recycled to encrypt the data, further ensuring authentication and secrecy. The receiver's PUBK is also utilized for this purpose. The receiver decrypts it at the other end using his or her PRIK after utilizing the sender's PUBK. The sole drawback of asymmetric ENC is the complexity and time it adds to the operation [17].

Figure 2 shows the block diagram of asymmetric ENC. Transport Layer Security (TLS) and Secure Sockets Layer (SSL), which offer HTTPS, are two of several protocols that depend on AC.Software applications essential to establish a secure connection across an unsecured network, such as web browsers, or essential to verify a digital signature also employ the ENC process. The main advantage of AC is enhanced data security. AC is the maximum secure ENC procedure since it never asks users to disclose or exchange their PRIKs, greatly reducing the likelihood of a cybercriminal obtaining one during transmission.

The public and PRIKs used in asymmetric ENC are mathematically connected and recycled for both ENC and DEC. If it uses a PUBK for ENC, there is also a PRIK to decrypt. The associated PUBK will be recycled for DEC if ENC employs the PRIK. Both the sender and receiver are involved in the asymmetric ENC process. The public and PRIKs for each one are unique. The first step is for the sender to get the PUBK of the receiver.

**Table 1. LWC algorithms review**

| Authors | Methods | Advantages | Limitations |
|---|---|---|---|
| Halak, Basel, Yildiran Yilmaz, and Daniel Shiu [13] | NIST Post-Quantum Cryptography | An efficient solution that prioritizes energy conservation | Cryptographic algorithms are becoming increasingly complex and quantum robust. |
| Duda, Jarosław, and Marcin Niemiec [14] | asymmetric numeral system | reducing the number of rounds of some cipher | ENC techniques are frequently too expensive |
| Mansour et al. [15] | asymmetric multi-recipient cryptographic scheme | better utilize network resources | high arrangement cost due to alteration in association |
| Justindhas, Y., as well as P. Jeyanthi [16] | IoT | to find the correct cryptographic algorithm based on the rate of device parameter | threat to security and privacy |

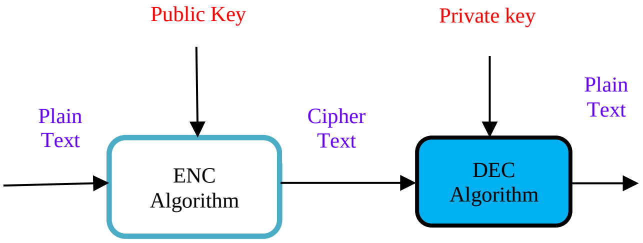

**Fig. 2 Block diagram of asymmetric ENC**

The following step is for the sender to encrypt the plaintext message employing the receiver's PUBK. The result is ciphertext. The receiver receives the cipher text and uses its PRIK to decrypt it, converting it to plaintext. As a result of the ENC function's one-way nature, even if both senders have the receiver's PUBK, neither can read the other's communications. AC is usually utilized to authenticate data using digital signatures. A digital signature is one measured method for ensuring the validity and integrity of digital documents, messages, or software. It serves the same purpose as a stamped seal or handwritten signature but in digital form. Some advantages of AC are:

- There's no need to exchange keys, eliminating the key distribution issue.
- No one will ever need to know or send the PRIKs, which increases security.
- To ensure that a message really originated from a certain sender, digital signatures are enabled.
- Nonrepudiation ensures that the sender cannot later claim they did not deliver the message.

AC has a number of drawbacks, including: When contrasted with symmetric cryptography, the procedure is sluggish.

- Consequently, decrypting bulk messages is not a good fit for it. A person cannot decrypt the messages they receive if they lose their PRIK. The lack of authentication in PUBKs makes it impossible to verify that a given PUBK really belongs to the owner.
- Users must thus confirm ownership of their PUBKs. The PRIK of a malicious attacker may read the messages of that person.

In contrast to symmetric cryptography, which uses one key for all ENC, asymmetric methods employ two distinct yet connected keys. While one key encrypts data, another key decrypts it. Symmetric ENC employs a similar key for both ENC and DEC. An asymmetric ENC system requires a calculated relationship between its public and PRIKs. Asymmetric keys must be longer to provide the same degree of security since malicious actors might possibly use this pattern to decrypt the ENC. Due to the large variation in key lengths, the security provided by symmetric keys with 128 bits of length and asymmetric keys with 2,048 bits of length is almost equal. Compared to its quicker counterpart, symmetric ENC, asymmetric ENC is noticeably slower.

The asymmetric algorithm with the largest user base is the Rivest-Shamir-Adleman algorithm (RSA). SSL/TLS embeds it to provide secure communications across a computer network. Many security professionals are beginning to see ECC as a viable alternative to RSA. The ECC method is a public-key ENC algorithm. Using the characteristics of the elliptic curve equation, it can generate cryptographic keys more efficiently, with less overhead, and in less time. It is much more difficult than factoring to calculate an elliptic curve discrete logarithm, which an attacker would need to do to defeat ECC. Consequently, ECC key sizes may be far smaller than RSA's requirements while providing the same security level while using less computational power and battery resources.

### *1.4. Problem Statement*

Strong security measures are becoming more important as IoT technology rises due to their high computational cost, energy consumption, and memory requirements; standard cryptographic methods present major challenges for IoT devices, especially those with restricted resources like RFID tags or low-power sensors. Due to their limited resources, these devices cannot use traditional asymmetric key cryptography, which is often prohibitively expensive. Lightweight Cryptography (LWC) solutions that efficiently balance security, performance, and resource consumption are therefore desperately required. Despite the best efforts of the LWC approaches, they often compromise security to lower the computational overhead and energy consumption of cryptographic operations.

The most challenging aspect is developing LWC protocols that are both feasible for situations with limited resources and secure enough to withstand possible assaults. Further, there is a lack of in-depth evaluations dealing with IoT devices' unique requirements and security flaws, which means there is a paucity of literature on LWC within the IoT ecosystem [18]. The goal of this review is to fill a gap in the existing research by looking at ECC and other simple cryptographic methods used in IoT applications. In order to find the best ways to improve the efficiency and security of IoT networks, this article analyzes how well they secure data transfers without using all available resources.

### *1.5. Contribution of Study*

This review conducted a Systematic Literature Review (SLR) to find, select, and analyze works focused on lightweight cryptography methods for IoT security. The search string is done, including the terms lightweight cryptography, IoT security, ECC for IoT, and performance of lightweight cryptographic methods. The IoT poses a number of obstacles to privacy protection. The inability of IoT devices to perform the complicated algorithms necessary for effective privacy protection is one key challenge [10, 19]. Also, the security algorithm should not require a lot of power, as the popular IoT devices are battery-operated [18]. The last step is to build a massive physical network out of simple sensors. Finally, deploying the security algorithm on as few devices as possible should be cost-effective.

Consequently, ensuring secure communication is a major obstacle in low-power and lossy systems. This highlights the need for LWC approaches like the elliptic curve for IoT security. This report includes the most recent research on ECC from 2020 to 2024. Additionally, it provides a comparison of the majority of current research on ECC with other algorithms, including hash, DSA, and RSA. The research also compares and evaluates the most current procedures in use. Therefore, the key takeaway from this research is: 1. It investigates the usage of ECC to advance the IoT network devices security. 2. This inquiry seeks to uncover the current gaps and issues related to using ECC for security on the IoT. 3. Suggested cryptographic methods and protocols that use ECC to resolve different issues. 4. Researchers may use this study to address current research difficulties and find inspiration to expand upon existing work. They can continue to advance IoT security using ECC [19]. The remainder of the article follows this structure: Part 2 takes a look at the related literature on ECC IoT-based systems, including things like the results of the search, the features, and the limits of the research. Section 3 concludes this work.

## 2. ECC- A Review

### *2.1. General*

In 1995, researchers V. Miller and N. Koblitz presented ECC, an asymmetrical key ENC system that relies only on mathematical processes yet uses PUBKs. In order to resolve the network or communications, ECC reviewed the attacker with a challenging exponential time task of moderate scale, which is its characteristic attribute. As a direct result, ECC provides lightweight hardware and software in addition to tiny keys, excellent security, and rapid ENC processes. Researchers are exploring and developing LWC to address this issue and meet the needs of devices with limited processing resources and power, which is also considered a crucial requirement for the eternal layer of the IoT architecture.

All of the most commonly used ENC algorithms are computationally intensive: AES, RSA, ECC,3DES, SHA as well as MD5. ECC is the most lightweight cryptographic method among several other popular public-key cryptography methods owing to the minimal resource requirements of IoT devices. Regarding restricted devices, ECC is a cryptography method that works. This algorithm ensures authenticity and data security by using two keys-one publicly and one privately-to represent the user's personal information. It as an asymmetric and PUBK algorithm. El-Gamal and Diffie-Hellman key algorithms should be able to secure IoT systems. However, ECC has recently surpassed all other security measures IoT systems employ.

### *2.2. ECC*

Imagine a big, finite set E that contains points on the elliptic curve's transformed plane ($x_i$, $y_i$). In this set, E defines a group addition operator, +, that operates on two points, P along Q that are provided. P + Q = R may be calculated with the help of this group operator, which allows for the inclusion of a third point, $R \in E$. The main objective is to determine, using this group operator, the sum of all elements of set E, starting with a point $G \in E$. The main idea underlying ECC is the difficulty of getting k from k × G. Attempting every conceivable combination of repeated additions would be necessary for an attacker. The discrete logarithm issue, upon which the ECC algorithm's security is based, is this obstacle [20]. The domain parameters of the elliptic curve check all three methods that make up the ECC cryptosystem: key generation, ENC, and DEC. Equation (1) reviewed the generic equation that gives the elliptic curve its name.

$$y^2 = x^3 + aw + b \tag{1}$$

#### *2.2.1. Adding Points in ECC*

The definition of a finite field bounded by the prime number p is a field that can be worked on exclusively using (mod p). It is common practice to multiply the initial value (P) of ECC by n times to get nP. A PUBK with the value of nP and a PRIK with the value of n. In order to join two points, choose two spots on the elliptic curve (R=P+Q).

*2.2.2. Subtraction Points in ECC*

Performing the subtraction on an elliptic curve. P - R = P + (−Q) if point Q is the subtracting point P result. To illustrate the negation operation, one may express the subtraction process on an elliptic curve in the following way: The identity R = P − Q = P + (−P) holds if (-Q) is the negative procedure of Q.

*2.2.3. Multiplication Point in ECC*

Multiplication is another name for repeating the basic coordinate curve's addition. There is a plethora of algorithms that can multiply points rapidly. Using point addition, multiplication on an elliptic curve E, denoted by Q = mP, is possible. Where m is an element of Z+ and (P, Q) are elements of $E^{2}$. In reality, scalar multiplication is a sequence of additions of points in Equation (2).

$$mP = P + P + \cdots + P \tag{2}$$

*2.2.4. Doubling Point in ECC*

To find multiples of P at point P by using the tangential connection to the curve. It is inevitable that this line will intersect the curve at some point. This point reflection concerning the x-axis is $R\ (x3, y3\ )\ =\ 2p(x1, y1\ )$.

*2.2.5. Infinity Point in ECC*

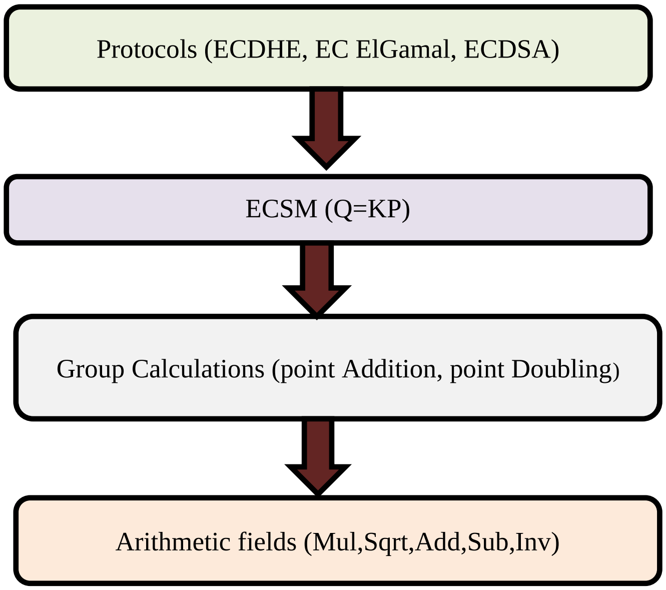
Protocols (ECDHE, EC ElGamal, ECDSA)
ECSM (Q=KP)
Group Calculations (point Addition, point Doubling)
Arithmetic fields (Mul,Sqrt,Add,Sub,Inv)

**Fig. 3 Operation in ECC is divided into four levels**

The points are said to meet at infinity, represented by the letter O, if either ($x_1$ = $x_2$, $y_1$ = $y_2$) = 0 or ($x_1$ = $x_2$, $y_1$) = $y^2$. To establish the sets of algorithms required to build an ECC cryptosystem, one should adhere to the hierarchy shown in Figure 3. Here, the ECEG protocol is used, but there are others you may choose. Then, the algorithms for doing an arithmetic operation in the field should be described, followed by the algorithms for doing Elliptic Curve Point Multiplication (ECPM). The addition and doubling of the points are then carried out as a sequence of operations on various entry point coordinates; these coordinates are parts of the field [25].

*2.2.6. Elliptic Curve Algorithm*

With its foundation in the algebraic structure of elliptic curves over finite fields, ECC delivers public-key cryptography. To provide the same degree of security, ECC employs smaller keys than those used by non-ECC cryptography methods (based on simple Galois fields), such as DH, RSA, and DSA. At present, in cryptography, an elliptic curve is a plane curve over a finite field Fp (instead of the real numbers) that includes the points and a distinct point at infinity, represented by ∞.

$$4a3\ +\ 27b2\ \ \neq\ 0$$

All four variables y, x, a, and bare integers modulo p belong to the field of binary fractions (FP). Coefficients a and b, often known as the curve's characteristic coefficients, define the locations of the curve's points. One requirement must be satisfied by the curve coefficients.

- *First, Generate Keys*: This is the most basic process for creating a public along with PRIK. The message will be encrypted using the sender's PUBK and decrypted using the receiver's PRIK. A number 'd' must be chosen from within the 'n' range in the following equation to generate a PUBK. Moreover, here is the equation: The equation $Q\ =\ d\ *P$ Where d is the random number designated from the range (1, n-1). The point on the curve is P. PUBK Q and PRIK d are equal.
- *ENC:* In order to convey a message m, it must be characterized on a curve. Assume that the point M is on a curve 'E', and that m is a function of m. The range [1 - (n-1)] is used to arbitrarily choose a number' k'. The two cipher texts that will be created and sent are $C_1$ as well as $C_2$. The equation $C_1$ = k * P The equation $C_2$ = M + k * Q
- *DEC:* The receiver performs the following process to recover the message: M=$C_2$-d*$C_1$ [41, 42, 43].

***2.3. ECC Design***

The design of the ECC processor comprises the primary control unit, an ECC ADD with a double unit, and an ECC unit for arithmetic operations. Curves are required for the construction of elliptic curve protocols. Figure 4 shows the ECC processor. With ECC, devices built on the IoT can implement cryptographic algorithms.

Advanced ENC Standard (AES) is a symmetric ENC technique that is recycled in conjunction with ECC for secure data transport and storage. One of the most secure ENC techniques known, it is also one of the most extensively utilized algorithms. For data integrity and authentication, utilize the Secure Hash Algorithm (SHA) family of hash functions. Using ECC may deliver secure digital signatures along with message authentication codes.

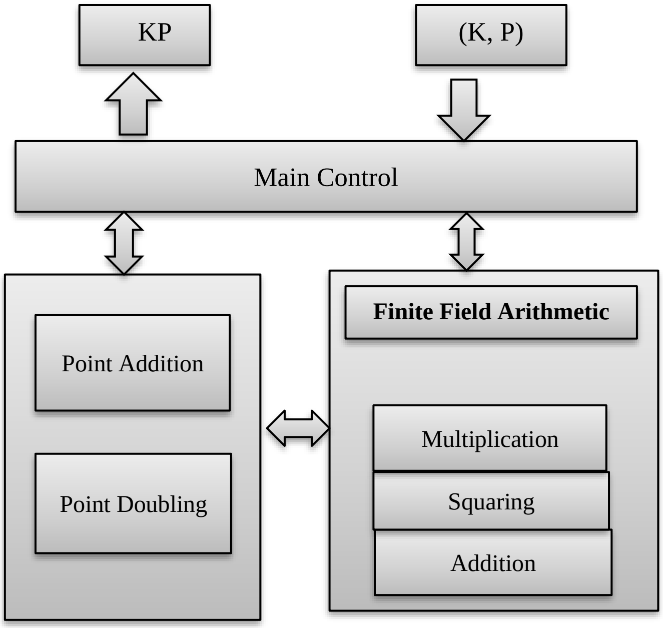

**Fig. 4 Processor for elliptic curve point multiplication**

If two parties want to produce a shared secret key, they may utilize the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol in conjunction with ECC. Data transmission and secure communication among IoT devices are both possible with it. The Elliptic Curve Digital Signature Method (ECDSA) is a digital signature method that may be employed in conjunction with ECC to offer data authentication and nonrepudiation. Online banking, e-commerce, and other sectors that need secure authorization and authentication often utilize it.

*2.3.1. Edwards-Curve*

EdDSA One more digital signature technique that builds on ECC is the recent EdDSA. It is gaining popularity in systems that rely on the IoT since it is quicker and more secure than ECDSA.

## 3. Review

This literature study aims to examine and shed light on the understudied aspects of ECC concerning IoT devices. Although there have been notable improvements in IoT security, there is still a noticeable lack of research that focuses on how to use best and optimize ECC in IoT settings when it considers how dependent on IoT devices-which are becoming more susceptible to security breaches as a result of insufficient data protection measures. Despite ECC's attractiveness as a solution to the specific problems faced by IoT systems-such as insufficient computing power and the necessity for effective data ENC-its capabilities in this area remain underexplored. This study analyses the present situation of ECC in IoT security, identifies areas that need more investigation, and justifies the need for this study. To reduce the danger of sensitive data disclosure, it aims to direct future research directions by using more efficient ECC algorithms designed for IoT systems. Wang et al. [21] discussed that both industrial output and economic growth are substantially aided by the IIoT or Industrial IoT. The security risks posed by the open nature of wireless communications, however, make them more susceptible to attack. In order to safeguard resource-constrained IoT devices, a lightweight combined Physical Layer ENC and Authentication (PLEA) technique is proposed in this study. A dynamic encrypting sequence and a tag are generated in the proposed PLEA system using Quadrature Phase Shift Keying (QPSK) modulation and extracting the quadrant feature in conjunction with the shared key. Phase reversal and power assignment are then used to implement Physical Layer ENC (PLE) along with tag embedding, respectively, in accordance with the encrypting sequence and the tag. Physical Layer Authentication (PLA) and DEC are carried out at the receiver using the same quadrant characteristic taken from the received signals to renew the tag along with the decrypting sequence. After the signal detection along with tag detection error rates are provided, the proposed PLA scheme's detection probability and false alarm probability may be calculated. Furthermore, in order to evaluate the PLE's efficacy, the combined regular moving power is both defined and computed. It has been shown via computer simulations that the proposed technique can possibly provide adequate security protection for IIoT.Gabsi et al. [22] defined smart cards, bankcards, Radio Frequency Identification (RFID) devices, and other similar security applications that rely on elliptical curves.

These cryptographic systems need to be resistant to several kinds of physical attacks to ensure the effective security of these applications. The Differential Power Analysis (DPA) attacks effectively used scalar multiplication algorithms. It provides a defence mechanism in this research for scalar multiplication algorithms that are fundamentally secure against Simple Power Analysis (SPA) as well as safe-error attacks, as well as DPA attacks. ECC algorithms tailored to low-cost applications are the work focus. Before discussing potential countermeasures for ECC-based cryptographic algorithms, an overview of the many side-channel attacks that these algorithms are vulnerable to. After that, a hardware implementation that is optimized for the most actual scalar multiplication algorithm that protects against safe-error and SPA attacks. It demonstrates the effectiveness of the proposed DPA countermeasure approach against further extensions of DPA attacks. Like the Basic Random Initial Point (BRIP) approach, which is solely suitable for the left-to-right algorithm, the proposed solution is comparable but not identical. The proposed technique protects against Refined Power Analysis (RPA), Zero-Value Point Attack (ZPA), and double attack by randomizing the processed data during the scalar multiplication algorithm's calculation. In the concluding part, the proposed technique is compared to existing countermeasure algorithms in the literature regarding computing cost. These algorithms include Montgomery-Ladder, BRIP, left-to-right, and Co-Z Mont-Ladder. Baccouri et al. [23] represented a lightweight authentication strategy that uses the Elliptic Curve ElGamal cryptosystem with ephemeral encoding parameters presented in this work. Validation using the Scyther verification tool confirms the efficacy and robustness of the proposed strategy. This protocol beats RSA and comparable ECC implementations in terms of time complexity, according to a thorough security study that compares improved ECEG with others. It also compares the authentication technique to one that uses blockchain technology to see how much more space-intensive it is. It may be concluded from the findings that the proposed approach makes better use of resources and needs less storage space for authentication-related data. By using ephemeral encoding parameters for authentication without sacrificing calculation time, the proposed technique substantially improves WSN security.

The results show that the lightweight authentication system is successful and practical, making it a good option for secure communication in low-resource settings. Hegde, Nagaratna P., and P. Deepthi. [24] applied an authentication technique; specifically, it describes an ECC-based authentication scheme that successfully maps messages to elliptic curves after encoding them. Being resistant to different cryptographic attacks, the proposed solution has the benefit of working with the coding stage. Also, to help illuminate how secure the proposed method is, this effort will do a security analysis based on evidence. Details the scheme's padding reduction characteristics and provides crucial output sets derived from the tried-and-true elliptic curves. Using attack resistance, padding size, encoding operations count, and decoding operations count as metrics, and this job demonstrates that authentication procedures are superior to alternative strategies.

The effects of processing cryptographic characteristics at the mapping tag other than the encoding tag may be investigated in future studies. Okediran T. M. et al. [25] described the purpose of electronic payment; this article details a security strategy that may be applied directly to IoT devices, including mobile phones and ATM cards, at the perceptual layer and the network and application layers. It offers authentication, key agreement, ENC, and DEC, all of which help protect user privacy and protect IoT Devices against Denial-of-Service attacks (DDoS), intrusion attacks, as well as falsification attacks throughout the IoT network. It utilized a Techno WX3 along with an ATM card with processor speeds of 1.2GHz as well as 8Bit since the ECC is a lightweight ENC algorithm that is ideal for low-resource IoT devices. This is because the processor performance of the sensor node is lesser. Due to the security scheme's disproportionate usage of the mobile phone's Random-Access Memory (RAM), the results demonstrated that this metric is more important than others. Because the system used more RAM when implemented on the ATM card, the card's RAM capacity was another factor needing extra care. Last but not least, the Jitter value was affected by the card's slower processing capabilities, which made the ENC and DEC time seem longer than on the mobile phone. Owing to the limited resources of IoT devices and the perceptual layer, the technique may be applied directly to these devices to protect them against falsification attacks, denial-of-service attacks, and botnet attacks employing ECC over binary fields. Hu et al. [26] described data confidentiality and user privacy as becoming more difficult as the IoT has grown. IoT endpoints are often placed in unsupervised areas and linked to public networks, subjecting them to physical manipulation and other network attacks. Up to this point, many Authentication Key Agreement (AKA) systems have been certified; nevertheless, most of these schemes either fail to address essential security characteristics or are unsuitable for end devices with limited resources. In addition, the real-or-random paradigm used to conduct their security proofs is not always secure when applied to actual application scenarios.

An AKA protocol was provided for both end devices and servers to mitigate the vulnerabilities. Message authentication using one-way hash functions and an ECC-based key exchange mechanism are used in the proposal to provide forward security, user anonymity, and mutual authentication. Using the conventional model along with the computational assumptions of elliptic curve ENC, a formal security proof of the proposed system was conducted, and formal verification was automated using ProVerif. In addition, this strategy improves security while reducing computation and transmission costs, as shown by the performance comparison. Alshudukhi et al. [27] implemented a wireless transmission of traffic status signals to enhance traffic safety and efficiency of vehicles in Vehicular Ad hoc Networks (VANETs). Issues with privacy and security must be thoroughly resolved before deploying the VANET system.

A lightweight authentication method that preserves conditional privacy provides secure communication in VANET. Uniting Tamper-Proof Device (TPD) and Roadside Unit (RSU)-based systems makes the proposed approach well-suited to tackle privacy and security challenges. Each TPD of the RSU, rather than the OBU's TPD, is preloaded with the system's initial public parameters as well as keys under the proposed technique, which is based on ECC. The proposed system also withstands typical security attacks and meets privacy and security criteria. Calculation and communication costs are two areas where the proposed approach outperforms other current schemes, according to the performance assessment. Hammi et al. [28] described the secure communication and access to these items in many instances. One of the biggest problems with the IoT right now is security. With the help of ECC and isogeny, a new method is proposed for generating One-Time Passwords (OTPs). Every time an IoT device communicates with a server, a new key is generated as an expanded version of the One-Time Password (OTP) idea. It also has an advantage over synchronous OTP-type techniques as this method does not need a timestamp or counter. This methodology does not want challenge/response handling like asynchronous OTP-type techniques. It implemented a real plan implementation using Java to assess its effectiveness. The comprehensive examination showed its great efficiency, particularly for constrained devices. In the future, it aims to (1) investigate how well the system performs when exposed to different forms of isogeny, (2) define a method for retransmitting unauthenticated and lost messages, and (3) secure the protocol, particularly against Denial-of-Service attacks that try to overwhelm the server's processing power by sending fictitious OTPs that the server must verify. Routis et al. [29] discussed the benefits of the recently popularised technology pattern known as the IoT, which is its ability to create networks of smart, interoperable devices.

With this in mind, it has sparked the development and expansion of VANETs, or vehicle ad hoc networks, which were first implemented to ensure driver safety and prevent traffic accidents. The disadvantage is that this rapid development raises important questions about user privacy, while the number of those who attempt to listen to and intercept data has substantially expanded. This reviewed a significant threat to automobiles navigating through a smart city. Considering that VANETs provide inadequate resources to users and drivers, this paper's study attempts to assess privacy protection strategies in VANET settings according to the efficiency and security level they guarantee. Additionally, ECC is addressed in the context of low-resource settings. The paper concludes by comparing the presentation of three cryptographic algorithms used for efficient authentication along with safe message transmission in VANETs: Hyperelliptic Curve Cryptography genus 3 (HECC-3), HECC genus 2 (HECC-2) as well as ECC.

The goal is to conclude the execution of each system in this particular application area. In most criteria, ECC outperforms HECC-2 and HECC-3, according to the assessment findings. Nevertheless, regarding some energy measurements, HECC-2 and HECC-3 outperform ECC. In general, HECC algorithms are still in their early stages and cannot hold their own against ECC. This is because HECC relies on very complicated mathematics, and the scientific community has not made enough headway in optimizing it. Nevertheless, there are signs that HECC will surpass ECC regarding speed and other metrics as its curves are optimized. This is because HECC-2 and HECC employ a much lower key size while maintaining the same degree of ECC security. Thakur et al. [30] implemented the concept of the IoT network, which was born out of the convergence of many technologies, including ongoing management, brainpower, product sensors, and embedded systems. IoT devices have recently had a significant effect on industrially critical infrastructures. IoT critical infrastructure security and privacy continue to be major concerns, nevertheless. To fix the problems with the current systems, this study suggests an elliptical curve-based cryptographically secure privacy-preserving authenticated key agreement method for an IoT network. This method creates a mutual key among the user along with the device. A comprehensive evaluation and testing process using the AVISPA methodology was conducted to demonstrate the system's security. With the quality evaluation results, the plan is both efficient and lightweight. The present framework provides new characteristics, including Established Session Key Protection, Key Compromise Impersonate Attack Resistance and Key Replication Resistance, with existing features. Majumder et al. [31] applied for communication among lightweight resource-constrained devices in an IoT network, and the Constraint Application Protocol (CoAP), an application layer-based protocol, is utilized. Commonly linked with the connectionless User Datagram Protocol (UDP), the representational state transfer architecture underpins the operation of the CoAP protocol.

For creating a secure session using current algorithms like Lightweight Establishment of Secure Session for communication among different IoT devices and distant servers, the CoAP is connected with the Datagram Transport Layer Security (DTLS) protocol. However, CoAP has a few restrictions regarding DTLS layer key management, session creation, and multicast message transmission. Therefore, a protocol for securely forming CoAP sessions must be developed to facilitate communication between IoT devices. Therefore, it proposed an efficient and lightweight communication technique to build session key cryptography between IoT devices and distant ECC key server cryptography to solve the recent limitations connected to key management along with multicast security in CoAP. The proposed ECC-based CoAP that implements CoAP for authentication in IoT networks is ECC-CoAP. Several familiar cryptographic attacks were examined to validate the security strength of the ECC-CoAP.

It was discovered that every attack is well-defended. Based on the results of the ECC-CoAP performance investigation, this method is both secure and lightweight. Itoo et al. [32] defined an agricultural country's economy as not complete without agriculture, which is why it's called the backbone of the economy. In addition to providing essential food ingredients, it generates many job openings. Consequently, in order to boost output, contemporary technology is essential in the agricultural sector. Soil acidity, soil moisture, humidity, light, and other meteorological data might be tracked in an agricultural field using Wireless Sensor Networks (WSN). Crop development, quality, and production are greatly affected by climatic conditions. Both the quantity and quality of agricultural output are enhanced by these variables. However, the security threats associated with WSN include impersonation, modification, interception, and interference, all of which have a detrimental impact on agricultural operations and crop output. Preserving privacy and enhancing security are the main concerns for agricultural WSN.

A privacy-preserving, as well as effective key agreement architecture for smart agricultural monitoring schemes, was proposed in this study using ECC along with hash functions. In addition to offering secure communication in smart agricultural monitoring schemes, the proposed framework is resistant to numerous security attacks. Using BAN logic, it explains the precision of the proposed protocol for mutual authentication and key exchange. The proposed framework simulates the security framework's security correctness using the well-known key verification tool Scyther. The proposed systems establish security using the ROR paradigm. In addition, it compares the proposed protocol to other comparable protocols in a similar setting based on security features, computation overheads, and communication overheads. Thus, the proposed protocol offers better security and efficiency than other current protocols in a similar setting.

**Table 2. ECC algorithms view**

| Authors | Application Domain | Objective | Contribution | Limitation | Effectiveness/ Outcomes |
|---|---|---|---|---|---|
| Ahmed et al.,[33] | IoT networks | A secure method of IoT cybersecurity that combines LWC with authentication | This research bridges the gap between ENC and elliptic curve authentication. | Weak bits, key generation, backtracing in IoT devices, along with easily forged digital signatures are among the issues. | Demonstrated strong security in a controlled IoT environment but struggled with scalability. |
| Hu, Tang, and Xie [34] | Smart cards | IoT authentication protocols | A two-factor authentication protocol that uses ECC, a password, along with smart cards. | Potential threats include credential guess attacks, replay attacks, impersonation attacks, and threats to sensor node acquisition. | Successfully implemented in smart card systems, with reduced risk of unauthorized access. |
| Oudah, and Maolood [35] | IoT: Smart as well as mobile devices | Based on enhanced ECDSA and Shamir secret sharing, this is a lightweight authentication architecture for the Internet of Things. | The research secured the IoT environment by combining an altered ECDSA with Shamir's secret sharing. | Release the PRIK data while decreasing the modular inverse operations count and arithmetic operations. | The solution significantly improved authentication times, but some vulnerabilities remain with key handling. |
| Nithisha, and Jesu [36] | Cloud environment | A novel approach to cloud data security that allows for the safe storage of sensitive data | The work focusses on three separate methods for prime number generation: digital signature key generation for DEC, ENC, and authorization. | Computational cost | Effectively secured cloud data storage with a high computational cost makes it less suitable for IoT. |
| Lee et al. [37] | IoT cloud environment | Protecting the cloud using a three-factor authentication system that allows users to remain anonymous | A three-factor authentication is based on the ECC approach to address the security flaws in existing authentication techniques. | Phishing aimed at personal information carries a man-in-the-middle level of risk and computational cost. | Strong user authentication, but still susceptible to phishing and Man-In-The-Middle (MIM) attacks. |
| Ayoub, Najat, and Jaafar [38] | IoT-Cloud | The IoT cloud paradigm requires a lightweight and secure CoAPA. | The restricted application protocol (CoAP) is the basis for this lightweight mutual authentication protocol, which is more appropriate for IoT devices than HTTP. To secure data transmission between the device and the cloud, it makes usage of the elliptic curve ENC. | MIM attack, data theft, Computational cost. | Successfully secured IoT-to-cloud communication, though vulnerabilities remain in MIM attacks. |

| | | | | | |
|---|---|---|---|---|---|
| Kumar et al. [39] | Medical security in IoT | For medical image IoT security, a hybrid visual, in addition to optimal ECC, is delivered. | Identify optimal global solutions that are more effective and accurate than existing approaches. | Computational cost | Successfully applied in healthcare IoT, but high computational cost limits its real-time effectiveness. |
| Rosy, and Kumar [40] | Cloud, Healthcare including heart disease detection | The Diffie-Hellman method is an ENC-based elliptic curve optimization method. | ECC enhances cloud security and privacy by employing the Diffie-Hellman algorithm, which is also employed for data DEC and ENC. | Forgery, transient secret leaking, and session key disclosure are all problems that insecure channels open to malicious attacks face. | Enhanced cloud security, but vulnerable to session key leaks over insecure channels. |

**Table 3. Comparison between different lightweight algorithms**

| Algorithm | Block size (variant) | Key size (variant) | Rounds of process (1) | Structure | | Attacks |
|---|---|---|---|---|---|---|
| | | | | Discrete Algorithm | Integer Factorization | |
| Diffie-Hellman | ✓ | ✓ | ✓ | ✓ | | Man-In-The-Middle-Attack |
| RSA | ✓ | ✓ | ✓ | | ✓ | Shor's Algorithm |
| Rabin | ✓ | ✓ | ✓ | | ✓ | Brute Force Attack |
| ElGamal | ✓ | ✓ | ✓ | ✓ | | Pohlig-Hellman Algorithm |
| ECC | ✓ | ✓ | ✓ | ✓ | | Brute Force Attack |
| DSA | ✓ | ✓ | ✓ | ✓ | | Brute Force Attack |

The proposed protocol outperforms similar protocols regarding the practical deployment of smart agricultural monitoring schemes [34]. Table 2 shows the ECC's existing reviews. Table 3 displays the algorithms used for LWC. From a structural perspective, there are two main types of ASYM algorithms. The algorithms are divided into two groups based on the complexity of the factorization of integer numbers. This category also includes the RSA and Rabin algorithms. The second category includes algorithms developed with DL difficulty in mind, such as El Gamal, DSA, and ECC. The second one is considered DL since it uses both linear algebra and DL. The ASYM algorithms often enable the algorithm users to choose the key length and the encryption block size, and the round number of these algorithms is not more than one [44]. Figures 5 and 6 compare the four methods' computational and communication costs [45- 48]. The method presented by B.P. Kavin et al. (2021) has a computation cost of 86.4 milliseconds. S.S. Ullah et al. (2020) 's method shows a slightly higher computation cost of 87.4 milliseconds. The method proposed by I. Ali et al. (2020) has a significantly lower computation cost of 55.6 milliseconds. Lalem et al. (2023) introduced a method with the lowest computation cost of 48.4 milliseconds. B.P. Kavin et al. (2021) 's method requires 512 bits for communication.The method proposed by S.S. Ullah et al. (2020) has a lower communication cost of 340 bits. I. Ali et al. (2020) 's method requires a significantly higher communication cost of 992 bits. Lalem et al. (2023) introduce the most efficient method with the lowest communication cost of 320 bits. Also, Figures 7 and 8 illustrate the encryption and decryption time for some different existing approaches. This study compares RSA, ECC, and Diffie-Hellman concerning many aspects of their respective encryption protocols. The long key requirements and considerable computational overhead make it susceptible to quantum attacks despite its widespread usage for electronic signatures and cryptography. Due to its ability to survive quantum attacks and use shorter keys, ECC is a viable option for settings with limited resources, such as mobile phones. When securing key exchange, Diffie-Hellman usually does a decent job. Based on the discrete logarithm challenge, this method is adaptable regarding key length.

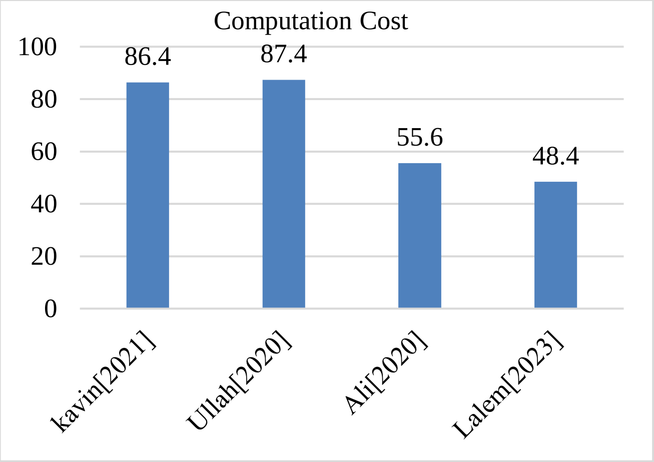

**Fig. 5 Computation cost comparison**

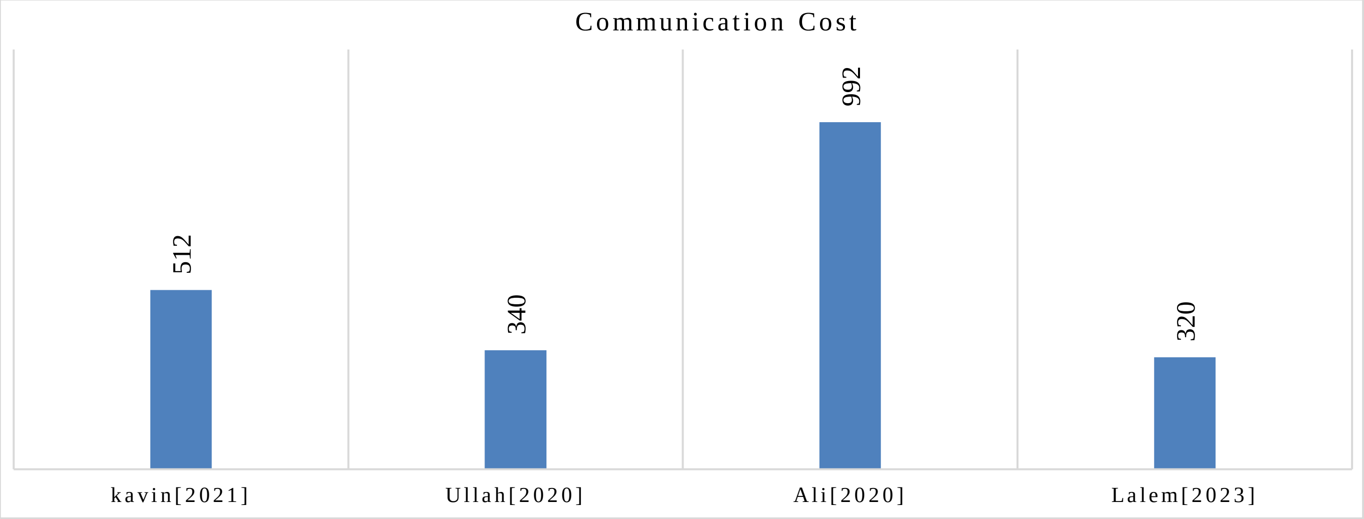

**Fig. 6 Communication cost comparison**

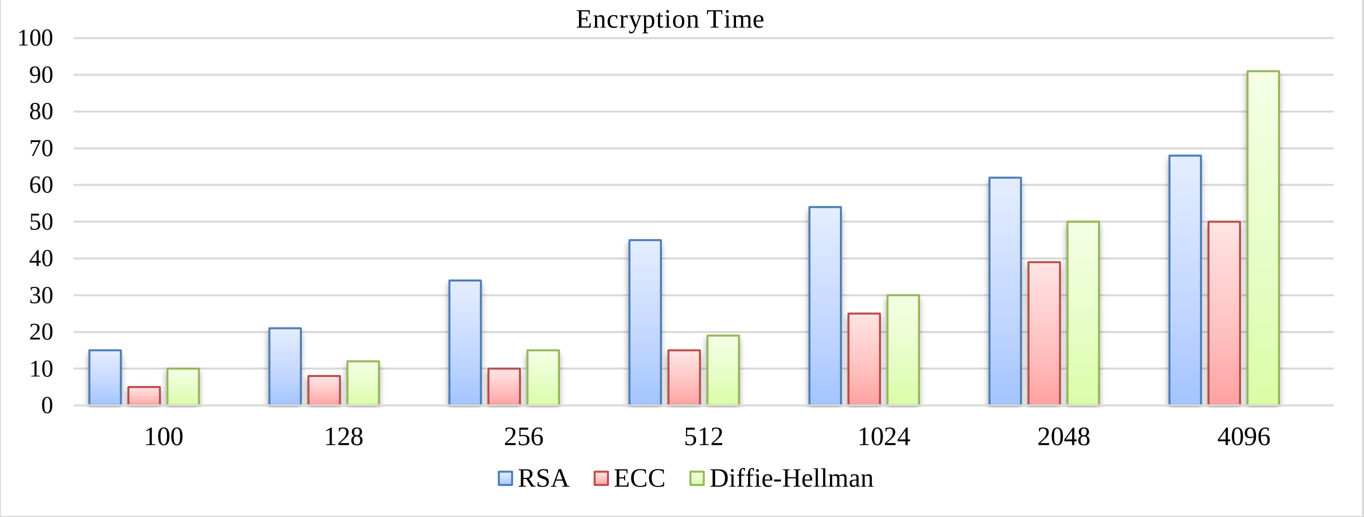

**Fig. 7 Encryption time**

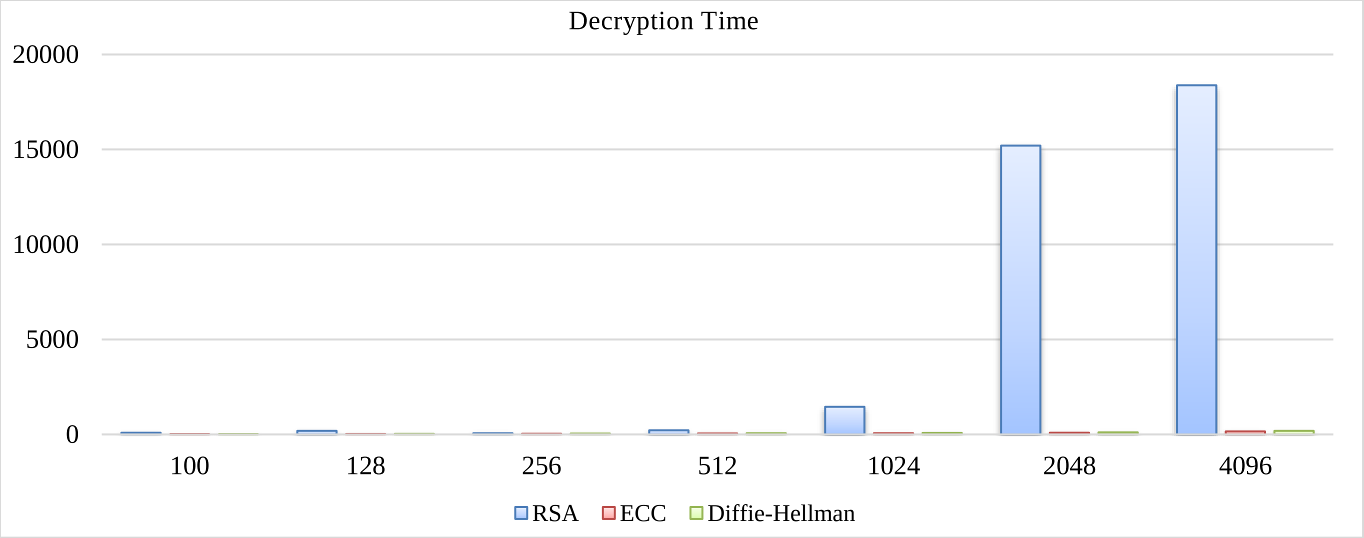

**Fig. 8 Decryption time**

To help with decision-making when selecting cryptographic protocols that fulfil various security needs and use cases, this concise description captures the key features. Three cryptographic protocols-Diffie-Hellman, ECC, and RSA-have their key lengths compared in this research. A clear distinction is discovered. Diffie-Hellman shows moderate growth, ECC does extremely well, and RSA becomes more important as the key length increases.

Curiously, ECC achieves the same security levels with much smaller key lengths. In order to assist decision-makers in selecting appropriate cryptographic algorithms to address security requirements, this concise overview shows the key length effects for all protocols. Three different cryptographic protocols-Diffie-Hellman, ECC, and RSA-have their decryption times compared in this research. A clear pattern emerges when looking at key lengths. When key lengths increase, the RSA decryption time may reach significantly higher levels.

ECC's inherent advantage in this area is that it consistently shows successful decryption at all key lengths. Diffie-Hellman is quicker than RSA overall and has a decryption time comparable to ECC. This concise study offers valuable visions into the decryption performance of all cryptographic protocols, allowing the selection of optimal protocols according to individual key length requirements [49].

- *The Computational Speed :* In order to accommodate the demands of several real-time applications, the encryption and decryption techniques must be sufficiently fast.
- *Value of Key Length :* Key management, a crucial component of encryption methods, illustrates the encryption process. Knowing the key length allows us to calculate the encryption ratio for image loss. The symmetric method takes advantage of the larger variable key length. Consequently, encryption processing relies heavily on key management.
- *Encryption Ratio:*The encryption ratio determines the amount of data that requires encryption. To make processing easier, reduce the encryption ratio as much as possible.
- *Safety and Security Issues :* Cryptographic security determines whether an encryption technique resists brute force attacks or other attacks that use plaintext and ciphertext. For critical multimedia applications, the encryption method must strictly follow cryptographic security protocols. For this study, the cryptographic security is classified as either low, medium, or high [50, 51].

Because it factors in big prime integers to generate keys, the RSA algorithm is more secure when using the asymmetric encryption approach. Consequently, this method establishes that the RSA algorithm is the best choice. Nevertheless, asymmetric cryptography algorithms like RSA, DSA, and ECC are ideal for use cases such as online banking, web applications, email verification, and key exchange via the web and mobile devices. Future studies may explore additional cryptographic algorithms and approaches to identify potential use areas.

### *3.1. Limitations*

The research may have missed other cryptographic techniques that are important for IoT security because it is so focused on ECC in IoT settings. The security solutions described may be too limited due to this restricted emphasis. Innovation in IoT and ECC technology happens at a breakneck pace. As more advanced methods and technology become available, the results of this research may become irrelevant. This research acknowledges its limitations and provides a clearer understanding of the context for interpreting its findings. Future research might solve these limitations, which helps set the foundation for that.

## 4. Conclusion

This research highlights the need for developing new security methods that are both lightweight and implemented on IoT devices with inadequate resources.This research highlights the need for developing new security methods that are both lightweight and implemented on IoT devices with inadequate resources. It also shows that ECC-based defenses are necessary to protect IoT systems from various attackers. Also highlighted in the report are some unanswered questions regarding ECC's role in IoT security, such as how to design elliptic curves with improved side-channel attack resistance, how to develop novel fault-tolerant ECC implementations that are resilient to both fault as well as man-in-the-middle attacks, also how to develop truly novel fault-tolerant ECC implementations.

Consequently, IoT systems must safeguard the privacy and anonymity of individuals and the confidentiality and integrity of information. Results showed that ECC techniques are an effective and flexible data security strategy for the IoT. A well-thought-out protocol, ECC offers practical ENC and DEC techniques that are well-suited to devices with limited resources. Integration of authentication, vulnerabilities (weak bits and chosen-ciphertext attacks), and other issues are some of the many worries with IoT security. Building a robust, efficient, and high-performance ECC algorithm is critical for confirming privacy along with the effectiveness of IoT-based systems' security. This can be achieved by either improving ECC or integrating it with other authentication protocols. Hence, breakthroughs in ECC techniques and a detailed explanation of the relevance of several security factors in IoT-based systems are both enhanced by this study. Several avenues for further study are open. ECC's small key sizes and low computational cost make it a popular option for IoT security, although there is room for improvement. It is also required to create a more reliable and efficient ECC-based approach for the edge.

### *4.1. Future Work*

Future research could identify an excellent design for IoT safety and resource restrictions and provide a secure combination of authentication and ENC to protect the confidentiality and integrity of data sent among IoT devices over an untrusted communications platform. The same holds true for unfinished business and may take it into account.

Elliptic curve ENC should be supplemented with different authentication protocols to enhance the performance of IoT-based systems. Additional safe as well as effective systems that improved suit the demands of users along with businesses may be achieved by advancing the existing works in ECC-IoT using the insights gained from this study. When considering ECC within the framework of IoT-based systems.

## References

[1] Sunil Kumar et al., “A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices,” *Computers, Materials and Continua*, vol. 78, no. 1, pp. 31-63, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Archana D. Wankhade, and Kishor P. Wagh, “Implementation of Secure Cloud Based IoT Communication Using Lightweight Cryptography,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1, pp. 310-316, 2024. [Publisher Link]

[3] Raed Ahmed Alhamarneh, and Manmeet Mahinderjit Singh, “Strengthening Internet of Things Security: Surveying Physical Unclonable Functions for Authentication, Communication Protocols, Challenges, and Applications,” *Applied Sciences*, vol. 14, no. 5, pp. 1-29, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sunil Cheruvu et al., *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*, Springer Nature, pp. 1-488, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Kinza Yasar, and Alexander S. Gillis, “What Is the Internet of Things (IoT)?, TechTarget, 2024. [Online]. Available: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT#:~:text=The%20internet%20of%20things%2C%20or,digital%20machines%20and%20consumer%20objects.

[6] Mohammad Nuruzzaman Bhuiyan et al., “Internet of Things (IoT): A Review of its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities,” *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10474-10498, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Shashvi Mishra, and Amit Kumar Tyagi, *The Role of Machine Learning Techniques in the Internet of Things-Based Cloud Applications*, Artificial Intelligence-Based Internet of Things Systems, Springer International Publishing, pp. 105-135, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Rose Adee, and Haralambos Mouratidis, “A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography,” *Sensors*, vol. 22, no. 3, pp. 1-23, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Christian Rechberger, and Roman Walch, *Privacy-Preserving Machine Learning using Cryptography*, Security and Artificial Intelligence, Springer, pp. 109-129, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Muhammad Rana, Quazi Mamun, and Rafiqul Islam, “Lightweight Cryptography in IoT Networks: A Survey,” *Future Generation Computer Systems*, vol. 129, pp. 77-89, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Paul C. Van Oorschot, “Public Key Cryptography’s Impact on Society: How Diffie and Hellman Changed the World,” *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pp. 19-56, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] L. Mary Shamala et al., “Lightweight Cryptography Algorithms for Internet of Things Enabled Networks: An Overview,” *AICTE Sponsored National E-Conference on Recent Advances in Smart System Automation, Computing and Communication*, vol. 1717, pp. 1-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Basel Halak, Yildiran Yilmaz, and Daniel Shiu, “Comparative Analysis of Energy Costs of Asymmetric vs Symmetric Encryption-Based Security Applications,” *IEEE Access*, vol. 10, pp. 76707-76719, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jarosław Duda, and Marcin Niemiec, “Lightweight Compression with Encryption Based on Asymmetric Numeral Systems,” *International Journal of Applied Mathematics and Computer Science*, vol. 33, no. 1, pp. 45-55, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ahmad Mansour, Khalid M. Malik, and Niko Kaso, “AMOUN: Asymmetric Lightweight Cryptographic Scheme for Wireless Group Communication,” *Computer Communications*, vol. 169, pp. 154-167, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Y. Justindhas, and P. Jeyanthi, “Secured Model for Internet of Things (IOT) to Monitor Smart Field Data With Integrated Real-Time Cloud Using Lightweight Cryptography,” *IETE Journal of Research*, vol. 69, no. 8, pp. 5134-5147, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Mehdi Gheisari et al., “OBPP: An Ontology-Based Framework for Privacy-Preserving In IOT-Based Smart City,” *Future Generation Computer Systems*, vol. 123, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Sudip Maitra et al., “Proof-of-Authentication Consensus Algorithm: Blockchain-Based IOT Implementation,” *IEEE 6th World Forum on Internet of Things (WF-IoT)*, New Orleans, LA, USA, pp. 1-2, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Abidemi Emmanuel Adeniyi, Rasheed Gbenga Jimoh, and Joseph Awotunde, "A Review on Elliptic Curve Cryptography Algorithm for Internet of Things: Categorization, Application Areas, and Security," *Application Areas, and Security*, pp. 1-41, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Meilin Liu, Kirill Kultinov, and Chongjun Wang, "The Implementations and Applications of Elliptic Curve Cryptography," *Proceedings of 39th International Conference on Computers and Their Applications*, vol. 98, pp. 89-102, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Junjie Wang et al., "A Lightweight Combined Physical Layer Encryption and Authentication Scheme for Industrial Internet of Things," *IEEE Access*, vol. 12, pp. 6961-6970, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Souhir Gabsi et al., "Proposal of a Lightweight Differential Power Analysis Countermeasure Method on Elliptic Curves for Low-Cost Devices," *Multimedia Tools and Applications*, vol. 83, no. 30, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Sondes Baccouri et al., "Lightweight Authentication Scheme Based on Elliptic Curve El Gamal," *Journal of Information and Telecommunication*, vol. 8, no. 2, pp. 231-261, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Nagaratna P. Hegde, and P. Deepthi, "Elliptic Curve Cryptography Using Authenticated Encryption," *International Journal of Engineering Research and Applications*, vol. 12, no. 4, pp. 35-40, 2022. [Google Scholar] [Publisher Link]

[25] T.M. Okediran et al., "Securing The Perceptual Layer of the Internet of Things (IOT) Devices Using Elliptic Curve Cryptography," *Research Square*, pp. 1-26, 2023. [CrossRef] [Google Scholar] [Publisher Linkc]

[26] Shunfang Hu et al., "Provably Secure ECC-Based Anonymous Authentication and Key Agreement for IOT," *Applied Sciences*, vol. 14, no. 8, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Jalawi Sulaiman Alshudukhi, Zeyad Ghaleb Al-Mekhlafi, and Badiea Abdulkarem Mohammed, "A Lightweight Authentication with Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography," *IEEE Access*, vol. 9, pp. 15633-15642, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] Badis Hammi et al., "A Lightweight ECC-Based Authentication Scheme for Internet of Things (IOT)," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440-3450, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] George Routis, Panagiotis Dagas, and Ioanna Roussaki, "Enhancing Privacy in the Internet of Vehicles via Hyperelliptic Curve Cryptography," *Electronics*, vol. 13, no. 4, pp. 1-29, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Vidyotma Thakur et al., "Cryptographically Secure Privacy-Preserving Authenticated Key Agreement Protocol for An Iot Network: A Step Towards Critical Infrastructure Protection," *Peer-To-Peer Networking and Applications*, vol. 15, no. 1, pp. 206-220, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] Suman Majumder et al., "ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1867-1896, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Samiulla Itoo et al., "A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System," *IEEE Access*, vol. 11, pp. 56875-56890, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[33] Adel A. Ahmed et al., "A Provable Secure Cybersecurity Mechanism Based on The Combination of Lightweight Cryptography and Authentication for The Internet of Things," *Mathematics*, vol. 11, no. 1, pp. 1-24, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[34] Bin Hu, Wen Tang, and Qi Xie, "A Two-Factor Security Authentication Scheme for Wireless Sensor Networks in IOT Environments," *Neurocomputing*, vol. 500, pp. 741-749, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[35] Mohammed Shakir Oudah, and Abeer Tariq Maolood, "Lightweight Authentication Model for IOT Environments Based on Enhanced Elliptic Curve Digital Signature and Shamir Secret Share," *International Journal of Intelligent Engineering and Systems*, vol. 5, no. 5, pp. 81-90, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[36] J. Nithisha, and P. Jesu Jayarin, "A Secured Storage and Communication System for the Cloud Using ECC, Polynomial Congruence and DSA," *Wireless Personal Communications*, vol. 126, no. 2, pp. 949-974, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[37] Hakjun Lee et al., "Secure Three-Factor Anonymous User Authentication Scheme for the Cloud Computing Environment," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, pp. 1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] Amrani Ayoub, Rafalia Najat, and Abouchabaka Jaafar, "A Lightweight Secure CoAP for IOT-Cloud Paradigm Using Elliptic-Curve Cryptography," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 3, pp. 1460-1470, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[39] L. Ashok Kumar et al., "Hybrid Visual and Optimal Elliptic Curve Cryptography for Medical Image Security in IOT," *ECTI Transactions on Computer and Information Technology*, vol. 16, no. 3, pp. 324-337, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[40] J. Vimal Rosy, and S. Britto Ramesh Kumar, "Optimized Encryption-Based Elliptical Curve Diffiehellman Approach for Secure Heart Disease Prediction," *International Journal of Advanced Technology and Engineering Exploration*, vol. 8, no. 83, pp. 1367-1382, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[41] A. Arkan Saffer, Soran A. Pasha, and Ammar M. Aliakbar, "Lightweight Cryptography Method in the Internet of Things Using Elliptic Curve and Crow Search Algorithm," *Science Journal of University of Zakho*, vol. 11, no. 3, pp. 323-332, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[42] G. Dhamodharan, S. Thaddues, and T. Manivannan, “A New Secure Mapping Scheme on Elliptic Curve Cryptography for Internet of Things,” *International Virtual Conference on Machine Learning Applications in Applied Sciences and Mathematics*, Chennai, India, vol. 2802, no. 1, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[43] Amrita et al., “Lightweight Cryptography for Internet of Things: A Review,” *EAI Endorsed Transactions on Internet of Things*, vol. 10, pp. 1-9, 2024. [CrossRef] [Publisher Link]

[44] Yashar Salami, Vahid Khajevand, and Esmaeil Zeinali, “Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges,” *Journal of Computer & Robotics*, vol. 16, no. 2, pp. 63-115, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[45] Balasubramanian Prabhu Kavin, and Sannasi Ganapathy, “A New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud Using Elliptic Curves,” *The International Arab Journal of Information Technology*, vol. 18, no. 2, pp. 180-190, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[46] Syed Sajid Ullah et al., “A Lightweight Identity-Based Signature Scheme for Mitigation of Content Poisoning Attack in Named Data Networking with Internet of Things,” *IEEE Access*, vol. 8, pp. 98910-98928, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[47] Ikram Ali, Tandoh Lawrence, and Fagen Li, “An Efficient Identity-Based Signature Scheme without Bilinear Pairing for Vehicle-To-Vehicle Communication in VANETs,” *Journal of Systems Architecture*, vol. 103, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[48] Farid Lalem et al., “A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques,” *Applied Sciences*, vol. 13, no. 8, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[49] P. Pranav Teja et al., “Secure Cloud Communication-A Comparative Study of Cryptographic Protocols,” *International Journal of Modern Developments in Engineering and Science*, vol. 2, no. 9, pp. 14-19, 2023. [Publisher Link]

[50] Vishal et al., “Comparative Analysis of Cryptographic Algorithms in Computer Network,” *Proceedings of the KILBY 100 7th International Conference on Computing Sciences*, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[51] Saurabh Singh et al., “Advanced Lightweight Encryption Algorithms for Iot Devices: Survey, Challenges and Solutions,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 15, no. 2, pp. 1625-1642, 2024. [CrossRef] [Google Scholar] [Publisher Link]