Proceedings of the 3rd International Conference on Applied Physics and Mathematical Modeling
DOI: 10.54254/2753-8818/2025.DL28336

Application of Elliptic Curve Cryptography in the Security Field of Resource-constrained Internet of Things

Mingze Sun

Pasadena City College, Pasadena, USA
msun41@go.pasadena.edu

Abstract. The rapid expansion of the Internet of Things (IoT) and connected objects has revealed significant security vulnerabilities in secure data transmission, device authentication, and privacy protection, especially in resource-constrained environments. This paper provides an in-depth look at the application of elliptic curve cryptography (ECC) as a critical cryptographic solution to address these challenges. The paper explores the mathematical foundations underlying ECC, including the fundamental concepts of elliptic curves and the elliptic curve discrete logarithm problem. The paper also discusses the practical application of ECC to IoT security, focusing on robust device authentication, secure data transmission and storage, and improved privacy protection mechanisms. This analysis highlights the inherent benefits of ECC, such as high security thanks to short keys, high computational performance, and reduced communication overhead, while also addressing challenges such as implementation complexity and standardization. Finally, this paper provides insights into selecting the appropriate ECC for various IoT scenarios and discusses future research directions, including the integration of quantum-safe cryptography.

Keywords: Elliptic Curve Cryptography, resource-constrained, IoT security, authentication and privacy

1. Introduction

The rapid development of the Internet of Things (IoT), characterized by the expansion of interconnected networks of automobiles, furniture, and devices, has significantly impacted various aspects of modern life. The explosive growth of connected devices such as health trackers and smartwatches is further expanding the scope of this interconnected system. People should acknowledge that these advanced devices offer great convenience. But they also introduce various security challenges and implementation difficulties. These challenges are common for IoT devices, especially for those small mobile devices which have limited processing power and memory. Key security concerns include device authentication to prevent unauthorized access and protecting sensitive information during data transfer. The goal is to ensure comprehensive confidentiality of vast amounts of personal and operational data. One solution to address these security requirements in resource-constrained IoT devices is to find encryption solutions that combine high security with excellent efficiency. Elliptic curve cryptography (ECC) is particularly well suited to addressing IoT security requirements due to its short key length, strong security, and relatively low computational

DOI: 10.54254/2753-8818/2025.DL28336

resource consumption compared to other public key cryptography methods such as RSA. This study aims to explore and comprehensively examine the practical implications of applying ECC to ensure the security of IoT ecosystems. This paper examines the basic principles of ECC, its various applications, advantages, and challenges. The ultimate goal is to provide a systematic overview and reference material to help users understand and implement ECC-based security solutions in the resource-constrained IoT domain.

2. Fundamental theory of Elliptic Curve Cryptography

This section focuses on the mathematics and basic cryptographic protocols underlying Elliptic Curve Cryptography (ECC). The reader will gain a solid understanding of these fundamentals and ECC's security properties. They will finally get to know ECC's suitability for constrained environments.

2.1. Basic concepts of elliptic curves

The construction of ECC is based on the elliptic curves. In the context of cryptography, commonly used form of elliptic curve is the Weierstrass equation, given by

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

where a and b are constants. These equations are defined over a finite field. Most rational points lie on the curve and form a Mordell-Weil group, except a conceptual point at infinity. The whole structure forms an abelian group under a uniquely defined point addition operation.

This addition operation is the key mechanism of ECC. Say people take two points P and Q on the elliptic curve, if they want to add these two points up, they need to draw a straight line through these two points. Then the straight line will intersect with the curve at a third point. Reflecting this third point across the x-axis gives the resulting point of P + Q, which is point addition. For a special case, if P and Q are the same point, the line drawn is the tangent to the curve at that point. The point symmetry of the intersection point with respect to x-axis is the result of point doubling. If the straight line is vertical, the point at infinity is considered to be connected with the chosen point. Here is the place where the conceptual point at infinity come in handy. The intersection between the straight line and curve will be the symmetry point of the original point with respect to x-axis. After reflecting the intersection point, it's just the chosen point. This geometric addition is the fundamental operation done in the group [1].

2.2. Elliptic curve discrete logarithm problem

The entire security paradigm of ECC protocols lies in the computational difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). This problem is similar to the Discrete Logarithm Problem in Elgamal cryptosystem. But the context is not the traditional finite groups, but the unique structure of elliptic curves and combination rules.

The premise is straightforward: Given a known base point G on an elliptic curve, which is the generator, and another point P on the same curve. P is derived by multiplying G by the secret key, which is an integer k. It is easy to calculate P if someone knows k and G. However, if one is only given P and G, it becomes extremely hard to solve for the secret key k. It is computationally infeasible to find out the secret scalar k in polynomial time on a classical computer, even with access to substantial computing power. This is similar to the one-way function in traditional discrete

DOI: 10.54254/2753-8818/2025.DL28336

logarithm problem. The process of solving it is asymmetry, which means it's easy to solve in one direction but extremely difficult in the reverse. The difficulty of solving ECDLP ensures that a hack cannot easily derive a private key from a released public key [2,3].

2.3. Elliptic Curve Cryptography: protocols and mechanisms

This subsection explains the practical applications of elliptic curve mathematics, especially in constructing widely used cryptographic protocols. It will illustrate how to translate the mathematical concepts into real world applicable security mechanisms.

2.3.1. Key generation

Key generation is a fundamental step in securing communication in ECC. Key generation begins with the selection of a private and public key. The private key is a large, randomly chosen integer. This number theoretically is only known by key owner. It's usually denoted as d. The corresponding public key (Q) is generated from the private key. It's the multiplication of the generator G and the private key d (i.e., Q = d * G). The private key determines the number of dot hops in the cyclic group to reach the final dot. Overall, the private key d is the private key for all operations in ECC, while the public key Q is shared and distributed to everyone. This allows others to encrypt the owner's messages or verify their signatures without needing the private key.

2.3.2. Elliptic Curve Digital Signature Algorithm

The Elliptic Curve Digital Signature Algorithm (ECDSA) is often used for ensuring the authenticity, integrity, and non-repudiation of digital information. Due to its diverse usage scenario, it becomes a crucial component in IoT environments. It's. The nonrepudiation means the sender cannot legitimately deny having signed the message. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a key component for ensuring the authenticity, integrity, and non-repudiation of digital information in IoT environments. Non-repudiation means that a sender cannot validly deny signing a message. When a sender wants to send a message, they use their private key to create a unique digital signature. This signature proves the message has not been altered and it's actually sent from the specific sender. This is a concise verification used for identity check. The ECDSA process consists of the several steps: First, the message is passed through a cryptographic hash function (e.g., SHA-256). The hash function will generate a fixed-size hash value. This will serve as the message's unique fingerprint. Then the sender uses their private key d and a random ephemeral key k to perform several point multiplications and modular arithmetic operations on an elliptic curve. They finally calculate two values r and s, which together form the digital signature (r, s). When the receiver receives the signed message, they run a verification algorithm using the sender's public key Q and the message hash value. If verification is successful, two important facts are confirmed: First, the message was sent by a specific sender who possesses the private key, and second, the message has not been tampered with since it was signed.

2.3.3. Elliptic Curve Diffie-Hellman Key Exchange Protocol

The Elliptic Curve Diffie-Hellman (ECDH) Key Exchange Protocol provides an elegant and highly efficient method for two parties to securely establish a shared secret key over an insecure communication environment. A key feature of ECDH is that the shared secret is never directly transmitted. This fact protects it from eavesdroppers [2].

DOI: 10.54254/2753-8818/2025.DL28336

The process goes like this: First, both parties (let's say Alice and Bob) each generate their own private-public key pair based on the same elliptic curve parameters. Alice chooses a private key d_A and computes her public key

$$Q_A = d_A \cdot G. \tag{2}$$

Bob chooses a private key d_B and computes his public key

$$Q_B = d_B \cdot G \tag{3}$$

Alice and Bob then exchange their public keys over the insecure channel. An eavesdropper can intercept these public keys but cannot derive the private keys due to the ECDLP. Alice then takes Bob's public key Q_B and multiplies it by her own private key d_A to compute a shared secret point

$$S_A = d_A \cdot Q_B. \tag{4}$$

Concurrently, Bob takes Alice's public key Q_A and multiplies it by his own private key d_B to compute a shared secret point

$$S_B = d_B \cdot Q_A. \tag{5}$$

Crucially, because of the associative property of point multiplication on elliptic curves

$$d_A \cdot Q_B = d_A \cdot (d_B \cdot G) = (d_A \cdot d_B) \cdot G = (d_B \cdot d_A) \cdot G = d_B \cdot (d_A \cdot G) = d_B \cdot Q_A. \tag{6}$$

Therefore, $S_A = S_B$. Alice and Bob can both personally derive the identical shared secret point. They will choose a derivation of this point, which is usually its x-coordinate, to be used as a symmetric key. The symmetric key will be widely used in encrypting and decrypting the actual data messages exchanged later, during their communication session [3,4]. This hybridization between ECC and D-H brings this protocol several advantages. It leverages ECC for secure key establishment and a faster symmetric cipher. This is really handy for bulk data encryption, ensuring both strong security and efficiency [5-7].

3. Applications of Elliptic Curve Cryptography in IoT security

In this section, the paper will explore various practical applications of ECC to address security challenges related to various aspects of the IoT ecosystem. From device identity verification to protecting user privacy, especially sensitive data, ECC can provide tailored solutions for resource-constrained environments.

3.1. IoT device authentication

Robust device authentication is a cornerstone of IoT security. If there are some malicious activities attacking the system, device authentication will be the first line of defense against unauthorized access. ECC-based schemes provide supper effective methods for verifying the identities of IoT devices, ensuring that only authorized devices are allowed to participate in the network [8,9].

DOI: 10.54254/2753-8818/2025.DL28336

3.1.1. Mutual authentication

ECC is really the cornerstone for developing robust mutual authentication protocols [8]. In these schemes, both an IoT device like a sensor and an actuator should prove their identities to each other before exchanging sensitive data. Even backend server or another communicating peer device should do the same examine process. This two-way verification is crucial for preventing common and dangerous attacks such as impersonation where an attacker attempts to mimic a legitimate device or server. It's also useful when protecting man-in-the-middle (MitM) attacks where an attacker intercepts, relays, and potentially alters communication between two legitimate parties. By establishing a verified trust relationship from both sides, mutual authentication greatly enhances the overall security of IoT communications.

3.1.2. Scalable authentication

For large-scale IoT networks, which can comprise thousands or even millions of diverse devices, traditional authentication mechanisms can become computationally prohibitive and resource-intensive. This can lead to significant delays and bottlenecks. In contrast, ECC-based authentication schemes are specifically designed to be lightweight and scalable [9]. This allows for the implementation of efficient group authentication strategies or hierarchical trust models where a central authority can efficiently authenticate numerous devices simultaneously or in batches, rather than individually. This scalability is critical for maintaining performance in vast IoT deployments [10,11].

3.2. Data transmission and storage security

Protecting the confidentiality, integrity, and availability of data is paramount throughout its lifecycle in IoT, from the moment it is generated and transmitted to its storage and subsequent access. ECC plays a critical role in securing these data-centric processes.

3.2.1. Secure data transmission (encryption)

Recall that ECC is inherently an asymmetric cryptography method. Therefore, while relatively easy to solve on the one hand, it is extremely complex, even impossible in polynomial time, on the other. However, key exchange protocols based on this basic structure (such as ECDH) are primarily used to establish short-lived symmetric keys for secure communication sessions. These symmetric keys are then used to encrypt and decrypt large amounts of data immediately afterward. This hybrid approach is much more feasible, i.e., computationally efficient, for large amounts of data than the continuous use of public-key encryption for every message. Schemes like ECDH guarantee high confidentiality while limiting resource usage, effectively meeting the stringent performance requirements of IoT devices [12]. The small key size of ECC also reduces exchange costs, making it ideal for frequent session key establishment operations.

3.2.2. Data integrity verification

Using the digital signature capabilities of ECC, including ECDSA, connected objects can sign data packets before sending them. The receiver can then verify this digital signature to ensure that the data has not been tampered with or corrupted during transmission [13]. This mechanism provides strong proof of data integrity. The protocol ensures the information received will be exactly matched

DOI: 10.54254/2753-8818/2025.DL28336

with the information sent. This is particularly important for critical IoT applications where data accuracy and authenticity are paramount. The application scenario of the data integrity verification includes preventing command tampering, and remote medical monitoring.

3.2.3. Access control for data storage

ECC-based cryptosystems can be directly integrated into access control solutions for IoT data stored in cloud environments, edge servers, or local databases. By properly leveraging digital signatures and secure key management, data owners can precisely authenticate specific devices and applications. They can also access, modify, and delete specific data sets, just like end users. This precise control ensures the confidentiality and integrity of data at rest. For example, a doctor can authorize a specific medical device to upload patient data to a secure cloud. An approval process can also be created to ensure that only authorized personnel with the correct ECC keys can access the data later.

3.3. Privacy protection in the IoT

In the IoT industry, it is becoming increasingly important to protect sensitive information from user devices. ECC helps ensure effective privacy protection and prevent unauthorized tracking and profiling [14].

3.3.1. Anonymous authentication

ECC can be utilized to design cryptographic protocols that enable IoT devices to authenticate with a network or service without revealing their permanent, unique identity [15]. This is often achieved through advanced techniques such as the generation of temporary pseudonyms. It can also be used in zero knowledge proofs where one party can prove knowledge of a secret without revealing the secret itself, or blind signatures. These methods protect user privacy and security. They prevent long-term tracking and correlation of activities across different sessions. These mechanisms are particularly useful in applications such as smart city infrastructure. They can also be used to help designing privacy-conscious smart streetlights that report their status without revealing their exact identity. They can even applied in connected cars for anonymous traffic data sharing and healthcare monitoring devices.

3.3.2. Location and identity obfuscation

There are some sophisticated techniques built upon ECC enable the verification of a device's attributes. These technologies allow people to verify that they present in particular area without leak their personal information about the device's precise location. Broad tracking and detailed profiling of users and devices will be ban under the use of these technologies. For example, using these technologies, smart home devices can prove their presence on a user's home network without disclosing their precise IP address to external services. These technics minimize the amount of transmit of personal information. They can significantly enhance privacy protection in distributed IoT environments.

DOI: 10.54254/2753-8818/2025.DL28336

4. Discussion

This section analyzes the overall benefits of ECC mechanisms as well as their inherent challenges. This paper discusses practical considerations for the appropriate selection and implementation of ECC in various IoT scenarios. A clear understanding of these aspects, advantages, and disadvantages is essential to effectively leverage ECC in resource-constrained environments.

4.1. Advantages of ECC in IoT security

ECC's innate mathematical properties contributes to several advantages that make it an ideal fit for the resource-constraint IoT ecosystem. It simultaneously brings a high security with short key lengths, which is really handy for a device with limited processing power and memory.

A primary advantage of ECC is its ability to provide a comparable level of cryptographic strength to other cryptosystem with much shorter key length. Other widely used public-key cryptosystems, such as RSA, achieves the same security level with significantly longer key lengths than ECC [13]. For instance, to get 128 bits security level, people only need a 256-bit ECC key, while if they want to use RSA, they need a 3072-bit RSA key. Other cryptosystems which rely on the discrete logarithm problem need the same key length as RSA, which means 3072 bits, such as Elgamal and DH. This huge reduction in key size directly translates to a smaller computational load required for cryptographic operations. It provides a notably reduced memory footprint, which solves the biggest pain point for those IoT devices with limited processing power and storage capacities.

Due to the mathematical properties that allow for smaller key sizes, ECC operations are generally faster and more energy-efficient. ECC consume less electrical power compared to equivalent RSA operations that have the same security level. This enhanced efficiency is really ideal for battery-powered IoT devices. In those devices, energy conservation directly impacts device longevity, maintenance costs, and overall operational viability. The smaller key length leads to faster operations, also contributes to reduced latency in real-time IoT applications.

ECC's shorter key and signature lengths also reduce the size of data packets exchanged over the network. This reduction in data transmission overhead is essential for conserving valuable network bandwidth. ECC's advantages are evident in large-scale IoT deployments, especially when many devices communicate simultaneously and messages become congested. ECC also improves the efficiency of low-bandwidth wireless channels.

Overall, reduced data transmission translates to lower communication energy costs, faster transaction times, and improved network efficiency [16].

4.2. Challenges faced by ECC in IoT applications

After thoroughly analyzing the compelling benefits of ECC, it is essential to recognize its integration into IoT. People should acknowledge that ECC introduce a smaller key scale in the encryption scheme. But with the widespread implementation in highly heterogeneous IoT environments, it also poses challenges. Overcoming these challenges is essential for the successful adoption of ECC. The primary implementation complexity lies in the difficulty of implementing ECC's entirely new mathematical structure and corresponding combination rules on devices. While theoretically efficient, the underlying mathematical operations are even more complex than traditional cryptosystems. In terms of key scale, ECC is much shorter than Elgamal and RSA. However, from a computational perspective, classical number-theoretic cryptosystems are computationally easier. The difficulty of elliptic curve computations increases implementation

DOI: 10.54254/2753-8818/2025.DL28336

complexity, posing significant challenges for deployment on ultra-low-power microcontrollers and dedicated IoT processors. This phenomenon is particularly pronounced in devices with limited instruction sets, limited clock frequencies, or small memory footprints. Improper or naive implementations are prone to inadvertently introducing side-channel vulnerabilities like timing analysis, power analysis attacks. An attacker can deduce this sensitive cryptographic information by observing physical characteristics of the device's operation, if not meticulously designed, optimized, and protected.

The standardization and interoperability also need to be discussed. Although the core ECC algorithms and commonly used curves are generally well-standardized by reputable bodies such as NIST (National Institute of Standards and Technology), ensuring seamless interoperability across the highly diverse and heterogeneous IoT landscape can be a substantial hurdle. Different IoT device manufacturers, application domains, or even regional regulatory frameworks might adopt varying elliptic curves, specific parameter sets, or unique protocol variations. This fragmentation can lead to significant compatibility issues when devices from different vendors or ecosystems attempt to communicate securely, hindering widespread adoption and potentially creating isolated security silos within the broader IoT. Efforts towards unified standards for ECC profiles in IoT are still ongoing [17].

4.3. Appropriate selection of ECC for IoT scenarios

Given the diverse nature of IoT applications and the wide range of device capabilities, the appropriate selection and configuration of ECC parameters and protocols are crucial for optimizing security, performance, and resource utilization. A "one-size-fits-all" approach is rarely effective. The choice of specific elliptic curve parameters like the chosen key size, the prime field used, the specific curve equation represents a fundamental and critical trade-off. It involves balancing the desired level of cryptographic security against the achievable computational performance on a given resource constrained device. For devices with extremely low power budgets and minimal processing capabilities like simple passive RFID tags or very basic environmental sensors, a smaller, more optimized curve like 160-bit ECC, it might be sufficient to meet basic security needs. Conversely, for critical infrastructure IoT devices handling highly sensitive data like in medical implants, industrial control systems, or autonomous vehicles, a larger and more robust curve, maybe 256-bit or 384-bit ECC, might be mandated, even if it incurs slightly higher computational costs. This decision should be based on a thorough risk assessment.

The choice of the specific ECC protocol or scheme should be meticulously aligned with the security services required by the particular IoT application. For fundamental data integrity and authenticity like verifying firmware updates, confirming the origin of sensor readings, or securing command and control messages, ECDSA is the primary and most suitable choice. For establishing secure and confidential communication channels, ECDH is the standard protocol for key exchange. ECDH is widely used for encrypted data exchange between smart meters and utility servers. It often employs symmetric encryption. To achieve more advanced privacy features, more sophisticated ECC methods may be required [18]. This includes the scenarios mentioned before, such as anonymous data collection in smart cities and identity verification without revealing identity.

To maximize the use of ECC in resource-constrained IoT devices, a hardware-software co-design approach is effective. This allows ECC implementations to be matched with specific cryptographic accelerators or dedicated instruction sets for modular arithmetic, improving the efficiency of ECC operations. It is also effective to develop optimized memory architectures that can be used with the target microcontroller or system-on-chip (SoC). Careful co-design of cryptographic primitives and

DOI: 10.54254/2753-8818/2025.DL28336

hardware functions allows ECC to be adapted to almost any environment. This allows developers to maximize efficiency, reduce power consumption, and minimize the overall resource footprint. The ultimate goal is to extend device life and improve performance.

5. Conclusion

5.1. Research results and conclusions

This research has thoroughly highlighted the critical role of ECC in dealing with the escalating security challenges within the expanding IoT. The author has demonstrated the compelling advantages ECC has compared to other cryptosystems. It can be designed to become uniquely suitable cryptographic solution for resource-constrained IoT devices due to the short key size and high security level. This can be translated directly into reduced computational overhead and efficient bandwidth utilization. The paper has detailed the basic concepts of elliptic curves and ECC's fundamental mathematical principles, including those unique combination rules and the difficulty of solving the ECDLP. Furthermore, the paper explored ECC's specific applications in key areas of IoT security. ECC is especially capable in mutual and scalable device authentication. The encryption schemes, like ECDH and ECDSA, stand out in various fields such as secure data transmission and storage, integrity verification, and access control. ECC also plays a vital role in privacy protection mechanisms such as anonymous authentication and identity obfuscation.

5.2. Impact and role of this research

This research significantly contributes to the current understanding of ECC's applicability and efficacy in IoT security. This paper synthesizes existing knowledge from recent academic literature and clearly identifies the key benefits and challenges inherent in ECC, providing a systematic and accessible framework for understanding this complex field. It is intended to serve as a reference for researchers working on developing new security protocols for IoT. It also serves as inspiration for developers implementing secure solutions in real-world IoT environments with resource constraints. By sharing this knowledge, this paper highlights gaps in the current state of ECC and offers precise suggestions for solving real-world IoT problems.

5.3. Outlook for future research

While ECC offers significant benefits for current IoT security, it is essentially a number-theoretic cryptography. Given technological advances and the constant evolution of cyber threats, future research must address several key points:

Implementation complexity and countermeasures: More robust and effective countermeasures against side-channel attacks must be continually sought. Finding customized solutions to manage the complexity of implementing ECC in constrained IoT environments is always key. ECC is good enough for the key scale, but not as ideal in the computational process in a resource-constraint environment.

Post-Quantum Cryptography (PQC): A significant long-term challenge is the emergence of quantum computers, which will break almost all the number theory-based cryptosystem. Theoretically quantum computer can break ECC algorithms easily. Further investigation into PQC integration with ECC is necessary. Investigation involves exploring hybrid cryptographic schemes that combine ECC with quantum-resistant algorithms. This could involve lattice-based cryptosystem, or McEliece cryptosystem, if possible.

DOI: 10.54254/2753-8818/2025.DL28336

By proactively addressing these areas, the IoT ecosystem can continue to leverage the strengths of ECC while adapting to future challenges. This is significant in ensuring a secure and trustworthy foundation for ubiquitous connectivity.

References

[1] Fadia, T., & Toufik, L. (2024). "Elliptic curves cryptography for lightweight devices in IoT system." Brazilian Journal of Technology, 7(4), e73725.
[2] Ullah, S., Jiangbin, Z., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey." Computer Science Review, 47, 100530.
[3] Koblitz, N. (1987). "Elliptic curve cryptosystems." Mathematics of Computation, 48(177), 203-209. (This is a foundational paper, not a recent one as previously cited, so the publication date is 1987.
[4] Khan, M. R., Upreti, K., Alam, M. I., Khan, H., Siddiqui, S. T., Haque, M., & Parashar, J. (2023). "Analysis of Elliptic Curve Cryptography & RSA." Journal of Information and Communication Technology Systems, 12(3), 358-368.
[5] Thapar, P., & Batra, U. (2022). "Implementation of Elliptical Curve Cryptography Based Diffie-Hellman Key Exchange Mechanism in Contiki Operating System for Internet of Things." International Journal of Electrical and Electronics Research, 10(2), 335-340.
[6] Mishra, S., Dwivedi, R., & Jha, R. K. (2023). "A Lightweight Authentication Scheme Based on ECC for IoT." In Proceedings of the International Conference on Applied and Theoretical Computing and Communication Technology. Springer.
[7] Khalique, A., Siddiqui, F., Ahad, M. A., & Hussain, I. (2025). "Lightweight authentication for IoT devices (LAID) in sustainable smart cities." PLOS ONE, 20(2), e0318064.
[8] Choubisa, M., & Jajal, B. (2025). "Analysis of Secure Authentication for IoT using Token-based access control." International Journal of Scientific Research in Computer Science and Engineering, 13(1).
[9] Li, B., Zhang, G., Lei, S., Fu, H., & Wang, J. (2022). "A Lightweight Authentication and Key Agreement Protocol for IoT Based on ECC." 2021 International Conference on Advanced Computing and Endogenous Security (ACES), 1-5.
[10] Al-Ghanim, H., Al-Mogren, A., & Al-Majed, H. (2025). "Design and analysis of lightweight and robust authentication protocol for securing the resource constrained IIoT environment." PLOS One, 20(2), e0318064.
[11] Nita, S. L., & Mihailescu, M. I. (2023). "Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain." Sensors, 23(3), 1371.
[12] AlMajed, H., & AlMogren, A. (2020). "A Secure and Efficient ECC-Based Scheme for Edge Computing and Internet of Things." Sensors, 20(21), 6158.
[13] Quiroz, E. A. P. (2023). "Elliptic curves cryptography for lightweight devices in IoT systems." ResearchGate. (This is a systematic review posted to ResearchGate, and a full formal reference is not available, but the authors are listed as Ana Simon Francia, Javier Solis-Lastra, and Erik Alex Papa Quiroz).
[14] Uslu, M. (2024). "PERFORMANCE COMPARISON OF ECC LIBRARIES FOR IOT DEVICES." Eskişehir Technic - Journal of Engineering Technology and Applied Sciences, 1(1), 21-29.
[15] Kavianpour, S., et al. (2025). "Security Evaluation of Provably Secure ECC-Based Anonymous Authentication and Key Agreement Scheme for IoT." Journal of Computer Networks and Communications, 2025.
[16] Lopez, J., Cadena, V., & Rahman, M. S. (2025). "Evaluating Post-Quantum Cryptographic Algorithms on Resource-Constrained Devices." arXiv preprint arXiv: 2507.08312.
[17] Wu, X. (2025). "How quantum computing will challenge IoT security." Insights2TechInfo. (This appears to be a blog post-style article, a full formal reference may not be available).
[18] Liu, T., Ramachandran, G., & Jurdak, R. (2024). "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization." arXiv preprint arXiv: 2401.17538.