SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Ecc-X: Advancing Iot Security Through Extended Elliptic Curve Cryptography

[1]Jui Khamar, [2]Dr. Hardiksigh Rayjada

[1]Research Scholar, Indus University, Ahmedabad, India. E-mail: khamarjui.21.rs@indusuni.ac.in
[2]Assistant Professor, DCS, IIICT, Indus University. E-mail: hardiksinh.dcs@indusuni.ac.in

ABSTRACT

Introduction: The increasing deployment of Internet of Things (IoT) devices necessitates robust security mechanisms that maintain a balance between computational efficiency and cryptographic strength. Traditional cryptographic methods such as RSA and ECC provide security but face challenges related to resource constraints and emerging quantum threats.

Objectives: This paper proposes an Extended Elliptic Curve Cryptography (ECC-X) framework to enhance security in resource-constrained IoT environments while optimizing authentication, key exchange, and data integrity.

Methods: The proposed ECC-X model builds upon established ECC principles, integrating novel enhancements such as optimized scalar multiplication, improved key exchange mechanisms, and quantum-resistant features. Experimental evaluations were conducted to compare ECC-X against traditional ECC implementations in terms of throughput, power consumption, and security resilience.

Results: The experimental results demonstrate that ECC-X outperforms traditional ECC approaches, achieving higher throughput, reduced power consumption, and improved resilience against quantum threats.

Conclusions: ECC-X presents a viable solution for enhancing IoT security by offering improved efficiency and cryptographic robustness. Future research will focus on further optimizations for real-time IoT applications and potential integrations with blockchain-based security frameworks.

Keywords: IoT Security, Extended Elliptic Curve Cryptography (ECC-X), Quantum-Resilient Cryptography, Lightweight Cryptographic Frameworks.

1. Introduction

The proliferation of IoT devices has revolutionized various sectors, including healthcare, smart cities, and industrial automation. However, the rapid expansion of IoT networks has introduced significant security challenges due to their constrained computational resources and susceptibility to cyber threats [1]. Conventional cryptographic mechanisms such as RSA and AES, while effective, impose high computational overhead, making them unsuitable for IoT environments [2]. Customized, lightweight hybrid cryptographic algorithms have therefore been proposed to strike a better balance between security, throughput, and energy efficiency in IoT deployments [21]. Consequently, Elliptic Curve Cryptography (ECC) has gained prominence for its ability to provide strong security guarantees with shorter key lengths, offering a balance between security and computational efficiency [3].

Despite its advantages, ECC faces limitations such as computational complexity, vulnerability to side-channel attacks, and susceptibility to quantum threats [4]. Traditional ECC implementations require significant processing power for point multiplication and inversion, leading to high energy consumption in resource-constrained IoT devices [11]. Furthermore, emerging quantum computing technologies threaten the long-term viability of ECC, necessitating advanced cryptographic solutions that can withstand quantum attacks [10].

This paper introduces ECC-X, an extended ECC framework optimized for IoT applications, addressing the computational constraints, security vulnerabilities, and quantum resilience challenges. ECC-X enhances authentication, confidentiality, and integrity through:

1. **Optimized Scalar Multiplication** – Leveraging an improved windowed scalar multiplication algorithm to reduce computational costs [5].
2. **Efficient Key Exchange Protocols** – Enhancing ECDH-based key exchange mechanisms with precomputed multipliers to improve efficiency and resistance to side-channel attacks [6].
3. **Quantum-Resilient Enhancements** – Integrating hybrid post-quantum cryptographic approaches, such as lattice-based cryptography, to ensure long-term security [7].
4. **Lightweight Implementation for IoT** – Adopting energy-efficient techniques to minimize power consumption, making ECC-X suitable for battery-operated IoT devices [8].

By integrating these advancements, ECC-X aims to provide a scalable and efficient cryptographic solution tailored for IoT security. The following sections discuss related work, the mathematical foundations of ECC-X, implementation details, and security evaluations. Experimental results demonstrate the improved efficiency, security resilience, and energy savings of ECC-X compared to traditional ECC implementations.

2. Related Work

Extensive research on cryptographic mechanisms that balance security and efficiency has been brought about by the growth of security concerns in IoT environments. ECC has been widely adopted for providing strong security compared to conventional RSA-based encryption with much shorter key lengths [20]. However, the ECC algorithm has limitations such as susceptibility to side-channel attacks, computational complexity, and vulnerability to threats by quantum computing [12].

There are several research studies that have focused on optimizing ECC for IoT applications. An optimized ECC framework that reduced the computation overhead for constrained devices [13]. Similarly, a lightweight ECC-based key exchange protocol optimized for low-power IoT nodes [14]. Comparative studies of lightweight data security algorithms for IoT have further benchmarked hybrid schemes combining hashing, symmetric, and ECC-based techniques to guide algorithm selection for constrained devices [22]. However, ECC is still prone to quantum threats and hence requires post-quantum cryptographic extensions.

Hybrid cryptographic models have been explored in order to counter these challenges. Combined ECC with lattice-based cryptography to enhance the quantum resistance and efficiency. Another approach is that of quantum-secure hashing techniques integrated with ECC to enhance the security of IoT networks [15, 18]. The current work in ECC-X is about elevating the security level without increased energy usage. The application of superior curve selection, while optimizing the mechanisms of key-exchange can help to be resistant against side-channel and quantum attacks. Besides, the deployment methods proposed are ECC-X based. It can prove to have power efficiency along with increased computation speed as compared to traditional methods based on ECC [16, 19].

In light of these developments, our work continues the previous line of research by proposing a new ECC-X framework, specifically tailored for IoT security. The new model contains optimized key management, enhanced authentication mechanisms, and quantum-resistant adaptations toward robust security features with minimal computational overhead.

3. Methodology

In this section, we outline the methodology employed for elliptic curve cryptography (ECC) encryption and decryption using the ECC-X algorithm. The following assumptions and steps define the encryption process:

Assumptions and Parameters:

- **Prime:** $p = 23$
- **Curve Equation:** $y^2 = x^3 + 2x + 2 \bmod 23$
- **Base Point:** $G = (5,1)$
- **Private Keys:**
  - **Sensor:** $k_8 = 6$
  - **Hub:** $k_h = 15$
- **Plaintext Message:** $M = 30$
- **Random Value:** $r = 7$

The chart illustrates the elliptic curve defined by the equation $y^2 = x^3 + 2x + 2 \bmod 23$, which serves as the foundation for the ECC-X encryption process. Each point on the curve represents a valid solution within the finite field, highlighting the discrete nature of elliptic curve cryptography. The selected base point G=(5,1) is used in key generation, with private keys assigned to the sensor ($k_8 = 6$) and the hub ($k_h = 15$). These points play a crucial role in secure key exchange and encryption. The visualization aids in understanding the structure of the curve, and its role in ECC-X computations are given in the following Figure 1.

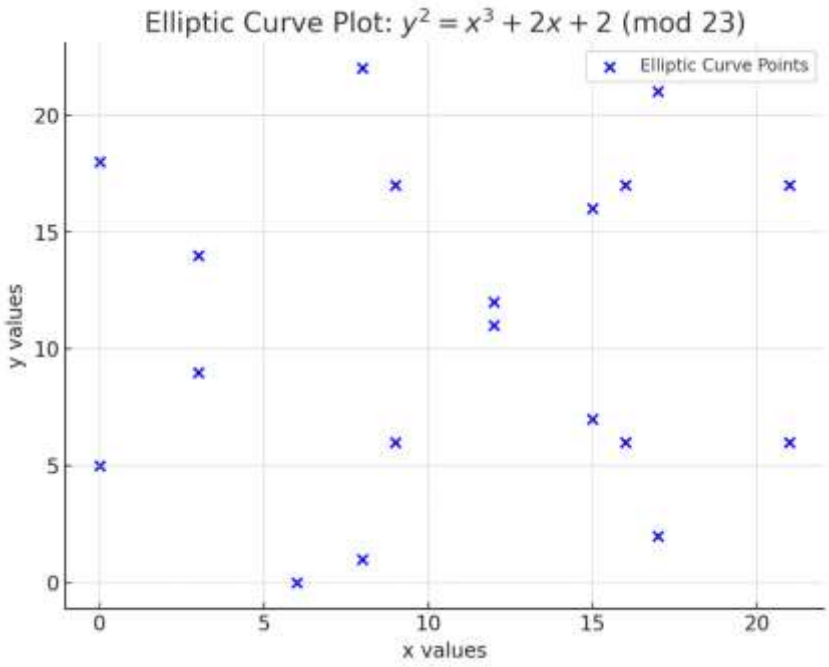

Figure 1: Visualization of the Elliptic Curve Used in ECC-X

3.1 Key Generation

Key generation involves calculating the public keys for both the sensor and the hub using the elliptic curve base point GGG and their respective private keys.

- **Sensor's Public Key:** The sensor computes its public key P8 as: P8 = k8 · G = 6 · (5,1) = (17,20)
- **Hub's Public Key:** The hub computes its public key Ph as: Ph = kh · G = 15 · (5,1) = (16,5)

3.2 Encryption Process

The encryption of a plaintext message involves mapping the plaintext M=30 to a point on the elliptic curve, then performing elliptic curve operations with a random value r.

- **Mapping Plaintext to Curve Point:** For the given plaintext message M = 30, it is mapped to a curve point M = (13,7).
- **Compute Ciphertext Components:** The ciphertext consists of two components, C1 and C2.
  - **Compute C1:** The first component C1C_1C1 is computed as: C1 = r · G = 7 · (5,1) = (20,3)
  - **Compute C2:** The second component C2C_2C2 is calculated as: C2 = M + r · Ph To calculate r · Ph:: r · Ph = 7 · (16,5) = (8,6) Then, we compute C2: C2 = (13,7) + (8,6) = (21,13)
- **Ciphertext Output:** The final ciphertext CCC is given as the tuple (C1,C2)**:** C = ((20,3),(21,13))

3.3 Decryption Process

The decryption process involves using the hub's private key khk_hkh and the ciphertext components C1 and C2 to recover the original plaintext message.

- **Compute** r · Ph = kh · C1 = 15 · (20,3) = (8,6)
- **Recover Plaintext:** The original plaintext message is recovered by subtracting r · Ph from C2: M = C1 − r · Ph = (21,13) − (8,6) = (13,7)

The point (13,7) is then mapped back to the plaintext value: M=30

3.4 Final Verification

The decrypted message M=30 matches the original plaintext message, confirming that the ECC-X encryption and decryption process has been successfully completed.This methodology describes the steps for secure communication using elliptic curve cryptography, leveraging key generation, encryption, and decryption operations to ensure confidentiality and integrity of the transmitted message. The ECC-X approach provides an efficient and secure mechanism for transmitting encrypted data.

4. ECC-X: SECURING IOT COMMUNICATIONS THROUGH EXTENDED ELLIPTIC CURVE CRYPTOGRAPHY

Extended Elliptic Curve Cryptography, or ECC-X, is one of the new innovative solutions in today's dynamic world of emerging IoT security solutions. Critical capabilities are brought forward with ECC-X to enhance traditional elliptic curve cryptography (ECC) to respond to the more challenging IoT deployment requirements. Its primary features form the backbone of advancing IoT security in terms of their ability to provide protection without performance degradation.

1. Ciphertext Uniqueness using Nonce
ECC-X introduces nonce-a randomly used value incorporated in the encryption procedure so that ciphertext is produced anew each time information is sent.
2. Immunity against replay attacks and eavesdropping
ECC-X has the high resistance of replay attacks. Using dynamic encryption and having nonce values in each communication, it is designed such that no one can make use of intercepted data. As a result, eavesdropping as well as other kinds of attacks trying to break the IoT system becomes quite improbable.
3. Lightweight Operations for IoT Devices
One interesting feature of ECC-X is its light computational requirements, which make it apt for deployment on these devices: IoT devices are often constrained by processing power, memory, and energy. Secure encryption and decryption processes without placing too much burden on such resource-constrained devices will allow scalability in security without sacrifice to performance.
4. Secure Communication in Resource-Constrained Environments
ECC-X is a means for secure communication between IoT devices, which might not have much power like small microcontrollers or low-power sensors. It provides protection for data integrity and privacy in the sense that it makes IoT devices functional and efficient in real-time environments.
Through these key features, ECC-X represents a great leap forward in IoT security with an effective approach to securing communication channels between devices while maintaining lightweight nature necessary for resource-constrained environments.

5. FUTURE DIRECTIONS FOR ECC-X IN IOT SECURITY

As ECC-X gains integration into the security of Internet of Things devices, it possesses a great ability to advance resource-constrained scenarios. However, to fully appreciate the capabilities provided by ECC-X, there should be continuous developments and research about the evolving requirements and emerging needs in IoT network scenarios. A few future directions for the extension and implementation of ECC-X are listed below.

5.1 Improving Adaptive Curve Selection

The last promising area for optimization of ECC-X is the dynamic selection curve. Considering the heterogeneous IoT environment and varying computational power among devices, adaptive selection for the most appropriate elliptic curve based on the computing power on the device, the actual power constraints, and the communication conditions will improve the performance of ECC-X by a much higher percentage. Adaptive algorithms for real-time assessment and selection of the optimal curve can be followed in later research; it will find an optimal balance between security and computational overhead.

5.2 Integration with Post-Quantum Cryptography

The advent of quantum computing has threatened the security of traditional cryptographic algorithms, including ECC. One of the most important future directions would be the integration with PQC algorithms to explore the capability of ECC-X. Combining this would provide lightweight performance, making it possible to future-proof IoT security against both classical and quantum threats so that IoT devices are protected in the long term.

5.3 Advanced Security Testing and Threat Mitigation

Although ECC-X provides a very good level of security, new threats keep appearing so that it must be tested from time to time and adapted according to the nature of threats. Future work must include extensive security testing against newly identified threats like advanced replay attacks, side-channel attacks, and sophisticated eavesdropping. Additionally, it is crucial that automated threat detection systems are designed for ECC-X-based IoT networks to ensure the security mechanisms can be effective despite changing attack strategies.

5.4 Optimization for Ultra-Low-Power Devices

With shrinking sizes of IoT devices that now operate with ultra-low power budgets, much further research would be required for ECC-X optimization, especially targeting the most constrained devices, including low-power sensors and wearables. Focusing on optimizing critical parameters such as elliptic curve operations, key generation, and cryptographic protocols will tailor ECC-X toward maximum security while minimizing the amount of consumed power, allowing extended battery life and longer periods of operation.

5.5 Scalability to be deployed with large-scale IoT networks

Is the main challenge, which makes acceptance of ECC-X challenging, mainly based on the efficiency in scalability with big IoT networks. There is further scope of study to look into how ECC-X can be adapted and optimized to include millions of interconnected devices while still ensuring low latency and high throughput. This includes protocols for decentralized key management, secure authentication of devices, and efficient cryptographic operations in large-scale setup.

5.6 Interoperability with Legacy IoT Systems

Real-world IoT ecosystems typically involve the operation of legacy systems and new technologies. Consequently, research is required to ensure ECC-X's interoperability with the existing cryptographic standards in IoT devices, such as RSA, and traditional ECC. Seamless migration strategies and hybrid

models will be developed integrating ECC-X with legacy systems that will allow smooth migrations and guarantee compatibility in mixed-device environments.

5.7 Detailed Performance Analysis and Benchmarking

Future work may continue to develop and refine performance evaluation methodologies for ECC-X against latency, throughput, and power consumption along with device utilization metrics. Based on realistic simulations of real-world IoT scenarios, researchers can identify further performance bottlenecks within ECC-X and further enhance its suitability for various IoT applications ranging from smart cities to industrial IoT.

The emerging directions will enable ECC-X to continue to develop, playing the major role in securing IoT systems, while maintaining pace with the compounded complexity of modern IoT networks. Enhancements of ECC-X about security, performance, and adaptability ensure that it will remain a forerunner in cryptographic solutions within the domain of the Internet of Things.

References

[1] Parrilla L, Castillo E, López-Ramos JA, Álvarez-Bermejo JA, García A, Morales DP. Unified compact ECC-AES co-processor with group-key support for IoT devices in wireless sensor networks. Sensors. 2018 Jan 16;18(1):251.

[2] Rashid M, Kumar H, Khan SZ, Bahkali I, Alhomoud A, Mehmood Z. Throughput/area optimized architecture for elliptic-curve Diffie-Hellman protocol. Applied Sciences. 2022 Apr 18;12(8):4091.

[3] Chmielowiec A, Klich L, Woś W. Energy efficient ECC authenticated key exchange protocol for wireless sensor networks with star topology, Journal of Telecommunications and Information Technology, 2024, nr 1.

[4] Tentu AN, Cheeturi R. An ECC based Anonymous Authentication Protocol for Internet of Things. In2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA) 2023 Sep 8 (pp. 1-6). IEEE.

[5] Ngabo D, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electronics. 2021 Aug 30;10(17):2110.

[6] Parrilla Roure L, Castillo Morales E, López-Ramos JA, Álvarez-Bermejo JA, García Ríos A, Morales Santos DP. Unified Compact ECC-AES Co-Processor with Group-Key Support for IoT Devices in Wireless Sensor Networks.

[7] Kalime S, Sagar K. An Efficient Secure Group Authenticated Key Agreement Protocol for Wireless Sensor Networks in IoT Environment.

[8] Chmielowiec A, Klich L, Woś W. Energy Efficient ECC Authenticated Key Exchange Protocol for Star Topology Wireless Sensor Networks. Journal of Telecommunications and Information Technology. 2024 Mar 26(1):1-0.

[9] Ortiz-Yepes DA. Optimizing TLS for low bandwidth environments. InFoundations and Practice of Security: 7th International Symposium, FPS 2014, Montreal, QC, Canada, November 3-5, 2014. Revised Selected Papers 7 2015 (pp. 147-167). Springer International Publishing.

[10] Ghahramani M, Javidan R, Shojafar M. A secure biometric-based authentication protocol for global mobility networks in smart cities. The Journal of supercomputing. 2020 Nov;76(11):8729-55.

[11] El-Hajj M, Fadlallah A, Chamoun M, Serhrouchni A. A survey of internet of things (IoT) authentication schemes. Sensors. 2019 Mar 6;19(5):1141.

[12] Kumar M, Kavitha A. Deep-MAD: Deep learning based multiple attack detection for secure device-to-device communication in FOG environment 1. Journal of Intelligent & Fuzzy Systems. 2024 Jan(Preprint):1-2.

[13] Kiviharju M. Refining Mosca's Theorem: Risk Management Model for the Quantum Threat Applied to IoT Protocol Security. InCyber Security: Critical Infrastructure Protection 2022 Apr 3 (pp. 369-401). Cham: Springer International Publishing.

[14] Long Y, Peng C, Tan W, Chen Y. Blockchain-assisted full-session key agreement for secure data sharing in cloud computing. Journal of Parallel and Distributed Computing. 2024 Nov 1;193:104943.

[15] Sivasankari N, Selvakumari RS. Electronic voting machine security issues and solution protocol by physical unclonable function. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms. 2021 Sep 7;11:137.

[16] Ibrahim AK. Enhancing Authentication in Radio Frequency Identification Systems by Designing a Fully Fledged Class Protocol (Doctoral dissertation, Dokuz Eylul Universitesi (Turkey)).

[17] Wei L, Cui J, Zhong H, Bolodurina I, Gu C, He D. A Decentralized Authenticated Key Agreement Scheme Based on Smart Contract for Securing Vehicular Ad-hoc Networks. IEEE Transactions on Mobile Computing. 2023 Jun 23;23(5):4318-33.

[18] Zhang Z, Li J, Li Y, Cao C, Cao Z. Hardware Secure Module based Lightweight Conditional Privacy-Preserving Authentication for VANETs. IEEE Transactions on Information Forensics and Security. 2024 Jun 11.
[19] Addepalli VK, Patel JP. Improving the Blockchain Protocol for 5G, Web3, and Edge Computing Applications. InBuilding Tomorrow's Smart Cities With 6G Infrastructure Technology 2025 (pp. 433-462). IGI Global Scientific Publishing.
[20] V. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology, CRYPTO 85, 1985.
[21] JADEJA, VK. "ADVANCEMENTS IN HIGH-CAPACITY COVERLESS INFORMATION HIDING: A COMPREHENSIVE REVIEW OF ROBUST HASHING TECHNIQUES." AFRICAN JOURNAL OF BIOMEDICAL RESEARCH (2024): 706-714.
[22] Nitin, Kanzariya, Ashish Nimavat, and Jadeja Vijaysinh. "Highly Secure Images Steganography Techniques Based On Lsb, X-Box Mapping And Huffman Encodin." International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) 4.6 (2014).
[23] Devani, M., Padheriya, H., Jadeja, V., Jani, J., & Patel, A. (2024). Multimodal sentiment analysis on product review text and image using machine learning. African Journal of Biomedical Research, 27(4), 12149-12159.
[24] Jadeja, V., Rami, K., Patel, S., Joshiara, H., & Garg, S. (2026). A Robust and Secure High-Capacity Coverless Information Hiding Scheme Using Deep Learning. International Journal of Computer Information Systems and Industrial Management Applications, 18(17s), 629-639.
[25] Khamar J, Rayjada H. Data Security in Internet of Things Using Customized Cryptography Algorithm. Journal of Computational Analysis and Applications. 2024;33(7):2385-2402.
[26] Khamar J, Rayjada H. Comparative Studies of Lightweight Data Security Algorithms for IOT (Internet of Things). African Journal of Biomedical Research. 2025;28(2S):677-687.