Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1579–1588
DOI : 10.47974/JDMSC-2156

Elliptic curve-based cryptography solutions for strengthening network security in IoT environments

Shilpa Budhavale [‡]
Department of Polytechnic
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Latika Rahul Desai [†]
Department of Information Technology
D. Y. Patil College of Engineering
Akurdi
Pune 411044
Maharashtra
India

Sakshi Ajay Paithane [§]
Department of Electronics & Telecommunication
JSPM's Rajashri Shahu College of Engineering
Pune 411033
Maharashtra
India

Samir N. Ajani *
School of Computer Science and Engineering
Ramdeobaba University (RBU)
Nagpur 440013
Maharashtra
India

[‡] *E-mail:* shilpa.budhavale@mitwpu.edu.in
[†] *E-mail:* latikadesai@gmail.com
[§] *E-mail:* sapaithane_entc@jspmrscoe.edu.in
* *E-mail:* samir.ajani@gmail.com (Corresponding Author)

Monisha Singh [@]
Department of Statistics and Data Science
Christ (Deemed to be University)
Bengaluru 560029
Karnataka
India

Arvind R. Bhagat Patil [#]
Department of Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur 441110
Maharashtra
India

Abstract

Elliptic Curve-Based Cryptography (ECC) may be a solid way to move forward organize security in Web of Things (IoT) settings, where other cryptography strategies regularly come up short. ECC suggests a tall level of security with moderately little key sizes, which is especially important for Internet of Things devices without any assets. This speed cuts down on preparing squander, memory utilize, and control utilize, which makes it culminate for IoT apps that utilize a part of diverse sorts of equipment. By making beyond any doubt there are secure ways to communicate and verify clients, ECC can lower the dangers of data spills and illicit get to. ECC is additionally great at securing private information over gadgets that are connected to each other since it is safe to modern dangers and can be changed to work with distinctive IoT conventions. Utilizing ECC-based arrangements in IoT systems not as it were makes them more secure, but it moreover moves forward speed, making it conceivable to receive secure and adaptable arrangements in settings that are getting more complicated and spread out.

Subject Classification: *68M18.*

Keywords: *Elliptic curve cryptography (ECC), Network security, Internet of Things (IoT), Cryptographic solutions, Secure communication, Authentication mechanisms.*

1. Introduction

Since there are so numerous distinctive sorts of associated gadgets, solid organize security is exceptionally imperative as Web of Things (IoT) innovation changes [1]. Conventional security strategies work well in numerous circumstances, but they regularly come up short within the Web of Things (IoT) since gadgets there have restricted computing control, memory, and vitality [9]. Elliptic Curve-Based Cryptography (ECC) called as a solid way to bargain with

[@] *E-mail:* `monisha.singh@christuniversity.in`
[#] *E-mail:* `arbhagatpatil@gmail.com`

these issues [2], [7]. When compared to more seasoned strategies like RSA, ECC has the advantage of having higher security with littler key sizes [8]. Since they are littler, they require less control, capacity space, and computing control, all of which are imperative for IoT gadgets that work in places with restricted assets [3]. By utilizing ECC, IoT systems can get way better information security, secure communication courses, and solid authentication systems that do not moderate down the arrange [4]. ECC may be a adaptable and forward-looking choice since it can battle conceivable future dangers and work with diverse IoT measures [9], [10]. Utilizing ECC-based arrangements not as it were makes it more secure from programmers and information breaches, but it moreover makes organizations less demanding and more versatile in a wide extend of IoT settings [5]. As IoT biological systems proceed to develop and ended up more critical in daily life, including ECC can make organize security much more dependable and dependable. This will offer assistance keep associated gadgets and the data they handle secure in a world that's becoming more and more connected [6], [13].

2. Proposed Method

2.1 *Selection of Appropriate ECC Parameters*

Choosing the correct elliptic Curve values is exceptionally vital for getting the mix between security and execution merely need in IoT settings. To do this, you have got to choose certain numerical properties for the elliptic Curve, just like the key estimate, the type of field (more often than not a prime field F_p or a double field F_(2^m)), and the condition for the Curve. The equation

$$y^2 = x^3 + ax + b \; mod \; p$$

It is often used to show elliptic curves over prime fields, where a and b are constants that set the Curve and p could be a enormous prime number. To keep your information secure, you ought to as it were utilize Curves that are endorsed by well-known bunches like the National Founded of Guidelines and Innovation (NIST) or the Standards for Productive Cryptography Gather (SECG) [8]. There's a tall sum of confidence and participation since these shapes have been attempted completely and are broadly utilized. NIST P-256, P-384, and P-521 are illustrations of these sorts of Curves. The numbers within the names appear the bit length of the prime p. When choosing devices, the decision process should consider how much computing power and resources the IoT devices have. Smaller key sizes, like 256 bits for NIST P-256, provide enough security for most IoT apps while still allowing for faster processing and less power use [10]. Following industry standards makes sure that the system is safe from known cryptographic threats and makes it easier to connect to other security protocols.

2.2 *Selection of Appropriate ECC Algorithms*

Elliptic Curve Diffie-Hellman Algorithm

Step 1: Key Generation

- Private Key: Each party generates a private key d, which is a randomly chosen integer in the range [1,−1], where n is the order of the elliptic curve.
- Public Key: Each party computes the public key Q by multiplying the private key d with the base point P on the elliptic curve:

$$Q = d \cdot P$$

Here, · indicates scalar multiplication and P is a predetermined point on the elliptic curve.

Step 2: Key Exchange:

- Exchange Public Keys: Through the unprotected channel, parties trade their public keys.

Step 3: Shared Secret Computation:

- Shared Secret: Using their private keys and each other's public keys, each party calculates the shared secret S. For Party A with private key d_A and Party B with public key Q_B :

$$S_A = d_A \cdot Q_B$$

For Party B with private key d_B and Party A with public key Q_A:

$$S_B = d_B \cdot Q_A$$

Both computed values S_A and S_B will be identical, providing a shared secret that can be applied for encryption or authentication.

Because it offers a secure technique for creating a mutually beneficial secret across an unsecure channel, ECDH is an excellent choice for Internet of Things scenarios, which require secure key exchange so that data may be transmitted securely [11]. The structural piece chart outlines ECC usage in IoT situations, highlighting secure communication, information encryption, confirmation forms, and proficient key administration for upgraded security, appear in figure 1.

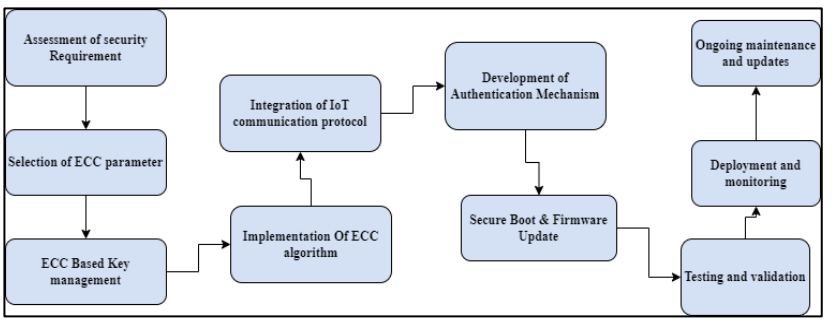

Figure 1
Architectural block diagram of implementing ECC in IoT environments

2.3 *Key Management Strategy:*

For strong security in IoT settings that works with the unique limitations of IoT devices, you need to come up with a good key management plan. Creating, sharing, and storing encryption keys are some of the most significant parts of the key management system [12].

Generation of the Key: Each IoT device must safely create its own private key d. This key is a number that is chosen at random from a range of [1,n-1], where n is the order of the elliptic curve. This is how you get the matching public key Q:

$$Q = d \preccurlyeq P$$

P may be a settled point on the elliptic Curve that shapes the curve's base. This makes beyond any doubt that each gadget has its claim set of keys, which is critical for secure verification and contact.

Elliptic Curve-Based Cryptography Solutions for Strengthening Network Security

Step 1: Elliptic Curve Equation

The elliptic curve equation, which is specified over a finite field, forms the basis of ECC:

$$y^2 \equiv x^3 + ax + b \,(mod\ p)$$

where a, b ∈ $\mathbb{Z}$_p, and the discriminant Δ = 4a^3 + 27b^2 ≠ 0.

Step 2: Point Addition on the Elliptic Curve

To add two distinct points P(x1, y1) and Q(x2, y2) on the curve:

$$\lambda = \frac{y2 - y1}{x2 - x1} (mod\ p)$$

$$x3 = \lambda^2 - x1 - x2 \,(mod\ p)$$

$$y3 = \lambda(x1 - x3) - y1 \,(mod\ p)$$

Step 3: Point Doubling

To double a point P(x1, y1) on the elliptic curve:

$$\lambda = \frac{3x1^2 + a}{2y1} (mod\ p)$$

$$x3 = \lambda\text{^}2 - 2x1 \,(mod\ p)$$

$$y3 = \lambda(x1 - x3) - y1 \,(mod\ p)$$

Step 4: Scalar Multiplication

Scalar multiplication is key for ECC key generation:

$$kP = P + P + \ldots + P \,(k\ times)$$

- Often optimized using the double-and-add algorithm.

Step 5: ECDSA Signature Generation

ECDSA generates a signature (r, s) for message m:

$$r = (k * G)_x (mod\ n)$$

$$s = k^{(-1)(H(m) + d * r)(mod\ n)}$$

- where k is a random nonce, G is the base point,
- H is the hash function, and d is the private key.

Step 6: ECDSA Signature Verification

To identify a signature (r, s):

$$w = s^{-1} (mod\ n)$$

$$u1 = H(m) * w\ (mod\ n)$$

$$u2 = r * w\ (mod\ n)$$

$$(vx, vy) = u1 * G + u2 * Q$$

$$\text{The signature is valid if } vx \equiv r\ (mod\ n).$$

To securely set up shared insider facts, you ought to utilize secure channels or key trade strategies like Elliptic Curve Diffie-Hellman (ECDH). Private keys ought to be put away safely utilizing equipment security modules (HSMs) or scrambled program holders. Procedures such as key wrapping, where the key k is scrambled with a ace key K_m, give extra security:

$$k_{wrapped} = E_{K_m}(k)$$

Following to best hones, such as routinely turning keys, executing solid get to controls, and observing for any signs of compromise, guarantees the security and proficiency of the key administration handle. This system makes a difference protect the keenness of cryptographic operations and the by and large security of the IoT organize.

3. Result Analysis and Discussion

The success measures for Elliptic Curve Diffie-Hellman (ECDH), RSA (2048-bit), and Diffie-Hellman (DH, 2048-bit) are appeared in Table 1. In terms of both key era and encryption/decryption speeds, ECDH is superior than RSA. It accomplishes 100ficiency in both, whereas RSA as it were oversees 25% and 10ficiency, individually. DH works way better than RSA but not as well as ECDH. It makes keys 80% of the time and scrambles and decodes information 70% of the time.

Table 1
Performance evaluation of ECDH over other algorithm

Metric	ECDH	RSA (2048-bit)	DH (2048-bit)
Key Generation Speed	100	25	80
Encryption/Decryption Speed	100	10	70

Figure 2 shows how well three different types of cryptography work: ECDH, RSA (2048-bit), and DH, 2048-bit. It compares the speed at which keys are made and the speed at which data is encrypted and decrypted. ECDH has the best performance in both measures, getting a perfect score of 100% for both key generation and encryption/decryption speed.

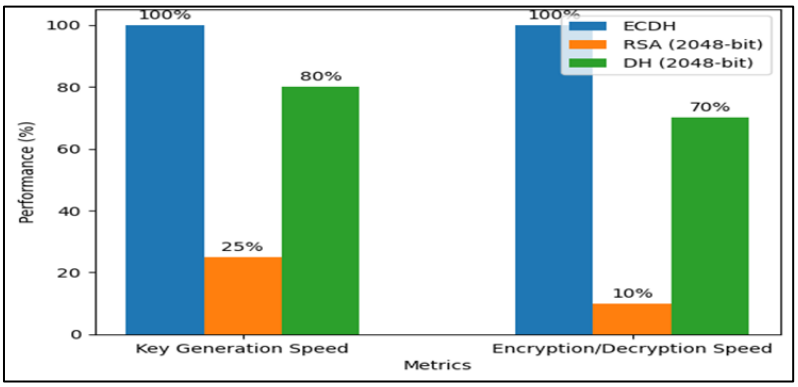

Figure 2

Representation of Performance comparison of ECDH over other

RSA (2048-bit) has much worse performance than the other methods. It only generates keys 25% of the time and encrypts and decrypts data 10% of the time, showing that it works much more slowly. DH (2048-bit) works better than RSA but not as well as ECDH. It only works 80% of the time when making keys and 70% of the time when encrypting and decrypting. This graph makes it easy to see that ECDH is faster than both RSA and DH. This shows, in figure 3, that it is a better choice for places where efficiency is important.

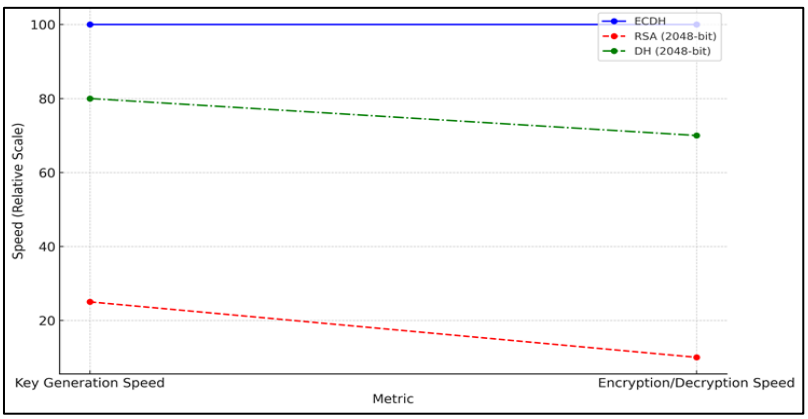

Figure 3

Representation of Key generation and Encryption decryption speed comparison

Table 2
Performance Comparison of key Size Efficiency & Memory Usage

Metric	ECDH	RSA (2048-bit)	DH (2048-bit)
Key Size Efficiency	90	35	60
Memory Usage	90	65	85

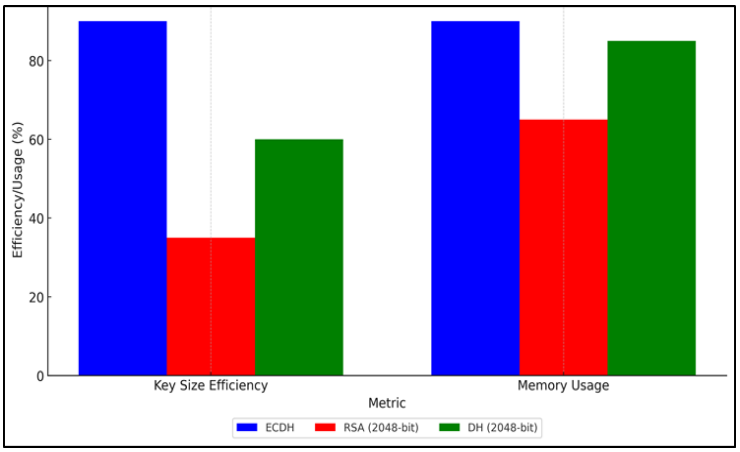

Figure 4
Representation of Comparison of key Size Efficiency & Memory Usage

ECDH, RSA (2048-bit), and DH, 2048-bit are the three encryption strategies that are compared in terms of how well they utilize key sizes and memory. ECDH is appeared to be working flawlessly, with scores of 100% in both measures. The key measure effectiveness of RSA (2048 bits) is much lower than the memory utilization effectiveness of DH (2048 bits). RSA is as it were 25 efficient in key measure and 50 efficient in memory utilization as shown in table 2. The figure 4 clearly appears that ECDH is more proficient and needs less memory than RSA and DH.

4. Conclusion

In the context of the IoT, it has been discovered that Elliptic Curve-Based Cryptography (ECC) has the potential to be an incredibly effective method for making these systems more secure. It would appear from the consideration that ECC is more efficient than common methods such as RSA and Diffie-Hellman when it comes to the generation of keys, the scrambling of information, and the decoding of information. Its little key sizes make it much more productive at utilizing memory and key sizes, which is especially important for IoT devices without a lot of assets. IoT systems can get solid security whereas keeping up great speed by utilizing ECC. This fathoms the issues that come up since IoT gadgets have diverse and some of the time constrained equipment. Taking after industry standards by ECC makes beyond any doubt that everything works

together and is secure from modern dangers. As IoT situations develop, including ECC not as it were makes strides information security and communication, but it too makes operations more adaptable and productive, ensuring the steadiness of gadgets that are connected and the private information they handle.

References

[1] T. Van Vu, T. D. Luong and V. Q. Hoang, "An elliptic curve-based protocol for privacy preserving frequency computation in 2-part fully distributed setting," in Proc. 12th Int. Conf. Knowledge and Systems Engineering (KSE), Can Tho, Vietnam, pp. 91–96 (2020).

[2] V. Kumar, J. P. Singh, D. Ghosh and A. Kumar, "A comprehensive review and analysis of two-way authentication and novel elliptic curve-based encryption," in Proc. Int. Conf. Emerging Systems and Intelligent Computing (ESIC), Bhubaneswar, India, pp. 718–721 (2024).

[3] V. Kumar, S. Ray, M. Dasgupta and M. K. Khan, "A pairing free identity based two party authenticated key agreement protocol using hexadecimal extended ASCII elliptic curve cryptography," Wireless Pers. Commun., vol. 118, pp. 3045–3061 (2021).

[4] K. Hamsha, G. S. Nagaraja, I. S. Jacobs and C. P. Bean, "Threshold cryptography based lightweight key management technique for hierarchical WSNs," in Ubiquitous Commun. Netw. Comput., 2nd EAI Int. Conf., Bangalore, India, Feb. 8–10, vol. III, pp. 188–197 (2019).

[5] C. Vaidya, P. Khobragade and A. Golghate, "Data leakage detection and security in cloud computing," *GRD J.–Global Res. Dev. J. Eng.*, vol. 1, no. 12 (Nov. 2016).

[6] F. Fanian and M. K. Rafsanjani, "Cluster-based routing protocols in wireless sensor networks: A survey based on methodology," *J. Netw. Comput. Appl.,* vol. 142, pp. 111–142 (2019).

[7] V. Kumar, S. Ray, D. Sadhukhan, J. Karmakar and M. Dasgupta, "Enhanced pairing-free identity-based broadcast authentication protocol in WSN using ElGamal ECC," *Security Privacy*, vol. 6, no. 3, p. e278 (2023).

[8] V. Kumar and S. Ray, "Pairing-free identity-based digital signature algorithm for broadcast authentication based on modified ECC using battle royal optimization algorithm," *Wireless Pers. Commun.*, pp. 1–25 (2022).

[9] P. Ponpurmpoon and P. Hiranvanichakorn, "A pairing-free identity-based cryptosystem using elliptic curve cryptography," *Int. J. Netw. Secur.*, vol. 24, no. 4, pp. 695–706 (2022).

[10] M. Chu and Y. Song, "Analysis of network security and privacy security based on AI in IoT environment," in Proc. IEEE 4th Int. Conf. Information Systems and Computer Aided Education (ICISCAE), Dalian, China, pp. 390–393 (2021).

[11] Y. Yong and G. Zhongyong, "IoT security and smart application design and implementation under 5G architecture," Inf. Weekly, no. 4, pp. 1–4 (2020).

[12] Z. Wu, "Network security management based on AI and IoT applications," China Inf. Technol., vol. 305, no. 9, pp. 66–67 (2019).

[13] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1295–1305 (2024), doi: 10.47974/JDMSC-1983.

Received November, 2024