Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2498

Enhancing secure access in RF communications through advanced elliptic curve encryption

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

Jayita Moulick [†]
Symbiosis Centre for Advanced Legal Studies and Research
Symbiosis Law School Pune (SLS-P)
Symbiosis International (Deemed University)
Pune 411014
Maharashtra
India

Jyoti Mohur *
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Hannah Jessie Rani R. [‡]
Department of Electrical and Electronics Engineering
Faculty of Engineering and Technology
JAIN (Deemed-to-be University)
Bengaluru 562112
Karnataka
India

[§] *E-mail:* samir.ajani@gmail.com
[†] *E-mail:* jayita.moulick@symlaw.ac.in
* *E-mail:* jyoti.mahur@niu.edu.in (Corresponding Author)
[‡] *E-mail:* jr.hannah@jainuniversity.ac.in

Amol Dattatray Sonawane [@]
Department of Electronics and Telecommunication Engineering
Nutan Maharashtra Institute of Engineering and Technology
Pune 410507
Maharashtra
India

Priti Shende [#]
Department of Electronics &Telecommunication
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

Abstract

Wireless communication technologies are developing so swiftly, particularly radio frequency (RF) interactions, that many people are concerned about the safety of transmitting data. Protecting the safety and security of data being delivered is a very important issue as RF communications are rather simple to intercept. This paper examines how sophisticated elliptic curve encryption (ECC) may be utilized to make RF interactions safer. ECC is well renowned for its favorable key size-to-security ratio. Its powerful method of safeguarding communication channels makes it ideal for locations with constrained processing power and speed. Our recommendation is a novel ECC-based encryption method meant to interact with RF communication systems and guard against typical issues such data leaks and illegal access. The suggested approach obviously speeds encryption and increases resistance against known attacks like espionage and man-in-the-middle. A complete study of how effectively the system operates in real-life RF environments shows that employing ECC not only increases security but also optimally uses resources. The results indicate that ECC may satisfy the rising need for safe, adaptable, and efficient RF transmission systems.

Subject Classification: *68M25.*

Keywords: *Elliptic curve cryptography, RF communications, Secure access, Encryption protocol, Data integrity.*

1. Introduction

Modern Wi-Fi structures are basically primarily based on Radio Frequency (RF) transmission. From cell smartphone networks to area communications, it enables wireless connection in an excellent type of situations. As the quantity of private data being transferred throughout RF lines increases [1], its protection has been greater quintessential. Even though they from time to time conflict

[@] *E-mail:* **amolsonawane1431@gmail.com**
[#] *E-mail:* **priti.jawale@dypvp.edu.in**

with the confined processing strength and bandwidth that accompany RF conversation technologies, traditional encryption strategies are powerful [2].

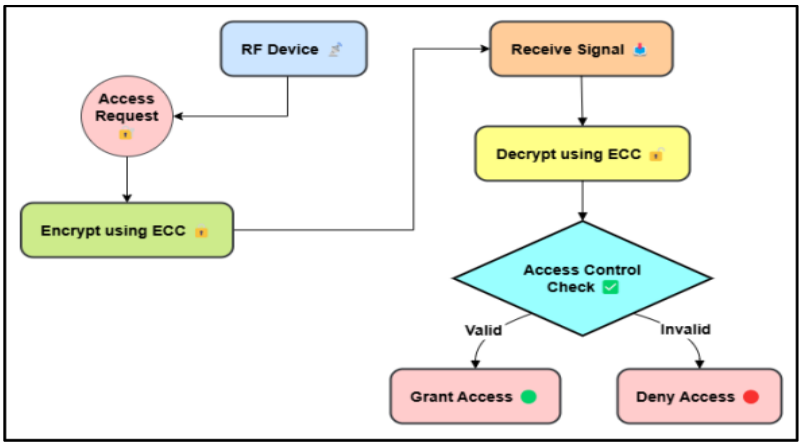

Figure 1

Illustrating Elliptic Curve Encryption in RF Access

This motivates individuals to are seeking stepped forward secure techniques that could provide strong protection besides the usage of too much device assets [3]. Elliptic curve encryption for safe RF gets right of entry to manage is proven in figure 1. Using elliptic curve cryptography (ECC) is one feasible method to increase protection in RF interactions [4]. As it gives a high diploma of protection with as an alternative modest key size while as compared to different cryptographic strategies like RSA [5][6], ECC is splendid for environments with limited assets. As it does not use a lot more processing electricity or information, ECC is an incredible choice for programs requiring both safety and pace. This look at discusses an extra state-of-the-art ECC-primarily based encryption scheme developed particularly for radio frequency communications [7]. The proposed solution protects against traditional radio frequency device weaknesses the usage of ECC's sturdy security characteristics, along with unauthorized get right of entry to by hackers, data change, and sign interception [8].

2. Computational hardness: Elliptic Curve Discrete Logarithm Problem (ECDLP)

The degree of protection of Elliptic Curve Cryptography (ECC) is predicated much on the problem of fixing the Elliptic Curve Discrete Logarithm trouble (ECDLP). Given two points on an elliptic curve, ECDLP is the approach of figuring out the number okay. For high quantities of ok, the trouble cannot be solved computationally, which guarantees the stableness of ECC [9]. Figure 2 shows the computational hardness of the ECDLP trouble.

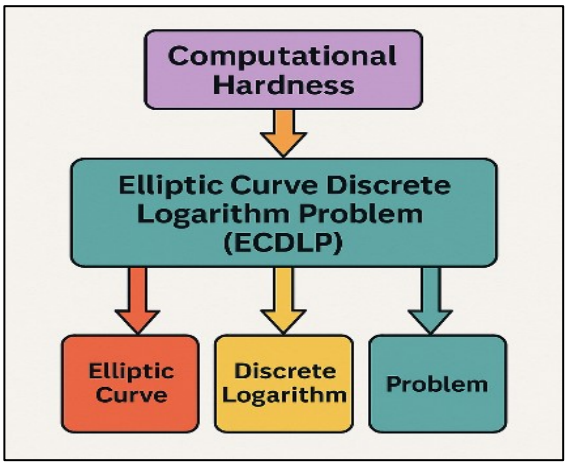

Figure 2

Elliptic Curve Discrete Logarithm Problem (ECDLP) Computational Hardness

Even though ECDLP is a famous hard problem, it has huge advantages over older cryptography strategies like RSA, which want lots bigger key sizes to get the same amount of safety [10][11]. Because the challenge goes up in a linear way as the curve gets bigger, ECC can provide safe encryption with much smaller key sizes. This makes it very useful in places with limited resources, like RF communications [12].

1. Elliptic Curve Equation

$$E: y^2 = x^3 + ax + b \,(mod\ p) \tag{1}$$

where a, b, and p are constants, and the curve is defined over a finite field F_p.

2. Base Point and Generator

$$P = (x_1, y_1) \tag{2}$$

where P is a base point on the elliptic curve.

3. Scalar Multiplication

$$Q = kP = (x_k, y_k) \tag{3}$$

where k is a scalar, and Q is the resulting point after multiplying P by k.

4. ECDLP Statement

Given P and Q, find k such that:

$$Q = kP \tag{4}$$

this is the essence of the problem — computing the discrete logarithm.

5. Point Addition

For any two points P = (x_1, y_1) and R = (x_2, y_2) on the elliptic curve:

$$P + R = (x_3, y_3) = \left(\frac{(x_1 y_2 - x_2 y_1)}{(x_1 - x_2)}, \frac{(y_1 y_2 - x_1 y_2)}{(x_1 - x_2)}\right) \quad (5)$$

This is the formula used for point addition in elliptic curve cryptography.

6. Scalar Multiplication by Doubling

   If k is even, k = 2m, then:

$$kP = 2mP = 2(mP) \quad (6)$$

   Where, kP the point doubling formula is used:

$$P + P = 2P = \frac{(3x_1^2 + a)}{(2y_1)} \quad (7)$$

7. Solving ECDLP

   The computational hardness lies in solving the equation:

$$Q = kP \quad (8)$$

   without directly knowing k. This involves iterating through potential values of k and checking if kP = Q.

8. Complexity and Security

   The best-known algorithm to solve ECDLP is the **Pollard's Rho Algorithm**, with a time complexity of:

$$O\big(sqrt(n)\big) \quad (9)$$

   where n is the order of the elliptic curve group.

3. Description of RF communication model

Transmitting and receiving electric information over radio waves is what RF communication is all about. Devices that encode and process data are used in these systems. An RF channel sends data between an emitter and a listener. Because RF channels are open, people can listen in on data transfer and get in without permission. The model usually has a source, a listener, and a transmission means in between that lets the RF signals travel. Protecting data security, privacy, and identification are hard parts of making this kind of communication safe, especially when mobile devices and wireless networks are involved.

1. Signal Transmission Equation (Baseband Signal):

$$s(t) = A * \cos(2 * pi * f_c * t + phi) \quad (10)$$

   where A is the amplitude, f_c is the carrier frequency, phi is the phase, and t is time.

2. Modulation of Signal (Phase Modulation):

$$x(t) = A * \cos\big(2 * pi * f_c * t + phi(t)\big) \quad (11)$$

   where phi(t) is the time-varying phase modulating the carrier signal.

3. Channel Impulse Response:

$$h(t, tau) = integral\ from\ -\inf\ to\ \inf\ of\ alpha(tau) * e^{j*2*pi*f_c*t} d(tau) \quad (12)$$

where alpha(tau) represents the time-varying attenuation factor, and tau is the delay in the communication channel.

4. Received Signal (Convolution of Transmit Signal and Channel Impulse Response):

$$r(t) = integral\ from\ -\inf to \inf of\ s(t - tau) * h(tau)d(tau) \quad (13)$$

where r(t) is the received signal, and s(t - tau) is the transmitted signal delayed by tau.

5. Noise Model (Additive White Gaussian Noise):

$$n(t) \sim N(0, sigma^2) \quad (14)$$

Where, n(t) is the noise, modeled as a zero-mean Gaussian process with variance sigma^2.

6. Signal-to-Noise Ratio (SNR) Calculation:

$$SNR = \frac{E[|r(t)|^2]}{E[|n(t)|^2]} \quad (15)$$

Where, E represents the expected value, and r(t) is the received signal.

4. Proposed Advanced Elliptic Curve Encryption Scheme

The use of the velocity and protection of ECC, the proposed more suitable elliptic curve encryption technique is deduced to make RF communication structures safer. facts is encrypted before transmission in this scheme using ECC-based public-key encryption, in which each message is allocated to a vicinity on an elliptic curve. The encryption method makes use of small key numbers to maintain amazing protection. This approves for instant encryption and decoding except immoderate use of machine assets. The strategy additionally offers techniques to alternate keys and use virtual signatures to affirm the real and safe interaction. The technique enhances real-time performance by dynamically altering the elliptic curve parameters. This addresses issues with RF transmission include signal interference and varying bandwidth.

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

(Define elliptic curve over finite field F_p with valid parameters a, b)

$$Q = kP$$

(Public key Q computed by scalar multiplication of private key k with base point P)

$$C_1 = rP, \quad C_2 = M + rQ$$

(Encrypt message M as ciphertext pair (C_1, C_2) using random scalar r)

$$M = C^2 - kC^1$$

(Decrypt message by subtracting kC_1 from C_2 using private key k)

5. Simulation Results and Discussion

The suggested advanced elliptic curve encryption method makes RF transmissions much safer by offering strong encryption with little extra work for

computers. Performance tests show that it can securely send data quickly and easily, even in RF settings with limited resources.

Table 1

Performance Evaluation of Encryption Scheme

Parameter	ECC-based Scheme	Traditional RSA-based Scheme
Encryption Time (ms)	15.5	125.3
Decryption Time (ms)	12.3	140.1
Key Size (bits)	256	2048
Throughput (Mbps)	50.7	15.3

The comparison of the ECC-based and RSA-based encryption methods' success is shown in Table 1. It shows that they are very different in how well they work. Both the encryption and decoding times are faster with the ECC-based scheme than with the usual RSA-based scheme.

ECC has a much faster working speed than RSA, which takes 125.3 milliseconds for encryption and 140.1 milliseconds for decryption. Encryption takes only 15.5 milliseconds and decryption takes 12.3 milliseconds. Because it is so efficient, ECC works well in places with limited resources, like RF communication. Additionally, the ECC-based method only needs a key size of 256 bits, whereas RSA needs a key size of 2048 bits to provide the same level of security.

Table 2

Security Evaluation of Encryption Scheme

Parameter	ECC-based Scheme	Traditional RSA-based Scheme
Resistance to Eavesdropping	92	75
Resistance to Man-in-the-Middle Attacks	90	60
Computational Complexity	35	83
Key Exchange Efficiency	90	44

Table 2 compares the security of the ECC-based and RSA-based encryption methods, showing how they vary in how hard they are to break into, how long they take to run, and how well they work.

With scores of 92 and 90, respectively, the ECC-based method is more resistant to spying and man-in-the-middle attacks than RSA, which has scores of 75 and 60. This shows that ECC is more secure at keeping hackers and other bad people from getting to and changing data while it's being sent.

6. Conclusion

If you want to make RF interactions safer, this study shows how advanced elliptic curve encryption can help. It is very important to have strong encryption methods because RF systems are being used more and more to send private data. The suggested ECC-based method uses the Elliptic Curve Discrete Logarithm Problem's (ECDLP) computing hardness to solve important security issues, such as data breaches and unauthorized access. The plan makes sure that encryption and decoding work well with smaller key sizes, which is very important for radio frequency communication where bandwidth and computing power are limited. For better protection and speed, our findings show that the ECC-based method is much better than standard encryption methods. Also, changing the values of the elliptic curve on the fly makes the method more flexible for changing RF situations. This study shows that ECC could be used to make future RF communication systems safer and more flexible, especially in situations where high security is needed without affecting how well the system works.

References

[1] A. S. Reegan and V. Kabila, "Highly secured cluster based WSN using novel FCM and enhanced ECC-ElGamal encryption in IoT," *Wireless Personal Communications,* vol. 118, pp. 1313–1329 (2021).

[2] S. R. Moosavi and A. Izadifar, "End-to-end security scheme for E-health systems using DNA-based ECC," in Proc. Silicon Valley Cybersecurity Conf., Berlin, Germany: Springer (2022).

[3] H. D. Tiwari and J. H. Kim, "Novel method for DNA-based elliptic curve cryptography for IoT devices," *ETRI Journal,* vol. 40, pp. 396–409 (2018).

[4] S. Das and S. Namasudra, "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure," *Computers & Electrical Engineering*, vol. 101, pp. 107991 (2022).

[5] S. Gabsi, Y. Kortli, V. Beroulle, Y. Kieffer, and B. Hamdi, "Proposal of a lightweight differential power analysis countermeasure method on elliptic curves for low-cost devices," *Multimedia Tools and Applications* (2024).

[6] K. Kumagai, S. Kakei, Y. Shiraishi, and S. Saito, "Distributed public key certificate-issuing infrastructure for consortium certificate authority using distributed ledger technology," *Security and Communication Networks* (2023).

[7] S. Limkar, S. Singh, A. Wankhede, V. Wadne, V. Vinod, R. Phursule, and S. N. Ajani, "Modified elliptic curve cryptography for efficient data protection in wireless sensor network," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-A, pp. 305–316 (2024).

[8] R. Jadhav, S. Kapse, S. Mane, and N. Bhagwat, "Advancements in AI-enabled mock interview platforms: A review of Interviewello's web application," *ITSI Trans. Electr. Electron. Eng.*, vol. 13, no. 2, pp. 35–40 (2025).

[9] D. Rangwani, D. Sadhukhan, S. Ray, M. K. Khan, and M. Dasgupta, "An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network," *Trans. Emerg. Telecommun. Technol.*, vol. 32, pp. e4218 (2021).

[10] A. Vangala, A. K. Sutrala, A. K. Das, and M. Jo, "Smart contract-based blockchain-envisioned authentication scheme for smart farming," *IEEE Internet Things J.*, vol. 8, pp. 10792–10806 (2021).

[11] S. V. Akram, P. K. Malik, R. Singh, G. Anita, and S. Tanwar, "Adoption of blockchain technology in various realms: Opportunities and challenges," *Security and Privacy*, vol. 3, pp. e109 (2020).

[12] S. Varma, S. Prajapati, Y. Gupta, K. Tondon, S. Sharma, M. Parate, and M. Churi, "NFT marketplaces: A comprehensive analysis of trading, security, and metadata challenges," *Int. J. Adv. Electr. Comput. Eng.*, vol. 14, no. 1, pp. 55–68 (2025).

Received April, 2025