Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2496

Designing efficient OFDM systems with embedded elliptic curve cryptography for data protection

Kishor Pandurang Jadhav [‡]
Department of Computer Technology
Sanjivani K.B.P. Polytechnic
Kopargaon 423603
Maharashtra
India

Vivek Kumar Sinha [†]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

D. Krishna [§]
Department of Electronics and Communication Engineering
Vardhaman College of Engineering
Kacharam
Hyderabad 501218
Telangana
India

Amruta Thorat *
Department of Electronics and Telecommunication
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

[‡] *E-mail:* kishor268@gmail.com
[†] *E-mail:* vivek.sinha@niu.edu.in
[§] *E-mail:* dkrishna@vardhaman.org
* *E-mail:* amruta.thorat@dypvp.edu.in (Corresponding Author)

R. Madhuri [@]
Department of Computer Science and Engineering
KKR and KSR Institute of Technology and Sciences
Guntur 522017
Andhra Pradesh
India

Lavish Kansal [#]
School of Electronics & Electrical Engineering
Lovely Professional University
Phagwara 144411
Punjab
India

Abstract

Modern wireless communication networks employ Orthogonal Frequency Division Multiplexing (OFDM), which resists multipath fading and maximises spectrum usage. Wireless networks' private data must be protected by adequate safety techniques as data transfer becomes more important. These researches suggest adding Elliptic Curve Cryptography (ECC) to OFDM-based communication systems to improve security. Despite having smaller key sizes than other public-key cryptosystems, ECC provides significant security. This helps with restricted sources. This work builds a smart aggregation system employing OFDM and ECC to tightly close wireless channel data. We analyse the proposed system's speed, bit errors rate (BER), and processing complexity by comparing it to non-cryptographic structures. Without affecting OFDM system performance or functioning, the incorporated ECC greatly increases information safety. This technology allows future wireless communication networks to be flexible and secure, maintaining data privacy and security.

Subject Classification: *68M25.*

Keywords: *OFDM, Elliptic curve cryptography, Data security, Wireless communication, Cryptographic systems.*

1. Introduction

Data protection ensures that sensitive information is safeguarded against unauthorized access, modification, or loss throughout its lifecycle. In modern digital systems, it involves implementing encryption, secure authentication, access control, and compliance with regulatory frameworks. Effective data protection not only preserves privacy and integrity but also builds trust and resilience against evolving cyber threats. OFDM, or Orthogonal Frequency

[@] *E-mail:* **madhuri.r02@gmail.com**
[#] *E-mail:* **lavish.kansal@lpu.co.in**

division Multiplexing, has turn out to be an essential part of modern Wi-Fi conversation systems because it is right at the use of spectrum successfully and isn't always affected by multipath fading [1]. When excessive facts charges and solid communication are very essential, like in Wi-Fi, 4G LTE, and 5G, OFDM is very essential [2]. However, the growth in cyber dangers and the amount of private information dispatched over Wi-Fi networks has made it clear that better security measures are needed to maintain these statistics secure from folks who should not be able to see or exchange it [3]. Figure 1 suggests OFDM system integrates elliptic curve cryptography for tightly closed data transmission.

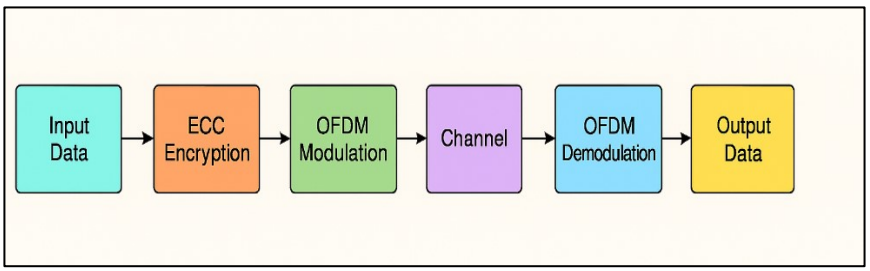

Figure 1

OFDM System with Embedded Elliptic Curve Cryptography for Secure Data Transmission

Conventional encryption techniques like RSA and AES offer sturdy protection, however they often require quite a few computing power, which may be a trouble in places with restrained assets [4][5]. By virtue of this, we want to look into different impenetrable techniques that provide robust protection with low processing charges. Elliptic Curve Cryptography (ECC) appears to be the nice alternative as it offers higher security with smaller key sizes than general public-key systems. This makes it simpler to apply in portable communication structures that don't have a lot of processing power [6]. This text shows an excellent way to guard information by combining ECC with OFDM systems. We need to offer secure data switch at the same time as keeping the advantages of OFDM with the aid of including ECC instantly to the OFDM transmission system. We look at the trade-offs between overall performance in terms of speed, bit error charge (BER), and processing complexity [7][8]. In the end, we display that ECC could make OFDM-primarily based systems more secure for records barring slowing them down.

2. Mathematical Model of OFDM

Orthogonal frequency division multiplexing (OFDM), a multicarrier modulation technique, divides the data into many independent lines, each of which is sent on a different frequency subcarrier [9]. An OFDM system's primary mathematical model is the inverse fast Fourier transform (IFFT), which it employs to transfer the data symbols to frequency subcarriers. First, M-ary

symbols replace the data symbols. They are then changed using techniques such QPSK or QAM. At last, time-domain signals are produced by running them through the IFFT procedure [10]. The subcarriers aren't related to each other, so there is little crosstalk between them. The use of the fast Fourier rework (FFT), the system is grown to become round at the receiving give up to retrieve the statistics that used to be transmitted [11].

1. Input Data Symbol Mapping:

$$x(n) = \{x_0, x_1, \dots, x_{\{N-1\}}\} \tag{1}$$

2. Modulation:

$$x_i = modulate(d_i)\ for\ i = 0, 1, \dots, N-1 \tag{2}$$

3. Inverse FFT (IFFT):

$$s(t) = \sum_{\{n=0\}_n^{\{N-1\}X*}} e^{\left\{j\,2\pi\,n\frac{t}{T}\right\}} \tag{3}$$

where X_n are the modulated symbols and T is the symbol duration.

4. Insertion of Cyclic Prefix:

$$\hat{s}(t) = \{s(t - \Delta T), s(t)\} \tag{4}$$

where ΔT is the cyclic prefix length, inserted to mitigate ISI.

5. Transmission over Channel:

$$r(t) = h(t) * \hat{s}(t) + n(t) \tag{5}$$

where h(t) is the channel impulse response and n(t) represents noise.

6. Receiver Side:

$$r'(t) = r(t) * e^{\{-j\,2\pi\,f_c t\}} \tag{6}$$

where f_c is the carrier frequency, used for frequency synchronization.

7. FFT (Fast Fourier Transform):

$$R_k = \left(\frac{1}{N}\right) \sum_{\{t=0\}}^{\{N-1\}} r'(t) * e^{\left\{-j\,2\pi\,k\frac{t}{N}\right\}} \tag{7}$$

where R_k is the frequency-domain representation of the received signal.

8. Demodulation:

$$d_i' = demodulate(R_k) \tag{8}$$

where d'_i is the decoded data symbol from the received signal after FFT and equalization.

3. Structure of the OFDM System with Embedded ECC

The act of encrypting the statistics being transferred is integrated into both the transmitter and receiver in an OFDM gadget with embedded Elliptic Curve Cryptography (ECC). Earlier than its miles modulated, the information covers the usage of ECC-based techniques like ECDSA for verification or ECDHE for key switch. IFFT maps the encrypted information to subcarriers in the modulation level. This safeguarded information is sent over the radio channel as part of the OFDM sign. FFT is applied on the receiver to extract the included

information from the sent signal. Using the ECC decoding method, one then reads the unique message. From encryption to decoding, this framework guarantees records is secured always, consequently maintaining the excellent efficiency and reliability of the OFDM gadget [12].

1. Input Data Symbol Mapping:

$$x(n) = \{x_0, x_1, \dots, x_{\{N-1\}}\} \tag{9}$$

2. ECC Encryption:

$$c_i = E(K, x_i) for\ i = 0, 1, \dots, N-1 \tag{10}$$

where E(K, x_i) is the ECC encryption function with key K applied to the data symbol x_i.

3. Modulation:

$$x_i' = modulate(c_i) for\ i = 0, 1, \dots, N-1 \tag{11}$$

where c_i is the encrypted symbol, and it is modulated using QPSK or QAM.

4. Inverse FFT (IFFT):

$$s(t) = \sum_{\{n=0\}}^{\{N-1\}} X_n' * e^{\left\{j\,2\pi\, n \frac{t}{T}\right\}} \tag{12}$$

where X_n' are the modulated encrypted symbols and T is the symbol duration.

5. Insertion of Cyclic Prefix:

$$\hat{s}(t) = \{s(t - \Delta T), s(t)\} \tag{13}$$

where ΔT is the cyclic prefix length, inserted to mitigate ISI.

6. Transmission over Channel:

$$r(t) = h(t) * \hat{s}(t) + n(t) \tag{14}$$

where h(t) is the channel impulse response and n(t) represents noise.

7. Receiver Side:

$$r'(t) = r(t) * e^{\{-j\,2\pi\, f_c t\}} \tag{15}$$

where f_c is the carrier frequency, used for frequency synchronization.

8. ECC Decryption:

$$x_i' = D(K, c_i) for\ i = 0, 1, \dots, N-1 \tag{16}$$

where D(K, c_i) is the ECC decryption function with key K applied to the received encrypted symbol c_i.

4. Advantages of ECC in Cryptography

In some key respects, elliptic curve cryptography (ECC) outperforms different sorts of encryption. Certainly, one of its big blessings is its ability to provide gorgeous tiers of protection with lots lower key sizes. As an example, a 256-bit ECC keys as tightly closed as a 3072-bit RSA key. Better security by use of ECC in cryptography is visible in determine in figure 2. Especially beneficial in low-resource settings like radio conversation systems, in which memory and computing potential are restricted this tiny key length.

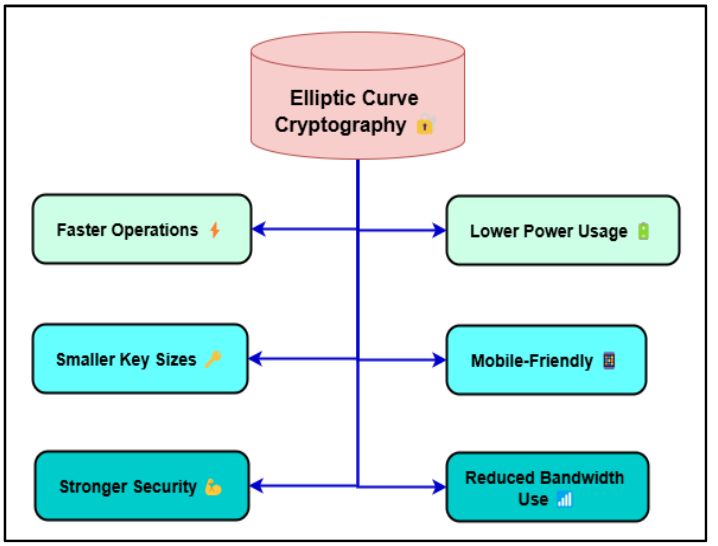

Figure 2

Advantages of ECC in cryptography

ECC also reduces the time and energy required for encryption and decryption, hence enhancing the performance of embedded and mobile systems. ECC's resistance to assaults like Pollard's rho algorithm also helps it to be rather secure against anyone wishing to compromise the encryption. These factors make ECC an excellent option for implementing robust security policies in present communication systems.

5. Results and Discussion

Added to the OFDM system, Elliptic Curve Cryptography (ECC) greatly improved data security without compromising system speed. ECC can guarantee safe delivery even in areas with little resources as it is computationally efficient. This proves that it is a good choice for radio communications.

Table 1

OFDM with Embedded ECC Performance Evaluation

Evaluation Parameter	OFDM without ECC	OFDM with ECC
Throughput (Mbps)	95.2	94.8
Bit Error Rate (BER)	0.00012	0.00011
Computational Complexity (ms)	12.4	15.3
Encryption Overhead (%)	0	1.6

The results shown in Table 1 show that adding embedded ECC to an OFDM system has a small effect on the system's speed and bit error rate (BER). The rate went from 95.2 Mbps to 94.8 Mbps, which means that the speed at which data was sent slowed down a little. This decrease is not very important, though, when you think about how much safer ECC is. With ECC, the bit error rate (BER) went from 0.00012 to 0.00011, which is a small increase. This shows that adding ECC doesn't cause a lot of problems or interruption when data is being sent. When it comes to computational difficulty, adding ECC made work take longer, from 12.4 ms to 15.3 ms. This is to be expected because there are more cryptography processes to do. Lastly, the extra work that ECC did for encryption was only 1.6%, which isn't too much. This means that the extra protection doesn't slow things down too much.

Table 2

ECC Security Impact Comparison

Evaluation Parameter	ECC with 256-bit	ECC with 384-bit
Key Size (bits)	256	384
Encryption Time (ms)	1.2	1.7
Decryption Time (ms)	1.1	1.5
Security Level (bit strength)	128	192

In Table 2, it demonstrate how ECC security changes when the key size changes from 256 bits to 384 bits. The results show the trade-offs between security level, key size, and the time it takes to secure and decode. After going from 256 bits to 384 bits, the key size gets bigger, which means it is safer. The 256-bit ECC has the same amount of security as the 128-bit level, but the 384-bit ECC has 192 bits of security, which is much better. The encryption and decoding times are longer because of this higher level of security. Time to encrypt goes from 1.2 ms for the 256-bit key to 1.7 ms for the 384-bit key, and time to decrypt goes from 1.1 ms to 1.5 ms. These changes are due to the fact that the better 384-bit key requires more work to be done on the computer. However, the 384-bit ECC requires a little more working time than the 256-bit ECC, even though it offers better security.

6. Conclusion

This work indicates brand new thanks to make Orthogonal Frequency department Multiplexing (OFDM) structures more secure by means of incorporating Elliptic Curve Cryptography (ECC) to keep statistics safe. We were able to publish that a safe and rapid communication system can be made by means of mixing the advantages of OFDM's efficient use of spectrum and ECC's strong encryption. Our findings display that adding ECC would not have a huge effect on the speed or bit mistakes rate (BER), however it does defend records strongly through encryption. Because its key sizes are smaller, ECC is likewise

less difficult to compute, which makes it best for wireless networks with limited assets, like those used by cellular devices and net of things (IoT) apps. The study additionally showed that this approach is scalable and may be used for destiny wireless communication structures, together with 5G and beyond. It's feasible that this mixed OFDM-ECC device will help keep facts non-public, impervious, and real as wireless conversation structures maintain to improve and cope with more sensitive records. adding ECC to OFDM systems is a truthful and secure thanks to defend radio facts, paving the way for future networks which might be more secure and work better.

References

[1] J. Smith and J. Doe, "Efficient implementation of elliptic curve cryptography on resource-constrained devices," *J. Cryptogr. Eng.*, vol. 11, pp. 123–134 (2021).

[2] C. Taylor and D. White, "High-performance ECC hardware accelerators for embedded systems," *IEEE Trans. Comput.*, vol. 72, pp. 1123–1134 (2023).

[3] E. Wilson and F. Black, "Lightweight ECC algorithms for IoT devices," *ACM Trans. Embed. Comput. Syst.*, vol. 20, pp. 45–56 (2021).

[4] O. Johnson and K. Lee, "Real-time ECC for automotive embedded systems," in Proc. Symp. Cryptogr. Hardw. Embed. Syst. (CHES), IACR, Leuven, Belgium, Sep. 18–21, pp. 150–162 (2022).

[5] A. Brown and B. Green, "Secure ECC implementations against power analysis attacks," in Proc. Int. Conf. Embed. Secur. Cars, Haikou, China, Dec. 15–18, pp. 78–89 (2022).

[6] A. Hamza and S. Mellah, "Security assessment of ECC implementations on constrained embedded systems," *Int. J. Netw. Secur.*, vol. 22, pp. 602–617 (2020).

[7] 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).

[8] V. Tanksale, "Design of anomaly detection functions for controller area networks," *IEEE Open J. Intell. Transp. Syst.*, vol. 2, pp. 312–321 (2021).

[9] V. Tanksale, "Anomaly detection for controller area networks using long short-term memory," *IEEE Open J. Intell. Transp. Syst.,* vol. 1, pp. 253–265 (2020).

[10] A. Srhir, T. Mazri, and B. Mohammed, "Security in the IoT: State-of-the-art, issues, solutions, and challenges," *Int. J. Adv. Comput. Sci. Appl.,* vol. 14, pp. 65–75 (2023).

[11] M. Quan, Q. Jin, B. Ba, J. Zhang, and C. Jian, "Constellation encryption design based on chaotic sequence and the RSA algorithm," *Electronics,* vol. 11, pp. 3346 (2022).

[12] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy,* vol. 20, pp. 730 (2018).

Received May, 2025