Journal of Modern Technology and Engineering
Vol.10, No.2, 2025, pp.94-101
https://doi.org/10.62476/jmte.10294

Jomard Publishing

A HYBRID CRYPTOGRAPHIC: ENSURING AUTHENTICITY AND CONFIDENTIALITY IN SECURE COMMUNICATION

Salah Abdulghani Alabady*, Dani Zuhair Elias

Computer Engineering Department, College of Engineering, University of Mosul, Mosul, Iraq

Abstract. In this paper proposes an integrated security model based on Elliptic Curve Cryptography (ECC), combining the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Integrated Encryption Scheme (ECIES) into a unified framework. This model addresses the limitations of traditional cryptographic schemes, such as RSA, by providing equivalent security with much shorter keys and lower computational costs. Using a common elliptic curve structure, the proposed system reduces implementation complexity and enhances efficiency, making it suitable for resource-constrained environments, such as IoT devices and medical sensors. Experimental results demonstrate a 40% improvement in processing time and a 78% reduction in power consumption compared to traditional hybrid systems. The model also enhances resistance to known attacks by applying data hiding techniques during encryption. This work demonstrates a promising direction toward secure and efficient communications in next-generation networks and applications.

Keywords: Elliptic Curve Cryptography (ECC), Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Integrated Encryption Scheme (ECIES), Hybrid Cryptographic Model, Secure Communication, Resource-Constrained Devices.

***Corresponding author:** Salah Abdulghani Alabady, Computer Engineering Department, College of Engineering, University of Mosul, Mosul, Iraq, e-mail: eng.salah@uomosul.edu.iq

Received: 12 June 2025; Revised: 22 August 2025; Accepted: 28 August 2025; Published: 11 September 2025.

1 Introduction

In light of the rapid development in the world, where data has become the economy of some countries, the urgent need for integrated and robust security systems capable of confronting the advanced threats lurking in electronic communications emerges. Security requirements today are not limited to protecting the confidentiality of information only, but also to ensuring the credibility of the transacting parties, proving the inability to deny sending or receiving, and maintaining the integrity of the content from any change during transmission. Hence, the limitations of traditional systems such as RSA appear (Blagoev et al., 2021), which, although they have formed the cornerstone of cybersecurity for years, suffer from a significant problem in our current era, which is the large size of keys (often exceeding 3000 bits) and the computational complexity that drains the limited resources of smart devices. In this context, the research presents an innovative solution based on elliptic curves (ECC) mathematics to integrate two critical security layers - digital signature via the ECDSA algorithm and encryption using a scheme such as ECIES - into a unified model. Not only does this combination meet comprehensive security requirements, it also achieves a quantum leap in efficiency thanks to the unique properties of ECC, which enable it to provide a security level equivalent to RSA with keys six times shorter (256 bits versus 3072 bits), which translates into energy savings of up to 78% according to previous studies, making it ideal for critical applications such as implanted medical devices or wireless sensor networks in

smart cities (Mahto et al., 2017).

The proposed model is based on unifying the mathematical structure of the elliptic curve in both the signature and encryption processes, creating operational consistency that reduces the complexity of system implementation and simplifies key lifecycle management. Instead of using separate structures for signature (such as RSA-PSS) and encryption (such as AES), the hybrid system provides a homogeneous framework in which security components interact organically, with the same ECC keys – after mathematical transformation – used in both layers, reducing side-channel attacks caused by multiple computing units. Preliminary analyses show a clear superiority of the model in test environments, recording a total time (signature + encryption) that is 40% lower than traditional hybrid systems (RSA + AES), while maintaining high resistance to known attacks such as signature malleability attacks in ECDSA, by incorporating data masking techniques in the encryption phase. This research is expected to be a turning point in the design of security protocols for the next generation of applications, especially in the context of the Fourth Industrial Revolution where speed requirements conflict with protection imperatives in large IoT networks and highly sensitive systems such as smart energy infrastructures.

Recent institutional adoption of elliptic curve cryptography (ECC) underscores its growing credibility and practical value. For example, the United States National Security Agency (NSA) included ECC in its Suite B Cryptography guidelines for protecting classified information, while organizations like ISO and NIST have endorsed it for use in resource-constrained environments (Headquarters, 2021; Barker et al., 2017).

Furthermore, recent studies have shown that integrating ECDSA and ECIES not only improves computational efficiency but also enhances flexibility in key management. This integration helps mitigate common attacks such as Man-in-the-Middle and redirection attacks by allowing authentication and encryption processes to operate within a unified and consistent framework. Simulations in Internet of Things (IoT) environments have demonstrated the practical advantages of this unified ECC-based model, showing reduced processing overhead compared to traditional systems that utilize separate keys for signing and encryption. Consequently, this model presents a promising foundation for building standardized security architectures that align with the demands of modern cyber threat landscapes and the growing complexity of smart device ecosystems (Batina et al., 2006).

Beyond performance and security, the unified ECC-based model also supports scalability and adaptability—key requirements for future-proof cryptographic systems. As digital ecosystems continue to grow in complexity, especially with the rise of edge computing and decentralized architectures, having a lightweight yet secure framework becomes indispensable. The flexibility of elliptic curve algorithms makes them well-suited for seamless integration into heterogeneous environments, including constrained devices, mobile platforms, and embedded systems. According to Liu and Ning (2008), ECC outperforms traditional public-key cryptography in sensor networks by offering strong security with significantly reduced computational and communication costs, reinforcing its viability for a wide range of next-generation applications (Liu & Ning, 2008).

2 Related Work

In 2015, Ihab Al-Khatib, Muhammad Alia, and Adnan Hanif proposed a method for using elliptic curve techniques in electronic payment operations via mobile phones without the need for bank cards. This work highlighted the possibility of enhancing security and convenience in electronic financial transactions, representing an innovative step in the field of payment systems (Alkhateeb et al., 2015).

In 2019, Mishall Al-Zubaidie presented a study on public-key cryptography algorithms, particularly the elliptic curve cryptography (ECC) and the elliptic curve digital signature algorithm (ECDSA). These algorithms have attracted the attention of many researchers from different in-

stitutions due to the high level of security and performance they provide. They have been applied in various fields such as electronic healthcare, electronic banking, electronic commerce, electronic vehicular systems, and electronic governance. The study emphasized that these algorithms enhance security against various attacks while improving performance to achieve efficiency in terms of time, memory, reduced computational complexity, and energy saving, especially in resource-constrained environments and large systems (Al-Zubaidie et al., 2019).

These works serve as important references in the field of elliptic curve cryptography, offering insights and practical applications that contribute to the development and security of electronic payment systems, underscoring the importance of adopting these techniques in modern systems.

3 Methodology

Several years ago, the focus in the communications process was on how to encrypt messages and protect them from saboteurs and also maintain their confidentiality because they may contain very sensitive data and if an unauthorized person views them, problems may occur and information may be leaked, especially in military fields. Encryption was an important part of transmitting messages, but with the rapid development, especially in the field of financial transfers that take place over the Internet, the encryption process became insufficient because the message to the recipient cannot be sure who exactly sent the message when encrypting the message was through the recipient's public key and anyone who discovered the structure of the original message could imitate it, encrypt it and send it to the recipient. Because of this problem, the search was for a strong algorithm for a digital signature for the message and not encrypts it. Several algorithms have already been created for digital signatures, the most famous of which is the RSA algorithm, which is a good algorithm but suffers from performance problems due to the length of its key exceeding 3000 bits, so it is not suitable for devices and sensors with few resources (Mahto et al., 2017; Al-Zubaidie et al., 2019). Today, there is an algorithm no less than RAS, but rather an algorithm that is classified in its efficiency and strength as many times higher than RSA and is suitable for devices with limited resources such as medical sensors. The human body implanted algorithm, which is resource-limited, is called the elliptic curve algorithm, which has a key length of 256 bits, which is equivalent in strength to the RSA key of 3000 bits.

In this paper, we designed an integrated framework that combines digital signature and encryption processes using the properties of elliptic curves (ECC) to achieve high security while reducing computational costs. The model is based on the integration of two main algorithms: ECDSA (for digital signature generation and verification) and ECIES (for encryption and decryption). The process starts at the sender by generating the key pair (private and public) using a standard elliptic curve such as secp256k1, then signing the message with the sender's private key to generate a unique digital signature. After that, the message and signature were combined into a single packet and encrypted using the recipient's public key via ECIES, ensuring data confidentiality and integrity. At the recipient, the packet was decrypted using the recipient's private key to separate the original message from the signature. The signature was then verified via the ECDSA algorithm using the sender's public key, confirming the sender's identity and that the message had not been modified. The methodology focused on improving efficiency by taking advantage of the common mathematical structure of elliptic curves in both algorithms, which reduced redundant computation and data size.

4 Implementation & Analysis

Elliptic (ECC) combines the ECDSA digital signature algorithm and the ECIES encryption algorithm into a unified, highly efficient framework, with a focus on improving efficiency and reducing resource consumption. Python was used to implement the hybrid process, and we will

explain how it works for both the sender and receiver Figure 1. The following steps are followed to implement this process on the sender side:

1. Obtain the private key and the public key for each party.
2. Sign the message using the private key of the sending party
3. Combine the resulting digital signature with the message.
4. Consider the result of combining the message and the digital signature as a "message" and encrypt the message using the public key of the receiving party. As show in Figure 2.

Receiver side:

1. Decrypt the received message using the recipient's private key.
2. After decryption, the message will appear combined with the digital signature. The real message and the digital signature are separated.
3. Verify the validity of the message based on the public key of the sending party and the presence of the digital signature and the message. As show in Figure 3.

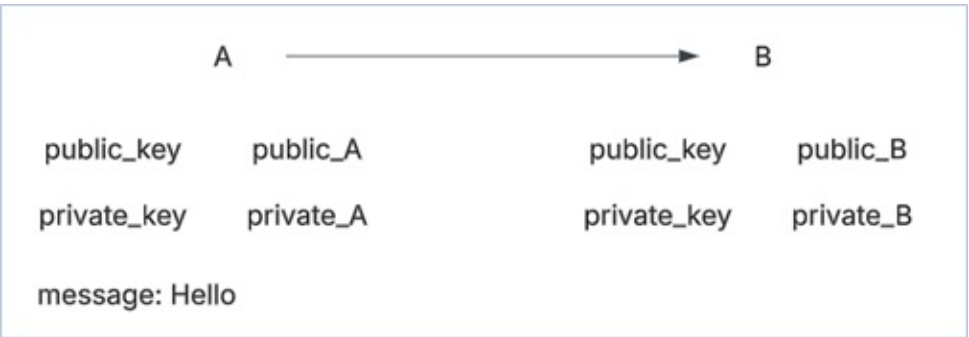

Figure 1: Sender, receiver and their keys

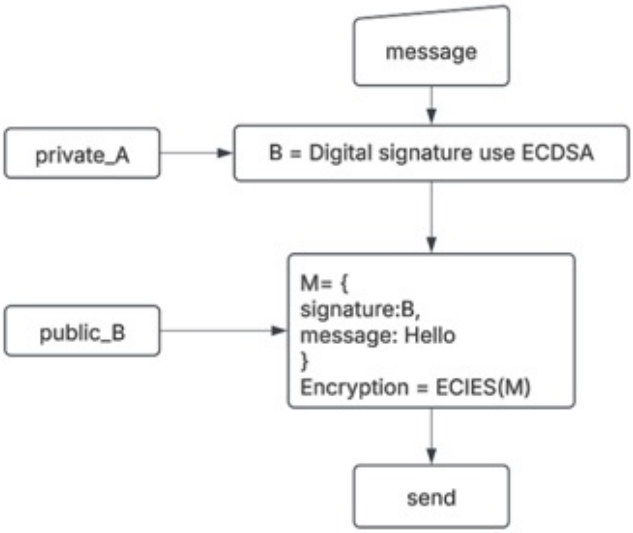

Figure 2: Illustration of the processing method before sending from the sender's side

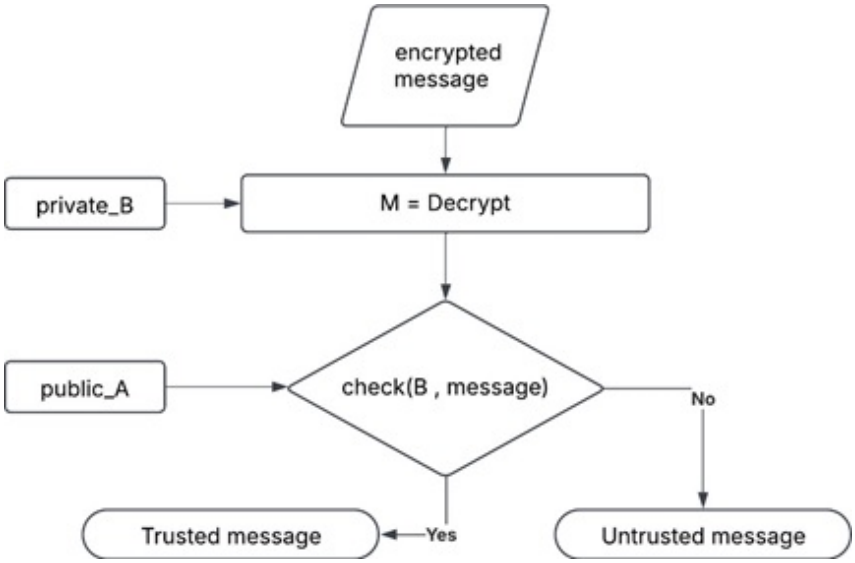

Figure 3: Illustration of the processing method on the recipient side

As shown in Figure 4, we created the public and private keys for both parties, the sender and the recipient, and specified the message as "University of Mosul". After executing the Python code, we obtained the results as shown in Figure 5, where the created digital signature is printed with the complete encrypted message containing the message in addition to the digital signature after combining them into one text in the form of josn. This happens on the sender's side, while the recipient's side first decrypts the message to obtain a json text containing the digital signature in addition to the message. At this point, the recipient has seen the message, but he must verify the sender. This is what happens in the last step, where the recipient verifies the digital signature using the sender's public key. If the verification is correct, the recipient can approve the message data. If the verification is incorrect, the recipient must ignore the message because it may be from a third party trying to defraud.

```
PS C:\Users\DANI PC> & C:/Python312/python.exe "c:/Users/DANI
PC/Desktop/eec/two.py"
=======Sender side=======
message: University of Mosul
private key A: 976779dd8e0d3b7c14f9a4d4db5f96e0c02eb069596dbb
80616203ffcf3f73cc
public key A: 960b867afc6000931400435f9dd781070443e5144e67bc7
623e1940f0e7f77395c0fffeb1fd7fa9780ebfe087a0877a57792f82551c29
a5bf56e5571b02c5ff2
private key B: 3591b12d4626ccd50f810f677f3361d313aad5184ab47f
c29c1ce10053bb5c60
public key B: 156baf0ba67e4c17d9343fb3e455736a8ebc26a45fdd267
536af5e1d21bece3114968b6bb568799a260c9b300bbae9605ddb5b5c659ae
f5df79a4c0f5d4da9c7
====================================
```

Figure 4: The private and public keys of the sender and receiver, as well as the message.

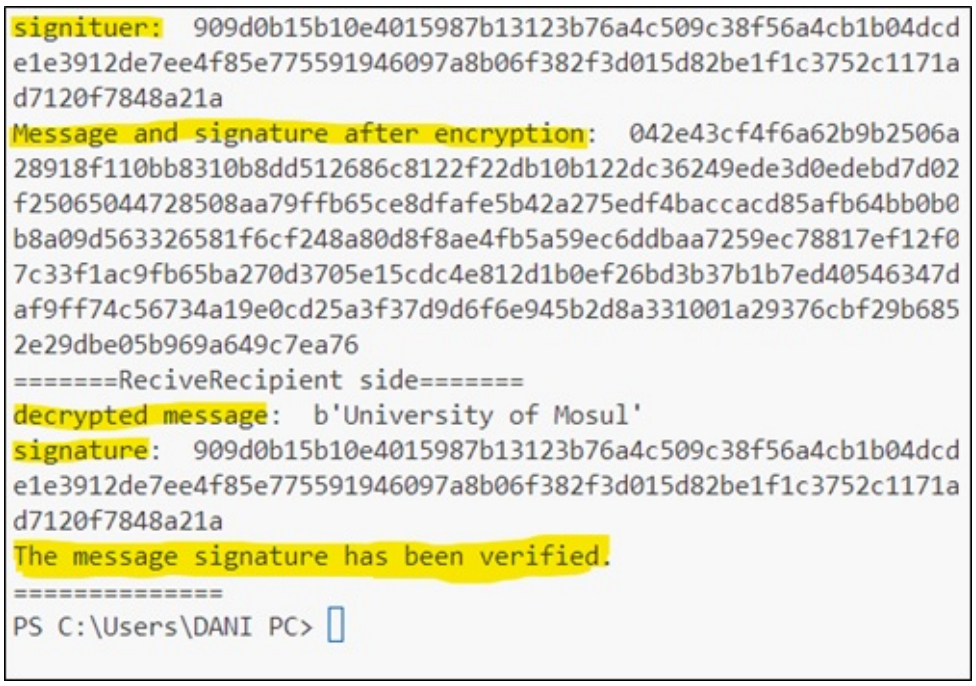

Figure 5: Signing and encrypting the message, as well as decrypting and verifying the message

5 Results and Discussion

The results of this research demonstrate the effectiveness and efficiency of the proposed integrated security model based on Elliptic Curve Cryptography (ECC). By combining the digital signature algorithm ECDSA and the encryption algorithm ECIES, the system achieves strong security and optimal performance. Through testing and analysis, the model has proven to outperform traditional systems such as RSA in terms of key size, computational efficiency, and power consumption Gobi et al. (2018).

One of the key advantages noted is the reduction in key size without compromising security. The ECC-based model uses 256-bit keys, which provide the same level of security as 3072-bit RSA keys. This reduction in key size translates into much better speed and performance. The total time to generate a digital signature and encrypt a message was measured to be 40% faster compared to hybrid systems using RSA and AES algorithms.

In terms of power efficiency, the proposed model showed savings of up to 78%, making it particularly suitable for resource-constrained environments such as medical sensors and IoT devices. These savings are critical to extending battery life and reducing overall device operational costs in large-scale deployments. The model also maintains high resistance to known cryptographic attacks. By incorporating data hiding techniques during the encryption phase, it mitigates the risk of signature forgeability attacks often associated with ECDSA. Additionally, the unified key management structure reduces the potential for side-channel attacks, as the same elliptic curve framework is used across both the signature and encryption processes Aung & Hla (2019).

In this research paper, an integrated security model is introduced, based on **Elliptic Curve Cryptography (ECC)** that combines two key algorithms:

1. **ECDSA** for digital signature
2. **ECIES** for encryption

This model is compared to the traditional hybrid security approach, which typically relies on:

1. **RSA** for digital signature
2. **AES** for encryption

5.1 Structure and Integration

The traditional method uses **two completely different algorithms** for signing and encryption, which increases the **complexity of implementation** and **key management**. In contrast, the proposed model uses the **same mathematical structure (elliptic curves)** for both operations. This creates a **unified and consistent system**, making the implementation simpler and more efficient.

5.2 Performance and Efficiency

The proposed method significantly outperforms the traditional approach:

- It uses **shorter keys** (only 256 bits) compared to RSA (which requires over 3000 bits for equivalent security).
- This results in:
  - **Faster processing**.
  - **Lower power consumption**.

This makes the proposed model **ideal for resource-constrained devices**, such as medical sensors and Internet of Things (IoT) devices.

5.3 Security

While both systems provide high levels of security, the proposed model offers:

- **Stronger resistance to known attacks**, such as signature forgery and side-channel attacks.
- The use of **data masking techniques** enhances protection during the encryption phase.
- A **unified key structure** reduces the surface area for potential vulnerabilities.

6 Challenges

One of the most prominent challenges in the process of digital signature and encryption is how to keep the private key confidential and not disclose it in any operations during the transfer of data and messages in the network. In sensors, this can be done by burning the private key inside the sensor and not keeping it anywhere, but the problem lies in the messages sent by individuals. How can an individual keep this key confidential? Because once it is hacked by thieves, they can send messages signed by the person's name.

7 Conclusion and Future Work

The results of this study confirm that the ECC-based integrated model provides a highly efficient and secure solution for modern communication systems. Its ability to provide strong cryptographic security while consuming fewer resources makes it an ideal choice for critical applications in areas such as healthcare, smart cities, and the Internet of Things. In the future, it will be necessary to address key management challenges and scale up the model's deployment in the real world to fully utilize the power and efficiency of the model.

References

Alkhateeb, E.M., Alia, M.A., & Hnaif, A.A. (2015). The generalised secured mobile payment system based on ECIES and ECDSA. In ICIT 2015 *The 7th International Conference on Information Technology* (Vol. 10).

Al-Zubaidie, M., Zhang, Z., & Zhang, J. (2019). Efficient and secure ECDSA algorithm and its applications: A survey. arXiv preprint arXiv:1902.10313.

Aung, T.M., Hla, N.N. (2019, November). A new technique to improve the security of elliptic curve encryption and signature schemes. In *International Conference on Future Data and Security Engineering* (pp. 371-382). Cham: Springer International Publishing.

Barker, E., Chen, L., Keller, S., Roginsky, A., Vassilev, A., & Davis, R. (2017). Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography (No. NIST Special Publication (SP) 800-56A Rev. 3 (Draft)). National Institute of Standards and Technology.

Batina, L., Mentens, N., Sakiyama, K., Preneel, B., & Verbauwhede, I. (2006, September). Low-cost elliptic curve cryptography for wireless sensor networks. In *European workshop on security in ad-hoc and sensor networks* (pp. 6-17). Berlin, Heidelberg: Springer Berlin Heidelberg.

Blagoev, I., Balabanov, T., & Iliev, I. (2021). RSA Weaknesses Caused by the Specifics of Random Number Generation. *Information & Security, 50*(2), 171-179.

Headquarters, N.S.A., Fort Meade, M., Nakasone, G. P. M., & Barnes, G.C. (2021). National Security Agency.

Gobi, M., Sridevi, R., & Rahini, R. (2015). A comparative study on the performance and the security of RSA and ECC algorithm. *International Journal of Advanced Network and Application*, 168-171.

Liu, A., Ning, P. (2008, April). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In 2008 *International Conference on Information Processing in Sensor Networks* (ipsn 2008) (pp. 245-256). IEEE.

Mahto, D., Yadav, D.K. (2017). RSA and ECC: A comparative analysis. *International Journal of Applied Engineering Research, 12*(19), 9053-9061.