International Journal of Mathematics and
Computer Science, **19**(2024), no. 1, 229–235

A New Approach for Enhancing AES-Based Data Encryption Using ECC

Fairouz Sherali

Department of Computer Science
Faculty of Education for Girls
Kufa University
Najaf, Iraq

email: fairoozm.jaafar@uokufa.edu.iq

(Received July 10, 2023, Accepted August 28, 2023,
Published August 31, 2023)

Abstract

Due to the wide variety of distant information transmission, data encryption has become an absolute necessity for practically all data transaction applications. Sensitive data gets uploaded to the cloud every day through many methods. AES algorithm is now the best option for many applications that require security services. Because of this, a lot of research has been carried out to improve the performance and efficiency of the algorithm. This paper's main goal is to propose an improved method for encrypting and decrypting data. As key sharing was a significant problem in the symmetric approach, we generate the key using the ECC and will encrypt and decrypt data using the AES using this key. The suggested algorithm, which is simpler than ECC and solely utilized for key generation-not data encryption or decryption-is more secure than AES because it circumvents the key-sharing issue that plagued AES.

Key words: Encryption, decryption, ECC, AES, cloud computing.
AMS (MOS) Subject Classifications: 68M25, 94A60.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

1 Introduction

The most well-known method of protecting highly sensitive information is data encryption [1], which makes use of an existing or prewritten conventional algorithms [2],[3]. Key generation, which includes two components-symmetric key generation and asymmetric key generation, is the most potent aspect of the encryption technique. The asymmetric encryption algorithms' key distribution and management are simple while the symmetric encryption algorithms provide good security, but key distribution and maintenance are difficult. With the use of current, highly sophisticated computing devices, hackers may now simply break the key [4]. Strongly encrypted data that cannot be decrypted using cryptanalysis is now needed.

Problem Statement:
AES utilizes a single secret key for encryption and decryption processes. The single key can make it less secure. In contrast, ECC employs asymmetric key encryption, which requires two keys: secret and public keys. In light of this, this type has a higher level of protection, which makes it challenging for intruders to decrypt two keys at once. ECC can offer the same level of security and a small key size compared to other encryption algorithms. In this paper, we study the problem of key management and use a hybrid of two techniques, ECC and AES encryption techniques, to solve this problem.

2 Preliminaries

2.1 ECC

In 1985, the authors in [5] found out the Elliptic Curve Cryptography (ECC). ECC's fundamental benefit is increasing security with a smaller key length size, whereas a 160-bit ECC provides the same degree of security as a 1024-bit RSA. In comparison to other methods, the calculation is quick, and less storage space is required. ECC [6] is based on the algebraic form of elliptic curves across a finite field. The following general equation defines an ECC across a prime field.

$$y^2 = x^3 + \alpha x + \beta, \tag{2.1}$$

where α and β are the coefficients of ECC.
The essential process in ECC is scalar multiplication. This process depends on two operations: Point doubling and Point addition.

Encryption and Decryption process:
The sender encrypts the message M and sends it to the receiver, this message must be presented on the elliptic curve as points [7, 8]. M is converted into the ciphered message $C_1 = d * P$ and $C_2 = M + d * Q$, where d is a random number from the range $[1 - (n - 1)]$. The sender sends C_1 and C_2 together to the recipient.

In the Decryption Process, the public key that was generated is utilized for decryption. The actual message M will be recovered by decryption from the cipher text C_1 and C_2, $M = C_2 - d * C_1$.

2.2 AES

AES cryptography stands for Advanced Encryption Standard. It is a symmetric block cipher utilized by the United States to encrypt sensitive information [9]. This type involves three block ciphers: 256, 192, and 128-bit secret keys for encryption and is more robust than the DES, which uses 56-bit keys.

Encryption and Decryption Process:
The AES algorithm creates ciphertext using a substitution-permutation network, with many rounds. The key size determines the number of rounds. For instance, AES does 10 rounds for 128-bit secret keys, 14 rounds for 256-bit secret keys, and 12 rounds for 192-bit secret keys. Every round in each case is the same, except the last round, which does not contain the step of the mix column. Before beginning any round-based encryption operations, the input state is XORed with the first four bytes of the key schedule. The four encryption steps used in each round are [10]: Bytes Transform, Shiftrows, Mixed Column, Addroundkeys. The AES decryption operation is the opposite of the encryption process where the four transformations are performed in the opposite order.

3 Proposed Method

In this paper, we present a new cipher method to secure the cipher key used in the AES algorithm. We apply a combination of asymmetric encryption ECC and symmetric AES. In the proposed encryption algorithms 1 and 2 below, we use the ECC algorithm to select eight points as a cipher key for the AES algorithm and store them in a square matrix as shown in figure 1. This cipher key is shared between two partners and encrypted using the ECC method's parameter. Then the algorithm uses the AES algorithm to encrypt

the plaintext by the mentioned encrypted key and produces the ciphertext. In the decryption process, we simply reverse the encryption process to get the plain text.

Cipher key			
x_1	y_1	x_2	y_2
x_3	y_3	x_4	y_4
x_5	y_5	x_6	y_6
x_7	y_7	x_8	y_8

Figure 1: Convert the points in ECC to square matrix

Algorithm1 : Key generator
Input :curve parameters α and β, generator point Z, the modulus r, order of the curve m, and the cofactor c.
Output :round key
- Apply the ECC algorithm
1- Generate points on an elliptic curve that satisfy specific equation (2.1)
2- Select eight points on the elliptic curve as round keys for the AES algorithm as shown in figure 1, where
$k_1 : w_0 = (x_1, y_1), (x_2, y_2)$
$k_1 : w_1 = (x_3, y_3), (x_4, y_4)$
$k_1 : w_2 = (x_5, y_5), (x_6, y_6)$
$k_1 : w_3 = (x_7, y_7), (x_8, y_8)$
3- Encrypt the round key using the parameter of the ECC method
4- Expand the encrypted round key

Algorithm2 : Encryption process
Input : plaintext, round key
output : ciphertext
- Apply AES algorithm
1- Add a round key to the plaintext (round 0)
2- Apply round 1...round 9 (Byte substitution, Shift rows, Mix columns, Add round key)
3- Apply round 10 (Byte substitution, Shift rows, Add round key.

4 Perfomance Analysis and Evaluation

Here, we compare the efficiency of ECC, AES, and the proposed methods (hybrid AES-ECC) using parameters such as encryption and decryption time.

Encryption time is the time consumed by any encryption process to change plaintext into ciphertext. Decryption time is the amount of time consumed to convert plaintext back to ciphertext. Figures 2 and 3 show the comparison between AES, ECC, and Hybrid AES-ECC algorithms. When we increase the size of text documents, we can see that the amount of time consumed for the encryption and decryption process of the proposed method is more than AES and ECC time, because it requires more computational processing.

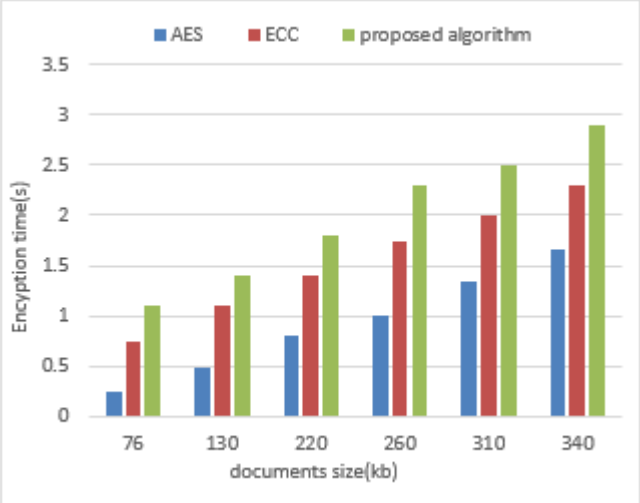

Figure 2: Time consumption to encrypt different documents

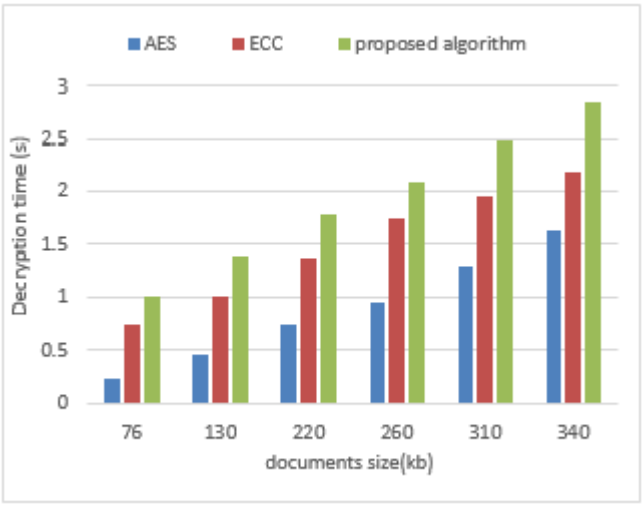

Figure 3: Time consumption to decrypt different documents

References

[1] V. K., A. S. Mitali, "A Survey of Various Cryptography Techniques," Int. J. Emerg. Trends Technol. Comput. Sci., Accessed: Nov. 5, 2022.

[2] William Stallings, Network Security Essentials: Applications and Standards.

[3] A. Kahate, "Cryptography and network security," (2013), 501, Accessed: Nov. 5, 2022.

[4] S. Ahmad, S. Mehfuz, J. Beg, "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment," J. Supercomput., **79,** (2023), 7377–7413.

[5] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 1987.

[6] R. K. Ansah, S. Effah-Poku, D. A. Addo, B. A. Adjei, B. K. Bawuah, P. Antwi, "Relvance of Elliptic Curve Tryptography in Modern-Day Technology," J. Math. Acumen Res.,**3,** no. 2, (2018), 1-10.

[7] S. M. C. Vigila, K. Muneeswaran, "Implementation of text-based cryptosystem using elliptic curve cryptography," 1st Int. Conf. Adv. Comput. (2009), 82–85.

[8] F. Amounas, E. H. El Kinani, "Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography," Int. J. Inf. Netw. Secur., **1,** no. 2, (2012), 54–59.

[9] "Announcing the Advanced Encryption Standard (AES)," Fed. Inf. Process. Stand. Publ., **197,** 2001.

[10] B. Liu, B. Baas, "Parallel AES encryption engines for many-core processor arrays," IEEE Trans. Comput., **62,** no. 3, (2013), 536–547.