DOI: 10.24996/ijs.2025.66.3.26

ISSN: 0067-2904

Hybrid Menezes Vanstone-ElGamal ECC Algorithm

Mohammed Hassan Alabiech [1], Haider M. Al-Mashhadi [2]

[1] *General Company of Electrical Energy Production – Southern Region, Ministry of Electricity, Basra, Iraq*

[2] *Department of Cybersecurity, College of Computer Science and Information Technology, University of Basrah, Basra, Iraq*

Received: 16/10/2023 Accepted: 11/3/2024 Published: 30/3/2025

Abstract

The larger public key techniques in RSA that are currently applied utilize 1024 bits for parameters. The NIST recommends that systems with 1024 bits are suitable for employment until 2010. Then, NIST advises that systems be updated to render security at a high level. One solution is to exploit the previous years of research and analysis in public key and move from former algorithms for public key to the Elliptic Curve (EC). This study suggests a public key technique that is faster than ElGamal ECC. The method in this paper is constructed by two standard methods: the Menezes-Vanstone ECC (MVECC) and the ElGamal ECC. The method is a hybrid of symmetric and asymmetric techniques to generate an asymmetric method. The proposed method does not rely on the Discrete Logarithm Problem (DLP) because the points generated are out of curve. The strategy of the proposed method is much like the ElGamal method, because each symbol generates two points without DLP. In addition, it is like the MVECC because there are no mapping points; in other words, the plaintext is not embedded into EC. It is faster than ElGamal ECC by around 5%–10%.

Keywords: Elliptic Curve Cryptography, Asymmetric Encryption, The Menezes - Vanstone ECC, ElGamal ECC.

خوارزمية منحنى الإهليلج الهجينة لمينيزيس–فانستون–الجمال

محمد حسن حالوب العبيج [1]*, حيدر محمد عبدالنبي [2]

[1] الشركة العامة لإنتاج الطاقة الكهربائية للمنطقة الجنوبية, وزارة الكهرباء, البصرة, العراق

[2] قسم الامن السيبراني, كلية علوم الحاسوب وتكنلوجيا المعلومات, جامعة البصرة, البصرة, العراق

الخلاصة

تستعمل التقنيات الرئيسية العامة الحالية في RSA أحجامًا أكبر من 1024 بت للخوارزميات. توصي المعايير الوطنية الأمريكية (NIST) بأن الأنظمة التي تحتوي على 1024 بت مناسبة للاستعمال حتى عام 2010. بعد ذلك، تنصح NIST بتحديث الأنظمة لضمان مستوى أمان عالٍ. الحل هو استغلال سنوات البحث والتحليل السابقة في المفتاح العام والانتقال من الخوارزميات السابقة للمفتاح العام إلى المنحنى الإهليلجي. (EC) تقدم هذه الدراسة تقنية مفتاح عام أسرع من ElGamal ECC . تم بناء الطريقة في هذه الورقة من خلال طريقتين قياسيتين Menezes-Vanstone ECC (MVECC) و ElGamal ECC

*Email: Mohplan@yahoo.com

الطريقة عبارة عن مزيج من التقنيات المتماثلة وغير المتماثلة لتوليد طريقة غير متماثلة.لا تعتمد الطريقة المقترحة على مشكلة الخوارزمية التكرارية المنفصلة(DLP) ، لأن النقاط التي تم إنشاؤها خارج المنحنى. استراتيجية المقترح تشبه إلى حد كبير طريقة ElGamal، لأنه لكل رمز يولد نقطتين ولكن بدون DLP بالإضافة إلى ذلك ، فهي تشبه MVECC لأنه لا توجد تعيين نقاط ، بعبارة أخرى، لا يتم تضمين النص العادي في EC . إنها أسرع من ElGamal ECC بحوالي (5٪−10٪).

1. Introduction

ECC is being moved from theoretical to adopted technology by an increasing number of entities due to two reasons: first, ECC is no longer new and has withstood a generation of attacks; second, there is an increase in the wireless industry [1]. ECC is usually implemented as a sequence of arithmetic operations in a finite field [2]. It is widely spread in several applications like smart cards [3–4], digital signal processing [3, 5], wireless devices [3, 6], and ECC is more suitable for secure email systems because of the higher security [7]. The security level of ECC also depends on the size of the used keys [8].

The fundamental benefit of using the ECC is that it uses a shorter key compared to the RSA, but with the same protection level. The ECC technique decreases the processing overhead as well as the processing time [8–9], and it is basically more complex to comprehend than RSA. The mathematics of the ECC technique is significantly more interesting than that of RSA and Discrete Logarithm (DL). Several environments are applied to the ECC technique, for example, cellular phones and email. Moreover, in view of the manifest development of the basic Elliptic Curve Discrete Logarithm Problem (ECDLP), it is suitable to enhance the security that is needed in software for all time [9].

The basic equation of EC over the value in the real numbers is known as [10–13]:

$$y^2 = x^3 + ax + b \tag{1}$$

Where, a and b are real numbers, and both satisfy the following condition

$$4a^3 + 27b^2 \neq 0 \tag{2}$$

Where x and y are any supposed real numbers.

The prime curve over Z_p (where $p > 3$) is used in the third-degree equation shown below:

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

Where,

$$(4a^3 + 27b^2)\ mod\ p\ \neq 0 \tag{4}$$

The security of an ECC is principally bounded by the cost of computing the DLP. Now, the study provides a summary overview of the parameters of security (key bit length) of the EC in comparison to the public key cryptosystem RSA [14–15]. Table 1 below shows the security strength of the ECC compared to the RSA in terms of key size and period in Million Instructions per Second (MIPS) [16].

Table 1: Secret and public key sizes with equivalent security levels.

ECC (bit)	RSA (bit)	Time to be break in MIPS
106	512	10^4
160	1024	10^{11}
210	2048	10^{20}
600	21000	10^{78}

The fundamental guarantee of ECC security primarily relies on the strength of the ECDLP [9]. ECDLP is considered the main procedure in the ECC technique, and it is a necessity since it is executed effectively. It is defined on EC as below:

$$T = tP = \underbrace{P + P + P \ldots}\ldots + P \tag{5}$$

\
t times

Where tP indicates that the point P over EC adds to itself t times, P is a distinct point over EC, and t is a big integer in Equation (5) [3]. When given T and P, it's computationally unwieldy to calculate the t value when t is sufficiently substantial [17–18], and when t is the case with the discrete logarithm problem modulo p, we have so far found no effective algorithm to solve the ECDLP [11].

The ElGamal ECC is an asymmetric encryption process that begins with converting every mapping point to two points (kG, P-m + kP_B), where k is a random integer $1\leq k \leq n\text{-}1$, n is the order of the group, G is the base point, P-m is plaintext, and P_B is the public key of the receiver. On the other side, in order to convert the ciphertext to plaintext, the algorithm should multiply the first point in the pair by secret nB and then subtract the consequence from the other point in the pair [19].

The Menezes-Vanstone ECC (MVECC) technique does not rely on DLP as in the previous cryptosystem. The elliptic curve is used for "masking." Plaintext and ciphertext allow arbitrary ordered pairs of nonzero elements. These pairs do not need to be points on the curve. The encryption algorithm takes four numbers: two numbers from plaintext (*m1, m2*) and the others from key points (*k1, k2*). Ciphertext (*c1, c2*) is represented by two numbers that have been computed. The ASCII of a symbol can be converted to a pair of numbers (*m1, m2*), e.g., the ASCII "97" is split into (9, 7) [20].

Encryption:

$$c_1 = m_1 * \ k_1 \, mod \, p \tag{6}$$

$$c_2 = m_2 * \ k_2 \, mod \, p \tag{7}$$

Decryption:

$$m_1 = \ c_1 * k_1^{-1} \, mod \, p \tag{8}$$

$$m_2 = \ c_2 * k_2^{-1} \, mod \, p \tag{9}$$

2. Related Work

Many scientists have tried to employ the criteria of the EC technique to implement it for application security.

Neal Koblitz introduced a public-key cryptosystem elliptic curve over a finite field [11]. W. Stallings has made the view of the ECC [9] easy. Guicheng Shen et al. used object-oriented technology as a tool and divided the Elliptic Curve Cryptosystem into several layers, with each layer representing a class. The properties and methods of these classes are discussed, and some of the methods are put into action. Finally, the analysis highlights the advantages, emphasizing that the cryptosystem, implemented with an advanced programming language, is easily transferrable [21]. R. Kodali and N. Sarma used ECC symmetric encryption with Koblitz's encoding to map the data into points located on EC. It requires about one-third of the total modulo operations used in the ECC encryption, which is good for WSN applications [17].

Laiphrakpam et al. introduced an image encryption/decryption implementation technique that incorporates a digital signature into the cipher image to ensure authenticity and integrity. The operation involved grouping pixels based on Elliptic Curve Cryptography (ECC) parameters, specifying the number of pixels that could be grouped. Instead of mapping these values to elliptic curve coordinates, the study employs the pairing of grouped pixel values. This approach eliminates the need for a reference-mapping table in encryption and decryption. The algorithm developed produces a low-correlated cipher image, even when the original image consists of identical pixel values [22]. Islam et al. identified deficiencies in Tan's

3PAKE protocol and subsequently developed an enhanced version tailored for mobile-commerce environments. The improved 3PAKE protocol omits symmetric key encryption/decryption techniques and relies on elliptic curve cryptography and a one-way cryptographic hash function. The security of the scheme was validated using the AVISPA software, demonstrating resilience against active and passive attacks, including replay and man-in-the-middle attacks. It is proven secure against various security threats such as man-in-the-middle attacks, impersonation attacks, parallel attacks, and key compromise impersonation attacks. It is designed with low computation [23].

Haider Al-Mashhadi and Mohammed Alabiech presented a new efficient practical algorithm for symmetric encryption using ECC. By sending a secret shared key between two entities, each symbol in a message will have a variable key. The described method's advantage in using a symbol key that the sender and receiver generate stands out. This generation is facilitated through both private and public keys using the Diffie-Hellman method, enabling the exchange of initial parameters. The primary contribution of this method resides in its approach to changing the secret key for each symbol. Even if the secret key for one symbol is exposed, it does not compromise the security of all symbol keys, ensuring a more robust encryption system [24].

To guarantee the secure sharing of private photos in the public cloud based on the block pixel position, this research provides three effective hybrid homomorphic encryption approaches for image encryption. The suggested procedures constrain El-Gamal and the Enhanced Homomorphic Cryptosystem (EHC) [25]. K. Sowjanya et al. introduced an improved lightweight end-to-end authentication protocol based on elliptic curve cryptography (ECC) to address security vulnerabilities found in Li et al.'s scheme. The proposed protocol undergoes formal security analysis using BAN logic and the AVISPA tool. The comparative analysis demonstrated that the new scheme not only rectifies security loopholes present in Li et al.'s scheme but also decreases the overall complexity [26].

Muhammed Habek et al. discussed the parameters and security attacks influencing the efficiency of digital image encryption in their work. They reviewed related studies, emphasizing the importance of considering both design criteria when developing new digital image encryption methods [27]. Abboud et al. created the System Determine Algorithm (SDA), which is meant to run system tasks in parallel, which makes the MOLAZ method of encryption faster and easier to understand. SDA generates independent sub-systems, optimizing hardware resources and allowing the concurrent use of 256-bit AES and 128-bit AES modules. The architecture aims to enhance data processing speed by combining the strength of AES-256 with the speed of AES-128, making it suitable for critical applications involving encryption and decryption of large datasets, such as those found in hard disks [28].

3. Proposed Method

The "Hybrid Menezes-Vanstone-ElGamal ECC" (HMVGECC) is a proposed scheme that uses the MVECC and the ElGamal ECC as its two standard construction methods. The method is a hybrid of symmetric and asymmetric techniques to generate asymmetric methods. The proposed method does not rely on DLP because the points generated are off the curve. The strategy of the proposed method is much like the ElGamal method because each symbol generates two points. In addition, it is like the MVECC because there is no mapping point; in other words, the plaintext is not embedded into EC. Algorithm 1 explains the encryption algorithm.

Algorithm 1: The HMVGECC encryption algorithm

Input: $G\in$ EC, m is plaintext, P_B is the public key of recipient
Output: The ciphertext [kG, C]
for i=1 to length (m)
    select $k_i \in [1, n\text{-}1]$
    compute $k_i\, G, k_i P_B$
$(d_1, d_2) \leftarrow$ ASCII (m_i)
$C_i \leftarrow (d_1, d_2) + k_i P_B$
end for
return kG, C

In the first, the algorithm selects a randomized number k between 1 and n-1 (n = 5407 in an example below) and then multiplies it with the base point G (k_iG) as well as multiplying it with the receiver public key (k_iP_B). The plaintext is allowed to contain arbitrary ordered pairs of (nonzero) elements, and the ASCII of a symbol can be converted to a pair of numbers (d_1, d_2). These pairs do not need to be points on the curve. Now, the algorithm adds (d_1, d_2) and (k_iP). The output of the algorithm, or the ciphertext, is two points.
As an example *, to start with the encryption process, let us assume p = *5449*, a = *1100*, and b = *750*. The #E(Fp) = *5407*, and the EC is represented by:
$$y^2 \bmod 5449 = (x^2 + 1100x + 750) \bmod 5449$$

The sender and receiver (Alice and Bob) must exchange the public keys by applying the Diffie-Hellman key exchange.
Let us assume base point G = (0, 1266), private key for Alice nA = 690, and Bob nB = 1710. The point multiplication is used between the private keys and G. As a consequence, the public key of Alice (P_A), which was sent to Bob, is (1186, 3477), and the public key of Bob (P_B), which was sent to Alice, is (2908, 3677).
When we try to encrypt "computer science&%^$", the Table 2 shows the encryption process.

Table 2: The encrypted points of the HMVGECC technique

Symbol	ASCII	(m_1, m_2)	k	kP_B	Ciphertext	
					kG	$(m_1, m_2) + kP_B$
c	99	(9,9)	790	(3569,3544)	(5279,1018)	(1193,1999)
o	111	(11,1)	4648	(4392,4423)	(5278,313)	(82,2344)
m	109	(10,9)	3389	(5173,3022)	(4536,2522)	(3752,965)
p	112	(11,2)	1912	(883,1307)	(36,4074)	(4512,5441)
u	117	(11,7)	2797	(4479,3466)	(2885,2190)	(85,3470)
t	116	(11,6)	2190	(3344,5292)	(2078,4765)	(1483,1539)
e	101	(10,1)	414	(3352,884)	(3036,693)	(1940,3350)
r	114	(11,4)	1308	(2748,5403)	(1015,4357)	(2706,5327)
space	32	(3,2)	672	(5161,3790)	(4716,5095)	(465,3147)
s	115	(11,5)	1002	(3178,3252)	(1780,371)	(2723,764)
c	99	(9,9)	1308	(2748,5403)	(1015,4357)	(4851,2386)
i	105	(10,5)	2274	(3501,3821)	(2227,3207)	(1638,4025)
e	101	(10,1)	271	(5061,399)	(3829,384)	(379,368)
n	110	(11,0)	4918	(3545,2089)	(169,2250)	(2786,3582)
c	99	(9,9)	5148	(5434,3400)	(1232,2308)	(4294,1722)
e	101	(10,1)	2675	(2176,2025)	(4264,2065)	(2635,897)
&	38	(3,8)	2232	(4118, 1158)	(1778, 506)	(3117,1737)
%	37	(3,7)	4577	(5228, 1241)	(1425, 2998)	(4637,1682)
^	94	(9,4)	2716	(2125, 4340)	(3416, 4487)	(2259,4213)
$	36	(3,6)	1239	(1618, 2112)	(2874, 1281)	(4265,4484)

Where symbol is the plaintext, ASCII is the ASCII code of the symbol, (m_1, m_2) is the ASCII symbol converted to a pair of numbers, k is the random number between 1 and n-1, kP_B is k multiplied by the public key of the receiver P_B, and kG is k multiplied by the base point G.

The decryption algorithm of the HMVGECC is demonstrated in Algorithm 2, and the result of the algorithm is displayed in Table 3.

Algorithm 2: The HMVGECC (Decryption Algorithm)

Input: The ciphertext [kG, C], n_B is the private key for recipient (Bob).
Output: m is plaintext.
1: for i=1 to length (C)
2: compute $n_B(kG)_i$
3: $m_i \leftarrow C_i - n_B(kG)_i$
4: **end for**
5: **return** m

On the receiver side, the ciphertext is a two-point (kG) and (C). The receiver multiplies his private key with (kG) and then subscribes to the result from (C).

Table 3: The decrypted points of the HMVGECC technique

Ciphertext *kG*	**$(m_1, m_2) + kP_B$**	**$n_B(kG)$**	**$(m_1, m_2) + kP_B - n_B(kG)$**	**ASCII**	**Symbol**
(5279,1018)	(1193,1999)	(3569,3544)	(9,9)	99	c
(5278,313)	(82,2344)	(4392,4423)	(11,1)	111	o
(4536,2522)	(3752,965)	(5173,3022)	(10,9)	109	m
(36,4074)	(4512,5441)	(883,1307)	(11,2)	112	p
(2885,2190)	(85,3470)	(4479,3466)	(11,7)	117	u
(2078,4765)	(1483,1539)	(3344,5292)	(11,6)	116	t
(3036,693)	(1940,3350)	(3352,884)	(10,1)	101	e
(1015,4357)	(2706,5327)	(2748,5403)	(11,4)	114	r
(4716,5095)	(465,3147)	(5161,3790)	(3,2)	32	Space
(1780,371)	(2723,764)	(3178,3252)	(11,5)	115	s
(1015,4357)	(4851,2386)	(2748,5403)	(9,9)	99	c
(2227,3207)	(1638,4025)	(3501,3821)	(10,5)	105	i
(3829,384)	(379,368)	(5061,399)	(10,1)	101	e
(169,2250)	(2786,3582)	(3545,2089)	(11,0)	110	n
(1232,2308)	(4294,1722)	(5434,3400)	(9,9)	99	c
(4264,2065)	(2635,897)	(2176,2025)	(10,1)	101	e
(1778, 506)	(3117,1737)	(4118, 1158)	(3,8)	38	&
(1425, 2998)	(4637,1682)	(5228, 1241)	(3,7)	37	%
(3416, 4487)	(2259,4213)	(2125, 4340)	(9,4)	94	^
(2874, 1281)	(4265,4484)	(1618, 2112)	(3,6)	36	$

Where $nB(k\text{G})$ is the private key of the receiver multiplied by kG.

4. Results and Analysis

A. Experimental Environment

The framework of the research is designed using MATLAB R2014a software on a 32-bit system with a 3.16 GHz Core i5 processor and 4.00 GB of RAM, run with the MS Windows 7 operating system.

To calculate the time of all encryption schemes, the schemes are performed on 5 text files that have different sizes (10, 20, 30, 40, and 50 KB) 10 times for each file. Then, the average of the 10 runs represents the final time. The study will use the same parameters as in Section 3.

B. Analysis of the Proposed Method

The HMVGECC technique is faster than ElGamal ECC and more confusing because the points are out of curve; hence, it is no analogue for DLP. The proposed method has more security than the MVECC scheme because it is asymmetric and MVECC is symmetric.

When the ElGamal ECC, MVECC, and the proposed technique are compared, the study finds a difference in time consumption, as clarified in Table 4.

Table 4: A Comparison of the Time Consumption of the Algorithms ElGamal ECC, MVECC, and HMVGECC

File size (KB)	Encryption and Decryption Time (Sec.)		
	ElGamal ECC	MVECC	HMVGECC
10	2.1933	0.0984	2.0396
20	4.3083	0.2012	4.0796
30	6.8469	0.2934	6.1832
40	8.5323	0.4366	8.0768
50	10.9983	0.5351	10.2606

From Table 4, the results show the long difference in processing time between the MVECC and the proposed. The time consumption for the MVECC is faster than the HMVGECC by about 95% because the MVECC is symmetric and the HMVGECC is asymmetric. Both the proposed method and the ElGamal ECC use asymmetric encryption, but the proposed method is faster by a factor of 5 to 10 percent. This is because the ElGamal ECC used a search algorithm to find symbols during the decryption process, but the proposed method did not. Figure 1 displays the processing times for both systems.

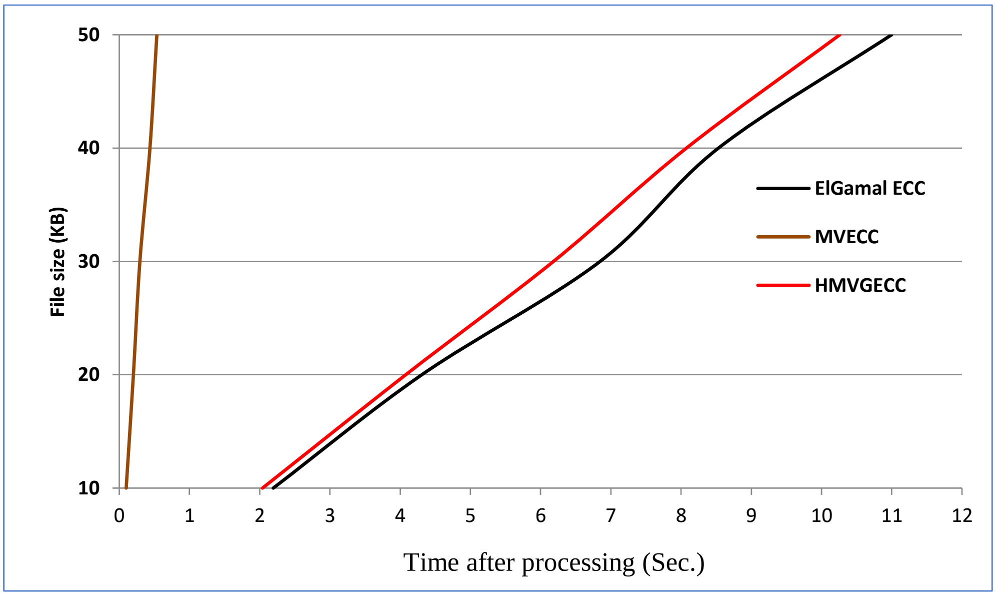

Figure 1: Processing time of the algorithms ElGamal ECC, MVECC, and HMVGECC

From Table 4 and Figure 1, the study concluded that the HMVGECC has high speed in implementation, and when analyzing encryption and decryption time, in Figure 2, the results show that the decryption time is shorter than the encryption time, which is very important for the receiver to read the message quickly.

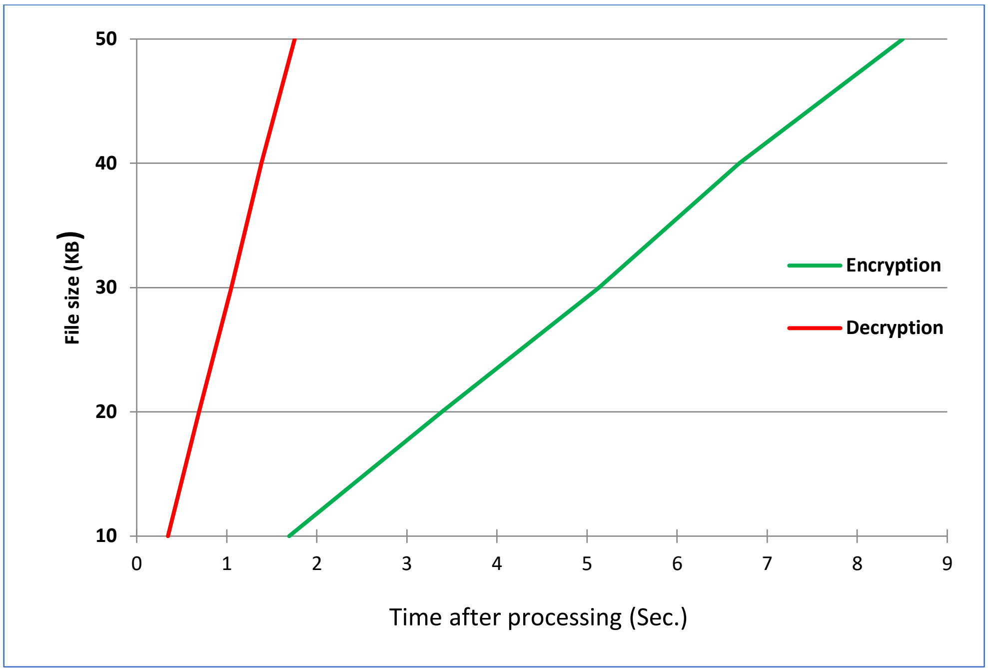

Figure 2: Processing time of encryption and decryption in the HMVGECC scheme

In the simulation above, the increase in the size of the files is 10 KB, and now let us assume that the increase is non-linear, as in Table 5.

Table 5: A Comparison of the Time Consumption of the Algorithms ElGamal ECC, MVECC, and HMVGECC with Files in Non-Liner

File size (KB)	Encryption and Decryption Time (Sec.)		
	ElGamal ECC	MVECC	HMVGECC
20	4.3083	0.2012	4.0796
27	5.9291	0.2711	5.5308
35	7.8856	0.3535	7.1477
47	10.3178	0.4506	9.6781
68	14.5139	0.7521	13.7405

In the above example*, the study took the value of a as 4 digits and b as 3 digits. How would the results be if the values of a and b were 4 digits? The answer to this question is to rely on the number of points on the curve bounded by $p + 1 - 2\sqrt{p} \leq \#E(F_p) \leq p + 1 + 2\sqrt{p}$ which is known as *Hasse bound*. Let us assume p= 5449, a= 1100, b= 2500, the #E(Fp) = 5408, but when p= 5449, a= 750, b= 750, the #E(Fp)= 5417. In this example, the number of points when a is 3 digits and b is 3 digits is greater when a is 4 digits and b is 4 digits. So, for #E(Fp) the results depend on the number of points in the curve and not on digits a or b.

C. Discussion

The following table summarizes the results of the proposed encryption technique.

Table 6: General Comparison of Algorithms ElGamal ECC, Menezes-VVanstone, and HMVGECC

Technique	Average Time consumption (Sec.)	Type	Analogue for DLP	Symbol Frequency	Diffusion	Confusion
ElGamal ECC	6.57582	Asymmetric	Yes	NO	Yes	Yes
Menezes - Vanstone	0.31294	Symmetric	NO	Yes	NO	Yes
HMVGECC	6.12796	Asymmetric	NO	NO	Yes	Yes

From Table 6, the slowest scheme is the ElGamal ECC because it is an asymmetric scheme that generates two points for each symbol and depends on random variables during the encryption process. Whereas the fastest one is the Menezes-Vanstone scheme because it is a symmetric scheme and does not use the search algorithm to find symbols in the decryption process.

On the other hand, the HMVGECC technique is a public key encryption; it has no frequency for the symbols and works out of the EC. The HMVGECC technique is diffused because it gives a different ciphertext for each encryption of the same plaintext. The HMVGECC's diffusion property can be studied using point multiplication on the elliptic curve. This is because diffusion means making sure that a change in one part of the plaintext or key affects a lot of the ciphertext. The spreading effect ensures that changes in the input (plaintext or key) produce extensive changes in the output (ciphertext or public key). All techniques in Table 6 are confused since the relationship between the ciphertext and the key is so complicated that the attack on the key is very difficult, and the confusion property in the HMVGECC relies on the complexity of mathematical problems. The difficulty of determining the private key from the public key ensures that even if an attacker knows parts of the plaintext, it remains computationally infeasible to reconstruct the private key. In short, the HMVGECC is better than others in terms of security performance.

5. Conclusions and Future Work

The proposed method in this paper is constructed by two standard methods: the Menezes-Vanstone ECC (MVECC) and the ElGamal ECC. The number of points that can be generated is faster than ElGamal ECC by around 5%–10%, as shown in Table 4,5, because ElGamal ECC used the search algorithm to find symbols in the decryption process while the proposed technique did not, and this technique uses "masking," meaning no mapping point. The proposed method is more confusing and diffuse when compared with the ElGamal ECC because the points generated are out of the curve, so the range of cipher points could be wider than the ElGamal ECC and can be used with the email server.

The speed of the method can be increased to a higher level by applying parallel processing through the Graphics Processing Unit (GPU). This is a good solution. The GPU can speed up the massive execution by using an NVidia graphics card (GeForce).

The idea of introducing quantum computing into the encryption process, especially using EC in general and proposed in particular, is an area of active research known as quantum-safe or post-quantum cryptography.

Finally, as with any cryptographic scheme, the new encryption method undergoes continuous evaluation, peer review, and refinement to address emerging security challenges and ensure its long-term viability. This iterative process involves collaboration with cryptographic experts and researchers to enhance the method's security and resilience over time.

References

[1] L. Savu, "Information Security on Elliptic Curves," in *Proceedings of the 5th WSEAS international conference on Communications and information technology, World Scientific and Engineering Academy and Society (WSEAS)*, pp. 69-72, 2011.

[2] Alrimeih, Hamad, and Daler Rakhmatov, "Fast and Flexible Hardware Support for ECC over Multiple Standard Prime Fields," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 12, pp. 2661-2674, 2014.

[3] H. Javashi and R. Sabbaghi-Nadooshan, "A Novel Elliptic Curve Cryptography Processor Using NoC Design," *International Journal of Computer Science*, vol. 8, no. 3, pp. 1-6, 2011.

[4] A. D. Woodbury, D. V. Bailey, and C. Paar, "Elliptic Curve Cryptography on Smart Cards without Coprocessors," in *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications, Bristol, United Kingdom, Springer*, pp. 71-92, 2000.

[5] Marzouqi, Hamad, Mahmoud Al-Qutayri, Khaled Salah, Dimitrios Schinianakis, and Thanos Stouraitis, "A High-Speed FPGA Implementation of an RSD-Based ECC Processor," *IEEE Transactions on very large scale integration (VLSI) systems*, vol. 24, no. 1, pp. 151-164, 2015.

[6] Chatterjee, Uddalak, Sangram Ray, Sharmistha Adhikari, Muhammad Khurram Khan, and Mou Dasgupta, "An Improved Authentication and Key Management Scheme in Context of IoT-Based Wireless Sensor Network Using ECC," *IEEE Wireless Communications*, vol. 209, pp. 47-62, 2023.

[7] Xia Lin, "The Application of Elliptic Curve Cryptography in Secure E-mail System," in *Proceedings of the International Conference on Advanced Material Science and Environmental Engineering (AMSEE), Atlantis Press*, pp. 293-296, 2016.

[8] Suárez-Albela, Manuel, Paula Fraga-Lamas, and Tiago M. Fernández-Caramés, "A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices," *Sensors*, vol. 18, no. 11, pp. 1-26, 2018.

[9] W. Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, India, 2006.

[10] D. Hankerson, A. J. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer Science & Business Media, 2004.

[11] Neal Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[12] Blake, Ian F., Gadiel Seroussi, and Nigel P. Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.

[13] Abdullah, K.E. and N.H.M. Ali, "A Secure Enhancement for Encoding/Decoding Data Using Elliptic Curve Cryptography," *Iraqi Journal of Science*, vol. 59, no. 1A, pp. 189-198, 2018.

[14] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC press, 2005.

[15] Ogunleye, G. and S. Akinsanya, "Elliptic Curve Cryptography Performance Evaluation for Securing Multi-Factor Systems in a Cloud Computing Environment," *Iraqi Journal of Science*, vol. 63, no. 7, pp. 3212-3224, 2022.

[16] S. Manickam and D. Kesavaraja, "Secure Multi Server Authentication System Using Elliptic Curve Digital Signature," in *Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT), IEEE*, pp. 1-4, 2016.

[17] Ravi Kishore Kodali and N.V.S Narasimha Sarma, "ECC Implementation Using Koblitz's Encoding", in *Proceedings of the Conference on Communication Engineering and Network Technologies (CENT), Elsevier*, pp. 411-417, 2012.

[18] Masaaki Shirase, "New operation and problems on elliptic curve and their application," in *Proceedings of the IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), IEEE*, pp. 1-2, 2018.

[19] Reegan, A. Selva, 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.

[20] Al-Saffar, N.F.H., M.D Said and M. Rushdan, "The Mathematical Complexity and the Time Implementation of Proposed Variants of Elliptic Curves Cryptosystems," *International Journal of Cryptology Research*, vol. 4, no. 1, pp. 42-54, 2013.

[21] Guicheng Shen and Xuefeng Zheng, "Research on Implementation of Elliptic Curve Cryptosystem in ECommerce", in *Proceedings of the Symposium on Electronic Commerce and Security, IEEE*, pp. 288-291, 2008.

[22] Laiphrakpam Dolendro, and Khumanthem Manglem, "Image Encryption Using Elliptic Curve Cryptography," *Procedia Computer Science, Elsevier*, vol. 54, pp. 472-21, 481, 2015.

[23] SK Hafizul Islama, Ruhul Aminb , G. P. Biswasb , Mohammad Farashc , Xiong Lid and Saru Kumarie, "An Improved Three Party Authenticated Key Exchange Protocol Using Hash Function and Elliptic Curve Cryptography for Mobile-Commerce Environments," *Journal of King Saud University-Computer and Information Sciences*, vol.29, no.3, pp.1-20, 2017.

[24] Haider Al-Mashhadi and Mohammed Alabiech, "Symmetric ECC with Variable Key Using Chaotic Map," *International Journal of Computer Science Issues*, vol. 14, no. 6, pp. 24-28, 2017.

[25] Haider Al-Mashhadi and Ala'a A. Khalf, " Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud," *International Journal of Computer Science and Network Security*, vol. 18, no. 3, pp. 48-55, 2018.

[26] K. Sowjanya, Mou Dasgupta and Sangram Ray, "An Elliptic Curve Cryptography based Enhanced Anonymous Authentication Protocol for Wearable Health Monitoring Systems," *International Journal of Information Security, Springer*, pp. 1- 18, 2019.

[27] Muhammed Habek, Yasin Genc, Nilay Aytas, Ahmet Akkoc, Erkan Afacan, and Erdem Yazgan, "Digital Image Encryption Using Elliptic Curve Cryptography: A Review," in *Proceedings of the International Congress on Human-Computer Interaction, Optimization and Robotic Applications, IEEE*, pp. 1-8, 2022.

[28] Udai Wasmi, and Moceheb Shuwandy, "SDA Plus: Improving the Performance of the System Determine Algorithm (SDA) of the Switching Between AES-128 and AES-256 (MOLAZ Method)," in *Proceedings of the IEEE 13th International Conference on System Engineering and Technology (ICSET), IEEE*, pp. 61-65, 2023.