International Journal of Cryptology Research 4(1): 42 - 54 (2013)

On the Mathematical Complexity and the Time Implementation of Proposed Variants of Elliptic Curves Cryptosystems

[1*] Najlae F. Hameed Al-Saffar and [2] Mohamad Rushdan Md Said

[1,2]Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 UPM Serdang, Malaysia

[1]Department of Mathematics,
Faculty of Mathematics and Computer Science,
54001 Kufa University, Iraq

E-mail: najlae_falah@yahoo.com and rushdan@math.upm.edu.my

*Corresponding author

ABSTRACT

The group of the elliptic curve points forms an abelian group, which is considered as a suitable choice for constructing a problem similar to the Discrete Logarithm Problem. This creates and opens a new door for treatments of the special group and new operations. In 2005, Al-Saffar (2005) proposed two new methods for elliptic curve cryptosystems using the keys from the algorithm of Diffie–Hellman Key Exchange. In addition, she introduced a variant of the ElGamal scheme. Also, three propositions were introduced to develop the Menezes-Vanstone Elliptic Curves Cryptosystem (MVECC). In this paper, we will discuss all of these propositions and will compare them with the original schemes (ElGamal and MVECC) according to the complexity and the time which they took to implement each scheme.

Keywords: Abelian group, Discrete Logarithm Problem, Diffie–Hellman Key Exchange, ElGamal scheme.

1. INTRODUCTION

Elliptic curve is a set of solution to binary equations. Elliptic curve cryptography prefer ably implemented using non-super singular because of its better security. The group Elliptic Curve systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz (1987) from the University of Washington, and Victor Miller (1986). The elliptic curve cryptosystem was thus created. Since then, numerous researchers and developers have spent years researching the strength of ECC and improving the techniques for its implementation. Today, the scientific efforts are looking for a smaller and faster public key cryptosystem, a practical and secure technology, even for the most constrained environments (see Henkerson and Menezes, (2003)). For any cryptographic system based on the discrete logarithm problem, there is an analogue for Elliptic Curve (Meng (2001)). One of these systems is Diffie – Helman key exchange system.

Discrete logarithm cryptosystems have been first described in the setting of the multiplicative group of the integers modulo a prime p. Such systems can be modified to work in the group of points on an elliptic curve. For example, the Diffie–Hellman key exchange can be adapted for elliptic curves as follows: Firstly, note that a random point on an elliptic curve E can serve as a key, since Ali and Benin can agree in advance on a method to convert it to an integer. So suppose that E is an elliptic curve over F_p , and P is a publicly known point on this curve. Ali secretly chooses a random integer kA and computes the point kAP, which he sends to Benin. Now, Benin secretly chooses a random kB, computes kBP, and sends it to Ali. Therefore the common key is $Q = kAkBP$. Ali computes Q by multiplying the point he received from Benin by his secret kA, and Benin computes Q by multiplying the point she received from Ali by her secret kB. An eavesdropper who wanted to spy on Ali and Benin would have to determine $Q = kAkBP$ knowing P, kAP, and kBP, but not kA or kB.

This paper, firstly will discuss ElGamal and MVECC which were considered as the original schemes in ECC. Secondly, we will discuss all propositions which have been introduced in Al-Saffar (2005). Finally, we will compare them with the original schemes according to the complexity and the time which they took to implement each scheme.

2. ElGamal ELLIPTIC CURVE CRYPTOSYSTEM (ElGamal ECC)

EIGamal elliptic curve cryptosystem is a popular and important cryptosystem because of its safety, efficiency and low complexity. Let $E(F_p)$ be an elliptic curve group and let B be a point on E. The user Benin first selects a private key d and generates a public key $Q = dB$. Second, Ali to encrypt and send a message P_m to Benin, he chooses a random positive integer e and produce the ciphertext C_m, such that:

$$C_m = \{C, eB\}, \text{ where } C = P_m + eQ.$$

To decrypt the ciphertext, Benin computes the following:

$$\begin{aligned} C - d(eB) &= P_m + eQ - d(eB) \\ &= P_m + e(dB) - d(eB) \\ &= P_m \end{aligned}$$

Example

Let E be an elliptic curve define over F_{11317} with parameters $a = 9817$, $b = 47$ where $(4a^3 + 27b^2) \bmod p = 7090 \neq 0$ and $\#E = 11489$. Since $\#E$ is prime number, then every point on E is base point (Al-Saffar, 2005), so let $B = (11117,3663)$. If Ali wishes to send the message $M = (10498,\ 1304)$ to Benin using ElGamal elliptic curve cryptosystem, what should they do?

Solution

Benin chooses a random integer d as a secret key, let $d = 7391$ and computes her public key $dB = 7391*(11117,\ 3663) = (8916,\ 7552)$.

Ali chooses a random integer e as a secret key, let $e = 6693$ and computes

$$\begin{aligned} & e(dB) = 6693*(8916,\ 7552) = (2094,\ 6145), \\ & eB = 6693\ *(11117,\ 3663) = (326,\ 2417), \\ & C = M + e(dB) \\ & \quad = (10498,\ 1304) + (2094,\ 6145) \\ & \quad = (3038,\ 367), \end{aligned}$$

and sends $\{(3038,\ 367),(326,\ 2417)\}$ to Benin.

Benin to decrypt the cipher text, she computes

$d(eB) = 7391*(326,\ 2417) = (2094,\ 6145)$, and computes

$$\begin{aligned} C - d(eB) &= (3038,\ 367) - (2094,\ 6145) \\ &= (3038,\ 367)\ +\ (2094, -6145) \\ &= (10498,\ 1304) \\ &= M. \end{aligned}$$

3. MENEZES–VANSTONE ELLIPTIC CURVE CRYPTOSYSTEM (MVECC)

This is a cryptosystem that has no analogue for discrete logarithm problem (i.e. this cryptosystem does not depend on discrete logarithm problem as the above cryptosystems). In this variation, the elliptic curves is used for "masking", and plaintexts and ciphertexts are allowed to be arbitrary ordered pairs of (nonzero) elements (i.e., they are not required to be points on E) (see Sagheer (2004) and Pietiläinen (2000)).

Algorithm for MVECC

If Ali wants to encrypt and send Benin the message M, then they do the following setup:

Setup:

- Ali and Benin agree upon an elliptic curve $E(F_p)$ and a base point B.
- Benin first selects a private key d and generates a public key $Q = dB$.
- Ali wishes to encrypt and send a message $M = (m_1, m_2)$ to Benin, he chooses a random positive integer e and produces the ciphertext C_m consisting of the pair of points $C_m = \{C, eB\}$ and send it to Benin, where $C = (c_1, c_2)$ and

$$\begin{aligned} c_1 &= m_1.k_1 \bmod p, \\ c_2 &= m_2.k_2 \bmod p, \\ eQ &= (k_1, k_2). \end{aligned}$$

- Benin likes to decrypt the ciphertext, she computes the following

$$\begin{aligned} (k_1, k_2) &= d(eB), \textit{ and then} \\ m_1 &= c_1.k_1^{-1} \bmod p, \\ m_2 &= c_2.k_2^{-1} \bmod p. \end{aligned}$$

4. PROPOSITION TO VARIANT ElGamal ECC

To vary the encryption and decryption of ElGamal ECC, let $E(F)$ be an Elliptic Curve group and let B be a base point on E . The user Benin first selects a private key d and generates a public key $Q = dB$. If Ali would like to encrypt and send a message M to Benin, he should choose a random positive integer e and produce the ciphertext C_M , such that $C_M = \{C, eB\}$ where $C = M - eQ$**.** To decrypt the ciphertext, Benin computes the following

$$C + d(eB) = M - eQ + d(eB) = M - e(dB) + d(eB) = M$$

5. PROPOSITION TO DEVELOPMENT OF MVECC

The development of the encryption and decryption of MVECC are as follows:

(1) Suppose Ali wants to send a message $M = (m_1, m_2)$ to Benin. Let d denote Benin's secret key and $Q = dB$ [B is a point on E] denote Benin's public key . Ali chooses a random integer e and sends $C_M : C_M = \{C, eB\},$ where $C = (c_1, c_2), (k_1, k_2) = eQ,$ $c_1 = (m_1 + k_1k_2) \bmod p,$ $c_2 = m_1(m_2 + k_2k_1) \bmod p.$ To decrypt the ciphertext Benin computes:

$$(k_1, k_2) = d(eB),\ m_1 = (c_1 - k_1k_2) \bmod p,\ m_2 = m_1^{-1}c_2 - k_1k_2) \bmod p.$$

(2) Suppose Ali wants to sent a message $M = (m_1, m_2)$ to Benin. Let d denotes Benin's secret key and $Q = dB$ (B is a point on E) denotes Benin's public key. Ali chooses a random integer e and sends $C_M : C_M = \{C, eB\},$ where $C = (c_1, c_2), (k_1, k_2) = eQ,$ $c_1 = (m_1 *$ $(k_1k_2 - k_1)) \bmod p,$ $c_2 = (m_2 * k_1k_2 - k_2)) \bmod p.$ To decrypt the ciphertext Benin computes:

$$(k_1, k_2) = d(eB),\ m_1 = (c_1 * (k_1k_2 - k_1)^{-1}) \bmod p,$$
$$m_2 = (c_2 * (k_1k_2 - k_2)^{-1}) \bmod p.$$

(3) Suppose Ali wants to send a message $M=(m_1,m_2)$ to Benin. Let d denotes Benin's secret key and $Q=dB$ [B is a point on E] denotes Benin's public key. Ali chooses a random integer e and sends $C_M : C_M = \{C, eB\}$, where $C=(c_1,c_2),(k_1,k_2)=eQ$, $c_1 = m_1 + (k_1k_2^{k_1}{}_2)^{-1} \bmod p$, $c_2 = m_2 +$ $(k_2k_1^{k_2})^{-1} \bmod p$. To decrypt the ciphertext Benin computes: $(k_1,k_2)=d(eB)$, $m_1=(c_1-(k_1k_2^{k_1})^{-1}) \bmod p$, $m_2=(c_2-(k_2k_1^{k_2})^{-1}) \bmod p$.

6. PROPOSITIONS ALGORITHMS FOR ELLIPTIC CURVE CRYPTOSYSTEM

In these algorithms they have tried to benefit from the Diffie-Hellman Key Exchange to use this key (the key comes from DHEK algorithm) as secret key in the following algorithms:

Algorithm of (PA$_1$)

– Ali and Benin Compute $edB = S = (s_1,s_2)$. (Using DHEK algorithm)
– Ali sends a message $M \in E(F_p)$ to Benin as follows:
  – Compute $(s_1 * s_2)(\bmod N) = K$. (Such that $\gcd(s_1 * s_2, N) = 1)^1$
  – Compute $K * M = C$, and send C to Benin.
– Benin receives C and decrypts it as follows:
  – Compute $(s_1 * s_2)(\bmod N) = K$.
  – Compute $K^{-1}(\bmod N)$. (Where $N = \# E$)
  – $K^{-1} * C = K^{-1} * K * M = M$.

Algorithm of (PA$_2$)

– Ali and Benin Compute $edB = S = (s_1,s_2)$.
  (Using Diffie–Hellman Scheme)
– Ali sends a message M to Benin as follows:
  – Compute $(s_1^{s_2})(\bmod N) = K$. (Such that $\gcd(s_1^{s_2}, N) = 1)^1$
  – Compute $K * M = C$, and send C to Benin.
– Benin receives C and decrypts it as follows:
  – Compute $(s_1^{s_2})(\bmod N) = K$.
  – Compute $K^{-1}(\bmod N)$.

- $K^{-1} * C = K^{-1} * K * M = M$.

The public keys are eB and dB where B is the base point on $E(F_p)$ and the secret keys for Ali and Benin are e and d respectively.

Example

Let E be an elliptic curve define over F_p where $p = 3023$ with parameters $a = 1$, $b = 2547$ where $(4a^3 + 27b^2) \mathrm{mod}\ p = 2027 \neq 0$ and $\# E = N = 3083$. Since $\# E$ is prime number then, every point on E is base point (Al-Saffar (2005)), so let $B = (2237, 2480)$.

To apply Algorithm of (PA_2), at first we must apply Diffie–Hellman Exchanging key

- Ali chooses a secret random integer $e = 2313$.
  $eB = 2313*(2237,\ 2480) = (934,\ 29)$. And send $(934,\ 29)$ to Benin .
- Benin chooses a secret random integer $d = 1236$.
  $dB = 1236*(2237,\ 2480) = (1713, 1709)$. And send $(1713,\ 1709)$ to Ali
- Ali computes the secret key $e(dB)$=$2313*(1713,1709)$.
  $edB = (2537,\ 1632) = S$.
- Benin computes the secret key $d(eB)$=$1236*(934,\ 29)$.
  $deB = (2537,\ 1632) = S$.

Now, Ali and Benin have the same point $S = (2537,\ 1632)$.

If Ali send a message $M = (2284,\ 2430)$ to Benin, he does the following:

- Compute $s_1^{s_2} \mathrm{mod} N = 25371632 \mathrm{mod} 3083 = 323 = K$.
- Compute $K * M = 323*(2284,\ 2430) = (2555,\ 1066) = C,$ and send it to Benin.
- Benin receives C and decrypts it as follows:
- Compute $s_1^{s_2} \mathrm{mod} N = 323 = K$.
- Compute K^{-1} $\mathrm{mod} N =$ 323^{-1} mod $3083 = 1594$.

$$\begin{aligned} K^{-1}C &= 1594*(2555,\ 1066) \\ &= (2284,\ 2430) \\ &= \text{M}. \end{aligned}$$

7. ANALYSIS OF ELLIPTIC CURVES CRYPTOSYSTEMS

The development of elliptic curves cryptosystems based on the mathematical framework of complexity theory and the time which is taken to implement them. In this section we will analyses the above cryptosystems according to the mathematical complexity and the time implementation.

1. According to the Mathematical Complexity

The complexity of elliptic curve cryptosystem (the difficulty of breaking it) is exactly equivalent to solving the discrete logarithm problem. Finding the discrete logarithm of one element in the elliptic will not help find the logarithm of any other element. In fact, let $\#E$ denote group order of E and let r be the largest prime factor of $\#E$. Then the best known algorithms for finding discrete logarithms in E have complexity $\mathrm{O}\left(\sqrt{r}/n\right)$, where n is the number of processors working on the problem. Therefore the mathematical complexity of elliptic curve cryptosystem depends on the largest prime factor of the group order of the elliptic which is used in the system. And on the number of operations which are used during the processing of encryption and decryption algorithms. So, we can discuss the mathematical complexity according to the above fact as follows:

(i) When we study the scheme of ElGamal elliptic curve cryptosystem, we see that a variant of this scheme can be developed, but with the same complexity, as in the proposition to variant ElGamal elliptic curve cryptosystem because the addition and subtraction have the same computational complexity.

(ii) The proposed development 1 of Menezes-Vanstone elliptic curve cryptosystem is more efficient than the Menezes-Vanstone elliptic curve cryptosystem, where in the encryption scheme there are three multiplication operations $(k_1k_2, m_1m_2$ and $m_1k_2k_1)$ and two addition operations. While the decryption scheme needed to compute the inverse operations for m_1, and three multiplication operations $(k_1k_2, m_1^{-1}c_2$ and $m_1^{-1}k_1k_2)$ and two subtraction operations.

(iii) The proposed development 2 of Menezes-Vanstone elliptic curve cryptosystem is more efficient than the previous proposition, where in the encryption scheme there are three multiplication operations $(k_1k_2, m_1k_1k_2, m_1k_1, m_2k_1k_2$ and $m_2k_2)$ and two subtraction operations. On other hand, the decryption scheme needs to compute the inverse operations for $(k_1k_2 - k_1$ and $k_1k_2 - k_2)$, and also there were two multiplication operations $(c_1(k_1k_2 - k_1)^{-1}$ and $c_2(k_1k_2 - k_2)^{-1})$.

(iv) The proposed development 3 of Menezes-Vanstone elliptic curve cryptosystem is more efficient than the previous propositions development 1 and 2, where in the encryption scheme they used the exponentiation operation between two keys to make the key more secure $(k_2^{k_1}$ and $k_1^{k_2})$, and this scheme needs to compute the inverse operations for $(k_1k_2^{k_1}$ and $k_2k_1^{k_2})$ also two addition operations. The decryption scheme needs to compute all the above operations in the encryption scheme and two subtraction operations.

(v) The two propositions (Algorithm of (PA_1) and Algorithm of (PA_2)) which have new design to encrypt and decrypt the ciphertext which should be a point on elliptic curve that has been used in the system. The second one is more complex than the first one that is because of the fact that the process of exponential operation is more complex than mathematical process of multiplication operation.

2. According to the time implementation

In order to measure the amount of time required to encrypt and decrypt any text we have simulated all programs with the MATLAB/ version 7.10.0.499/ 32-bit (The Language of Technical Computing).

Cryptosystems often take slightly different amounts of time to process different inputs, so in this section we used different elliptic curves with different prime numbers (size of digits) and different messages to compare between all above systems accordance with the time required to implement each process.

In each term we found that the encryption process in all systems has taken a longer time if we compare it with time which has been taken in the decryption process except the process in the proposed algorithms 2 for elliptic curve cryptosystems, where the time to decrypt the ciphertext is longer than the time to encrypt it.

The ElGamal elliptic curve cryptosystem is the longer system to encrypt and decrypt followed by Menezes-Vanstone elliptic curve cryptosystem and then the development 3 of Menezes-Vanstone elliptic curve cryptosystem, the development 1 of Menezes-Vanstone elliptic curve cryptosystem, the development 1 of Menezes-Vanstone elliptic curve cryptosystem, Variant of ElGamal elliptic curve cryptosystem, the development 1 of Menezes-Vanstone elliptic curve cryptosystem and Proposed Algorithms 1 for elliptic curve cryptosystems, while the faster system was the proposed algorithms 2 for elliptic curve cryptosystems.

All in all, however the difference between them was very small, but the systems which have been introduced in (Al-Saffar, 2005) were faster than the popular systems such as Elgamal or Menezes-Vanstone elliptic curve cryptosystem. We will sample the above by the following:

Example

Suppose that we have E be an elliptic curve define over F_{8233} with parameters $a=0$ and $b=139$ where $\left(4a^3+27b^2\right) \bmod 8233 \equiv 2988 \neq 0$. And $\#E=8089$, with base point $B=(8216,7477)$. If Ali wishes to send the message M to Benin using different elliptic curves cryptosystems he will choose a random integer e as a secret key (let $e=6234$) and Benin will choose a random integer d as a secret key (let $d=3541$). Now we will compute the time it takes to encrypt and decrypt M .

Messages	$M=(8228,5025)$		$M=(8219,7676)$		$M=(7570,7470)$	
Times Cryptosystems	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds
ElGamal ECC	0.292592	0.176354	0.290878	0.170969	0.283419	0.203476
MVECC	0.276297	0.203651	0.291875	0.178164	0.269145	0.15916
Variant of ElGamal Elliptic Curve Cryptosystem	0.276215	0.18720	0.287232	0.170789	0.298354	0.205623
Development 1 of MVECC	0.278417	0.159984	0.273756	0.156647	0.252891	0.163366
Development 2 of MVECC	0.275221	0.162163	0.277906	0.157675	0.256112	0.211674
Development 3 of MVECC	0.257683	0.200873	0.273627	0.222853	0.284028	0.1973921
PA_1	0.194398	0.198476	0.184653	0.118473	0.218362	0.1234291
PA_2	0.158134	0.143794	0.135682	0.163982	0.153319	0.1855610

Example

Suppose that we have E be an elliptic curve define over F_{11317} with parameters $a = 9817$ and $b = 47$ where $\left(4a^3 + 27b^2\right) \bmod 11317 \equiv 7090 \neq 0$. And $\# E = 11489$, with base point $B = (11117, 3663)$. If Ali wishes to send the message M to Benin using different elliptic curves cryptosystems he will choose a random integer e as a secret key (let $e = 6693$) and Benin will choose a random integer d as a secret key (let $d = 7391$). Now we will compute the time it takes to encrypt and decrypt M.

Messages	$M = (10498,1304)$		$M = (10502\ ,2413)$		$M = (11312,8637)$	
Times Cryptosystems	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds
ElGamal ECC	0.303633	0.200691	0.288211	0.193807	0.284580	0.201079
MVECC	0.303031	0.203651	0.264538	0.191914	0.295950	0.196345
Variant of ElGamal Elliptic Curve Cryptosystem	0.292426	0.199810	0.287838	0.192543	0.292264	0.202633
Development 1 of MVECC	0.305693	0.205576	0.284990	0.185032	0.271444	0.202973
Development 2 of MVECC	0.299248	0.1936698	0.266064	0.189023	0.293386	0.200534
Development 3 of MVECC	0.302547	0.211924	0.287557	0.210300	0.291263	0.192026
PA_1	0.196150	0.114944	0.199117	0.119267	0.204562	0.124658
PA_2	0.162633	0.195674	0.141658	0.171439	0.160308	0.188047

Example

Suppose that we have E be an elliptic curve define over F_{105557} with parameters $a = 1111$ and $b = 2224$ where $\left(4a^3 + 27b^2\right) \bmod 105557 \equiv 10021 \neq 0$ and $\# E = 105143$, with base point $B = (105280, 12229)$. If Ali wishes to send the message M to Benin using different elliptic curves cryptosystems he will choose a random integer e as a secret key (let $e = 66612$) and Benin will choose a random integer d as a secret key (let $d = 85611$). Now we will compute the time it takes to encrypt and decrypt M .

Messages	$M = (105551, 81862)$		$M = (72235, 49583)$		$M = (105272, 97099)$	
Times Cryptosystems	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds	Encryption Time/ seconds	Decryption Time/ seconds
ElGamal ECC	0.304600	0.223485	0.315133	0.207181	0.399384	0.289173
MVECC	0.307071	0.213422	0.264538	0.215553	0.338914	0.299122
Variant of ElGamal Elliptic Curve Cryptosystem	0.300871	0.227340	0.288938	0.199833	0.299892	0.248201
Development 1 of MVECC	0.305693	0.205576	0.229170	0.195232	0.279134	0.281244
Development 2 of MVECC	0.299248	0.1936698	0.272649	0.188261	0.294489	0.293852
Development 3 of MVECC	0.302547	0.211924	0.293721	0.247238	0.299913	0.199912
PA_1	0.196150	0.114944	0.199872	0.119473	0.222349	0.123821
PA_2	0.162633	0.195674	0.199821	0.192371	0.163326	0.192741

8. CONCLUSION

ElGamal cryptosystem is dependent on the additive operation on elliptic curve group. If the sender wants to send any message to the receiver, the sender must use the public key of receiver (as the other public key cryptosystem), and in way, it can change it with the same complexity as in proposition 4, because the addition and subtraction have the same computational complexity. However, the MVECC is a very important public key cryptosystem because of the following:

- It does not depend on additive operation on elliptic curve group.
- The message need not be a point on elliptic curve.

Therefore Al-Saffar (2005) has used this to develop the encryption and decryption scheme with more complexity than the original scheme. The two have different methods to encrypt and decrypt the message. We have discussed all of these propositions and compared them with the original schemes (ElGamal and MVECC) according to the complexity and the time which they took to implement each scheme.

REFERENCES

Al-Saffar, Najlae Falah Hameed (2005). *Proposed Developments of Elliptic Curves Cryptosystem*. Master's thesis, University of Babylon.

Hankerson, D. and Menezes, A. (2003). *Elliptic Curve Cryptography*. University of Waterloo.

Koblitz, N. (1987). Elliptic curve cryptosystems, *Mathematics of Computation*. **48**: 203-209.

Meng, T.K. (2001). *Curves for the Elliptic Curve Cryptosystem*. M.S.C. Thesis, University of Singapore.

Miller, V. (1986). Use of elliptic curves in cryptography. Advances in cryptology - CRYPTO 85, Springer. *Lecture Notes in Computer Science.* **218**: 417-426.

Saeki, M. K. (1997). *Elliptic Curve Cryptosystems*, M.S.C. Thesis, McGill University, Montreal.

Sagheer, A. M. (2004). *Enhancement of Elliptic Curves Cryptography Methods,* M.S.C. Thesis, University of Technology, Baghdad.

Pietiläinen, H. (2000). *Elliptic Curve Cryptography on smart cards,* M.S.C. Thesis, University of Technology.