AL-Qadisiya Journal For Science Vol .15 No.3 Year2010

Proposed Developments of

Sattar B. Sadkhan
Sciences College, Babylon University, Iraq
Najlae Falah
Elliptic Curves Cryptosystem Hameed
Department of Mathematics, College of mathematics and Computer Science, Kufa University

2010

Abstract

The group of the elliptic curve points forms an abelian group, which considered as a suitable choice for constructing a problem similar to the Discrete Logarithm Problem (DLP). This creates and open a new door for treatments the special group and new operations.

In this paper, we discuss some propositions to varying ElGamal scheme on Elliptic Curves and to development Menezes-Vanstone (MV) Elliptic Curves Cryptosystem.

1-Introduction

Elliptic Curves as algebraic (geometric) entities have been studied extensively for the 150 years, and from these studies has emerged a rich and deep theories [1]. Elliptic Curve systems as applied to cryptography were first proposed in 1985 independently by ***Neal Koblitz*** from the University of Washington, and ***Victor Miller***, who was then at IBM, Yorktown Heights [2], [3].

This paper at first describes in brief review of ***ElGamal*** and ***Menezes-Vanstone*** (***MV***) Elliptic Curve Cryptosystem and at second, discuss some Propositions to varying ElGamal scheme on Elliptic Curves and to development MV Elliptic Curves Cryptosystem.

2-ElGamal Public Cryptosystem [6]

To establish a private/public key pair, Ali[1] chooses a large prime p and a generator g of Z_{p^*}.[2] He then selects a random a, $1 \le a \le p-2$ and computes $\beta = g^a \bmod p$.

Ali publishes his public key (p, g, β), and keeps his private key a (as a secret key).

When Benin wishes to send a message $m \in Z_p$ to Ali she chooses a random k, $1 \le k \le p-2$, and computes and sends this value (γ, δ) to Ali where

$$(\underbrace{g^k \bmod p}_{\gamma}, \underbrace{m \cdot \beta^k \bmod p}_{\delta}).$$

When Ali receives Benin's message, he computes:

$$\gamma^{p-1-a} \cdot \delta \bmod p = (g^k)^{p-1-a} \cdot m \cdot \beta^k \bmod p$$

[1] Ali and Banin are two users.

[2] $Z_{p^*} = \{a^i : 0 \le i \le p-1\}$, where a is primitive element (whose order $p-1$), and p is an odd prime.

$$= (g^k)^{p-1-a} \cdot m \cdot (g^a)^k \bmod p$$
$$= m \cdot (g^k)^{p-1-a} \cdot (g^k)^a \bmod p$$
$$= m \cdot (g^k)^{p-1} \bmod p$$
$$= m \cdot 1 \bmod p$$
$$= m.$$

Example: Let $p = 7$ and $g = 3$. Suppose that Ali chooses ($a = 4$ as private), so that his $\beta = 4$.

In order to send Ali $m = 5$, Benin draws a random number k, say 2, and sends to Ali the following value:

$$(g^k \bmod p, m \cdot \beta^k \bmod p) = (3^2 \bmod 7, 5 \cdot 4^2 \bmod 7) = (2,3).$$

Ali then computes the following value:

$$\gamma^{p-1-a} \cdot \delta \bmod p = (3^2 \cdot 2) \bmod 7 = 5 = m.$$

3-ElGamal Elliptic Curve Cryptosystem

This system is very simple for two commutations (sender and receiver) in cryptography operation, since there is one sender operation and one receiver operation. Now let us illustrate this system.

Let $E(F)$ be an Elliptic Curve group and let B be a point on E. The user Benin first selects a private key d and generate a public key $Q = dB$.

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 : $C_m = \{C, eB\}$

Where $C = P_m + eQ$

To decrypt the ciphertext, Benin computes the following:

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

4- Proposition to Variant ElGamal Elliptic Curve Cryptosystem

To vary the encryption and decryption of ElGamal Elliptic Curve Cryptosystem. 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 likes 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:

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

Example:

Let Elliptic Curve E defined over F_p ($p = 72169$ with parameters $a = 71669, b = 71470$ where $(4a^3 + 27b^2) \bmod p = 44301 \neq 0$). Suppose the private

key of Benin is $d = 6243$, and the private key of Ali is $e = 4781$. and let $B = (71825,71861)$ be a base point on E, if $M = (72116,71495)$ is the message point, discuss what Ali and Benin should do if Ail want to send M to Benin.

Solution:

Since $d = 6243$ thus the public key of Benin is

$Q = 6243(71825,71861) = (38216,4751)$, If Ali wishes to a message to Benin he should do the following:

- Compute $eQ = 4781(38216,4751) = (59583,55703)$
- Compute $eB = 4781(71825,71861) = (56130,21458)$
- Compute C :

$$C = M - eQ = (72116,71495) - (59583,55703)$$
$$= (72116,71495) + (59583,-55703)$$
$$= (925,59468)$$

Then Ali send $C_M = \{C, eB\}$

$= \{(925,59468),(56130,21458)\}$ to Benin.

To decrypt the ciphertext, Benin does the following:

- Compute $d(eB) = 6243(56130,21458)$

$= (59583,55703)$

- Compute M :

$$M = C + d(eB)$$
$$= (925,59468) + (59583,55703)$$
$$= (72116,71495)$$
$$= M.$$

5- Menezes–Vanstone Elliptic Curve Cryptosystem(MVECC)

This is cryptosystem that has no analogue for DLP (i.e. this cryptosystem dose not depend on DLP as the above cryptosystems).

In this variation (*MVECC*), the EC 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) [4], [5]. Now let us take the following algorithm to illustrate this system.

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 EC $E(F_p)$ and a base point B.
- Benin first selects a private key d and generates a public key $Q = d\,B$.
- 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 where $c_1 = m_1 * k_1 \bmod p$,

  $c_2 = m_2 * k_2 \bmod p$.

  $eQ = (k_1,k_2)$
- Benin likes to decrypt the ciphertext, she computes the following:

  $(k_1,k_2) = d\,(eB)$, and then

  $m_1 = c_1 * k_1^{-1} \bmod p$

$m_2 = c_2 * k_2^{-1} \bmod p.$

6- Proposition to Development of MVECC

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

(6 .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 $C = (c_1, c_2)$

$$(k_1, k_2) = eQ$$

$$c_1 = (m_1 + k_1 k_2) \bmod p$$

$$c_2 = m_1 (m_2 + k_2 k_1) \bmod p$$

To decrypt the ciphertext Benin computes:

$$(k_1, k_2) = d (e B)$$

$$m_1 = (c_1 - k_1 k_2) \bmod p$$

$$m_2 = (m_1^{-1} c_2 - k_1 k_2) \bmod p$$

Proof:

$$(c_1 - k_1 k_2) \bmod p = (m_1 + k_1 k_2 - k_1 k_2) \bmod p$$

$$= m_1 .$$

$$(m_1^{-1} c_2 - k_1 k_2) \bmod p = (m_1^{-1} m_1 (m_2 + k_2 k_1) - k_1 k_2) \bmod p$$

$$= m_2 .$$

(6.2) 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 $C = (c_1, c_2)$

$$(k_1, k_2) = e Q$$

$$c_1 = (m_1 * (k_1 k_2 - k_1)) \bmod p$$

$$c_2 = (m_2 * (k_1 k_2 - k_2)) \bmod p$$

To decrypt the ciphertext Benin computes:

$$(k_1, k_2) = d (e B)$$

$$m_1 = (c_1 * (k_1 k_2 - k_1)^{-1}) \bmod p$$

$$m_2 = (c_2 * (k_1 k_2 - k_2)^{-1}) \bmod p$$

Proof:

$$(c_1 * (k_1 k_2 - k_1)^{-1}) \bmod p = (m_1 * (k_1 k_2 - k_1) * (k_1 k_2 - k_1)^{-1}) \bmod p$$

$$= m_1 .$$

$$(c_2 * (k_1 k_2 - k_2)^{-1}) \bmod p = (m_2 * (k_1 k_2 - k_2) * (k_1 k_2 - k_2)^{-1}) \bmod p$$

$$= m_2 .$$

(6.3) 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 $C = (c_1, c_2)$

$$(k_1, k_2) = e q$$

$$c_1 = m_1 + (k_1 k_2^{k_1})^{-1} \bmod p$$

$c_2 = m_2 + (k_2\, k_1^{k2})^{-1} \mod p$

To decrypt the ciphertext Benin computes:

$(k_1, k_2) = d\,(e\,B)$

$m_1 = (c_1 - (k_1\, k_2^{k_1})^{-1}) \mod p$

$m_2 = (c_2 - (k_2\, k_1^{k_2})^{-1}) \mod p$

Proof:

$(c_1 - (k_1\, k_2^{k_1})^{-1}) \mod p = (m_1 + (k_1\, k_2^{k_1})^{-1} - (k_1\, k_2^{k_1})^{-1}) \mod p$

$= m_1 .$

$(c_2 - (k_2\, k_1^{k_2})^{-1}) \mod p = (m_2 + (k_2\, k_1^{k_2})^{-1} - (k_2\, k_1^{k_2})^{-1}) \mod p$

$= m_2 .$

Example:

Let EC E defined over F_p ($p = 105557$ with parameters $a = 1111, b = 2224$ where $(4a^3+27\,b^2) \mod p = 10021 \neq 0$.

Suppose the private key of Benin is $d = 85611$, then the public key of Benin is $Q = d\,B$ ($B = (105280, 12229)$ is a base point on E)

$\therefore Q = 85611\,(105280, 12229)$

$= (67153,10117)$

and the private key of Ali is $e = 66612$.

Solution:

- Using **(6.1)** method : If Ali wishes to send a message $M = (72235, 49583) = (m_1, m_2)$ to Benin, then he should do the following:

–Compute $e\,Q = 66612\,(67153,10117)$

$= (53134, 60702)$

$= (k_1, k_2)$

–Compute $e\,B = 66612\,(105280, 12229)$

$= (86328,15185)$

–Compute C:

$C = (c_1, c_2)$

$c_1 = (m_1 + k_1\, k_2) \mod p$

$= (72235 + 53134 * 60702) \mod 105557$

$= 12611$

$c_2 = m_1\,(m_2 + k_2\, k_1) \mod p$

$= 72235\,(49583 + 53134 * 60702) \mod 105557$

$= 76069$

Then Ali sends $C_M = \{C, e\,B\}$

$= \{(12611, 76069) , (86328,15185)\}$ to Benin.

To decrypt the ciphertext , Benin should do the following:

–Compute $d\,(e\,B) = 85611\,(86328,15185)$

$= (53134, 60702)$

$= (k_1, k_2)$

–Compute M:

$M = (m_1, m_2)$

$m_1 = c_1 - k_1\, k_2 \mod p$

$= (12611 - 53134 * 60702) \mod 105557$

$= 72235$

$= m_1$

$m_2 = (m_1^{-1} c_2 - k_1 k_2) \bmod p$

$m_1^{-1} = (72235)^{-1} \bmod 105557$

$= 11781$

then $m_2 = (11781 * 76069 - 53134 * 60702) \bmod 105557$

$= 49583$

$= m_2$

- Using ***(6.2)*** method : If Ali wishes to send a message $M = (72235, 49583) = (m_1, m_2)$ to Benin, then he should do the following:

–Compute $e\ Q = 66612\ (67153,10117)$

$= (53134, 60702)$

$= (k_1, k_2)$

–Compute $e\ B = 66612\ (105280, 12229)$

$= (86328,15185)$

–Compute C:

$C = (c_1, c_2)$

$c_1 = (m_1 * (k_1 k_2 - k_1)) \bmod p$

$= (72235 * (53134 * 60702 - 53134)) \bmod 105557$

$= 20661$

$c_2 = (m_2 * (k_1 k_2 - k_2)) \bmod p$

$= (49583 * (53134 * 60702 - 60702)) \bmod 105557$

$= 63139$

Then Ali sends $C_M = \{C, e\ B\}$

$= \{(20661, 63139), (86328,15185)\}$ to Benin.

To decrypt the ciphertext, Benin should do the following:

–Compute $d\ (e\ B) = 85611\ (86328,15185)$

$= (53134, 60702)$

$= (k_1, k_2)$

–Compute M:

$M = (m_1, m_2)$

$(k_1 k_2 - k_1)^{-1} \bmod p = (53134 * 60702 - 53134)^{-1} \bmod 105557$

$= 98356^{-1} \bmod 105557$

$= 90913$

$m_1 = (c_1 *(k_1 k_2 - k_1)^{-1}) \bmod p$

$= 20661 * 90913 \bmod 105557$

$= 72235$

$= m_1$.

$(k_1 k_2 - k_2)^{-1} \bmod p = (53134 * 60702 - 60702)^{-1} \bmod 105557$

$= 90788^{-1} \bmod 105557$

$= 55012$

$m_2 = (c_2 * (k_1 k_2 - k_2)^{-1}) \bmod p$

$= 63139 * 55012 \bmod 105557$

$= 49583$

$= m_2$.

•Using ***(6.3)*** method : If Ali wishes to send a message $M = (72235, 49583) = (m_1, m_2)$ to Benin, then he should do the following:

–Compute $e\ Q = 66612\ (67153,10117)$
$= (53134, 60702)$
$= (k_1, k_2)$

–Compute $e\ B = 66612\ (105280, 12229)$
$= (86328,15185)$

–Compute C:

$C = (c_1, c_2)$

$c_1 = (m_1 + (k_1 k_2^{k_1})^{-1}) \bmod p$

$= (72235 + (53134 * 60702^{53134})^{-1}) \bmod 105557$

$= (72235 + (31223)^{-1}) \bmod 105557$

$= (72235 + 22509) \bmod 105557$

$= 94744$

$c_2 = (m_2 + (k_2 k_1{}^{k_2})^{-1} \bmod p$

$= (49583 + (53134 * 60702^{60702})^{-1}) \bmod 105557$

$= (49583 + (51389)^{-1}) \bmod 105557$

$= (49583 + 18764) \bmod 105557$

$= 68347$

Then Ali sends $C_m = \{C, e\ B\}$
$= \{(94744, 68347), (86328,15185)\}$ to Benin.

To decrypt the ciphertext, Benin should do the following:

–Compute $d\ (e\ B) = 85611\ (86328,15185)$
$= (53134, 60702)$
$= (k_1,k_2)$

–Compute M:

$M = (m_1, m_2)$

$m_1 = (c_1 - (k_1 k_2{}^{k_1})^{-1}) \bmod p$
$= (94744 - 22509) \bmod 105557$
$= 72235$
$= m_1$

$m_2 = (c_2 - (k_2 k_1{}^{k_2})^{-1}) \bmod p$
$= (68347 - 18764) \bmod 105557$
$= 49583$
$= m_2$.

7- Conclusion:

ElGamal cryptosystem is dependent on the additive operation on elliptic curve group. If the sender went 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 cannot be development, but we can change it with same complexity as in proposition ***4***, because the additive and subtraction have the same computation complexity.

However, in the MVECC which is a very important system of a public key cryptosystem because the following:

- It is not depend on additive operation on elliptic curve group.
- The message needs not to be a point on elliptic curve.

Therefore we can use this to development the encryption and decryption scheme more complexity of the original scheme

8- References

[1] Evans, P.D. (2001), "Timing attack on Elliptic Curve Cryptography", University of Virginia.
[2] Hankerson, D. and Menezes, A. (2003), "Elliptic Curve Cryptography", University of Waterloo.
[3] Lenore Zuck "Lecture 6" Computer Security March 5, 2001.
[4] Pietiläinen, H. (2000), "Elliptic Curve Cryptography on smart cards", M.S.C. Thesis, University of Technology.
[5] Saeki, M.K. (1997),"Elliptic Curve Cryptosystems", M.S.C. Thesis, McGill University, Montreal.
[6] Wiener, M.J. and Zuccherato, R. J. (1998),"Faster Attacks on Elliptic Curve Cryptosystems", Entrust Technologies, Canada.

التطويرات المقترحة لأنظمة التشفير
باستخدام
المنحنيات الاهليلجية

ستار بدر سدخان
كلية العلوم/ جامعة بابل/ العراق
نجلاء فلاح حميد
قسم الرياضيات/ كلية الرياضيات وعلوم الحاسبات/ جامعة الكوفة/ العراق

المستخلص

تُشكّلُ مجموعةُ نقاطِ المنحنى الإهليليجيةِ زمرة ابدالية، التي إعتبرتْ إختيار مناسب لبِناء مشكلة مشابهة لمشكلةِ اللوغاريتمِ المنفصلةِ. هذا ينشأ ويفتح باب جديد لمعالجةِ زمراً خاصّة وعمليات الجديدة.

في هذه البحث، نُناقشُ بَعْض المقترحاتِ لتغيير الخطط الخاصة بنظام تشفير الكمال بإستخدام المنحنيات الإهليليجيةِ، وإلى تطويرِ نظام تشفيرمينيزيس فانستون بأستخدام المنحنيات الاهليليجية.