International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 09 Issue 10 ǁ 2021 ǁ PP. 68-72

Building a signature of the identifier cryptosystem based on the Elliptic curve

Dao Thi Phuong Anh
Faculty of Information Technology, Hanoi University of Natural Resources & Environment, Hanoi, Vietnam

Abstract
The current identity system is being considered as a new cryptographic system with many advantages compared to other cryptosystems. A widely used and public-key identity system that allows a user to compute a public key from any string. This string, as an identifier representation and used to compute the public key, may contain information about the validity of the key to prevent a user from using a key for a long time or to allow another user to use the key. compute the public key from any string. This paper proposes encryption and decryption using an identity system based on Elliptic curves.

Keywords: *Identification System, Encryption and Decryption, Elliptic curve, Discrete Logarithms, Known Message Attacks.*

Date of Submission: 18-10-2021 Date of acceptance: 02-11-2021

I. INTRODUCTION

Elliptic Curve Cryptography (ECC) is a public key code based on algebra structure of Elliptic Curve on limited field. The safety of ECC based Elliptic Curve Cryptography Algorythm Problem (ECDLP). Noway, with ECDLP till now there is still unable to find out sub-exponential algorithm to solve.

Elliptic Curve has security equivalent uith every traditional cipher system, while it is shorter than much more. For example: 3248 bit of RSA is equal with 256 ECC. So ECC use less system resource, consume less energy… With shorter length, ECC is now use in many fields.

Elliptice Curve is a collection of sastify point for a math equation. Equation for a elliptic curve:

y^2=x^3+ax+b (1)

It's like this:

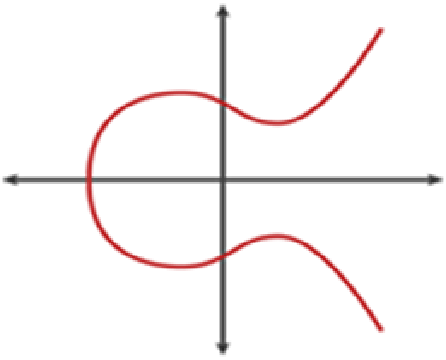

Figure 1: Performance graph of Elliptic Curve: y^2=x^3+ax+b

The identity system is first showed by Shamir in 1984 [1], the main advantage of it is don't need to authenticate public key, this key is derivated from ID, email or user's identity card number. There are many digital signature scheme based on identity system [1] or [2], [3]. These documents recommend encode and decode using identity system based on Elliptic curve.

II. MATH BASE

2.1. Elliptic Curve on limited field

2.1.1. Limited field Fq with q is a prime number

Elliptic curve on F_q field (p is a prime number). p is a prime number(p>3), $a, b \in F_p$ with $4a^3 + 27b^2 \neq 0$ in F_p field.

An elliptic curve E on F_q (is defined by a and b) is a collection of pair of values (x,y) $(x, y \in \mathbb{F}_q)$ sastified with:

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

With O is a special point called infinity point and can be perform as:

$$O = (x, \infty).$$

The number of point of $E(\mathbb{F}_q)$ (is $\neq E(\mathbb{F}_q)$ sastify Hasse theorem.

The complex of building on Elliptic curve algorythm based on number of points on that curve.

The degree of point: With P(x,y) belong to Elliptic curve. The degree of P(x,y) is a integer sastified:

$$nP = O \tag{3}$$

2.1.2. Elliptic curve on $\mathbb{F}_2^m$

An elliptic curve $E(\mathbb{F}_{2^m})$ is defined by $a, b \in \mathbb{F}_{2^m}$ (with $b \neq 0$) is a collection of P(x,y) with $x, y \in \mathbb{F}_{2^m}$ sastify with:

$$y^2 + xy = x^3 + ax^2 + b \tag{4}$$

With O is point at infinity.

The number of point belong to $E(m\,\mathbb{F}_2)$ symbol is $\neq E(m\,\mathbb{F}_2)$ sastify with Hasse:

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q} \text{ trong đó } p = 2^m \tag{5}$$

Beside, $E(\mathbb{F}_{2^m})$ is an even number

The collection of point on $E(\mathbb{F}_{2^m})$ create a group that sastify with these natures:

$$O + O = O \tag{6}$$

$$`(x, y) + O = (x, y), \forall (x, y) \in E(\mathbb{F}_{2^m}) \tag{7}$$

$$(x, y) + (x, -y) = O, \forall (x, y) \in E(\mathbb{F}_{2^m}) \tag{8}$$

Then, $(x, -y)$ is a opposite point of (x, y) on $E(\mathbb{F}_{2^m})$.

III. RECOMMENDED SCHEMA

3.1. Encoded and decoded schema

3.1.1. Number generator

G_1 is a cyclic plus group with degree is a prime number q and birth element is P. G_T is a cyclic multiply group has same degree q. e is a bijection:

$$e: G_1 \times G_1 \rightarrow G_T$$

k is a secret key, sastify with condition p is a prime number.

$$p | \#\, E(\mathbb{F}_q)$$

$$p^2 \chi \neq E(\mathbb{F}_q) \tag{9}$$

With: $p \in G_1$ và $G_T \in \mathbb{F}^*_{q^k}$

Select 1 random point on Elliptic curve

$$P \in E(\mathbb{F}_q)[p] \ ;$$

$$G_1 = \langle P \rangle$$

$$G_T = \langle e(P, P) \rangle \tag{10}$$

Select random number sastify with:

$s \in \mathbb{Z}_p^*$ (to calculate sP)

Mapping ID to a point Q_{ID}, here we use hash function.

H_1, H_2 are hash functions used for security and defined as: $H_1 : \{0,1\}^* \rightarrow G_1;\ H_2 : G_T \rightarrow \{0,1\}^n$

Declare system parameter is:

$$\text{Params} = (n, e, q, G_1, G_T, H_1, H_2, sP) \tag{11}$$

3.1.2. Encode

1. $Q_{ID} = H_1(ID)$
2. Calculate private key by getting $Q_{ID} \times s$ we have: sQ_{ID}
3. Create a integer that sastify:

$r \in \mathbb{Z}_p^*$ và tính rP

4. Calculate K we have $Q_{ID} = H_1(ID)$

So: $K = H_2(e(rQ_{ID}, sP))$

Use code correspond with C we have:

$$C = (C_1, C_2)$$

With: $C_1 = rP\ ;\ C_2 = M \oplus K$

3.1.3 Decode

When receive code:
$C = (rP, M \oplus H_2(e(rQ_{ID}\,,\ sP)) = (C_1, C_2)$
Execute the following steps:

1. Calculate
   $K = H_2(e(sQ_{ID}, C_1))$ from code component C_1 and private key sQ_{ID} (12)
2. Calculate $M = C_2 \oplus K$
3. We change C_1 and calculate K we have:

$$K = H_2\big(e(rQ_{ID}, sP)\big) = H_2\big(e(Q_{ID}, sP)\big)^{rs}$$
$$= H_2\big(e(rQ_{ID}, C_1)\big) = H_2(e(Q_{ID}, P))^{rs} \quad (13)$$

3.2. Prove the exactness of recommend schema

3.2.1. Prove that there is always a point p on the Elliptic curve

Assume E is Elliptic curve $E(\mathbb{F}_q)$ [4], with:

$$y^2 = x^3 + 1 \quad (14)$$

q is a prime number: $q \equiv 11(\text{mod } 12)$ và G_1 is a small group of $p \in E(\mathbb{F}_q)$.
we use hash function:

$$H_1 : \{0,1\}^* \rightarrow G_1$$

Use $Q \in E(\mathbb{F}_q)$ and get coordinate x, y on Elliptic curve sastify:

$$x = (y^2 - 1)^{1/3}$$

Adopt theorem Euler [4] we have:

$$a^{q-1} \equiv 1 \ (\text{mod } q)$$
$$a^{2q-1} \equiv a \ (\text{mod } q)$$
$$a^{(2q-1)/3} \equiv a^{1/3} \ (\text{mod } q) \quad (15)$$

We have: $3|(2q-1)$khi $q \equiv 11(\text{mod } 12)$
Then calculate coordinate x of Q point:

$$Q_{ID} \in E\big(\mathbb{F}_q\big)[p]$$

Then we multiply with 1 constant we have:

$$Q_{ID} = \frac{\neq E\big(\mathbb{F}_q\big)}{p}.Q$$
$$Q_{ID} = \frac{q+1}{p}.Q$$

Because:

$$p|\# E(\mathbb{F}_q)$$
$$p^2\,\chi \neq E(\mathbb{F}_q)$$

So always have:

$$p \in E(\mathbb{F}_q) \quad (16)$$

While:

$$Q_{ID} \in G_1 \quad (17)$$

3.2.2 Example

Assume E is a Elliptic curve: $E/(\mathbb{F}_{131})$ with:

$$y^2 = x^3 + 1$$

And:

$$P = (98{,}58) \in E(\mathbb{F}_{131}) \ [11]$$
$$G_1 = \langle P \rangle$$
$$G_T = \langle e(P, P) \rangle \quad (18)$$

Call G_1 is a cyclic plus group with degree is prime number q and birth element is P. G_T is a cyclic multiply group with same degree q. e is a bijective:

$$e: G_1 \times G_1 \rightarrow G_T = e(P, \emptyset Q)^{1560} \quad (19)$$

While $\emptyset\,(x, y) = (\xi x, y)$ với $\xi = 65 + 112i$

Choose: $s = 7; sP = (33,100)$

$$Q_{ID} = H_2(ID_B) = (128,57)$$
$$sQ_{ID} = (113,8)$$

Encode with: $s = 7;$

$$rQ_{ID} = (5)(128,57) = (98,73)$$

And: $r = 5 \in \mathbb{Z}_{11}^*$
So: $rP = 5P = (34,23)$
Calculate:

$$K = H_2\big(e(rQ_{ID}, sP)\big) = H_2\big(e(98,73), (33,100)\big)$$
$$= H_2(49 + 58i)$$

But:

$$C_1 = rP;$$

So:

$$K = H_2\big(e(sQ_{ID}, C_1)\big) = H_2\big(e(113,8), (34,23)\big)$$
$$= H_2(49 + 58i)$$

Then: $C_2 = M \oplus K = (M \oplus K) \oplus K = M$

Recommended schema prevent type of attack collective multi-component digital signature:

A. Random Message Attacks [5]

Recommended schema is said is unable to fake with any polymonial $l(\cdot)$ and with any polymonial time algorythms of attacker $\boldsymbol{\mathcal{A}}$, success chance is a pitiful small function:

$$\epsilon_{\mathcal{A}}(k)$$
$$\stackrel{\text{def}}{=} Pr\begin{bmatrix} \{m_{i_m}\}_{i_m=1}^{l} \leftarrow M_k; \\ \{(PK_i, SK_i) \leftarrow \boldsymbol{Gen}(Params, 1^k)\}_{i=1}^{NSIG}; \\ PK_{pub} \leftarrow \{\boldsymbol{GenPub}\left(PK_i, \text{ע}_i\right)\}_{i=1}^{NSIG}; 1 \leftarrow \boldsymbol{VerifyPub}(PK_{pub}, m, \alpha_{pub}, \text{ע}) \\ \alpha_i \leftarrow \{\boldsymbol{Sign}^R(SK_i, m_{i_m}, \text{ע}_i)\}_{i=1}^{NSIG}; \wedge m \notin \{m_1 \dots m_l\} \\ \alpha_{pub_{i_m}} \leftarrow \{\boldsymbol{SignPub}^R(\alpha_i)\}_{i=1}^{NSIG}; \\ (m, \alpha_{pub}) \leftarrow \mathcal{A}(PK_{pub}, \{\left(m_{i_m}, \alpha_{pub_{i_m}}\right)\}_{i_m=1}^{l} \end{bmatrix}$$
$$\epsilon_{\mathcal{A}}(k) = negl(k) \qquad (20)$$

(1) String $l = l(k)$ text $m_1, \dots, m_l$ is randomly chosen in M_k
(2) Execute algorythm in schema to create signature $\alpha_{pub_{i_m}}$.
(3) Algorythm $\boldsymbol{\mathcal{A}}$ with input is PK_{pub}, $\{m_{i_m}, \alpha_{pub_{i_m}})\}$ and output is (m, α_{pub}).
(4) Execute attack success if:

$$1 \leftarrow \boldsymbol{VerifyPub}(PK_{pub}, m, \alpha_{pub}, \text{ע})\ and\ m \neq m_{i_m}.$$

B. Known Message Attacks [5]

Recommended schema is said is unable to fake with KMA and with any polymonial time algorythms of attacker $\boldsymbol{\mathcal{A}}$, success chance is a pitiful small function:

$$\epsilon_{\mathcal{A}}(k)$$
$$\stackrel{\text{def}}{=} Pr\begin{bmatrix} \{m_{i_m}\}_{i_m=1}^{l} \leftarrow \mathcal{A}(1^k); \\ \{(PK_i, SK_i) \leftarrow \boldsymbol{Gen}(Params, 1^k)\}_{i=1}^{NSIG}; \\ PK_{pub} \leftarrow \{\boldsymbol{GenPub}\left(PK_i, \text{ע}_i\right)\}_{i=1}^{NSIG}; 1 \leftarrow \boldsymbol{VerifyPub}(PK_{pub}, m, \alpha_{pub}, \text{ע}) \\ \alpha_i \leftarrow \{\boldsymbol{Sign}^R(SK_i, m_{i_m}, \text{ע}_i)\}_{i=1}^{NSIG}; \wedge m \notin \{m_1 \dots m_l\} \\ \alpha_{pub_{i_m}} \leftarrow \{\boldsymbol{SignPub}^R(\alpha_i)\}_{i=1}^{NSIG}; \\ (m, \alpha_{pub}) \leftarrow \mathcal{A}(PK_{pub}, \{\left(m_{i_m}, \alpha_{pub_{i_m}}\right)\}_{i_m=1}^{l} \end{bmatrix}$$
$$\epsilon_{\mathcal{A}}(k) = negl(k) \qquad (21)$$

(1) String $l = l(k)$ text $m_1, \dots, m_l$ is randomly choosen in M_k
(2) Execute algorythm in schema to create signature $\alpha_{pub_{i_m}}$.
(3) Algorythm $\boldsymbol{\mathcal{A}}$ with input is PK_{pub}, $\{m_{i_m}, \alpha_{pub_{i_m}})\}$ and output (m, α_{pub}).
(4) Execute attack success if:

$$1 \leftarrow \boldsymbol{VerifyPub}(PK_{pub}, m, \alpha_{pub}, \text{ע}) \text{ and } m \neq m_{i_m}.$$

C. Adaptive Chosen Message Attacks [6]

This is the strongest attack type, attackers can choose text to sign base on public key and digital signature before. We can perform this by access to Oracle function, symbol is $Sign(\cdot)_{sk}$.

Recommended schema is said is unable to fake with ACMA and with any time polymonial algorythms of attacker $\boldsymbol{\mathcal{A}}$, success chance is a pitiful small function:

$$\epsilon_{\mathcal{A}}(k)$$

$$\overset{\text{def}}{\equiv} Pr\left[\begin{array}{c} \{m_{i_m}\}_{i_m=1}^{l} \leftarrow M_k; \\ \{(PK_i, SK_i) \leftarrow \boldsymbol{Gen}(Params, 1^k)\}_{i=1}^{NSIG}; \\ PK_{pub} \leftarrow \{\boldsymbol{GenPub}\left(PK_i, \text{ע}_i\right)\}_{i=1}^{NSIG}; 1 \leftarrow \boldsymbol{VerifyPub}(PK_{pub}, m, \alpha_{pub}, \text{ע}) \\ \alpha_i \leftarrow \{\boldsymbol{Sign}^R\left(SK_i, m_{i_m}, \text{ע}_i\right)\}_{i=1}^{NSIG}; \wedge m \notin \{m_1 \dots m_l\} \\ \alpha_{pub_{i_m}} \leftarrow \{\boldsymbol{SignPub}^R(\alpha_i)\}_{i=1}^{NSIG}; \\ (m, \alpha_{pub}) \leftarrow \boldsymbol{\mathcal{A}}^{Sign(\cdot)_{sk}}(PK_{pub}) \end{array}\right]$$

$$\epsilon_{\mathcal{A}}(k) = negl(k) \qquad (22)$$

(1) String $l = l(k)$ text $m_1, \dots, m_l$ is randomly choosen in M_k

(2) Execute algorythm in schema to create signature $\alpha_{pub_{i_m}}$.

(3) Algorythm $\boldsymbol{\mathcal{A}}$ with input is PK_{pub} and can access to $Sign(\cdot)_{sk}$ with any text and have digital signature output (m, α_{pub}). This query text area is called M.

(4) Execute attack success if:

$$1 \leftarrow VerifyPub(PK_{pub}, m, \alpha_{pub}, \text{ע})\ v\text{à}\ m \neq M$$

Attack scrypt 1

To attack delegate collective digital signature, attackers must find trapdoor of one-way function of Logarithm on Elliptic curve, it means find out secret key of members.

When find out public key to find the secret key, attacker must handle Logarithm Elliptic curve and this is a hard math that can't be handle in polymonial time.

Attack scrypt 2

Attacker fake value h_3 in signature component, success chance is $1/_q$, if q enough large, this probality is pitiful small.

Attack scrypt 3

Attacker fake digital signature by fake all values $U_{pi} = x_i P$ và $\sigma_{p_i} = h_3 S_{pk_i} + x_i P_{pub}$ but to do it need to find value x_i and to find this value, attacker must keep logarithm discrete on Elliptic curve and this is unsolved math.

IV. CONCLUSION

In this article, the author has showed encode and decode using identity system base on Elliptic curve. Base on safety level of ECC on logarit discrete until now still unable to solve by algorythm exponential function. So safety level and this document the author used simple math, easy to setup, high calculate speed. Prove by math that exactness of recommended have base. But this document only just mention 1 point on Elliptic curve, can be expand to 2 point on Elliptic curve.

REFERENCES

[1]. A. Shamir, "Identity-based Cryptosystems and Signatures Schemes," Proc. of Crpto'84, (1984), pp. 48–53.

[2]. A. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme," Public-Key Cryptography – PKC 2003, pp. 31–46, 2002.

[3]. X. Li and K. Chen, "Multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings," Applied Mathematics and Computation, vol 169, no. 1, pp. 437–450, 2005.

[4]. R. A. Sahu and S. Padhye, "Multi-Proxy Multi-Signature Scheme," Int'l Conf. on Computer & Communication Technology, pp. 60–63, 2010.

[5]. R. A. Sahu and S. Padhye, "Identity-based multi-proxy multi-signature scheme provably secure in random oracle model," European Transactions on Telecommunications, vol. 25, no. 3, pp. 294–307, 2014.

[6]. R. Dutta, R. Barua, P. Sarkar, and B. T. Road, "Pairing-Based Cryptographic Protocols: A Survey Introduction Preliminaries Key Agreement Schemes Conclusion," IACR Eprint archive, 2004