P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2008,(2), (1) :106-115

ELLIPTIC CURVES PUBLIC KEY TRAITOR TRACING SCHEME

Ali M. Sagheer

College of Computer, University of Al-Anbar, Iraq

ARTICLE INFO

Received: 1 / 4 /2008
Accepted: 24 / 4 /2008
Available online: 30/4/2008
DOI: 10.37652/juaps.2008.15446

Keywords:
Traitor Tracing Scheme,
Elliptic Curves Cryptography,
DDH,
ECDDH.

ABSTRACT

In this paper we use the elliptic curves system in the Public Key Traitor Tracing Scheme. The Elliptic Curve points form Abelian group that used in the Public Key Traitor Tracing Scheme. The main advantage of elliptic curves systems is thus their high cryptographic strength relative to the size of the key. We design and implement an elliptic curves public key encryption scheme, in which there is one public encryption key, but many private decryption keys which are distribute through a broadcast channel, the security of the elliptic curves public key encryption scheme based on the Elliptic Curves Decisional Diffie Hellman(ECDDH) problem that is analogous to Decisional Diffie Hellman(DDH) problem, but it is more intractable than DDH problem.

Introduction

The secure distribution of a digital content stream to an exclusive set of subscribers is an important problem that has many applications in the entertainment industry. The typical setting is that of Pay-TV: the content distributor transmits scrambled streams of video of the channel line-up that are received by the subscribers using a decoder device (e.g. a cable-box).

The digital content should be encrypted in such a way so that eavesdroppers are incapable of intercepting the stream. On the other hand, each legitimate subscriber possesses a decryption mechanism (essentially: a cryptographic decryption key) that enables him/her to receive the content.

One major problem faced by administrators of such systems is "piracy": the illegal reception of the scrambled content that is made possible by taking advantage of "insider information." Current encryption mechanisms are strong enough to ensure that an eavesdropper is incapable of inverting the scrambling method used in the broadcast to the legitimate subscribers. However, illegal reception of the digital content can still occur if some of the legitimate users of the system leak (some of) their key information to a third party. Such users are called traitors and a third party that uses subscriber-key information for illegal data reception is called a pirate.

Traitor Tracing Schemes

Consider an application which provides data that should be available to authorized users only. The number

* Corresponding author at: College of Computer, University of Al-Anbar, Iraq, Iraq.E-mail address: ali_makki_sagheer@yahoo.com

of authorized users is big enough so that broadcasting the data is much more efficient than establishing a secure channel between the data provider and each authorized user. The data could obviously be protected from unauthorized access by encryption. And the data supplier could provide the decryption keys to the authorized users only, and broadcast the encrypted ciphertext.

However this does not prevent one or more authorized users from retransmitting the plaintext they have obtained by decrypting the received ciphertext, or simply disclosing their personal keys to some unauthorized users. In this event, unauthorized users have access to data that they are not entitled to. We call this unauthorized access piracy. The traitors are the groups of authorized users who allow unauthorized users to obtain the data, either by retransmitting the plaintext, or disclosing their personal decryption keys. The unauthorized users who obtained the data are called pirate users.

Traitor tracing schemes or traceability schemes are cryptographic techniques preventing traitors from distributing their personal keys to enable pirates decrypting the data. In such a scheme, each authorized user is given a decoder which contains the user's personal decryption key.

A symmetric encryption algorithm (such as DES) is used to encrypt the data using a randomly generated session key. The data distributer encrypts the session key in a way such that only an authorized user's decoder is able to decrypt the session key and hence recover the data. Suppose a group of traitors contribute their personal keys to build a pirate decoder which can also decrypt the ciphertext. The scheme should discover the keys in the pirate decoder and determine one or more traitors who have helped build the pirate decoder by contributing their personal keys. The scheme which can trace the traitor if there is only one traitor [6].

An alternative approach to piracy prevention in digital content distribution systems was proposed by Chor, Fiat and Naor under the framework of Traitor Tracing Schemes (TTS) [3] also [4]. In a TTS, each subscriber has a decryption key that is associated with his identity (it can be thought of as a fingerprinted decryption key).

Malicious subscribers (traitors) might again try to leak their personal key information to a pirate. However, in a traitor-tracing scheme the distributors (or the authorities) possess a “traitor tracing” procedure that, given the pirate decoder, is capable of recovering the identities of at least one of the traitors. Even though the existence of such a mechanism cannot eliminate piracy, it can effectively deter users from leaking their personalized keys to a pirate.

Public Key Traitor Tracing scheme had been introduced by Boneh and Franklin [1] in 1999. It is a public key broadcast encryption scheme and a k-collusion resistant traitor tracing scheme. The construction of the keys is algebraic and tracing is deterministic. The scheme gains full tracing, that is, if at most k traitors have participated in generating a new key, they can all be traced. Moreover, the tracing algorithm is error free. Innocent users are never blamed (assuming the coalition of traitors has had at most k members).

Elliptic Curves

Elliptic curves are curves having a specific base point, these are given by explicit polynomial equations called “ Weierstrass equations” [9]. Using these explicit

equations, we show that the set of points of an elliptic curve forms an Abelian group[10].

For fields of various characteristics, the Weierstrass equation can be transformed (and simplified) into different forms by a linear change of variables. We get easier equation for prime field of characteristic $\neq 2,3$ and binary field [5,7,8,9].

Definition: An elliptic curve E over the finite field Fp is defined by an equation of the form[8]:

$y^2 = x^3 + ax + b$……(1)

where $a, b \in Fp$, *and* $4a^3 + 27b^2 \neq 0$ *(mod p), together with a special point O, called the point at infinity.*

The set $E(Fp)$ consists of all points (x, y), $x \in Fp$, $y \in Fp$, which satisfy the defining equation (1), together with O.

An elliptic curve can have many points; any straight line connecting two points of them intersects a third point. The point at infinity O is the third point of intersection of any two points of a vertical line with the elliptic curve E. This makes it possible to generate all points out of jest a few [10].

The Arithmatic operations of the Elliptic Curves Group

In order to define a cryptosystem on the set of points on an elliptic curve, we need to define an algebraic structure on the points. The easiest algebraic structure, which provides us with all necessary tools, is the group. Therefore we need to define neutral element, inverse elements, and the addition of two elliptic curve points, which needs to be associative [8], and the multiplying the point by integer number:

- The neutral element is O.
- The inverse of point $P=(x, y)$ is $-P=(x, -y)$.
- The addition of two elliptic curve points is:

Let $P=(x_1, y_1)$, $Q=(x_2, y_2)$, $R=(x_3, y_3)$, $P,Q,R \in E(F_p)$, then $R=P + Q$ as follows

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda (x_1 - x_3) - y_1$$

where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \text{if } x_1 \neq x_2$$

and

$$\lambda = \frac{3x_1^2 + a}{2y_1}, \quad \text{if } x_1 = x_2$$

- The multiplying of point by integer refers to computing $Q=kP$, where P and Q are points on an elliptic curve and k is an integer. This really means that we add P to itself k times.

Elliptic Curves Public Key Traitor Tracing Scheme

When Boneh and Franklin introduce them scheme, they mentioned to possibility for applying this scheme on the elliptic curve points group [1]. This mention makes me apply this scheme on the elliptic curve points group. Initially, I'm proposed Elliptic Curves Decision Diffie Hellman Problem that the security of the system depend on this problem, then I'm proposed Elliptic Curves Public Key Traitor Tracing. Finally, I'm implemented the proposed system.

Elliptic Curves Decisional Diffie Hellman (ECDDH) Problem

The security of the public key traitor tracing scheme depends on The Decisional Diffie Hellman

problem [1], was introduced by D. Boneh in 1998 [2]. I well introduce the analogous of the DDH problem - which work in cyclic group Gp-. This analogous works in cyclic group E(Fp), I called it Elliptic Curve Decisional Diffie Hellman (ECDDH) Problem.

We work in a multiplicative cyclic group E(Fp) of large order over which solving the Elliptic Curve Decisional Diffie Hellman (ECDDH) Problem is hard:

Definition ECDDH:

Let B ∈ E(Fp) be a generator. Consider triples of the form R, (aB, bB, cB) with a, b, c < order(B) and triples of the form D, (aB, bB, abB) with a, b < order(B). A predicate solves the ECDDH problem if it can distinguish the collection D from the collection R.

The ECDDH-Assumption for E(Fp) suggests that any predicate that solves the ECDDH problem has distinguishing probability negligible in log(order(B)).

Let h0, h1, …… , hv be random points of E(Fp) so that hj = rjB for j = 0, 1, …….., v. For a certain element y = bB of E(Fp) a representation of y with respect to the base h0, h1, ……, hv is a (v + 1)-vector $\vec{\delta}$ =(δ0, δ1,……δv) such that y = δ0 h0 + δ1 h1 +……+ δv hv .

Elliptic Curve Public Key Traitor Tracing

The elliptic curves public key traitor tracing encryption scheme is a public key encryption system in which there is a unique encryption key and multiple decryption keys using the group of the elliptic curves points. The scheme is made up off our components:

Key Generation: The key generation algorithm takes as input a security parameters and a number of private keys to generate. It outputs a public encryption key e and a list of private decryption d1, d2, d3,…, dl. Any decryption key can be used to decrypt a ciphertext created using the encryption key.

Encryption: The encryption algorithm takes a public encryption key e and a message M and outputs a ciphertext C.

Decryption: The decryption algorithm takes a ciphertext C and any of the decryption keys di and outputs the message M. This is an "open" scheme in the sense that only the short decryption keys are secret while the decryption method can be public.

Representations: Occasionally, we will refer to the term representation. If $y = \sum_{j=1}^{2k} \delta_j (h_j)$, we say that ($\delta_1, \delta_2, \ldots\ldots\ldots\delta_{2k}$) is a representation of h with respect to the base h1, h2,……, h2k .

Tracing: Suppose a pirate get *s* hold of *k* decryption keys $d_1, d_2, d_3, \ldots, d_k$. Using the *k* key she creates a pirate decryption box (or decryption software) *D*. Any representation ($\delta_1, \delta_2, \ldots\ldots\ldots, \delta_{2k}$) of *y* with respect to the base h_i can be used as a decryption key. This is because $\sum_{j=1}^{2k} \delta_j (ah_j) = y^a$. The traitors can form new representations of *y* from the representations $\theta_i \cdot \bar{\gamma}^{(i)}$. If there are at most *k* traitors working together, the pirate keys are linear combinations of at most *k* codewords. In fact, this is the only effective way the traitors can find new decryption keys [1].

P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2008,(2), (1) :106-115

The Encryption Scheme

Let $E(F_p)$ be a group of elliptic curve points of order q (i.e. the number of elliptic curve points is q). The security of our encryption scheme relies on the difficulty of computing ECDLP in $E(F_p)$. More precisely, the security is based on the difficulty of the our Elliptic Curve Decision Diffie-Hellman problem in $E(F_p)$ as discussed below.

System setup:

1. Choose a suitable elliptic curve $E(F_p)$ defined over prime field F_p .
2. Compute the elliptic curve point $\#E$, let $q=\#E$.

Key generation: Perform the following steps:

1. Let B be a generator point of $E(F_p)$.
2. For j = 1,……., $2k$ choose a random $r_j \in Z_q$ and compute $h_j = r_j B$.
3. The public key is (y, h_1, ……., h_{2k}), where $y = \sum_{j=1}^{2k} \alpha_j h_j$, for random α_1,……., $\alpha_{2k} \in Z_q$.
4. A private key is an element $\theta_i \in Z_q$ such that $\theta_i \cdot \gamma^{(i)}$ is a representation of y with respect to the base h_1, ……., h_{2k}. The i'th key θ_i is derived from the i'th codeword $\gamma^{(i)} = (\gamma_1, \ldots\ldots\ldots, \gamma_{2k}) \in \Gamma$ by

$$\theta_i = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(i)}} \pmod{q} \quad \ldots\ldots\ldots(2)$$

To simplify the exposition we frequently refer to the private key as being the representation $\bar{d}_i = \theta_i \cdot \gamma^{(i)}$. Note however that only θ_i needs to be kept secret since the code Γ is public. One can verify that $\bar{d}_i$ is indeed a representation of y with respect to the base h_1, … h_{2k}.

Encryption: To encrypt a message M in G_p do the following: first pick a

1. random element $a \in Z_q$.
2. Compute ay
3. Compute ah_1, ah_1, ……., ah_{2k}
4. Let $(x_{ay}, z_{ay}) = ay$
5. Set the ciphertext C to be

$$C = \left\langle M \cdot x_{ay} \bmod p, ah_1, ah_2, ..., ah_{2k} \right\rangle$$

Decryption: To decrypt a ciphertext $C = \left\langle S, H_1, ..., H_{2k} \right\rangle$ using user i'th secret key θ_i compute:

1. Compute $U_i = \sum_{j=1}^{2k} \gamma_j^{(i)} H_j$,
2. Compute $\theta_i U_i$,
3. Let $(x_{\theta_i U_i}, z_{\theta_i U_i}) = \theta_i U_i$
4. Compute $M = \frac{S}{x_{\theta_i U_i}} \bmod p$

Here $\gamma^{(i)} = (\gamma_1, \ldots\ldots\ldots, \gamma_{2k}) \in \Gamma$ is the codeword from which θ_i is derived. The cost of computing U is far less than $2k$+1 scalar multiplication thanks to simultaneous fast group operatoin [10]. Also note that U can be computed without knowledge of the private key, leaving only a single scalar multiplication by the private key holder to complete the decryption.

Before going any further we briefly show that the encryption scheme is sound, i.e. any private key θ_i correctly decrypts any ciphertext. Given a ciphertext $C = \left\langle M \cdot x, ah_1, ah_2, ..., ah_{2k} \right\rangle$ where x is the x-axes cordinate of the point ay decryption will yield:

$\frac{M \cdot x_{ay}}{x_{\theta_i U_i}}$, where $U_i = \sum_{j=1}^{2k} \gamma_j^{(i)} (ah_j)$

Then

$$\theta_i U_i = \theta_i(\sum_{j=1}^{2k} a r_j \gamma_j^{(i)} B)$$

$$= a\theta_i(\sum_{j=1}^{2k} r_j \gamma_j^{(i)})B$$

$$= a\frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(i)}}(\sum_{j=1}^{2k} r_j \gamma_j^{(i)})B$$

$$= a(\sum_{j=1}^{2k} r_j \alpha_j)B = a(\sum_{j=1}^{2k} \alpha_j h_j)$$

$$= ay$$

as needed. The third equality follows from Equation (2). More generally, it is possible to decrypt given any representation $(\delta_1, \delta_2, \ldots\ldots\ldots \delta_{2k})$ of y with respect to the base $h_1, \ldots\ldots, h_{2k}$), since $\sum_{j=1}^{2k} \delta_j (ah_j) = ay$.

Implementation

The $E(F_p)$be the elliptic curve defined over p, where p is a prime, that formed an Abelian group has q points.Let the elliptic curve E defined over F_p, where p=3023.

System setup:

1. Choose a suitable elliptic curve $E(F_p)$ defined over prime field F_p ,

Let $E(F_{3023})$: $y^2 = x^3 + x + 2825$.

2. Compute the elliptic curve point $\#E$, let q= $\#E$=3109.

Key generation: Perform the following steps:

1. Let B =(873, 1491) be a generator point of $E(F_p)$.

2. For j = 1,……, 2k choose a random $r_j \in Z_q$

Let r = [456, 1134, 2109, 2599] ,

Compute $h_j = r_j B = [r_1 B, r_2 B, \ldots\ldots, r_{2k} B]$

= [456 (873, 1491), 1134 (873, 1491), 2109 (873, 1491), 2599 (873, 1491)].

= [(376, 2435), (1682, 2288), (965, 2096), (2979, 779)]

3. The public key is (y, h_1, ……., h_{2k}), where $y = \sum_{j=1}^{2k} \alpha_j h_j$, for random $\alpha_1, \ldots\ldots\ldots, \alpha_{2k} \in Z_q$.

Let α= [2198, 2534, 934, 1717] ,

y = 2198 (376, 2435)+2534(1682, 2288) + 934(965, 2096) + 1717(2979, 779)

= (2351, 379) + (196, 491) + (1214, 1188) + (2417, 628)

= (193, 2887).

4. A private key is an element $\theta_i \in Z_q$ such that $\theta_i \cdot \gamma^{(i)}$ is a representation of y with respect to the base $h_1, \ldots\ldots, h_{2k}$. The i'th key θ_i is derived from the i'th codeword $\gamma^{(i)} = (\gamma_1, \ldots\ldots\ldots, \gamma_{2k}) \in \Gamma$ by

$$\theta_i = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(i)}}$$

Let the codeword of users is:

$$\Gamma = \begin{bmatrix} 1144 & 2956 & 2181 & 1646 \\ 573 & 1884 & 709 & 2087 \\ 915 & 904 & 166 & 2658 \\ 1296 & 756 & 441 & 2589 \\ 584 & 2175 & 1728 & 1836 \\ 1706 & 412 & 238 & 1858 \end{bmatrix}$$

$l \times 2k$

Therefore the private keys of all users are:

1. The private key of user (1):

$$\theta_1 = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(1)}} \bmod q$$

$$= \frac{\begin{array}{l}456*2198+1134*2534\\+2109*934+2599*1717\end{array}}{\begin{array}{l}456*1144+1134*2956\\+2109*2181+2599*1646\end{array}} \bmod 3109 = 809$$

2. The private key of user (2):

$$\theta_2 = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(2)}} \bmod q$$

$$= \frac{\begin{array}{l}456*2198+1134*2534\\+2109*934+2599*1717\end{array}}{\begin{array}{l}456*573+1134*1884\\+2109*709+2599*2087\end{array}} \bmod 3109 = 2697$$

3. The private key of user (3):

$$\theta_3 = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(3)}} \bmod q$$

$$= \frac{\begin{array}{l}456*2198+1134*2534\\+2109*934+2599*1717\end{array}}{\begin{array}{l}456*915+1134*904\\+2109*166+2599*2658\end{array}} \bmod 3109 = 743$$

4. The private key of user (4):

$$\theta_4 = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(4)}} \bmod q$$

$$= \frac{\begin{array}{l}456*2198+1134*2534\\+2109*934+2599*1717\end{array}}{\begin{array}{l}456*1296+1134*756\\+2109*441+2599*2589\end{array}} \bmod 3109 = 988$$

5. The private key of user (5):

$$\theta_5 = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(5)}} \bmod q$$

$$= \frac{\begin{array}{l}456*2198+1134*2534\\+2109*934+2599*1717\end{array}}{\begin{array}{l}456*584+1134*2175\\+2109*1728+2599*1836\end{array}} \bmod 3109 = 1027$$

6. The private key of user (6):

$$\theta_6 = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j^{(6)}} \bmod q$$

$$= \frac{\begin{array}{l}456*2198+1134*2534\\+2109*934+2599*1717\end{array}}{\begin{array}{l}456*1706+1134*412\\+2109*238+2599*1858\end{array}} \bmod 3109 = 2676$$

Encryption: To encrypt a message M in G_p do the following: first pick a

1. random element $a \in Z_q$, let a = 712.

2. Computeay = 712(193, 2887) = (2870, 744).

3. Compute $ah_1, ah_1, \ldots\ldots, ah_{2k}$

= [712(376, 2435), 712(1682, 2288), 712(965, 2096), 712(2979, 779)]

= [(612, 1223), (1868, 2264), (2709, 2820), (1577, 163)]

4. Let $(x_{ay}, z_{ay}) = ay$,

x_{ay} = 2870,

z_{ay} = 744

5. Set the ciphertext C to be

$$C = \left\langle M \cdot x_{ay} \bmod p, ah_1, ah_2, \ldots\ldots\ldots, ah_{2k} \right\rangle,$$

M* x_{ay} = 1234*2870 = 1647,

$$C = \left\langle \begin{matrix} 1647, [(612, 1223), (1868, 2264), \\ (2709, 2820), (1577, 163)] \end{matrix} \right\rangle$$

Decryption: To decrypt a ciphertext $C = \langle S, H_1, ..., H_{2k} \rangle$ using user *i*'th secret key θ_i compute:

1) Compute $U_i = \sum_{j=1}^{2k} \gamma_j^{(i)} H_j$,

2) Compute $(x_{\theta_i U_i}, z_{\theta_i U_i}) = \theta_i U_i$

3) Compute $M = \frac{S}{x_{\theta_i U_i}} \mod p$

The decryption of the ciphertext by all users private keys:

1. The decryption of the ciphertext by user (1) private key:

1) $U_1 = \sum_{j=1}^{2k} \gamma_j^{(1)} H_j$

= 1144 (612, 1223) + 2956 (1868, 2264) + 2181 (2709, 2820) +
1645 (1577, 163)
= (139, 1492) + (2450, 507) + (909, 371) + (1829, 35)
= (2846, 117) + (909, 371) + (1829, 35)
= (640, 2225) + (1829, 35)
= (1877, 1256)

2) $(x_{\theta_1 U_1}, z_{\theta_1 U_1}) = \theta_1 U_1$ = 809 (1877, 1256) = (2870, 744)

3) $M = \frac{S}{x_{\theta_i U_i}} \mod p = \frac{1647}{2870} \mod 3023$
$= 1647 * 2870^{-1} \mod 3023$
= 1647*1225 mod 3023
=1234

2. The decryption of the ciphertext by user (2) private key:

1) $U_2 = \sum_{j=1}^{2k} \gamma_j^{(2)} H_j$
= 573 (612, 1223) + 1884 (1868, 2264) + 709 (2709, 2820) +
2087(1577, 163)
= (406, 825)

2) $(x_{\theta_2 U_2}, z_{\theta_2 U_2}) = \theta_2 U_2$ = 2697 (406, 825) = (2870, 744)

3) $M = \frac{S}{x_{\theta_2 U_2}} \mod p = \frac{1647}{2870} \mod 3023$
$= 1647 * 2870^{-1} \mod 3023$
= 1647*1225 mod 302 = 1234

3. The decryption of the ciphertext by user (3) private key:

1) $U_3 = \sum_{j=1}^{2k} \gamma_j^{(3)} H_j$
= 915 (612, 1223) + 904 (1868, 2264) + 166 (2709, 2820) +
2658 (1577, 163)
= (2051, 309)

2) $(x_{\theta_3 U_3}, z_{\theta_3 U_3}) = \theta_3 U_3$ = 743 (2051, 309) = (2870, 744)

3) $M = \frac{S}{x_{\theta_3 U_3}} \mod p = \frac{1647}{2870} \mod 3023$
$= 1647 * 2870^{-1} \mod 3023$
= 1647*1225 mod 3023
=1234

4. The decryption of the ciphertext by user (4) private key:

1) $U_4 = \sum_{j=1}^{2k} \gamma_j^{(4)} H_j$

= 1296 (612, 1223) + 756 (1868, 2264) + 441 (2709, 2820) +

2589 (1577, 163)

= (2140, 922)

2) $(x_{\theta_4 U_4}, z_{\theta_4 U_4}) = \theta_4 U_4$ = 988 (2140, 922) = (2870, 744)

3) $M = \frac{S}{x_{\theta_4 U_4}} \bmod p = \frac{1647}{2870} \bmod 3023$

$= 1647 * 2870^{-1} \bmod 3023$

= 1647*1225 mod 3023

=1234

5. The decryption of the ciphertext by user (5) private key:

1) $U_5 = \sum_{j=1}^{2k} \gamma_j^{(5)} H_j$

= 584 (612, 1223) + 2175 (1868, 2264) + 1728 (2709, 2820) +

1836 (1577, 163)

= (2778, 2279)

2) $(x_{\theta_5 U_5}, z_{\theta_5 U_5}) = \theta_5 U_5$ = 1027 (2778, 2279) = (2870, 744)

3) $M = \frac{S}{x_{\theta_5 U_5}} \bmod p = \frac{1647}{2870} \bmod 3023$

$= 1647 * 2870^{-1} \bmod 3023$

= 1647*1225 mod 3023

=1234

6. The decryption of the ciphertext by user (6) private key:

1) $U_6 = \sum_{j=1}^{2k} \gamma_j^{(6)} H_j$

= 1706 (612, 1223) + 412 (1868, 2264) + 238 (2709, 2820) +

1858 (1577, 163)

= (2380, 498)

2) $(x_{\theta_6 U_6}, z_{\theta_6 U_6}) = \theta_6 U_6$ = 2676 (2380, 498) = (2870, 744)

3) $M = \frac{S}{x_{\theta_6 U_6}} \bmod p = \frac{1647}{2870} \bmod 3023$ =

$= 1647 * 2870^{-1} \bmod 3023$

1647*1225 mod 3023

=1234

Conclusion

We present an elliptic curves public key solution to the traitor tracing problem. Our construction is based on the representation for Elliptic Curve Discrete Logarithm Problem (ECDLP). Traceability follows from the hardness of ECDLP. The semantic security of the encryption scheme against a passive attack follows from the Elliptic Curve Decisional Diffie-Hellman assumption. A simple extension achieves security against an adaptive chosen ciphertext attack under the same hardness assumption.

The main advantage of our proposed system that the ECDDH problem harder than DDH problem, because the DDH problem depend on the exponentiation operation, while the ECDDH problem depend on the group operation. The complications associated with elliptic curves derive from the wide variety of possible group structures of points on an elliptic curve, and from the fact that addition on elliptic curves is somewhat

complicated. This to attraction of using elliptic curves compared to other is that it appears to offer equal security for a far smaller bit size, thereby reducing processing overhead.

Refereneces

[1] D. Boneh and M. Franklin (1999). An efficient public key traitor tracing scheme, Advances in Cryptology - Crypto '99, Lecture notes in Computer Science 1666, pp. 338–353. <http://crypto.stanford.edu/ adabo/abstracts/traitors.html>.

[2] D. Boneh (1998). The Decision Diffie-Hellman problem, In proc. of the Third Algorithmic Number Theory Symposium (ANTS), Lecture Notes in Computer Science 1423, , pp. 48–63.

[3] B. Chor, Amos Fiat, and Moni Naor (1994). Tracing Traitors, Advances in Cryptology - Crypto '94, Lecture Notes in Computer Science 839, pp. 257–270.

[4] B. Chor, Amos Fiat, Moni Naor and Benny Pinkas (2000). Tracing Traitors, IEEE Transactions on Information Theory, Vol. 46, no. 3, pp. 893-910.

[5] P. Y. Huang, M. L. Hsieh & K. W. Lan (2000), Generating Elliptic Curve Over Finite Fields, Part I, II.

[6] Jason Q. Chen (2000). A Survey on Traitor Tracing Schemes, MSc. Thesis, University of Waterloo, Canada.

[7] T. K. Meng (2001). Curves for The Elliptic Curve Cryptosystem, M.Sc. Thesis, University of Singapore.

[8] E. Oswald (2002), Introduction to Elliptic Curve Cryptography, Institute for Applied information Processing and Communication A-8010 Inffeldgasse 16a, Graz, Austria.

[9] J. H. Silverman (1986), The Arithmetic of Elliptic Curves, Graduate Text in Mathematics 106, Springer-Verlag.

[10] S.Y. Yan (2000), Number Theory for Computing, Springer-Verlag.

طريقة إقتفاء الخائن ذات المفتاح المعلن باستخدام المنحنيات الاهليلجية

علي مكي صغير

E.mail: ali_makki_sagheer@yahoo.com

الخلاصة:

في هذا البحث لقد استعملنا نظام المنحنيات الاهليلجية في طريقة إقتفاء الخائن ذات المفتاح المعلن. حيث ان نقاط المنحني الإهليلجي تشكل زمرة ابيلية تستخدم في طريقة إقتفاء الخائن ذات المفتاح المعلن. ان الفائدة الرئيسية لأنظمة المنحنيات الإهليليجية هو ان قوة التشفير بها عالية مقارنة بحجم المفتاح. في هذه البحث صممنا ونفذنا نظام تشفير ذو المفتاح المعلن باستخدام المنحنيات الإهليليجية ، الذي يستخدم فيه مفتاح معلن واحد للتشفير، لكن العديد من مفاتيح الحل الخاصة التي توزع خلال قنوات الارسال، ان أمنية نظام تشفير ذو المفتاح المعلن باستخدام المنحنيات الإهليليجية تعتمد على مسالة ECDDH التي تماثل مسالة DDH، لكن مسالة ECDDH أكثر تعقيد من مسالة DDH.