SCIS2000 The 2000 Symposium on Cryptography and Information Security
Okinawa, Japan, January 26-28, 2000

Cryptosystems Based on Pairing

Ryuichi Sakai * Kiyoshi Ohgishi † Masao Kasahara ‡

Abstract— This paper presents a new ID based non-interactive key sharing system based on the Weil pairing and the Tate pairing and show that the collusion attacks against the proposed IDNIKS is infeasible, by proving that if some conventional collusion attacks should succeed the discrete logarithm problem on the elliptic curve or discrete logarithm on the finite fields could be solved. This paper also presents some new digital signature schemes based on the pairing. The schemes can use same information data of the new IDNIKS, and apply the multiple or group signature and the signature which can specify the verifiers.

Keywords: pairing, key sharing, non-interactive, group digital signature

1 Introduction

Nowadays, the various classes of cryptosystems are being applied to the information transmission and storage systems. The more efficient and secure cryptosystems are desired for the constructions of the world-wide digital communication networks. The fast encryption and decryption cryptosystem is indispensable for the secure digital communication networks with the large capacity. The systems of the common key cryptosystems are currently the essential techniques for the fast encryptions and decryptions. The common key-sharing system then is a key technology for the secure and convenient common key cryptosystems. One of the common key-sharing systems can be realized by using the public key cryptosystem with the public key verification center. However, this system is necessary to rewrite the list of public key, when the new users subscribe the cryptosystem. The ID based non-interactive key sharing system with the trustful center (hereafter, we shall call this system IDNIKS) realizes the convenient cryptosystem which generates the common key with ID information such as E-mail address, thus the system is not necessary to rewrite the list of public key[1],[2],[3][4],[5].

This paper presents a new ID based non-interactive key sharing system and some digital signature schemes all of which are based on the pairings on the elliptic curves over finite fields. Section 2 describes properties of the pairings and introduces a new ID based non-interactive key sharing system based on the Weil pairing and the Tate pairing both of which are defined on the elliptic curve over finite field. Section 3 discusses the security of the proposed IDNIKS and show that the collusion attacks against the proposed IDNIKS is infeasible, by proving that if some conventional collusion attacks can succeed the discrete logarithm problem on the elliptic curve or discrete logarithm on the finite fields can then be solved. Section 4 presents some new digital signature shames based on the Weil pairing. These shames are not able to execute so fast as the conventional schemes but the schemes can use same information data of the new IDNIKS proposed in this paper, and apply the multiple or group signature and the signature which can specify the verifiers.

* Dept. of Lightwave Sciences, Osaka electro-communication University. 18-8, Hatsu-cho, Neyagawa City, Osaka 572-8530 Japan, e-mail: sakai@isc.osakac.ac.jp
† Matsushita Electric Industrial Co. Ltd. 1006, Kadoma, Kadoma City, Osaka 571-8501 Japan
‡ Dept. of Electronics and Information Science, Kyoto Institute of Technology, Matsugasaki, Sakyo-ku, Kyoto 606-8585 Japan

2 IDNIKS based on Pairing

In this section, we propose the IDNIKS based on the pairing, and a basic method of the key sharing. The several pairings over the elliptic curve, such as the hight pairing, the Tate pairing and the Weil pairing have been widely known[6],[7],[8].

2.1 Pairing

Let $(\ ,\ )$ denote a pairing which is a mapping from the additive group A to the multiple group M, then the pairing $(\ ,\ ) \in M$ of $a, b, c \in A$ holds the following properties:

$$\begin{array}{lcll} (a,b) & = & 1 \text{ for all } a \in A & \text{non-degenerate} \\ & & \text{if and only if } b = 0 & \\ (a,b) & = & (b,a)^{-1} & \text{alternating} \\ (a+b,c) & = & (a,c)(b,c) & \left.\begin{array}{l}\\ \text{bilinear}\end{array}\right\} \\ (a,b+c) & = & (a,b)(a,c) & \end{array}$$

The following equations hold by the property of the bilinear

$$(ma,b) = (a,b)^m$$

$$(a, mb) \quad = \quad (a, b)^m$$

2.2 IDNIKS based on Pairing

Using the pairing, We propose the IDNIKS as follows.

Preparation : Let ID_i denote the ID information of user $\boldsymbol{i}$. The trustful center publicizes the algorithm $(\ ,\ )$ and $f()$, where $(\ ,\ )$ is a pairing and $f()$ is a function which embeds the ID information ID_i to the element P_i of the group A. The center generates a large random secret integer l and calculates $S_i = lP_i$. The center then send S_i secretly to user $\boldsymbol{i}$. These data are summarized as follows.

Center's secret data	:	l (random integer)
Center's public algorithm	:	$f()$, $(\ ,\ )$
User $\boldsymbol{i}$'s secret data	:	S_i
User $\boldsymbol{i}$'s public data	:	ID_i, P_i

For user $\boldsymbol{a}$ and $\boldsymbol{b}$, ID_a, ID_b are the ID information of user $\boldsymbol{a}$ and $\boldsymbol{b}$, $P_a = f(ID_a)$ and $P_b = f(ID_b)$ are the elements of group A and $S_a = lP_a$ and $S_b = lP_b$ are the secret informations of users $\boldsymbol{a}$ and $\boldsymbol{b}$ respectively.

Key sharing scheme : We assume that the alphabetical order of ID_a and ID_b is given. The user $\boldsymbol{a}$ generates the common key $K_{ab} \in G$ with the user $\boldsymbol{b}$ by

$$K_{ab} = (S_a, P_b) = (P_a, P_b)^l$$

and the user $\boldsymbol{b}$ generates the common key $K_{ba} \in G$ with the user $\boldsymbol{a}$ by

$$K_{ba} = (P_a, S_b) = (P_a, P_b)^l.$$

Applying the properties of the pairing to the equations, it is clear that the equation $K_{ab} = K_{ba}$ holds. If the order of ID_a and ID_b is not given, let

$$k_{ab} = (S_a, P_b) = (P_a, P_b)^l$$

and

$$k_{ba} = (S_b, P_a) = (P_b, P_a)^l,$$

then the user $\boldsymbol{a}$ generates the common key with the user $\boldsymbol{b}$ by

$$K_{ab} = k_{ab} + k_{ab}^{-1}$$

and the user $\boldsymbol{b}$ generates the common key with the user $\boldsymbol{a}$ by

$$K_{ba} = k_{ba} + k_{ba}^{-1}.$$

2.3 IDNIKS based on Weil and Tate Pairing

The proposed IDNIKS in the above section can use Weil or Tate pairing as the pairing $(\ ,\ )$. In these case, the algorithm $(\ ,\ )$ uses the elliptic curve over finite field $E/\boldsymbol{F}_q$. The elliptic curve should satisfy the following conditions:

1. q is larger than 2^{160} .
2. There exists the integer k such that $\#E/\boldsymbol{F}_q | q^k - 1$ and $q^k \simeq 2^{1024}$.

The first condition is necessary because the discrete logarithm problems on the elliptic curve(ECDLP) is made difficult enough. The second is necessary because the discrete logarithm problems on the finite field over $\boldsymbol{F}_{q^k}$(DLP) is made difficult and the pairing algorithm $(\ ,\ )$ can be computed practically.

The construction algorithm of the appropriate elliptic curves are written in Appendix.

- In this section, we use the pairing on the elliptic curve, however we can use the Weil pairing on hyper elliptic curves in a straightforward manner.
- The proposed IDNIKS can be constructed based on other pairing.

2.4 IDNIKS based on Pairing and ID Vector

In this section, we propose an extended method of IDNIKS based on the paring.

2.5 Construction

Let user $\boldsymbol{a}$'s ID vector, $\overrightarrow{P_a}$, such that

$$\overrightarrow{P_a} = \begin{pmatrix} P_{a1} & P_{a2} & \cdots & P_{an} \end{pmatrix}.$$

The center generates the symmetric matrix, L, such that

$$\begin{aligned} L &= L^t \\ &= \begin{pmatrix} l_{11} & l_{12} & \cdots & l_{1n} \\ l_{21} & l_{22} & \cdots & l_{2n} \\ \vdots & \vdots & & \vdots \\ l_{n1} & l_{n2} & \cdots & l_{nn} \end{pmatrix} \end{aligned}$$

as the secret parameters.

The center calculates the user $\boldsymbol{a}$'s secret vector, $\overrightarrow{P_a}$, such that

$$\overrightarrow{S_a} = \overrightarrow{P_a} L$$

and send $\overrightarrow{S_a}$ to the user $\boldsymbol{a}$ through a secure channel.

The user $\boldsymbol{a}$ calculates a shared key with the user $\boldsymbol{b}$, K_{ab}, such that

$$\begin{aligned} K_{ab} &= \overrightarrow{S_a}\overrightarrow{P_b}^t \\ &= \overrightarrow{P_a} L \overrightarrow{P_b}^t \\ &= \begin{pmatrix} P_{a1} & P_{a2} & \cdots & P_{an} \end{pmatrix} \begin{pmatrix} l_{11} & l_{12} & \cdots & l_{1n} \\ l_{21} & l_{22} & \cdots & l_{2n} \\ \vdots & \vdots & & \vdots \\ l_{n1} & l_{n2} & \cdots & l_{nn} \end{pmatrix} \begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^{n} l_{i1} P_{ai} & \sum_{i=1}^{n} l_{i2} P_{ai} & \cdots & \sum_{i=1}^{n} l_{in} P_{ai} \end{pmatrix} \begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \end{aligned}$$

$$= \prod_{j=1}^{n}\left(\sum_{i=1}^{n} l_{ij}P_{ai}, P_{bj}\right)$$
$$= \prod_{j=1}^{n}\prod_{i=1}^{n}(P_{ai}, P_{bj})^{l_{ij}}$$

where point and point product means Weil pairing.

Therefore

$$K_{ab} \times K_{ba} = 1.$$

3 Security Analysis

In this section, we discuss the security of the new IDNIKS proposed in section ?.

3.1 Security of Center Secret

We first consider whether the center secret l can be revealed or not. If the attacker of the user $\boldsymbol{a}$ try to find l by P_a and $S_a = lP_a$ or by (P_a, P_b) and $K_{ab} = (P_a, P_b)^l$, it cannot be revealed, because l is a discrete logarithm of S_a and P_a and (P_a, P_b) and K_{ab}. Therefore any user cannot find l. Even if the attacker $\boldsymbol{a}$ tries to forge the another user's key $K_{bc}l$ by P_a and $S_a = lP_a$, it cannot be forged, because S_b and S_c are secret of the users $\boldsymbol{b}$ and $\boldsymbol{c}$, and these cannot be computed without l. Therefore only one user cannot forge K_{bc}.

3.2 Collusion Attacks

Here we discuss the collusion attacks against the proposed IDNIKS. We show that if the conventional collusion attacks succeed, the discrete logarithm problem on finite fields(DLP) and discrete logarithm problem on the group of elliptic curve over finite fields(ECDLP) can be solved. Then as long as the given DLP and ECDLP are not able to be solved, any conventional collusion attacks becomes infeasible.

Let n be the number of colluders and i denote the i-th colluders. The ID information, the public information and the secret information of the i-th colluder are denoted by ID_i, P_i and S_i respectively.

Users secret data

We now discus whether the secret of the user $\boldsymbol{b}$ can be forged or not. The public data $P_b \in E/\boldsymbol{F}_q$ of the user $\boldsymbol{b}$ can be denoted by the linear combination of the colluders data $\{P_i\}$ such that

$$P_b = u_1P_1 + u_2P_2 + \cdots + u_nP_n. \quad (1)$$

Then if the coefficients u_i of Equation (1) are revealed, the secret data of the user $\boldsymbol{b}$ can be forged by

$$\begin{aligned} S_b &= u_1S_1 + u_2S_2 + \cdots + u_nS_n \\ &= u_1(lP_1) + u_2(lP_2) + \cdots + u_n(lP_n) \\ &= l(u_1P_1 + u_2P_2 + \cdots + u_nP_n) \\ &= lP_b. \end{aligned}$$

In order to certify the complexity of the problem to computes the coefficients u_i of Equation (1), we shall define the generalized elliptic curve discrete logarithm problem (GECDLP) as follows.

GECDLP is a problem for computing u_1 and u_2 such that

$$P = u_1G_1 + u_2G_2,$$

where P is any point on $E/\boldsymbol{F}_q$ and (G_1, G_2) are generators of $E/\boldsymbol{F}_q$.

Let the order of G_1 and G_2 denote $\#(G_1)$ and $\#(G_2)$ respectively where $\#(G_1)|\#(G_2)$. If GECDLP could be solved, the coefficient u_1, u_2 such that $P = u_1G_1 + u_2G_2$ and the coefficient v_1, v_2 such that $Q = v_1G_1 + v_2G_2$ are derived and ECDLP $Q = lP$ could be solved by the following equations.

$$\begin{aligned} lu_1 &\equiv v_1 \pmod{\#(G_1)} \\ lu_2 &\equiv v_2 \pmod{\#(G_2)} \\ l &\equiv \frac{v_1}{u_1}\left(\mathrm{mod}\ \frac{\#(G_1)}{\gcd(u_1, \#(G_1))}\right) \\ l &\equiv \frac{v_2}{u_2}\left(\mathrm{mod}\ \frac{\#(G_2)}{\gcd(u_2, \#(G_2))}\right) \end{aligned}$$

We next consider the equivalence between the problem to solve Equation (1) and GECDLP. If Equation (1) could be solved, $l_{i,j}$ of

$$P_i = \sum_{\substack{j=1 \\ j\neq i}}^{n} l_{i,j}P_j (1 \le i \le n-2) \quad (2)$$

could be derived and the equation

$$\begin{pmatrix} -1 & l_{1,2} & \cdots & l_{1,n-2} \\ l_{2,1} & -1 & \cdots & -l_{2,n-2} \\ \vdots & \vdots & & \vdots \\ l_{n-2,1} & l_{n-2,2} & \cdots & -1 \end{pmatrix}\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_{n-2} \end{pmatrix}$$
$$= -\begin{pmatrix} l_{1,n-1} & l_{1,n} \\ l_{2,n-1} & l_{2,n} \\ \vdots & \vdots \\ l_{n-2,n-1} & l_{n-2,n} \end{pmatrix}\begin{pmatrix} P_{n-1} \\ P_n \end{pmatrix}$$

could be solved under the assumption of the determinant of the left hand side of $n-2 \times n-2$ matrix is coprime to $\#(G_2)$ where $P_{n-1} = G_1, P_n = G_2$. If the determinant is not coprime to $\#(G_2)$, we can choose the another solutions $l_{i,j}$ of Equation (2). Consequently we have

$$\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_{n-2} \end{pmatrix} = \begin{pmatrix} l'_{1,n-1} & l'_{1,n} \\ l'_{2,n-1} & l'_{2,n} \\ \vdots & \vdots \\ l'_{n-2,n-1} & l'_{n-2,n} \end{pmatrix}\begin{pmatrix} P_{n-1} \\ P_n \end{pmatrix}.$$

GECDLP of P_i and (G_1, G_2) then could be solved if Equation (1) could be solved.

We shall next show that if GECDLP could be solved Equation (1) could be solved. GECDLP's of P_i and (G_1, G_2) are denoted by

$$\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} l_{1,1} & l_{1,2} \\ l_{2,1} & l_{2,2} \\ \vdots & \vdots \\ l_{n,1} & l_{n,2} \end{pmatrix} \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}.$$

GECDLP of P_b and (G_1, G_2) is denoted by

$$P_b = v_1 G_1 + v_2 G_2.$$

Then the following relations hold

$$v_1 G_1 + v_2 G_2. = \sum_{i=1}^{n} u_i l_{i,1} G_1 + \sum_{i=1}^{n} u_i l_{i,2} G_2$$

$$\left.\begin{aligned} v_1 &= \sum_{i=1}^{n} u_i l_{i,1} \\ v_2 &= \sum_{i=1}^{n} u_i l_{i,2} \end{aligned}\right\}$$

Clearly if v_j and $l_{i,j}$ are given, u_i can be solved. Here we finished the proof of the equivalence between GECDLP and the problem of the solving of Equation (1). If the group of the elliptic curve is cyclic, it is clear that the GECDLP equal the ECDLP. Therefore the problem of the solving of Equation (1) is equivalent to ECDLP in this case.

There are some other collusion attacks. The collusion attack to forge the K_{bc} from the colluder's secret S_i without S_b and S_c are the same problem of the forging of the S_b from the S_i. The collusion attack to forge the K_{bc} from the common keys K_{ij} of the outsiders $\boldsymbol{i}$ and $\boldsymbol{j}$ becomes the difficult problem because without knowing the center secret l, the problem to forge K_{bc} result in the Diffe-Hellman type problem.

4 Digital Signatures based on Pairing

4.1 Identity Based Digital Signature Scheme based on Pairing

We propose an ID based digital signature scheme based on the pairing.

4.1.1 Construction

Let the signer $\boldsymbol{a}$'s public algorithms are the pairing $(\ ,\ )$ and a function $f()$ which embedded the ID information ID_a of the user $\boldsymbol{a}$ to the elements $P_a \in A$. Let the signer $\boldsymbol{a}$'s secret data are a large integer l and $Q_a = lP_a$. Then the user $\boldsymbol{a}$ choose a random element $R \in A$ and make R and $R' = lR$ public. These data are summarized as follows.

User $\boldsymbol{a}$'s secret data	:	l, Q_a
User $\boldsymbol{a}$'s public algorithm	:	$f()$, $(\ ,\ )$, R', R

In order to create the signature, the signer $\boldsymbol{a}$ first choose a random integer r and embed the massage m to $M \in A$. The signer then signs the message $M \in \boldsymbol{E}/F_q$ by:

$$\begin{aligned} S_a^{(0)} &= Q_a + rM, \\ S_a^{(1)} &= rR, \qquad \text{Signature} : (S_a^{(0)}, S_a^{(1)}). \end{aligned}$$

The signature is a pair of $S_a^{(0)}$ and $S_a^{(1)}$. The verifier computes the following pairing from the signature.

$$\begin{aligned} v_1 &= e_n(S_a^{(0)}, R) = e_n(P_a, R)^l e_n(M, R)^r \\ v_2 &= e_n(P_a, R') = e_n(P_a, R)^l \\ v_3 &= e_n(M, S_a^{(1)}) = e_n(M, R)^r \end{aligned}$$

The verifier can check the validity of the signature by checking the validity of the following equations:

$$v_2 v_3 = v_1,$$

Assuming the existence of the trustful center, letting the secret data l be the center's secret, $Q_a = lP_a$ and $R, R' = lR$ are computed by the center, the R and R' are publicized by the center. Consequently, the signature can be created by the signer and the verifier can then check the validity of the signature by using the center public common data R, R' and $P_a = h(ID_a)$.

4.2 Identity Based Multiple Digital Signature Scheme based on Pairing

We propose identity based multiple digital signature schemes based on the pairing. This scheme can specify verifier.

4.2.1 Construction

The pairing $(\ ,\ ) \in A$ is the center's public algorithm. Center's public parameters are points , R_1, and $R_2 (= lR_1)$, on the elliptic curve, E, and his secret parameter is scalar, l.

Center calculates signer A_i's $(1 \le i \le n)$ secret key, Q_i, such that

$$Q_i = lP_i,$$

and send Q_i to signer A through a secure channel. These data are summarized as follows.

Center's secret data	:	l (random integer)
Center's public algorithm	:	$f()$, $(\ ,\ )$, $, R, R'$
Signer A_i's secret data	:	Q_i
Signer A_i's public data	:	ID_i, P_i

The signature algorithm is given by the following:

Step 1. Signer A_1 converts message m to point, M, on the elliptic curve, $E/\boldsymbol{F}_q$ and generates random number, r_1. Signer A_1 then calculates $S_1^{(0)} = Q_1 + r_1 M$ and $S_1^{(1)} = r_1 R$, and sends $S_{1,1}$, and $S_{1,0}$ to signer A_2.

Step 2. Signer A_2 generates random number, r_2. Signer A_2 then calculates $S_2^{(0)} = Q_2 + r_2 S_{10}$, $S_2^{(1)} = r_2 S_1^{(1)}$ and $S_2^{(2)} = r_2 P_1$, Signer A_2 then sends $S_2^{(j)}$ $(0 \le j \le 2)$ to signer A_3.

Step 3. Signer A_3 generates random number, r_3 and calculates $S_3^{(0)} = Q_3 + r_3 S_2^{(0)}$, $S_3^{(1)} = r_3 S_2^{(1)}$, $S_3^{(2)} = r_3 S_2^{(2)}$, and $S_3^{(3)} = r_3 P_2.$, Signer A_3 then sends $S_3^{(j)}$ $(0 \le j \le 3)$ to signer A_4.

Step 4. Signer A_i generates random number, r_i and calculates $S_i^{(0)} = Q_i + r_i S_{i-1,0}$, $S_i^{(j)} = r_i S_{i-1,j}$ where $2 \le j \le i-1$, and $S_i^{(i)} = r_i P_{i-1}.$, Signer A_i then sends $S_i^{(j)}$ $(0 \le j \le i)$ to signer A_{i+1}.

Step 5. Signer A_n generates random number, r_n and calculates

$$\begin{aligned} S_n^{(j)} &= r_n S_{n-1}^{(j)} \\ &= \prod_{k=j}^{n} r_k P_{j-1} \quad (2 \le j \le n), \end{aligned}$$

$$\begin{aligned} S_n^{(1)} &= r_n S_{n-1}^{(1)} \\ &= \prod_{k=1}^{n} r_k R_1, \end{aligned}$$

and

$$\begin{aligned} S_n^{(0)} &= Q_n + r_n S_{n-1}^{(0)} \\ &= \sum_{j=1}^{n-1} \left(\prod_{k=j+1}^{n} r_k Q_j \right) + \prod_{k=1}^{n} r_k M. \end{aligned}$$

The verifying algorithm of the message and the sign of the signer A_n is given by the followings:

Step 1. Verifier calculates

$$P_a = P_n + \sum_{j=2}^{n} \left(\prod_{k=j}^{n} r_k P_{j-1} \right).$$

Step 2. Verifier calculates

$$v_1 = (S_n^{(0)}, R_1),$$

$$v_2 = (P_a, R_2),$$

and

$$v_3 = \left(M, \prod_{k=1}^{n} r_k R_1 \right).$$

Step 3. Verifier checks

$$v_1 = v_2 \times v_3$$

The verifying algorithm of the sign of the signer A_i $(1 \le i \le n-1)$ is given by the following:

Step 1. Verifier checks

$$(S_n^{(i+1)}, P_i) = 1.$$

Note that the scheme can keeps the signed order secret against the verifier without the n-th signer.

4.3 Extension of Specified Verifier

The proposed scheme can be extended to the scheme with the specified verifier $\boldsymbol{v}$. This scheme is to change center's public parameters, R_1 and R_2 to verifier's identity, $R = P_v$, and secret parameter, $R' = Q_v = lP_v$), respectively.

Furthermore, the scheme can be extended to the scheme with multiple verifiers. This is to change verifier's identity, R, and secret parameter, R', to verifiers' identity, $R_i = P_i$ $(1 \le i \le n)$, and secret parameter, $R_i' = Q_i$ $(1 \le i \le n)$. Note that the signature data $S_n^{(i)}$ can be common without $S_n^{(1)}$ because the only of the data $S_n^{(1)}$ is generated by P_i . Therefore the signature for the m multiple specified verifiers is given by:

$$\begin{pmatrix} S_n^{(0)} & S_n^{(2)} & S_n^{(3)} & & \cdots & S_n^{(n)} \\ S_{n,1}^{(1)} & S_{n,2}^{(1)} & S_{n,3}^{(1)} & \cdots & S_{n,m}^{(1)} & \end{pmatrix}$$

where $S_{n,i}^{(1)}$ is used by the i-th verifier.

4.4 Extension to Verification of Signed Order

The proposed scheme can be extended to the scheme which can verify the signed order. The extended scheme can be realized by changing $S_i^{(0)}$ as follows:

$$S_i^{(0)} = Q_i + i r_i S_{i-1}^{(0)} \quad (1 \le i \le n-1).$$

Note that the order of n-th signer is also verified on the scheme in 4.2.

5 Extension to Multiple Centers

In the proposed IDNIKS and the signature schemes, the trustful center can be a big brother. However by setting up the multiple centers, we can construct the system with no big brother on the condition that no centers conspire.

6 Conclusion

We have proposed the IDNIKS and some signature schemes and have shown the equivalences between the the conventional collusion attacks against the proposed IDNIKS and the generalized ECDLP and the DLP.

There are the open problem whether the proposed ID-NIKS is secure against the any collusion attacks. Further work should be to analyze the security of the proposed signature schemes.

Appendix

We present some methods to construct the appropriate elliptic curves for the proposed cryptosystems. One of the construction algorithm of the appropriate elliptic curves for the Tate pairing is given as follows: to

Algorithm A1

Step 1. Set negative integer $D \equiv 0$ or $1 \pmod 4$ such that $h(D)$ is small, where $h(D)$ is the class number of D, and generate a large prime number m such that $2^{400} \leq m \leq 2^{480}$

Step 2. Set a random integer $t \simeq \frac{2^{511}}{m\sqrt{-D}}$ and set $y = 2tm$.

Step 3. Set $p = \frac{2^2 - y^2 D}{4} \simeq 2^{1024}$ and test the primarity of p. If not, go back **Step 2**.

Step 4. Derive the j invariant of an elliptic curve by factoring the Hilbert class polynomial $H(D)$ and set the parameter of the elliptic curve corresponding to j.

The constructed elliptic curve has trace 2 and Tate pairing can be calculated over $\boldsymbol{F}_p$.

The appropriate elliptic curves for the Weil pairing are super-singular elliptic curves[7]. The algorithm for constructing the super-singular elliptic curve over $\boldsymbol{F}_q (q = p^r)$ are given as follows:

Algorithm A2

Step 1. Set negative integer $D \equiv 0$ or $1 \pmod 4$ such that $h(D)$ is small, where $h(D)$ is the class number of D, and set the size of p and $q = p^r$ appropriately.

Step 2. Generate a large prime number p such that $p \simeq \sqrt[r]{q}$ and $\left(\frac{D}{p}\right) = -1$.

Step 3. Compute the super-singular j polynomial assigned to the imaginary quadratic field with the discriminant with D.

Step 4. Check the order of the constructed elliptic curve $\#E/\boldsymbol{F}_q$ and the size of q^k where $\#E/\boldsymbol{F}_q | q^k - 1$. If the size of q^k is larger or smaller than the practical uses, go back **Step 2**.

References

[1] R.Blom, "Non-public key distribution", Proceeding of Crypto'82, pp.231-236, 1982.

[2] A.Shamir, "Identity-based cryptosystems and signature schemes", Proceeding of Crypto'84, pp.47-53, 1984.

[3] T.Matsumoto and H.Imai, "On the key predistribution system: A practical solution to the key distribution problem", Proceeding of Crypto'87, pp.185-193, 1987.

[4] H.Tanaka, "A realization scheme for the identity-based cryptosystem, ", Proceeding of Crypto'87, pp.340-349, 1987.

[5] S.Tsujii, G.Nisio and J.Chao, "An ID-Based Cryptosystem Based on the Discrete Logarithm Problem", IEEE Journal on Selected Areas in Communications, Vol.7, No.4, 1989.

[6] Joseph H. Silverman, "The Arithmetic of Elliptic Curves," Springer-Verlag, 1986.'

[7] A. Menezes, T. Okamoto, S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," IEEE Trans. Inf. Theory 39, pp.1639–1646, 1993.

[8] Ian Blake, Gadiel Seroussi, Nigel Smart, Elliptic Curves in Cryptography, London Mathematical Society Lecture Note Series 265, Cambridge University Press, 1999.

[9] K.Ohgishi, R.Sakai, M.Kasahara, "Notes on ID-based Key Sharing Systems over Elliptic Curve" IEICE Technical Report ISEC99-, Nov.1999.