ID based Cryptosystems with Pairing on Elliptic Curve

Ryuichi SAKAI * Masao KASAHARA †

Abstract

The pairings on elliptic curves have been applied for realizing the secure ID based cryptosystems that can be invulnerable to the collusion attacks. The computation of the pairing are necessary for the cryptosystems, though the computation of the pairing requires high cost compared with the computation cost for the power operation over the finite fields or on the elliptic curve when the parameters are securely to be provided.

In this paper we propose an efficient method for a class of ID based cryptosystems which have been proposed by the present authors. The proposed method is able to reduce the number of the computations for the pairing for verifying the ID based signature and also for decoding of the ID based public key cryptosystems with the authentication, by a factor of 2.

Moreover we propose the ID based public key cryptosystems with signature and the ID based public key cryptosystems having the multiple centers.

1 Introduction

The pairings on elliptic curves are applied for the secure ID based cryptosystems that can be invulnerable to the collusion attacks. The computation of the pairing are necessary for the cryptosystems, though the computation of the pairing requires high cost compared with the computation cost for the power operation over the finite fields or on the elliptic curve when the parameters are securely to be provided.

In this paper we propose an efficient method for the ID based signature scheme and the new ID based public key cryptosystem with the authentication which have been proposed by the present authors [3][4][8][9][10][11]. The proposed method is able to reduce the number of the computations of the pairing for the verification of the ID based signature and also for the decoding of the ID based public key cryptosystems with the authentication, by a factor of 2. Moreover we propose the ID based public key cryptosystems with the signature and the ID based public key cryptosystems having the multiple centers.

2 Reduction of Computation for Verification of ID based signature

2.1 Verification Equation

The equation for verifying the signature will be referred to as the verification equation. The idea of the reducing the computation cost for the verification is based on the modifying of the verification equation.

The type of the verification equation of the ID based signature [8][9] can be described as follows:

$$e_n(aP, bQ) = A \cdot e_n(cP, dQ), \tag{1}$$

or

$$A = e_n(aP, bQ) \cdot e_n(cP, -dQ), \tag{2}$$

where a, b, c and d are appropriately chosen integers in $\mathbb{Z}_n$. Weil pairings or Tate pairings must be computed twice for checking whether the verification equation holds or not. The cost of the computation of the pairing is not small. To improve this, we propose the reduced verification equation as follows:

$$\begin{aligned} e_n(aP + dQ, cP + bQ) &= e_n(aP, cP)e_n(aP, bQ)e_n(dQ, cP), e_n(dQ, bQ)) \\ &= e_n(aP, bQ)/e_n(cP, dQ) = A. \end{aligned} \tag{3}$$

It should be noted that $e_n(P, P) = e_n(Q, Q) = 1$ and $e_n(Q, P) = e_n(P, Q)^{-1}$.

*Faculty of Engineering, Osaka Electro-Communication University, Hatsucho 18–8, Neyagawa-shi, 572-8530 Japan, Email:sakai@isc.osakac.ac.jp

†Faculty of Informatics, Osaka Gakuin University Kishibeminami 2–36–1, Suita-shi, 564-8511 Japan

2.2 Preliminary

The trustful center generates the elliptic curve such that the pairing on the curve can be computed and the discrete logarithm problem on the curves and over the group of the n-th group formed by the values of the pairing are difficult. We assume here that n is a 160bits prime from a practical point of view. [1] The center chooses 2 n-torsion points $P, Q \in E[n]$ such that $\langle P \rangle \neq \langle Q \rangle$ and the random integer $l \in \mathbb{Z}_n$. Let I_U denotes the identity(ID) information of user **U** where $E[n]$ is an n-torsion group of $E(\mathbb{F}_{q^\gamma})$. The trustful center publicizes the algorithms $e_n(\ ,\ )$ and $f()$, where $e_n(\ ,\ )$ is a pairing and $f()$ is a one way function which embeds the ID information I_U to the element $P_U = f(I_U)$ of the n-torsion group $E[n] \in E(\mathbb{F}_{q^\gamma})$. The center then computes $K_U = lP_U$ and sends K_U secretly to the user **U**.

2.3 Conventional ID based Signature with Pairings(ElGamal Type)

The ElGamal type signature scheme can be described as follows[8][9] :

Signature : The signer **A** generates the signature $\{R, S\}$ of the message m as follows:

$$R = kQ = (x_R, y_R), \tag{4}$$

$$S = \frac{h(m)}{k}P_A + \frac{x_R}{k}K_A = \frac{h(m) + x_R l}{k}P_A. \tag{5}$$

Verification : The verifier **V** can verify the signature $\{R, S\}$ by checking if the following verification equation holds or not:

$$e_n(S, R) = e_n(P_A, h(m)Q + x_R lQ). \tag{6}$$

The verifier must compute the pairings twice for checking if the above equation holds or not.

On the other hand, the above verification equation can be represented as Eq(1), where $A = 1$,

$$a = \frac{h(m) + x_R l}{k}, \quad b = k, \quad c = 1, \quad d = h(m) + x_R l.$$

Consequently, the verifier **V** can verify the signature $\{R, S\}$ by checking if the following equation holds or not:

$$e_n(S + h(m)Q + x_R(lQ), P_A + R) = e_n(S, R)e_n(P_A, (h(m) + x_R l)Q)^{-1} = 1. \tag{7}$$

Note that the verifier can verify the signature by computing a pairing only once with this equation.

2.4 Conventional ID based Signature with Pairings(Schnorr Type)

The Schnorr type signature scheme can be described as follows[9]:

Signature : The signer **A** generates the signature $\{e, S\}$ of the message m as follows:

$$r = e_n(P_A, kQ) = e_n(P_A, Q)^k, \tag{8}$$

$$e = h(m||r), \tag{9}$$

$$S = eK_A + kP_A = (el + k)P_A. \tag{10}$$

Verification : The verifier **V** can verify the signature $\{e, S\}$, by checking if the following verification equations hold or not:

$$w = e_n(S, Q)e_n(P_A, -elQ) = e_n(P_A, Q)^k, \tag{11}$$

$$e = h(m||w). \tag{12}$$

The verifier must compute the pairings twice for checking if the above equation holds or not.

On the other hand, the above verification equation can be represented as Eq.(3). Therefore, the verifier **V** can compute w by the following equation:

$$\begin{aligned} w &= e_n(S + elQ, P_A + Q) \\ &= e_n(S, P_A)e_n(S, Q)e_n(elQ, P_A)e_n(elQ, Q) \\ &= e_n(S, Q)e_n(P_A, -elQ). \end{aligned} \tag{13}$$

Note that the verifier can verify the signature by computing a pairing only once with this equation.

[1] The group formed by the values of pairing equal to the group of n-th root of unity on $\mathbb{F}_{q^\gamma}$. In order to the discrete logarithm over these groups become difficult, n has a prime factor of size 160bits or lager.

3 Reduction of Computation for ID based Public Key Cryptosystems

3.1 Preliminary

The trustful center generates an elliptic curve such that the pairing on the curve can be computed and the discrete logarithm problem on the curves and over the group of the n-th group formed by the values of the pairing are difficult. The center chooses 2 n-torsion points $P, Q \in E[n]$ such that $\langle P \rangle \neq \langle Q \rangle$ and the random polynomial $f(x)$ over $\mathbb{Z}_n$ such that

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0. \tag{14}$$

The center then publicizes the algorithms $e_n(\ ,\ )$, and public information $a_i Q \in E[n]$ $(i = 0, \cdots, d)$ and $y = e_n(P, Q) \in \mathbb{F}_{q^\gamma}$.[2] Finally, the center computes **U**'s secret key K_U as follows:

$$K_U = \frac{1}{f(I_U)} P, \tag{15}$$

and sends K_U secretly to the user **U**.

3.2 ID based Public Key Cryptosystem with Authentication

When using the keys described above[10], it is difficult to construct the ID based key sharing scheme. However, the ID based public key can be modified to the ID based public key cryptosystems with the authentication [11].

Encryption : The sender **B** chooses 2 random integers r and k and encrypts the message m for the receiver **A** as follows:

$$\begin{aligned} C_1 &= r \sum_{i=0}^{d} {I_A}^i a_i Q + k K_B \\ &= r f(I_A) Q + \frac{k}{f(I_B)} P, \end{aligned} \tag{16}$$

$$C_2 = m \oplus y^{r+k}. \tag{17}$$

The sender sends the encrypted data C_1, C_2 to the receiver **A**.

Decryption : Using the secret key K_A, the receiver **A** can decrypt the message as follows:

$$C_2 \oplus e_n(K_A,\ C_1)\ e_n\left(C_1,\ \sum_{i=0}^{d} {I_B}^i a_i Q\right) \tag{18}$$

$$\begin{aligned} &= m \oplus y^{r+k} \oplus y^r y^k \\ &= m. \end{aligned} \tag{19}$$

On the above equation, for the given n-torsion points $P, Q, R \in E[n]$, the following product must be computed:

$$e_n(P, R) e_n(R, Q). \tag{20}$$

The product of the pairings can be reduced to a pairing by the binomial property as

$$\begin{aligned} e_n(P, R) e_n(R, Q) &= e_n(P, R) e_n(-Q, R) \\ &= e_n(P - Q, R). \end{aligned} \tag{21}$$

Therefore, the above decryption can be computed as follows:

$$C_2 \oplus e_n\left(K_A - \sum_{i=0}^{d} {I_B}^i a_i Q,\ C_1\right)$$

[2] It should be noted that if the user **U** has already received the key K_U, the user can generate y as follows :

$$y = e_n(K_U, \sum_{i=0}^{d} {I_U}^i a_i Q) = e_n(K_U, f(I_U) Q) = e_n(P, Q).$$

$$
\begin{aligned}
&= C_2 \oplus e_n\left(\frac{1}{f(I_A)}P - f(I_B)Q,\ rf(I_A)Q + \frac{k}{f(I_B)}P\right) \\
&= y^{r+k} \oplus e_n\left(\frac{1}{f(I_A)}P,\ rf(I_A)Q\right) e_n\left(\frac{k}{f(I_B)}P,\ f(I_B)Q\right) \\
&= m \oplus y^{r+k} \oplus y^r y^k \\
&= m. \qquad (22)
\end{aligned}
$$

3.3 ID based Public Key Cryptosystem with Signature

The ID based public key cryptosystem with the authentication described in 3.2 cannot prevent the receiver from substituting another message for the encrypted message. Therefore, the system cannot be used for the signature scheme. Modifying the ID based public key cryptosystem with the authentication described in 3.2, we can construct a new ID based public key cryptosystem with the signature as we shall show below.

Encryption : The sender **B** chooses random integers r, k and encrypts the message m for the receiver **A** as follows:

$$
\begin{aligned}
C_1 &= k\left(\sum_{i=0}^{d} {I_A}^i a_i Q + h(m)K_B\right) \\
&= k\left(f(I_A)Q + \frac{h(m)}{f(I_B)}P\right), \qquad (23) \\
C_2 &= m \oplus y^{k(1+h(m))}. \qquad (24)
\end{aligned}
$$

The sender **B** then sends the encrypted data C_1, C_2 to the receiver **A**.

Using the secret key K_A, the receiver **A** can decrypt and verify the message as follows:

Decryption :

$$
\begin{aligned}
D &= e_n\left(K_A - \sum_{i=0}^{d} {I_B}^i a_i Q,\ C_1\right) = y^{k(1+h(m))}, \qquad (25) \\
m &= C_2 \oplus D. \qquad (26)
\end{aligned}
$$

Verification :

$$
e_n\left(K_A,\ C_1\right)^{(1+h(m))} = D. \qquad (27)
$$

Another computation of the decryption and verification for the new ID based public key cryptosystem with the signature can be given as follows:

Decryption :

$$
\begin{aligned}
D_1 &= e_n\left(K_A,\ C_1\right) = y^k, \qquad (28) \\
D_2 &= e_n\left(C_1,\ \sum_{i=0}^{d} {I_B}^i a_i Q\right) = y^{kh(m)}, \qquad (29) \\
m &= C_2 \oplus D_1 D_2. \qquad (30)
\end{aligned}
$$

Verification :

$$
D_1^{h(m)} = D_2. \qquad (31)
$$

4 Multiple Centers

4.1 Conventional Cryptosystems

It is easy to modify the conventional ID based cryptosystems to the systems having the multiple center as we shall show in the following[1][2].

We assume here that L centers are exist. The i-th center C_i chooses a random integer $l_i \in \mathbb{Z}_n$ and computes the secret key for the user **A** as

$$K_{Ai} = l_i P_A. \tag{32}$$

The user then computes his or her secret key by

$$K_A = \sum_{i=1}^{L} K_{Ai} = \sum_{i=1}^{L} l_i P_A. \tag{33}$$

4.2 Key Generation

For the ID based public key cryptosystems and the signature schemes proposed in [10], it is difficult to establish the multiple key generation centers. In this section, we present a new method for the establishing of two centers.

The 1st center and the 2nd center generate the secret key of the system as follows:

$$f(x) = a_0 + a_1 x, \tag{34}$$
$$g(x) = b_0 + b_1 x. \tag{35}$$

The 1st center generates the public key as sa_0Q, sa_1Q and the 2nd center generates the public key, tb_0P, tb_1P. The 1st center then generates the private key of user **A** as

$$k_A = \frac{1}{f(I_A)} P, \tag{36}$$

and the 2nd center generates the private key of user **A** as

$$\tilde{k_A} = \frac{1}{g(I_A)} Q. \tag{37}$$

Then the user **A** computes the private key by

$$K_A = k_A - \tilde{k_A} = \frac{1}{f(I_A)} P - \frac{1}{g(I_A)} Q. \tag{38}$$

The additional public keys of the centers are y^s, y^t where $y = e_n(P, Q)$.

4.3 Public Key Cryptosystem

Using the key described above, the sender can encrypt the message m in the following way.

Encryption :

The sender chooses a random integer k and encrypts the message m for the receiver **A** as follows:

$$C_1 = k(sa_0Q + I_A sa_1 Q + tb_0 P + I_A tb_1 P)$$
$$= ksf(I_A)Q + ktg(I_A)P, \tag{39}$$
$$C_2 = m \oplus y^{k(s+t)}. \tag{40}$$

Decryption : Using the secret key K_A, the receiver **A** can decrypt the message as follows:

$$C_2 \oplus e_n(K_A,\ C_1) = m \oplus y^{k(s+t)} \oplus e_n(ksP, Q) e_n(-Q, ktP)$$
$$= m. \tag{41}$$

4.4 Signature Scheme

Using the key described above, the signer can sign the message m in the following ways.

[ElGamal TYPE]

Signature : The signer **A** chooses a random integer k and generates the signature $\{R, S\}$ of the message m as follows :

$$R = ksf(I_A)Q + ktg(I_A)P = (x_R, y_R), \tag{42}$$
$$S = \frac{h(m)}{k}(P - Q) + \frac{x_R}{k} K_A$$
$$= \frac{h(m)f(I_A) + x_R}{kf(I_A)} P - \frac{h(m)g(I_A) + x_R}{kg(I_A)} Q. \tag{43}$$

Verification : The verifier **V** can confirm the validity of the signature $\{R, S\}$, when the following equations hold :

$$\begin{aligned} e_n(S,R) &= y^{h(m)(sf(I_A)+tg(I_A))+(s+t)x_R}, \quad (44) \\ &= \left((y^{sa_0}y^{tb_0})(y^{sa_1}y^{tb_1})^{I_A}\right)^{h(m)} y^{(s+t)x_R}. \end{aligned}$$

[Schnorr TYPE]
Signature : An signature set $\{e, S\}$ of the message m is computed by

$$\begin{aligned} r &= \left(y^{sf(I_A)+tg(I_A)}\right)^k \quad (45) \\ e &= h(m||r), \quad (46) \\ S &= eK_A + k(P-Q) \\ &= \left(\frac{e}{f(I_A)}+k\right)P - \left(\frac{e}{g(I_A)}+k\right)Q. \quad (47) \end{aligned}$$

Verification : The verifier **V** can confirm the validity of the signature $\{e, S\}$ when the following equations hold :

$$\begin{aligned} w &= e_n(S, sf(I_A)Q + tg(I_A)P) \cdot y^{-e(s+t)} \\ &= y^{k(sf(I_A)+tg(I_A))}, \quad (48) \\ e &= h(m||w). \quad (49) \end{aligned}$$

5 Conclusions

We have proposed the efficient method for a class of ID based cryptosystems, the ID based public key cryptosystem with signature and the ID based cryptosystems having the multiple centers.

References

[1] Kiyoshi Ohgishi, Ryuichi Sakai and Masao Kasahara, "Notes on ID-based Key Sharing Systems over Elliptic Curve", Technical Report of IEICE, ISEC99-57, Nov.1999.

[2] Ryuichi Sakai, Kiyoshi Ohgishi and Masao Kasahara, "Cryptosystems Based on Pairing", Proc. of SCIS2000,C20,Jan.2000.

[3] Ryuichi Sakai, Kiyoshi Ohgishi and Masao Kasahara, "Crypt schemes based on Weil Pairing", preprint. May,2000.

[4] Ryuichi Sakai, Kiyoshi Ohgishi and Masao Kasahara, "Cryptosystems based on Pairing over Elliptic Curve", Proc. of SCIS2001,7B-2,Jan.2001.

[5] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing", Proc. of CRYPTO 2001, LNCS vol.2139 , Springer-Verlag, pp. 213-229, 2001.

[6] Shigeo Mitsunari, Ryuichi Sakai and Masao Kasahara, "A New Traitor Tracing", IEICE Trans. Vol. E85-A, No.2, pp. 481–484, Feb.2002.

[7] Ryuichi Sakai, Shigeo Mitsunari and Masao Kasahara, "Cryptographic Schemes based on Pairing over Elliptic Curve", Technical Report of IEICE, ISEC2001-29, Jul.2001.

[8] Kenneth G. Paterson, "ID-based Signature from Pairings on Elliptic Curves", IACR eprint 004/2002.

[9] Ryuichi Sakai and Masao Kasahara, "Cryptographic Schemes based on Pairing over Elliptic Curve(Part2)", Technical Report of IEICE, ISEC2002-52, Jul.2002.

[10] Ryuichi Sakai and Masao Kasahara, "Cryptographic Schemes based on Pairing over Elliptic Curve(Part3)", Technical Report of IEICE, ISEC2002-63, Sep.2002.

[11] Ryuichi Sakai and Masao Kasahara, "Cryptosystems based on Pairing over Elliptic Curve" Proc. of SCIS2003,8C-1,Jan.2003.