Commun. Korean Math. Soc. **20** (2005), No. 3, pp. 611–621

AN IDENTITY BASED AUTHENTICATED KEY AGREEMENT PROTOCOL ON THE TATE PAIRING

Suk Bong Yoon

Abstract. This paper introduces an ID based authenticated two pass key agreement protocol of Smart[4] which used the Weil pairing. We propose other an ID based authenticated two pass key agreement protocol which using the Tate Pairing. We will compare protocol of Smart with this protocol.

1. Introduction

Modern protocol for key agreement was based on the Diffie-Hellman protocol, however this protocol is not key authenticated, so Diffie-Hellman protocol suffers from the man-in-the-middle attack because it does not authenticated the communicating parties. A solution for this problem is to combine a key agreement protocol with a digital signature scheme, so-called an authenticated key agreement protocol(or AK protocol) ([6, 8]). In [4], N. P. Smart proposed an AK protocol using the Weil pairing. The Weil pairing and Tate pairing are used to attack for elliptic curve cryptosystem. Recently the Weil and Tate pairing have been used to construct cryptosystem such as the tripartite Diffie-Hellman protocol of Joux[5], the identity-based encryption scheme of Boneh and Franklin[1], the short signature scheme of Boneh, Lynn and shacham[10], and so on.

Tate pairing is more efficient than the Weil pairing for computation. In section 7, we will show that the computation of Tate pairing is faster than, that of Weil pairing. This paper propose an identity based authenticated key agreement protocol using the Tate pairing.

Received April 14, 2005.

Key words and phrases: Enge-Gaudry index calculous algorithm, GHS Weil descent attack, relation of hyperelliptic curve parameters.

This work was supported by Dongeui University Research Foundation Grant (2002AA084).

We now summarize the paper, section 2 introduces the elliptic curve, section 3 introduce key exchange protocol of Diffie-Hellman and man-in-the-middle attack on the Diffie-Hellman protocol, section 4 describes the basics of the Weil pairing and Tate pairing, section 5 introduces an AK protocol(ID based authenticated key agreement protocol based on the Weil pairing) of Smart[4], section 6 proposes other protocol based on the Tate pairing, section 7 shows example of pairings, section 8 show conclusion.

2. Elliptic curve

Let $E/\mathbb{F}_q$ be an elliptic curve given by the smooth Weierstrass equation.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 - (*)$$

where $a_1, a_2, a_3, a_4, a_5 \in \mathbb{F}_q$.

Let $\mathbb{K}(= \mathbb{F}_q)$ be a finite field with $q = p^m$ elements, where p is prime and $m \geq 1$. The ECDLP in $E/\mathbb{F}_\mathbf{q}$ is defined to find $0 \leq l \leq n-1$ such that $R = lP$ given $P \in E(\mathbb{K})$ and $R \in < P >$, where n is the order of the finite cyclic group $< P >$. $E(\mathbb{K}) := \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid (x, y) \text{ satisfies } (*)\} \cup \{O\}$ is called the set of $\mathbb{K}$-rational points of an elliptic curve E, where O is the identity element of the group. The following quantities are related to E,

$$\begin{aligned}
&b_2 = {a_1}^2 + 4a_2 \\
&b_4 = 2a_4 + a_1a_3 \\
&b_6 = {a_3}^2 + 4a_6 \\
&b_8 = {a_1}^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2{a_3}^2 - {a_4}^2 \\
&c_4 = {b_2}^2 - 24b_4 \\
&\Delta = -{b_2}^2b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2b_4b_6 \\
&j(E) = {c_4}^3/\Delta.
\end{aligned}$$

The quantity Δ is called the discriminant of the Weierstrass equation, while $j(E)$ is called the j-invariant of E if $\Delta \neq 0$.

Elliptic curves can be simplified over fields of different characteristics by means of coordinate transformation. If char($\mathbb{K}$) $\neq 2$, the first step is completing the square on the left hand side of the Weierstrass equation. The corresponding admissible change of variables $(x, y) \mapsto (x, y - \frac{1}{2}(a_1x + a_3))$ transforms E to an equation

$$E' : y^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

If furthermore $\mathrm{char}(\mathbb{F}) \neq 3$, a similar process can be applied to the right hand side for eliminating the x^2 term. The transformation $(x, y) \mapsto (x - \frac{1}{3}a_2{}', y)$ yields

$$E'' : y^2 = x^3 + a_4''x + a_6''.$$

If $\mathrm{char}(\mathbb{K}) = 3$, we want to eliminate at least one of the terms in equation E' . If $a_2{}' = 0$ (i.e., $j' = \frac{a_2{}'^6}{\Delta} = 0$ for $\Delta \neq 0$), E is already the desired normal form. Otherwise the substitution $(x, y) \mapsto (x + \frac{a_4{}'}{a_2{}'}, y)$ yields a curve of the form

$$E'' : y^2 = x^3 + a_2{}''x^2 + a_6{}''.$$

For $\mathrm{char}(\mathbb{K}) = 2$, a similar case distinction starting with E is necessary. If $a_1 = 0$, which means $j = \frac{a_1{}^{12}}{\Delta} = 0$ for $\Delta \neq 0$, the substitution $(x, y) \mapsto (x + a_2, y)$ additionally eliminates the x^2 term. Otherwise the admissible change of variables $(x, y) \mapsto (a_1{}^2x + \frac{a_3}{a_1}, a_1{}^3y + \frac{a_1{}^2a_4 + a_3{}^2}{a_1{}^3})$ results in a curve of the form

$$E'' : y^2 + xy = x^3 + a_2{}''x^2 + a_6{}''.$$

It is well known that the points on an elliptic curve from an abelian group under a certain addition. Let E be an elliptic curve given by the Weierstrass equation $(*)$. Let E be an elliptic curve over the real numbers, and let P and Q be two points on E. Then the addition rules are given. If P is the point at infinity O, then $-P$ is also O, and $P+Q = Q + P = Q$. This means that O will act as the additive identity of the group of points. If $P = (x_1, y_1) \neq O$, then $-P = (x_1, -y_1 - a_1x_1 - a_3)$. If P and Q have different x-coordinate, then we can see that the line intersects the curve in exactly one more point R. Then define $P + Q$ to be $-R$. If $Q = -P$ then we define $P + Q = O$. The last possibility is if $P = Q$. If this conditions is true, l would then be the tangent line to the curve at P. Thus "+" makes E into an abelian group with identity element O .

3. Diffie-Hellman key exchange

In 1976, Diffie and Hellman in their seminal paper ([9]) on public key cryptography described a protocol whereby two people, A and B, can derive and share common piece of secret information over an insecure communications channel. We describe this protocol, known as the Diffie-Hellman key exchange, in terms of an arbitrary group.

<Diffie-Hellman key exchange>

Setup: A and B publicly select a finite group G and an element $\alpha \in G$

	A		B
1. private key	$a \in G$	$\leftrightarrows$	$b \in G$
2. compute	α^a		α^b
3. compute	$(\alpha^b)^a = \alpha^{ab}$		$(\alpha^a)^b = \alpha^{ab}$

A and B now share the common group element α^{ab}. This protocol is not an authenticated key exchange since any third party C could impersonate either A or B. However, the protocol can easily be modified by requiring a central trusted authority to certify ahead of time the element α^a for each user A.

This protocol suffers from the man-in-the-middle attack. Suppose an adversary C in capable of intercepting A's communications with B, impersonating A to the other entity and impersonating the other entity to A. We write $C(A)$ to indicate that the adversary C is impersonating A in sending or receiving messages intended for or originating from A. Similarly, $C(B)$ denotes an adversary impersonating B. Let $x, y \in \mathbb{Z}_q{}^*$ be random values of C's choice. We assume that A initiates a run of Diffie-Hellman protocol. The man-in-the-middle attack is then executed as follow:

1. $C(B)$ intercepts α^a from A, and $C(A)$ forwards α^x to B.
2. $C(A)$ intercepts α^b from B,and $C(B)$ forwards α^y to A.

At the end of this attack, C impersonating A has agreed a key $K_{C(A)B} = \alpha^{xb}$ with B, while C impersonating B has agreed a second key $K_{AC(B)} = \alpha^{ay}$ with A. If these keys are used to encrypt subsequent communications, then C, by appropriately decrypting and re-encrypting messages, can now continue his masquerade as A to B and B to A.

4. The Weil and Tate pairing

In this section we shall summarize the properties of the Weil and Tate pairing.

4.1. The Weil pairing

We let E be an elliptic curve over the field F_q with $q = p^m$ elements (p is prime, and $m \geq 1$). Let l be a positive integer coprime to p, and let μ_l be the group of l^{th} roots of unity and let $E[l]$ define a prime order subgroup of an elliptic curve. Let $P, Q \in E[l]$ and let A and B be divisors of degree 0 such that $A \sim (P) - (O), B \sim (Q) - (O)$, and A, B have disjoint support. Let $f_A, f_B \in \mathbb{K}(E)$ such that $div(f_A) = lA, div(f_B) = lB$. We now define the Weil Pairing, e_l, is a map

$$e : E[l] \times E[l] \mapsto \mu_l$$

and is define as $e(P,Q) = f_A(B)/f_B(A)$.

This map satisfies the following properties :

1. Identity : For all $P \in E[l], e(P,P) = 1$.
2. Alternation : For all $P, Q \in E[l], e(P,Q) = e(Q,P)^{-1}$.
3. Bilinearity : For all $P, Q, R \in E[l], e(P+Q,R) = e(P,R) \cdot e(Q,R)$ and $e(P, Q+R) = e(P,Q) \cdot e(P,R)$.
4. Non-degeneracy : If $P \in E[l]$ then $e(P,O) = 1$. Moreover, if $e(P,Q) = 1$ for all $Q \in E[l]$, then $P = O$.
5. If $E[l] \subseteq E(\mathbb{K})$, then $e(P,Q) \in \mu_l$ for all $P, Q \in E[l]$.

We can compute the Weil pairing. Let l be an integer coprime to p, and let $P, Q \in E[l]$. Pick points $T, U \in E$ such that $P + T \neq U, Q + U$ and $T \neq U, Q + U$. Let $A = (P+T) - (T)$, then

$A \sim (P) - (O)(\because A - (P) + (O) = (P) + (T) - (T) - (P) + (O) \in \text{Prin}(E))$.

Similarly, let $B = (Q+U) - (U)$ then $B \sim (Q) - (0)$. Let $f_A, f_B \in \mathbb{K}(E)$ with $\text{div}(f_A) = l(P+T) - l(T), \text{div}(f_B) = l(Q+U) - l(U)$, then

$$e(P,Q) = \frac{f_A(B)}{f_B(A)} = \frac{f_A((Q+U)-(U))}{f_B((P+T)-(T))} = \frac{f_A(Q+U) \cdot f_B(T)}{f_A(U) \cdot f_B(P+T)}.$$

We now define the modified Weil pairing[1]. Let G denoted a prime order subgroup of an elliptic curve E over the field $\mathbb{F}_q$.

The modified Weil pairing is a map

$$\hat{\text{e}} : G \times G \to F^*{}_{q^k},$$

defined by $\hat{\text{e}}(P,Q) = e(P, \phi(Q))$ where ϕ is an automorphism of the group of points on the elliptic curve E.

This map satisfies the following properties:

1. Bilinearity :

$$\hat{e}(P+R,Q) = \hat{e}(P,Q) \cdot \hat{e}(R,Q),$$
$$\hat{e}(P,R+Q) = \hat{e}(P,R) \cdot \hat{e}(P,Q).$$

2. Non-degeneracy : There exists a $P \in G$ such that $\hat{e}(P,P) \neq 1$.
3. Computable : One can compute $\hat{e}(P,Q)$ in polynomial time.

The Weil pairing was introduced into cryptography by Menezes, Okamoto and Vanstone[2] who used it to attack the elliptic curve discrete logarithm problem on certain elliptic curve. We note that pairings have recently been used to create several cryptographic primitives, including

ID-based encryption ([1]) and signature schemes, as well as an identity-based authenticated key agreement protocol ([4]). Our focus in this paper is to construct the ID-based authenticated two pass key agreement protocol based on the Tate pairing.

4.2. Tate pairing

The Tate pairing was introduced into cryptography by Frey and Rück[3] in their extension of the work of Menezes, Okamoto and Vanstone. We use the same notation as in [11].

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Let l be a positive integer coprime to p. In most applications l is a prime and $l|(q-1)$. Let k be a positive integer such that the field $\mathbb{F}_{q^k}$ contains the l^{th} roots of unity (in other word, $l|(q^k-1)$). Let $G = E(\mathbb{F}_{q^k})$ and write $G[l]$ for the subgroup of points of order l and G/lG for the quotient group (which is also a group of exponent l). Then the Tate pairing is a mapping

$$t : G[l] \times G/lG \to {\mathbb{F}^*}_{q^k}/({\mathbb{F}^*}_{q^k})^l.$$

The Tate pairing is defined as follows. Given the point P there is a function g such that the divisor of g is equal to $l(P) - l(O)$. There is a divisor D is disjoint from the support of g, then the value of the tate pairing is

$$t(P,Q) = g(D),$$

where $g(D) = \prod_i g(P_i)^{n_i}$ if $D = \sum_i n_i(P_i)$.

The Tate pairing satisfies the following properties :

1. Well-defined : $t(O,Q) = 1$ for all $Q \in G/lG$ and
$$t(P,Q) = 1 \text{ for all } P \in G[l], Q \in G/lG.$$
2. Bilinearity : For any $P, R \in G, t(P+R,Q) = t(P,Q) \cdot t(R,Q)$.
3. Non-degeneracy : If $t(P,Q) = 1$ for all $Q \in G/lG$ then $P = O$.

We define the modified Tate pairing :

$$\hat{t}\colon G[l] \times G/lG \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^l$$

defined by $\hat{t}(P,Q) = t(P,\phi(Q))$ where ϕ is an automorphism of the group of points on the elliptic curve E.

5. ID based authenticated two pass key agreement protocol based on the Weil pairing

In [4], N. P. Smart proposed an AK protocol using the Weil pairing. We now describe this protocol.

Suppose that a subgroup of an elliptic curve for which the modified Weil pairing ê maps into the finite field $\mathbb{F}_{q^k}$. We assume that the elliptic curve contains a large prime subgroup of order l, such that solving discrete logarithms in the subgroup of order l is also infeasible.

Suppose two users A and B wish to agree a key. The key generation center choose secret key $s \in \{1, ..., l-1\}$. The key generation center produces a random $P \in G$ and computes $P_{KGS} = [s]P$. Then key generation center publishes P and P_{KGS}. When users A and B with identity(ID) wishes to obtain a public/private key pair, the public key is given by

$$Q_{ID(A)} = H(ID(A)), Q_{ID(B)} = H(ID(B)),$$

where H is a cryptographic hash function($H : \{0,1\}^* \to G$). The key generation center computes the associated private key via

$$S_{ID(A)} = [s]Q_{ID(A)}, S_{ID(B)} = [s]Q_{ID(B)}.$$

A and B choose a ephemeral privative key a and b respectively.

<Authenticated Key Exchange>

$$\begin{array}{ccc} \text{User A} & & \text{User B} \\ a & & b \\ T_A = [a]P & \longrightarrow & T_A \\ T_B & \longleftarrow & T_B = [b]P \end{array}$$

User A compute : $k_A = \hat{e}([a]Q_{ID(B)}, P_{KGS}) \cdot \hat{e}(S_{ID(A)}, T_B)$
User B compute : $k_B = \hat{e}([b]Q_{ID(A)}, P_{KGS}) \cdot \hat{e}(S_{ID(B)}, T_A)$

Therefore, the agreement secrete key is $k = V(k_A) = V(k_B)$, where V is a key derivation function ($V : \mathbb{F}^*{}_{q^k} \to \{0,1\}^*$).
We show that the secrete shared keys agree,

$$\begin{aligned} k_A &= \hat{e}([a]Q_{ID(B)}, P_{KGS}) \cdot \hat{e}(S_{ID(A)}, T_B) \\ &= \hat{e}(Q_{ID(B)}, P)^{as} \cdot \hat{e}(Q_{ID(A)}, P)^{bs} \\ &= \hat{e}(S_{ID(B)}, T_A) \cdot \hat{e}([b]Q_{ID(A)}, P_{KGS}) \\ &= \hat{e}([b]Q_{ID(A)}, P_{KGS}) \cdot \hat{e}(S_{ID(B)}, T_A) \\ &= k_B. \end{aligned}$$

6. ID based authenticated two pass key agreement protocol based on the Tate pairing

We now construct AK protocol using the Tate pairing. We protocol have two message flows. In the first setup step, the key generation center choose two random points $P, Q \in G$.

Suppose two users A and B wish to agree a key. We assume that the elliptic curve contains a large prime subgroup of order l, such that solving discrete logarithms in the subgroup of order l is also infeasible.

Step 1. Key generation center choose a secret key :

$$s \in \{1, ..., l-1\}$$

and compute $P_{KGS_1} = [s]P$, $P_{KGS_2} = [s]Q$,

Step 2. Key generation center publishes :

$$(P, Q, P_{KGS_1}, P_{KGS_2})$$

Step 3. Public key of users :

$$Q_{ID(A)}, = H(ID(A)),\ Q_{ID(B)} = H(ID(B)),$$

where H is cryptographic hash function$(H : \{0,1\}^* \to G)$.

Step 4. Key generation center generate private key of users,

$$S_{ID(A)} = [s]Q_{ID(A)}, S_{ID(B)} = [s]Q_{ID(B)}$$

A and B choose a ephemeral privative key a and b respectively.

<Authenticated Key Exchange>

$$\begin{array}{ccc}
\text{User A} & & \text{User B} \\
a & & b \\
T_{A_1} = [a]P, T_{A_2} = [a]Q & \longrightarrow & (T_{A_1}, T_{A_2}) \\
(T_{B_1}, T_{B_2}) & \longleftarrow & T_{B_1} = [b]P, T_{B_2} = [b]Q
\end{array}$$

User A compute : $k_A = \hat{t}([a]Q_{ID(B)}, P_{KGS}) \cdot \hat{t}(S_{ID(A)}, T_B)$

User B compute : $k_B = \hat{t}([b]Q_{ID(A)}, P_{KGS}) \cdot \hat{t}(S_{ID(B)}, T_A)$,

where $P_{KGS} = (P_{KGS_1}) - (P_{KGS_2})$, $T_A = (T_{A_1}) - (T_{A_2})$, $T_B = (T_{B_1}) - (T_{B_2})$. Therefore the agreement secrete key is $k = V(k_A) = V(k_B)$, where V is a key derivation function$(V : \mathbb{F}^*{}_{q^k} \to \{0,1\}^*)$.

THEOREM. The secrete shared keys agree with users A and B.

PROOF.

$$\begin{aligned} k_A &= \hat{t}([a]Q_{ID(B)}, P_{KGS}) \cdot \hat{t}(S_{ID(A)}, T_B) \\ &= \hat{t}(Q_{ID(B)}, ([s]P) - ([s]Q))^a \cdot \hat{t}([s]Q_{ID(A)}, ([b]P) - ([b]Q)) \\ &= \hat{t}(Q_{ID(B)}, (P) - (Q))^{as} \cdot \hat{t}(Q_{ID(A)}, (P) - (Q))^{bs} \\ &= \hat{t}([s]Q_{ID(B)}, [a](P) - [a](Q)) \cdot \hat{t}([b]Q_{ID(A)}, [s](P) - [s](Q)) \\ &= \hat{t}(S_{ID(B)}, T_A) \cdot \hat{t}([b]Q_{ID(A)}, P_{KGS}) \\ &= \hat{t}([b]Q_{ID(A)}, P_{KGS}) \cdot \hat{t}(S_{ID(B)}, T_A) \\ &= k_B. \end{aligned}$$

7. Example of pairings

In this section, we compare Weil pairing with Tate pairing for computation speed. This example describes in [12].

EXAMPLE 1. We consider the elliptic curve $E/\mathbb{F}_p : y^2 = x^3 + 1$. where $p = 5ffffffffac04f444cfea7cea7efae05bf8cc5aaa1 (\approx 2^{160})$ and $|E(\mathbb{F}_p)| = p + 1 = 5ffffffffac04f444cfea7cea7efae05bf8cc5aaa2$. Then the pair of points in $E(\mathbb{F}_q)$ is mapping to $\mathbb{F}_{p^2}$ by Weil pairing. Choose random two points $P, R \in E(\mathbb{F}_p)$.

$P = (51c11cb2f0c6040d13ce61a46f35b9b0550826b0b,$
$\qquad 4b189455128463a7c89e3953ded75cc822db4a23c),$

$R = (5b7f372f122c17796f4025e31af03c1def5147a23,$
$\qquad 29f5eac67fe67f939da0fba97d8b99f8ba2cecb9),$

then $e(P, Q) = a_1\alpha + a_0 \in \mathbb{F}_{p^2}$ with $a_1, a_0 \in \mathbb{F}_p$ where

$$a_1 = 47902f1efaaf3c3770e750388320048e9aaa86073$$
$$a_0 = 19f98d92d4f0e1c6ba6d8d8d62e403047de0b3d8d$$

and $e(R, Q) = b_1\alpha + b_0 \in \mathbb{F}_{p^2}$ with $b_0, b_1 \in \mathbb{F}_p$ where

$$b_1 = 5e1f60f1d79d2ef2d723a9b0d6b70272a90ba492c$$
$$b_0 = 522798105affc6baf315af0c21a35901f07da3dd9.$$

Then the time of computing $e(P, Q), e(R, Q)$: 47.828 sec(CPU : Pentium 650 MHz).

EXAMPLE 2. We consider the elliptic curve $E/\mathbb{F}_p : y^2 = x^3 + 1$. where $p = 5ffffffffac04f444cfea7cea7efae05bf8cc5aaa1 (\approx 2^{160})$ and $|E(\mathbb{F}_p)| = p + 1 = 5ffffffffac04f444cfea7cea7efae05bf8cc5aaa2$. Then the pair of points in $E(\mathbb{F}_q)$ is mapping to $\mathbb{F}_{p^2}$ by Tate pairing. Choose random two points $P, R \in E(\mathbb{F}_p)$.

$P = (163882c78e8378ded60e7c23116a6ba57b4b69036,$

$$\begin{aligned} &\quad 3618be44e80f49aca3482c00b45697e518ab1a66b), \\ R = &(5797abdf028c47eb97949ffabab8223b486409eff, \\ &\quad 1e70e3a03be3befb5004022f370850ca0a13d10b3), \end{aligned}$$

then $t(P, Q) = a_1\alpha + a_0 \in \mathbb{F}_{p^2}$ with $a_1, a_0 \in \mathbb{F}_p$ where

$$\begin{aligned} a_1 &= 1a43a6ae8b2cea2d654e2f10af270164f397c99e7, \\ a_0 &= 37390e1e03f49121dd4bb72a024cd1111f4e8ce7. \end{aligned}$$

and $t(R, Q) = b_1\alpha + b_0 \in \mathbb{F}_{p^2}$ with $b_0, b_1 \in \mathbb{F}_p$ where

$$\begin{aligned} b_1 &= 38fcbf9e98bdb58526b3d4355d256542c19358033, \\ b_0 &= 5885462a0490494a237fd4b01496bc9d27f637c76. \end{aligned}$$

Then the time of computing $t(P, Q), t(R, Q)$: 15.242 sec(CPU : Pentium 650 MHz).

In example 1 and example 2, we can find that computation of Tate pairing is faster than that of Weil pairing.

8. Conclusion

We proposed an ID based authenticated key agreement protocol using the Tate pairing. The protocol have two message flows but Tate pairing is more efficient than the Weil pairing in the computation. In the future, we shall work that with efficiency and security.

References

[1] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, In Advances in Cryptology-CRYPTO 2001, Springer-Verlag LNCS **2139** (2001), 213–229.

[2] A. J. Menezes, T. Okamoto, and Vanstone, *Reducing elliptic curve logarithms in a finite field*, IEEE Trans. Inform Theory **39** (1993), 1639–1646.

[3] G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 685–874.

[4] N. P. Smart, *An identity based authenticated key agreement protocol based on the weil pairing*, Cryptology ePrint Archive, Report 2001/111, 2001. http://eprint.iacr.org/.

[5] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, in W. Bosma(ed.), ANTS-IV, Springer LNCS **1838** (2000), 385–393.

[6] L. Law, A. Meneze, M. Qu, J. Solinas, and S. Vanstone, *An efficient protocol for authenticated key agreement*, Technical Report CORR 98-05, Department of C & O, University of Waterloo, 1998. to appear in Designs, Code and Cryptography.

[7] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scoott, *Efficient algorithms for pairing-based cryptosystems*, Cryptology ePrint archive: Report 2002/008 (February 6, 2002).

[8] S. Blake-Wilson and A. Meneze, *Authenticated Diffie-Hellman key agreement protocols*, In S. Tavares and H. Meijer, editors, 5th Annual Workshop on Selected Areas in Cryptography (SAC'98), volume 1556 of Lecture Notes in Computer Science, pages 339-361. Springer Verlag, 1998.

[9] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **22** (1976), 644–654.

[10] D. Boneh, B. Lynn, and H. Shacham, *Short signature from the Weil pairing*, In Advances in Cryptology-Asiacrypto, 2001, Springer-Verlag LNCS **2248** (2001), 514–532.

[11] S. D. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate pairing.*

[12] Y. S. Lee, *Applications of Pairings and their implementations*, 2002.

Department of Mathematics
Dongeui University
Busan 614-714, Korea
E-mail: yoon@sukbong.pe.kr