An Efficient Implementation of Tate and Ate Pairings

Intae Kim[1] and Seong Oun Hwang[2,*]

[1]*Department of Electronics and Computer Engineering, Hongik University, Republic of Korea, tarot13@naver.com*
[2]*Department of Computer and Information Communications Engineering, Hongik University, Republic of Korea, sohwang@hongik.ac.kr*
[*]*Corresponding author, Telephone: +82-41-860-2298, Fax: +82-41-865-0460*

Abstract

Most implementations of pairing-based cryptography are using pairing-friendly curves with an embedding degree $k \leq 12$. They have security levels of up to 128 bits. In this paper, we consider a family of pairing-friendly curves with embedding degree k = 24, which have an enhanced security level of 192 bits. We also describe an efficient implementation of Tate and Ate pairings using field arithmetic in $F_{q^{24}}$; this includes a careful selection of the parameters with small hamming weight and a novel approach to final exponentiation, which reduces the number of computations required. When comparing with the latest implementation available in the research community, ours is 15% faster due to both our selection of efficient elliptic curve parameters and faster multiplication on $F_{q^{24}}$*. Therefore, it can significantly contribute to most contemporary identity-based or attributed-based encryption or signature schemes whose basic and essential operations are based on paring, known as one of the most time-consuming operations.*

Keywords: *pairing-friendly curve, Tate pairing, Ate pairing.*

1. Introduction

Pairing can be defined as a computable bilinear map between an elliptic curve group $E(F_q)$ and a multiplicative group of an extension field F_{q^k}, where k is called the embedding degree of the elliptic curve. A pairing operation is considered to be secure if the discrete logarithm problem in the groups is computationally infeasible. In fact, the security of a pairing operation depends on the selected elliptic curve $E(F_q)$ and finite field F_{q^k}. Therefore, over the last few decades, many papers have been published on the construction of pairing-friendly curves [5,8,9,10]. Pairing-friendly curves are parameterized by an embedding degree k and prime number q. For optimal security, the parameters k and q should be selected such that the discrete logarithm problem is difficult to solve even when using the best known algorithm [10]. Many researchers have examined the issue of constructing elliptic curves with a recommended embedding degree.

Menezes *et al.* [11] showed that a supersingular elliptic curve must have an embedding degree $k \leq 6$. Miyaji *et al.* [12] described the complete characteristics for ordinary elliptic curves of prime order with the embedding degree $k = 3$, *4*, or *6*. Barrento *et al.* [8] also provided a method for the construction of curves of prime order with $k = 12$.

Security level is an extremely important aspect of real systems. The National Institute of Standards and Technology recommends the use of different algorithms to raise the security level [14]. The use of either a *192*- or *256*-bit key is recommended for top security agencies or a military environment, where security levels stronger than those in commercial

environment are required. Thus, in this paper, we focus on the implementation of pairing-friendly curves with embedding degree $k = 24$, which have a *192*-bit security level. The implementation of these types of curves has never been studied in detail at the time of starting this paper.

The paper is organized as follows: In Section 2, we provide a detailed background about pairing. The main contributions of this paper are presented in Sections 3 and 4 where we describe a pairing-friendly elliptic curve, a Tate pairing, and an Ate pairing. We describe our computational experiments in Section 5. In section 6, we compare ours with another implementation with the same embedding degree that is presumed to be proposed almost at the same time. We finally conclude this paper in Section 7.

2. Preliminaries

We declare that most of the following materials such as definitions, properties, and theorems come from [1] and [3] with/without modifications.

2.1. Elliptic Curves

Definition 1. An elliptic curve is the set of points satisfying an equation of the form $y^2=x^3+ax+b$ where the coefficients a and b are elements of a field F with the characteristic of F is not equal to 2 or 3. We write E/F to indicate this and say that the elliptic curve is over the field. Such a curve is said to be in *Weierstrass normal form*.

Definition 2. The *discriminant* of an elliptic curve in Weierstrass normal form $y^2=x^3+ax+b$ is the quantity $\Delta=-16(4a^3+27b^2)$.

Definition 3. An elliptic curve for which the discriminant $\Delta=0$ is called *singular*. An elliptic curve for which the discriminant $\Delta\neq0$ is called *nonsingular*.

Property 1. If F is field and E is an elliptic curve then $E(F)$ is a group.

The point at infinity acts as the identity element for this group. Note that there is only one operation defined for $E(F)$, which we are thinking of as addition, so it is impossible to multiply or divide elements of $E(F)$. Thus, $E(F)$ cannot be a field, which requires two operations that we think of as being addition and multiplication.

Definition 4. A formal sum of a set S is series $\{s_0,s_1,s_2,\ldots\}$ of elements of S. A formal sum is often written using a placeholder, with the understanding that the placeholder is not to be evaluated.

Definition 5. Let E be an elliptic curve. A divisor on E is a formal sum of the form

$$D=\sum_{P\in E} n_P(P)$$

where each n_p is an integer and all but finitely many n_p are zero.

Definition 6. We sat that a divisor D is a principal divisor if there is a rational function f such that $D=div(f)$. An equivalent definition is that a divisor D on an elliptic curve is principal if we can write

$$D=\sum_i a_i(P_i)$$

where $\sum a_i=0$ and $\sum a_iP_i=O$, with the last sum using the addition of points on an elliptic curve. In particular, if P is a point of order n, then the divisor $n(P)-n(O)$ is a principal divisor.

Definition 7. If *E* is an elliptic curve and

$$D = \sum_{P \in E} n_P (P)$$

is a divisor then the support of *D* is the set of all points *P* such that $n_P \neq 0$.

Definition 8. Let D_1 and D_2 be divisor. Then we say that D_1 and D_2 have disjoint support if the intersection of the support of D_1 and the support of D_2 is the empty set, or $D_1 \bigcap D_2 = \varnothing$.

Definition 9. If *D* is a divisor of the form

$$D = \sum_i a_i (P_i)$$

then we define what it means to evaluate a rational function *f* at *D* by

$$f(D) = \sum_i f(P_i)^{a_i}$$

Property 2. Let *f* and *g* be rational functions defined on some field *F*. If *div(f)* and *div(g)* have disjoint support then we have that *f(div(g))=g(div(f))*.

Definition 10. Divisors D_1 and D_2 are equivalent if they differ by a principal divisor, that is, $D = D_1 - D_2$ is a principal divisor.

Definition 11. Let $P \in E(F)$ for some elliptic curve *E/F*. We say that the *order* of a point is *n* if *n* is the smallest positive integer such that *nP=O*.

Definition 12. If *E* is an elliptic curve over a field *F* and *n* is a positive integer, we write *E(F)[n]* for the set of points of order *n* in *E(F)*. If the field *F* is clear from the context, this can be abbreviated to *E[n]*. *E(F)[n]* is a subgroup of *E(F)*. The points in *E(F)[n]* are also called the *n-torsion points* of the curve *E*.

Definition 13. We write *#E(F)* to indicate the order of the group *E(F)*, which is the number of points on an elliptic curve *E* over a field *F*, including the point at infinity, *O*. Determining the value of *#E(F)* for an arbitrary elliptic curve is a nontrivial problem.

Definition 14. If E is an elliptic curve over $\mathbb{F}_q$ and we have $\#E(\mathbb{F}_q) = q+1-t$, then *t* is called the *trace of Frobenius*, or simply the *trace*.

Hasse's theorem tells us that an elliptic curve $E/\mathbb{F}_q$ has to have approximately *q+1* points on it, and that the trace tells us roughly how far from this expected behavior a particular curve is.

Property 3. (Hasse's theorem) For an elliptic curve $E/\mathbb{F}_q$, the trace of Frobenius satisfies the inequality $|t| \leq 2\sqrt{q}$. Thus the number of points on an elliptic curve over $\mathbb{F}_q$ is approximately *q+1*.

Definition 15. Let *p* be the characteristic of $\mathbb{F}_q$ and *E* be an elliptic curve over $\mathbb{F}_q$ and *t* be the trace of *E*. If *p* divides *t* then we say that the elliptic curve *E* is *supersingular*. A curve that is not supersingular is said to be *ordinary*.

Definition 16. Let $E/\mathbb{F}_q$ be an elliptic curve and *n* be an integer such that $n | \#E(\mathbb{F}_q)$. If *k* is the smallest positive integer such that $n | (q^k - 1)$ then *k* is called the *embedding*

degree of *E* with respect to *n*. If $n=\#E(\mathbb{F}_q)$ then we can abbreviate this to saying that *k* is the embedding degree of *E*.

If *k* is the embedding degree of $E/\mathbb{F}_q$, we can think of $\mathbb{F}_{q^k}$ as being an extension of $\mathbb{F}_q$ in which $E(\mathbb{F}_q)$ is a subgroup of $\mathbb{F}_{q^k}^*$. This gives us the ability to multiply points, an operation that we cannot perform in an elliptic curve group, where only the operation of addition is defined.

2.1.1. Pairing-Friendly Elliptic Curves

Given an elliptic curve *E* defined over a finite field F_q, a pairing operation takes points on *E* that are defined over F_q or over an extension field F_{q^k} as inputs and give an element of $F^{\times}_{q^k}$ as output. For a pairing-based cryptosystem to be secure, the discrete logarithm problems in the group $E(F_q)$ of F_q-rational points on *E* and in the multiplicative group $F^{\times}_{q^k}$ must both be computationally infeasible. The best known discrete logarithm algorithm on elliptic curves is the parallelized Pollard rho algorithm [17, 18], which has running time $O(\sqrt{r})$ where *r* is the size of largest prime-order subgroup of $E(F_q)$. On the other hand, the best algorithm for discrete logarithm computation in finite fields is the index calculus attack [19] which has running time subexponential in the field size. Thus to achieve the same level of security in both groups, the size q^k of the extension field must be significantly larger than *r*. The ratio of these sizes is measured by two parameters: the embedding degree and the parameter $\rho = \log q/\log r$, which measures the base field size relative to the size of the prime-order subgroup on the curve. An elliptic curve with a small embedding degree and a large prime-order subgroup are commonly referred to as *pairing-friendly*. Table 1 shows the relationship between the security level and the embedding degree [3].

Table 1. Key size Security in Bits

Security level (bits)	Subgroup size r (bits)	Extension field size q^k(bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 - 1280	6 – 8	2-4
128	256	3000 - 5000	12 – 20	6-10
192	384	8000 - 10000	20 – 26	10-13
256	512	12000 - 18000	28 – 36	14-18

Remark. If *K* is a finite field $\mathbb{F}_q$ and $r|\#E(\mathbb{F}_q)$ is relatively prime to *q*, the following three conditions are equivalent:

(1) *E* has embedding degree *k* with respect to *r*.

(2) *k* is the smallest integer such that *r* divides $q^k - 1$.

(3) *k* is the order of *q* in $(\mathbb{Z}/r\mathbb{Z})^{\times}$.

Definition 17. Suppose *E* is an elliptic curve defined over a finite field F_q. We say that *E* is *pairing-friendly* if the following two conditions hold:

(1) there is a prime $r \geq \sqrt{q}$ dividing $\#E(F_q)$, and

(2) the embedding degree of *E* with respect to r is less than $\log_2(r)/8$.

Let *E* be an elliptic curve defined over a field *K*; we may also use *E/K* (read "*E* over *K*") to denote such a curve. We denote by *E(K)* the group of *K*-rational points of *E*, and by *#E(K)* the order of this group when it is finite. For any integer *r*, we let *E[r]* denote the group of all *r*-torsion points of *E*, and by *E(K)[r]* the group of *r*-torsion points of *E* that are defined over *K*.

Let G_1 and G_2 be additive groups and G_3 be a multiplicative group. Let be a bilinear pairing. Let F_q be a finite field with a characteristic q and $E(F_q)$ be an elliptic curve defined over F_q. Let n be the order of $E(F_q)$, r a large prime number that n is divisible by, and k, the smallest positive integer such that $r|q^k-1$. The integer k is the embedding degree of E with respect to r. We know that the r-th roots of unity are contained in F_{q^k}.

Freeman et al. [3] gave a classification of the known methods for constructing pairing-friendly elliptic curves. At the highest level, pairing-friendly elliptic curves can be classified as either individual curves or families of curves. The former type (supersingular curves, Cocks-Pinch curves, DEM curves) gives integers q and r such that there is an elliptic curve E over $\mathbb{F}_q$ with a subgroup of order r and embedding degree k with respect to r. The latter type (sparse families: MNT, GMV, Freeman; complete families: cyclotomic, sporadic, Scott-Barreto) gives integers $q(x)$ and $r(x)$ such that if $q(x_0)$ is a prime power for some value of x_0, there is an elliptic curve E over $F_{q(x0)}$ with a subgroup of order $r(x_0)$ and embedding degree k with respect to $r(x_0)$.

Construction of supersingular curves with embedding degree k=2:

Explicitly, in fields $\mathbb{F}_q$ of characteristic 2, the trace-zero supersingular curves over $\mathbb{F}_q$ are

$$E/\mathbb{F}_q : y^2 + y = x^3 + \delta x$$

if $q = 2^s$ with s even, where $Tr_{\mathbb{F}_q/\mathbb{F}_4}\delta \neq 0$, and

$$E/\mathbb{F}_q : y^2 + y = x^3$$

if $q = 2^s$ with s odd [25].

Construction of supersingular curves over prime fields of characteristic greater than 3 makes use of the following theorem:

Theorem 1 [26]. Let L be a number field, and E/L be an elliptic curve with complex multiplication. Suppose $End_L(E) \otimes Q = Q(\sqrt{-D})$. Let $\mathfrak{P} | p$ be a prime of L where E has good reduction. Then the reduction of E mod $\mathfrak{P}$ is supersingular if and only if $\mathfrak{P}$ does not split in $Q(\sqrt{-D})$, i.e., $-D/p \neq 1$.

Given a subgroup size r, if we choose any h such that $q=hr-1$ is prime, then we have the following algorithm (combining the constructions of Koblitz and Menezes [23] and Broker [27] for constructing a curve over $\mathbb{F}_q$ with embedding degree 2 with respect to r).

Algorithm 1. Input: a prime $q \geq 5$. Output: a supersingular elliptic curve $E/\mathbb{F}_q$.

(1) If $q \equiv 3 \pmod 4$, return $y^2 = x^3 + ax$ for any $a \in \mathbb{F}_q^X$ with $-a \in (\mathbb{F}_q^X)^2$.

(2) If $q \equiv 5 \pmod 6$, return $y^2 = x^3 + b$ for any $b \in \mathbb{F}_q^X$.

(3) If $q \equiv 1 \pmod{12}$, do the following:

(a) Let D be the smallest prime such that $D \equiv 3 \pmod 4$ and $-D/p = -1$.

(b) Compute the Hilbert class polynomial H_D of $Q(\sqrt{-D})$.

(c) Compute a root $j \in \mathbb{F}_q$ of $H_D \pmod q$.

(d) Let $m=j/(1728-j)$, and return $y^2 = x^3 + 3mc^2x + 2mc^3$ for any $c \in \mathbb{F}_q^X$.

Construction of supersingular curves with embedding degree k=3:

A supersingular curve over $\mathbb{F}_q$ has embedding degree k=3 with respect to a subgroup of prime order r>3 if and only of $q = p^s$ with s even, and $t = \pm\sqrt{q}$ [28]. In characteristic p>3, the only such curves are those of the form

$$E/\mathbb{F}_q : y^2 = x^3 + \gamma$$

where γ is a non-cube in $\mathbb{F}_q^X$ [29].

Construction of supersingular curves with embedding degree k=4:

Supersingular curves that have embedding degree k=4 with respect to a subgroup of prime order r>2 only exist over finite fields of characteristic 2. Then necessarily, $q = 2^s$ with s odd, and $t = \pm\sqrt{2q}$ [28]. The only possible such curves are ([25])

$E/\mathbb{F}_q : y^2 + y = x^3 + x$ and $E/\mathbb{F}_q : y^2 + y = x^3 + x + 1$.

Construction of supersingular curves with embedding degree k=6:

Supersingular curves that have embedding degree k=6 with respect to a subgroup of prime order r>3 only exist over finite fields of characteristic 3. Then necessarily, $q = 3^s$ with s>1 odd, and $t = \pm\sqrt{3q}$ [28]. The only possible such curves are ([29])

$E/\mathbb{F}_q : y^2 = x^3 - x + \delta$ and $E/\mathbb{F}_q : y^2 = x^3 - x - \delta$.

where $\delta \in \mathbb{F}_q$ with $Tr_{\mathbb{F}_q/\mathbb{F}_3}\delta = 1$.

The Cocks-Pinch Method:

Theorem 2 [15]. Fix a positive integer k and a positive square-free integer D. Execute the following steps.

(1) Let r be a prime such that $k|r-1$ and $-D/r = 1$.

(2) Let z be k-th root of unity in $(\mathbb{Z}/r\mathbb{Z})^X$. (Such a z exists because $k|r-1$.) Let $t' = z+1$.

(3) Let $y' = (t'-2)/\sqrt{-D} \pmod r$.

(4) Let $t \in \mathbb{Z}$ be congruent to t mod r, and let $y \in \mathbb{Z}$ be congruent to y' mod r. Let $q = (t^2 + Dy^2)/4$.

If q is an integer and prime, then there exists an elliptic curve E over $\mathbb{F}_q$ with an order-r subgroup and embedding degree k. If $D<10^{12}$, then E can be constructed via the CM method.

The Dupont-Enge-Morain Method:

Theorem 3 [30]. Fix a positive integer k and execute the following steps.

(1) Compute the resultant

$$R(a)=\mathrm{Res}_x(\Phi_k(x-1),a+(x-2)^2)\in\mathbb{Z}[a]$$

(2) Choose $a\in\mathbb{Z}$ such that $R(a)$ is prime and set $r=R(a)$.

(3) Compute $g(x)=\gcd(\Phi_k(x-1),a+(x-2)^2)$ in $\mathbb{F}_r[x]$ and let $t'\in\mathbb{F}_r$ be a root of the polynomial g.

(4) Let $t\in\mathbb{Z}$ be congruent to t' mod r. Let $q=(t^2+a)/4$.

If q is an integer and prime, then there exists an elliptic curve over $\mathbb{F}_q$ with an order-r subgroup and embedding degree k. If $a=Dy^2$ with $D<10^{12}$, then E can be constructed via the CM method.

MNT Curves:

Theorem 4 [28]. Let q be a prime, and let $E/\mathbb{F}_q$ be an ordinary elliptic curve such that $r=\#E(\mathbb{F}_q)$ is prime. Let $t=q+1-r$.

(1) E has embedding degree k=3 if and only if there exists $x\in\mathbb{Z}$ such that $t=-1\pm 6x$ and $q=12x^2-1$.

(2) E has embedding degree k=4 if and only if there exists $x\in\mathbb{Z}$ such that $t=-x$ or $t=x+1$ and $q=x^2+x+1$.

(3) E has embedding degree k=6 if and only if there exists $x\in\mathbb{Z}$ such that $t=1\pm 2x$ and $q=4x^2+1$.

Cyclotomic Families:

Theorem 5 [9]. Fix a positive integer k and a positive square-free integer D. Execute the following steps.

(1) Find an irreducible polynomial $r(x)\in\mathbb{Z}[x]$ with positive leading coefficient such that $K=Q[x]/(r(x))$ is a number field containing $\sqrt{-D}$ and the cyclotomic field $Q(\zeta_k)$.

(2) Choose a primitive k-th root of unity $\zeta_k\in K$.

(3) Let $t(x)\in Q[x]$ be a polynomial mapping to ζ_k+1 in K.

(4) Let $y(x)\in Q[x]$ be a polynomial mapping to $(\zeta_k-1)/\sqrt{-D}$ in K.

(So, if $\sqrt{-D}\mapsto s(x)$, then $y(x)\equiv(2-t(x))s(x)/D \bmod r(x)$.)

(5) Let $q(x) \in Q[x]$ be given by $(t(x)^2 + Dy(x)^2)/4$.

Suppose that *q(x)* represents primes and $y(x_0) \in \mathbb{Z}$ for some $x_0 \in \mathbb{Z}$. Then the triple *(t(x),r(x),q(x))* parameterizes a complete family of elliptic curves with embedding degree *k* and discriminant *D*. The ρ-value of this family is

$$\rho(t,r,q) = \frac{2\max\{\deg t(x), \deg y(x)\}}{\deg r(x)}.$$

Construction. Let k be odd, k<1000. Let

$$r(x) = \Phi_{4k}(x),$$

$$t(x) = -x^2 + 1,$$

$$q(x) = (x^{2k+4} + 2x^{2k+2} + x^{2k} + x^4 - 2x^2 + 1)/4.$$

Then *(t,r,q)* parameterizes a complete family of pairing-friendly elliptic curves with embedding degree *k* and discriminant 1. The ρ-value of this family is $(k+2)/\varphi(k)$.

Sporadic Families of Brezing-Weng Curves

Example of Barreto-Naehrig curves. Let

$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1,$$

$$t(x) = 6x^2 + 1,$$

$$q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1.$$

Then *(t,r,q)* parameterizes a complete family of curves with embedding degree *k*=12, discriminant 3, and ρ-value 1.

Scott-Barreto Families

Example. Let *l* be an even integer, and let *D* be a positive square-free integer. Define *(t,r,q)* by:

$$t(x) = 2$$

$$r(x) = x,$$

$$q(x) = Dl^2x^2 + 1.$$

Then *(t,r,q)* parameterizes a complete family of curves with embedding degree 1 and discriminant *D*. The ρ-value of this family is 2.

2.2. Tate Pairing

Let $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$. For each integer *i* and point *P*, let $f_{i,P}$ be a rational function on *E* such that $(f_{i,P}) = i(P) - (iP) - (i-1)(O)$. Let *D* be a divisor which is linearly equivalent to $(Q) - (O)$ with its support disjoint from $(f_{r,P})$. The Tate pairing is a bilinear map $\hat{e}: E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$, $\hat{e}(P,Q) = f_{r,P}(D)$.

Definition 18. Assume that curve $E(\mathbb{F}_q)$ has a subgroup of prime order r and embedding degree $k>1$. Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$ be linearly independent points. The Tate pairing of order r is defined as $e(P,Q) = f(D)^{(q^k-1)/r}$, where $D \sim (Q)-(O)$ and $(f) = r(P)-r(O)$.

Property 4. The Tate pairing has the following properties:

1. The Tate pairing is *nondegenerate*, that is, for each $P \in E(\mathbb{F}_q)[n]/\{O\}$, there is some $Q \in E(\mathbb{F}_{q^k})$ with $e(P,Q) \neq 1$.
2. The Tate pairing is *bilinear*, that is, for each $P, P_1, P_2 \in E(\mathbb{F}_q)[n]$ and $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})$ we have $e(P_1+P_2,Q) = e(P_1,Q)e(P_2,Q)$ and $e(P,Q_1+Q_2) = e(P,Q_1)e(P,Q_2)$.

Computation of the Tate pairing is helped by the following properties [22].

Property 5. For any $d>1$ such that $d|k$, $q^{k/d}-1$ is a factor of $(q^k-1)/r$.

Property 6. $e(P,Q) = f(Q)^{(q^k-1)/r}$ for $Q \neq O$.

Property 7. Let n be a prime, $P = E(\mathbb{F}_q)[n] \setminus \{O\}$, $Q = E(\mathbb{F}_{q^k})$ be linearly independent from P, and $k>1$. Then we have that $e(P,Q)$ is nondegenerate [16].

So if we have $P \in E(\mathbb{F}_q)[n]$ and a nontrivial embedding degree, that is, we have $k>1$, then one way to make sure that the Tate Pairing $e(P,Q)$ is nondegenerate is to make sure that Q is linearly independent of P. One way to do this is to use a distortion map, so that instead of computing $e(P,Q)$, we compute $e(P,\phi(Q))$ instead, where ϕ is an appropriate distortion map. Another way is to compute $e(P,\phi_d(Q))$ where $Q \in E'$ is on the twist of the elliptic curve E and $\phi_d : E' \to E$ is the mapping defined later. In either case, we denote the resulting pairing by $\hat{e}(P,Q)$, where either $\hat{e}(P,Q) = e(P,\phi(Q))$ or $\hat{e}(P,Q) = e(P,\phi_d(Q))$ as appropriate and call such an $\hat{e}$ the *modified Tate Pairing*.

Definition 19. Let $E/\mathbb{F}_q$ be an elliptic curve and n be an integer relatively prime to q, and P a point of order n in $E(\mathbb{F}_q)$. A *distortion map* with respect to (or for) P is an endomorphism ϕ that maps the point P to a point $\phi(P)$ that is linearly independent from P. The following property implies that distortion maps do not exist for ordinary curves.

Property 8. Let E be an elliptic curve over F_q which has a distortion map. Then E is supersingular.

Definition 20. A twist of $E/\mathbb{F}_q$ is an elliptic curve $E'/\mathbb{F}_q$ that is isomorphic to E over $\overline{\mathbb{F}_q}$. The minimal d for which E and E' are isomorphic over $\mathbb{F}_{q^d}$ is the degree of the twist.

Definition 21. The *trace map* is the mapping $\mathrm{Tr} : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$ defined as $Tr(P) = P + \Phi(P) + \Phi^2(P) + \cdots + \Phi^{k-1}(P)$. We have $Tr(\Phi(P)) = \Phi(tr(P)) = tr(P)$ for any $P = (x,y) \in E(\mathbb{F}_{q^k})$

where the sum is elliptic curve point addition. The trace map is a group homomorphism and $Tr(P) \in E(\mathbb{F}_q)$.

It follows that if $P \in E(\mathbb{F}_{q^k})$ has prime order *r*, $P \notin E(\mathbb{F}_q)$ and $Tr(P) \neq O$, then $e(Tr(P),P) \neq 1$.

The trace map transforms points which are defined over a large field into points defined over a small field, whereas distortion maps go the other way around.

The trace map enables mapping into a specific cyclic subgroup of $E(\mathbb{F}_{q^k})$ of order *r* (called the trace zero subgroup *T*) as follows. If *P* is a randomly chosen element of $E(\mathbb{F}_{q^k})$ of order *r*, then $P' = [k]P - Tr(P)$ is easily seen to satisfy $Tr(P') = O$. Furthermore, if $P \notin E(\mathbb{F}_q)$ and if *r* is coprime to k, then $P' \neq O$.

For some curves $E/\mathbb{F}_q$ it is possible to create twists. In these cases we have $E' : y^2 = x^3 + a'x + b'$ where $a' = v^{4/d}a$ and $b' = v^{6/d}b$, and *v* is a root degree *d* but not a root of less than degree *d* over *F*, which we can call a *twist of degree d*. All elliptic curves have quadratic (i.e., degree 2) twists. The only curves with higher-order twists are those with CM discriminant 1 (defined by equations of the form $y^2 = x^3 + ax$), which have quartic twists, and those with CM discriminant 3 (defined by equations of the form $y^2 = x^3 + b$), which have cubic and sextic twists. The possible twists are summarized in Tables 2, 3, and 4.

Table 2. Elliptic Curves and Their Twists

Degree of Twist *d*	Form of *E*	Form of *E'*
2 (quadratic)	$y^2 = x^3 + ax + b$	$y^2 = x^3 + v^2ax + v^3b$
3 (cubic)	$y^2 = x^3 + b$	$y^2 = x^3 + vb$
4 (quartic)	$y^2 = x^3 + ax$	$y^2 = x^3 + vax$
6 (sextic)	$y^2 = x^3 + b$	$y^2 = x^3 + vb$

Table 3. Points on Twists of Elliptic Curves

Degree of Twist *d*	Typical Point on *E*	Corresponding Point on *E'*
2 (quadratic)	(x,y)	$(vx, v^{3/2}y)$
3 (cubic)	(x,y)	$(v^{1/3}x, v^{1/2}y)$
4 (quartic)	(x,y)	$(v^{1/2}x, v^{3/4}y)$
6 (sextic)	(x,y)	$(v^{1/3}x, v^{1/2}y)$

Table 4. Mappings $\phi_d : E' \to E$

Degree of Twist *d*	$\phi_d : E' \to E$
2 (quadratic)	$\phi_2(x,y) = (v^{-1}x, v^{-3/2}y)$
3 (cubic)	$\phi_3(x,y) = (v^{-1/3}x, v^{-1/2}y)$
4 (quartic)	$\phi_4(x,y) = (v^{-1/2}x, v^{-3/4}y)$
6 (sextic)	$\phi_6(x,y) = (v^{-1/3}x, v^{-1/2}y)$

A twist of degree *k* on a curve with embedding degree *k* would be ideal for implementation, as it would allow all curve points and pairing values to be given over the base field $\mathbb{F}_q$. Unfortunately, such a curve must either be supersingular or have $\rho-$ value nearly 2.

When implementing pairings on pairing friendly non-supersingular curves, one of the parameters is placed on the curve defined over the base field $\mathbb{F}_q$, and the other is typically placed on a 'twisted' curve, where there exists a group of points of order *r* which are isomorphic to a group of points on the curve defined over the full *k*-th extension of the base field. For example if the pairing is the ate pairing, or one of its variants, the pairing is *e(Q,P)*, where $Q \notin E'(\mathbb{F}_{q^{k/d}})$, where *k* is the embedding degree and *d* is the degree of the twist. Points on the twisted curve are defined over a smaller field, and are thus obviously much faster to manipulate. However when required in the pairing calculation (for example for evaluation of the line function) they can be quickly mapped to a point on $E(\mathbb{F}_{q^k})$.

If the embedding degree *k* is even then the quadratic twist (*d*=2) can be used. If the pairing-friendly curve has a CM discriminant of *D*=1, and 4|*k*, then we can use a quartic twist associated with *d*=4. Similarly if the curve has *D*=3, and 6|*k*, then a sextic twist can be used *d*=6.

Consider first the case of the quadratic twist [21] with the elliptic curve in its standard Weierstrass representation

$$y^2 = x^3 + Ax + B$$

The twisted curve over the field of definition $\mathbb{F}_{q^{k/d}}$ will be

$$y^2 = x^3 + Ax/i^2 + B/i^3$$

where *i* is any quadratic non-residue in the field of definition. Since the chosen QNR *i* appears here as a divisor, we call this a type D twist. To map from the twisted curve to the original curve

$$E' \to E : (x, y) \to (ix, i^{3/2} y)$$

An alternative and perhaps simpler way to address this issue is to represent the twisted curve by the isomorphic curve

$$y^2 = x^3 + i^2 Ax + i^3 B$$

We call this a type M twist. To effect the mapping in this case

$$E' \to E : (x, y) \to (x/i, i^{1/2} y/i^2)$$

The equation for the type D sextic twist [20] associated with our choice of *i* is

$$y^2 = x^3 + B/i$$

But an isomorphic curve is the M-type twist

$$y^2 = x^3 + i \cdot B$$

For the D-type twist we can move from the twisted curve back to the original curve using

$$E' \to E : (x, y) \to (i^{1/3}x, i^{1/2}y)$$

For the M-type twist the mapping is slightly more complicated

$$E' \to E : (x, y) \to (i^{2/3}x / i, i^{1/2}y / i)$$

2.3. Miller's algorithm [2]

Victor Miller gave an algorithm to compute the Tate pairing. Miller's idea is to use the double-and-add method. Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$. Let $l_{R,T}$ be the equation of the line through points *R* and *T*, and let v_S be the equation of the vertical line through point *S*. For $i, j \in \mathbb{Z}$, we have $f_{i+j,P}(Q) = f_{i,P}(Q) f_{j,P}(Q) \frac{l_{iP,jP}(Q)}{v_{(i+j)P}(Q)}$.

Using the above formula, $f_{r,P}(Q)^{(q^k-1)/r}$ can be computed in polynomial time by Miller's algorithm.

Algorithm 2. Miller's Algorithm

Input : $r = \sum_{i=0}^{n} l_i 2^i$, where $l_i \in \{0,1\}$, $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$.
Output : $e(P, Q)$

1. $T \leftarrow P$, $f_1 \leftarrow 1$
2. for i = n-1, n-2, …, 1, 0 do
   2.1 $f_1 \leftarrow f_1^2 \cdot \frac{l_{T,T}(Q)}{v_{2T}(Q)}$, $T \leftarrow 2T$
   2.2 if $l_i = 1$ then
   2.3 $f_1 \leftarrow f_1 \cdot \frac{l_{T,P}(Q)}{v_{T+P}(Q)}$, $T \leftarrow T + P$
3. return $f_1^{(q^k-1)/r}$

2.4. Ate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where *p* is a prime. Let *E* be an ordinary elliptic curve over $\mathbb{F}_q$, *r* a large prime satisfying $r | \#E(\mathbb{F}_q)$ and let *t* denote the trace of Frobenius, i.e., $\#E(\mathbb{F}_q) = q + 1 - t$. Let T=t-1 and then $T \equiv q \ mod \ r$. Let π_q be the Frobenius endomorphism, $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$. Denote $Q \in G_2 = E[r] \cap Ker(\pi_q - [q])$ and $P \in G_1 = E[r] \cap Ker(\pi_q - [1])$. Let $N = \gcd(T^k - 1, q^k - 1) > 0$ and $T^k - 1 = LN$, where *k* is its embedding degree. Denote the normalized function $f_{T,Q}^{norm} = f_{T,Q} / (z^r f_{T,Q})(O)$, where $Q \in G_2$ and *z* is a local parameter for the infinity point *O*. Then the Ate pairing is defined as $f_{T,Q}^{norm}(P)$ and $e(Q,P)^L = f_{T,Q}^{norm}(P)^{c(q^k-1)/N}$, where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \bmod N$.

2.5. Extension Field Arithmetic

Arithmetic in the extension field $\mathbb{F}_{q^k}$ can be implemented very efficiently if this field can be built up as a "tower" of extension fields,

$$\mathbb{F}_q \subset \mathbb{F}_{q^{d_1}} \subset \mathbb{F}_{q^{d_2}} \subset \cdots \subset \mathbb{F}_{q^k}$$

where the *i*th extension field $\mathbb{F}_{q^{d_i}}$ is obtained by adjoining a root of a polynomial $x^{d_i/d_{i-1}} + \beta_i$ for some $\beta_i \in \mathbb{F}_{q^{d_{i-1}}}$ that are "small" in the sense that they can be represented using very few bits. This property is likely to apply if $k = 2^a 3^b$ for some *a*, *b*, so pairings may be computed more quickly on curves with embedding degree of this form.

Koblitz and Menezes [23] show that if $k = 2^a 3^b$ and $q \equiv 1 \pmod{12}$, then $\mathbb{F}_{q^k}$ can be built in one step by adjoining a root of $x^k + \beta$ for some (not necessarily small) $\beta \in \mathbb{F}_q$. Barreto and Naehrig [24] give a construction for *k=12* consisting of adjoining a square root followed by a sixth root.

3. Pairing-friendly Elliptic Curve with Embedding Degree *k=24*

We implemented a method to generate pairing-friendly elliptic curves over a prime field, with embedding degree *k = 24*. Freeman *et al.*[3] described a general method to generate ordinary curves using the Cocks-Pinch method [15]. The Cocks-Pinch method has an advantage in that it can produce curves with prime-order subgroups of nearly arbitrary sizes.

Theorem 6. [3] Fix a positive integer *k* and a positive square-free integer *D*. Execute the following steps:

(1) Find an irreducible polynomial *r(x)* with a positive leading coefficient such that *K=Q[x]/(r(x))* is a number field containing $\sqrt{D}$ and the cyclotomic field $Q(\xi_k)$.

(2) Choose a primitive *k*-th root of unity $\zeta_k \in K$.

(3) Let $t(x) \in Q[x]$ be a polynomial mapping to $\zeta_k + 1$ in *K*.

(4) Let $y(x) \in Q[x]$ be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in *K*.

(5) Let $q(x) \in Q[x]$ be given by $(t(x)^2 + Dy(x)^2)/4$.

Let *q(x)* represent primes and $y(x_0) \in Z$ for some $x_0 \in Z$. Then the triple *(t(x), r(x), q(x))* parameterizes a complete family of elliptic curves with an embedding degree *k* and discriminant *D*.

In the paper, we follow the Cocks-Pinch method and the method proposed by Freeman *et al.* [3] to generate a family of elliptic curves with embedding degree *k=24*. Reference [3] classified families in all cases where *k* is not divisible by *18*.

The equation of the curve is *E:* $y^2 = x^3 + b$, with $b \neq 0$. The trace of the curve, the prime number *r* by which the order of the curve is divisible, and the characteristic of F_q are parameterized as follows:

$$t(x) = x + 1$$
$$r(x) = x^8 - x^4 + 1$$
$$q(x) = \frac{1}{3}(x^{10} - 2x^9 + x^8 - x^6 + 2x^5 - x^4 + x^2 + x + 1)$$

We can calculate the ρ value like as follows:

$$\rho = deg\ q(x)/deg\ r(x) = 10/8 = 1.25$$

Example 1. Using the proposed pairing-friendly curves, we present an example of an elliptic curve with embedding degree $k = 24$. Let $x = -562956395872256$. Then $t = x+1$ is *50* bits, r is *489* bits, q is *393* bits, and the hamming weight of x is *3*. The desired curve has the form of $y^2=x^3+10$ with

t=*-562956395872255*

r=1065678788090687414781234809487409796360705132976322386052516761893902274102196368903858053299667708716351625059695223776148550871771850476603746987, and

q=10656787880906874147812348094874097963607051329763223860525167618939022741021963689038580532996677087163516250596952237761485508717718504766037469 87

4. Computation of Bilinear Pairings over Elliptic

4.1. Tower Extension of Finite Field $F_{q^{24}}$

The elements in the field are represented through a polynomial of degree k - *1*, i.e., $F_{q^k} = F_q[x]/(f(x))$, where $f(x)$ is an irreducible polynomial of degree k. In the paper, we construct the extension field $F_{q^{24}}$ as a tower of finite extensions: quadratic on top of a cubic on top of a quadratic, i.e., *1-2-4-12-24*. The irreducible polynomials for the tower of extensions are detailed in Table 5.

Table 5. Tower of Extension Fields

Extension	Construction	Representation
F_{q^2}	$F_q[u]/(u^2+1)$	$a = a_0 + a_1 u$
F_{q^4}	$F_{q^2}[v]/(v^2-(1+u))$	$a = a_0 + a_1 v$
$F_{q^{12}}$	$F_{q^4}[w]/(w^3-v)$	$a = a_0 + a_1 w + a_2 w^2$
$F_{q^{24}}$	$F_{q^{12}}[z]/(z^2-w)$	$a = a_0 + a_1 z$

4.2. Sextic Twist and Miller's Algorithm

We describe the Tate and Ate pairing operations in this section. The pairing operations take points $P=(x_P,y_P) \in E(Fq)$ and $Q=(x_Q,y_Q) \in E(F_{q^{24}})$. For optimization, we can compress points in $E(F_{q^{24}})$ to points in a sextic twist $E'(F_{q^4})$. Let $i \in F_{q^4}$ be such that x^6-i is irreducible over F_{q^4}. Then the elliptic curve E admits a sextic twisted curve $E': y^2=x^3+b/i$ with

$\#E'(F_{q^4})=q^4+1-(3f+T)/2$ where $T=t^4-4qt^2+2q^2$ and $f=\sqrt{(4q^4-T^2)/3}$ [4]. Let $\theta \in F_{q^{24}}$ be a root of x^6-i. Then the injective homomorphism $E' \to E:(x',y') \to (\theta^2 x', \theta^3 y')$ maps the points on the sextic twisted curve to the original curve.

Tate and Ate pairing can be computed by using Miller's algorithm such as [5]. When we compute the line function of Ate pairing, we can use sextic twist formula like [6]:

For $A=(x_A,y_A)=(x_A'\theta^2, y_A'\theta^3), B=(x_B,y_B)=(x_B'\theta^2, y_B'\theta^3) \in E(F_{q^{24}})$, let $l_{A,B}$ be a line passing through A and B. Then we have

$$l_{A,B}(P)=(-y_P)+(x_P\lambda_{A',B'})\theta+(y_A'-x_A'\lambda_{A',B'})\theta^3$$

where $\lambda_{A',B'}=(y_B'-y_A')/(x_B'-x_A')$.

4.3. Final Exponentiation

Both Tate and Ate pairing algorithms compute a final exponentiation $(q^{24}-1)/r$ after running the Miller algorithm. This exponentiation is factored into three parts to speed up our implementation: $(q^{12}-1)$, $(q^{12}+1)/\phi_{24}(q)$, $\phi_{24}(q)/r$ where $\phi_{24}(q)$ is the *24*-th cyclotomic polynomial [7]. Here, $\phi_{24}(q)/r$ is called the hard exponentiation. It can be easily shown by computation that $\phi_{24}(q)=q^8-q^4+1$, $r(x)=x^8-x^4+1$. Then these exponents are explicitly expressed as $(q^{12}-1)$, (q^4+1), and $(1+(q^3+xq^2+x^2q+x^3)(q^4+x^4-1)(x-1)^2/3)$. The exponentiation for the first two parts is easy to compute because of the Frobenius.

Algorithm 3. Hard Exponentiation

Input : f, x, q

Output : $f^{(1+(q^3+xq^2+x^2q+x^3)(q^4+x^4-1)(x-1)^2/3)}$

1. Compute f^q, f^{q^2}, and f^{q^3} using Frobenius
2. Compute $f' \leftarrow (f^{q^3}) \cdot (((f^{q^2})((f^q)(f)^x)^x)^x$
3. Compute $(f')^{q^4}$ using Frobenius
4. $f'' \leftarrow \left((f')^{q^4}\right) \cdot (f')^{x^4} \cdot (f')^{-1}$
5. $f \leftarrow f \cdot (f'')^{(x-1)^2/3}$

However, the exponentiation of the third part is difficult to compute. Therefore, instead of using the expensive multi-exponentiation method, we exploit the polynomial description of q and r to obtain Algorithm 3, which can produce equivalent result with lesser exponentiation. Our experiments show that this method is twice as fast as compared to multi-exponentiation.

4.4. Final Exponentiation

In the case of particular prime p such that $p = 3 \bmod 4$, $p = 1 \bmod 6$ and $p = 7 \bmod 12$, we can speed up the abovementioned final exponentiation by converting exponentiations to multiplications as follows:

If we let

$$E = 1 + u, F_1 = E^{(p-1)/2}, F_2 = E^{(p-1)/6}, F_3 = E^{(p-7)/12}, \ F_4 = E^{(p-3)/4}$$

then we have

$$z^p = z^{p-7} z^6 z = (z^{12})^{(p-7)/12} vz = E^{(p-7)/12} vz = F_3 vz$$

$$w^p = (w^6)^{(p-1)/6} w = F_2 w, v^p = F_1 v, u^p = -u$$

Therefore we obtain the following Table 6.

Table 6. Tower of Extension Fields and their Frobenius Constants used in the Proposed Implementation

Extension	Representation	Frobenius
F_{q^2}	$a = a_0 + a_1 u$	$a^p = a_0 - a_1 u$
F_{q^4}	$a = a_0 + a_1 v$	$a^p = a_0{}^p + a_1{}^p F_1 v$
$F_{q^{12}}$	$a = a_0 + a_1 w + a_2 w^2$	$a^p = a_0{}^p + a_1{}^p F_2 w + a_2{}^p F_2{}^2 w^2$
$F_{q^{24}}$	$a = a_0 + a_1 z$	$a^p = a_0{}^p + a_1{}^p F_3 vz$

5. Computation Experiment

The performances of the Tate and Ate pairings were measured using a Window 7 system with a 2.91GHz AMD Athlon™ II processor. The results have been listed in Table 7.

The MIRACL v5.4.2 library (http://www.shamus.ie) was used in our test; this library supports multi-precision arithmetic and a number of powerful optional optimizations. Internally, prime field elements are in Montgomery representations [13], which allows for fast reduction without divisions. The measured times for the Ate and Tate pairings are listed in Table 7. The Ate pairing over the proposed curve takes approximately *0.320* seconds, which is quite efficient for present-day use.

Table 7. Timings in Seconds for 2.91GHz AMD Athlon™ II.

	Tate pairing	Ate pairing
Miller loop	0.740s	0.073s
Final exponentiation	0.254s	0.247s
Total	0.994s	0.320s

6. Comparison

As we mentioned earlier, when we started this research, there was no implementation of elliptic curve with $k = 24$. The highest implementation available in terms of embedding degree was only *18* at that time. After completing our implementation, we found that a newer version v5.5.3 of MIRACL was released to support $k = 24$ recently.

To compare ours with MIRACL v5.5.3, we changed our elliptic curve parameters according to those of MIRACL v5.5.3 as follows: We used $x = 1614090106449621913 6$. Then $t = x+1$ is *64* bits, r is *637* bits, q is *511* bits, and the hamming weight of x is *7*. The desired curve has the form of $y^2 = x^3 + 6$ with

t=1614090106449621913 7,

r=400088898064826925869644434632929196411688861570349174953922125729666724618990351845046702275328759232148773178481556970294293494181311515261254630747346973699227695948818501146537094645143211, and

q=460704234614103206661594769464552427257146343533990447600104644994807392242507196604947450374865683100850849405202069011443816730758909256814967153229824 1

One of the major differences between ours and MIRACL v5.5.3 is tower of extension shown in Table 8: we used *1-2-4-12-24*, while MIRACL v5.5.3 used *1-2-4-8-24*.

Table 8. Tower of Extension Fields and their Frobenius Constants used in MIRACL v5.5.3

Extension	Representation	Frobenius
$F_{q^4} \cong F_{q^2}[u]/(u^2+1)$	$a = a_0 + a_1 u$	$a^p = a_0 - a_1 u$
$F_{q^4} \cong F_{q^2}[v]/(v^2-(u+1))$	$a = a_0 + a_1 v$	$a^p = a_0^p - a_1^p F_1 v$
$F_{q^8} \cong F_{q^4}[w]/(w^2-v)$	$a = a_0 + a_1 w$	$a^p = a_0^p - a_1^p F_4 w$
$F_{q^{24}} \cong F_{q^8}[z]/(z^3-w)$	$a = a_0 + a_1 z + a_2 z^2$	$a^p = a_0^p - a_1^p F_3 vz + a_2^p F_3^2 Ez^2$

Table 9 shows the performance comparison result between MIRACL v5.5.3 and ours. Ours is approximately more than *15%* faster than MIRACL v5.5.3. The reason behind this is that multiplication on $F_{q^{24}}$ in ours is faster than that of MIRACL v5.5.3 as shown in Table 10. In addition, by directly comparing the total time in Table 7 with that in Table 9, we confirm that our selection of elliptic curve parameters is more efficient than those of MIRACL v5.5.3.

Table 9. Performance Comparison

Ate pairing	MIRACL v5.5.3	Proposal
Miller loop	0.160s	0.124s
Final exponentiation	0.504s	0.437s
Total	0.664s	0.561s

Table 10. Comparison of Multiplications on $F_{q^{24}}$.

ZZn24	MIRACL v5.5.3	Proposal
Multiplication	1.357ms	1.030ms

7. Conclusion

In this paper, we described our novel implementation of the Tate and Ate pairings over the proposed elliptic curves with embedding degree *k = 24*. We also compared the time required to compute the pairings with the latest version available in the research community. From the experiment, we conclude that the proposed implementation is considerably efficient in terms

of computation time. In the near future, we plan to continue optimizing the pairing operations, particularly the final exponentiation, in lightweight devices such as sensor nodes or mobile devices.

Acknowledgements

This work is an extended version of the paper published at ASL (Advanced Science Letter). It was supported by National Research Foundation of Korea Grant funded by the Korean Government (2009-0066003).

References

[1] L. Martin, Introduction to identity-based encryption, Artech House, **(2008)**.

[2] V. S. Miller, "The Weil pairing and its efficient calculation", Journal of Cryptography **(2004)**, vol. 17, no. 4, pp. 235-261.

[3] D. Freeman, M. Scott and E.Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves", Journal of Cryptology **(2010)**, vol. 23, pp. 224-280.

[4] M. Scott, "A note on twists for pairing friendly curves", ftp://ftp.coomputing.dcu.ie/pub/resources/crypto/twists.pdf **(2005)**.

[5] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing based cryptosystems", Proc. CRYPTO 2002, LNCS, Springer-Verlag, Heidelberg **(2002)**, Vol. 2442, pp. 354-369.

[6] A. J. Devegili, M. Scott and R. Dahab, "Implementing Cryptographic Pairing over Barento-Naehrig Curves", Proc. Pairing 2007, Springer-Verlag **(2007)**, Vol. 4575, pp.197-207.

[7] R. Granger, D. Page and N.P. Smart, "High security pairing-based cryptography revisited", Algorithm Number Theory, LNCS, Springer-Verlag, Heidelberg **(2006)**, vol. 4076, pp. 480-494.

[8] P. S. L. M. Barreto and M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order", Proc. SAC 2005, LNCS, Springer-Verlag **(2006)**, vol. 3897, pp.319-331.

[9] F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography", Designs, Codes and Cryptography, Springer-Verlag **(2005)**, vol. 37, no. 1, pp.133-141.

[10] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10", Proc. ANTS-VII, LNCS, Springer-Verlag **(2006)**, vol. 4076, pp.452-465.

[11] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", IEEE Transactions on Information Theory **(1993)**, Vol. 39, pp.1639-1646.

[12] A. Miyaji, M. Nakabayashi and S. Takano, New explicit conditions of elliptic curve traces for FR-reduction, IEICE Transactions on Fundamentals **(2001)**, vol. E84-A(5), pp.1234-1243.

[13] P. L. Montgomery, "Modular multiplication without trial division", Mathematics of Computation **(1985)**, vol. 44, no. 170, pp.519-521.

[14] CNSS Policy, no. 15, fact sheet no. 1, National Policy on the Use of the Advanced Encryption Standard(AES) to Protect National Security Systems and National Security Information. NIST **(2003)**.

[15] C. Cocks and R.G.E. Pinch, "Identity-based cryptosystems based on the Weil pairing", Unpublished manuscript **(2001)**.

[16] E. Verheul, "Evidence That XTR Is More Secure Than Supersingular Elliptic Curve Cryptosystems", Journal of cryptology (**2004**), Vol. 17, No. 4, pp. 277-296.

[17] A. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance", Advances in Cryptology – Eurocrypt (**1984**), Lecture Notes on Computer Science, vol. 209, pp. 224-314.

[18] J. Pollard, "Monte Carlo methods for index computation (mod p)", Math. Comput. (**1978**) Vol. 32, pp. 918-924.

[19] M. Naehrig, P.S.L.M. Barreto and P. Schwabe, "On compressible pairings and their computation", Progress in Cryptology – Africacrypt **(2008)**, Notes on Computer Science, vol. 5023, pp. 371-388.

[20] F. Hess, N. Smart, and F. Vercauteren, "The eta pairing revisited", IEEE Trans. Information Theory (**2006**), 52:4595-4602.

[21] M. Scott, "A note on twists for pairing friendly curves", Personal webpage: ftp://ftp.computing.dcu.ie/pub/resources/crypto/twists.pdf, February **(2009)**.

[22] P. S. L. M. Barreto, B. Lynn and M. Scott, "On the Selection of Pairing-Friendly Groups", Selected Areas in Cryptography – SAC 2003 **(2003)**, Lecture Notes in Computer Science, vol. 3006, (Springer, Berlin, 2003), pp. 17-25.

[23] N. Koblitz and A. Menezes, "Pairing-basec cryptography at high security levels", in Proceeding of Cryptography and Coding: 10th IMA International Conference **(2005)**, Lecture Notes in Computer Science, vol. 3796 (Springer, Berlin, 2005), pp. 13-36.

[24] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order", in Selected Area in Cryptography – SAC 2005 **(2005)**, Lecture Notes in Computer Science, vol. 3897 (Springer, Berlin, 2006), pp. 319-331.

[25] A. Menezes and S. Vanstone, "Isomorphism classes of elliptic curve over finite fields od characteristic 2", Util. Math. 38 **(1990)**, pp. 135-153

[26] S. Lang, "Elliptic Functions", (Springer, Berlin, 1987) **(1987)**.

[27] R. Broker, "Constructing elliptic curve of prescribed order", Ph.H. thesis, Dept. of Mathematics, Leiden University, **(2006)**, Available at: http://www.math.leidenuniv.al/~reinier/thesis.pdf.

[28] A. Miyaji, M. Nakabayashi and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", IEICE Trans. Fundam. E84-A(5) **(2001)**, pp. 1234-1243.

[29] F. Morain, "Classes d'isomorphismes des courbes elliptiques supersingulieres en caracteristique≥3. Util. Math. 53 (**1997**), pp. 241-253.

[30] R. Dupont, A. Enge and F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields", J. Cryptol. 18 **(2005)**, pp. 79-89.

Authors

Intae Kim

Intae Kim received his BS and MS degree, all in computer and information communications engineering, respectively in 2010 and 2012 from Hongik University. Currently he is a PhD degree candidate at Hongik University. His research interests include cryptography and network security.

Seong Oun Hwang

Seong Oun Hwang (corresponding author) received his BS degree in mathematics in 1993 from Seoul National University, his MS degree and PhD degree, all in computer science, respectively in 1998 from POSTECH, and in 2004 from KAIST. Since 2008, he has been working as an assistant professor with the Department of Computer and Information Communication Engineering of Hongik University, Korea. His research interests include cryptography and security.