International Journal of Pure and Applied Mathematics
Volume 105 No. 2 2015, 187-200
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v105i2.6

EFFICIENT SIGNATURE SCHEME FROM SELF-PAIRING ON ELLIPTIC CURVES

Rajeev Kumar[1] §, S.K. Pal[2], Arvind[3]

[1]Dyal Singh College
University of Delhi
Delhi, INDIA

[2]DRDO, Delhi, INDIA

[3]Hansraj College
University of Delhi
Delhi, INDIA

Abstract: A Self-pairing $e_s(P, P)$ is a special subclass of bilinear pairing where both input points in a group are equal. Self-pairings have some interesting applications in cryptographic scheme and protocols. Recently some novel methods for constructing self-pairings on supersingular elliptic curves have been proposed. In this paper we first give the construction of self-pairings on some supersingular elliptic curves. We will show that the proposed self pairings are efficient than the general pairings on the corresponding curves. Secondly, we present a digital signature scheme from self-pairing on elliptic curves. We also show that the signature scheme from self-pairing is more efficient than the previous one.

AMS Subject Classification: 94A60
Key Words: elliptic curves, self-pairing, weil pairing, tate pairing, pairing-based cryptography

Received: August 16, 2015

§Correspondence author

1. Introduction

Pairing based cryptography [1] has become one of the most active areas in elliptic curve cryptography since 2000. The first notable application of pairings to cryptography was the work of Menezes, Okamato and Vanstone. They showed that the discrete logarithm problem can be shift from an elliptic curve to a finite field through the Weil pairing as the discrete logarithm problem is more easily solved over a finite field than over an elliptic curve. Many successful cryptographic protocols have been designed by using the pairings. In order to make these cryptographic protocols practical, computation of pairings need to be efficiently carried out. For the purpose of fast developments of algorithmic foundation of pairings, many efficient pairings such as Weil pairing [2, 3, 4], Tate pairing [2, 3, 5, 6], Ate pairing [7, 8], optimal pairing [9] and pairing lattices [10] have been proposed. For speed up pairing computation, many efficient techniques such as shortening the loop length in miller's algorithm [7, 10, 11], or speeding up doubling and addition steps in Miller's algorithm [12, 13], etc., have been presented.

Self-pairing $e_s(P, P)$ [14] is a special subclass of bilinear pairing where both input points in a group are equal. Self-pairings have been used in some cryptographic protocols and schemes such as short signature [15, 16], ID-based Chameleon hashing scheme [17], etc. It is well known that $e(P, P) = 1$ for any P if we directly compute Weil pairing. Thus for cryptographic applications, the latter P should be mapped to another independent point for keeping non- degeneracy. The point P could be mapped to another independent point by using distortion maps. But the distortion maps exist only on ordinary curves with embedding one [18] and supersingular curves. By using the distortion maps on supersingular elliptic curves with even embedding degree, the author of [14] proposed the self-pairing with a simple final exponentiation. Later this idea also has been generalized to the hyper elliptic curves [19]. The author of [20] and [21] proposed the efficient self-pairings on ordinary elliptic curves and self pairings on supersingular elliptic curves with embedding degree 3 respectively.

It was proposed in [14] a novel method for constructing self-pairings on some supersingular elliptic curves with even embedding degree. In this paper we use this method to present self-pairings on some different supersingular elliptic curves. We use the distortion maps on the supersingular elliptic curves $E_1 : y^2 + y = x^3$ over $\mathbb{F}_{2^n}$, where n is odd and $E_2 : y^2 = x^3 - x + 1$ over $\mathbb{F}_{3^n}$, where n is odd, to proposed self-pairings on these curves. We also construct the self-pairing on the supersingular elliptic curve $E_3 : y^2 = x^3 + b$ over the prime field $\mathbb{F}_p$, where $p \equiv 2 \ mod \ 3$. The author of [14] discussed the self-pairing

on the curve like E_3 but we are taking the curve in general form. The general bilinear pairing on the curve E_1 has been studied by Soonhak Kwon [22]. We also present an efficient signature scheme from self-pairing on elliptic curves.

The paper is organized as follows. In Section 2, we provide some background and notations of pairing on elliptic curves used through this paper. In Section 3, we present new self-pairings on supersingular elliptic curves. In Section 4, we present efficient signature scheme by using self-pairing. In Section 5, we discuss the efficiency of the signature scheme. We draw our conclusion in Section 6.

2. Mathematical Background

In this section, we give some required mathematical background for pairing based cryptosystems. We recall the definition of the elliptic curve, Weil and Tate pairing. We also give some facts about supersingular elliptic curves.

2.1. Elliptic Curves

An elliptic curve [23] over a field K is set of all points on the curve (given by the Weirstrass equation)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

together with O, the "point at infinity". If the characteristic p of the field K is not equal to two or three, then the Weirstrass equation convert to

$$y^2 = x^3 + ax + b$$

with the condition that $4a^3 + 27b^2 \neq 0 \mod p$. The points on elliptic curve form an abelian group under the group law. To define this group law consider two points, say P and Q, on elliptic curve and draw line from P to Q until it hit the curve again. From this we get another point on the curve. Now we draw a line from the point at infinity, O, through this new point. The point where this line intersects the elliptic curve again is $P + Q$. If $P = Q$, we consider the line between P and Q to be the tangent at P and proceed in the same as above. If the line from P to Q does not intersect the curve anywhere on the finite plane then we say it intersect at O. We denote this group by $E(K)$. The most popular choice of the field K is prime field $\mathbb{F}_p$. If $P(x_1, y_1)$ and $Q(x_2, y_2)$ be two points on the elliptic curve $y^2 = x^3 + ax + b$ over the field $\mathbb{F}_p$, then $Q(x_3, y_3) = P + Q$ and $2P = P + P$ are defined as:

$$x_3 = s^2 - x_1 - x_2 \mod p$$

$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$
$$s = (y_2 - y_1)/(x_2 - x_1) \bmod p; \qquad \text{if } P \neq Q \text{ (point addition)}$$
$$\text{and} \quad s = (3x_1^2 + a)/2y_1 \bmod p; \qquad \text{if } P = Q \text{ (point doubling).}$$

The group $E[m] = \{P \in \bar{E} | [m]P = O\}$ i.e. the group of points of order m on $E(\bar{\mathbb{F}}_p)$, called m- torsion subgroup of E.

2.2. Weil Pairing

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with $q = p^n$, where p is a prime number. Let m be a fixed integer coprime to p and k be least positive integer such that $E[m] \subset E[\mathbb{F}_{q^k}]$. Suppose $P, Q \in E[m]$ be two points. Let D_P and D_Q be divisors such that $D_P \sim (P) - (O)$ and $D_Q \sim (Q) - (O)$, and D_P and D_Q have disjoint support. Since P and Q are m-torsion points, it follows that mD_P and mD_Q are principle divisors. So there are rational functions say $f_{m,P}$ and $f_{m,Q}$ on $E[\mathbb{F}_{q^k}]$ such that $div(f_{m,P}) = mD_P$ and $div(f_{m,Q}) = mD_Q$. With these notions, the Weil pairing [4] is a bilinear map

$$e_m : E[m] \times E[m] \to \mu_m$$
$$e_m(P, Q) = \frac{f_{m,P}(D_Q)}{f_{m,Q}(D_P)}.$$

The Weil pairing e_m as defined above is well defined i.e. maps to a m^{th} root of unity and is independent of the choice of D_P and D_Q and the functions $f_{m,P}$ and $f_{m,Q}$. This e_m is non-degenerate and efficiently computable. We use Miller's algorithm [4, 24] to compute rational functions $f_{m,P}$ and $f_{m,Q}$ at the divisors D_Q and D_P.

2.3. Tate Pairing

Let E be an elliptic curve which is defined the same as in Weil pairing. Let m be a large prime such that $m|\#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ denotes the order of the rational point group $E(\mathbb{F}_q)$. Let k be the smallest positive integer satisfying $m|q^k - 1$. This k is called embedding degree with respect to m. Let $P \in E(\mathbb{F}_(q^k))[m]$, then $m(P) - m(O)$ is a principal divisor. So we get a rational function $f_{m,P} \in E(\mathbb{F}_{q^k})$ such that $div(f_{m,P}) = m(P) - m(O)$. Now let Q be a point from $E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k})$, then we construct a divisor D of degree zero such that $D \sim (Q) - (O)$. Support of this D should be disjoint from the support of the divisor of $f_{m,P}$. With these notations, the Tate pairing [5] is a bilinear map

$$\bar{e} : E(\mathbb{F}_{q^k})[m] \times E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) \to \mu_m$$

$$\bar{e}(P,Q) = f_{m,P}(D)^{(q^k-1)/m}.$$

Tate pairing is also non-degenerate. It is well defined in the sense that choice of $f_{m,P}$ and D does not matter. It is notable that the evaluation of $f_{m,P}$ at the divisor D can be computed by Miller's algorithm in polynomial time.

2.4. Supersingular Elliptic Curve

An elliptic curve E defined over a field $\mathbb{F}_q$ with $q = p^n$, where p is a prime, is supersingular if $p|t$. Here $t = q + 1 - \#E(\mathbb{F}_q)$ is called trace of the curve E. If $p \nmid t$ then E is ordinary elliptic curve. First Koblitz considered the supersingular elliptic curve $E_1 : y^2 + y = x^3$ over $\mathbb{F}_{2^n}$ and find that $\#E_1(\mathbb{F}_{2^n}) = 2^n + 1$ if n is odd. The embedding degree of this supersingular elliptic curve is $k = 2$. Miller and Kaliski also constructed the popular supersingular elliptic curves with embedding degree $k = 2$. Koblitz (1998) constructed other supersingular elliptic curve $E_2 : y^2 = x^3 - x + 1$ over $\mathbb{F}_{3^n}$. The embedding degree of this curve is $k = 6$ and $\#E_2(\mathbb{F}_{3^n}) = 3^n + 3^{(n+1)/2} + 1$ if n is odd.

The distortion map on a supersingular elliptic curve E over $\mathbb{F}_q$ is a non-rational map that takes a point in $E(\mathbb{F}_q)$ to a point in $E(\mathbb{F}_{q^k})$. Distortion maps play an important role in computing the pairings on supersingular elliptic curves. The map $\phi : (x, y) \to (x + 1, y + x + t)$, where $t \in \mathbb{F}_{2^2}$ with $t^2 + t + 1 = 0$ is a distortion map on the supersingular elliptic curve E_1. This map is an automorphism and its inverse is $\phi^{-1} : (x, y) \to (x + 1, y + x + t + 1)$. The distortion map on the second supersingular elliptic curve E_2 is defined by $\phi : (x, y) \to (\alpha - x, \rho y)$, where $\rho \in \mathbb{F}_{3^{2n}}$ and $\alpha \in \mathbb{F}_{3^{3n}}$ satisfy $\rho^2 + 1 = 0$ and $\alpha^3 - \alpha - 1 = 0$. This map is also an automorphism and its inverse is defined by $\phi^{-1} : (x, y) \to (\alpha - x, -\rho y)$. The distortion map on the curve E_3 is given by $\phi : (x, y) \to (\omega x, y)$, where $\omega^3 = 1$. The inverse of this map is $\phi^{-1} : (x, y) \to (\omega^2 x, y)$.

3. Self Pairing

Practically, the self-pairing $e_s(P, P)$ can be designed by Type 1 pairing, i.e., it can be constructed on supersingular elliptic curves. We construct the self-pairings on the following supersingular elliptic curves:

$$\begin{aligned} E_1 : y^2 + y = x^3 \quad & \text{over the field } \mathbb{F}_{2^n}, \text{ where } n \text{ is odd,} \\ E_2 : y^2 = x^3 - x + 1 \quad & \text{over } \mathbb{F}_{3^n}, \text{ where } n \text{ is odd,} \\ \text{and } E_3 : y^2 = x^3 + b \quad & \text{over the prime field } \mathbb{F}_p, \text{ where } p \equiv 2 \ mod\ 3. \end{aligned}$$

Note that the computation of general bilinear pairing on the curve E_1 has been discussed in [22] and on the curves E_2, E_3 have been discussed in [18].

In this section, we compute the self-pairings on the above curves by using the method of [14]. We use his construction to define self-pairing on the mentioned curves.

Theorem 1. *[14] Let E be supersingular elliptic curves over the ground field $\mathbb{F}_q$ as above in E_1, E_2 and E_3. Let m be a large prime dividing the order of the group $E(\mathbb{F}_q)$. Suppose the embedding degree with respect to m is k. Let π_q be Frobenius endomorphism and let $P \in G_1 = Ker(\pi_q - [1]) \cap E[m]$. Then the self-pairing based on the Weil pairing is defined by*

$$e_s(P,P) \triangleq e_m(P, \phi(P))^{2(q^{k/2}-1)} = f_{m,P}(\phi(P))^{4(q^{k/2}-1)}.$$

Proof. The definition of Weil pairing follows that

$$e_s(P,P) \triangleq e_m(P, \phi(P))^{2(q^{k/2}-1)} = \left(\frac{f_{m,P}(\phi(P))}{f_{m,\phi(P)}(P)}\right)^{2(q^{k/2}-1)}.$$

Note that it has been proved in the paper [25] that

$$f_{m,\phi(P)}(P)^{(q^{k/2}-1)} = f_{m,P}(\phi^{-1}(P))^{(q^{k/2}-1)}.$$

So to prove our result, it is suffices to demonstrate that

$$\left(\frac{1}{f_{m,P}(\phi^{-1}(P))}\right)^{(q^{k/2}-1)} = f_{m,P}(\phi(P))^{(q^{k/2}-1)}$$

i.e. we show that

$$(f_{m,P}(\phi^{-1}(P)) f_{m,P}(\phi(P)))^{(q^{k/2}-1)} = 1. \tag{1}$$

Now let $P = (x_P, y_P) \in G_1$. We show that the equation (1) holds for all the curves E_1, E_2 and E_3.

Case-I: We first consider the supersingular elliptic curve E_1. In this curve $q = 2^n$, where n is odd. By using the result [26] the rational function $f_{m,P}$ on E_1 can be written as $a(x) + b(x)y$, where $a(x)$ and $b(x)$ are rational functions over the finite field $\mathbb{F}_{2^n}$ in terms of x. For convenience, we use the notations a and b in place of $a(x_P + 1)$ and $b(x_P + 1)$. Thus we have

$$\begin{aligned} f_{m,P}(\phi^{-1}(P)) &= a + b(y_P + x_P + t + 1) \\ &= (a + by_P + bx_P) + b(t+1) \end{aligned}$$

and

$$\begin{aligned} f_{m,P}(\phi(P)) &= a + b(y_P + x_P + t) \\ &= (a + by_P + bx_P) + bt \end{aligned}$$

Since $t^2 + t + 1 = 0$, therefore equation (1) follows from Fermat's little theorem.

Case-II: Now we are consider our second curve E_2. In this curve $q = 3^n$, where n is odd. Again by using [26], the rational function $f_{m,P}$ on the curve E_2 can be written as $a(x) + b(x)y$, where $a(x)$ and $b(x)$ are rational functions over $\mathbb{F}_{3^n}$ in terms of x. For convenience, again we use the notations a and b in place of $a(\alpha - x_P)$ and $b(\alpha - x_P)$. Then we have

$$f_{m,P}(\phi^{-1}(P)) = a + by_P\rho$$

and

$$f_{m,P}(\phi(P)) = a - by_P\rho.$$

Now since $\rho^2 + 1 = 0$, therefore equation (1) follows from Fermat's little theorem.

Case III: Now we consider our final curve E_3. In this curve we have $q \equiv 2 \ mod\ 3$. By the same argument, the rational function $f_{m,P}$ on the curve E_3 can be written as $c(y) + d(y)x + e(y)x^2$, where $c(y)$, $d(y)$, and $e(y)$ are rational functions over $\mathbb{F}_q$ in terms of y. Since $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$, so we get

$$\begin{aligned} f_{m,P}(\phi(P)) &= c(y_P) + d(y_P)x_P\omega + e(y_P)x_P^2\omega^2 \\ &= (c(y_P) - e(y_P)x_P^2) + (d(y_P)x_P - e(y_P)x_P^2)\omega \end{aligned}$$

and

$$\begin{aligned} f_{m,P}(\phi^{-1}(P)) &= c(y_P) + d(y_P)x_P\omega^2 + e(y_P)x_P^2\omega^4 \\ &= (c(y_P) - d(y_P)x_P) + (e(y_P)x_P^2 - d(y_P)x_P)\omega \\ &= (c(y_P) - e(y_P)x_P^2) - (d(y_P)x_P - e(y_P)x_P^2)(\omega + 1). \end{aligned}$$

Therefore equation (1) follows from the fact that $\omega^2 + \omega + 1 = 0$ and Fermat's little theorem. So equation (1) holds in all cases and this complete the proof of the theorem 1. □

The general bilinear pairing (Tate pairing) on the curve E_1 was discussed by Soonhak Kwon. The final exponentiation of the proposed self-pairing on E_1 is equal to $4(2^m - 1)$, and that of the Tate pairing $(2^m - 1)$. After computing $(2^m - 1)$, one cubing and one multiplication are required for the proposed self-pairing.

On the other hand, the computation of the rational function $f_{m,P}(\phi(P))$ in Kwon method is very costly because of many inverses and multiplications in field. So the proposed self-pairing is faster than the self-pairing based on the Tate pairing of Kwon. The proposed self-pairings on E_2 and E_3 are faster than the self-pairings based on reduced Tate pairing since the final exponentiation of these self-pairings are simple than that of the latter and Miller's loop are the same for both of them. However, the Miller loop length for the η_T pairing on the curve E_2 is half of the length of that required for the reduced Tate pairing. So the self-pairing proposed in theorem 1 on the curve E_2 will be slower than the self-pairing based on η_T pairing. We provide the improvement of the self-pairing on E_2, as compared to the self-pairing based on η_T pairing by using lemma 1 of [14] and the previous theorem.

Proposition 1. *Let m be a large prime satisfying $m|\#E_2(\mathbb{F}_q)$, where $q = 3^n$ and let t be the trace of the Frobenius endomorphism. Suppose k is the embedding degree with respect to m. Write $T = t - 1$. For $T^i = (t-1)^i \equiv q^i \bmod m$, where $1 \leq i \leq k-1$, we denote $T_i = T^i \bmod m$. Let a_i be least positive integer satisfying $T_i^{a_i} \equiv 1 \bmod m$. Because of this, there exists an integer L_i such that $T_i^{a_i} - 1 = L_i m$. Given the two points $P, Q \in G_1 = Ker(\pi_q - [1]) \cap E_2[m]$, we have*

$$e_m(P, \phi(Q))^{2(q^{k/2}-1)L_i} = \left(\frac{f_{T_i,P}(\phi(Q))}{f_{T_i,Q}(\phi^{-1}(P)} \right)^{2(q^{k/2}-1)c},$$

where $c = \sum_{j=0}^{a_i-1} T_i^{a_i-1-j} q^j \equiv a_i q^{i(a_i-1)} \bmod m$. [See the proof in [14]]

Using the notations as in proposition 1, we define improved self-pairing based on η_T pairing as

$$e_s(P,P) \triangleq \left(\frac{f_{T_i,P}(\phi(P))}{f_{T_i,P}(\phi^{-1}(P))} \right)^{2(q^{k/2}-1)} = f_{T_i,P}(\phi(P))^{4(q^{k/2}-1)}.$$

Proof of this result is immediate from the proposition 1 and theorem 1. This self-pairing is non-degenerate

Remark 1. For the curve $E_2(\mathbb{F}_{3^n})$, a collection of the self-pairings is obtained by varying i and one with the shortest miller loop is considered to be optimal. This optimal self-pairing should have the same Miller loop length as the η_T pairing. Now the final exponentiation of the optimal self-pairing equals $4(3^{3n}-1)$, and that of the η_T pairing which equals $(3^{3n}-1)(3^n+1)(3^n - 3^{(n+1)/2}+1)$. So after computing the exponent $(3^{3n}-1)$ and cubing and one multiplication are required for optimal self-pairing. This is faster than

computing the exponent $(3^n + 1)(3^n - 3^{(n+1)/2} + 1)$ required for η_T pairing. Therefore optimal self-pairing on the curve $E_2(\mathbb{F}_{3^n})$ will be more efficient than the self-pairing based on η_T pairing at any security level.

4. Signature Scheme Based on Self-Pairing

In this section we present digital signature scheme by using proposed self-pairing on supersingular elliptic curves. The author of [16] proposed a new signature scheme without random oracles from bilinear pairing. We use new self-pairing in this scheme to improve the efficiency of the scheme. The security of this scheme depends on a complexity assumption called $(k + 1)$ square roots assumption [16]. We first recall the $(k + 1)$ square root assumption and then present the construction of the scheme.

4.1. The $(k + 1)$ Square Root's Assumption

The $(k + 1)$ square root problem in the system (G, G_T) of groups is as follows:

For an integer k and $x \in_R Z_q, g \in G$, given

$$\{g, \alpha = g^x, h_1, ..., h_k \in Z_q, g^{(x+h_1)^{1/2}}, ..., g^{(x+h_k)^{1/2}}\},$$

compute $g^{(x+h)^{1/2}}$ for some $h \notin \{h_1, h_2, ..., h_k\}$.

We say that $(k + 1)$ square root problem is (t, ε)-hard if for any t-time adversary $\mathcal{A}$, we have

$Pr[\mathcal{A}(g, \alpha = g^x, g^{(x+h_1)^{1/2}}, ..., g^{(x+h_k)^{1/2}} : x \in_R Z_q, g \in G, h_1, ..., h_k \in Z_q) = g^{(x+h)^{1/2}}, h \notin h_1, h_2, ..., h_k] < \varepsilon$, where ε is negligible.

We say that the $(k + 1, t, \varepsilon)$-square root assumptions holds if no t-time algorithm has advantage at least ε in solving the $(k + 1)$-square root problem in (G, G_T), i.e., $(k + 1)$ square root problem is (t, ε)-hard in (G, G_T).

4.2. Construction of the Scheme

Let $e : G \times G \to G_T$ be a bilinear pairing where $|G| = |G_T| = q$ for some prime number q. We assume that the prime q and message m are such that $|q| \geq 160$ and $|m| = 160$. If the signature scheme is intended to be used directly for signing message, then $|m| = 160$ is good enough, since given a suitable collision resistant hash function, one can first hash the message to 160 bits, and then sign the resulting value. Hence the message m can be regarded as an element of Z_q.

To give an exact security proof with a good bound for this signature scheme, we assume that $q \equiv 3 \ mod \ 4$, and the message space is $\{1, 2, ..., (q-1)/2\}$. For any message $m \in \{1, 2, ..., (q-1)/2\}$, if m is not a quadratic residue module q, then $q - m$ will be a quadratic residue modulo q. So system parameters are (G, G_T, q, e, g), where $g \in G$ is a random generator. We describe the signature scheme in the following steps:

Key Generation: We randomly select $x, y \in_R Z_q^*$, and compute $u = g^x, v = g^y$. Then the public and secret keys are (u, v) and (x, y) respectively.

Signing: Given a secret key (x, y), where $x, y \in_R Z_q^*$, and a message $m \in \{1, 2, ..., (q-1)/2\}$, we pick a random integer $r \in_R Z_q^*$. If m is a quadratic residue modulo q, then we compute $\sigma = g^{(x+my+r)^{1/2}} \in G$. Otherwise we compute $\sigma = g^{(x+(-m)y+r)^{1/2}} \in G$. Here $(x + my + r)^{1/2}$ or $(x + (-m)y + r)^{1/2}$ is computed modulo q. If these are not quadratic residues modulo q, we try again with a different random r. So signature is (σ, r).

Verification: Given a public key (G, G_T, q, g, u, v), a message $m \in \{1, 2, ..., (q-1)/2\}$, and a signature (σ, r), we verify that

$$e_s(\sigma, \sigma) = e(uv^m g^r, g)$$

or

$$e_s(\sigma, \sigma) = e(uv^{-m} g^r, g).$$

This verification is correct due to the following properties of pairing:

$$\begin{aligned} e_s(\sigma, \sigma) &= e_s(g^{(x \pm my+r)^{1/2}}, g^{(x \pm my+r)^{1/2}}) \\ &= e_s(g, g)^{(x \pm my+r)^{1/2} . (x \pm my+r)^{1/2}} \\ &= e_s(g, g)^{(x \pm my+r)} \\ &= e(uv^{\pm m} g^r, g). \end{aligned}$$

4.3. Security of Scheme

The security of above scheme based on $(k+1)$-square roots problem in (G, G_T). The following theorem proves that the above scheme is existentially unforgeable in the strong sense under chosen message attacks, provided that the $(k+1)$-square roots assumption holds in (G, G_T).

Theorem 2. *Suppose the $(k+1, t', \varepsilon')$-square root assumption holds in (G, G_T). Then the above signature scheme is (t, q_S, ε)-secure against existential forgery under an adaptive chosen message attack provided that*

$$q_S < k+1, \varepsilon = 2\varepsilon' + 4\frac{q_S}{q} \approx 2\varepsilon', t \leq t' - \Theta(q_S T).$$

Here T is the maximum time for computing a square root in Z_q^* and an exponentiation in G. (For more details see [16])

5. Efficiency of the Scheme

In this section we discuss the efficiency of the signature scheme based on the self-pairing. There exist some secure signature schemes without random oracles from the bilinear pairings, namely $BB04$ scheme [27], $BMS03$ scheme [28] and $CL04$ [29] scheme etc. Compared to $BMS03$ and $CL04$ schemes, this scheme has the advantages in all parameters, such as the public key, signature lengths and performance.

The new signature scheme requires one computation of square root in Z_q^* and one exponentiation in G to sign. For verification, it requires one self-pairing, one or two general pairing. Pairing computation is the most time-consuming in pairing based cryptosystems. Although many papers have been proposed to discuss the complexity of pairings and how to speed up the pairing computation, it still remains time consuming. In this scheme if we pre-compute the pairing $e(u, g) = a, e(v, g) = b$ and $e_s(g, g) = c$, and publish them as a part of the signer's public key. Then, for a message $m \in Z_q^*$, and a signature (σ, r), the verification can be done by $e_s(\sigma, \sigma) = a.b^{\pm m}.c^r$ is true or not. Now verification requires only one self-pairing and two exponentiations in G_T, and exponentiations in G_T are significantly faster than pairing computations.

A signature in this scheme contains of two elements σ and r, where one element σ is in G and other is in Z_q^*. When using a supersingular elliptic curve over finite field $\mathbb{F}_{p^n}$ with embedding degree $k = 6$ and modified Weil pairing, the length of the signature is approximate $2log_2q$ bits. To be more precisely, suppose G is derived from the elliptic curve $E(\mathbb{F}_{3^{97}})$ defined by $y^2 = x^3 - x + 1$, which has 923-bit discrete-log security.

Since on the above defined supersingular elliptic curve, η_T pairing is faster than the modified Weil pairing, so this improves the efficiency of the scheme. We used self-pairing to describe the above scheme and as we showed in section 3 that the self-pairing computation on the above mentioned curve is faster than the general pairing computation. Therefore this scheme now becomes more efficient.

6. Conclusion

In this paper, we first presented the construction of self-pairings on some supersingular elliptic curves. We showed that the proposed self-pairings are efficient than the other ones on the corresponding elliptic curves. Then we presented a signature scheme from self-pairing on elliptic curves. We also showed that the signature scheme from self-pairing is more efficient than the previous one.

References

[1] A.J. Menezes, T.T. Okamoto and S.A. Vanstone, Reducing Elliptic Curve logarithms in a Finite Field, *IEEE Transactions on information theory,* **39** (1993), 1639-1639

[2] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press (2005)

[3] I.F. Blake, G. Seroussi, N.P. Smart, *Advances in Elliptic Curve Cryptography*, Cambridge University Press (2005)

[4] V.S. Miller, The Weil pairing and its efficient calculation, *J. Cryptology* **17(44)** (2004), 235-261

[5] G. Frey, H.G. Ruck, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, *Math. Comp.* **62(206)** (1994), 865-874

[6] E. Lee, H.S. Lee, C.M. Park, Efficient and generalized pairing computation on Abelian varieties, *IEEE Trans. Inform. Theory* **55(4)** (2009), 1793-1803

[7] F. Hess, N.P. Smart, F. Vercauteren, The Eta pairing revisited, *IEEE Trans. Inform. Theory* **52** (2006), 4595-4602

[8] S. Matsuda, N. Kanayama, F. Hess, E. Okamoto, Optimized Versions of the Ate and twisted Ate pairings, *Springer, Heidelberg* LNCS **4887** (2007), 302-312,

[9] F. Vercauteren, Optimal pairings, *IEEE Trans. Inform. Theory* **56** (2010), 455-461

[10] F. Hess, *Pairing Lattices,* In: S.D. Galbraith, K.G. Paterson (ed.) Pairing (2008)

[11] I. Duursma, H.S. Lee, Tate pairing implementation for Hyperelliptic curves $y^2 = x^p - x = d$, In: C.S. Laih (ed.) *ASIACRYPT 2003*, LNCS, **2894** (2003), 111-123.

[12] D.F. Aranha, K. Karabina, P. Longa, C.H. Gebotys, J. Lopez, Faster Explicit Formulas for Computing Pairing over Ordinary Curves, In: K.G. Paterson (ed.) , *EUROCRYPT 2011*, LNCS, **6632** (2011). 48-68

[13] C. Arene, T. Lange, M. Naehrig, C. Ritzenthaler, Faster computation of the Tate pairing, *Journal of Number Theory* **131** (2011), 842-857

[14] C.A. Zhao, F. Zhang, D. Xie, *Faster computation of Self-Pairings*, IEEE Trans. On Inform. Theory, **58(5)** (2012)

[15] F. Zhang, R. Safavi-Naini, W. Susilo, F. Bao, R. Deng, J. Zhou, An efficient signature scheme from bilinear pairings and its applications, *in Proc. Public Key Cryptography*, LNCS **2947** (2004), 277-290

[16] F. Zhang, X. Chen, W. Susilo, and Y. Mu, A new signature scheme without random oracles from bilinear pairings, *in Proc. Int. Conf. Cryptology, Vietnam*, LNCS, **4341** (2006), 67-80.

[17] F. Zhang, R. Safavi-Naini, W. Susilo, ID-based chameleon hashes from bilinear pairings, *Cryptology ePrint Archive, Report* **208** (2003) [online], Available: http://eprint.iacr.org/203

[18] N. Koblitz and A. Menezes, Pairing-based cryptography at high security levels, in Cryptography and Coding, ser. Lecture notes in Computer Science, N. Smart(ed.), *Berlin Germany, Springer*, **3796** (2005), 13-36

[19] S.D. Galbraith, C.A. Zhao, Self-pairings on Hyperelliptic curves, *Preprint, to appear in J. Math. Crypto*, (2012)

[20] H. Wu, R. Feng, Efficient Self-pairing on Ordinary elliptic Curves, *Springer-Verlag Berlin Heidelberg*, LNCS **7876** (2013), 282-293

[21] B. Chen and C.A. Zhao, Self-pairings on supersingular elliptic corves with embedding degree three, Finite Fields and their Applications, *Elsevier*, **28** (2014) 78-93

[22] Soonhak Kwon, Efficient Tate pairing Computation for supersingular elliptic curves over binary fields, *Springer-Verlag Berlin, Heidelberg*, LNCS **3574** (2005), 134-145

[23] William Stallings, *Cryptography and Network Security, Principles and Practice ed.*, Prentice Hall, New Jersey, (2003)

[24] V.S. Miller, *Short programs for functions on curves*, (1986)

[25] C. Park, M. Kim, and M. Yung, A remark on implementing the Weil pairing, *in Inform. Security and Cryptology, ser. Lecture Notes in Computer Science, Berlin, Germany: Springer*, **3822** (2005), 313-323

[26] S.D. Galbraith, F. Hess, and F. Vercauteren, Aspects of pairing inversion, *IEEE Trans. Inform. Theory*, **54(32)** (2008), 5719-5728

[27] D. Boneh and X. Boyen, Short signatures without random oracles, *Advances in Cryptology-Euro crypt*, LNCS **3027** (2004), 56-73

[28] D. Boneh, I. Mironow and V. Shoup, A secure signature scheme from bilinear maps, *CT-RSA* , LNCS **2612** (2003), 98-110

[29] J. Camenisch and A. Lysyanskaya, Signature schemes and anonymous credentials from bilinear maps, *Advances in Cryptology-Crypto*, LNCS **3152** (2004), 56-72,