Skew-Frobenius map on twisted Edwards curve *

Mingqiang Wang[1] Xiaoyun Wang[1] Tao Zhan[2] Yuliang Zheng[3]

1. Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University 250100, Jinan, China

2. School of Mathematics, Jilin University, 130012, Changchun, China

3. Department of Software and Information Systems,
University of North Carolina at Charlotte
9201 University City Blvd Charlotte, NC 28223, USA

Abstract

In this paper, we consider the Frobenius endomorphism on twisted Edwards curve and give the characteristic polynomial of the map. Applying the Frobenius endomorphism on twisted Edwards curve, we construct a skew-Frobenius map defined on the quadratic twist of an twisted Edwards curve. Our results show that the Frobenius endomorphism on twisted Edwards curve and the skew-Frobenius endomorphism on quadratic twist of an twisted Edwards curve can be exploited to devise fast point multiplication algorithm that do not use any point doubling. As an application, the GLV method can be used for speeding up point multiplication on twisted Edwards curve.

Keywords: Edwards curves; birationally equivalent; τ- expansion; skew-Frobenius map

1 Introduction

Edwards [5] introduced a new form of elliptic curves

$$x^2 + y^2 = 1 + dx^2y^2$$

*This work was supported by Major State Basic Research Development Program 973(Grant NO. 2007CB807902); and Nature Science of Shandong Province (Grant No Y2008G23); and Doctoral Fund of Ministry of Education of China (Grant No 20090131120012)

with $d \notin \{0, 1\}$. In [1], this form is generalized to twisted Edwards form $E_{E,a,d}$ defined by

$$ax^2 + y^2 = 1 + dx^2y^2$$

where $a, d \in k$ with $ad(a - d) \neq 0$.

Bernstein and Lange [2] showed that scalar multiplication on Edwards curve is competitive with the Montgomery form for single-scalar multiplication and is the new speed leader for multi-scalar multiplication.

In order to get more efficient cryptosystems, Iijima, Matsuo, Chao and Tsujii[8] proposed a method using a Frobeinus map on the quadratic twist of an elliptic curve. Kozaki, Matsuo, and Shimbara[11] call this map the skew-Frobenius map and show constructions of the skew-Frobenius maps on hyperelliptic curves of genus 2 and 3.

Fix a field k with $char(k) \neq 2$, every twisted Edwards curve over k is birationally equivalent over k to an elliptic curve. By applying the birational map between twisted Edwards curve and elliptic curve, we consider the Frobenius map Π_q on twisted Edwards curves defined over finite field $\mathbb{F}_q$ and give the characteristic polynomial of the Frobenius map. The result shows that the Frobenius endomorphism on Edwards curve can be exploited to devise fast point multiplication algorithm.

Applying the Frobenius map on twisted Edwards curves, we generalize the method in [8] and construct a skew-Frobenius maps on quadratic twist of an twisted Edwards curves. Our result shows that the skew-Frobenius map can be used to speed up point multiplication on twisted Edwards curve. Extended the method in Galbraith et al. [6], the GLV method can be applied to point multiplication on twisted Edwards curve.

We note that the methods of scalar computation on twisted Edwards curves in this paper are much faster than the previous methods.

The paper is organized as follows: section 2 reviews Edwards curves and Frobenius map on elliptic curve. The Frobenius map of twisted Edwards curve are given in section 3. The skew-Frobenius maps are discussed in section 4. Section 5 applies the Frobenius map and the skew-Frobenius to speed up the point multiplication on twisted Edwards curve. The last section is the conclusion.

2 Preliminaries

This section briefly introduces the definitions and notations required in the following sections.

2.1 Edwards curves and twisted Edwards curves

Edwards [5] introduced a new form of elliptic curves

$$x^2 + y^2 = 1 + dx^2y^2$$

with $d \notin \{0, 1\}$, $(0, 1)$ as neutral element and gave a simple and symmetric addition law for such curves:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Here the Edwards curve is denoted by E_d. In [1], this form is generalized to twisted Edwards form $E_{E,a,d}$ defined by

$$ax^2 + y^2 = 1 + dx^2y^2$$

where $a, d \in k$ with $ad(a - d) \neq 0$. The affine addition formula for twisted Edwards in [2] is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Every twisted Edwards curve is birationally equivalent to an elliptic curve in Montgomery form, and vice versa.

The twisted Edwards curve $E_{E,a,d}$ is a quadratic twist of the Edwards curve $E_{E,1,d/a}$. More generally, $E_{E,a,d}$ is a quadratic twist of $E_{E,\overline{a},\overline{d}}$ for any $\overline{a}, \overline{d}$ satisfying $\overline{d}/\overline{a} = d/a$. Conversely, every quadratic twist of a twisted Edwards curve is isomorphic to a twisted Edwards curve; i.e., the set of twisted Edwards curves is invariant under quadratic twists.

2.2 Frobenius map on elliptic curves

Let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) \neq 2$. An elliptic curve E over $\mathbb{F}_q$ is defined as

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

with the point at infinity P_∞, where $a_2, a_4, a_6 \in \mathbb{F}_q$. The q-th power Frobenius map π_q of E is defined as

$$\begin{array}{rccc} \pi_q : & E & \longmapsto & E \\ & (x, y) & \longmapsto & (x^q, y^q). \end{array}$$

Let N_l denote the number of $\mathbb{F}_{q^l}$-points on E. By the Hasse's Theorem, $N_1 = q + 1 - t$ where $t \leq 2\sqrt{q}$, and the characteristic polynomial $\chi_q \in \mathbb{Z}[x]$ of π_q is given by

$$\chi_q(x) = x^2 - tx + q,$$

which satisfies

$$(\pi_q^2 - t\pi_q + q)P = P_\infty$$

for all $P \in E(\overline{\mathbb{F}}_q)$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.

3 Frobenius map on twisted Edwards curves

Let $\mathbb{F}_q$ be a finite field with characteristic different from 2 and $E_{E,a,d}$ defined over $\mathbb{F}_q$. In this section, we consider the q-Frobenius map Π_q of $E_{E,a,d}$

$$\begin{array}{rccc} \Pi_q : & E_{E,a,d} & \longmapsto & E_{E,a,d} \\ & (x,y) & \longmapsto & (x^q, y^q). \end{array}$$

Now we state the main result of this section.

Theorem 1 *Let $E_{E,a,d}$ be a twisted Edwards curve defined over a finite field $\mathbb{F}_q$ and $\sharp E_{E,a,d} = q + 1 - t$. Then the Frobenius map Π_q of $E_{E,a,d}$ satisfies*

$$(\Pi_q^2 - t\Pi_q + q)P = P_\infty$$

for all $P \in E_{E,a,d}(\overline{\mathbb{F}}_q)$.

In order to prove Theorem 1, the following lemmas are needed.

Lemma 1 *[1] Fix a field k with $char(k) \neq 2$. Every twisted Edwards curve over k is birationally equivalent over k to an elliptic curve.*

From Lemma 1, one can see that there exists a elliptic curve E over $\mathbb{F}_q$ such that $E_{E,a,d}(\overline{\mathbb{F}}_q) \cong E(\overline{\mathbb{F}}_q)$. Let σ be the isomorphism. By Theorem 3.2 in [2], $E(\mathbb{F}_q)$ can be defined as

$$v^2 = u^3 + Au^2 + u,$$

where $A = \frac{2(a+d)}{a-d}$. The map

$$\sigma : (x,y) \mapsto (u,v) = \left(\frac{1+y}{1-y}, \frac{\sqrt{B}(1+y)}{(1-y)x}\right)$$

is a birational equivalence from $E_{E,a,d}$ to E, with inverse

$$(u,v) \mapsto (x,y) = \left(\frac{\sqrt{B}u}{v}, \frac{u-1}{u+1}\right),$$

where $B = \frac{4}{a-d}$.

Lemma 2 *Let $E_{E,a,d}$ be a twisted Edwards curve defined over $\mathbb{F}_q$ and E be the birationally equivalent elliptic curve of $E_{E,a,d}$ over $\mathbb{F}_q$. Let $\sharp E(\mathbb{F}_q) = q + 1 - t$ and let σ is the birational map defined as above. Let π_q be the q-power Frobenius map on E. Define $\psi = \sigma^{-1} \circ \pi_q \circ \sigma$. Then*

1. *$\psi \in End(E_{E,a,d})$(i.e. ψ is a homomorphism map on $E_{E,a,d}$).*
2. *For all $P \in E_{E,a,d}(\overline{\mathbb{F}}_q)$, we have*

$$\psi^2(P) - [t]\psi(P) + [q](P) = \mathcal{O}_{E_{E,a,d}}.$$

Proof By the discussion in [1], we have that σ is isomorphism from $E_{E,a,d}$ to E, and π_q is an isogeny from E to itself defined over $\mathbb{F}_q$. Hence ψ is an isogeny of $E_{E,a,d}$ to itself defined over $\mathbb{F}_q$.

For $P \in E_{E,a,d}(\overline{\mathbb{F}}_q)$ writing $Q = \sigma(P) \in E(\overline{\mathbb{F}}_q)$, we have

$$(\pi_q^2 - t\pi_q + q)Q = \mathcal{O}_E.$$

So

$$\sigma^{-1}(\pi_q^2 - t\pi_q + q)\sigma(P) = \mathcal{O}_{E_{E,a,d}}$$

implies

$$\psi^2(P) - [t]\psi(P) + [q](P) = \mathcal{O}_{E_{E,a,d}}.$$

This completes the proof.

Proof of Theorem 1 Let E be the birational equivalent elliptic curve of $E_{E,a,d}$, and ψ be the endomorphism of $E_{E,a,d}$ in Lemma 2. By the definition of ψ, for all $P = (x, y) \in E_{E,a,d}(\overline{\mathbb{F}}_q)$,

$$\begin{aligned}\psi(x,y) &= (\sigma^{-1} \circ \pi_q \circ \sigma)(x,y) = (\sigma^{-1} \circ \pi_q)\left(\frac{1+y}{1-y}, \frac{\sqrt{B}(1+y)}{(1-y)x}\right) \\ &= \sigma^{-1}\left(\frac{(\sqrt{B})^q(1+y^q)}{1-y^q}, \frac{1+y^q}{(1-y^q)x^q}\right) = ((\sqrt{B})^{1-q}x^q, y^q).\end{aligned}$$

If B is not an square in $\mathbb{F}_q$, then $(\sqrt{B})^{1-q} = -1$, therefore for all $P \in E_{E,a,d}(\overline{\mathbb{F}}_q)$, $\psi(P) = -\Pi_q(P)$. In this case $\sharp E(\mathbb{F}_q) = q + 1 + t$. If B is an square in $\mathbb{F}_q$, then $(\sqrt{B})^{1-q} = 1$. Hence we have for all $P \in E_{E,a,d}(\overline{\mathbb{F}}_q)$, $\psi(P) = \Pi_q(P)$ and furthermore $\sharp E(\mathbb{F}_q) = \sharp E_{E,a,d}(\mathbb{F}_q) = q + 1 - t$. Hence by Lemma 2, we can complete the proof of Theorem 1.

We will apply the Frobenius map to accelerate the scalar multiplication speed on twisted Edwards curve.

4 Skew-Frobenius map on quadratic twist of an Edwards curves

In this section, we will construct a skew-Frobenius map on quadratic twist of a twisted Edwards curve according to the Frobenius map on twisted Edwards curves defined in section 3. This construction extends the result in [8].

In general, the twisted Edwards curve $E_{E,a,d}$ defined over $\mathbb{F}_q$ is a quadratic twist of a twisted Edwards curve $E_{E,\overline{a},\overline{d}}$ for any $\overline{a}, \overline{d}$ satisfying $\frac{\overline{d}}{\overline{a}} = \frac{d}{a}$. Let

$$\begin{array}{rccc} \phi: & E_{E,a,d} & \longmapsto & E_{E,\overline{a},\overline{d}} \\ & (x,y) & \mapsto & (\sqrt{\alpha}x, y) \end{array}$$

where $\alpha = \frac{a}{\overline{a}}$. If α is not a square in the field $k = \mathbb{F}_q$, then the map ϕ is an isomorphism from $E_{E,a,d}$ to $E_{E,\overline{a},\overline{d}}$ over $k(\sqrt{\alpha})$. A quadratic twist Edwards curve of $E_{E,a,d}$ is denoted by $E^t_{E,a,d}$.

Remark. In practice cases, we may need $\alpha \in \mathbb{F}_{q^n}$, for some positive integer n.

We will show how to construct the skew Frobenius map Π^t_q on $E^t_{E,a,d}$. According to the definition of the Frobenius map Π_q defined on $E_{E,a,d}$, a skew Frobenius map of $E^t_{E,a,d}$ can be defined as follows:

$$\Pi^t_q: \quad E^t_{E,a,d} \overset{\phi^{-1}}{\longmapsto} E_{E,a,d} \overset{\Pi_q}{\longmapsto} E_{E,a,d} \overset{\phi}{\longmapsto} E^t_{E,a,d}.$$

Therefore

$$\Pi^t_q P = (\sqrt{\alpha}^{q-1} x^q, y^q)$$

for all $P = (x,y) \in E^t_{E,a,d}(\overline{\mathbb{F}}_{q^2})$.

Theorem 2 *Let $E_{E,a,d}$ be a twisted Edwards curve defined over $\mathbb{F}_q$ and $E^t_{E,a,d}$ be a quadratic twist Edwards curve of $E_{E,a,d}$. Let $\sharp E_{E,a,d}(\mathbb{F}_q) = q + 1 - t$ and let the map ϕ is an isomorphism from $E_{E,a,d}$ to $E^t_{E,a,d}$ over $k(\sqrt{\alpha})$. Let Π_q be the q-power Frobenius map on $E_{E,a,d}$. Define $\Pi^t_q = \phi \circ \pi_q \circ \phi^{-1}$. Then for all $P \in E^t_{E,a,d}(\overline{\mathbb{F}}_{q^2})$ we have*

$$(\Pi^t_q)^2(P) - [t]\Pi^t_q(P) + [q](P) = \mathcal{O}_{E^t_{E,a,d}}.$$

Proof The proof is similar to Theorem 1, we omit it here.

Like the the Frobenius map Π_q, the skew-Frobenius map Π^t_q defined on $E^t_{E,a,d}$ can be used to accelerate the scalar multiplication speed on twisted Edwards curve.

5 Applications

To accelerate the scalar multiplication, Solinas[12, 13] exploit the Frobenius endomorphism to devise fast point multiplication algorithm that do not use any point doubling. The following expansion of nP based on the characteristic polynomial of the Frobenius endomorphism of elliptic curve, has been used to compute the scalar multiplication

$$nP = \sum_{i \geq 0} c_i \tau^i P,$$

where the c_i are elements of a small set, e.g., $\{-q/2, \cdots, q/2\}$. For this type of curves, scalar multiplication can be improved by using the nonadjacent form of base-τ expansion of the scalar [10, 3]. When the characteristic finite field $\mathbb{F}_q$ is large, the Gallant, Lambert and Vanstone[7] design a method for speeding up point multiplication.

5.1 Application 1: τ-adic method

Let $E_{E,a,d}$ be a twisted Edwards curve defined over $\mathbb{F}_q$ and $E^t_{E,a,d}$ be the quadratic twist of $E_{E,a,d}$. By Theorem 2 there exists a complex number τ such that the skew-Frobenius endomorphism on $E^t_{E,a,d}$ can be identified as τ. τ can be interpreted as a complex number defined by the equation:

$$\tau^2 - t\tau + q = 0,$$

where $t = q + 1 - \sharp E^t_{E,a,d}$. A window width w τ nonadjacent form (w-τNAF) for $k \in Z[\tau]$ is the following representation of k:

$$k = \sum_{i=0}^{t-1} b_i \tau^i,$$

where

1. for each $i = 0, 1, \ldots, t-1$, $b_i \in C$;
2. any w consecutive coefficients $b_i, b_{i+1}, \cdots, b_{i+w-1}$ contains at most one nonzero element.

For $P \in E^t_{E,a,d}(\overline{\mathbb{F}}_{q^2})$, the evaluation of nP can be done efficiently by

$$nP = \sum_{i=0}^{t-1} (\Pi_q^t)^i (b_i P). \tag{1}$$

The $(\Pi_q^t)^i P$ can be computed as

$$(\Pi_q^t)^i P = (\sqrt{\alpha}^{q^i-1} x^{q^i}, y^{q^i}).$$

Applying the Frobenius map Π_q on $E_{E,a,d}$, the above method can be used on twisted Edwards curve.

For $\beta \in \mathbb{F}_{q^k}$, the computation of β^q is very easy if the element is represented with a normal base of $\mathbb{F}_{q^k}$. Although computation of Π_q^t costs more multiplication than Π_q, the scalar computation on Edwards curve using the formula (1) can be much faster than the previous methods, if $\sharp E_{E,a,d}^t(\mathbb{F}_{q^2})$ is of almost-prime order.

5.2 Application 2: GLV method

In this subsection, we apply the GLV method to point multiplication on Edwards curve by extending the method in Galbraith et al. [6].

Theorem 3 *Let $char(\mathbb{F}_q) > 3$ be a prime number and let $E_{E,a,d}$ be a twisted Edwards curve over $\mathbb{F}_q$ with $q+1-t$ points. Let $E_{E,a,d}^t$ over $\mathbb{F}_{q^2}$ be the quadratic twist of $E_{E,a,d}(\mathbb{F}_{q^2})$, then $\sharp E_{E,a,d}^t(\mathbb{F}_{q^2}) = (q-1)^2 + t^2$. Let $r|\sharp E_{E,a,d}^t(\mathbb{F}_{q^2})$ be a prime number such that $r > 2q$. Let $\phi : E_{E,a,d} \longmapsto E_{E,a,d}^t$ be the twisting isomorphism defined over $\mathbb{F}_{q^4}$. Let*

$$\Pi_q^t = \phi \circ \Pi_q \circ \phi^{-1}.$$

For $P \in E_{E,a,d}^t(\mathbb{F}_{q^2})[r]$, we have $(\Pi_q^t)^2(P) + P = \mathcal{O}_{E_{E,a,d}^t}$.

Proof By the well-known Weil theorem, we have $E_{E,a,d}(\mathbb{F}_{q^2}) = (q+1)^2 - t^2$ and $E_{E,a,d}^t(\mathbb{F}_{q^2}) = (q-1)^2 + t^2$. Since $r > 2q$, hence $r \nmid \sharp E_{E,a,d}(\mathbb{F}_{q^2}) = (q+1-t)(q+1+t)$. Therefore by the assumption of the theorem, one have $r|\sharp E_{E,a,d}^t(\mathbb{F}_{q^4}) = \sharp E_{E,a,d}^t(\mathbb{F}_{q^2})\sharp E_{E,a,d}(\mathbb{F}_{q^2})$ while $r \nmid \sharp E_{E,a,d}^t(\mathbb{F}_{q^4})$. This implies that for $P \in E_{E,a,d}^t(\mathbb{F}_{q^2})[r]$, $\Pi_q^t(P)$ belongs to $E_{E,a,d}^t(\mathbb{F}_{q^2})[r]$. It follows that for $P \in E_{E,a,d}^t(\mathbb{F}_{q^2})[r]$ there exists $\lambda \in \mathbb{Z}$ such that $\Pi_q^t(P) = \lambda P$.

By the definition as above, $\Pi_q^t(x,y) = (\alpha^{\frac{q-1}{2}} x^q, y^q)$, where $\alpha \in \mathbb{F}_{q^2}$ is not a square in $\mathbb{F}_{q^2}$. And Hence

$$(\Pi_q^t)^2(x,y) = (\alpha^{\frac{q^2-1}{2}} x^{q^2}, y^{q^2}).$$

Since $\alpha \in \mathbb{F}_{q^2}$ and is not a square in $\mathbb{F}_{q^2}$, so $\alpha^{\frac{q^2-1}{2}} = -1$. By the assumption of the theorem, $P \in E_{E,a,d}^t(\mathbb{F}_{q^2})$, we have $x^{q^2} = x, y^{q^2} = y$. Therefore,

$$(\Pi_q^t)^2(x,y) = (-x,y).$$

This completes the proof.

As an example, we will concentrate on the twisted Edwards curve defined over $\mathbb{F}_q$ to describe the method.

Example 2 Let $p = 2^{255} - 19$ be a prime. $d = \frac{121665}{121666}$ is not a square in the field $\mathbb{F}_p$. Then quadratic twist Edwards curve of $E_{E,1,d}$ over $\mathbb{F}_p^4$ is $E_{E,\sqrt{d},(\sqrt{d})^3}$. The twisting isomorphism over $\mathbb{F}_{q^4}$ can be defined as

$$\phi : E_{E,1,d} \longmapsto E_{E,\sqrt{d},(\sqrt{d})^3}, \quad (x, y) \mapsto (d^{-\frac{1}{4}}x, y)$$

The twist Frobenius map on $E_{E,\sqrt{d},(\sqrt{d})^3}$ is written as

$$\Pi_p^t(x, y) = (d^{\frac{1-p}{4}}x^p, y^p).$$

For $P \in E_{E,\sqrt{d},(\sqrt{d})^3}(\mathbb{F}_{p^2})$,

$$(\Pi_p^t)^2(x, y) = (d^{\frac{1-p^2}{4}}x^{p^2}, y^{p^2}).$$

Since d is not a square in $\mathbb{F}_p$ and $p \equiv 1(\text{mod}4)$, one has $d^{\frac{1-p^2}{4}} = -1$ in $\mathbb{F}_{p^2}$. Therefore, for $P \in E_{E,\sqrt{d},(\sqrt{d})^3}(\mathbb{F}_{p^2})$ we have $(\Pi_p^t)^2(P) + P = \mathcal{O}_{E_{E,\sqrt{d},(\sqrt{d})^3}}$.

6 Conclusion

The main purpose of this paper is to discuss the endomorphism on the twisted Edwards curves defined over finite field $\mathbb{F}_q$. Firstly, properties of the Frobenius map on twisted Edwards curve are investigated and the characteristic polynomial of the map is given. Applying the the Frobenius endomorphism on twisted Edwards curve, we construct the skew-Frobenius map defined on the quadratic twist of twisted Edwards curve. Our results show that the Frobenius endomorphism on Edwards curve and the skew-Frobenius endomorphism on twisted Edwards curve can be used for speeding up point multiplication on twisted Edwards curve.

Acknowledgement The author gratefully acknowledges Dr. Guangwu Xu for his useful comments.

References

[1] Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 389-405. Springer, Heidelberg (2008)

[2] Bernstein, D. J., Lange, T.: Faster addition and doubling on elliptic curves, in ASIACRYPT 2007, LNCS, Vol. 4833, pp. 29-50. Springer, (2007)

[3] Blake, I., Murty V. K., Xu, G.: Efficient algorithms for Koblitz curves over fields of characteristic three. *Journal of Discrete Algorithms*. 3, 113-124(2005)

[4] I. Blake, V. K. Murty and G. Xu, Nonadjacent radix-τ expansions of integers in Euclidean imaginary quadratic number fields, *Canadian Journal of Mathematics*, 60, 1267-1282(2008)

[5] Edwards, H.M.: A normal form for elliptic curves. Bulletin of the AMS 44(3), 393-422 (2007)

[6] Galbraith, S., Xibin Lin, Scott, M.: Endomophisms for faster elliptic cryptography on a large class of curves. Eurocrypt 2009, LNCS 5479, p.518-535(2009)

[7] Gallant, R.P., Lambert, R.J., Vanstone, S.A.: Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 190-200. Springer, Heidelberg (2001)

[8] T. Iijima, K. Matsuo, J. Chao, and S. Tsujii: Cnstruction of Frobenius maps of twist elliptic curves and its application to elliptic scalar multiplication. In Proc. of SCIS2002, pp 699C702,(2002)

[9] Koblitz, N.: An elliptic curve implementation of the finite field digital signature algorithm. In: *Advances in Cryptology–CRYPTO'1998*. LNCS, vol. 1462, pp.327-337(1998)

[10] Koblitz, N.: CM-curves with good cryptographic properties. In: *Advances in Cryptology–CRYPTO'1991*. LNCS, vol. 218, pp.279-287(1991)

[11] Kozaki, S., Matsuo, K., Shimbara, Y.: Skew-Frobenius Maps on Hyperelliptic Curves, IEICE Trans. E91-A(7), 1839-1843 (2008)

[12] Solinas, J.: Efficient arithmetic on Koblitz curves. *Designs, Codes and Cryptography*. 19, 195-249(2000)

[13] Solinas, J.: An improved algorithm for arithmetic on a family of elliptic curves, Advances in Cryptology Crypto '97, 357-371(1997)