SCIS 2002 The 2002 Symposium on Cryptography and Information Security
Shirahama,Japan, Jan.29-Feb.1,2002
The Institute of Electronics,
Information and Communication Engineers

Construction of Frobenius maps of twists elliptic curves and its application to elliptic scalar multiplication

Tsutomu IIJIMA * Kazuto MATSUO † Jinhui CHAO ‡ Shigeo TSUJII *

Abstract— The Frobenius expansion is known as an efficient method to implement addition of the Mordel-Weil group of elliptic curves and has been successfully applied to fast elliptic curve cryptosystems. However since the elliptic curves on which the Frobenius expansion can be used are defined over extension fields $\mathbb{F}_{q^n}/\mathbb{F}_q$, so that the $\#E(\mathbb{F}_{q^n})$ cannot be a prime number. Thus only a subgroup of the Mordell-Weil group can be used in the cryptosystems, which means certain loss of computational efficiency.

This paper firstly shows a method to apply the Frobenius expansion to quadratic twists of elliptic curves. Such twist curves can be constructed to be of prime order then applied to cryptosystems. The existence of prime order curves is also confirmed experimantally.

Keywords: Elliptic curves, Elliptic curve cryptosystems, Quadratic twists of elliptic curves, Frobenius map, Frobenius expansion

1 Introduction

Let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) \neq 2, 3$. An elliptic curve E over $\mathbb{F}_q$ is defined as

$$E : Y^2 = X^3 + aX + b \tag{1}$$

with the point at infinity P_∞, where $a, b \in \mathbb{F}_q$, $4a^3 + 27b^2 \neq 0$.

The q-th power Frobenius map π_q of E is defined as

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

Notice that the P_∞ is mapped into itself by π_q. The Frobenius map π_q acts non–trivially for all $P \in E(\overline{\mathbb{F}}_q) \backslash E(\mathbb{F}_q)$.

The characteristic polynomial $\chi_q \in \mathbb{Z}[X]$ of π_q is given by

$$\chi_q(X) = X^2 - tX + q, \ |t| \leq 2\sqrt{q}, \tag{2}$$

which satisfies

$$(\pi_q^2 - t\pi_q + q)P = P_\infty \tag{3}$$

for all the $P \in E(\overline{\mathbb{F}}_q)$.

In an cryptosystem based on the Mordell-Weil group of the elliptic curve (1) over $E(\mathbb{F}_{q^n})$, encryption and decryption times is dominated by computation of scalar multiplications kP for $P \in E(\mathbb{F}_{q^n})$, $k \in \mathbb{Z}$. To reduce the processing time, the following expansion of kP, based on (3), has been used to compute the scalar multiplications

$$kP = \sum_{i \geq 0} c_i \pi_q^i P. \tag{4}$$

We will call this expansion the Frobenius expansion. Computation of the right hand side of (4) turned out to be faster than computation of kP by any other methods in many cases. Recently, various researches have been reported on fast elliptic curve cryptosystems over $E(\mathbb{F}_{q^n}), n > 1$ using the Frobenius expansion [1][2][3].

In a cryptosystem using the Frobenius expansion, the order of the base point $P \in E(\mathbb{F}_{q^n})$, $\#\langle P \rangle$ should be a prime number from security consideration. However, since $E(\mathbb{F}_{q^n}) \supseteq E(\mathbb{F}_q)$, there is no any point P of a prime order $\#\langle P \rangle$ which can generate the Mordell-Weil group or $\langle P \rangle = E(\mathbb{F}_{q^n})$ for $n > 1$.

Such a property of these curves is undesirable to be used in cryptosystems, in the sense that (i) a Mordell-Weil group $E(\mathbb{F}_{q^n})$ of unnecessarily larger size has to be used, (ii) the search for random points in $\langle P \rangle$ will be slower.

As to the (i), we know that among general curves $E/\mathbb{F}_{q^n}$ there are curves whose $\mathbb{F}_{q^n}$–rational points $E(\mathbb{F}_{q^n})$ are prime orders. Also there exists base points $P \in E(\mathbb{F}_{q^n})$ such that $\langle P \rangle = E(\mathbb{F}_{q^n})$ and

$$\#\langle P \rangle = \#E(\mathbb{F}_{q^n}) \approx q^n.$$

In the case of elliptic curve cryptosystems using the Frobenius expansion on $E/\mathbb{F}_q$, however, one can at most expect

$$\#E(\mathbb{F}_{q^n}) = \#E(\mathbb{F}_q)\#\langle P \rangle$$

even if the base point $P \in E(\mathbb{F}_{q^n})$ was chosen as with the maximal order. In this case, the order of $\langle P \rangle$ can

* Department of Information and System Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan
† Research and Development Initiative, Chuo University, 42-8 Ichigaya Honmura-cho, Shinjuku-ku, Tokyo, 162-8473 Japan
‡ Department of Electrical and Electronic Engineering, Chuo University 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

at most be

$$\#\langle P\rangle \approx q^{n-1}$$

since $\#E(\mathbb{F}_q) \approx q$. Therefore, in order to obtain the same security, the cryptosystems using the Frobenius expansion have to use curves $E/\mathbb{F}_{q^{n+1}}$. In the other words, extra cost for the field operation is necessary comparing with using curves of prime orders defined over $\mathbb{F}_{q^n}$,

If one can find a way to use prime order curves and at the same time the Frobenius expansion can be applied, then more efficient cryptosystems can be constructed on these curves. This paper firstly shows that the quadratic twists of curves can be used with such properties. Then construction of Frobenius map on these curves is presented. Moreover, distribution of orders of the twist curves is investigated by experiments.

2 Quadratic twists of elliptic curves

This section defines the quadratic twist of an elliptic curve E and discusses its properties.

Let $c \in \mathbb{F}_{q^n}$ be a non–quadratic residue over $\mathbb{F}_{q^n}$. A quadratic twist E_t of E over $\mathbb{F}_{q^n}$ is defined as

$$E_t : Y^2 = X^3 + ac^2X + bc^3. \tag{5}$$

Close relations are known between E and E_t. e.g., although

$$E_t(\mathbb{F}_{q^n}) \ncong E(\mathbb{F}_{q^n}),$$

however,

$$E_t(\overline{\mathbb{F}}_{q^n}) \cong E(\overline{\mathbb{F}}_{q^n}).$$

In particular,

$$E_t(\mathbb{F}_{q^{2n}}) \cong E(\mathbb{F}_{q^{2n}}) \cong E(\mathbb{F}_{q^n}) \times E_t(\mathbb{F}_{q^n}). \tag{6}$$

Moreover the q^n–th power Frobenius map of E_t is $-\pi_q^n$ and

$$End(E_t) \cong End(E) \cong \mathcal{O} \subset K,$$

where $\mathcal{O}$ is an order of the CM field K of E.

Therefore there exists a map in $End(E_t)$ whose characteristic polynomial is the same as that of π_q i.e. $\chi_q(X)$. If this map can be efficiently computed, one can obtain efficient cryptosystems on $E_t(\mathbb{F}_{q^n})$ using its Frobnius expansion.

3 Construction of the Frobenius map of E_t

This section shows how to define and compute the Frobenius map π_q^t of E_t.

According to (6), defining π_q^t as

$$\pi_q^t : \ E_t(\mathbb{F}_{q^{2n}}) \xrightarrow[\sigma_1]{\sim} E(\mathbb{F}_{q^{2n}}) \xrightarrow[\pi_q]{} E(\mathbb{F}_{q^{2n}}) \xrightarrow[\sigma_2]{\sim} E_t(\mathbb{F}_{q^{2n}}) \tag{7}$$

then both the π_q^t and the π_q have the same characteristic polynomial $\chi_q(X)$ obviously. Moreover it is well known that σ_i in (7) are defined as follows [4]:

$$\begin{aligned} \sigma_1 : E_t(\mathbb{F}_{q^{2n}}) &\longrightarrow E(\mathbb{F}_{q^{2n}}) \\ (x,y) &\longmapsto (c^{-1}x, c^{-3/2}y), \end{aligned}$$

$$\begin{aligned} \sigma_2 : E_t(\mathbb{F}_{q^{2n}}) &\longrightarrow E(\mathbb{F}_{q^{2n}}) \\ (x,y) &\longmapsto (cx, c^{3/2}y). \end{aligned}$$

Therefore,

$$\pi_q^t P = (c^{1-q}x^q, c^{3(1-q)/2}y^q) \tag{8}$$

for all $P = (x,y) \in E_t(\mathbb{F}_{q^{2n}})$.

Now we denote the restriction of π_q^t to $E_t(\mathbb{F}_{q^n})$ with the same symbol π_q^t. Then we have $\pi_q^t P \in E_t(\mathbb{F}_{q^n})$ for all $P \in E_t(\mathbb{F}_{q^n})$ because $2 \mid 1-q$ hence $c^{3(1-q)/2} \in \mathbb{F}_{q^n}$. Therefore the π_q^t is well–defined as a nondegenerated map on $E_t(\mathbb{F}_{q^n})$ as follows:

$$\begin{aligned} \pi_q^t : E_t(\mathbb{F}_{q^n}) &\longrightarrow E_t(\mathbb{F}_{q^n}) \\ (x,y) &\longmapsto (c^{1-q}x^q, c^{3(1-q)/2}y^q). \end{aligned}$$

P_∞ is again fixed by the π_q^t.

For $P \in E_t(\mathbb{F}_{q^n})$, kP can be computed by

$$kP = \sum_{i \geq 0} c_i (\pi_q^t)^i P \ , \ i \in \mathbb{Z}_{>0} \tag{9}$$

with the same c_i given in (4).

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

$$(\pi_q^t)^i P = (c^{1-q^i}x^{q^i}, c^{3(1-q^i)/2}y^{q^i}).$$

Although computation of π_q^t costs two more multiplications than π_q, the scalar multiplication using (9) can be faster than previous methods, if $E_t(\mathbb{F}_{q^n})$ has a prime order.

4 Distribution of $\#E_t(\mathbb{F}_{q^n})$

The previous section showed that π_q^t can be efficiently computed on $E_t(\mathbb{F}_{q^n})$. Therefore if $E_t(\mathbb{F}_{q^n})$ has a prime order, a faster elliptic curve cryptosystem can be constructed on it.

This section discusses whether $E_t(\mathbb{F}_{q^n})$ could have a prime order or not in either cases of $n \neq 2^m$ or $n = 2^m$, where m is a positive integer.

Since it is necessary for the distribution of the orders to have enough randomness to apply E_t to the cryptosystems, this section also calculates the distribution of $E_t(\mathbb{F}_{q^n})$ by experiments.

4.1 In the case of $n \neq 2^m,\ m \geq 0$

Let $n = 2^e n_r$ such that $2 \nmid n_r$, E_{t_0} be a quadratic twist of E over $\mathbb{F}_{q^{2^e}}$. For such a E_{t_0},

$$E_{t_0}(\mathbb{F}_{q^n}) \ncong E(\mathbb{F}_{q^n}),$$
$$E_{t_0}(\mathbb{F}_{q^{2n}}) \cong E(\mathbb{F}_{q^{2n}}) \cong E(\mathbb{F}_{q^{2n}}) \times E_{t_0}(\mathbb{F}_{q^{2n}}).$$

These relations and (5) induce

$$E_{t_0}(\mathbb{F}_{q^n}) \cong E_t(\mathbb{F}_{q^n}).$$

Therefore

$$\#E_{t_0}(\mathbb{F}_{q^{2^e}}) \mid \#E_t(\mathbb{F}_{q^n})$$

and the $E_t(\mathbb{F}_{q^n})$ cannot have a prime order.

4.2 In the case of $n = 2^m,\ m \geq 0$

The $E_t(\mathbb{F}_{q^n})$ could have a prime order in this case. The following example shows a prime order $E_t(\mathbb{F}_{q^n})$.

Example

Let $p = 2^{20} - 3$ and $n = 8$. An elliptic curve E over $\mathbb{F}_p$ is defined as

$$E:\ Y^2 = X^3 + 440307X + 451281.$$

The characteristic polynomial of the p–th power Frobenius map π_p of E is given as

$$\chi_p(X) = X^2 - 475X + p.$$

Now we define a twist E_t of E over $\mathbb{F}_{p^n}$ as

$$E_t:\ Y^2 = X^3 + 440307c^2X + 451281c^3,$$

where $c \in \mathbb{F}_{p^n}$ is a non–quadratic residue. Then $E_t(\mathbb{F}_{p^n})$ has a 160bit prime order

$$\#E_t(\mathbb{F}_{p^n}) = 146146818654806866052591765 \\ 9233378417576832630689.$$

4.3 Computation of order distribution

We computed $\#E_t(\mathbb{F}_{p^n})$ of all $E/\mathbb{F}_p$ for each $p = 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049$ and $n = 1, 2, 4, 8, 16, 32$.

The Figure 1–6 show the distributions of $\#E_t(\mathbb{F}_{p^n})$. The distribution is normalized and expressed in the number of curves versus deviation of their orders from the center of the Hasse range. Specifically, the number of curves is a sum of curves over different characteristic fields but whose orders have almost the same deviation from the center of the Hasse range.

The distribution of $\#E_t(\mathbb{F}_p)$, which is the same as that of $\#E(\mathbb{F}_p)$, follows the Sato conjecture by the Figure 1. It seems that the distributions of $\#E_t(\mathbb{F}_{p^n}), n > 2$ have enough randomness, so that we can obtain enough prime order curves over such extension fields. In conclusion, enough many secure cryptosystems can be constructed on $E_t(\mathbb{F}_{p^n}), n > 2$.

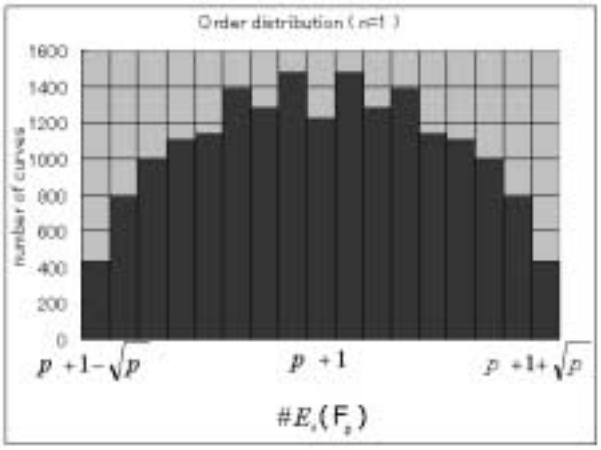

Figure 1: The distribution of $\#E_t(\mathbb{F}_p)$

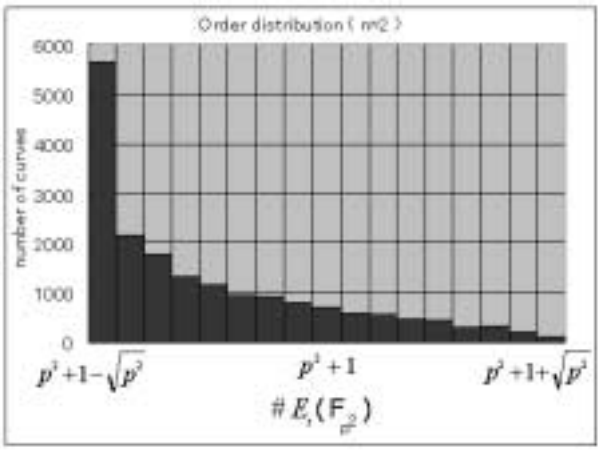

Figure 2: The distribution of $\#E_t(\mathbb{F}_{p^2})$

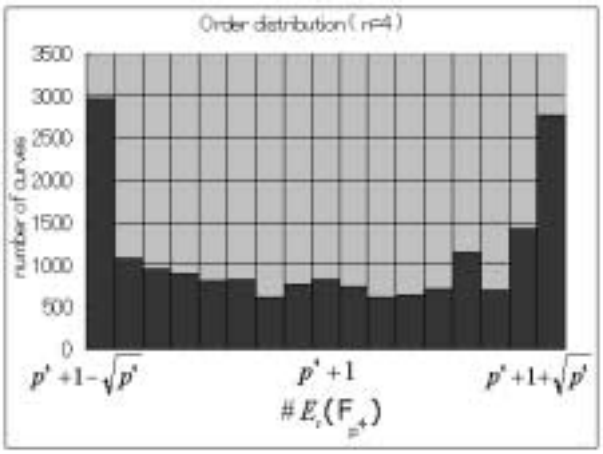

Figure 3: The distribution of $\#E_t(\mathbb{F}_{p^4})$

5 Conclusion

This paper showed that the Frobenius expansion can be efficiently applied to the quadratic twists of elliptic curves and also enough many prime order twist curves can be constructed. These results suggest that cryptosystems using the twists and their Frobenius maps can be faster than the systems by the previous methods. However the proposed method costs two more multiplications over $\mathbb{F}_{q^n}$ than the previous method. Thus further research, especially implementations, is necessary to approve the practical efficiency of the proposed method.

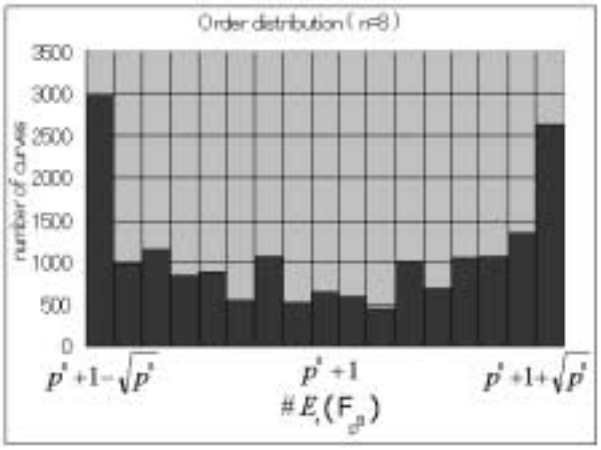

Figure 4: The distribution of $\#E_t(\mathbb{F}_{p^8})$

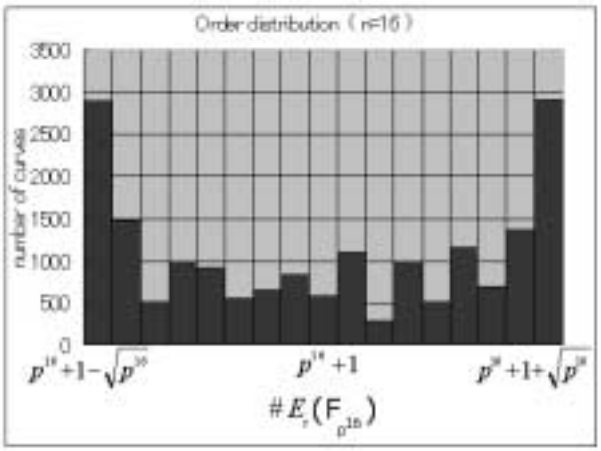

Figure 5: Distribution of $\#E_t(\mathbb{F}_{p^{16}})$

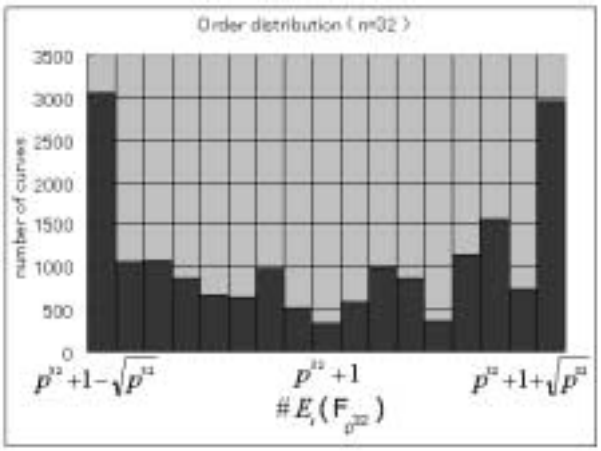

Figure 6: Distribution of $\#E_t(\mathbb{F}_{p^{32}})$

Acknowledgement

The authors would like to thank Dr. Kazumaro Aoki whose comments motivated this research.

A part of this research was supported by Telecommunications Advancement Organization of Japan (TAO).

References

[1] K.Aoki, F.Hoshino, and T.Kobayashi, *A cyclic window algorithm for ECC defined over extension fields*, to appear in Proc. of ICICS2001,2001.

[2] T.Kobayashi, H.Morita, K.Kobayashi, F.Hoshino, *Fast elliptic curve algorithm combining Frobenius map and table reference to adapt to higher characteristic*, Advances in Cryptology - EUROCRYPTO'99, Lecture Notes in Computer Science, no.1592,Springer-Velag,1999,pp.176-189.

[3] N.Koblitz, *CM-curves with good cryptographic properties*, Advances in Cryptology-CRYPTO'91,Lecture Notes in Computer Science, no.576,1992,pp.279-287.

[4] J.H.Silverman, *The arithmetic of elliptic curves*, Graduate Text in Mathematics, no.106, Springer-Velag, 1988.

[5] J.A.Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*,Advances in Cryptology - CRYPTO'97, Lecture Notes in Computer Science, no.1294, Springer-Verlag,1997, pp.357-371.

[6] H.Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, 1993.