An Improved Method of Multiplication on Certain Elliptic Curves

Young-Ho Park[1,⋆], Sangho Oh[1], Sangjin Lee[1,⋆⋆],
Jongin Lim[1], and Maenghee Sung[2]

[1] CIST, Korea University, Seoul, Korea
{youngho,sangho,sangjin,jilim}@cist.korea.ac.kr
[2] KISA, Seoul, Korea
mhsung@kisa.or.kr

Abstract. The Frobenius endomorphism is known to be useful in efficient implementation of multiplication on certain elliptic curves. In this note a method to minimize the length of the Frobenius expansion of integer multiplier, elliptic curves defined over small finite fields, is introduced. It is an optimization of previous works by Solinas and Müller. Finally, experimental results are presented and compared with curves recommended in standards by time-performance of multiplication.

1 Introduction

Recent issues of implementation of elliptic curve cryptosystems(for short, ECC) are primarily focused on fast scalar multiplication on elliptic curves. Traditional 'exponentiation' methods for multiplicative groups are straightforwardly applied to scalar multiplication. Such a modification seems to be a bottleneck in accelerating multiplication on elliptic curves since doubling operation is as expensive as addition. In [4], [9], [5] and [6], multiplication on elliptic curves defined over small finite fields is carried out rapidly using the Frobenius map. As known recently in [8], in case of odd characteristic field, it is also possible to speed up scalar multiplication in a similar way. In addition, the length of the Frobenius expansion can be reduced to one half with the use of a division algorithm by a specific algebraic integer whose norm is equal to the order of a given elliptic curve. Roughly replacing doublings by the Frobenius maps together with the reduction gives the running time improvement of 400% (see [9,6]).

ECC-related standards almost all recommend to use so-called 'good' curves. Here the 'good' curves mean that they are cryptographically secure and efficient in implementation. To satisfy such two properties, commonly recommended curves may be chosen to be of compactness in that the security parameter of each curve is almost the same as its field-size. This requirement may come to extreme restriction of the use of Frobenius-based methods since the size of defining

[⋆] This work was supported by grant RND project 2001-S-092 of KISA

[⋆⋆] This work was supported by grant No. 1999-10300-001-2 from the Basic Research Program of the Korea Science & Engineering Foundation.

D. Naccache and P. Paillier (Eds.): PKC 2002, LNCS 2274, pp. 310–322, 2002.

fields should be very small, say like a binary field. We here would like to discuss an observation in order to extend properly the concept of the compactness. For cryptographic uses of elliptic curves, their order should has a large prime factor and scalar multiplication is performed actually on a cyclic subgroup of the large prime order, rather than on the whole group. This observation indicates that the reduction method mentioned above holds a redundant factor. In this note we'll introduce a method to minimize the length of the Frobenius expansion for scalar multiplication on certain elliptic curves by cutting off the redundant and so show that this approach can widen the margin of the 'good' curve.

This paper is organized as follows: In Section 2 an introduction to elliptic curves is given and the previous works, for convenient description, are reviewed briefly. In Section 3 we describe an improved reduction method which removes the redundant. Curves for use in public key cryptography are listed in Table 3 and we compare the length of Frobenius expansion on them by using three different methods in Section 4. In Section 5 we present new 'good' curves with efficient and secure property and give a comparison of them with recommended curves in standards. In Section 6 attacks known so far against subfield curves are introduced.

2 Frobenius Map and Integer Representation

From the viewpoint of application, a class of non-supersingular curves defined over finite fields of characteristic two has attracted attention of cryptographers. In particular, we are concentrated on elliptic curves defined over small fields, say, $\mathbb{F}_{2^s}$ $s \leq 5$. The reason that we restrict the category of fields is to speed up multiplication on elliptic curves. As well-known, expensive doubling operations on non-supersingular curves defined over small fields, can be replaced by the much easier Frobenius map. Hence, in what follows, all elliptic curves mean non-supersingular curves defined over small finite fields of characteristic two and their underlying fields are extensions of the small defining field with odd prime exponents. Let $\mathbb{F}_q$ be a finite field of q elements where q is a power of characteristic 2, which is rather small. We denote by $\overline{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$. Take an elliptic curve $E/\mathbb{F}_q$ given by the Weierstrass equation of the form

$$y^2 + xy = x^3 + a_2x^2 + a_6 \tag{1}$$

where a_2, a_6 in $\mathbb{F}_q$ and $a_6 \neq 0$. Then the qth-power Frobenius endomorphism of $E/\mathbb{F}_q$ is defined by

$$\Phi : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q).$$

From Hasse's famous result, the number of $\mathbb{F}_q$-rational points of E is closely related to an integer t by the formula:

$$\#E(\mathbb{F}_q) = q + 1 - t$$

where t is the trace of the Frobenius endomorphism Φ satisfying the equation

$$\Phi^2 - t\Phi + q = 0.$$

Note that t should be odd for a non-supersingular elliptic curve $E/\mathbb{F}_q$. Some facts related with the Frobenius expansion of elements in $\mathbb{Z}[\Phi]$ are presented with no proof. For details, the reader can be referred to [6].

Lemma 1. *[6] Let $\rho \in \mathbb{Z}[\Phi]$, there exists an integer r, $-q/2 \leq r \leq q/2$, and $u \in \mathbb{Z}[\Phi]$ such that*

$$\rho = u\Phi + r.$$

In particular, if we choose $r \in \{-q/2+1, \cdots, q/2\}$, then r and u are unique.

Lemma 2. *For $q \geq 4$, let $\rho \in \mathbb{Z}[\Phi]$ be such that $N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\rho) \leq (\sqrt{q}+1)^2$. Then ρ has a Φ-expansion of length at most 4, where the magnitude of each integral coefficient is bounded by $q/2$.*

Theorem 1. *[6] For $q \geq 4$, let $\rho \in \mathbb{Z}[\Phi]$. Then ρ can be represented as*

$$\rho = \sum_{i=0}^{k} r_i \Phi^i$$

where $r_i \in \{-q/2+1, \cdots, q/2\}$ and $k \leq \lceil 2 \log_q \|\rho\| \rceil + 3$.

In Theorem 1, $\| \cdot \|$ means the Euclidean norm.

Algorithm 1 (Frobenius expansion of ρ)

```
 Input: $\rho = r_1 + r_2\Phi \in \mathbb{Z}[\Phi]$.
Output: $m_i$ is a sequence of integers such that
        $\rho = \sum_{i=0}^{k} m_i\Phi^i, m_i \in [-q/2+1, q/2]$

1)  Set $x = r_1$, $y = r_2$ and $i = 0$.
2)  While $|x| > q/2$ or $|y| > q/2$, do the followings :
 a)   Compute $z \equiv x \pmod{q}$.
 b)   Set $m_i = \begin{cases} z & \text{if } z \leq q/2, \\ z - q & \text{otherwise.} \end{cases}$
 c)   Set $h = (m_i - x)/q,\ x = y - th,\ y = h$, and $i = i + 1$.
3)  $m_i = x, m_{i+1} = y$.
4)  Return $m_i$.
```

3 Reduction of the Length of Frobenius Expansions

For public key cryptography, the group order of $E(\mathbb{F}_{q^n})$ should have a large prime factor p. Let P be a point of $E(\mathbb{F}_{q^n})$ of prime order p. We denote $\#E(\mathbb{F}_{q^n})$ the group order of $E(\mathbb{F}_{q^n})$ and write $\#E(\mathbb{F}_{q^n}) = hp$ where h is called the cofactor of $E(\mathbb{F}_{q^n})$. The main computational problem in elliptic curve public key cryptosystems is scalar multiplication mP for a large integer $m < p$. According to

Theorem 1, the length of Frobenius expansion of m depends on the norm of m, i.e $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(m) = m^2$ which is approximately equal to q^{2n}. As in [9] and [8], by a reduction modulo $\Phi^n - 1$, they could reduce the expansion length by nearly 50% as follows:

1') $\Phi^n(Q) = Q$ implies $(\Phi^n - 1)Q = O$ for any point $Q \in E(\mathbb{F}_{q^n})$, where O denotes the point at infinity.
2') Dividing m by $\Phi^n - 1$, we obtain a remainder $\rho' \in \mathbb{Z}[\Phi]$ such that
$$N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\rho') < \frac{9+4q}{4} N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\Phi^n - 1) = \frac{9+4q}{4} \# E(\mathbb{F}_{q^n}) \approx q^{n+1}.$$
3') We have $mQ = \rho' Q$ for any point $Q \in E(\mathbb{F}_{q^n})$.
4') Replacing multiplication by m by multiplication by ρ' reduces its expansion length by nearly half.

Under the consideration of cryptographic applications, we want to utilize scalar multiplication on the subgroup $< P >$ rather than that on all points of it. In this aspect, if the cofactor h is not trivial, that is $h \geq \# E(\mathbb{F}_q) \neq 1$, then this approach for reduction has some redundant factor. Because it is achieved by modulo $\Phi^n - 1$ whose norm is the order of an elliptic curve, that is $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\Phi^n - 1) = \# E(\mathbb{F}_{q^n})$.

To exclude the aforementioned redundant and so to minimize the length of the Frobenius expansion, we now will give an improved method which generalizes that of Müller[6] and Smart[8]. Let us consider multiplication on the cyclic subgroup $< P >$ of large prime order p, rather than on the whole group $E(\mathbb{F}_{q^n})$. Recall that the Frobenius map Φ acts on $< P >$ as a multiplication map λ, where λ is a root of the characteristic polynomial of Φ modulo p. Hence, we have $\Phi(P) = \lambda P$ and since $\Phi^2 - t\Phi + q$ is the characteristic polynomial of Φ, $\bar{\Phi} = t - \Phi$ is the conjugate of Φ. We assume that there exists an element $\alpha = a + b\Phi \in \mathbb{Z}[\Phi]$ such that
$$N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(a + b\Phi) = s_p p \ \text{ and } (a + b\Phi)P = O \tag{2}$$
for some small positive integer s_p. In fact, if we find $\alpha = a + b\Phi \in \mathbb{Z}[\Phi]$ such that $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\alpha) = s_p p$ then we have
$$(a + b\lambda)(a + bt - b\lambda) \equiv 0 \pmod{p}$$
since $(a + b\Phi)(a + b\bar{\Phi}) = (a + b\Phi)(a + b(t - \Phi)) = (a + b\Phi)(a + bt - b\Phi) = s_p p$. Therefore, we have $(a + b\Phi)P = O$ or $(a + b\bar{\Phi})P = O$.

Remark 1. It is clear that there exists a positive integer $s_p \leq h = \# E(\mathbb{F}_{q^n})/p$ satisfying (2) since $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\Phi^n - 1) = \# E(\mathbb{F}_{q^n}) = hp$. But the s_p is in general smaller than the cofactor h. (See Theorem 2 and Table 1.)

Roughly speaking, the main idea of our method is to replace $\Phi^n - 1$ by $\alpha = a + b\Phi$ by which we divide a multiplier m in order to reduce the expansion length. Since $\mathbb{Z}[\Phi]$ is μ-Euclidean for some positive real number μ (see [8]), we can divide m by α and obtain a remainder ρ with $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\rho) < \mu N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\alpha)$.

So we replace mP by ρP. Our method gives the Frobenius expansion of ρ which is shorter than that of ρ' by the previous works and in fact, it has minimal length. It will be shown theoretically and on experiment that this method reduces the expansion length by roughly $\lfloor \log_q(\#E(\mathbb{F}_{q^n})/(s_p p)) \rfloor = \lfloor \log_q(h/s_p) \rfloor$ (see Theorem 3 and Table 3). Compared with the cofactor h, the fact that s_p is small leads us to decrease the length. But notice that it does not work on all of points of $E(\mathbb{F}_{q^n})$ but all of points of order p. This method can be briefly described as follows:

1) Find $\alpha = a + b\Phi$ such that $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\alpha) = s_p p$ for some small positive integer s_p and $(a + b\Phi)P = O$.
2) Dividing m by $\alpha = a + b\Phi$, we obtain a remainder $\rho \in \mathbb{Z}[\Phi]$ such that

$$N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\rho) < \mu N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\alpha), \quad \text{with } 0 < \mu \leq \frac{(9+4q)}{16}.$$

3) We have $mP = \rho P$ for any point in the subgroup of order p.
4) Replacing multiplication by m by multiplication by ρ reduces its expansion length by a little more than that of [9] and [8].

Now we describe our method in detail. First, we give a good upper bound on s_p satisfying (2) which guarantees that s_p be a small integer.

Lemma 3. *(See [10]). Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field. Then every non-zero ideal $\mathcal{P}$ of K has an ideal $\mathcal{I}$ with $N_{K/\mathbb{Q}}(\mathcal{I}) \leq \frac{2}{\pi}\sqrt{|D|}$ such that $\mathcal{I}\mathcal{P} = (\alpha)$ for some $\alpha \in O_K$, the ring of integers in K.*

Theorem 2. *Let $\#E(\mathbb{F}_{q^n})$ be divisible by a large prime p and $p^2 \nmid \#E(\mathbb{F}_{q^n})$. If $D = t^2 - 4q$ has no square factor, then there exists an element $\alpha = a + b\Phi \in \mathbb{Z}[\Phi]$ such that*

$$N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(a + b\Phi) = s_p p$$

for some positive integer $s_p < 1.28\sqrt{q}$.

Proof. Let $\#E(\mathbb{F}_{q^n}) = hp$ and $K = \mathbb{Q}(\sqrt{D})$. Since $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\Phi^n - 1) = N_{K/\mathbb{Q}}(\Phi^n - 1) = \#E(\mathbb{F}_{q^n}) = hp$, it is obviously that p splits in $K/\mathbb{Q}$. Let $\mathcal{P}$ be a prime ideal of K such that $N_{K/\mathbb{Q}}(\mathcal{P}) = p$. By Lemma 3, there exists an ideal $\mathcal{I}$ such that $\mathcal{I}\mathcal{P} = (\alpha)$ for some $\alpha \in O_K$ and $N_{K/\mathbb{Q}}(\mathcal{I}) \leq \frac{2}{\pi}\sqrt{|D|}$. Set $s_p = N_{K/\mathbb{Q}}(\mathcal{I})$. From Hasse theory, we have

$$s_p \;\leq\; \frac{2}{\pi}\sqrt{|D|} \;=\frac{2}{\pi}\sqrt{|t^2 - 4q|} \;\leq\; \frac{2}{\pi}2\sqrt{q} \;<\; 1.28\sqrt{q}.$$

Hence we have $\alpha \in O_K$ such that $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\mathcal{I}\mathcal{P}) = s_p p$ with $s_p < 1.28\sqrt{q}$. Now it remains to prove that $\alpha \in \mathbb{Z}[\Phi]$. Notice that $O_K = Z[\theta]$ where $\theta = (1 + \sqrt{D})/2$ because t is odd and $D \equiv 1 \pmod 4$. Since $\Phi^2 - t\Phi + q = 0$, we have $\Phi = (t \pm \sqrt{D})/2$ and

$$\theta = \begin{cases} \Phi - (t-1)/2 & \text{if } \Phi = (t + \sqrt{D})/2, \\ -\Phi + (t+1)/2 & \text{if } \Phi = (t - \sqrt{D})/2. \end{cases}$$

Therefore $\alpha \in O_K$ if and only if $\alpha \in \mathbb{Z}[\Phi]$, which completes the proof. □

Corollary 1. *Under the condition above, assume that $D = t^2 - 4q$ has a square factor, $s^2 | D$ and $D' = D/s^2$ has no square factor. Then there exists an element $\alpha = a + b\Phi \in \mathbb{Z}[\Phi]$ such that*

$$N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\rho)(a + b\Phi) = s_p p$$

for some positive integer $s_p < 1.28 s^2 \sqrt{q}$.

Proof. From the fist part of the proof of Theorem 2, we have

$$\alpha' \in O_K \text{ such that } N_{K/\mathbb{Q}}(\alpha') = s'_p p$$

with $s'_p < 1.28\sqrt{q}$. But in general $\alpha' \notin \mathbb{Z}[\Phi]$. It is easy to check that $s\alpha' \in \mathbb{Z}[\Phi]$. Put $\alpha = s\alpha' \in \mathbb{Z}[\Phi]$ and $s_p = s^2 s'_p$. Then $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\alpha) = s_p p$, which completes the proof. □

In Theorem 2, we have obtained an upper bound $1.28\sqrt{q}$ on s_p if $D = t^2 - 4q$ has no square factor. Since q is small, so is the upper bound and notice that $\log_q s_p < 1$. If $D = t^2 - 4q$ has a square factor, it is also guaranteed that there exists an element $\alpha \in \mathbb{Z}[\Phi]$ such that $N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\alpha) = s_p p$. But s_p in general increases in size. The case where $q = 16, n = 47, t = -1$ in Table 3 is an example. It is easily checked that $D = t^2 - 4q = -3^2 \cdot 7$. Since the ring of integers of $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-7})$ is principal domain, we have $s'_p = 1$ and so $s_p = s^2 s'_p = 9$. The following Table 1 gives upper bounds on s_p for $q = 2^s \leq 32$ where $D = t^2 - 4q$ has no square factor.

Table 1. Upper bounds on small positive integer s_p for $q = 2^s \leq 32$

q	2	4	8	16	32
$\lfloor 1.28\sqrt{q} \rfloor$	1	2	3	5	7

It should be briefly pointed out that we need in advance to find $\alpha \in \mathbb{Z}[\Phi]$ satisfying (2). The problem of solving norm equations in $\mathbb{Z}[\Phi]$ can be done using the known methods such as Shanks' algorithm [7], lattice reduction method [11] or Cornacchia's algorithm [1]. In fact, this can be performed in the setup procedure for elliptic curve $E(\mathbb{F}_{q^n})$ and so it takes no costs for scalar multiplication.

Proposition 1. *Let $\alpha = a + b\Phi \neq 0 \in \mathbb{Z}[\Phi]$. If $\beta \in \mathbb{Z}[\Phi]$ then there exist $\delta, \rho \in \mathbb{Z}[\Phi]$ such that $\beta = \delta\alpha + \rho$ and $N_{\mathbb{Q}[\Phi]/\mathbb{Z}}(\rho) < \mu N_{\mathbb{Q}[\Phi]/\mathbb{Z}}(\alpha)$ with $0 < \mu \leq (9 + 4q)/16$.*

Proof. Since $\Phi^2 - t\Phi + q$, we say $\Phi = (t + \sqrt{D})/2$ where $D = t^2 - 4q$. Set $N_\alpha = N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\alpha)$ and $c = -\lfloor t/2 \rfloor$. Setting $\Phi' = \Phi + c$, we change a $\mathbb{Z}$-basis $\{1, \Phi\}$ to $\{1, \Phi'\}$ and then $\mathbb{Z}[\Phi] = \mathbb{Z}[\Phi']$. Notice that $\Phi' = (1 + \sqrt{D})/2$ since t is odd. Then α can be written by $a_1 + b_1\Phi'$ in term of this new basis. For a given dividend β, we let $\gamma = \beta/\alpha$ and then we have

$$\gamma = \beta/\alpha = \beta\bar{\alpha}/N_\alpha = \frac{x_1 + x_2\Phi'}{N_\alpha}$$

where $\bar{\alpha}$ denotes the complex conjugate of α. Take $\delta = y_1 + y_2\Phi'$ with $y_i = \lfloor x_i/N_\alpha \rceil$ $(i = 1, 2)$, where $\lfloor x \rceil$ denotes the nearest integer to x. Finally, take $\rho = \alpha(\gamma - \delta)$, then since $\beta = \alpha\gamma, \alpha\delta \in \mathbb{Z}[\Phi]$, $\rho \in \mathbb{Z}[\Phi]$. It is easily checked that

$$\begin{aligned} N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\rho)/N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\alpha) &= N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\gamma - \delta) \leq N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\tfrac{1}{2} + \tfrac{1}{2}\tfrac{1+\sqrt{D}}{2}) \\ &= \tfrac{1}{4}N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\tfrac{3+\sqrt{D}}{2}) = \tfrac{1}{4}(\tfrac{9-D}{4}) \\ &< \tfrac{1}{4}((9+4q)/4). \qquad \square \end{aligned}$$

Proposition 1 shows that $\mathbb{Z}[\Phi]$ is μ-Euclidean for some μ such that $0 < \mu \leq (9+4q)/16$. This improves a bound of μ by $1/4$ compared to that of [8, Theorem 5]. Our computational experiments show in Table 2 that the averages of upper bounds of μ's listed in Table 3 are roughly 70% smaller than that of Proposition 1.

Table 2. Experimental Comparison of μ for $q = 2^s \leq 32$

q	2	4	8	16	32
$(9+4q)/16$	1.06	1.56	2.56	4.56	8.56
Average of upper bounds of μ	0.25	0.40	0.69	1.21	2.29

Using the proof of Proposition 1, we consequently give an efficient Algorithm to compute a remainder ρ from m, q, t and $\alpha = a + b\Phi$.

Algorithm 2 (**Divide** m **by** $\alpha = a + b\phi$)

```
Input:  $m \in \mathbb{N}, q, t$ and $\alpha = a + b\Phi$.
Output: $\rho = r_1 + r_2\Phi$ such that $N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\rho) < \mu N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\alpha)$.

Precomputations
1) $N_\alpha = N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\alpha) = s_p p,\ c = -\lfloor t/2 \rfloor$
2) Set $\Phi' = \Phi + c$ and $N = N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\Phi')$.
3) $a_1 = a - bc,\ b_1 = b$. (Represent $\alpha = a_1 + b_1\Phi'$).
Main
4) $x_1 = m(a_1 + b_1)$ and $x_2 = -mb_1$.
5) $y_i = \lfloor x_i/N_\alpha \rceil$ $(i = 1, 2)$.
6) $r'_1 = m - (a_1y_1 - Nb_1y_2)$ and $r'_2 = -(a_1y_2 + b_1y_1 + b_1y_2)$.
7) $r_1 = (r'_1 + r'_2c)$ and $r_2 = r'_2$.
8) Return $r_1, r_2$.
```

Proof. From the proof of Preposition 1, if we put $c = -\lfloor t/2 \rfloor$ and $\Phi' = \Phi + c$, then $\alpha = a + b\Phi = a + b(\Phi' - c) = (a - bc) + b\Phi' = a_1 + b_1\Phi'$. Note that Putting $\beta = m$ and $T = Tr_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\Phi')$ in the proof of Proposition 1, we have

$$\gamma = m/\alpha = m\bar{\alpha}/N_\alpha = \frac{m(a_1 + b_1 T) - m b_1 \Phi'}{N_\alpha} = \frac{x_1 + x_2\Phi'}{N_\alpha}.$$

Since $\delta = y_1 + y_2\Phi'$ with $y_i = \lfloor x_i/N_\alpha \rceil$ $(i = 1, 2)$, we have

$$\rho = m - \alpha\delta = m - (a_1 y_1 - N b_1 y_2) - (a_1 y_2 + b_1 y_1 + T b_1 y_2)\Phi'.$$

Notice that $T = Tr_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\Phi') = 1$ if t is odd, which justifies Algorithm 2. □

According to Proposition 1, the length of Frobenius expansion of ρ obtained by dividing m by α instead of $\Phi^n - 1$ can be determined in the following Theorem.

Theorem 3. *For any integer m, let $\rho \in \mathbb{Z}[\Phi]$ be a remainder obtained by dividing m by $\alpha = a + b\Phi$ in Algorithm 2. The expansion length of ρ is at most $\lceil \log_q(\mu s_p p) \rceil + 4$.*

Proof. It follows from Theorem 1 that the length $k + 1$ of Frobenius expansion of ρ is at most $\lceil 2 \log_q ||\rho|| \rceil + 4 = \lceil \log_q N_{\mathbb{Q}[\Phi]/\mathbb{Q}}(\rho) \rceil + 4 \leq \lceil \log_q(\mu s_p p) \rceil + 4$ by Proposition 2. □

For a random large integer $m \approx p$, the expansion length of ρ is in general equal to $\lceil \log_q(\mu s_p p) \rceil + 4$, and similarly that of ρ' obtained by dividing m by $\Phi^n - 1$ is in general equal to $\lceil \log_q(\mu \# E(\mathbb{F}_{q^n})) \rceil + 4$. Hence, the difference of the two lengths is roughly $\lfloor \log_q(\# E(\mathbb{F}_{q^n})/(s_p p)) \rfloor = \lfloor \log_q(h/s_p) \rfloor$. It will be exactly shown in our computational experiments.

4 Experimental Results

In this section we will first deal with a general method computing the order $\# E(\mathbb{F}_{q^n})$ of an elliptic curve E defined over a small field $\mathbb{F}_q$, which can be described as follows: Let $t_0 = 2, t_1 = t = q + 1 - \# E(\mathbb{F}_q)$, and for $l \geq 2$,

$$t_l = t_1 t_{l-1} - q t_{l-2}.$$

Then the group order of E is given as $\# E(\mathbb{F}_{q^n}) = q^n + 1 - t_n$.

Now experimental results for the previous theoretical claims are given for $q \leq 2^5$. This restriction of q allows us to use the Frobenius map for fast multiplication on elliptic curves. For reference, the larger q is hardly useful in practical implementation since it requires too much precomputation. Also, for cryptographic use, the order of each curve should have a large prime factor. We looked at extension fields $\mathbb{F}_{q^n}$ with $q^n \leq 2^{550}$ and tried to find curves whose order have a large prime factor p at least 160 bits and whose cofactor $h < 2^{24}$. The cases of its cofactor being equal to the order of the group $E(\mathbb{F}_q)$ were left out in Table 3.

In Table 3, we compared the lengths of expansion by using three different methods with 10^5 random numbers $m \in [1, p-1]$ for each curve. If one uses no reduction method, the length of expansion of m is expected to be less than or equal to $\lceil \log_q m^2 \rceil + 4$. If one uses a reduction method modulo $\Phi^n - 1$ to obtain a remainder ρ' then its expansion length of ρ' is expected to be less than or equal to $\lceil \log_q(\mu \# E(\mathbb{F}_{q^n})) \rceil + 4$. In a similar way, if one divides m by α satisfying (2) to obtain a remainder ρ, we expect that the length of expansion of ρ is at most $\lceil \log_q(\mu s_p p) \rceil + 4$. To minimize the length of expansion we applied the new reduction method to these curves, which was more efficient than the previous methods (see Table 3).

Table 3. The case $q = 2$

						The expansion length by using		
n	t	$\log_2 p$	h	s_p	μ	no reduction	$\Phi^n - 1$	α
277	1	264	15514	1	0.25	523	274	260
307	-1	289	351212	1	0.25	575	304	286

Table 3. (continue). The case $q = 4$

						The expansion length by using		
n	t	$\log_2 p$	h	s_p	μ	no reduction	$\Phi^n - 1$	α
97	1	179	58204	1	0.42	176	96	88
139	1	266	6676	1	0.42	264	138	131
163	3	316	1306	1	0.25	315	162	157
181	1	349	13036	1	0.42	347	180	173
191	-1	363	880134	1	0.42	361	190	180
239	-1	464	20082	2	0.42	462	238	231
251	-1	482	1518054	1	0.42	480	250	239
271	1	522	1645516	1	0.42	519	270	259

5 New Concept of Compactness

We begin by recalling the concept of compactness mentioned in the introduction. A compact curve has the security parameter which is almost the same with the bit-size of the underlying field. Table 4 lists a correspondence of ECC(in [12]) to RSA, where the securities of ECC and RSA are estimated in terms of the Pollard-ρ method and the general number field sieve method respectively. Curves in Table 4 are used widely in almost all standards for public-key cryptography including P1363 and ANSI X9.62. They are secure and compact. For example, the security parameter and the underlying field size of the curves in sect193

Table 3. (continue). The case $q = 8$

						The expansion length by using		
n	t	$\log_2 p$	h	s_p	μ	no reduction	$\Phi^n - 1$	α
71	-3	199	30684	2	0.58	131	70	66
71	-1	200	12790	2	0.75	131	70	66
89	3	257	1074	2	0.58	170	88	85
101	-1	288	62630	1	0.75	190	100	95
107	1	309	6856	1	0.74	204	106	102

Table 3. (continue). The case $q = 16$

						The expansion length by using		
n	t	$\log_2 p$	h	s_p	μ	no reduction	$\Phi^n - 1$	α
47	-1	166	5042178	9	1.42	82	46	42
97	3	367	2118494	3	1.25	183	96	91

Table 3. (continue). The case $q = 32$

						The expansion length by using		
n	t	$\log_2 p$	h	s_p	μ	no reduction	$\Phi^n - 1$	α
37	-5	163	7491206	4	2.25	64	37	33
41	3	183	8297610	5	2.60	72	40	37
41	9	195	1992	1	1.08	77	41	38
47	-1	220	57562	4	2.75	87	46	44
73	-3	349	120924	6	2.60	138	72	70
101	-7	491	32360	2	1.76	195	101	98
101	1	491	19424	2	2.72	195	100	98

series are 192-bit and 193-bits respectively. In particular, sect163, 233 and 283, except for sect193, include elliptic curves defined over $\mathbb{F}_2$.

As well-known in [9], multiplication on them is performed very fast using the Frobenius map, when compared with that on curves defined over large finite field. Table 5 shows that efficient implementation of curve arithmetic is essential in ECC for constrained applications such as mobile communication. In fact, the running time of multiplication on sect163r1 is not adequate for practical mobile service, say digital signature. In this context, it is natural that we focus on elliptic curves defined over small finite fields of characteristic 2 which are the Frobenius operation-available. Except for binary curves, they may not fulfill the previous concept of compactness. Here we want to expand it reasonably in order to contain them into the category of 'good' curves.

Now we note two factors which play an important role in efficient implementation of arithmetic in curves given here. One of them is the size of the underlying field. The other is the length of the Frobenius expansion for multiplication on such curves. The previous sections show how to minimize that easily. Table 6 shows that harmonizing properly two factors can give a new concept of compactness in aspects of efficiency and security. Indeed, a new curve $E(\mathbb{F}_{2^{213}})$ have a good favor over the sect193. For example, the former allows the stronger security and higher performance as compared with them of the latter. In particular, we note that no Frobenius-operation available curves defined over $\mathbb{F}_{2^{193}}$ exist.

Hence we propose to add to a family of compact curves, the Frobenius operation-available curves with the sufficiently large security parameter.

Table 4. Comparison of ECC with RSA

ECC	RSA	security($\frac{\sqrt{\pi n}}{2}$)
sect163[12]	1024 bits	2^{80}
sect193[12]	1536 bits	2^{96}
sect233 [12]	2240 bits	2^{112}
sect283[12]	3456 bits	2^{128}

Table 5. Elliptic Curve Arithmetic on mobile

1 full multiplication	CDMA3100 (ARM7 TDMI)	PentiumII 650Mhz
sect163k1	0.48 sec	1.32 ms
sect163r1	1.82 sec	5.02 ms

Table 6. Elliptic Curves for ECC

Elliptic Curves	$q = 8, n = 71, t = -3$ $s_p = 2$ $p = 199$ bits	$q = 8, n = 101, t = -1$ $s_p = 1$ $p = 288$ bits
Reduction by α (Full multiplication)	$\mathbb{F}_{2^{213}}$ (9.01 ms)	$\mathbb{F}_{2^{303}}$ (25.29 ms)
Reduction by $\Phi^n - 1$ (Full multiplication)	$\mathbb{F}_{2^{213}}$ (9.62 ms)	$\mathbb{F}_{2^{303}}$ (26.71 ms)
Elliptic Curves	sect193 [12]	sect283 [12]
With no Frobenius map (Full multiplication)	$\mathbb{F}_{2^{193}}$ (20.4 ms)	$\mathbb{F}_{2^{283}}$ (53.32 ms)

6 Attacks against Subfield Curves

Let E be an elliptic curve defined over a subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^n}$, where q is a power of 2. We can consider attacks against the discrete logarithm problem(for short, DLP) on the curve E in two ways. In case of n being a large prime, the DLP is infeasible under all attacks known so far, including the GHS attack [2] and the Pollard ρ-methods [3,13]. For the others, it can be broken by taking an isogeny $E \to E'$ such that E' is defined over $\mathbb{F}_{q^n}$ and applying to the GHS attack. The underlying fields focused in this paper satisfy the former condition and are secure.

7 Conclusion

We have introduced a method of improving performance of scalar multiplication on certain elliptic curves and have presented theoretical reasons on it. The proposed method is to minimize the length of the Frobenius expansion under the consideration of cryptographic use and takes roughly the improvement of $\lfloor \log_q(\#E(\mathbb{F}_{q^n})/(s_p p)) \rfloor = \lfloor \log_q(h/s_p) \rfloor$, compared with the old reduction methods. As pointed out in previous sections, the proposed method shows that a lot of efficient curves for ECC can be optimized in aspects of compactness. To conclude, we propose the Frobenius operation-available curves for use in mobile-based ECC.

References

1. G. Cornacchia, *"Su di un metodo per la risoluzione in numeri interi dell' equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$"*, Giornale di Matematiche di Battaglini, **46** (1908), 33-90.
2. P. Gaudry, F. Hess and N. Smart, *"Constructive and destructive facets of Weil descent on elliptic curves",* to appear J. Cryptology.
3. R. Gallant, R. Lambert, and S. Vanstone, *"Improving the parallelized Pollard lambda search on binary anomalous curves",* Math. of Com., **69** (2000), 1699-1705.
4. N. Koblitz, *"CM-curves with good cryptographic properties"*, In Advances in Cryptology, CRYPTO 91, LNCS 576, Springer-Verlag (1992), 279-287.
5. W. Meier, O. Staffelbach, *"Efficient multiplication on certain non-supersingular elliptic curves"*, Advances in Cryptology, Crypto'92, 333-344.
6. V. Müller, *"Fast multiplication on elliptic curves over small fields of characteristic two"*, Journal of Cryptology, **11** (1998), 219-234.
7. D. Shanks, *"Five number theoretic algorithms"* In Proc. 2nd Manitoba Conference on Numerical Mathematics (1972), 51-70.
8. N.P. Smart, *"Elliptic curve cryptosystems over small fields of odd characteristic"*, Journal of Cryptology, **12** (1998), 141-151.
9. J. Solinas, *"Efficient arithmetic on Koblitz curves",* Design, Codes and Cryptography, **19** (2000), 195-249.
10. I. Stewart, D. Tall, *"Algebraic Number Theory"*, Chapman and Hall, Halsted Press, 1979.

11. B. Vallée,*Une approche géométrique des algorithmes de réduction des réseaux en petite dimension"*, (1986) Thése, Université de Caen.
12. 'Standard for Efficient Cryptography'.
13. M. Wiener and R. Zuccherato, 'Faster Attacks on Elliptic Curve Cryptosystems', contribution to IEEE P1363.