Two Efficient Algorithms for Arithmetic of Elliptic Curves Using Frobenius Map

Jung Hee Cheon, Sungmo Park, Sangwoo Park, and Daeho Kim

Electronics and Telecommunications Research Institute,
161 Kajong-Dong,Yusong-Gu, Taejon, 305-350, ROK
{cheon, smp, psw, dhkim}@dingo.etri.re.kr

Abstract. In this paper, we present two efficient algorithms computing scalar multiplications of a point in an elliptic curve defined over a small finite field, the Frobenius map of which has small trace. Both methods use the identity which expresses multiplication-by-m maps by polynomials of Frobenius maps. Both are applicable for a large family of elliptic curves and more efficient than any other methods applicable for the family.
More precisely, by Algorithm 1(Frobenius k-ary method), we can compute mP in at most $2l/5 + 28$ elliptic additions for arbitrary l bit integer m and a point P on some elliptic curves. For other curves, the number of elliptic additions required is less than l. Algorithm 2(window method) requires at average $2l/3$ elliptic additions to compute mP for l bit integer m and a point P on a family of elliptic curves. For some 'good' elliptic curves, it requires $5l/12 + 11$ elliptic additions at average.

1 Introduction

To implement elliptic curve cryptosystems, it is important to compute efficiently scalar multiplications of a point in a given elliptic curve. The problem of multiplying a point P of an elliptic curve by an integer m is analogous to exponentiation of an element in a multiplicative group to the m-th power. The standard algorithm for this problem on elliptic curves is the binary method which repeats 'doublings' and 'additions' of points. This method requires at average $3l/2$ elliptic operations to compute mP for l bit integer m and a point P in an elliptic curve. A generalization of the binary method is the signed binary method (or the addition-subtraction method) [8]. This method use the fact that subtraction of points on an elliptic curve is just as efficient as addition. It performs the same procedure with the binary method except that it allows subtractions of points. This method requires at average $4l/3$ elliptic operations to compute mP for l bit integer m and a point P in an elliptic curve.

One can use also complex multiplications to speed up scalar multiplications. Every elliptic curve over a finite field is equipped with a set of operations (One of them is called the Frobenius map.) which can be viewed as multiplication by complex algebraic integers. These operations can be carried out efficiently for certain families of elliptic curves if we take normal basis for base field representation. This method is first suggested by Koblitz in [5] and [4] and improved by Meier and Staffelbach in [6]. The method in [6] requires at average $l/2$ elliptic operations to compute mP for l bit integer m and a point P in an elliptic curve. Further improvements were made by Solinas in [11], which requires at average $l/2$ elliptic operations. But these methods in [4], [6] and [11] can be applied just for two special elliptic curves, the anomalous binary curve(or ABC) defined over $\mathbf{F}_2$ and its twist.

In this paper, we present two methods using complex multiplications. Both methods use the identity which expresses multiplication-by-m maps by polymomials of the Frobenius map and are applicable for a larger family of elliptic curves than the methods in [4], [6] and [11]. These methods are efficient for elliptic curves defined over a small finite field, the Frobenius map of which has small trace. For some elliptic curves, the first methods requires at maximum $2l/5+28$ elliptic operations to compute mP for arbitrary l bit integer m and arbitrary point P in the elliptic curves.

We assume throughout this paper that elliptic curves are defined over a finite field $\mathbf{F}_q$ for $q = 2^r$ and the elements of finite fields are represented by normal basis, where the Frobenius map is just a bit rotate.

2 Frobenius Map

Consider an elliptic curve E defined over $\mathbf{F}_q$ with q elements. We define the q-th power Frobenius map ϕ_q on $E(\mathbf{F}_q)$ as follows [7] :

$$\phi_q : (x, y) \mapsto (x^q, y^q)$$

Then the followings are equivalent :

1. $\#E(\mathbf{F}_q) = q + 1 - t$
2. The trace of ϕ_q is t

3. $\phi_q^2 - t\phi_q + q = 0$

In particular, we call E to be supersingular if $t = 0$ and to be anomalous binary curve(or ABC) if $t = 1$.

For any poitive integer k, put $N_k = \#E(\mathbf{F}_{q^k})$. By the Weil theorem on elliptic curves [7] [10],

$$N_k = q^k + 1 - t_k,$$

where t_k is the sequence satisfying

$$t_0 = 2, t_1 = t \text{ and } t_{k+1} = t_k^2 - q^k t_{k-1} \quad (k \geq 1). \tag{1}$$

Since $\phi_{q^k} = \phi_q^k$, ϕ_q satisfies the equation as a map :

$$\phi_q^{2k} - t_k \phi_q^k + q^k = 0. \tag{2}$$

Hence when t_k is small, we can calculate efficiently $q^k M$ for $M \in E(\mathbf{F}_{q^k})$ using the above equation.

Note that following Waterhouse theorem [7], we know that if q is the power of 2, for any odd number t with $|t| \leq 2\sqrt{q}$, there exist elliptic curves E such that $\#E(\mathbf{F}_q) = q+1-t$, i.e. the Frobenius map of E has the trace t. Furthermore, all of them are not supersingular since the characteristic 2 of q does not divide t.

3 Frobenius *k*-ary Method

For an elliptic curve E defined over $\mathbf{F}_q$ where $q = 2^r$, let E_n be the curve regarded over the extension field $\mathbf{F}_{2^{nr}}$. Assume that the Frobenius map ϕ_{2^r} of E has small trace t so that we have an identity $2^r = t\phi_{2^r} - \phi_{2^r}^2$ from (2). Then we can calculate qP efficiently using this identity so that we can reduce the number of elliptic additions to compute mP for an integer m and $P \in E_n$. Now, using the Frobenius map, we present an algorithm which improves the usual k-ary method [1].

Theorem 1 (Frobenius k-ary Method). *Assume that an elliptic curve E is defined over $\mathbf{F}_{q^n}$. Let $P \in E(\mathbf{F}_{q^n})$ and $m = (e_{n-1}e_{n-2}\cdots e_1e_0)_q$*

be the radix representation of the multiplier m with base q and $0 \leq e_i < q$. Then $Q = mP$ can be computed using the following algorithm.

Algorithm 1 (Input: $P = (x, y)$; Output $Q = mP$)

```
1. Precomputation
   (a) $P_0 \leftarrow O$, $P_1 \leftarrow P$
   (b) For $i = 2$ to $q - 1$, $P_i = P_{i-1} + P$ (i.e. $P_i = iP$)
2. $Q \leftarrow P_{e_{n-1}}$
3. For $i = n - 2$ to 0
   (a) $Q \leftarrow t\phi_q(Q) - \phi_q^2(Q)$ (i.e. $Q \leftarrow qQ$)
   (b) $Q \leftarrow Q + P_{e_i}$
4. Return(Q)
```

Let $\epsilon(t)$ be the number of additions required to compute the multipication-by-t map. Notice that Step 1(b) requires $q - 2$ additions, Step 3(a) requires $(n - 1)(\epsilon(t) + 1)$ additions and Step 3(b) requires $n - 1$ additions. Since ϕ_q is just bit rotate for the normal base representation, the maximal complexity C of this method is thus $(n - 1)(\epsilon(t) + 2) + q - 2$ additions. That is, for any l-bit integer m, we can compute mP in C elliptic additions. If we let $l = nr$ for convenience, we have

$$C = (\frac{l}{r} - 1)(\epsilon(t) + 2) + q - 2. \tag{3}$$

For example, if $q = 2^4$ and $t = 1$, then the maximal complexity becomes $C = l/2 + 14$, which is very efficient compared with the average complexity $4l/3$ of the addition-subtraction method [8]. When both of q and r varies, the maximal complexities of Frobenius k-ary method are shown in Table 1.

The maximal complexities for most of all elliptic curves in Table 1 are less than the average complexity $4l/3$ of the addition-subtraction method. The best cases for $l \approx 160$ are the elliptic curves with $t = \pm 1$ defined over $\mathbf{F}_{2^5}$. In this case, the maximal complexity is $2l/5 + 28$. That is, we can compute mP in $2l/5 + 28$ elliptic additions for arbitrary l bit integer m.

q	$t=\pm1$	$t=\pm3$	$t=\pm5$	$t=\pm7$	Memory($\times l$ bits)
2^2	l	$2l-2$	$-$	$-$	2
2^3	$2l/3+4$	$4l/3+2$	$5l/3+1$	-	6
2^4	$l/2+12$	$l+10$	$5l/4+9$	$3l/2+8$	14
2^5	$2l/5+28$	$4l/5+26$	$l+25$	$6l/5+24$	30
2^6	$l/3+60$	$2l/3+58$	$5l/6+57$	$l+56$	62

Table 1. The maximal complexities of Frobenius k-ary method

4 Window Method

We start this section with an example.

Example 1. Let E be an elliptic curve defined over $\mathbf{F}_{2^{12}}$ with the trace 3 of the Frobenius map $\phi_{2^{12}}$ and E_n be the curve regarded over the extension field $\mathbf{F}_{2^{12n}}$. Then we have $2^{12}P = 3\phi_{2^{12}}(P) - \phi_{2^{12}}^2(P)$ for any $P \in E_n$ from (2). For any $12n$-bit integer m, write m as a Non-Adjacent Form(NAF) as follows[8] :

$$m = \sum_{j=0}^{12n} c_j 2^j \quad \text{with } c_j = 0, \pm 1$$

where $c_j = 0$ with the probability 2/3. Then for any $P \in E_n$, we can write mP as follows :

$$\begin{aligned} mP = \sum_{j=0}^{12n-1} c_j 2^j P &= \sum_{i=0}^{n-1} (\sum_{j=0}^{11} c_{12i+j} 2^j) 2^{12i} P && (4) \\ &= \sum_{j=0}^{11} 2^j (\sum_{i=0}^{n-1} c_{12i+j} 2^{12i} P) && (5) \\ &= \sum_{j=0}^{11} 2^j (\sum_{i=0}^{n-1} c_{12i+j} P_i) \quad \text{for } P_i = 2^{12i}P, \quad 0 \le i \le n-1 && (6) \end{aligned}$$

We need 3 additions to compute $2^{12}P$ and at average $12n/3 + 11$ additions to compute mP when we know $P_i's$ for $1 \le i \le n-1$, because $c_j = 0$ with the probability 2/3. Hence we totally need at average $(4n + 11) + 3(n - 1) = 7n + 8$ additions, which is less than $12n \times 4/3 = 16n$ of the addition-subtraction method. In this case, we improved the addition-subtraction method efficiently more than two times.

More generally, for an elliptic curve E defined over $\mathbf{F}_{2^r}$, let E_n be the curve regarded over the extension field $\mathbf{F}_{2^{nr}}$. Assume that the Frobenius map ϕ_{2^r} of E has the small trace t so that we have an identity $2^r = t\phi_{2^r} - \phi_{2^r}^2$ from (2). For a nr-bit integer m, we can write m as a Non-Adjacent Form as follows :

$$m = \sum_{j=0}^{nr-1} c_j 2^j \quad \text{with } c_j = 0, \pm 1$$

where $c_j = 0$ with the probability 2/3. Then for any $P \in E_n$, we can write mP as follows :

$$\begin{aligned} mP = \sum_{j=0}^{nr-1} c_j 2^j P &= \sum_{i=0}^{n-1} (\sum_{j=0}^{r-1} c_{ri+j} 2^j) 2^{ri} P && (7) \\ &= \sum_{j=0}^{r-1} 2^j (\sum_{i=0}^{n-1} c_{ri+j} 2^{ri} P) && (8) \\ &= \sum_{j=0}^{r-1} 2^j (\sum_{i=0}^{n-1} c_{ri+j} P_i) \quad \text{for } P_i = 2^{ri} P, \quad 0 \le i \le n-1 && (9) \end{aligned}$$

Hence we have the following algorithm :

Theorem 2 (Window Method). *Assume that an elliptic curve E is defined over $\mathbf{F}_{2^r}$. Let $P \in E(F_{2^{nr}})$, $t = 2^r + 1 - \#E(\mathbf{F}_{2^r})$ and $m = \sum_{j=0}^{nr} c_j 2^j$ be the Non-Adjacent Form of m with $c_j = 0, \pm 1$. Then $Q = mP$ can be computed using the following algorithm.*

Algorithm 2 (Input: $P = (x, y)$; Output $Q = mP$)

```
1. Precomputation
   (a) $P_0 \leftarrow P$
   (b) For $i = 1$ to $n-1$, $P_i = t\phi_{2^r}(P_{i-1}) - \phi_{2^r}^2(P_{i-1})$ (i.e. $P_i = 2^r P_{i-1} = 2^{ri} P$)
2. $Q \leftarrow O$
3. For $j = r-1$ to 0
```

```
    (a) $R \leftarrow O$
    (b) For $i = 0$ to $n - 1$, $R \leftarrow R + c_{ri+j} P_i$
    (c) $Q \leftarrow R + 2Q$
4. Return($Q$)
```

Step 1(b) requires $\epsilon(t) + 1$ additions. Also Step 3 requires at average $nr/3 + r$ additions because $c_j = 0$ with the probability $2/3$. Hence the average complexity C is $C = nr/3 + r + (\epsilon(t) + 1)(n - 1)$. If we let $l = nr$, then we have

$$C = l/3 + r + (\epsilon(t) + 1)(l/r - 1), \tag{10}$$

which is less than the average complexity $4l/3$ of the addition-subtraction method if $\epsilon(t) + 1 < r$.

Note that the order of an elliptic curve must be prime or a product of a large prime and a small integer in order that the discrete logarithms on the elliptic curve are intractable. Since $\#E(\mathbf{F}_q)$ divides $\#E_n = E(\mathbf{F}_{q^n})$ and $\#E(\mathbf{F}_q) \approx q$, an elliptic curve E defined over $\mathbf{F}_q$ for large q is not good for elliptic curve cryptosystems.

We present in Table 2 the average numbers of elliptic additions required to compute to mP for nr-bit m and $P \in E_n$ where E is defined over $\mathbf{F}_{2^r}$ for small r. For convenience, we put $l = nr$.

q	$t = \pm 1$	$t = \pm 3$	$t = \pm 5$	$t = \pm 7$
2^2	$4l/3$	$7l/3 - 2$		
2^3	$l + 2$	$5l/3 - 1$	$2l - 2$	
2^4	$7l/12 + 3$	$13l/12 + 1$	$4l/3$	$19l/12 - 1$
2^5	$8l/15 + 4$	$14l/15 + 2$	$17l/15 + 1$	$4l/3$
2^6	$l/2 + 5$	$5l/6 + 3$	$l + 2$	$7l/6 + 1$
2^7	$10l/21 + 6$	$16l/21 + 4$	$19l/21 + 3$	$22l/21 + 2$
2^8	$11l/24 + 7$	$17l/24 + 5$	$5l/6 + 4$	$23l/24 + 3$
2^9	$4l/9 + 8$	$2l/3 + 6$	$7l/9 + 5$	$8l/9 + 4$
2^{10}	$13l/30 + 9$	$19l/30 + 7$	$22l/30 + 6$	$5l/6 + 5$
2^{12}	$5l/12 + 11$	$7l/12 + 9$	$2l/3 + 8$	$3l/4 + 7$

Table 2. The average complexities of window method using $q = t\phi_q - \phi_q^2$

In Table 2, we see that when $q \geq 2^8$, the average numbers of elliptic additions for $l \approx 160$ are less than $l/2$ for $t = \pm 1$. Even for the case of $t = \pm 7$, the number of elliptic additions are less than l, which is more efficient result, compared with the average complexity $4l/3$ of addition-subtraction method. For the best case, it requires at average $5l/12 + 11$ elliptic additions to compute mP for l bit integer m.

We can also make use of t_2 and t_3 instead of $t = t_1$. We also explain this method by an example.

Example 2. Let E be an elliptic curve defined over $\mathbf{F}_{2^2}$ with the trace $t = 1$ of the Frobenius map ϕ_{2^2}. Consider $E_n = E(\mathbf{F}_{2^{2n}})$. Since $t_6 = -7$ in (1), we have $4^6 = 2^{12} = -7\phi_4^6 - \phi_4^{12}$ from (2) so that we need just 5 elliptic additions to multiply 2^{12} to a point in E_n. Apply Algorithm 2 for $r = 12$ and $t = t_6$. Then $3l/4 + 7$ elliptic additions are required for computing mP for l-bit integer m and $P \in E_n$. In this case, since $\#E(\mathbf{F}_{2^2}) = 4$, it is probable that E_n is 4 times a prime when we take n to be prime.

More generally, we can take an elliptic curve E defined over $\mathbf{F}_q$ for small q, the Frobenius map of which has the trace t satisfying $t_s \approx 0$ for some s. But it is not frequent case that t_s is small for $s \geq 4$. The previous example is just one case we found for $q = 2^r$ and $r \leq 20$.

For $s = 3$, there are two cases. One example is the case of $t_3 = \pm 5$ for the elliptic curves with $t = \pm 5$ defined over $\mathbf{F}_{2^3}$. In this case, we have the identity $2^9 = 5\phi_{2^3}^3 - \phi_{2^3}^6$ from(2) so that the average complexity becomes $7l/9 + 5$ by (10). Another example is the case of $t_3 = \pm 7$ for the elliptic curves with $t = \pm 7$ defined over $\mathbf{F}_{2^4}$. In this case, we have the identity $2^{12} = 7\phi_{2^4}^3 - \phi_{2^4}^6$ so that the average complexity becomes $3l/4 + 7$ by (10).

For $q = 2$, there are lots of examples. For an elliptic curve E defined over $\mathbf{F}_q$ for $q = 2^r$, consider $E_n = E(\mathbf{F}_{q^n})$. If we take t near $\sqrt{2q}$, we have $t_2 \approx 0$ since $t_2 = t^2 - 2q$. Then use the identity $q^2 = t_2\phi_q - \phi_q^2$ from (2) to compute q^2P for $P \in E_n$. For the elliptic curve with small t_2, Table 3 presents the number of elliptic additions required to compute mP for l-bit integer m and $P \in E_n$.

In all cases, the average complexities are far less than l, which are improved results. The best case is the elliptic curve with $t =$

q	t	t_2	Possible Multiple	$\epsilon(t_2)+1$	# of E.Addition
2^2	3	1	2^4	1	$7l/12+3$
2^3	5	9	2^9	4	$7l/9+5$
2^4	5	-7	2^8	5	$23l/24+3$
2^5	7	-15	2^{10}	6	$14l/15+4$
2^5	9	17	2^{10}	6	$14l/15+4$
2^6	11	-7	2^{12}	5	$3l/4+7$
2^7	15	-31	2^{14}	7	$5l/6+7$
2^7	17	33	2^{14}	7	$5l/6+7$
2^8	23	17	2^{16}	6	$17l/24+10$
2^9	31	-63	2^{18}	8	$7l/9+10$
2^9	33	65	2^{18}	8	$7l/9+10$
2^{10}	45	-23	2^{22}	7	$43l/66+15$
2^{12}	90	-92	2^{24}	9	$17l/24+15$
2^{12}	91	89	2^{24}	9	$17l/24+15$
2^{14}	181	-7	2^{28}	5	$43l/84+23$
2^{16}	362	-28	2^{32}	7	$53l/96+25$
2^{18}	724	-112	2^{36}	9	$7l/12+27$
2^{20}	1448	-448	2^{40}	11	$73l/120+29$

Table 3. The average complexities of window method using $q^2 = t_2\phi_q^2 - \phi_q^4$

181 defined over $\mathbf{F}_{2^{14}}$. In this case, the average complexity becomes $43l/84+23$, which is 109 less than $2l/3$ for $l = 168(= 14 \cdot 12)$.

5 Conclusion

In this paper, we have presented two efficient methods to compute scalar multiplications of a point of elliptic curves. Both methods use the identity expressing multiplication-by-m maps to some polynomials of the Frobenius map. Both methods can be applicable for a large family of elliptic curves with small defining field and small trace and more efficient than any other methods applicable for the family. By Algorithm 1(Frobenius k-ary method), we can compute mP in $2l/5+28$ elliptic additions for any l bit integer m and a point P for some 'good' curves. For other curves, the number of elliptic additions needed is also less than l.

Algorithm 2(window method) requires at average $2l/3$ elliptic additions to compute mP for $P \in E$ and l bit integer m. For some 'good' curves, it requires just $5l/12+11$ elliptic additions.

Our methods are useful when one implements elliptic curve cryptosystems in small hardware such as a smart card, because our methods provide high computational speed and require small size of memories.

References

1. J. Guajardo and C. Paar, “Efficient algorithms for elliptic curve cryptosystems”, *Proc. Crypto '97*, Springer-Verlag, 1997, pp. 342-356.
2. K. Koyama and Y. Tsuruoka, “Speeding up Elliptic Cryptosystems by using a singed binary window method”, *Proc. Crypto'92*, Springer-Verlag, 1993, pp. 43-56.
3. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1991.
4. N. Koblitz, “CM curves with good cryptographic properties”, *Proc. Crypto '91*, Springer-Verlag, 1992, pp. 279-287.
5. N. Koblitz, “Hyperelliptic Cryptosystems”, *Journal of Cryptology* 1(1989), pp. 139-150.
6. W. Meier and O. Staffelbach, “Efficient multiplication on certain non-supersingular elliptic curves”, *Proc. Crypto '92*, Springer-Verlag, 1993, pp. 333-344.
7. A. Menezez, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.
8. F. Morain and J. Olivos, “Speeding up the computations on an elliptic curve using additions-subtraction chains”, *Inform. Theory. Appl. 24 (1990)*, pp.531-543.
9. R. Schoof, “Elliptic curves over finite fields and the computation of square roots mod p”, *Math. Comp.* 44(1985), pp.483-494.
10. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1992.
11. J. Solinas, “An improved algorithm for arithmetic on a family of elliptic curves”, *Proc. Crypto '97*, Springer-Verlag, 1997, pp. 357-371.