Algorithms on Elliptic Curves over Fields of Characteristic Two with Non-Adjacent Forms

Tzu-Chun Lin
Department of Applied Mathematics, Feng Chia University,
100 Wenhwa Road, Taichung 407, Taiwan, R.O.C.
(Email: lintc@fcu.edu.tw)
(Received May 5, 2008; revised and accepted July 11, 2008)

Abstract

Let $\mathbb{F}_q$ be a finite field of characteristic two and let ϕ be the Frobenius endomorphism of an elliptic curve. To find or improve efficient algorithms for scalar multiplication sP of point P in the elliptic curve cryptography, it is always an important subject. If $\mathbb{F}_q = \mathbb{F}_2$, Solinas [5] has developed an algorithm for computing the ϕ-NAF. In this note, we extend Solinas' ϕ-NAF algorithm to $\mathbb{F}_q$, where q is a power of two, and give another efficient algorithms for ϕ-NAF, thereby show that the length of ϕ-NAF is at most two bits longer than the length of ϕ-expansion.

Keywords: Elliptic curves, Frobenius endomorphism, Frobenius expansion

1 Introduction

In recent years, elliptic curves over finite fields $\mathbb{F}_q$ play more important role in public key cryptography. The design of the elliptic curve cryptosystems (ECC) was proposed by Koblitz [1, 2]. The performance of an ECC depends on the efficient computation of scalar multiplications: Given an elliptic curve point P and an integer s, compute sP. It is convenient to express an integer s in a binary form $s = \sum_{i=0}^{k} b_i 2^i$, $b_i \in \{0, 1\}$. Moreover, it can be improved to so-called the Non-Adjacent Form. A signed binary form $s = \sum_{i\geq 0} b_i 2^2$ is called a **Non-Adjacent Form** (in short, NAF), if the coefficients $b_i \in \{0, \pm 1\}$ and $b_i b_{i+1} = 0$ for all $i \geq 0$ [3]. Instead of the binary form we may use the expansion with the Frobenius endomorphism ϕ as basis

$$s = \sum_{i=0}^{k} b_i \phi^i$$

with integer coefficients b_i so that $| b_i | \leq \frac{q}{2}$ for ECC.

We consider nonsingular elliptic curves over finite fields $\mathbb{F}_{2^m}$ of characteristic 2. Müller has proved the existence of ϕ-expansions of integers and determined their lengths. If $q = 4, 8, 16$, the upper bounds of the length of ϕ-expansions can be even improved. Solinas has developed an algorithm for computing $\phi - NAF$ so that the average density of a ϕ-NAF is 1/3. In this note, we extend Solinas' ϕ-NAF algorithm to $\mathbb{F}_q$, where q is a power of two. For elliptic curves $E : y^2 + xy = x^3 + ax + 1$ with $a = 0, 1$, we explore how to compute the ϕ-NAF of an integer from its ϕ-expansion.

2 Frobenius Endomorphism ϕ

Let $\mathbb{F}_q$ be a finite field of characteristic two with q elements. We consider nonsingular elliptic curves defined over a finite field $\mathbb{F}_q$ for elliptic curve cryptosystem

$$E : y^2 + xy = x^3 + ax^2 + b$$

with $a, b \in \mathbb{F}_q$, $b \neq 0$. The symbol $E(\overline{\mathbb{F}}_q)$ is denoted as the additive abelian group of $\overline{\mathbb{F}}_q$-rational points on E with identity ∞, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. This is the group on which the public-key protocols are performed. The Frobenius endomorphism ϕ on $E(\overline{\mathbb{F}}_q)$ is given by

$$\phi : E(\overline{\mathbb{F}}_q) \longrightarrow E(\overline{\mathbb{F}}_q),\ (x, y) \mapsto (x^q, y^q)$$

for each $(x, y) \in E(\overline{\mathbb{F}}_q)$. The Frobenius endomorphism ϕ satisfies the equation

$$\phi^2 - c\phi + q = 0. \tag{1}$$

where c is the trace of ϕ so that $| c | \leq 2\sqrt{q}$ is odd. This means

$$\phi^2(P) - c\phi(P) + qP = \infty.$$

for all points $P \in E(\overline{\mathbb{F}}_q)$. On the other hand, the Frobenius endomorphism ϕ is corresponding to the complex number $\frac{c+\sqrt{c^2-4q}}{2}$. The ring $\mathbb{Z}[\phi]$ is an Euclidean domain, also any element of $\mathbb{Z}[\phi]$ satisfies a division algorithm.

Müller has showed that every nonzero integer can be represented as an expansion with the Frobenius homomorphism ϕ as basis and determined its length.

Theorem 1. *[4] Let $s \in \mathbb{Z}[\phi]$.*

1) *There are* $t \in \mathbb{Z}[\phi]$ *and* $r \in \mathbb{Z}$ *such that*

$$s = t\phi + r \text{ and } \mid r \mid \leq \frac{q}{2}.$$

2) *There exist integers* $r_j \in \{r \in \mathbb{Z} \mid -\lceil \frac{q}{2} \rceil \leq r \leq \lceil \frac{q}{2} \rceil\}$ *such that*

$$s = \sum_{j=0}^{k} r_j \phi^j,$$

where $k \leq \lceil 2 \log_q \| s \| \rceil + 3$. *This form is called a* ϕ**-adic expansion of** s **with length** k *if* $r_k \neq 0$ *and* $r_i = 0$ *for all* $i > k$.

Corollary 1. *[4] Let* $s \in \mathbb{Z} \subseteq \mathbb{Z}[\phi]$.

1) *If* $q = 4$ *and*
   a. *if* $c = \pm 1$, *then there exists a* ϕ*-adic expansion for* s *with length* $k \leq \lceil \log_2 \mid s \mid \rceil + 1$.
   b. *if* $c = \pm 3$, *then there exists a* ϕ*-adic expansion for* s *with length* $k \leq \lceil \log_2 \mid s \mid \rceil + 4$.
2) *If* $q = 8$ *and*
   a. *if* $c = \pm 1, \pm 3$, *then there exists a* ϕ*-adic expansion for* s *with length* $k \leq \lceil \frac{2}{3} \log_2 \mid s \mid \rceil + 1$.
   b. *if* $c = \pm 5$, *then there exists a* ϕ*-adic expansion for* s *with length* $k \leq \lceil \frac{2}{3} \log_2 \mid s \mid \rceil + 2$.
3) *If* $q = 16$, *then there exists a* ϕ*-adic expansion for* s *with length* $k \leq \lceil \frac{1}{2} \log_2 \mid s \mid \rceil + 1$.

3 ϕ-NAF

In this section, we examine the algorithms for ϕ-NAFs of any nonzero integers.

Definition 1. *Let* s *be an element of an Euclidean domain* $\mathbb{Z}[\phi]$. *A* ϕ*-adic expansion of* s

$$\sum_{i \geq 0} m_i \phi^i$$

is called a ϕ**-adic nonadjacent form** *(in short,* ϕ**-NAF***) and denoted as* ϕ*-NAF(s), if*

1) $m_i \in G_{q^2-1}$ *for all* $i \geq 0$,
2) $m_{i+1} \cdot m_i = 0$ *for all* $i \geq 0$,

where G_{q^2-1} *is denoted as the digit set* $\{r \in \mathbb{Z} \mid \mid r \mid \leq \lceil \frac{q^2-1}{2} \rceil\} \setminus \{r \in \mathbb{Z} \mid \mid r \mid = bq, b \in \mathbb{N}\}$. *Usually* ϕ*-NAF(s) is denoted as the string* $(m_k, \cdots, m_1, m_0)_\phi$.

Lemma 1. *Let* $c_0 + c_1\phi \in \mathbb{Z}[\phi]$, $c_0, c_1 \in \mathbb{Z}$.

1) $c_0 + c_1\phi$ *is divisible by* ϕ *if and only if* c_0 *is divisible by* q.
2) $c_0 + c_1\phi \in \mathbb{Z}[\phi]$ *is divisible by* ϕ^2 *if and only if* $c_0 \equiv qc_1 \bmod q^2$.

Theorem 2. *Every integer has at most one* $\phi - NAF$.

Proof. Suppose that there are two different ϕ-NAF for an integer s, say $\phi - \text{NAF}(s) = (a_k, \cdots, a_1, a_0)_\phi = (b_l, \cdots, b_1, b_0)_\phi$. Let $k \leq l$. If s is divisible by ϕ, then $a_0 = b_0 = 0$. Otherwise, a_0, b_0 are not equal to 0. We suppose that $a_0 \neq b_0$. Since $a_0 \equiv b_0 \bmod q^2$ and $\mid a_0 - b_0 \mid \leq 2\lceil \frac{q^2-1}{2} \rceil$, it must be $a_0 = b_0$. Thus $(a_k, \cdots, a_1)_\phi = (b_l, \cdots, b_1)_\phi$. By induction on k, then we get $a_i = b_i$ for all $i \leq k$ and $b_j = 0$ for $k < j \leq l$. □

The above lemma quart trees the existence of ϕ-NAF of any integer.

Theorem 3. *Every element* $s \in \mathbb{Z}$ *can be represented as a* ϕ*-NAF with the digit set* G_{q^2-1}.

We will recommend two methods to change an integer into its ϕ-NAF.

Method 1. *Assumed that* $s \in \mathbb{Z} \subset \mathbb{Z}[\phi]$. *Let* $s_0 = s, s_i = s_{i+1}\phi + r_i$, *where* $n_i, n_{i+1} \in \mathbb{Z}$ *and* $r_i \in G_{q^2-1}$, *for* $i \geq 0$. *Set* $s_i = c_{i0} + c_{i1}\phi$ *with* $c_{i0}, c_{i1} \in \mathbb{Z}$. *If* c_{i0} *is not divisible by* q, *then the remainder* r_i *satisfies* $c_{i0} - qc_{i1} \equiv r_i \bmod q^2$, *where* r_i *is the absolute smallest residue of* s_i *mod* q^2; *otherwise,* $r_i = 0$. *It is easy to show that the pair*

$$(c_{i+1,0}, c_{i+1,1}) = (c_{i1} + c\frac{c_{i0} - r_i}{q}, -\frac{c_{i0} - r_i}{q}) \in \mathbb{Z} \times \mathbb{Z}$$

and there is an integer l *so that* $(c_{l+1,0}, c_{l+1,1}) = (r_l, 0)$. *Thus the string* $(r_l, \cdots, r_2, r_1, r_0)$ *is equal to the* ϕ*-NAF of* s.

Algorithm 1 Computation of ϕ-NAF depends on Method 1

Input: integers r_0, r_1
Output: ϕ-NAF$(r_0 + r_1\phi)$
Computation:
Set $c_0 \leftarrow r_0$, $c_1 \leftarrow r_1$
Set $S \leftarrow <>$
while $c_0 \neq 0$, or $c_1 \neq 0$ **do**
  if c_0 is not divisible by q **then**
    set $r \leftarrow (c_0 - qc_1 \bmod q^2)$
    set $c_0 \leftarrow c_0 - r$
  else
    set $r \leftarrow 0$
  end if
  Prepend r to S
  Set $(c_0, c_1) \leftarrow (c_1 - c\frac{c_0}{q}, -\frac{c_0}{q})$
end while
Output S

Method 2. *Let* $s_0 = s$ *and* $s_i = s_{i+1}\phi + r_i$, *where* $s_i, s_{i+1} \in \mathbb{Z}[\phi]$, $r_i \in G_{q^2-1}$, *for* $i \geq 0$, *and let the string* $\alpha_0 = \epsilon$ *empty. Set* $s_i = c_{i0} + c_{i1}\phi$, *where* $c_{i0}, c_{i1} \in \mathbb{Z}$ *for* $i \geq 0$. *If* c_{i0} *is not divisible by* q, *then the remainder* r_i *satisfies* $c_{i0} - qc_{i1} \equiv r_i \bmod q^2$, *and the string* $\alpha_{i+1} = 0r_i \| \alpha_i$. *It is easy to show that the pair*

$$(c_{i+1,0}, c_{i+1,1}) = (\frac{c_{i1}}{c} + \frac{c^2 - q}{c} d_1, d_1) \in \mathbb{Z} \times \mathbb{Z},$$

where $d_1 = -\frac{c(c_{i0}-r)+qc_{i1}}{q^2}$*; otherwise,* $r_i = 0$*,* $\alpha_{i+1} = 0\|\alpha_i$*, and the pair*

$$(c_{i+1,0}, c_{i+1,1}) = (c_{i1} + c\frac{c_{i0}}{q}, -\frac{c_{i0}}{q}) \in \mathbb{Z} \times \mathbb{Z}.$$

Thus the string $(\cdots, \alpha_2, \alpha_1, \alpha_0)$ *is equal to the* ϕ*-NAF of* s*.*

Algorithm 2 Computation of ϕ-NAF depends on Method 2

Input: integers r_0, r_1; string α
Output: ϕ-NAF$(r_0 + r_1\phi)$
Computation:
Set $c_0 \leftarrow r_0$, $c_1 \leftarrow r_1$, $\alpha \leftarrow \varepsilon$ "empty"
while $c_0 \neq 0$, or $c_1 \neq 0$ **do**
  if c_0 is not divisible by q **then**
    set $r \leftarrow (c_0 - qc_1 \bmod q^2)$
    set $c_0 \leftarrow c_0 - r$
    set $(c_0, c_1) = (\frac{c_1}{c} + \frac{c^2-q}{c} \cdot \frac{cc_0+qc_1}{q^2}, -\frac{cc_0+qc_1}{q^2})$
    set $\alpha \leftarrow 0r\|\alpha$
  else
    set $r \leftarrow 0$
    set $(c_0, c_1) \leftarrow (c_1 + c\frac{c_0}{q}, -\frac{c_0}{q})$
    set $\alpha \leftarrow 0\|\alpha$
  end if
end while
Output α

The above Methods (1) and (2) are both transformed into ϕ-NAFs directly from integers. If the Frobenius ϕ satisfies the equation $\phi^2 \pm \phi + q = 0$, then the ϕ-NAFs can be transformed from ϕ-expansions. The following describes how to change the coefficients of ϕ-expansion to the ϕ-NAF.

Theorem 4. *If the trace* $c = \pm 1$*, then every* ϕ*-adic expansion of an integer can be transformed to the* ϕ*-NAF.*

Proof. Let $s = m_0 + m_1\phi + m_2\phi^2 + m_3\phi^3 + \cdots + m_k\phi^k$ be a ϕ-adic expansion of an integer s, where $m_i \in \{0, \pm 1, \cdots, \pm\frac{q}{2}\}$. The coefficients m_i can be changed through the equation $\phi^2 - \phi + q = 0$. We show the result for $q = 2, 4$ and $c = 1$ (the case $c = -1$ can be treated symmetrically). Assumed that $m_0 \neq 0$ and $m_1 \neq 0$. The constant m_0 is replaced with $m_0(-(q-1)+\phi-\phi^2)$. Therefore

$$s = -(q-1)m_0 + (m_1+m_0)\phi + (m_2-m_0)\phi^2 + m_3\phi^3 + \cdots$$

In the case $q = 2$. $s = -m_0 + (m_1+m_0)\phi + (m_2-m_0)\phi^2 + m_3\phi^3 + \cdots$ with $m_i \in \{0, \pm 1\}$. If $m_1 = -m_0$, then

$$s = -m_0 + 0\phi + (m_2 - m_0)\phi^2 + m_3\phi^3 + \cdots.$$

If $m_1 = m_0$, then take $2\phi = (\phi - \phi^2)\phi$, and thus

$$s = -m_0 + 0\phi + m_2\phi^2 + (m_3 \mp 1)\phi^3 + \cdots.$$

The first three coefficients satisfy the definition of the ϕ-NAF. We repeat this process until all coefficients becoming ϕ-NAF.
In the case $q = 4$. $s = -3m_0 + (m_1 + m_0)\phi + (m_2 - m_0)\phi^2 + m_3\phi^3 + \cdots$ with $m_i \in \{0, \pm 1, \pm 2\}$. First, we take $-3m_0 = a \pm 4$ with $|a| \leq 2$, then

$$\begin{aligned} s &= a \pm 4 + (m_1 + m_0)\phi + (m_2 - m_0)\phi^2 + m_3\phi^3 + \cdots \\ &= a \pm (\phi - \phi^2) + (m_1 + m_0)\phi + (m_2 - m_0)\phi^2 + m_3\phi^3 + \cdots \\ &= a + (m_1 + m_0 \pm 1)\phi + (m_2 - m_0 \mp 1)\phi^2 + m_3\phi^3 + \cdots \quad (2) \end{aligned}$$

Consider the first two terms of Equation (2). If $|m_1 + m_0 \pm 1| = 4$, then

$$s = a + (\phi - \phi^2) + (m_2 - m_0 \mp 1)\phi^2 + m_3\phi^3 + \cdots.$$

If $|a + 4(m_1 + m_0 \pm 1)| > 7$, then take $(m_1 + m_0 \pm 1)\phi = 4\phi - (4 - m_1 - m_0 \mp 1)\phi = (\phi - \phi^2)\phi - (4 - m_1 - m_0 \mp 1)(\phi^2 + 4)$; otherwise, take $(m_1 + m_0 \pm 1)\phi = (m_1 + m_0 \pm 1)(\phi^2 + 4)$. Thus, the first three coefficients of Equation (2) is changed the coefficients which satisfy the definition of the ϕ-NAF

$$s = a_0 + 0\phi + (m_2 + e)\phi^2 + (m_3 + f)\phi^3 + m_4\phi^4 \cdots,$$

with $f \in \{0, \pm 1\}$. □

Therefore, it is easy to verify the length of ϕ-NAF.

Corollary 2. *Let* s *be an integer and* $c = \pm 1$*. Then the length of the* $\phi - \mathrm{NAF}(s)$ *is at most* 2 *bits longer than the length of its* ϕ*-adic expansion.*

Algorithm 3 Transformation from ϕ-adic expansion to ϕ-NAF

Input: $q, c, m_0, m_1, \cdots, m_k$
Output: ϕ-NAF of $m_0, m_1, \cdots, m_k, m_{k+1}, m_{k+2}$
Begin
for $(i \geq 1; i \leq k; i++)$ **do**
  if $(|m_{i-1}| == q)$ **then**
    $m_{i-1} = 0$,
    $m_i = m_i + c$,
    $m_{i+1} = m_{i+1} - 1$,
  else
    using the look-up table to get the values of a_0, e, f (Look-up table for $q = 2$ and $q = 4$ are shown in Appendix)
    $m_{i-1} = a_0$,
    $m_i = 0$,
    $m_{i+1} = m_{i+1} + e$,
    $m_{i+2} = m_{i+2} + f$,
  end if
end for

4 Conclusion

In this paper, in analog to Solinas' result, we propose two efficient algorithms to computing ϕ-NAFs directly from integers. An efficient algorithm from ϕ-adic expansions to ϕ-NAF for the Frobenius ϕ satisfying $\phi^2 - c\phi + q = 0$ with $| c |= 1$ is presented. Unfortunately, this kind of computing technology is not suitable to use the situation $| c |> 1$.

References

[1] M. Hedabou, "A frobenius map approach for an efficientand secure multiplication on koblitz curves," *International Journal of Network Security*, vol. 3, no. 3, pp. 239-243, 2006.

[2] N. Koblitz, "CM-curves with good cryptographic properties," *Advances in Cryptology- CRYPTO' 91*, LNCS 576, pp. 279-287, Springer-Verlag, 1992.

[3] J. R. Lin, *A Study of Non-Adjacent Forms*, Master Thesis, Feng Chia University, 2007.

[4] V. Müller, "Fast multiplication on elliptic curves over small fields of characteristic two," *Journal of Cryptology*, vol. 11, pp. 219-234, 1998.

[5] J. A. Solinas, "Efficient arithmetic on Koblitz curves," *Designs, Codes and Cryptography*, vol. 19, pp. 195-249, 2000.

Appendix

Look-up table for $q = 2$

c	m_{i-1}	m_i	a_0	e	f
1	1	1	−1	0	−1
1	1	−1	−1	−1	0
1	−1	1	1	1	0
1	−1	−1	1	0	1
−1	1	1	−1	−1	0
−1	1	−1	−1	0	1
−1	−1	1	1	0	−1
−1	−1	−1	1	1	0

Look-up table for $q = 4$

c	m_{i-1}	m_i	a_0	e	f
1	1	1	5	1	0
1	1	−1	−3	−1	0
1	1	2	−7	−1	−1
1	1	−2	−7	−2	0
1	−1	−1	−5	−1	0
1	−1	1	3	1	0
1	−1	−2	7	1	1
1	−1	2	7	2	0
1	2	1	6	1	0
1	2	−1	−2	−1	0
1	2	2	−6	−1	−1
1	2	−2	−6	−2	0
1	−2	−1	−6	−1	0
1	−2	1	2	1	0
1	−2	−2	6	1	1
1	−2	2	6	2	0
−1	1	1	−3	−1	0
−1	1	−1	5	1	0
−1	1	2	−7	−2	0
−1	1	−2	−7	−1	1
−1	−1	1	−5	−1	0
−1	−1	−1	3	1	0
−1	−1	2	7	1	−1
−1	−1	−2	7	2	0
−1	2	1	−2	−1	0
−1	2	−1	6	1	0
−1	2	2	−6	−2	0
−1	2	−2	−6	−1	1
−1	−2	1	2	1	0
1	−2	−1	−6	−1	0
−1	−2	2	6	2	0
−1	−2	−2	6	1	−1

Tzu-Chun Lin is an assistant professor in the Department of Applied Mathematics of Feng Chia University in Taiwan, R.O.C. She received her PhD in Mathematics from Göttingen University in Germany. Her current research interests include Invariant Theory of Finite Groups and Elliptic Curve Cryptography.