Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Discrete Algorithms 3 (2005) 113–124
JOURNAL OF DISCRETE ALGORITHMS
www.elsevier.com/locate/jda

Efficient algorithms for Koblitz curves over fields of characteristic three

Ian F. Blake [a,*], V. Kumar Murty [b], Guangwu Xu [c]

[a] *Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada, M5S 3G4*
[b] *Department of Mathematics, University of Toronto, Toronto, Ontario, Canada, M5S 3G3*
[c] *Ganita Lab, University of Toronto at Mississauga, Mississauga, Ontario, Canada, L5L 1C6*

Received 19 February 2004; accepted 26 April 2004

Available online 2 July 2004

Abstract

The nonadjacent form method of Koblitz [Advances in Cryptology (CRYPTO'98), in: Lecture Notes in Comput. Sci., vol. 1462, 1998, pp. 327–337] is an efficient algorithm for point multiplication on a family of supersingular curves over a finite field of characteristic 3. In this paper, a further discussion of the method is given. A window nonadjacent form method is proposed and its validity is proved. Efficient reduction and pre-computations are given. Analysis shows that more than 30% of saving can be achieved.

MSC: primary 11Y16, 11Y40, 14G50

Keywords: Algorithm; Elliptic curves; Cryptography; Window nonadjacent expansion

1. Introduction

Koblitz or subfield curves, are curves defined over $\mathbb{F}_q$ for q relatively small, and a subgroup of the set of rational points over $\mathbb{F}_q^n$ is of interest. This approach allows efficient scalar point multiplication (e.g., [9,11,14]) as well as point counting via the zeta function

* Corresponding author.
E-mail addresses: ifblake@comm.utoronto.ca (I.F. Blake), murty@math.toronto.edu (V. Kumar Murty), gxu@comm.utoronto.ca (G. Xu).

1570-8667/$ – see front matter
doi:10.1016/j.jda.2004.04.011

(e.g., [2]). Such curves can play an important role in certain elliptic curve cryptographic systems first suggested in [8,13].

The window τ-adic NAF technique of Solinas [14] is a very efficient method for scalar multiplication for Koblitz curves over finite fields of characteristic 2. This method requires some pre-computations.

Recently, a family of supersingular elliptic curves over finite field $\mathbb{F}_{3^m}$ was presented by Koblitz [10]. For this type of curve, point multiplication can be sped up by using the nonadjacent form of base-τ expansion of the scalar. Such an expansion is proved to exist and be unique [10, Theorem 1]. Applying Koblitz' algorithm to implement ECDSA, the speed can be significantly improved (by factor of 12, see [10]).

For supersingular elliptic curves, the algorithm of Menezes–Okamoto–Vanstone reduces the discrete logarithm problem in elliptic curves over $\mathbb{F}_q$ to a discrete logarithm problem in a finite field $\mathbb{F}_{q^K}$ with $K \leqslant 6$. See [12] and [4]. Therefore, care should be taken when using supersingular curves in certain cryptographic applications.

Recent work on parings in cryptography has shown directions of positive use of supersingular curves, such as for example, a one round protocol for tripartite Diffie-Hellman key exchange by Joux [7], an efficient identity-based encryption (IBE) system by Boneh and Franklin [3], and many others. It is noted that the Koblitz curves over $\mathbb{F}_{3^m}$ are included in [1,5] for efficient implementations of pairings.

In this paper, a further discussion on the Koblitz' base-τ nonadjacent form method is given for Koblitz curves over finite fields of characteristic three. For each integer $w > 1$, a width w window base-τ nonadjacent form is derived for any scalar. Our algorithm is inspired by the window τNAF algorithm of Solinas for Koblitz curves [14] over $\mathbb{F}_{2^m}$. When $w > 2$, this method requires a pre-computation, and the validity of the algorithm is proved if the pre-computation is suitably chosen. The method achieves greater efficiency.

The organization of the paper is as follows. All work is for Koblitz curves over finite fields of characteristic 3. In Section 2, we describe the nonadjacent form method of Koblitz for point multiplication for Koblitz curves and another form of the algorithm of Koblitz is given. This method is extended to window form in Section 3, and a suitable pre-computation is chosen. The final section discusses the issues of performance and implementation.

2. NAF base-τ expansions

Let to be an integer with no factor 2 or 3, and $q = 3^m$. Consider the following supersingular elliptic curve

$$E_a\colon\ y^2 = x^3 - x - (1)^a,$$

over $\mathbb{F}_q$, where $a = 0$ or 1. From now on, we write μ for $(-1)^a$.

Let N_m denote the number of $\mathbb{F}_q$-points on E. The *Frobenius map* is defined to be

$$\begin{aligned}\tau &: E_a(\mathbb{F}_{3^m}) \to E_a(\mathbb{F}_{3^m})\\ &(x, y) \to (x^3, y^3)\end{aligned}$$

and $\tau(\mathcal{O}) = \mathcal{O}$.

Notice that $\tau^2(P) + 3P = 3\mu\tau(P)$ for all $P \in E_a(\mathbb{F}_{3^m})$, τ can be interpreted as a complex number defined by the next equation:

$$\tau^2 - 3\mu\tau + 3 = 0.$$

Let ω be the 6th root of unity

$$\omega = \frac{\mu + \sqrt{3}i}{2},$$

then $\mu\omega$ is a primitive 6th root of unity and $\tau = \mu + \omega$. Thus $\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega = \mathbb{Z} + \mathbb{Z}\tau$, and it is a set of automorphisms of E_a in the sense that

$$(a + b\tau)P = aP + b\tau(P)$$

for every $P \in E_a(\mathbb{F}_{3^m})$.

It is observed in [10] that the point multiplication ωP is trivial: let $P = (P_x, P_y) \in E_a$, then

$$\omega P = (P_x - \mu, -\mu P_y).$$

So it costs very little for performing $\tau^k P$ and $\omega^l P$, where $k \in \mathbb{N}$ and $0 < l < 6$. Therefore, to compute nP, one first gets a reduction $a + b\tau$ of n in the sense that

$$n = a + b\tau \bmod (\tau^m - 1).$$

Here the fact $(\tau^m - 1)P = \mathcal{O}$ should be noted. The next step is to seek a *nonadjacent form* (NAF) of $a + b\tau$:

$$a + b\tau = \sum_{j=0}^{N} \eta_j \tau^j,$$

with $\eta_j \in \{0, \pm 1, \pm\omega, \pm\omega^2\}$ and $\eta_j \eta_{j+1} = 0$. Finally, one gets

$$nP = \sum_{j=0}^{N} \eta_j \tau^j(P).$$

The procedure above is guaranteed by the following result, see [10]:

Theorem (Koblitz). *Every element of* $\mathbb{Z}[\omega]$ *reduced modulo* $\tau^m - 1$ *has a unique NAF base-*τ *expansion with digits* $\{0, \pm 1, \pm\omega, \pm\omega^2\}$, *in which at most* $(m + 1)/2$ *digits are nonzero. Asymptotically on average* 60% *of the digits are zero.*

The proof of the above theorem in [10] is inherent in the following algorithm. Here the notation *mods* means

$$a = b \text{ mods } n \quad \text{iff} \quad a \equiv b \pmod{n} \text{ and } -\frac{n}{2} \leqslant a < \frac{n}{2}.$$

Algorithm 2.1 (*Koblitz base-τ NAF method*).
INPUT: an element $\rho = r_0 + r_1\tau$ of $\mathbb{Z}[\omega]$
OUTPUT: S, the array of coefficients of τ-NAF of ρ.

```
S ← ⟨ ⟩
While r0 ≠ 0 or r1 ≠ 0
  ε ← r0 mods 3
  r3 ← (r0 − ε) div 3
  r0' ← r1 + 3μr3
  r1' ← −r3
  If ε = 0 or 3|r0', then
    r0 ← r0'
    r1 ← r1'
    prepend ε to S
  Else
    If 3|(r0' − με) then
      r0 ← r0' + 2με
      r1 ← r1' − ε
      prepend εω^2 to S
    Endif
    If 3|(r0' + με) then
      r0 ← r0' + με
      r1 ← r1'
    prepend −εω to S
    Endif
  Endif
Endwhile
Return S
```

Notice that

$$\tau^2 | a + b\tau \quad \Leftrightarrow \quad 3|a \text{ and } 3|b,$$

and

$$-1 + \mu\tau = \mu\omega, \quad -2 + \mu\tau = \omega^2,$$

another proof of Koblitz Theorem can be described by the following algorithm:

Algorithm 2.2 (*Koblitz base-τ NAF method*).
INPUT: an element $\rho = r_0 + r_1\tau$ of $\mathbb{Z}[\omega]$
OUTPUT: S, the array of coefficients of τ-NAF of ρ.

```
S ← ⟨ ⟩
While r0 ≠ 0 or r1 ≠ 0
  If 3∤r0 then
    x ← r0 mods 3
    y ← r1 mods 3
    If x = μy then
```

```
        x ← −2x
      Endif
      r0 ← r0 − x
      r1 ← r1 − y
      prepend x + yτ to S
    Else
      prepend 0 to S
    Endif
    t ← r0
    r0 ← μr0 + r1
    r1 ← −t/3
  Endwhile
Return S
```

The treatment of Algorithm 2.2 and the algorithm in the next section are inspired by the algorithms of Solinas in [14].

3. Window base-τ NAF method

It is known that the Solinas window τNAF method [14] for Koblitz curves over $\mathbb{F}_{2^m}$ is a very efficient method for point multiplication. In this section, a window base-τ NAF method for the curves E_a over $\mathbb{F}_{3^m}$ is suggested. This method is proved to have the "norm reducing" property and hence produces a converging algorithm.

Given a natural number w, the idea of the width w window base-τ NAF method is to seek the following expansion (*window τ-NAF*) of an element $a + b\tau \in \mathbb{Z}[w]$:

$$a + b\tau = \sum_{j=0}^{N} u_j \tau^j \tag{1}$$

with the property that each nonzero u_j is taken from a suitable set called the *pre-computation set* and each segment $\{u_j, u_{j+1}, \ldots, u_{j+w-1}\}$ contains at most one nonzero element.

To compute $(a + b\tau)P$ for some $P \in E_a(\mathbb{F}_{3^m})$, one first sets up a pre-computation: perform uP for each u in the pre-computation set, and compute $\sum_{j=0}^{N} \tau^j(u_j P)$.

The next lemma is crucial in our discussion.

Lemma 3.1. *Let k be a positive integer and $a + b\tau \in \mathbb{Z}[\omega]$, then*

(1) $\tau^k = 3^{\lfloor k/2 \rfloor}(\mu\omega)^{\lfloor k/2 \rfloor}\tau^{\lceil k/2 \rceil - \lfloor k/2 \rfloor}$,
(2) $\tau^k | a + b\tau \Leftrightarrow 3^{\lceil k/2 \rceil} | a$ *and* $3^{\lfloor k/2 \rfloor} | b$.

Proof. (1) Notice that $\tau^2 = 3(\mu\omega)$. The argument follows from induction.
(2) By (1), τ^k is associated to $3^{\lfloor k/2 \rfloor}\tau^{\lceil k/2 \rceil - \lfloor k/2 \rfloor}$. □

Consider the set of all elements of $\mathbb{Z}[\omega]$ which are not divisible by τ. By Lemma 3.1, a set of representatives of congruence classes of such elements modulo τ^w is

$$\{x + y\tau\colon\ 0 \leqslant x \leqslant 3^{\lceil w/2\rceil} - 1,\ 0 \leqslant y \leqslant 3^{\lfloor w/2\rfloor} - 1,\ \text{and } 3 \nmid x\}.$$

For each $x + y\tau$, let $\tilde{x} + \tilde{y}\tau$ be an element with least norm in the congruence class of $x + y\tau$ modulo τ^w. A pre-computation set (nonzero coefficients of expression (1)) can be formed as follows:

$$\text{MinPre}_w = \{\tilde{x} + \tilde{y}\tau\colon\ 0 \leqslant x \leqslant 3^{\lceil w/2\rceil} - 1,\ 0 \leqslant y \leqslant 3^{\lfloor w/2\rfloor} - 1,\ \text{and } 3 \nmid x\}.$$

For $w > 1$, the next algorithm generates the coefficients of the width w window base-τ NAF expansion.

Algorithm 3.1 (*Width w window base-τ NAF method*).
INPUT: an element $\rho = r_0 + r_1\tau$ of $\mathbb{Z}[\omega]$
OUTPUT: S, the array of coefficients of window τ-NAF of ρ.

```
S ← ⟨ ⟩
While r0 ≠ 0 or r1 ≠ 0
  If 3 ∤ r0 then
    x ← r0 mod 3^⌈w/2⌉
    y ← r1 mod 3^⌊w/2⌋
    r0 ← r0 − x̃
    r1 ← r1 − ỹ
    prepend x̃ + ỹτ to S
  Else
    prepend 0 to S
  Endif
  t ← r0
  r0 ← μr0 + r1
  r1 ← −t/3
Endwhile
Return S
```

It is obvious that the Koblitz algorithm (Algorithm 2.2) is a special case of the above algorithm, i.e., the case $w = 2$.

The next example displays a width 3 window base-τ nonadjacent form of $2330 - 963\tau$ with $\mu = 1$. It is expressed in terms of algebraic formulas based on which the algorithm is developed.

$$\begin{aligned}
2330 - 963\tau &= -1 + (2331 - 963\tau)\\
&= -1 - \tau^4(62 + 45\tau)\\
&= -1 - \tau^4\big(-1 + (63 + 45\tau)\big)\\
&= -1 - \tau^4\big(-1 + \tau^4(22 - 17\tau)\big)\\
&= -1 - \tau^4\big(-1 + \tau^4\big((4 - 2\tau) + (18 - 15\tau)\big)\big)
\end{aligned}$$

$$= -1 - \tau^4\big(-1 + \tau^4\big((4-2\tau) - \tau^3(4-\tau)\big)\big)$$
$$= -1 + \tau^4 - (4-2\tau)\tau^8 + (4-\tau)\tau^{11}.$$

Here $\tau^3 = -9 + 6\tau$ and $\tau^4 = -18 + 9\tau$. The elements $4 - 2\tau$ and $4 - \tau$ are congruent to $4 + \tau$ and $4 - \tau$ respectively, and they have the least norms in the corresponding classes.

We must show that Algorithm 3.1 is valid, i.e., the `while` loop inside the algorithm terminates.

Recall that for an arbitrary element $r_0 + r_1\tau \in \mathbb{Z}[\omega]$, its norm is given by the formula

$$N(r_0 + r_1\tau) = r_0^2 + 3\mu r_0 r_1 + 3r_1^2.$$

Let

$$U_6 = \big\{(\mu\omega)^j\colon\ j = 0, 1\ldots, 5\big\},$$

then U_6 contains all elements of norm 1 of $\mathbb{Z}[\omega]$.

The following fact about MinPre_w is useful.

Lemma 3.2. *For $w > 1$,*

$$U_6 \subseteq \mathrm{MinPre}_w.$$

Proof. Since $w > 1$, and

$$U_6 = \{1, -1 + \mu\tau, -2 + \mu\tau, -1, 1 - \mu\tau, 2 - \mu\tau\},$$

by Lemma 3.1, any two elements in U_6 are not congruent modulo τ^w. □

Let $\succ$ denote a typical reduction by a single round of the `while` loop inside the algorithm. So the relation

$$r_0 + r_1\tau \succ r_0' + r_1'\tau$$

indicates that starting from element $r_0 + r_1\tau$, we get $r_0' + r_1'\tau$ at the end of one round of the `while` loop. It is immediate that

$$r_0' + r_1'\tau = \frac{r_0 + r_1\tau - (\tilde{x} + \tilde{y}\tau)}{\tau},$$

here it is understood that if $3|r_0$, $\tilde{x} = \tilde{y} = 0$. Furthermore, if $3 \nmid r_0$, then there exists a reduction chain of length w of the form:

$$r_0 + r_1\tau \succ \frac{r_0 + r_1\tau - (\tilde{x} + \tilde{y}\tau)}{\tau} \succ \cdots \succ \frac{r_0 + r_1\tau - (\tilde{x} + \tilde{y}\tau)}{\tau^w}.$$

In the next theorem, it is shown that the above chain is norm reducing, and hence the argument that the algorithm terminates follows.

Theorem 3.1. *The width w window base-τ NAF method terminates with respect to* MinPre_w.

Proof. Let us start with element $r_0 + r_1\tau$.

By Lemma 3.2, we may assume that $N(r_0 + r_1\tau) > 1$. This implies that $N(r_0 + r_1\tau) \geqslant \sqrt{3}$.

If $3|r_0$, then

$$r_0 + r_1\tau \succ \frac{r_0 + r_1\tau}{\tau}.$$

It is obvious that

$$N\left(\frac{r_0 + r_1\tau}{\tau}\right) = \frac{N(r_0 + r_1\tau)}{3} < N(r_0 + r_1\tau).$$

If $3 \nmid r_0$, then

$$r_0 + r_1\tau \succ \frac{r_0 + r_1\tau - (\tilde{x} + \tilde{y}\tau)}{\tau} \succ \cdots \succ \frac{r_0 + r_1\tau - (\tilde{x} + \tilde{y}\tau)}{\tau^w}.$$

Since $\mathbb{Z}[\omega]$ is Euclidean, $N(\tilde{x} + \tilde{y}\tau) < N(\tau^w) = 3^w$.

$$\begin{aligned}
\frac{|r_0 + r_1\tau - (\tilde{x} + \tilde{y}\tau)|}{|\tau^w||r_0 + r_1\tau|} &\leqslant \frac{1}{|\tau|^w}\left(1 + \frac{|\tilde{x} + \tilde{y}\tau|}{|r_0 + r_1\tau|}\right) \\
&\leqslant \frac{1}{|\tau|^w}\left(1 + \frac{|\tilde{x} + \tilde{y}\tau|}{\sqrt{3}}\right) \\
&\leqslant \frac{1}{|\tau|^w} + \frac{|\tilde{x} + \tilde{y}\tau|}{\sqrt{3}|\tau|^w} \\
&\leqslant \frac{1}{3} + \frac{1}{\sqrt{3}} < 1,
\end{aligned}$$

i.e.,

$$N(r_0 + r_1\tau) > N\left(\frac{r_0 + r_1\tau - (\tilde{x} + \tilde{y}\tau)}{\tau^w}\right).$$

Therefore, under the algorithm, an element of a smaller norm can be obtained by at most w reductions and the algorithm must terminate. □

It is remarked that when $w = 1$, Algorithm 3.1 is not valid. In other words, not every element in $\mathbb{Z}[\omega]$ can be expressed as

$$\sum_{j=0}^{N} u_j \tau^j$$

with $u_j \in \{0, 1, -1\}$. For example, take $\mu = 1$. If we had $2 - \tau = \sum_{j=0}^{N} u_j \tau^j$, then all u_j would be -1 and N would be infinity.

4. Performance and implementation

In this section, the issues of implementation and performance are discussed. First an efficient and clean form of a reduced scalar modulo $\tau^m - 1$ is given. Then we illustrate how to perform an efficient pre-computation. Finally, analysis shows how much we gain from the window base-τ NAF method.

4.1. Efficient reduction modulo $\tau^m - 1$

In practice, we are only interested in the subgroup of $E_a(F_{3^m})$ whose order is a large prime. According to [10], the case of to being a prime is a good choice. Note that by Weil's theorem,

$$N_m = N(\tau^m - 1) = 3^m - \mu\left(\frac{3}{m}\right)3^{\frac{m+1}{2}} + 1,$$

where $\left(\frac{3}{m}\right)$ is the Jacobi symbol. In many cases, N_m or $N_m/7$ is a prime, see [10].

As noted previously, it is sufficient to consider a remainder $a + b\tau \in \mathbb{Z}[\omega]$ of k modulo $\tau^m - 1$, since $kP = (a + b\tau)P$ for any $P \in E_a$. Since the norm of $a + b\tau$ can be less than N_m, so the size of $a + b\tau$ can be around $m/2$. A trick in [6] shows that the reduction can be achieved by applying division with remainder for integers. Following a similar idea, we reduce an integer k modulo $\tau^m - 1$ by using Lemma 3.1 and a more explicit expression of the remainder is obtained.

Let $m > 3$ be a prime. Then $3^{\lceil \frac{m}{2} \rceil} = 3^{\frac{m+1}{2}}$. Using the division with remainder for integers, we find an integer q and a non-negative integer $r < 3^{\frac{m+1}{2}}$ such that

$$k = q3^{\frac{m+1}{2}} + \tau.$$

By Lemma 3.1, $3^{\frac{m+1}{2}} = \tau^m((\mu\omega)^{-\frac{m-1}{2}}(3\mu - \tau))$, so

$$k = q\big((\mu\omega)^{\frac{1-m}{2}}(3\mu - \tau)\big)(\tau^m - 1) + \big(r + q\big((\mu\omega)^{-\frac{m-1}{2}}(3\mu - \tau)\big)\big).$$

Notice that

$$(\mu\omega)^{\frac{1-m}{2}}(3\mu - \tau) = \begin{cases} 3\mu - \tau & \text{if } m \equiv 1 \pmod{12} \\ \tau & \text{if } m \equiv -1 \pmod{12} \\ -\tau & \text{if } m \equiv 5 \pmod{12} \\ -(3\mu - \tau) & \text{if } m \equiv -5 \pmod{12}. \end{cases}$$

Therefore, the following is true:

Proposition 4.1. *Let k, q, r be integers such that*

$$k = q3^{\frac{m+1}{2}} + r.$$

Then a remainder of k modulo $\tau^m - 1$ can be expressed as

$$a + b\tau = \begin{cases} r + q\tau' & \text{if } m \equiv 1 \pmod{12} \\ r + q\tau & \text{if } m \equiv -1 \pmod{12} \\ r - q\tau & \text{if } m \equiv 5 \pmod{12} \\ r - q\tau' & \text{if } m \equiv -5 \pmod{12} \end{cases}$$

where $\tau' = 3\mu - \tau$.

In practice, k is chosen to be less than N_m. Suppose that $k > 0$, then $q \leqslant 3^{\frac{m-1}{2}} + 1$. A bound of the norm of $\alpha + b\tau$ is obtained:

$$N(a + b\tau) = r^2 \pm 3\mu rq + 3q^2 < 7 \cdot 3^m + 5 \cdot 3^{\frac{m+1}{2}} + 3.$$

4.2. Efficient pre-computation

The Koblitz base-τ NAF method needs no pre-computation since its pre-computation set is U_6. It is a width 2 window base-τ NAF method. When the width w of window base-τ NAF method increases, pre-computation is required. Since we select MinPre_w as the pre-computation set, some further optimization can be done to get better performance.

First of all, for the set

$$\left\{\tilde{x}+\tilde{y}\tau\colon\ x=1,2,4,5,\ldots,3^{\lceil w/2\rceil}-1,\ y=0,1,\ldots,3^{\lfloor w/2\rfloor}-1\right\}$$

only half of it need to be used for pre-computation, i.e., the subset

$$\left\{\tilde{x}+\tilde{y}\tau\colon\ x=1,2,4,5,\ldots,\frac{3^{\lceil w/2\rceil}-1}{2},\ y=0,1,\ldots,3^{\lfloor w/2\rfloor}-1\right\}.$$

The other half is simply the negation of the elements from the above set. Secondly, U_6 is not considered for pre-computation though it is a subset of MinPre_w. Therefore, there are at most

$$\frac{(\frac{2}{3}\cdot 3^{\lceil w/2\rceil})3^{\lfloor w/2\rfloor}-6}{2}=3^{w-1}-3$$

elements for pre-computation.

Careful arrangement of the order of pre-computation also contributes to efficiency. We first start with prime elements. Computation of point multiplication by other elements can be partially based on multiplication by primes. If two primes are associated to each other, only one is needed for pre-computation.

For example, let us consider the case of $w=3$ and $\mu=1$. The next table presents a method for efficient pre-computation:

$x+y\tau$	$\tilde{x}+\tilde{y}\tau$	$N(\tilde{x}+\tilde{y}\tau)$	Efficient form	$(\tilde{x}+\tilde{y}\tau)P$
1	1	1	1	$P_0=P$
2	2	4	2	$P_1=2P$
4	$4-3\tau$	7	$1-\tau^2$	$P_3=P-\tau^2(P)$
$1+\tau$	$1+\tau$	7	$-\omega^2(1-\tau^2)$	$P_4=-\omega^2(P_3)$
$2+\tau$	$2-2\tau$	4	-2ω	$P_5=-\omega(P_1)$
$4+\tau$	$4-2\tau$	4	$-2\omega^2$	$P_7=-\omega(P_1)$
$1-\tau$	$1-\tau$	1	$-\omega$	$P_8=-\omega(P)$
$2-\tau$	$2-\tau$	1	$-\omega^2$	$P_9=-\omega^2(P)$
$4-\tau$	$4-\tau$	7	$1-\omega^2\tau$	$P_{11}=P+P_{10}$

This computation uses 2 point-additions and 1 point-doubling and the other operations involved are much cheaper.

Applying the same principle to the case of $w=4$ and $\mu=1$, the pre-computation needs 6 point-additions and 1 point-doubling. Details are omitted.

4.3. Analysis

As indicated in [10], the average density of nonzero coefficients of a base-τ NAF expansion of length n is $\frac{2}{5}n$. For a width w window base-τ NAF expansion of length n, the average density becomes

$$\frac{2}{2w+1}n.$$

Now suppose $\mu = 1$. We select three fields size: $m < 100$, $m = 163$ (N_{163} is a prime, see [10]) and $m > 200$. The length of the base-τ expansion is roughly m.

The next three tables reveal the performance of the window base-τ NAF method corresponding to the above three lengths. The comparison base is width $= 2$.

$m \sim 100$

Width	Pre-computation	Nonzero terms	Total operations	Saving
2	0	40	40	
3	3	28.6	31.6	21%
4	7	22.2	29.2	27%

$m \sim 163$

Width	Pre-computation	Nonzero terms	Total operations	Saving
2	0	68.4	68.4	
3	3	46.6	49.6	27%
4	7	36.2	43.2	37%

$m \sim 200$

Width	Pre-computation	Nonzero terms	Total operations	Saving
2	0	80	80	
3	3	57.1	60.1	25%
4	7	44.4	51.4	36%

We see that, if we choose the window width to be 4, we can expect more than 30% computational saving. The number of pre-computations for width 5 is much larger, so we do not expect an overall improvement when the window width increases further.

Another remark is that in the case of scalar multiplication of a fixed point (for example, key generation), we could choose a reasonably large window width, say $w = 8$ or 10.

Acknowledgement

We would like to thank the referees for their comments and suggestions.

References

[1] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, Efficient algorithms for pairing-based cryptosystems, in: Advances in Cryptology (CRYPTO '02), in: Lecture Notes in Comput. Sci., vol. 2442, 2002, pp. 354–368.

[2] I. Blake, G. Seroussi, N. Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.
[3] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in: Advances in Cryptology (CRYPTO '01), in: Lecture Notes in Comput. Sci., vol. 2139, 2001, pp. 213–239.
[4] G. Frey, H.G. Rück, A remark concerning m-divisibility and the discrete logarithm in divisor class group of curves, Math. Comput. 62 (1994) 865–874.
[5] S. Galbraith, K. Harrison, D. Soldera, Implementing the Tate pairing, in: Algorithm Number Theory Symposium (ANTS-V), in: Lecture Notes in Comput. Sci., vol. 2369, 2002, pp. 324–337.
[6] L. Hu, D. Feng, T. Wen, Fast multiplication on a family of Koblitz elliptic curves, J. Software (Chinese) 14 (2003) 1907–1910.
[7] A. Joux, A one round protocol for tripartite Diffie-Hellman, in: Algorithm Number Theory Symposium (ANTS-IV), in: Lecture Notes in Comput. Sci., vol. 1838, 2000, pp. 385–393.
[8] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (1987) 203–209.
[9] N. Koblitz, CM-curves with good cryptographic properties, in: Advances in Cryptology (CRYPTO '91), in: Lecture Notes in Comput. Sci., vol. 576, 1992, pp. 279–287.
[10] N. Koblitz, An elliptic curves implementation of the finite field digital signature algorithm, in: Advances in Cryptology (CRYPTO '98), in: Lecture Notes in Comput. Sci., vol. 1462, 1998, pp. 327–337.
[11] W. Meier, O. Staffelbach, Efficient multiplication on certain nonsupersingular elliptic curves, in: Advances in Cryptology (CRYPTO '92), in: Lecture Notes in Comput. Sci., vol. 740, 1992, pp. 333–344.
[12] A.J. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Trans. Inform. Theory 39 (1) (1993) 639–1646.
[13] V. Miller, Uses of elliptic curves in cryptography, in: Advances in Cryptology (CRYPTO '85), in: Lecture Notes in Comput. Sci., vol. 218, 1985, pp. 417–462.
[14] J. Solinas, Efficient arithmetic on Koblitz curves, Designs, Codes and Cryptography 19 (2000) 195–249.