Journal of Math-for-Industry, Vol.2(2010A-7) , pp.75-83

Math-for-industry
Education & Research Hub

Explicit lower bound for the length of minimal weight τ-adic expansions on Koblitz curves

Keisuke Hakuta, Hisayoshi Sato and Tsuyoshi Takagi

Received on March 2, 2010

Abstract. Elliptic curve cryptosystems (ECC) are emerging cryptographic standards which can be used instead of RSA cryptosystems, and are practically used. In ECC, scalar multiplication (or point multiplication) is the dominant operation, namely computing an integer multiple for a given integer and a point on an elliptic curve. However, for practical use, it is a very important matter to improve the efficiency of scalar multiplication. The τ-adic non-adjacent form (τ-NAF) proposed by Solinas, is one of the most efficient algorithms to compute scalar multiplications on Koblitz curves. Avanzi, Heuberger, and Prodinger have proven the minimality of the Hamming weight of the τ-NAF on Koblitz curves. However, the lower bound for the length of minimal Hamming weight τ-adic expansions is not known yet. In this paper, we shall derive an explicit lower bound for the length of minimal Hamming weight τ-adic expansions. We shall also give a new proof of the minimality of the Hamming weight of the τ-NAF on Koblitz curves. Further, by using the proof of the lower bound and the new proof of the minimality, we classify a minimal length τ-adic expansion with minimal Hamming weight except for two special cases. The classification shows that the τ-NAF has *almost* minimal length among all τ-adic expansions of minimal Hamming weight and we can easily convert the τ-NAF into a minimal length τ-adic expansion without changing the Hamming weight. This fact follows immediately from the proof of the lower bound and our new proof.

Keywords. Koblitz Curves (Anomalous Binary Curves), Scalar Multiplication, τ-adic Non-Adjacent Form (τ-NAF), Minimal Length

1. Introduction

Many public key cryptosystems are based on the computational complexity of number-theoretic problems (i.e. integer factoring problem, discrete logarithm problem in finite fields or elliptic curves). In such cryptosystems, number-theoretic computations are the dominant operations. The de facto standards for public-key cryptosystems are RSA cryptosystems [24], which are based on the difficulty of integer factorization. However, due to advances in algorithms to solve integer factoring problem and improvements of computing power, at least 2048 bit RSA is recommended after 2010 [21]. On the other hand, elliptic curve cryptosystems (ECC) [13], [15] which depend on the elliptic curve discrete logarithm problem, provide shorter key length and faster computation speed than those of RSA cryptosystems. For example, 224 bit ECC provides the same security level as 2048 bit RSA [21]. In ECC, scalar multiplication (or point multiplication) is the dominant operation, namely computing dP from a point P on an elliptic curve and d is an integer, defined as the point resulting of adding $P + P + \cdots + P$, d times. However, for practical use, it is a very important matter to improve the efficiency of scalar multiplication.

A common way for computing scalar multiplication is known as the double-and-add method:

$$dP = 2\big(\cdots 2(d_{\ell-1}2P + d_{\ell-2}P) + \cdots + d_1P\big) + d_0P,$$

where $\sum_{i=0}^{\ell-1} d_i 2^i = (d_{\ell-1}, d_{\ell-2}, \ldots, d_1, d_0)_2$ is the binary representation of d. In order to improve the performance of scalar multiplication, recoding methods of scalars play an important role. Especially, number systems which have low Hamming weight and short length, are attractive to accelerate scalar multiplication, and many efficient methods have been proposed (cf. [9], [23], [27], [28]).

On the other hand, instead of integer bases, efficiently computable endomorphisms on elliptic curves (as complex numbers) bases number systems are also attractive because it can be expected that the endomorphism-and-add method is more efficient than the double-and-add method (cf. [10], [14], [20], [22], [26]). Koblitz [14] introduced a family of elliptic curves which admit especially fast scalar multiplication. These curves are called *Koblitz curves* [*1] (also known as *anomalous binary curves*). Koblitz curves are defined by

$$E_a : y^2 + xy = x^3 + ax^2 + 1, \quad a \in \mathbb{F}_2 \tag{1}$$

[*1] The reason that Koblitz curves are so named is because Koblitz [14] firstly suggested that the curves are suitable for efficient implementation of ECC.

over a finite field $\mathbb{F}_2$. We identify $\{0,1\}(\subset \mathbb{Z})$ with $\mathbb{F}_2$ via the natural map $f : \{0,1\} \to \mathbb{F}_2$, $a \mapsto a \bmod 2$. For some cryptographic usage, we focus on the group of $\mathbb{F}_{2^m}$-rational points $E_a(\mathbb{F}_{2^m})$ for some $m \geq 2$. In practical use, the extension degree m is usually chosen to be a prime at least 163 (cf. [8]). Let τ be the Frobenius map on E_a,

$$\tau : E_a(\mathbb{F}_{2^m}) \to E_a(\mathbb{F}_{2^m}), \quad (x,y) \mapsto (x^2, y^2). \tag{2}$$

We can regard τ as a complex number which satisfies the following characteristic equation

$$\tau^2 - \mu\tau + 2 = 0, \quad \text{where} \quad \mu = (-1)^{1-a}. \tag{3}$$

The roots of Equation (3) are $\tau = (\mu \pm \sqrt{-7})/2$, that is, the Koblitz curve has complex multiplication by τ [*2]. Since the cost of the Frobenius map τ is cheaper than that of point doubling, and a scalar can be written as a τ-adic expansion, the Frobenius map allows for scalar multiplication without the need for point doubling [14].

Solinas [27] proposed a low Hamming weight τ-adic expansion on Koblitz curves, namely *the width-w τ-adic non-adjacent form* (*w-τ-NAF* for short). w-τ-NAF of $d \in \mathbb{Z}[\tau]$ with digit set $\mathcal{D}_w$, is a τ-adic expansion $d = \sum_{i=0}^{\ell-1} e_i \tau^i$ such that

$$e_i \neq 0 \text{ implies } e_{i+w-1} = \cdots = e_{i+1} = 0 \tag{4}$$

and $e_i \in \mathcal{D}_w$ for all i, where $\mathcal{D}_w$ is a finite subset of the rational integer ring $\mathbb{Z}$. In this paper, we focus on the digit set of zero and the odd integers with absolute value less than 2^{w-1}, that is, $\mathcal{D}_w = \{0, \pm 1, \pm 3, \ldots, \pm(2^{w-1}-1)\}$ [*3]. Solinas proved some desired properties [*4] of the τ-NAF with respect to the Hamming weight, namely, the τ-NAF has the existence and uniqueness, and the non-zero density of the τ-NAF is asymptotically 1/3 [27]. Subsequently, Avanzi, Heuberger, and Prodinger [1] have proven the minimality of the Hamming weight of the 2-τ-NAF (or τ-NAF [*5]).

The computational cost of scalar multiplication dP using the τ-and-add method with τ-NAF, is approximately $(\ell/3)\mathcal{A} + \ell\mathcal{F}$, where ℓ is the length of the τ-NAF of d, and $\mathcal{A}, \mathcal{F}$ stand for the computational cost of the point addition, the Frobenius map, respectively.

In order to take advantage of the efficiency of the τ-NAF, it is necessary that the τ-NAF has appropriate length. The length of the τ-NAF of d using [27, Algorithm 1] is $\log_2(N_{\mathbb{Z}[\tau]/\mathbb{Z}}(d)) = 2\log_2 d$, which is twice the length of the NAF of d. In order to circumvent the problem, Solinas [27] has developed modular reduction in $\mathbb{Z}[\tau]$. This technique is called the reduced τ-NAF. By using modular reduction in $\mathbb{Z}[\tau]$, we can reduce the length ℓ to a maximum of $m+a$, where a is the coefficient in Equation (1), and m is the extension degree. However, a lower bound for the length of minimal Hamming weight τ-adic expansions with digit set $\{0, \pm 1\}$, is not known yet. If the lower bound is quite small compared to the length of the τ-NAF, further speed up can be achieved in the case of polynomial basis representation.

In this paper, we shall derive an explicit lower bound for the length of minimal Hamming weight τ-adic expansions. Firstly, we give a lemma which will be needed in the proof of the lower bound and a new proof of the minimality of the Hamming weight of the τ-NAF. Secondly, we derive an explicit lower bound for the length of minimal Hamming weight τ-adic expansions based on the lemma. We also give a new proof of the minimality of the Hamming weight of the τ-NAF on Koblitz curves using the lemma. Further, by using the proof of lower bound and the new proof of the minimality of the Hamming weight of the τ-NAF, we classify a minimal length τ-adic expansion with minimal Hamming weight except for two special cases. The classification shows the following two facts. One is that the τ-NAF has *almost* minimal length among all τ-adic expansions of minimal Hamming weight with digit set $\{0, \pm 1\}$. The other is that we can easily convert the τ-NAF into a minimal length τ-adic expansion without changing the Hamming weight. These facts follow immediately from the proof of the lower bound and our new proof.

This paper is organized as follows. Section 2 prepares some notation. Section 3 shows a key lemma which will be needed in the proof of the lower bound and our new proof of the minimality of the Hamming weight of the τ-NAF. Section 4 derives an explicit lower bound for the length of minimal Hamming weight τ-adic expansions. Section 5 gives the new proof of minimality of the Hamming weight of the τ-NAF on Koblitz curves. Section 6 classifies a minimal length τ-adic expansion except for two special cases.

2. Notation

Throughout this paper, we use the symbols $\mathbb{N}, \mathbb{Z}, \mathbb{C}, \mathbb{F}_q$ to represent the natural numbers, the integers, complex numbers, and a finite field with q elements respectively. Denote by $\mathbb{Z}_{>0}$ the set of positive integers. For any non-zero complex number $\psi \in \mathbb{C} \setminus \{0\}$, we denote ψ-adic expansion $\sum_{i=0}^{\ell-1} c_i \psi^i$ with $c_i \in \mathbb{Z}$ by $(c_{\ell-1}, \ldots, c_0)_\psi$. The symbol '$*$' means a non-zero digit of τ-adic expansions. We denote by E_a the Koblitz curve defined by Equation (1) and by τ the Frobenius map on E_a defined by (2). Let $\mathcal{D} := \mathcal{D}_2 = \{0, \pm 1\}$. Note that for a fixed coefficient $a \in \mathbb{F}_2$ in Equation (1), it satisfies that $\mathcal{D} = \{0, \pm\mu\}$.

For any element α in $\mathbb{Z}[\tau]$, we denote by $\alpha = \sum_{i=0}^{\ell-1} b_i \tau^i$ ($b_i \in \mathcal{D}$) the τ-NAF of α, and by $\alpha = \sum_{i=0}^{\ell'-1} c_i \tau^i$ ($c_i \in \mathcal{D}$) be any τ-adic expansion of α, respectively. The length of τ-NAF of α is denoted by $\ell_{\tau\text{-NAF}}(\alpha)$. We denote by

[*2] For detail, refer to [25].

[*3] A digit set which has the property (4), is called a *width-w non-adjacent digit set* (w-NADS). Otherwise it is called a non-w-NADS. w-NADS have already been investigated in the case of w-NAF (cf. [18], [5]). Solinas also proposed the digit set of minimal norm representatives [27]. Subsequently, Avanzi, Heuberger, and Prodinger [2], [4] proposed another two digit sets.

[*4] For the width-w non-adjacent form (w-NAF), the desired properties are shown in [5], [17], [18], [19], [27].

[*5] For $w = 3$, the minimality with digit set has also been shown by Avanzi, Heuberger, and Prodinger [2]. Unlike in the case of $w = 2, 3$, this is *not* true for $w \in \{4, 5, 6\}$ [11]. Similar results for the τ-NAF and its desired properties are proved in [6] and in [12] on another special types of elliptic curves, respectively.

$\ell_{\min}(\alpha)$ the length of τ-adic expansion of minimal length among all τ-adic expansions of minimal Hamming weight with digit set $\mathcal{D}$. Additionally, we use the following notation in Section 3 and Section 5. If $\ell > \ell'$ then put $c_{\ell'} = c_{\ell'+1} = \cdots = c_{\ell-1} = 0$. Otherwise, put $b_\ell = b_{\ell+1} = \cdots = b_{\ell'-1} = 0$. Furthermore, replace $\max\{\ell, \ell'\}$ by ℓ if necessary. We put $S_\alpha := \{i \in \{0, 1, \ldots, \ell-1\} | b_i \neq 0\}$, and $T_\alpha := \{i \in \{0, 1, \ldots, \ell-1\} | c_i \neq 0\}$.

3. Key Lemma

In this section, we show a key lemma (Lemma 2) which will be needed in the proof of the lower bound and the new proof. We begin with recursive formulas to convert any τ-adic expansion into the τ-NAF. The following lemma is useful to obtain such recursive formulas.

Lemma 1. *Let $\ell \in \mathbb{N}$ be a natural number. If $\sum_{i=0}^{\ell-1} a_i\tau^i = 0$ ($a_i \in \mathcal{D}$), then $a_i = 0$ for all i ($0 \le i \le \ell-1$).*

Proof. From $\sum_{i=0}^{\ell-1} a_i\tau^i = a_0 + \left(\sum_{i=1}^{\ell-1} a_i\tau^i\right)$ and $\tau | 0$, we have $2|a_0$. By $a_0 \in \mathcal{D}$, we have $a_0 = 0$. We put $\alpha' := \{\left(\sum_{i=0}^{\ell-1} a_i\tau^i\right) - a_0\}/\tau$. By the same argument as above, it satisfies $a_1 = 0$. Similar to the case of a_0 and a_1, we also have $a_2 = 0, \ldots, a_{\ell-1} = 0$. Therefore $a_i = 0$ for all i. □

The τ-adic expansion $\sum_{i=0}^{\ell-1}(b_i - c_i)\tau^i$ is not necessarily τ-adic expansion with $\mathcal{D}$, because $(b_i - c_i) \in \{0, \pm1, \pm2\}$. However, by using the following carry rules from right to left (i.e. from the least significant digit to the most significant digit), we can convert $\sum_{i=0}^{\ell-1}(b_i - c_i)\tau^i$ into τ-adic expansion $\sum_{i=0}^{\ell-1} a_i\tau^i$ ($a_i \in \mathcal{D}$). For each i ($i = 0, 1, 2, ..., \ell-1$), a_i's are obtained by the following recursive formulas:

$$a_i = (b_i - c_i) - \mu D_{i-1}^* + D_{i-2}^* + D_i, \tag{5}$$

where $D_{-1}^* = D_{-2}^* = 0$, and for all i,

(6)

$$D_i := \begin{cases} -\left\lfloor \frac{(b_i - c_i) - \mu D_{i-1}^* + D_{i-2}^*}{2} \right\rfloor \times 2 \\ \qquad \text{(if } (b_i - c_i) - \mu D_{i-1}^* + D_{i-2}^* \ge 0\text{)}, \\ \left\lfloor \frac{-\left((b_i - c_i) - \mu D_{i-1}^* + D_{i-2}^*\right)}{2} \right\rfloor \times 2 \qquad \text{(otherwise)}, \end{cases}$$

and

$$D_i^* = D_i/2 \ (i \ge 0). \tag{7}$$

From (5) and (6), it follows that by applying Lemma 1 for $\sum_{i=0}^{\ell-1} a_i\tau^i$, each a_i is an element in $\{0, \pm1\}$. From Lemma 1, we have $a_i = 0$ for all i. In other words, for any $\alpha \in \mathbb{Z}[\tau]$ and any τ-adic expansion $\alpha = \sum_{i=0}^{\ell'-1} c_i\tau^i$ with digit set $\mathcal{D}$, we can compute the τ-NAF of α ($\alpha = \sum_{i=0}^{\ell-1} b_i\tau^i$) using the recursive formulas (5), (6), and (7).

The lower bound and our new proof of the minimality of the Hamming weight of the τ-NAF are based on the following lemma.

Lemma 2. [Key Lemma for Lower Bound and Our New Proof]

Let $S := \{0, \pm1\} \times \{0, \pm1\} \times \{0, \pm1\} \times \{0, \pm1\} \times \{0, \pm2\}$ be the direct product of four copies of $\{0, \pm1\}(\subset \mathbb{Z})$ and $\{0, \pm2\}(\subset \mathbb{Z})$. Let $H_i := (b_i, c_i, D_{i-1}^*, D_{i-2}^*, D_i) \in S$ for i ($0 \le i \le \ell-1$). Let $A_1 := \{(\mu, 0, 1, 0, 0), (-\mu, 0, -1, 0, 0)\}$,
$A_2 := \{(\mu, 0, 0, -\mu, 0), (-\mu, 0, 0, \mu, 0)\}$,
$A_3 := \{(\mu, 0, -1, 0, -2\mu), (-\mu, 0, 1, 0, 2\mu)\}$,
$A_4 := \{(\mu, 0, 0, \mu, -2\mu), (-\mu, 0, 0, -\mu, 2\mu)\}$ be the subset of S, respectively.

(1) *$D_i = 0, \pm2$ ($D_i^* = 0, \pm1$) for all i.*

(2) *If $c_{i+1} = 0, b_{i+1} \neq 0$ for some $i \ge 0$, then $H_{i+1} \in A_1 \cup A_2 \cup A_3 \cup A_4$.*

(3) *If $H_{i+1} \in A_1 \cup A_3$, then $b_i = 0, c_i \neq 0$. If $H_{i+1} \in A_4$, then it hold $b_{i+2} = 0$ and $c_{i+2} \neq 0$. In particular, if $H_i \in A_4$, then $H_{i+2} \notin A_1 \cup A_3$.*

(4) *For $i_0 \in \{0, 1, \ldots, \ell-1\}$, the following conditions are equivalent:*
   (a) *$\sum_{i=0}^{i_0} b_i\tau^i = \sum_{i=0}^{i_0} c_i\tau^i$;*
   (b) *$D_{i_0-1} = 0$ and $D_{i_0} = 0$.*

(5) *Suppose that $H_{i+1} \in A_2$. If $(D_{j+1}, D_j) \neq (0, 0)$ for all j ($-1 \le j \le i-1$), then $i \ge 2$ and*

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix}$$

satisfies one of the following two cases:

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} \in \Gamma_1, \tag{8}$$

or

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} \in \Gamma_2, \tag{9}$$

where

$$\Gamma_1 = \left\{ \begin{pmatrix} 0 & 0 & 1 \\ 0 & -\mu & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ 0 & \mu & 1 \end{pmatrix} \right\},$$

$$\Gamma_2 = \left\{ \begin{pmatrix} * & 0 & 1 \\ * & -\mu & -1 \end{pmatrix}, \begin{pmatrix} * & 0 & -1 \\ * & \mu & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 \\ 0 & \mu & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1 \\ 0 & -\mu & 1 \end{pmatrix} \right\}.$$

In particular, if

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} \in \left\{ \begin{pmatrix} -1 & 0 & 1 \\ 0 & \mu & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1 \\ 0 & -\mu & 1 \end{pmatrix} \right\} \subset \Gamma_2$$

holds, then $i \ge 3$, $H_2 \in A_4$, and

$$\begin{pmatrix} b_3 & b_2 & b_1 & b_0 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix} \in \Gamma_3, \tag{10}$$

where

$$\Gamma_3 = \left\{ \begin{pmatrix} 0 & -1 & 0 & 1 \\ \mu & 0 & \mu & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & -1 \\ -\mu & 0 & -\mu & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 & 1 \\ -\mu & 0 & \mu & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & -1 \\ \mu & 0 & -\mu & 1 \end{pmatrix} \right\}. \tag{11}$$

Proof. (1) Let us assume the contrary and seek a contradiction. Suppose that there exists $i \in \{0,1,2,\ldots,\ell-1\}$ such that i does not satisfy $D_i = 0, \pm 2$, and i_0 be the minimal such $i \in \{0,1,2,\ldots,\ell-1\}$. We evaluate the range of D_{i_0}. For i which satisfies $i \leq i_0 - 1$, we have $D_i = 0, \pm 2$ ($D_i^* = 0, \pm 1$). Then

$$\begin{aligned} & |b_{i_0} - c_{i_0} - \mu D^*_{i_0-1} + D^*_{i_0-2}| \\ \leq\ & |b_{i_0}| + |c_{i_0}| + |\mu D^*_{i_0-1}| + |D^*_{i_0-2}| \\ \leq\ & 1+1+1+1 = 4. \end{aligned}$$

By Equation (6), D_i is an even number, and $|D_{i_0}| > 2$, we have $D_{i_0} = \pm 4$. There are two cases to consider, $D_{i_0} = -4$ and $D_{i_0} = 4$. We only consider the former because the latter may be treated similar to the former case. From $|b_{i_0}|, |c_{i_0}| \leq 1, |D^*_{i_0-1}|, |D^*_{i_0-2}| \leq 1$, we must have $b_{i_0} = 1$, $c_{i_0} = -1$, $D^*_{i_0-1} = -\mu$, $D^*_{i_0-2} = 1$ in order to satisfy $0 = a_{i_0} = b_{i_0} - c_{i_0} - \mu D^*_{i_0-1} + D^*_{i_0-2} + D_{i_0}$. So $D_{i_0-1} = 2D^*_{i_0-1} = -2\mu$. On the other hand, $(b_{\ell-1}, \ldots, b_1, b_0)_\tau$ is the τ-NAF, so $b_{i_0} = 1$ implies $b_{i_0-1} = 0$. Hence

$$\begin{aligned} 0 = a_{i_0-1} &= b_{i_0-1} - c_{i_0-1} - \mu D^*_{i_0-2} + D^*_{i_0-3} + D_{i_0-1} \\ &= -c_{i_0-1} - \mu * 1 + D^*_{i_0-3} - 2\mu \\ &= -c_{i_0-1} + D^*_{i_0-3} - 3\mu, \end{aligned}$$

we obtain $c_{i_0-1} = D^*_{i_0-3} - 3\mu$. However, $D^*_{i_0-3} \in \{0, \pm 1\} = \{0, \pm\mu\}$, we have $|c_{i_0-1}| = |D^*_{i_0-3} - 3\mu| \geq |\,|D^*_{i_0-3}| - |3\mu|\,| \geq |\,|D^*_{i_0-3}| - 3| \geq 2$. This is a contradiction.

(2) We assume that $c_{i+1} = 0, b_{i+1} = \pm\mu$. Then we have $0 = a_{i+1} = b_{i+1} - \mu D^*_i + D^*_{i-1} + D_{i+1}$. It is necessary to treat the cases $D_{i+1} = 0$ and $D_{i+1} \neq 0$ separately.

(Case 1) $D_{i+1} = 0$.

It is easy to see that $H_{i+1} \in A_1 \cup A_2$.

(Case 2) $D_{i+1} \neq 0$.

If the sign of b_{i+1} is same as that of D_{i+1}, we must have $|b_{i+1} + D_{i+1}| = 3$. So it does not occur that $b_{i+1} - \mu D^*_i + D^*_{i-1} + D_{i+1} = 0$. Hence from b_{i+1} and D_{i+1} have the opposite signs, we have $H_{i+1} \in A_3 \cup A_4$.

Therefore, if $c_{i+1} = 0, b_{i+1} \neq 0$ then $H_{i+1} \in A_1 \cup A_2 \cup A_3 \cup A_4$.

(3) First, we assume that $H_{i+1} \in A_1$. Since $(b_{\ell-1}, \ldots, b_1, b_0)_\tau$ is the τ-NAF and $b_{i+1} \neq 0$, we have $b_i = 0$. We substitute $b_i = 0$ into $a_i = (b_i - c_i) - \mu D^*_{i-1} + D^*_{i-2} + D_i = 0$, we have $c_i = -\mu D^*_{i-1} + D^*_{i-2} + D_i$. Since $H_{i+1} \in A_1$ and $c_i = -\mu * 0 + D^*_{i-2} \pm 2 = D^*_{i-2} \pm 2 \neq 0$, we have $c_i \neq 0$.

Next, suppose that $H_{i+1} \in A_3$. Similar to the above case, since $c_i = -\mu * 0 + D^*_{i-2} \mp 2 = D^*_{i-2} \mp 2 \neq 0$, we also have $b_i = 0, c_i \neq 0$.

We assume that $H_{i+1} \in A_4$. Since $(b_{\ell-1}, \ldots, b_1, b_0)_\tau$ is the τ-NAF and $b_{i+1} \neq 0$, we have $b_{i+2} = 0$. From $a_{i+2} = b_{i+2} - c_{i+2} - \mu D^*_{i+1} + D^*_i + D_{i+2} = 0$ and $c_{i+2} = \pm 1 + D_{i+2} \neq 0$, we have $c_{i+2} \neq 0$. Moreover, if $H_i \in A_4$, from $D_i = \mp 2\mu$, we have $D^*_i = \mp\mu$. Therefore it does not occur that $H_{i+2} \in A_1 \cup A_3$.

(4)

$$\begin{aligned} & \sum_{i=0}^{i_0} b_i \tau^i = \sum_{i=0}^{i_0} c_i \tau^i \\ \iff\ & \sum_{i=0}^{i_0} (b_i - c_i)\tau^i = 0 \\ \iff\ & \sum_{i=0}^{i_0} (b_i - c_i)\tau^i + \sum_{i=0}^{i_0} (\tau^2 - \mu\tau + 2) D^*_i \tau^i = 0 \\ \iff\ & \sum_{i=0}^{i_0} \{(b_i - c_i) - \mu D^*_{i-1} + D^*_{i-2} + D_i\}\tau^i \\ & \qquad + (D^*_{i_0}\tau - \mu D^*_{i_0} + D^*_{i_0-1})\tau^{i_0+1} = 0 \\ \iff\ & \sum_{i=0}^{i_0} a_i \tau^i + (D^*_{i_0}\tau - \mu D^*_{i_0} + D^*_{i_0-1})\tau^{i_0+1} = 0 \\ \iff\ & (D^*_{i_0}\tau - \mu D^*_{i_0} + D^*_{i_0-1})\tau^{i_0+1} = 0 \\ \iff\ & D^*_{i_0}\tau + (-\mu D^*_{i_0} + D^*_{i_0-1}) = 0 \\ \iff\ & D_{i_0-1} = 0, D_{i_0} = 0 \end{aligned}$$

(5) Since $(D_0, D_{-1}) \neq (0,0)$ and $D_{-1} = 0$, we must have $D_0 \neq 0$. There are two cases to consider, $D_0 = -2$ and $D_0 = 2$. We only consider the former because the latter may be treated similar to the former case. From $D_0 = -2$, we must have $b_0 = 1$ and $c_0 = -1$. Since $(b_{\ell-1}, \ldots, b_1, b_0)_\tau$ is the τ-NAF and $b_0 \neq 0$, we have $b_1 = 0$. Hence from $b_1 - c_1 - \mu D^*_0 + D^*_{-1} + D_1 = -c_1 + \mu + D_1 = 0$, we have $(c_1, D_1) = (-\mu, -2\mu)$ or $(\mu, 0)$.

(Case 1) $(c_1, D_1) = (-\mu, -2\mu)$.

By $b_2 - c_2 - \mu D^*_1 + D^*_0 + D_2 = b_2 - c_2 + D_2 = 0$, we have $(b_2, c_2, D_2) = (0,0,0)$, $(\pm 1, \pm 1, 0)$, or $(\pm\mu, \mp\mu, \mp 2\mu)$, where double signs are taken in the same order. Thus $\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -\mu & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & -\mu & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 \\ -1 & -\mu & -1 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 1 \\ -\mu & -\mu & -1 \end{pmatrix}$, or $\begin{pmatrix} -\mu & 0 & 1 \\ \mu & -\mu & -1 \end{pmatrix}$.

(Case 2) $(c_1, D_1) = (\mu, 0)$.

By $b_2 - c_2 - \mu D^*_1 + D^*_0 + D_2 = b_2 - c_2 + D_2 - 1 = 0$, we have $(b_2, c_2, D_2) = (0,1,2)$, $(0,-1,0)$, $(-1,0,2)$, or $(1,0,0)$. Thus, in the cases of $(b_2, c_2, D_2) = (0,1,2)$ or $(0,-1,0)$, we have

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & \mu & -1 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 0 & 1 \\ -1 & \mu & -1 \end{pmatrix}.$$

In the case of $(b_2, c_2, D_2) = (-1, 0, 2)$, from $b_3 - c_3 - \mu D^*_2 + D^*_1 + D_3 = -c_2 - \mu + D_3 = 0$, we have $(c_2, D_3) = (\mu, 2\mu)$ or $(-\mu, 0)$. Thus

$$\begin{pmatrix} b_3 & b_2 & b_1 & b_0 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 1 \\ \mu & 0 & \mu & -1 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & -1 & 0 & 1 \\ -\mu & 0 & \mu & -1 \end{pmatrix}.$$

Moreover, if $(c_2, D_3) = (\mu, 2\mu)$, then $H_2 = (-1, 0, 0, -1, 2) \in A_4$, and if $(c_2, D_3) = (-\mu, 0)$, then $H_2 = (-\mu, 0, 0, -\mu, 2\mu) \in$

A_4. In the case of $(b_2, c_2, D_2) = (1, 0, 0)$, we have $(D_1, D_2) = (0, 0)$. This is a contradiction.

Hence we obtain

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} \in \Gamma_1 \cup \Gamma_2,$$

or

$$\begin{pmatrix} b_3 & b_2 & b_1 & b_0 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix} \in \Gamma_3.$$

In particular,

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & * \\ 0 & * & * \end{pmatrix}, \begin{pmatrix} * & 0 & * \\ * & * & * \end{pmatrix}, \begin{pmatrix} 0 & 0 & * \\ * & * & * \end{pmatrix}$$

or

$$\begin{pmatrix} b_3 & b_2 & b_1 & b_0 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix} = \begin{pmatrix} 0 & * & 0 & * \\ * & 0 & * & * \end{pmatrix}.$$

It is easy to see that $i \geq 2$ when

$$\begin{pmatrix} b_2 & b_1 & b_0 \\ c_2 & c_1 & c_0 \end{pmatrix} \in \Gamma_1 \cup \Gamma_2,$$

and $i \geq 3$ when

$$\begin{pmatrix} b_3 & b_2 & b_1 & b_0 \\ c_3 & c_2 & c_1 & c_0 \end{pmatrix} \in \Gamma_3.$$

□

4. Lower Bound for the Length

This section derives an explicit lower bound for the length of minimal Hamming weight τ-adic expansions. From the definition of $\ell_{\min}$, the following upper bound for $\ell_{\min}$ is trivially true for all $\alpha \in \mathbb{Z}[\tau]$:

$$\ell_{\min}(\alpha) \leq \ell_{\tau\text{-NAF}}(\alpha).$$

An lower bound $\ell_{\min}$ can also be derived in terms of the length of the τ-NAF. The following lower bound for $\ell_{\min}$ is based on Lemma 2.

Theorem 1. [Lower Bound for $\ell_{\min}(\alpha)$]
Suppose that $\ell' < \ell$. Then for any $\alpha \in \mathbb{Z}[\tau]$,

$$\ell_{\tau\text{-NAF}}(\alpha) - 3 \ (= \ell - 3) \leq \ell'. \tag{12}$$

In particular,

$$\ell_{\tau\text{-NAF}}(\alpha) - 3 \leq \ell_{\min}(\alpha). \tag{13}$$

Proof. The latter part follows immediately from the former part. We show the former part. We assume that $c_{\ell'} = 0$, $c_{\ell'+1} = 0, \ldots, c_{\ell-1} = 0$. Note that $b_{\ell-1} \neq 0$ and $c_{\ell-1} = 0$. From Lemma 2 (2), it satisfies that $H_{\ell-1} \in A_1 \cup A_2 \cup A_3 \cup A_4$. Since $\sum_{i=0}^{\ell-1} b_i \tau^i = \sum_{i=0}^{\ell-1} c_i \tau^i$, we have $D_i = 0$ for all $i \geq \ell - 2$. It follows that $H_{\ell-1} \notin A_1 \cup A_3 \cup A_4$. We only deal with the case of $H_{\ell-1} \in A_2$. There are two cases to consider, $H_{\ell-1} = (\mu, 0, 0, -\mu, 0)$ and $H_{\ell-1} = (-\mu, 0, 0, \mu, 0)$. Without loss of generality, we may assume that $H_{\ell-1} = (\mu, 0, 0, -\mu, 0)$ because the latter may be treated in exactly the same way. By $b_{\ell-1} \neq 0$, it satisfies $b_{\ell-2} = 0$. From

$$\begin{aligned} a_{\ell-2} &= (b_{\ell-2} - c_{\ell-2}) - \mu D^*_{\ell-3} + D^*_{\ell-4} + D_{\ell-2} \\ &= -c_{\ell-2} + 1 + D^*_{\ell-4} \\ &= 0, \end{aligned}$$

we have $c_{\ell-2} = D^*_{\ell-4} + 1$. Hence we obtain $(c_{\ell-2}, D^*_{\ell-4}) = (1, 0)$ or $(0, -1)$.

(Case 1) $(c_{\ell-2}, D^*_{\ell-4}) = (1, 0)$.
It is easily to see that $\ell' = \ell - 1$.

(Case 2) $(c_{\ell-2}, D^*_{\ell-4}) = (0, -1)$.
It holds that

$$\begin{aligned} a_{\ell-3} &= (b_{\ell-3} - c_{\ell-3}) - \mu D^*_{\ell-4} + D^*_{\ell-5} + D_{\ell-3} \\ &= (b_{\ell-3} - c_{\ell-3}) + \mu + D^*_{\ell-5} - 2\mu \\ &= (b_{\ell-3} - c_{\ell-3}) + D^*_{\ell-5} - \mu \\ &= 0. \end{aligned}$$

So

$$\begin{aligned} (b_{\ell-3}, c_{\ell-3}, D^*_{\ell-5}) = (0, 0, \mu), (0, -\mu, 0), (\mu, 0, 0), \\ (\mu, \mu, \mu), (\mu, -\mu, -\mu), \text{ or } (-\mu, -\mu, \mu). \end{aligned}$$

However, if $(b_{\ell-3}, c_{\ell-3}, D^*_{\ell-5}) = (\mu, \mu, \mu)$ or $(-\mu, -\mu, \mu)$, then $b_{\ell-3} \neq 0$ and $b_{\ell-4} \neq 0$. This contradicts the fact that $\alpha = \sum_{i=0}^{\ell-1} b_i \tau^i$ is the τ-NAF of α. Therefore it does not occur that $(b_{\ell-3}, c_{\ell-3}, D^*_{\ell-5}) = (\mu, \mu, \mu)$ and $(-\mu, -\mu, \mu)$. If $(b_{\ell-3}, c_{\ell-3}, D^*_{\ell-5}) = (0, -\mu, 0)$ or $(\mu, -\mu, -\mu)$, then $\ell' = \ell - 2$.

It remains to consider the case that $(b_{\ell-3}, c_{\ell-3}, D^*_{\ell-5}) = (0, 0, \mu)$ and $(\mu, 0, 0)$. If $(b_{\ell-3}, c_{\ell-3}, D^*_{\ell-5}) = (0, 0, \mu)$, then from

$$\begin{aligned} a_{\ell-4} &= (b_{\ell-4} - c_{\ell-4}) - \mu D^*_{\ell-5} + D^*_{\ell-6} + D_{\ell-4} \\ &= (b_{\ell-4} - c_{\ell-4}) + D^*_{\ell-6} - 3 \\ &= 0, \end{aligned}$$

we have $(b_{\ell-4}, c_{\ell-4}, D^*_{\ell-6}) = (1, -1, 1)$. This indicates that $\ell' = \ell - 3$. If $(b_{\ell-3}, c_{\ell-3}, D^*_{\ell-5}) = (\mu, 0, 0)$, we must have $b_{\ell-4} = 0$. Then

$$\begin{aligned} a_{\ell-4} &= (b_{\ell-4} - c_{\ell-4}) - \mu D^*_{\ell-5} + D^*_{\ell-6} + D_{\ell-4} \\ &= -c_{\ell-4} + D^*_{\ell-6} - 2 \\ &= 0. \end{aligned}$$

Hence we obtain $(c_{\ell-4}, D^*_{\ell-6}) = (-1, 1)$. Thus $\ell' = \ell - 3$.

Combining (Case 1) and (Case 2), we obtain Inequality (12). □

As already mentioned, τ-NAF has the smallest Hamming weight with digit set $\{0, \pm 1\}$. Further, Theorem 1 tells us that τ-NAF also has *almost minimal length* with digit set $\{0, \pm 1\}$.

5. Our New Proof

In this section, we give a new proof of minimality of the Hamming weight of the τ-NAF on Koblitz curves.

5.1. The Main Idea of Our New Proof

The minimality of the Hamming weight of the τ-NAF on Koblitz curves was first proved by Avanzi, Heuberger, and Prodinger [1], [3]. They have presented two proofs for the minimality. One is referred as *the Direct proof*, which is induction on the Hamming weight. The other is referred as *the Automatic proof*, which is based on a weighted digraph induced by the transducer to compute the τ-NAF from any τ-adic expansion from right to left (see [1], [3] for proofs).

The strategy of our new proof of the minimality is as follows. For any $\alpha \in \mathbb{Z}[\tau]$, we directly construct an injection map from S_α into T_α. Notice that if it is possible to construct an injection map from S_α to T_α for any α and any τ-adic expansion of α, then the Hamming weight of the τ-NAF of α is always smaller than that of the τ-adic expansion, that is, the τ-NAF minimizes the Hamming weight with digit set $\{0, \pm 1\}$.

A similar strategy is already used for the proof of minimality of the Hamming weight of the generalized nonadjacent form (GNAF) [9]. We briefly review the strategy to prove the minimality of the Hamming weight of the GNAF. Let $r \geq 2$ be a positive integer, β be any element of $\mathbb{Z}_{>0}$. We denote by $\beta = \sum_{i=0}^{\ell-1} g_i r^i$ ($g_i \in \mathcal{D}_{\mathrm{G}}$) the GNAF of β, where $\mathcal{D}_{\mathrm{G}} = \{0, \pm 1, \ldots, \pm(r-1)\}$. Let $\beta = \sum_{i=0}^{\ell'-1} h_i r^i$ ($h_i \in \mathcal{D}_{\mathrm{G}}$) be any r-adic expansion of β. If $\ell > \ell'$, then put $h_{\ell'} = h_{\ell'+1} = \cdots = h_{\ell-1} = 0$. Otherwise, put $g_\ell = g_{\ell+1} = \cdots = g_{\ell'-1} = 0$. Furthermore, replace $\max\{\ell, \ell'\}$ by ℓ if necessary. We put $S_\beta := \{i \in \{0, 1, \ldots, \ell-1\} | g_i \neq 0\}$, and $T_\beta := \{i \in \{0, 1, \ldots, \ell-1\} | h_i \neq 0\}$.

Then the following claim holds.

Claim 1. [The Key Point of the Minimality [9]] *If $h_{i+1} = 0$ for some $i \geq 0$, then either $g_{i+1} = 0$ or $h_i \neq 0$ and $g_i = 0$.*

Thus from Claim 1, we can construct the following simple injection map.

$$\begin{array}{rccll} \varphi_\beta : & S_\beta & \to & T_\beta & \\ & \cup & & \cup & \\ & i & \mapsto & i & (g_i \neq 0,\ h_i \neq 0), \\ & i & \mapsto & i-1 & (g_i \neq 0,\ h_i = 0). \end{array}$$

We can see that Lemma 2 is analogous result for τ-adic expansion.

5.2. Our New Proof

We are now in a position to give our new proof of the minimality of the Hamming weight of the τ-NAF on Koblitz curves.

Our New Proof of the Minimality.

With notation as above, we directly construct an injection map $\varphi_\alpha : S_\alpha \to T_\alpha$ for each case.

(Case 1) $H_i \notin A_2$ for all i $(0 \leq i \leq \ell - 1)$.

We define a map $\varphi_\alpha : S_\alpha \to T_\alpha$ as follows.

$$\begin{array}{rccll} \varphi_\alpha : & S_\alpha & \to & T_\alpha & \\ & \cup & & \cup & \\ & i & \mapsto & i & (b_i \neq 0,\ c_i \neq 0), \\ & i & \mapsto & i-1 & (H_i \in A_1 \cup A_3), \\ & i & \mapsto & i+1 & (H_i \in A_4). \end{array}$$

From the recursive formula (5) and $D^*_{-1} = D^*_{-2} = 0$, it does not occur that $b_0 \neq 0$ and $c_0 = 0$. This implies that if $0 \in S_\alpha$, then $\varphi_\alpha(0) \in T_\alpha$. From Lemma 2 (3), the map φ_α does not satisfy $\varphi_\alpha(i) = i+1$ and $\varphi_\alpha(i+2) = i+1$ for any i. Thus, the map $\varphi_\alpha : S_\alpha \to T_\alpha$ is injective.

(Case 2) $H_i \in A_2$ for some i $(0 \leq i \leq \ell - 1)$.

Let $\{i_1, i_2, \ldots, i_k\}$ be the set so that $H_{i_j} \in A_2$ for $1 \leq j \leq k$ and $k < k'$ implies $i_k < i_{k'}$. We denote $i_0 := -1$ for convenient. Since $H_{i_j} \in A_2$ and $(D_{-1}, D_{-2}) = (0, 0)$, we have $(D_{i_j}, D_{i_j - 1}) = (0, 0)$ for $0 \leq j \leq k$. From Lemma 2 (4), we have $\sum_{i=i_j+1}^{i_{j+1}} b_i \tau^i = \sum_{i=i_j+1}^{i_{j+1}} c_i \tau^i$ for $0 \leq j \leq k-1$.

For each i_j $(1 \leq j \leq k)$, we denote

(14)

$$M_j := \{n \in \mathbb{Z} | i_{j-1} \leq n \leq i_j - 1, (D_n, D_{n-1}) = (0, 0)\}.$$

Note that for $1 \leq j \leq k$, the set M_j is not empty, because $i_{j-1} \in M_j$. We put $m_j = \max M_j$. Then, we have $(D_n, D_{n-1}) \neq (0, 0)$ for $m_j + 1 \leq n \leq i_j - 1$. By Lemma 2 (5), we have $(b_{m_j+2}, c_{m_j+2}) = (0, *)$.
Moreover, from Lemma 2 (5), if

$$\begin{pmatrix} b_{m_j+4} & b_{m_j+3} & b_{m_j+2} & b_{m_j+1} \\ c_{m_j+4} & c_{m_j+3} & c_{m_j+2} & c_{m_j+1} \end{pmatrix} \in \Gamma_3,$$

then $H_{m_j+2} \in A_4$. Therefore we obtain

$$i_0 \leq m_1 \leq i_1 \leq \cdots \leq m_j \leq i_j \leq \cdots \leq m_k \leq i_k. \tag{15}$$

Furthermore, by Lemma 2 (5), if

$$\begin{pmatrix} b_{m_j+3} & b_{m_j+2} & b_{m_j+1} \\ c_{m_j+3} & c_{m_j+2} & c_{m_j+1} \end{pmatrix} \in \Gamma_1 \cup \Gamma_2,$$

then $i_j \geq m_j + 3$, and if

$$\begin{pmatrix} b_{m_j+4} & b_{m_j+3} & b_{m_j+2} & b_{m_j+1} \\ c_{m_j+4} & c_{m_j+3} & c_{m_j+2} & c_{m_j+1} \end{pmatrix} \in \Gamma_3,$$

then $i_j \geq m_j + 4$. We define a map $\varphi_\alpha : S_\alpha \to T_\alpha$ as follows.

$$\begin{array}{rccll} \varphi_\alpha : & S_\alpha & \to & T_\alpha & \\ & \cup & & \cup & \\ & i & \mapsto & i & (b_i \neq 0,\ c_i \neq 0), \\ & i & \mapsto & i-1 & (H_i \in A_1 \cup A_3), \\ & i & \mapsto & i+1 & (H_i \in A_4), \\ & i_j & \mapsto & m_j + 2 & (H_{i_j} \in A_2). \end{array}$$

By the same argument as (Case 1), if $0 \in S_\alpha$, then $\varphi_\alpha(0) \in T_\alpha$. By Lemma 2 (5), for all i which satisfy $i \notin \{i_1, i_2, \ldots, i_k\}$, it does not occur $\varphi_\alpha(i) = m_j + 2$. Thus, the map $\varphi_\alpha : S_\alpha \to T_\alpha$ is injective. This completes the proof. □

6. τ-adic Minimal Length Form

This section classifies a minimal length τ-adic expansion with minimal Hamming weight except for two special cases. In the case of the ordinary NAF, minimal length binary representation with minimal Hamming weight is shown in [7, Corollary 3]. From Theorem 1 and our new proof, we now obtain analogous result for τ-adic expansion. Corollary 1 shows that we can convert τ-NAF into a minimal length τ-adic expansion without changing the Hamming weight. This fact follows immediately from the proof of the lower bound and our new proof of the minimality of the Hamming weight of the τ-NAF.

Corollary 1. [τ-adic Minimal Length Expansion] *Let d be an element of $\mathbb{Z}[\tau]$, and $\sum_{i=0}^{\ell-1} e_i\tau^i$ ($e_i \in \mathcal{D}$, $e_{\ell-1} \neq 0$) be the τ-NAF of d. We convert the τ-NAF $d = \sum_{i=0}^{\ell-1} e_i\tau^i$ into $d = \sum_{i=0}^{\ell'-1} e'_i\tau^i$ ($e'_i \in \mathcal{D}$, $e'_{\ell'-1} \neq 0$) as follows.*

(Case 1) $\ell < 6$.

If $(e_{\ell-1}, \ldots, e_0)_\tau$ is equal to one of the τ-NAF in Table 1 (*double signs are taken in the same order*), *then we convert $(e_{\ell-1}, \ldots, e_0)_\tau$ into $(e'_{\ell'-1}, \ldots, e'_0)_\tau$ using* Table 1. *Otherwise, $\ell = \ell'$ and $e_i = e'_i$ for all i.*

Table 1: Conversion of the τ-NAF into the τ-MLF ($\ell < 6$)

$(e_{\ell-1}, \ldots, e_0)_\tau$	$(e'_{\ell'-1}, \ldots, e'_0)_\tau$	ℓ	ℓ'
$(\pm\mu, 0, 0, \pm 1)_\tau$	$(\mp\mu, \mp 1)_\tau$	4	2
$(\pm\mu, 0, 0, \pm 1, 0)_\tau$	$(\mp\mu, \mp 1, 0)_\tau$	5	3
$(\pm\mu, 0, \pm\mu)_\tau$	$(\pm 1, \mp\mu)_\tau$	3	2
$(\pm\mu, 0, \pm\mu, 0)_\tau$	$(\pm 1, \mp\mu, 0)_\tau$	4	3
$(\pm\mu, 0, \pm\mu, 0, 0)_\tau$	$(\pm 1, \mp\mu, 0, 0)_\tau$	5	4
$(\pm\mu, 0, \pm\mu)_\tau$	$(\pm 1, \mp\mu)_\tau$	3	2
$(\pm\mu, 0, \pm\mu, 0)_\tau$	$(\pm 1, \mp\mu, 0)_\tau$	4	3
$(\pm\mu, 0, \pm\mu, 0, \pm\mu)_\tau$	$(\mp\mu, \mp 1, \pm\mu)_\tau$	5	3
$(\pm\mu, 0, \pm\mu, 0, \mp\mu)_\tau$	$(\pm 1, \mp\mu, 0, \mp\mu)_\tau$	5	4

(Case 2) $\ell = 6$.

We convert $(e_{\ell-1}, \ldots, e_{\ell-6})_\tau$ into $(e'_{\ell'-1}, \ldots, e'_{\ell-6})_\tau$ using Table 2 (*double signs are taken in the same order*).

(Case 3) $\ell \geq 7$.

(i) $(e_{\ell-1}, \ldots, e_{\ell-7})_\tau = (\pm\mu, 0, \pm\mu, 0, 0, 0, \mp\mu)_\tau$.
$e_i = e'_i$ for all $i \leq \ell - 8$, $\ell' = \ell - 3$, and we convert $(e_{\ell-1}, \ldots, e_{\ell-7})_\tau = (\pm\mu, 0, \pm\mu, 0, 0, 0, \mp\mu)_\tau$ into $(e'_{\ell'-1}, \ldots, e'_{\ell-7})_\tau = (\mp 1, 0, \pm 1, \pm\mu)$.

(ii) $(e_{\ell-1}, \ldots, e_{\ell-7})_\tau = (\pm\mu, 0, \pm\mu, 0, \mp\mu, 0, \mp\mu)_\tau$.
$e_i = e'_i$ for all $i \leq \ell - 8$, $\ell' = \ell - 3$, and we convert $(e_{\ell-1}, \ldots, e_{\ell-7})_\tau = (\pm\mu, 0, \pm\mu, 0, \mp\mu, 0, \mp\mu)_\tau$ into $(e'_{\ell'-1}, \ldots, e'_{\ell-7})_\tau = (\mp 1, \mp\mu, \pm 1, \pm\mu)$.

(iii) $(e_{\ell-1}, \ldots, e_{\ell-7})_\tau \neq (\pm\mu, 0, \pm\mu, 0, 0, 0, \mp\mu)_\tau$ and $(\pm\mu, 0, \pm\mu, 0, \mp\mu, 0, \mp\mu)_\tau$.
$e_i = e'_i$ for all $i \leq \ell - 7$ and we convert $(e_{\ell-1}, \ldots, e_{\ell-6})_\tau$ into $(e'_{\ell'-1}, \ldots, e'_{\ell-6})_\tau$ using Table 2.

Then, except for the cases that $(e_{\ell-1}, \ldots, e_{\ell-6})_\tau = (\mu, 0, \mu, 0, \mu, 0)_\tau$ and $(e_{\ell-1}, \ldots, e_{\ell-6})_\tau = (-\mu, 0, -\mu, 0, -\mu, 0)_\tau$,

Table 2: Conversion of the τ-NAF into the τ-MLF ($\ell \geq 6$)

$(e_{\ell-1}, \ldots, e_{\ell-6})_\tau$	$(e'_{\ell'-1}, \ldots, e'_{\ell-6})_\tau$	ℓ'
$(\pm\mu, 0, 0, 0, 0, 0)_\tau$	$(\pm\mu, 0, 0, 0, 0, 0)_\tau$	ℓ
$(\pm\mu, 0, 0, 0, 0, \pm\mu)_\tau$	$(\pm\mu, 0, 0, 0, 0, \pm\mu)_\tau$	ℓ
$(\pm\mu, 0, 0, 0, 0, \mp\mu)_\tau$	$(\pm\mu, 0, 0, 0, 0, \mp\mu)_\tau$	ℓ
$(\pm\mu, 0, 0, 0, \pm\mu, 0)_\tau$	$(\pm\mu, 0, 0, 0, \pm\mu, 0)_\tau$	ℓ
$(\pm\mu, 0, 0, 0, \mp\mu, 0)_\tau$	$(\pm\mu, 0, 0, 0, \mp\mu, 0)_\tau$	ℓ
$(\pm\mu, 0, 0, \pm 1, 0, 0)_\tau$	$(\mp\mu, \mp 1, 0, 0)_\tau$	$\ell - 2$
$(\pm\mu, 0, 0, \pm 1, 0, \pm 1)_\tau$	$(\mp\mu, \mp 1, 0, \pm 1)_\tau$	$\ell - 2$
$(\pm\mu, 0, 0, \pm 1, 0, \mp 1)_\tau$	$(\mp 1, \pm\mu, \pm 1)_\tau$	$\ell - 3$
$(\pm\mu, 0, 0, \mp 1, 0, 0)_\tau$	$(\pm\mu, 0, 0, \mp 1, 0, 0)_\tau$	ℓ
$(\pm\mu, 0, 0, \mp 1, 0, \pm 1)_\tau$	$(\pm\mu, 0, 0, \mp 1, 0, \pm 1)_\tau$	ℓ
$(\pm\mu, 0, 0, \mp 1, 0, \mp 1)_\tau$	$(\pm\mu, 0, 0, \mp 1, 0, \mp 1)_\tau$	ℓ
$(\pm\mu, 0, \pm\mu, 0, 0, 0)_\tau$	$(\pm 1, \mp\mu, 0, 0, 0)_\tau$	$\ell - 1$
$(\pm\mu, 0, \pm\mu, 0, 0, \pm 1)_\tau$	$(\pm 1, \mp\mu, 0, 0, \pm 1)_\tau$	$\ell - 1$
$(\pm\mu, 0, \pm\mu, 0, 0, \mp 1)_\tau$	$(\mp 1, \mp\mu, \pm 1)_\tau$	$\ell - 3$
$(\pm\mu, 0, \pm\mu, 0, \pm\mu, 0)_\tau$	$(\mp\mu, \mp 1, \pm\mu, 0)_\tau$	$\ell - 2$
$(\pm\mu, 0, \pm\mu, 0, \mp\mu, 0)_\tau$	$(\pm 1, \mp\mu, 0, \mp\mu, 0)_\tau$	$\ell - 1$
$(\pm\mu, 0, \mp\mu, 0, 0, 0)_\tau$	$(\pm\mu, 0, \mp\mu, 0, 0, 0)_\tau$	ℓ
$(\pm\mu, 0, \mp\mu, 0, 0, \pm\mu)_\tau$	$(\pm\mu, 0, \mp\mu, 0, 0, \pm\mu)_\tau$	ℓ
$(\pm\mu, 0, \mp\mu, 0, 0, \mp\mu)_\tau$	$(\pm\mu, 0, \mp\mu, 0, 0, \mp\mu)_\tau$	ℓ
$(\pm\mu, 0, \mp\mu, 0, \pm\mu, 0)_\tau$	$(\pm\mu, 0, \mp\mu, 0, \pm\mu, 0)_\tau$	ℓ
$(\pm\mu, 0, \mp\mu, 0, \mp\mu, 0)_\tau$	$(\pm\mu, 0, \mp\mu, 0, \mp\mu, 0)_\tau$	ℓ

the τ-adic expansion $d = \sum_{i=0}^{\ell'-1} e'_i\tau^i$ is a minimal length τ-adic expansion with minimal Hamming weight. We call the τ-adic expansion $\sum_{i=0}^{\ell'-1} e'_i\tau^i$ ($e'_i \in \mathcal{D}$, $e'_{\ell'-1} \neq 0$) τ-adic minimal length form (τ-MLF for short).

Remark 1. As described in Corollary 1, if $(e_{\ell-1}, \ldots, e_{\ell-6})_\tau = (\pm\mu, 0, \pm\mu, 0, \pm\mu, 0)_\tau$, then the τ-adic expansion $d = \sum_{i=0}^{\ell'-1} e'_i\tau^i$ is not necessarily a minimal length τ-adic expansion with minimal Hamming weight.

For example, consider $d = -11\mu$. The τ-NAF of d is $(\mu, 0, \mu, 0, \mu, 0, \mu, 0, \mu)_\tau$ and $\ell = 9$. From Corollary 1, $\ell' = \ell - 2$ and the τ-MLF of d is $(-\mu, -1, \mu, 0, \mu, 0, \mu)_\tau$. However, minimal length τ-adic expansion with minimal Hamming weight of d is $(-1, 0, 1, \mu, -1, -\mu)_\tau$ and $\ell_{\min}(d) = \ell - 3$.

Another example is $d = 5\mu - 5$, where $\mu = -1$. The τ-NAF of d is $(\mu, 0, \mu, 0, -\mu, 0, 0, -1)_\tau$ and $\ell = 8$. From Corollary 1, $\ell' = \ell - 2$ and the τ-MLF of d is $(-\mu, -1, \mu, 0, 0, -1)_\tau$. However, minimal length τ-adic expansion with minimal Hamming weight of d is $(-1, 0, 1, \mu, -1)_\tau$ and $\ell_{\min}(d) = \ell - 3$. These issues remain to be discussed.

7. Conclusion

In this paper, we derived an explicit lower bound for the length of minimal Hamming weight τ-adic expansions. We also gave a new proof of the minimality of the Hamming weight of the τ-NAF on Koblitz curves. Further, by using the proof of the lower bound and the new proof of the minimality of the Hamming weight of the τ-NAF, we classified a minimal length τ-adic expansion with minimal

Hamming weight except for two special cases. The classification shows that the τ-NAF has *almost* minimal length among all τ-adic expansions of minimal Hamming weight and we can easily convert the τ-NAF into a minimal length τ-adic expansion without changing the Hamming weight.

Acknowledgments

The authors would like to thank anonymous reviewers for their careful reading and very helpful comments on earlier versions of this manuscript.

References

[1] Avanzi, R.M., Heuberger, C., and Prodinger, H.: Minimality of the Hamming Weight of the τ-NAF for Koblitz Curves and Improved Combination with Point Halving, in: *the 12th International Workshop on Selected Areas in Cryptography, SAC 2005*, Vol.3897 of Lecture Notes in Computer Science (2006), Springer-Verlag, 332–344.

[2] Avanzi, R.M., Heuberger, C., and Prodinger, H.: On Redundant τ-adic Expansions and Non-Adjacent Digit Sets, in: *the 13th International Workshop on Selected Areas in Cryptography, SAC 2006*, Vol.4356 of Lecture Notes in Computer Science (2007), Springer-Verlag, 285–301.

[3] Avanzi, R.M., Heuberger, C., and Prodinger, H.: Scalar Multiplication on Koblitz Curves Using the Frobenius Endomorphism and Its Combination with Point Halving: Extensions and Mathematical Analysis, in: *Algorithmica* Vol.46, No.3-4 (2006), 249–270.

[4] Avanzi, R.M., Heuberger, C., and Prodinger, H.: Redundant τ-adic Expansions I: Non-Adjacent Digit Sets and their Applications to Scalar Multiplication, Cryptology ePrint Archive, Report 2008/148, 2008. Available at `http://eprint.iacr.org/2008/148`

[5] Avoine, G., Monnerat, J., and Peyrin, T.: Advances in Alternative Non-adjacent Form Representations, in: *Progress in Cryptology - INDOCRYPT 2004, the 5th International Conference on Cryptology in India*, Vol.3348 of Lecture Notes in Computer Science (2004), Springer-Verlag, 260–274.

[6] Blake, I.F., Murty, V.K., and Xu, G.: Nonadjacent radix-τ Expansions of Integers in Euclidean Imaginary Quadratic Number Fields, in: *Canadian Journal of Mathematics*, Vol.60, No.6 (2008), 1267–1282.

[7] Bosma, W.: Signed Bits and Fast Exponentiation, in: *Journal de Théorie des Nombres de Bordeaux*, Vol.13, No.1 (2001), 27–41.

[8] Standards for Efficient Cryptography Group, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000. Available at `http://www.secg.org`

[9] Clark, W.E. and Liang, J.J.: On arithmetic weight for a general radix representation of integers, in: *IEEE Transactions on Information Theory*, Vol.19, No.6 (1973), 823–826.

[10] Gallant, R., Lambert, R., and Vanstone, S.: Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms, in: *Advances in Cryptology - CRYPTO 2001*, Vol.2139 of Lecture Notes in Computer Science (2001), Springer-Verlag, 190–200.

[11] Heuberger, C.: Redundant τ-adic Expansions II: Non-Optimality and Chaotic Behaviour, Cryptology ePrint Archive, Report 2008/153, 2008. Available at `http://eprint.iacr.org/2008/153`

[12] Hakuta, K., Sato, H., and Takagi, T.: Efficient Arithmetic on Subfield Elliptic Curves Over Small Finite Fields of Odd Characteristic, in: *the 4th Information Security Practice and Experience Conference, ISPEC 2008*, Vol.4991 of Lecture Notes in Computer Science (2008), Springer-Verlag, 304–318.

[13] Koblitz, N.: Elliptic curve cryptosystems, in: *Mathematics of Computation*, Vol.48, No.177 (1987), 203–209.

[14] Koblitz, N.: CM-curves with good cryptographic properties, in: *Advances in Cryptology - CRYPTO 1991*, Vol.576 of Lecture Notes in Computer Science (1992), Springer-Verlag, 279–287.

[15] Miller, V.: Uses of elliptic curves in cryptography, in: *Advances in Cryptology - CRYPTO 1985*, Vol.218 of Lecture Notes in Computer Science (1986), Springer-Verlag, 417–426.

[16] Morain, F. and Olivos, F.: Speeding up the Computations on An Elliptic Curve Using Addition-Subtraction Chains, in: *Theoretical Informatics and Applications*, Vol.24, No.6 (1990), 531–543.

[17] Miyaji, A., Ono, T., and Cohen, H.: Efficient elliptic curve exponentiation, in: *the 1st International Conference on Information and Communication Security, ICICS 1997*, Vol.1334 of Lecture Notes in Computer Science (1997), Springer-Verlag, 282–290.

[18] Muir, J.A. and Stinson, D.R.: Alternative Digit Sets for Nonadjacent Representations, in: *SIAM Journal on Discrete Mathematics*, Vol.19, No.1 (2005), 165–191.

[19] Muir, J.A. and Stinson, D.R.: Minimality and Other Properties of the width-w Nonadjacent Form, in: *Mathematics of Computation*, Vol.75, No.253 (2006), 369–384.

[20] Müller, V.: Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two, in: *Journal of Cryptology*, Vol.11, No.4 (1998), 219–234.

[21] National Institute of Standards and Technology, Recommendation for Key Management – Part 1: General (Revised), Special Publication 800-57, March 2007. Available at `http://csrc.nist.gov/publications/PubsSPs.html`

[22] Park, T.J., Lee, M.K., and Park, K.: New Frobenius Expansions for Elliptic Curves with Efficient Endomorphisms, in: *the 5th International Conference on Information Security and Cryptology, ICISC 2002*, Vol.2587 of Lecture Notes in Computer Science (2003), Springer-Verlag, 264–282.

[23] Reitwiesner, G.W.: Binary Arithmetic, in: *Advances in Computers*, Vol.1 (1960), 231–308.

[24] Rivest, R., Shamir, A., and Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, in: *Communications of the ACM*, Vol.21, No.2 (1978), 120–126.

[25] Silverman, J.H.: *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.

[26] Smart, N.P.: Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic, in: *Journal of Cryptology*, Vol.12, No.2 (1999), 141–151.

[27] Solinas, J.A.: Efficient Arithmetic on Koblitz Curves, in: *Designs, Codes and Cryptography*, Vol.19, No.2-3 (2000), 195–249.

[28] Takagi, T., Yen, S.M., and Wu, B.C.: Radix-r Non-adjacent Form, in: *the 7th International Information Security Conference, ISC 2004*, Vol.3225 of Lecture Notes in Computer Science (2004), Springer-Verlag, 99–110.

Keisuke Hakuta
Hitachi, Ltd., Systems Development Laboratory, 292, Yoshida-cho, Totsuka-ku, Yokohama, 244-0817, Japan.
E-mail: keisuke.hakuta.cw(at)hitachi.com

Hisayoshi Sato
Hitachi, Ltd., Systems Development Laboratory, 292, Yoshida-cho, Totsuka-ku, Yokohama, 244-0817, Japan.
E-mail: hisayoshi.sato.th(at)hitachi.com

Tsuyoshi Takagi
School of Systems Information Science, Future University Hakodate, 116-2, Kamedanakano-cho, Hakodate, 041-8655, Japan.
E-mail: takagi(at)fun.ac.jp