A Note on Signed Binary Window Algorithm for Elliptic Curve Cryptosystems

Fanyu Kong and Daxing Li

Institute of Network Security, Shandong University, Shanda Nanlu Road, Jinan 250100, Shandong, R.P. China
phd_kong@yahoo.com, lidaxing@vip.sina.com

Abstract. The window algorithms for various signed binary representations have been used to speed up point multiplication on elliptic curves. While there's been extensive research on the non-adjacent form, little attention has been devoted to non-sparse optimal signed binary representations. In the paper, we prove some properties of non-sparse optimal signed binary representations and present a precise analysis of the non-sparse signed window algorithm. The main contributions are described as follows. Firstly, we attain the lower bound $k+1/3$ of the expected length of non-sparse optimal signed binary representations of k-bit positive integers. Secondly, we propose a new non-sparse signed window partitioning algorithm. Finally, we analyze Koyama-Tsuruoka's non-sparse signed window algorithm and the proposed algorithm and compare them with other methods. The upper bound $\frac{5}{6} \cdot 2^{w-1} - 1 + \frac{(-1)^w}{3}$ of the number of precomputed windows of the non-sparse signed window algorithms is attained.

Keywords: elliptic curve cryptosystems, point multiplication, signed window algorithm, signed-digit number representations.

1 Introduction

Elliptic Curve Cryptosystems, as introduced by Koblitz [1] and Miller [2], are based on the intractability of the discrete logarithm problem on elliptic curves. The fundamental operation on elliptic curves is point multiplication, which is an analogous operation as exponentiations on multiplicative groups. Hence, the binary algorithm, the m-ary algorithm and the sliding window algorithm [3–7] for exponentiations can be applied to point multiplication on elliptic curves.

Fortunately, a significant property of elliptic curve cryptosystems is that the inverse of a point can be computed essentially for free. Therefore, signed binary representations of an integer n, as introduced by Booth [8] and Reitwiesner [9], can be used to speed up point multiplication. In 1990, Morain and Olivos [10] firstly suggested to apply the non-adjacent form (NAF) to construct the addition-subtraction chain for point multiplication, which can save 11.11% operations compared to the binary algorithm. Furthermore, at Crypto'1992, Koyama and Tsuruoka [11] proposed a signed binary window algorithm for a non-sparse

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 223–235, 2005.

optimal signed binary representation (called the KT recoding), which requires fewer operations by using the sliding window method.

In [11], the KT recoding was considered better than the NAF with respect to window technique since that the former has a larger average zero-run length. However, it was noted in [12, 13] that in comparing various signed binary window algorithms, it is important to take into account the number of the precomputations. By far, in the previous literature [11-13, 21] the number of precomputed windows of Koyama-Tsuruoka's signed window algorithm [11] is counted by $2^{w-1}-1$. It is still a problem what is the precise number of precomputed windows of the non-sparse signed window algorithm.

Note that an efficient sliding window technique, known as the width-w nonadjacent form (w-NAF), was independently introduced by Miyaji, Ono and Cohen [14] and Solinas [15]. Some properties of the w-NAF have be extensively discussed in [16, 17, 18]. Recently, much attention has been devoted to left-to-right w-NAF recodings. Joye and Yen [19] first developed a left-to-right NAF recoding algorithm. Some left-to-right recodings with the same weight as the w-NAF ($w > 2$), are respectively proposed by Avanzi [20], by Okeya et al. [21], and by Muir and Stinson [22]. Furthermore, Möller [23, 24] introduced the fractional window method, which can provide more flexibility in order to make best use of the memory that is available.

In this paper, we propose some properties of non-sparse optimal signed binary representations and make a precise analysis of the non-sparse signed binary window algorithm. Firstly, we prove the lower bound $k+1/3$ of the expected length of non-sparse optimal signed binary representations. Secondly, we propose a new non-sparse signed window partitioning algorithm, which is slightly better than Koyama-Tsuruoka's algorithm practically for the window width $w = 4, 5, 6, 7$. Finally, we analyze the two non-sparse signed window algorithms, i.e. Koyama-Tsuruoka's algorithm and the proposed algorithm, and prove the upper bound $\frac{5}{6} \cdot 2^{w-1} - 1 + \frac{(-1)^w}{3}$ of the number of precomputed windows. Furthermore, we give a comparison of various algorithms based on signed binary representations including the w-NAF and the fractional window method.

The rest of this paper is organized as follows. Section 2 reviews signed binary representations. Section 3 proves some properties of non-sparse optimal signed binary representations of positive integers. Section 4 proposes a new non-sparse signed window algorithm. Section 5 analyzes Koyama-Tsuruoka's algorithm and the proposed algorithm and compare them with other algorithms, such as the w-NAF and so on. Finally, Section 6 concludes the paper.

2 Background

2.1 Notation

If an integer $n = \sum_{i=0}^{k-1} n_i 2^i$ with $n_i \in \{0, 1\}$, we call $(n_{k-1}, \ldots, n_1, n_0)_2$ the binary representation of n. In a signed-digit number system, if $n = \sum_{i=0}^{k} n'_i 2^i$ with $n'_i \in \{\overline{1}, 0, 1\}$, we call $(n'_k, \ldots, n'_1, n'_0)_2$ a signed binary representation of n. Moreover, let $\overline{1}$ denote -1 for convenience.

2.2 Signed Binary Representations

A signed binary representation $\left(n'_{k-1}, \ldots, n'_1, n'_0\right)_2$ is called an optimal signed binary representation of n, if its hamming weight (the number of non-zero digits) is minimal among all the signed binary representations. One of the most important optimal signed binary representations is the non-adjacent form (NAF). Some properties of signed binary representations have be presented in the literature [8, 9, 25-31]. We now give some required definitions and results.

Definition 1. *[9] A signed binary representation* $\left(n'_{k-1}, \ldots, n'_1, n'_0\right)_2$ *with no two adjacent digits being both non-zero is variously called the canonical, sparse or non-adjacent form (NAF), which satisfies* $n'_i \cdot n'_{i+1} = 0$ *for all* $0 \leq i \leq k-1$.

Property 1. [9, 25, 26, 27] The NAF has the following properties:

(1) Every integer n has a unique NAF.
(2) The NAF is an optimal signed-digit binary representation.
(3) For any integers n, the length of the NAF of n is at most one digit larger than that of the binary representation of n.

Lemma 1. *[29, 32] The probability that in an NAF the digit immediately to the left of a* 0 *is another* 0 *is* 1/2 *and that it is* 1 *or* -1 *is in each case* 1/4.

Let T_k denote the number of integers requiring at most k bits in the NAF representations. Let T'_k denote the number of integers requiring exactly k bits in the NAF representations. Let T''_k denote the number of positive integers requiring exactly k bits in the NAF representations.

Theorem 1. *[27, 29]*

$$T_k = (2^{k+2}+(-1)^{k+1})/3, \quad T'_k = (2^{k+1}+(-1)^{k+1}\cdot 2)/3, \quad T''_k = (2^k+(-1)^{k+1})/3$$

Various optimal signed binary representations can be obtained. Optimal signed binary representations other than the NAF are called non-sparse optimal signed binary representations. For example, the binary representation of the integer $n = 413$ is $(110011101)_2$. The NAF representation is $(10\overline{1}0100\overline{1}01)_2$ and a non-sparse optimal signed-digit representation is $(1101000\overline{11})_2$.

3 Properties of Non-sparse Optimal Signed Binary Representations

While there's been extensive research on the properties of the NAF, little attention has been devoted to non-sparse optimal signed binary representations. Now we propose two theorems on the lengths of non-sparse optimal signed binary representations, which can be applied to the analysis of the non-sparse signed window algorithm.

Note that the NAF representation can be converted into a non-sparse optimal signed-digit representation by replacing '$10\overline{1}$' and '$\overline{1}01$' with '011' and '$0\overline{11}$'.

Hence, we can derive the expected length of non-sparse optimal signed binary representations by counting the corresponding NAF representations. According to the property of the NAF, the length of the corresponding NAF of a k-bit positive integer is k or $k+1$ bits. In fact, the NAF representations of the exactly k-bit positive integers consist of three cases:

(1) the k-bit NAF representations.
(2) the $(k+1)$-bit NAF representations, which have the leading digits '$10\overline{1}0$'.
(3) the $(k+1)$-bit NAF representations, which have the leading digits other than '$10\overline{1}0$'.

Lemma 2. *If the leading digits of $(k+1)$-bit NAF representations of an integer n are '$10\overline{1}0$',the length of the binary representation of n is k bits.*

Proof. According to the property of the NAF, the NAF representation of an integer n is unique and the $(k+1)$-bit NAF representation has a corresponding k-bit or $(k+1)$-bit binary representation. Since that the leading digits of the $(k+1)$-bit NAF representation of n are '$10\overline{1}0$', we have

$$n = 2^k + (-1) \times 2^{k-2} + \sum_{i=0}^{k-4} n_i' 2^i, \qquad n_i' \in \{\overline{1}, 0, 1\}$$

Since $2^{k-2} > \sum_{i=0}^{k-4} n_i' 2^i$, we can obtain $n < 2^k$. Hence the integer n must be a k-bit binary integer. □

Theorem 2. *For the exactly k-bit positive integers:*

(1) the number of the k-bit NAF representations is $C_k = 2^{k-1}/3 + 1/2 + (-1)^{k+1}/6$.
(2) the number of the $(k+1)$-bit NAF representations, which have the leading digits '$10\overline{1}0$', is $C_k' = (2^{k-1} + (-1)^k)/3$.
(3) the number of the $(k+1)$-bit NAF representations, which have the leading digits other than '$10\overline{1}0$', is $C_k'' = 2^{k-1}/3 - 1/2 + (-1)^{k+1}/6$.

Proof. First consider the second case. When the leading digits of the $(k+1)$-bit NAF representations are '$10\overline{1}0$', the remaining bit string can be any of the $(k-3)$-bit NAF representations. By Theorem 1, the number of the $(k-3)$-bit NAF representations is $T_{k-3} = (2^{k-1} + (-1)^k)/3$. Hence, we obtain $C_k' = (2^{k-1} + (-1)^k)/3$.

Let C_k denote the number of the k-bit NAF representations of the exactly k-bit positive integers and C_k'' denote the number of the $(k+1)$-bit NAF representations of the exactly k-bit positive integers, which have the leading digits other than '$10\overline{1}0$'. Hence we have

$$\begin{cases} C_k + C_k' + C_k'' = 2^{k-1} \\ C_k + C_{k-1}' + C_{k-1}'' = T_k'' \end{cases} \tag{1}$$

By solving the above equation (1), we obtain $C_k = 2^{k-1}/3 + 1/2 + (-1)^{k+1}/6$ and $C_k'' = 2^{k-1}/3 - 1/2 + (-1)^{k+1}/6$. □

Theorem 3. *For the exactly k-bit positive integers, the lower bound of the expected length of the non-sparse optimal signed binary representations is $k + 1/3$ and the upper bound is $k + 2/3$.*

Proof. Note that a non-sparse optimal signed binary representation can be obtained by replacing '$10\overline{1}$' and '$\overline{1}01$' with '011' and '$0\overline{11}$' from the NAF representation. Moreover, only the conversion from '$10\overline{1}0$' to '0110' of the most significant digits of the $(k+1)$-bit NAF representations can reduce the length by 1. Hence the expected length of the shortest non-sparse optimal signed binary representation is $k + C''_k/2^{k-1}$, which is approximately $k+1/3$.

Similarly, the expected length of the longest non-sparse optimal signed binary representation of the exactly k-bit positive integers is approximately $k+2/3$, which is equal to the expected length of the NAF representation. □

4 New Non-sparse Signed Window Partitioning Algorithm

Koyama and Tsuruoka [11] proposed a signed window algorithm based on the KT recoding, which is a non-sparse optimal signed binary representation. The KT recoding allows a few adjacent non-zeros, which can reduce the number of the non-zero windows. Before the analysis of the non-sparse signed window algorithm, we propose a new signed window partitioning algorithm, which can obtain non-sparse signed windows by scanning the NAF representation. The basic idea is converting the most significant digits '$10\overline{1}$' or '$\overline{1}01$' of a window into '011' or '$0\overline{11}$', which increases the window length by 1. The proposed method is described as Algorithm 1.

Note that for w=3, the proposed Algorithm 1, Koyama-Tsuruoka's signed window algorithm [11] and the window algorithm for the NAF [29, 32] have the same expected zero-run length 1.5 and are indeed equivalent. For $w \geq 4$, we obtain the following Theorem 4.

Theorem 4. *For a k-bit NAF representation and the window width $w \geq 4$, the expected number of non-zero windows of Algorithm 1 is*

$$\frac{k}{w + \frac{4}{3} + \frac{(-1)^w}{3 \cdot 2^{w-1}} - (\frac{1}{2})^{w-3} + (2 + (-1)^w) \cdot (\frac{1}{2})^{\frac{w}{2} - \frac{3}{4} \cdot (1 - (-1)^w)}}.$$

Proof. The window partitioning process in Algorithm 1 can be modeled as a Markov chain, whose states are the different possible windows. In [32], Semay analyzed the the sliding window algorithm for the NAF representation. Since Algorithm 1 outputs the non-sparse signed windows by scanning the NAF, we adopt a similar analysis as that in [32]. Let i be the number of the non-zero digits of a width-w window for the NAF representation. Let $\star$ denote a non-zero digit 1 or $\overline{1}$. For $w \geq 4$, the different windows (states) are:

Algorithm 1. New signed window partitioning algorithm

Input: the NAF $n = \sum_{i=0}^{k} n_i 2^i$, $n_i \in \{\overline{1}, 0, 1\}, 0 \le i \le k$, the window width $w \ge 3$.
Output: the windows $W_1, W_2, \ldots, W_r$.

1. $j := 1$;
2. $i := k$;
3. while $i \ge 0$ do
4. if $n_i = 0$ then
5. $W_j := 0$;
6. $j := j + 1$;
7. $i := i - 1$;
8. else if $(n_i, \ldots, n_{i-w+1}) = (1, 0, \overline{1}, \ldots)$ or $(\overline{1}, 0, 1, \ldots)$ then

/* For $i - w + 1 < 0$, take $(n_i, \ldots, n_0)$. Similarly, so do Step 9 and 13. */

9. $W_j := (0, 1, 1, n_{i-3}, \ldots, n_{i-w})$ or $(0, \overline{1}, \overline{1}, n_{i-3}, \ldots, n_{i-w})$;
10. $j := j + 1$;
11. $i := i - w - 1$;
12. else
13. $W_j = (n_i, \ldots, n_{i-w+1})$;
14. $j := j + 1$;
15. $i := i - w$;
16. end if.
17. end while.

$i = 0$	$S_1 = 0$	
$i = 1$	$S_2 = \star 0 \ldots 0$	(length w)
$i = 2$	$S_3 = \star 0 \ldots 0 \star$	(length w)
	$S'_4 = 1010 \ldots 0$ or $\overline{1}0\overline{1}0 \ldots 0$	(length w)
	$S''_4 = 10\overline{1}0 \ldots 0$ or $\overline{1}010 \ldots 0$	(length $w+1$)
	$S'''_4 = 10\overline{1}0 \ldots 0\star$ or $\overline{1}010 \ldots 0\star$	(length $w+1$)
	$S''''_4 = \star 0 \ldots 0 \star 0 \ldots 0$	(length w)
...		
$3 \le i \le \lfloor \frac{w+1}{2} \rfloor$	$S'_{2i-1} = 1010(0\|\star 0)^* \star$ or $\overline{1}0\overline{1}0(0\|\star 0)^*\star$	(length w)
	$S''_{2i-1} = 10\overline{1}0(0\|\star 0)^* \star 0$ or $\overline{1}010(0\|\star 0)^* \star 0$	(length $w+1$)
	$S'''_{2i-1} = \star 00(0\|\star 0)^*\star$	(length w)
	(When $w = 2i-1, S'''_w$ is not included.)	
	$S'_{2i} = 1010(0\|\star 0)^*$ or $\overline{1}0\overline{1}0(0\|\star 0)^*$	(length w)
	$S''_{2i} = 10\overline{1}0(0\|\star 0)^*0$ or $\overline{1}010(0\|\star 0)^*0$	(length $w+1$)
	$S'''_{2i} = 10\overline{1}0(0\|\star 0)^* \star$ or $\overline{1}010(0\|\star 0)^*\star$	(length $w+1$)
	$S''''_{2i} = \star 00(0\|\star 0)^*$	(length w)
	(When $w = 2i, S''''_w$ is not included.)	

Note that the states S'_{2i-1},S''_{2i-1} and S'''_{2i-1} correspond to the state S_{2i-1} in [32] and the states S'_{2i}, S''_{2i}, S'''_{2i} and S''''_{2i} correspond to the state S_{2i} in [32]. By a similar analysis as that in [32], we can calculate the stationary distribution of the Markov chain, which is $(\pi_1, \pi_2, \pi_3, \ldots, \pi'_w, \pi''_w, \pi''_w)$ for w odd and

$(\pi_1, \pi_2, \pi_3, \ldots, \pi'_w, \pi''_w, \pi'''_w)$ for w even. Let $f(w) = \frac{3}{7 \cdot 2^{w-1} + (-1)^w}$, then the probabilities are obtained as follows.

$$\pi_1 = f(w) \cdot (2^{w+1} + (-1)^w)/3, \qquad \pi_2 = \pi_3 = f(w) \cdot 2.$$

For $i \geq 2$:

$$\begin{aligned}
&\pi'_{2i} = f(w) \cdot 2^{i-1}, && \pi'_{2i+1} = f(w) \cdot 2^{i-1},\\
&\pi''_{2i} = f(w) \cdot 2^{i-2}, && \pi''_{2i+1} = f(w) \cdot 2^{i-1},\\
&\pi'''_{2i} = f(w) \cdot 2^{i-2}, && \pi'''_{2i+1} = f(w) \cdot \left[\tbinom{w-i-2}{i-1} - 1 \right] \cdot 2^i,\\
&\pi''''_{2i} = f(w) \cdot \left[\tbinom{w-i-1}{i-1} - 1 \right] \cdot 2^i.
\end{aligned}$$

The expected number of the non-zero windows is :

— For w odd:

$$\begin{aligned}
& k \cdot \frac{1 - \pi_1}{1 \cdot \pi_1 + w \cdot (1 - \pi_1) + \sum_{i=2}^{\frac{w-1}{2}} [f(w) \cdot 2^i]} \\
&= \frac{k}{w + \frac{4}{3} + \frac{(-1)^w}{3 \cdot 2^{w-1}} - (\frac{1}{2})^{w-3} + (\frac{1}{2})^{\frac{w-3}{2}}}
\end{aligned} \tag{2}$$

— For w even:

$$\begin{aligned}
& k \cdot \frac{1 - \pi_1}{1 \cdot \pi_1 + w \cdot (1 - \pi_1) + \sum_{i=2}^{\frac{w-2}{2}} [f(w) \cdot 2^i] + f(w) \cdot 2^{\frac{w}{2}-1}} \\
&= \frac{k}{w + \frac{4}{3} + \frac{(-1)^w}{3 \cdot 2^{w-1}} - (\frac{1}{2})^{w-3} + 3 \cdot (\frac{1}{2})^{\frac{w}{2}}}
\end{aligned} \tag{3}$$

Thus, by (2) and (3) we have the result

$$\frac{k}{w + \frac{4}{3} + \frac{(-1)^w}{3 \cdot 2^{w-1}} - (\frac{1}{2})^{w-3} + (2 + (-1)^w) \cdot (\frac{1}{2})^{\frac{w}{2} - \frac{3}{4} \cdot (1 - (-1)^w)}}. \tag{4}$$

□

According to Theorem 4, we obtain the average zero-run length of Algorithm 1 in Table 1.

Table 1. The Average Zero-run Length of Algorithm 1

width	w=3	w=4	w=5	w=6	w=7	w=8
length	1.5	1.625	1.5625	1.59375	1.515625	1.4921875

It is shown that the proposed algorithm is slightly better than Koyama-Tsuruoka's signed window algorithm [11] for $w = 4, 5, 6$ and 7, which cases are particularly attractive for elliptic curve cryptosystems.

5 Analysis and Comparisons

5.1 Analysis of Non-sparse Signed Window Algorithms

Now we analyze Koyama-Tsuruoka's signed window algorithm and the proposed Algorithm 1, which have the same upper bound of the number of precomputed windows. There are two problems on the analysis of Koyama-Tsuruoka's signed window algorithm in the literature [11–13]:

(1) In [11], the average length of the KT recoding is counted by $k + 1/4$. However, according to Theorem 3 in Section 3, the lower bound of the average length of the shortest non-sparse optimal signed binary representations is $k+1/3$. Therefore, the previous result is incorrect and we revise it.

(2) In [11–13], the number of precomputed windows for non-sparse signed window algorithm is counted by $2^{w-1} - 1$. However, we note that some window values can't appear in non-sparse optimal signed binary representations and needn't be precomputed. Hence there must be a upper bound smaller than $2^{w-1} - 1$ and the previous analysis is inaccurate.

Now we consider the second problem. The sliding algorithm for computing point multiplication $n \cdot P$ on elliptic curves is described as Algorithm 2. The overall number of operations includes the number of the precomputations, the number of the non-zero windows and the number of point doublings. Moreover, since the inverse of a point on elliptic curves is easily computed, only odd positive windows need be precomputed.

The overall number of operations of Koyama-Tsuruoka's signed window algorithm is $(k + 1.75 - w) + \frac{k+1/4}{w+1.5} + (2^{w-1} - 1)$ in [11, 13], where $k = \lfloor \log n \rfloor + 1$. Now we count the precise number of precomputed windows.

Algorithm 2. The sliding window algorithm for point multiplication $Q = n \cdot P$

Input: $n = \sum_{i=0}^{k} n_i' 2^i$, $n_i \in \{\overline{1}, 0, 1\}$, $0 \le i \le k$, a point P, the window width w.
Output: $Q = n \cdot P$.
1. Partition and precompute the left-to-right windows W_1,W_2,...,W_r .
2. $Q := W_1 P$;
3. for $i = 2$ to r do
3.1 $Q := 2^{L(W_i)} Q$;
3.2 $Q := Q + W_i \cdot P$;
4. end for.
5. Output Q.

Theorem 5. *For the window width $w \ge 2$, the sliding window algorithm for non-sparse optimal signed binary representations has:*

(1) The upper bound of the number of precomputed windows is $\frac{5}{6} \cdot 2^{w-1} - 1 + \frac{(-1)^w}{3}$.

(2)The maximum precomputed window is $\frac{5}{6} \cdot 2^w - \frac{1}{3}$ for w even, whose representation is $11(01)^{w/2-1}$ and $\frac{5}{6} \cdot 2^w - \frac{5}{3}$ for $w \ge 5$ and odd, whose representation

is $11(01)^{(w-1)/2-2}001$. *For* $w = 3$, *the maximum precomputed window is* 5, *whose representation is* 101.

Proof. Note that only odd positive windows of at most w bits need be precomputed. The number of precomputed windows of non-sparse optimal signed representations includes the number of precomputed windows of the NAF representation and the number of the $(k+1)$-bit NAF representations, which have the leading bits '$10\overline{1}0$'.

According to [29, 32], the number of precomputed windows of the NAF representation is $\frac{1}{3} \cdot 2^w - 1 - \frac{(-1)^w}{3}$.

By Theorem 2, for the exactly k-bit positive integers, the number of the $(k+1)$-bit NAF representations, which have the leading bits '$10\overline{1}0$', is $C'_k = (2^{k-1} + (-1)^k)/3$. Hence,we can obtain the number of the odd positive integers, which have the leading bits '$10\overline{1}0$' in their $(k+1)$-bit NAF representations, is $\frac{1}{6} \cdot 2^{w-1} + \frac{(-1)^w}{6} + \frac{(-1)^w}{2}$.

Therefore, the number of precomputed windows of the sliding window algorithm for non-sparse optimal signed binary representations has is $\frac{5}{6} \cdot 2^{w-1} - 1 + \frac{(-1)^w}{3}$. The results on the maximum precomputed window follows. □

Remark 1. Note that modified-NAF has been analyzed in [27]. In fact, the modified-NAF can be converted into non-sparse optimal signed binary representations by replacing some '$10\overline{1}$' or '$\overline{1}01$' with '011' or '$0\overline{11}$' and vice versa.

Let m is an odd positive integer such that $1 \leq m \leq 2^{w-1} - 3$ for the fractional w-NAF method by Möller [23,24]. We present the maximum precomputed window for various representations in Table 2. Taking $w = 5$ as an example, the maximum precomputed window for non-sparse optimal signed binary representations is 25, whose representation is $(11001)_2$. The representation $(11011)_2$, $(11101)_2$ and $(11111)_2$ of the odd positive integers 27, 29 and 31 can't appear in non-sparse optimal signed binary representations.

Table 2. The Maximum Precomputed Window

Representation	w=2	w=3	w=4	w=5	w=6
Binary	$3=(11)_2$	$7=(111)_2$	$15=(1111)_2$	$31=(11111)_2$	$63=(111111)_2$
NAF	$1=(1)_2$	$5=(101)_2$	$9=(1001)_2$	$21=(10101)_2$	$41=(101001)_2$
Non-sparse	$3=(11)_2$	$5=(101)_2$	$13=(1101)_2$	$25=(11001)_2$	$53=(110101)_2$
w-NAF	$1=(1)_2$	$3=(11)_2$	$7=(111)_2$	$15=(1111)_2$	$31=(11111)_2$
Factional w-NAF	$1=(1)_2$	$4+m$	$8+m$	$16+m$	$32+m$

Theorem 6.
(1) The expected number of operations of Koyama-Tsuruoka's non-sparse signed window algorithm is:

$$(k - w + \frac{11}{6}) + \frac{k + 1/3}{w + 3/2} + \frac{5}{6} \cdot 2^{w-1} - 1 + \frac{(-1)^w}{3}.$$

(2) Let $s = \frac{4}{3} + \frac{(-1)^w}{3 \cdot 2^{w-1}} - (\frac{1}{2})^{w-3} + (2 + (-1)^w) \cdot (\frac{1}{2})^{\frac{w}{2} - \frac{3}{4} \cdot (1-(-1)^w)}$. *The expected number of operations of Algorithm 1 is:*

$$(k + \frac{1}{3} - w + s) + \frac{k + 1/3}{w + s} + \frac{5}{6} \cdot 2^{w-1} - 1 + \frac{(-1)^w}{3}$$

Proof. By Theorem 5, the number of precomputed windows is $\frac{5}{6} \cdot 2^{w-1} - 1 + \frac{(-1)^w}{3}$. By Theorem 3, the lower bound of the average length of non-sparse optimal signed-digit representations is $k + 1/3$. Due to the equation in the literature [12, 13, 28, 29], this result can be obtained. □

5.2 Comparisons with Other Algorithms

Let L denote the length of the signed or unsigned binary representation of n. Let s and t denote the average zero-run length and the number of precomputed windows. The number of the non-zero windows can be determined by $\frac{L}{w+s}$. Note that t precomputed windows $\{3P, 5P, 7P, \ldots, (2t+1)P\}$ can be obtained via the addition chain $P, 2P, 3P, 5P, 7P, \ldots, (2t+1)P$. Hence, the number of operations of the sliding window algorithm is counted by as follows [11-14, 28, 29]:

$$L - w + s + (\frac{L}{w + s} - 1) + (t + 1)$$

The expected zero-run length of the binary representation is 1. The expected zero-run length of the NAF representation is $\frac{4}{3} + \frac{(-1)^{w+1}}{3 \cdot 2^{w-2}}$ [12, 13, 28, 29, 32]. The expected zero-run length of the KT recoding [11] is 3/2. Note that the w-NAF should be seen as a width-$(w-1)$ window algorithm with the zero-run length 2.

Let m be an odd positive integer such that $1 \leq m \leq 2^{w-1} - 3$. The fractional w-NAF method has the signed fractional windows $\{\pm 1, \pm 3, \ldots, \pm(2^{w-1} + m)\}$ and the number of precomputed windows is $2^{w-2} - 1 + (m + 1)/2$ for $w \geq 3$. The average density of the fractional w-NAF method is $\frac{1}{w + \frac{m+1}{2^{w-1}+1}}$.

Therefore, we give a comparison of the non-zero density and the number of precomputed windows of various representations in Table 3. Note that m is an odd positive integer such that $1 \leq m \leq 2^{w-1} - 3$. It is shown that when $w \leq 5$, there is a difference not more than 2 between the NAF and non-sparse signed-digit representations.

For a signed window algorithm, there is an optimal window width w for k-bit integers, which minimizes the number of operations. When k varies from 160 to 600, the optimal window width w varies from 3 to 6. For example, for k=233, the binary method (double-and-addition) and the NAF method (double-and-addition/subtraction) require 347.5 and 309.5 operations, respectively. For k=233 and w=4, a comparison of various sliding window algorithms is given in Table 4.

It is shown in Table 4 that there is a small difference among the various signed window algorithms for $k = 233$. The w-NAF combined the fractional window method can achieve the best performance by choosing a proper m.

Table 3. The Non-zero Density and Number of Precomputed Windows

Representation	w=2	w=3	w=4	w=5	w=6
Binary	0.333(1)	0.250(3)	0.200(7)	0.167(15)	0.143(31)
NAF	0.333(0)	0.222(2)	0.190(4)	0.157(10)	0.137(20)
KT recoding	0.286(1)	0.222(2)	0.182(6)	0.154(12)	0.133(26)
Algorithm 1	0.333(0)	0.222(2)	0.178(6)	0.152(12)	0.132(26)
w-NAF	0.333(0)	0.250(1)	0.200(3)	0.167(7)	0.143(15)
Fractional w-NAF	0	1+(m+1)/2	3+(m+1)/2	7+(m+1)/2	15+(m+1)/2

Table 4. Comparison of Various Algorithms ($k = 233, w = 4$)

Algorithm	Precomputed	Number of Operations
Binary+Window	7	283.6
NAF+Window	4	278.5
KT's window	6	279.2
Algorithm 1	6	278.4
5-NAF	7	277.4
Fractional 4-NAF ($m = 5$)	6	278.36
Fractional 5-NAF ($m = 1$)	8	277.5

6 Conclusion

We present a precise analysis of Koyama-Tsuruoka's signed window algorithm and the new proposed non-sparse signed window algorithm. We also give comparisons of various algorithms and it is shown that the w-NAF combined the fractional window method is more efficient than the others. Furthermore, the properties of non-sparse signed binary representations can be applied to analyze the performance of various algorithms based on non-sparse signed binary representations.

Acknowledgments. The authors are very grateful to the anonymous referees for their valuable comments, corrections and suggestions, and for drawing the authors' attention to related work on the w-NAF and the fractional window method. The authors would also like to thank Ming Li for his interesting discussions on this paper.

References

1. N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203-209, 1987.
2. V. S. Miller, "Use of elliptic curve in cryptography," Advances in Cryptology - CRYPTO'85, LNCS 218, Springer-Verlag , pp. 417-426, 1986.
3. D. E. Knuth, The Art of Computer Programming, vol. 2: Seminumerical Algorithms, Addison-Wesley, 3rd edition, 1998.

4. H. Cohen, A Course in Computational Algebraic Number Theory, vol. 138 of Graduate Texts in Mathematics, Springer-Verlag, 1993.
5. C. K. Koc, "Analysis of sliding window techniques for exponentiation," Computers and Mathematics with Applications, 30(10), pp.17-24, 1995.
6. O. Rizzo, "On the complexity of the 2^k-ary and of the sliding window algorithms for fast exponentiation," Rivista di Matematica dell'Universitá di Parma. 7(3). 2004.
7. D. M. Gordon, "A Survey of Fast Exponentiation Methods," Journal of Algorithms, vol. 27 , pp. 129-146,1998.
8. A. D. Booth, "A Signed Binary Multiplication Technique," Q. J. Mech. Appl. Math., vol. 4, no. 2, pp. 236-240, 1951.
9. G. W. Reitwiesner, "Binary arithmetic," Advances in Computers, vol. 1, pp. 231-308, 1960.
10. F. Morain and J. Olivos, "Speeding up the computations on an elliptic curve using addition-subtraction chains," Theoretical Informatics and Applications, vol. 24, pp. 531-543, 1990.
11. K. Koyama and T. Tsuruoka, "Speeding up elliptic curve cryptosystems using a signed binary window method," Advances in Cryptology - CRYPTO'92, LNCS 740, Springer-Verlag , pp. 345-357, 1992.
12. N. Kunihiro and H. Yamamoto, "Window and extended window methods for addition-subtraction chain," IEICE Trans. on Fundamentals, vol.E81-A, no.1, pp. 72-81, Jan. 1998.
13. E. De Win, S. Mister, B. Preneel and M. Wiener, "On the Performance of Signature Schemes based on Elliptic Curves," Proc. of ANTS'98, Springer-Verlag, LNCS 1423, pp. 252-266, 1998.
14. A. Miyaji, T. Ono and H. Cohen, "Efficient elliptic curve exponentiation," In Proceedings ICICS'97, LNCS 1334, pp. 282-290, Springer-Verlag, 1997.
15. J. A. Solinas, "An improved algorithm for arithmetic on a family of elliptic curves," In Proceedings of CRYPTO '97, LNCS 1294, pp. 357-371, Springer-Verlag, 1997.
16. J. A. Solinas, "Efficient arithmetic on Koblitz curves," Designs, Codes and Cryptography, vol. 19 , pp. 195-249, 2000.
17. H. Cohen, "Analysis of the sliding window powering algorithm," J. of Cryptology, vol. 18, no.1, pp.63-76, 2005.
18. J. A. Muir and D. R. Stinson, "Minimality and Other Properties of the Width-w Nonadjacent Form," to appear in Mathematics of Computation. Available at: `http://www.ccsl.carleton.ca/~jamuir/papers/wNAF-revised-3.pdf`.
19. M. Joye, and S. M. Yen, "Optimal left-to-right binary signed-digit recoding," IEEE Trans. on Comp. 49 (7), pp. 740-748, 2000.
20. R. M. Avanzi, "A Note on the Signed Sliding Window Integer Recoding and a Left-to-Right Analogue," In: H. Handschuh and A. Hasan (Eds.): SAC 2004, LNCS 3357, pp. 130-143, Springer-Verlag, 2005.
21. Katsuyuki Okeya, Katja Schmidt-Samoa, Christian Spahn, Tsuyoshi Takagi, "Signed Binary Representations Revisited," CRYPTO 2004, LNCS 3152, pp. 123-139, Springer-Verlag, 2004.
22. J. A. Muir, and D. R. Stinson, "New Minimal Weight Representations for Left-to-Right Window Methods," CT-RSA 2005 ,Lecture Notes in Computer Science 3376, pp. 366-383, Springer-Verlag, 2005.
23. B. Möller, "Improved Techniques for Fast Exponentiation," Information Security and Cryptology - ICISC 2002, Lecture Notes in Computer Science 2587, pp. 298-312, Springer-Verlag, 2002.

24. B. Möller, "Fractional Windows Revisited: Improved Signed-Digit Representations for Efficient Exponentiation," Information Security and Cryptology - ICISC 2004, Lecture Notes in Computer Science 3506 , pp. 137-153, Springer-Verlag, 2005.
25. S. Arno and F. S. Wheeler, "Signed digit representations of minimal hamming weight," IEEE Transactions on Computers, vol. 42, no. 8, pp. 1007-1010, 1993.
26. O. Egecioglu and C. K. Koc, "Exponentiation using canonical recoding," Theoretical Computer Science, 129(2), pp. 407-417, 1994.
27. W. Bosma, "Signed Bits and Fast Exponentiation," J. Théor. Nombres Bordeaux, 13(1), pp. 27-41, 2001.
28. R. M. Avanzi, "On multi-exponentiation in cryptography," Technical Report 2002/154, Cryptology ePrint Archive(2002), Available at: `http://eprint.iacr.org/2002/154`.
29. R. M. Avanzi, "On the complexity of certain multi-exponentiation techniques in cryptography," J. of Cryptology, Online First, 2005.
30. Clemens Heuberger and Peter Grabner, "On the number of optimal base 2 representations of integers," Preprint available at: `http://www.opt.math.tu-graz.ac.at/~cheub/publications`.
31. B. Phillips and N. Burgess, "Minimal Weight Digit Set Conversions," IEEE Transactions on Computers, vol.53, no.6, pp. 666-677, 2004.
32. Olivier Semay, "Efficiency analysis of window methods using Markov chains," Diplomarbeit, Sommer 2004. Available at: `http://www.cdc.informatik.tu-darmstadt.de/reports/reports/KP/Olivier_ Semay.diplom.ps`.