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.