Computers and Electrical Engineering 35 (2009) 150–158

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

New left-to-right minimal weight signed-digit radix-*r* representation

Baodong Qin [a,*], Ming Li [b,c], Fanyu Kong [b,c], Daxing Li [b,c]

[a] College of Computer Science and Technology, Southwest University of Science and Technology, 59 Qinglong Road, Mianyang 621010, Sichuan, PR China
[b] Institute of Network Security, Shandong University, 27 Shanda Nanlu Road, Jinan 250100, Shandong, PR China
[c] Key Laboratory of Cryptographic Technology and Information Security, 27 Shanda Nanlu Road, Jinan 250100, Shandong, PR China

ARTICLE INFO

Article history:
Received 4 January 2008
Accepted 18 September 2008
Available online 13 November 2008

Keywords:
Non-adjacent form
Left-to-right recoding
Integer recoding
Pairing based cryptosystems
Signed radix-*r* representation

ABSTRACT

Recently, signed-digit radix-*r* ($r \geqslant 2$) representation is used to speed up the scalar multiplication of pairing based cryptosystems. One such representation is *wr*NAF proposed by Takagi et al. at the international conference on information security 2004 (ISC 2004). This representation is obtained from right to left. In this paper, we present a new signed-digit radix-*r* representation with the same average weight, that is $\frac{r-1}{w(r-1)+1}$ as the *wr*NAF. The new representation uses the same digits as the *wr*NAF but has the advantage that it can be deduced using a left-to-right algorithm. Further, we show that like the *wr*NAF, the new representation has a minimal number of non-zero digits. Interleaved with the left-to-right scalar multiplication, the new representation can reduce both the time and space complexity of the computation compared to the right-to-left *wr*NAF.

1. Introduction

Pairing based cryptosystems [13] such as the ID-based cryptosystems or short signature schemes have recently been used for applications in cryptography. The basic operations of pairing based cryptosystems are scalar multiplication kP and bilinear pairing computation $e(P,Q)$, where k is an integer scalar and P,Q are points on an elliptic curve. In order to efficiently perform these two operations, Barreto et al. [4] and Galbraith et al. [10] showed efficient algorithms over supersingular elliptic curves with characteristic three. Several efficient arithmetic of elliptic curves over finite fields of characteristic three have been investigated [5,12,26,28].

Duursma [9] and Barreto [3] proposed two efficient algorithms for computing Tate pairing over hyperelliptic curves with characteristic *r*. Thus, the signed radix-*r* representations which have minimal number of non-zero digits have been widely used for the efficient implementation of pairing based cryptosystems. One of these representations is GNAF [7], using the digits $D = \{0, \pm 1, \cdots, \pm(r-1)\}$, another is *wr*NAF [29], using the digits $D_w = \{0, \pm 1, \ldots, \pm\lfloor \frac{r^w-1}{2} \rfloor\} \setminus \{\pm 1r, \pm 2r, \ldots, \pm\lfloor \frac{r^{w-1}-1}{2} \rfloor r\}$. However both of them are obtained from right to left, which means that it is necessary to finish the recoding and to store the recoding string additionally. An attractive problem at here is how to design left-to-right recoding algorithms, which can interleave with the left-to-right scalar multiplication.

The first left-to-right NAF analogues recoding algorithm was proposed by Joye and Yen [14]. Furthermore, some left-to-right analogues of the *w*NAF representations have been investigated [1,2,6,16,21,22,24,25]. For signed radix-*r* representation, Joye and Yen [15] proposed a minimal weight left-to-right analogue of the GNAF representation. Different from Joye and Yen's method, Muir [23] presented a simple new family of minimal weight signed radix-*r* representations which can be constructed using a left-to-right on-line algorithm. Furthermore, Kong et al. [18] proposed a left-to-right radix-*r* GNAF recoding algorithm, which is an extension of Joye et al.'s left-to-right NAF recoding algorithm.

* Corresponding author. Tel.: +86 15883740775; fax: +86 08166089363.
E-mail address: bd_qin@yahoo.com (B. Qin).

0045-7906/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2008.09.007

In this paper, we are mainly concerned with signed-digit radix-r representations. First we define a middle radix-r recoding, namely GMOF (general mutual opposite form), an extension of the MOF [24]. Second, we present a new left-to-right signed radix-r recoding with the same digits as wrNAF. Our analysis shows that the proposed algorithm can generate a minimal average Hamming weight (asymptotically $\frac{r-1}{w(r-1)+1}$) representation. Finally, we compare our algorithm with the previous ones and it shows that interleaved with the left-to-right scalar multiplication, the new representation can reduce both the time and space complexity of the computation compared to the right-to-left algorithms.

The rest of this paper is organized as follows. Section 2 reviews some facts about MOF and signed radix-r representation. In Section 3 we extend the MOF to GMOF and present a new minimal weight left-to-right analogue of the wrNAF representation. The analysis of our algorithm is presented in Section 4 with some necessary proofs. In Section 5, we compare our method with previous algorithms and give an application of the new representation. Finally, Section 6 concludes this paper.

2. Background

2.1. Mutual opposite form (MOF)

In this subsection, we recall some basic facts about mutual opposite form. For details see [24].

Definition 1. The mutual opposite form (MOF) is a signed binary string that satisfies the following properties:

(1) The signs of adjacent non-zero bits (without considering 0 bits) are opposite.
(2) The most non-zero bit and the least non-zero bit are 1 and -1, respectively, unless all bits are zero.

An example of MOF is $0\ 1\ 0\ 0\ -1\ 0\ 1\ 0\ 0\ 0\ -1\ 0\ 0\ 1\ -1\ 0$.

Theorem 1. *Every non-negative integer N has a representation as MOF, which is unique except for the number of leading zeros.*

Proposition 1. *The n-bit binary string N can be converted to MOF from left to right.*

2.2. Signed radix-r representation

Let $N = \sum_{i=0}^{n-1} a_i r^i$ be a radix-r representation. We denote by $(a_{n-1}, \ldots, a_1, a_0)$ the radix-r representation of N. It is well known that any non-negative integer has a unique radix-r representation with digit set $\{0, 1, \ldots, r-1\}$. In this paper, we usually speak above representations as radix-r representations.

At ISC 2004 [29] Takagi et al. proposed the width-w non-adjacent form of radix-r representation (wrNAF). The definition and some results of wrNAF are presented in the following.

Definition 2. A signed radix-r representation $N = (a_{n-1}, \ldots, a_1, a_0)$ is called the width-w radix-r non-adjacent form (wrNAF) if it satisfies the following conditions.

(1) There is at most 1 non-zero digit among any w adjacent digits.
(2) $a_i \in \{0, \pm 1, \ldots, \pm\lfloor \frac{r^w-1}{2} \rfloor\} \setminus \{\pm 1r, \pm 2r, \ldots, \pm\lfloor \frac{r^{w-1}-1}{2} \rfloor r\}$.
(3) The leftmost non-zero digit is positive. The number of non-trivial digits (except $\{0, \pm 1\}$ and ignoring their sign) is $\frac{r^w - r^{w-1} - 2}{2}$.

Note that if we choose $w = 2$, then the definition is equal to rNAF.

Theorem 2

(1) Every positive integer N has a unique wrNAF representation.
(2) The wrNAF representation of N has the smallest Hamming weight.
(3) The non-zero density of the wrNAF is asymptotically $\frac{r-1}{w(r-1)+1}$.

3. New left-to-right signed-digit radix-r representation

3.1. General mutual opposite form (GMOF)

At Crypto 2004, Okeya et al. proposed a new canonical representation of signed binary strings, namely MOF, which can be computed in any order. The MOF strings have a good property that the width-w sliding window conversion can be performed on MOF from left to right. Moreover, the analogue right-to-left conversion on MOF yields wNAF. In this subsection, we define an analogous form for radix-r ($r \geqslant 2$), namely GMOF in the following.