JOURNAL OF FORMALIZED MATHEMATICS
Volume 12, Released 2000, Published 2003
Inst. of Computer Science, Univ. of Białystok

High-Speed Algorithms for RSA Cryptograms

Yasushi Fuwa
Shinshu University
Nagano

Yoshinori Fujisawa
Shinshu University
Nagano

Summary. In this article, we propose a new high-speed processing method for encoding and decoding the RSA cryptogram that is a kind of public-key cryptogram. This cryptogram is not only used for encrypting data, but also for such purposes as authentication. However, the encoding and decoding processes take a long time because they require a great deal of calculations. As a result, this cryptogram is not suited for practical use. Until now, we proposed a high-speed algorithm of addition using radix-2^k signed-digit numbers and clarified correctness of it ([6]). In this article, we defined two new operations for a high-speed coding and encoding processes on public-key cryptograms based on radix-2^k signed-digit (SD) numbers. One is calculation of $(a*b)$ mod c $(a,b,c$ are natural numbers). Another one is calculation of (a^b) mod c $(a,b,c$ are natural numbers). Their calculations are realized repetition of addition. We propose a high-speed algorithm of their calculations using proposed addition algorithm and clarify the correctness of them. In the first section, we prepared some useful theorems for natural numbers and integers and so on. In the second section, we proved some properties of addition operation using a radix-2^k SD numbers. In the third section, we defined some functions on the relation between a finite sequence of k-SD and a finite sequence of $\mathbb{N}$ and proved some properties about them. In the fourth section, algorithm of calculation of $(a*b)$ mod c based on radix-2^k SD numbers is proposed and its correctness is clarified. In the last section, algorithm of calculation of (a^b) mod c based on radix-2^k SD numbers is proposed and we clarified its correctness.

MML Identifier: `RADIX_2`.

WWW: `http://mizar.org/JFM/Vol12/radix_2.html`

The articles [10], [14], [11], [7], [12], [1], [4], [3], [13], [9], [5], [2], [8], and [6] provide the notation and terminology for this paper.

1. Some Useful Theorems

In this paper k denotes a natural number.

One can prove the following propositions:

(1) For every natural number a holds $a \bmod 1 = 0$.

(2) Let a, b be integers and n be a natural number. If $n > 0$, then $((a \bmod n) + (b \bmod n)) \bmod n = (a + (b \bmod n)) \bmod n$ and $((a \bmod n) + (b \bmod n)) \bmod n = ((a \bmod n) + b) \bmod n$.

(3) For all integers a, b and for every natural number n such that $n > 0$ holds $a \cdot b \bmod n = a \cdot (b \bmod n) \bmod n$ and $a \cdot b \bmod n = (a \bmod n) \cdot b \bmod n$.

(4) For all natural numbers a, b, i such that $1 \leq i$ and $0 < b$ holds $(a \bmod b^i) \div b^{i -' 1} = (a \div b^{i -' 1}) \bmod b$.

(5) For all natural numbers i, n such that $i \in \mathrm{Seg}\, n$ holds $i + 1 \in \mathrm{Seg}(n + 1)$.

2. Properties of Addition Operation Using Radix-2^k Signed-Digit Numbers

We now state several propositions:

(6) For every natural number k holds $\mathrm{Radix}\,k > 0$.

(7) For every 1-tuple x of $k-\mathrm{SD}$ holds $\mathrm{SDDec}\,x = \mathrm{DigA}(x,1)$.

(8) For every integer x holds $\mathrm{SD\_Add\_Data}(x,k) + \mathrm{SD\_Add\_Carry}\,x \cdot \mathrm{Radix}\,k = x$.

(9) Let n be a natural number, x be a $n+1$-tuple of $k-\mathrm{SD}$, and x_1 be a n-tuple of $k-\mathrm{SD}$. Suppose that for every natural number i such that $i \in \mathrm{Seg}\,n$ holds $x(i) = x_1(i)$. Then $\sum \mathrm{DigitSD}\,x = \sum((\mathrm{DigitSD}\,x_1) \frown \langle \mathrm{SubDigit}(x,n+1,k)\rangle)$.

(10) Let n be a natural number, x be a $n+1$-tuple of $k-\mathrm{SD}$, and x_1 be a n-tuple of $k-\mathrm{SD}$. Suppose that for every natural number i such that $i \in \mathrm{Seg}\,n$ holds $x(i) = x_1(i)$. Then $\mathrm{SDDec}\,x_1 + (\mathrm{Radix}\,k)^n \cdot \mathrm{DigA}(x,n+1) = \mathrm{SDDec}\,x$.

(11) Let n be a natural number. Suppose $n \geq 1$. Let x, y be n-tuples of $k-\mathrm{SD}$. If $k \geq 2$, then $\mathrm{SDDec}\,x' +' y + \mathrm{SD\_Add\_Carry}\,\mathrm{DigA}(x,n) + \mathrm{DigA}(y,n) \cdot (\mathrm{Radix}\,k)^n = \mathrm{SDDec}\,x + \mathrm{SDDec}\,y$.

3. Definitions on the Relation Between a Finite Sequence of k-SD and a Finite Sequence of $\mathbb{N}$ and Some Properties about them

Let i, k, n be natural numbers and let x be a n-tuple of $\mathbb{N}$. The functor $\mathrm{SubDigit2}(x,i,k)$ yielding an element of $\mathbb{N}$ is defined by:

(Def. 1) $\mathrm{SubDigit2}(x,i,k) = (\mathrm{Radix}\,k)^{i-'1} \cdot x(i)$.

Let n, k be natural numbers and let x be a n-tuple of $\mathbb{N}$. The functor $\mathrm{DigitSD2}(x,k)$ yields a n-tuple of $\mathbb{N}$ and is defined by:

(Def. 2) For every natural number i such that $i \in \mathrm{Seg}\,n$ holds $(\mathrm{DigitSD2}(x,k))_i = \mathrm{SubDigit2}(x,i,k)$.

Let n, k be natural numbers and let x be a n-tuple of $\mathbb{N}$. The functor $\mathrm{SDDec2}(x,k)$ yields a natural number and is defined as follows:

(Def. 3) $\mathrm{SDDec2}(x,k) = \sum \mathrm{DigitSD2}(x,k)$.

Let i, k, x be natural numbers. The functor $\mathrm{DigitDC2}(x,i,k)$ yielding a natural number is defined as follows:

(Def. 4) $\mathrm{DigitDC2}(x,i,k) = (x \bmod (\mathrm{Radix}\,k)^i) \div (\mathrm{Radix}\,k)^{i-'1}$.

Let k, n, x be natural numbers. The functor $\mathrm{DecSD2}(x,n,k)$ yielding a n-tuple of $\mathbb{N}$ is defined as follows:

(Def. 5) For every natural number i such that $i \in \mathrm{Seg}\,n$ holds $(\mathrm{DecSD2}(x,n,k))(i) = \mathrm{DigitDC2}(x,i,k)$.

Next we state four propositions:

(12) For all natural numbers n, k and for every n-tuple x of $\mathbb{N}$ and for every n-tuple y of $k-\mathrm{SD}$ such that $x = y$ holds $\mathrm{DigitSD2}(x,k) = \mathrm{DigitSD}\,y$.

(13) For all natural numbers n, k and for every n-tuple x of $\mathbb{N}$ and for every n-tuple y of $k-\mathrm{SD}$ such that $x = y$ holds $\mathrm{SDDec2}(x,k) = \mathrm{SDDec}\,y$.

(14) For all natural numbers x, n, k holds $\mathrm{DecSD2}(x,n,k) = \mathrm{DecSD}(x,n,k)$.

(15) Let n be a natural number. Suppose $n \geq 1$. Let m, k be natural numbers. If m is represented by n, k, then $m = \mathrm{SDDec2}(\mathrm{DecSD2}(m,n,k),k)$.

4. A High-Speed Algorithm of Calculation of $(a*b) \bmod b$ Based on Radix-2^k Signed-Digit Numbers and its Correctness

Let q be an integer, let f, j, k, n be natural numbers, and let c be a n-tuple of $k-$SD. The functor $\mathrm{Table1}(q,c,f,j)$ yielding an integer is defined as follows:

(Def. 6) $\mathrm{Table1}(q,c,f,j) = q \cdot \mathrm{DigA}(c,j) \bmod f$.

Let q be an integer, let k, f, n be natural numbers, and let c be a n-tuple of $k-$SD. Let us assume that $n \geq 1$. The functor $\mathrm{Mul\_mod}(q,c,f,k)$ yields a n-tuple of $\mathbb{Z}$ and is defined by the conditions (Def. 7).

(Def. 7)(i) $(\mathrm{Mul\_mod}(q,c,f,k))(1) = \mathrm{Table1}(q,c,f,n)$, and

(ii) for every natural number i such that $1 \leq i$ and $i \leq n-1$ there exist integers I_1, I_2 such that $I_1 = (\mathrm{Mul\_mod}(q,c,f,k))(i)$ and $I_2 = (\mathrm{Mul\_mod}(q,c,f,k))(i+1)$ and $I_2 = (\mathrm{Radix}\, k \cdot I_1 + \mathrm{Table1}(q,c,f,n -' i)) \bmod f$.

Next we state the proposition

(16) Let n be a natural number. Suppose $n \geq 1$. Let q be an integer and i_1, f, k be natural numbers. Suppose i_1 is represented by n, k and $f > 0$. Let c be a n-tuple of $k-$SD. If $c = \mathrm{DecSD}(i_1,n,k)$, then $(\mathrm{Mul\_mod}(q,c,f,k))(n) = q \cdot i_1 \bmod f$.

5. A High-Speed Algorithm of Calculation of $(a^b) \bmod b$ Based on a Radix-2^k Signed-Digit Numbers and its Correctness

Let n, f, j, m be natural numbers and let e be a n-tuple of $\mathbb{N}$. The functor $\mathrm{Table2}(m,e,f,j)$ yields a natural number and is defined by:

(Def. 8) $\mathrm{Table2}(m,e,f,j) = m^{e_j} \bmod f$.

Let k, f, m, n be natural numbers and let e be a n-tuple of $\mathbb{N}$. Let us assume that $n \geq 1$. The functor $\mathrm{Pow\_mod}(m,e,f,k)$ yielding a n-tuple of $\mathbb{N}$ is defined by the conditions (Def. 9).

(Def. 9)(i) $(\mathrm{Pow\_mod}(m,e,f,k))(1) = \mathrm{Table2}(m,e,f,n)$, and

(ii) for every natural number i such that $1 \leq i$ and $i \leq n-1$ there exist natural numbers i_2, i_3 such that $i_2 = (\mathrm{Pow\_mod}(m,e,f,k))(i)$ and $i_3 = (\mathrm{Pow\_mod}(m,e,f,k))(i+1)$ and $i_3 = ({i_2}^{\mathrm{Radix}\, k} \bmod f) \cdot \mathrm{Table2}(m,e,f,n -' i) \bmod f$.

One can prove the following proposition

(17) Let n be a natural number. Suppose $n \geq 1$. Let m, k, f, i_4 be natural numbers. Suppose i_4 is represented by n, k and $f > 0$. Let e be a n-tuple of $\mathbb{N}$. If $e = \mathrm{DecSD2}(i_4,n,k)$, then $(\mathrm{Pow\_mod}(m,e,f,k))(n) = m^{i_4} \bmod f$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[2] Grzegorz Bancerek. Joining of decorated trees. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/trees_4.html`.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finseq_1.html`.

[4] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[5] Czesław Byliński. The sum and product of finite sequences of real numbers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/rvsum_1.html`.

[6] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Journal of Formalized Mathematics*, 11, 1999. `http://mizar.org/JFM/Vol11/radix_1.html`.

[7] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/real_1.html`.

[8] Andrzej Kondracki. The Chinese Remainder Theorem. *Journal of Formalized Mathematics*, 9, 1997. `http://mizar.org/JFM/Vol9/wsierp_1.html`.

[9] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/binarith.html`.

[10] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

[11] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[12] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

[13] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_4.html`.

[14] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/subset_1.html`.

Received February 1, 2000

Published January 2, 2004