UDC 681. 03

V.A. Krasnobayev[1], O.I. Tyrtyshnikov[1], S.V. Somov[1], S.A. Koshman[2], G.V. Sokol[1], N.V. Rvachova[1]

[1] *Poltava National Technical Yuri Kondratyuk University, Poltava*
[2] *Kharkov National Technical University of Agriculture named after Peter Vasylenko, Kharkov*

MATHEMATICAL MODEL AND TABULAR METHOD IMPLEMENTATION OF MODULAR ARITHMETIC OPERATIONS WITH CRYPTO TRANSFORMATIONS IN THE RESIDUE CLASS

The method is considered for realization of public-key cryptographic transformations based on the use of the position-independent base notation system in the remainder classes.

Keywords: *non-position number system, modular number system, cryptographic transformations.*

Introduction

Present-day public-key cryptographic transformations are based on the algebraic curves transformations (elliptic curves (EC), hyper- elliptic curves (HEC), the Picard curves (PC) and super-elliptic curves (SEC)). The trend of cryptographic methods development is moving towards the increased key lengths that, in its turn, results in decreasing of the speed of public-key cryptographic transformations. This is especially crucial at providing for the prescribed resistance while realizing the EC-based cryptographic transformations in special systems and devices where there exist substantial restrictions with respect of the memory capacity and the weight-and-dimension characteristics, i.e., in those cases when it is impossible to use powerful stationary high-efficiency computers with a large exponential grid. This phenomenon stipulates the importance and actuality of seeking for the methods of increasing the efficiency, reliability and trustworthiness of the cryptographic transformations.

Analysis of reference

The analysis of the methods for increasing of the efficiency of SEC in the HEC Jacobian allowed to theoretically substantiate and to practically demonstrate the dependence of the realization of the efficiency of SEC operations in the Jacobian of HEC upon the aggregate of the following basic characteristics - type of realization of cryptographic transformations (software, hardware and software-hardware); algorithm type of the SEC divisors; the prescribed base field, over which the given curve is set; the type of the curve; the values of the curve coefficients; the selected system of coordinates, in which the HEC Jacobian divisors (affinity, projective, weighted and mixed) are represented; the accepted method of arithmetical transformations etc. The known methods of realization of the SEC algorithm (the Quantor divisor summation method, the Kobliz method, the method of arithmetic transformations of divisors in the HEC Jacobian of the second, the third and the fourth kinds, methods of summation of divisors with different weights, the Karatsuba method for multiplication and reduction of the polynomial functions by the module in the field, the method based upon several results of the Chinese remainder theorem etc.) do not always satisfy the requirements with respect to the efficiency of cryptographic transformations. At the same time, the reference sources [1 – 5] demonstrate high efficiency of the modular arithmetic (MA) codes, i.e., the system of computation in remainder classes (CRC) while solving separate problems of digital data processing (solving of filtering problems, problems of realization of FFT, DFT etc.) from the point of view of the high efficiency of their realizations. Thus, it is known that the Fourier transformation is related to calculation of the polynomial of the kind $P(x) = \sum_{i=1}^{n-1} \alpha_i x^i$. One of the applications of the Fourier transformation lies in calculation of the convolution $\sum_{i=1}^{n} \alpha_i \beta_i$ of two n-dimensional vectors $A = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $B = (\beta_1, \beta_2, ..., \beta_n)$. In the given case the convolution operation is the complete analogue to the realization of arithmetic operations of multiplication of two numbers *A* and *B* in MA with consequent summation of the components of the kind $\alpha_i \beta_i (\mathrm{mod}\, m_i) + \alpha_j \beta_j (\mathrm{mod}\, m_j)$.

In the given aspect this phenomenon stipulates the importance and actuality of the search for the methods for increasing of the efficiency, reliability and validity of the public-key cryptographic transformations on the basis of the using the properties of the position-independent MA code structures.

The objective of the paper is to develop a highly efficient method for realization of public-key cryptographic transformations on the basis of the using the position-independent MA codes of position-independent structures, i.e., CRC codes.

Recitals

The influence of the CRC main parameters (independence, equality and short form of the operand-representing remainders) upon the structure and the principles of operation of the data processing system (DPS) in MA are considered in details in [1 – 6]. In particular, it is demonstrated that short form of the rests in representation of numbers in modular arithmetic provides for the possibility of wide selection between the options of system engineering solutions at realization of the modular arithmetic operations.

It is known that there exist four principles of realization of arithmetic operations in MA – the summation principles (SP) (on the base of short binary summators [1]); the table principle (TP) (on the base of using ROM [1, 6, 10]); the direct logical principle of realization of arithmetic operations based on description of module operations at the level of the systems of switching functions by means of which the values of binary digits of the resulting deductions are formed (it is reasonable to use systolic and programmable logical matrices as well as EPLD [6] as the element base for technical realization of the given principle); the principle of ring shift (PRS) based on using of the ring shift register (RSR) [6 – 9, 11].

The absence of bit-to-bit associations (the absence of the transport process) between the binary digits in operands processed in DPS during the process of cryptographic transformations (at realization of module operations) on the basis of TP or PRS is one of the main and the most attractive particularities of modular arithmetic. Within the base notation system (BNS) the performance of an arithmetic operation assumes the subsequent processing of operands digits upon the rules determined by the contents of the given operation and cannot be finished up to the moment until the values of all of the intermediate results considering all the relationships between the bits, are sequentially determined. Thus, BNS in which the information is represented and processed in the present-day DPS, have a substantial drawback - the presence of bit-to-bit associations which impose their imprint upon the methods of realization of arithmetic operations; make the hardware more complicated, decrease the trustworthiness of calculations and restrict the computing speed of crypto-graphic transformations realization. Therefore, it is only natural to seek for the opportunities of creation of the kind of arithmetic, in which the bit-by-bit associations would be absent. In this connection it is worth to pay attention to the base notation system in the residual classes. The system of residual classes possesses a valuable parameter of independence of the remainders upon each other pursuant to the accepted system of bases. This independence opens up wide opportunities to the development of not only the new kind of machine arithmetic but also to the principally new structural realization of DPS, which, in its turn, is substantially extending the sphere of application of the machine arithmetic. In most of the reference sources it is noted that implementation of non-traditional methods for data representation and processing in the numerical systems with parallel structure and, in particular, within the so-called modular base notation systems possessing the maximal level of the internal parallelism in organization of the data processing procedures is one of the practical trends in increasing of the user efficiency of computing equipment. The position-independent computing system in the residual classes is also referred to the above systems.

Short form of the rests, which represent the operand, is one of the CRC properties. It is just this property that allows to substantially increase the computing speed at execution of the arithmetic operations due to the possibility of application (unlike in BNS) of the table arithmetic where the arithmetic operations of addition, deduction and multiplication are performed practically in one and the same cycle [10]. The search for the way of increasing of the data processing efficiency led to the necessity of development of the table method for realization of modular operations on the basis of PRS.

The known table method for realization of the modular multiplication operation is realized in CRC by means of using the table multiplication code (TMC) [1, 10]. In this case the table $\alpha_i\beta_i(\mathrm{mod}\, m_i)$ of modular multiplication for the arbitrary base m* of the CRC is symmetrical with respect to the left-hand side (the main one) and the right-hand side diagonals as well as of the vertical and the horizontal. The symmetry with reference to the left-hand side diagonal is determined by the switching capabilities of the operation $\alpha_i\beta_i$, of multiplication and the symmetry with respect to the right-hand side diagonal is determined by the fact that

$$(m_i - \alpha_i)(m_i - \beta_i) \equiv \alpha_i\beta_i \,(\mathrm{mod}\, m_i). \qquad (1)$$

The symmetry relative to the vertical and the horizontal is determined from the condition of the module multiplicity to the sum of the symmetric numbers from the multiplication table.

$$\alpha_i\beta_i + \alpha_i(m_i - \beta_i) \equiv 0(\mathrm{mod}\, m_i), \qquad (2)$$

$$\alpha_i\beta_i + \beta_i(m_i - \alpha_i) \equiv 0(\mathrm{mod}\, m_i). \qquad (3)$$

Considering the above it is evident that for the table realization of the modular multiplication operation $\alpha_i\beta_i(\mathrm{mod}\, m_i)$ it would be sufficient to have numerical information about its one-eighth portion only. Hence there occurs the possibility to simplifay the modular multiplication table.

To the most efficient realize of the operation $\alpha_i\beta_i(\mathrm{mod}\, m_i)$ there are applied special encryption methods allowing to decrease modular multiplication

table by four times. Solving to the set problem is possible as the result of application of special codes. Let us consider one of the options of performing of the modular multiplication operation by means of using TMC (see Tables 1 and 2 (for $m_i = 5$)).

Let the input values of α_i and β_i are given and the values $\alpha_i(\beta_i)$ lying within the range of $[0,(m_i-1)/2)$ may be encoded in an arbitrary way and the values $\alpha_i(\beta_i)$ lying within the range of $[(m_i+1)/2, m_i-1)$ are encoded as $m_i-\alpha_i(m_i-\beta_i)$.The following index (attribute) of TMC is introduced in order to distinguish between the ranges:

$$\gamma_\alpha\left(\gamma_\beta\right)=\begin{cases}0, \text{ if } 0\le\alpha_i\left(\beta_i\right)\le\left(m_i-1\right)/2,\\ 1, \text{if } \left(m_i+1\right)/2\le\alpha_i\left(\beta_i\right)\le m_i-1.\end{cases} \quad (4)$$

A set of analytical relations (1) – (4) is a mathematical model of the process table of the modular arithmetic operations. It is the basis of the method set out below a table of the modular arithmetic operations.

The method to determine the result of the modular multiplication operation $\alpha_i'\beta_i'(\mathrm{mod}\, m_i)$ in CRC by means of using of TMC are the following – if two operands are set in TMC

$$\alpha_i=(\gamma_\alpha,\alpha_i'),\ \beta_i=(\gamma_\beta,\beta_i'),$$

then, in order to obtain the product of these numbers upon the module m_i; it is sufficient to find the product $\alpha_i'\beta_i'(\mathrm{mod}\, m_i)$ and to invert its generalized index γ_i in the case when γ_α if different from γ_β, i.e.,

$$\alpha_i\beta_i\left(\mathrm{mod}\, m_i\right)=\left(\gamma_i,\alpha_i'\beta_i'\left(\mathrm{mod}\ m_i\right)\right),$$

where

$$\gamma=\begin{cases}\overline{\gamma}_i, \text{ if } \gamma_\alpha\ne\gamma_\beta,\\ \gamma_i, \text{ if } \gamma_\alpha=\gamma_\beta;\end{cases} \quad (5)$$

$$\alpha_i'=\begin{cases}\alpha_i, \text{ if } \gamma_\alpha=0,\\ m_i-\alpha_i, \text{ if } \gamma_\alpha=1.\end{cases}$$

While using this method, the ROM, which is realizing the modular multiplication operation, is structurally decreased by four times. At performing the operation with the help of the table methods additional decreasing of the equipment is possible in some cases due to the fact that it is not only one table that is built for modular operations but **k** smaller tables allowing to provide the answers to each of **k** digits of the result, where **k** is the register capacity necessary for storing of the digits of the remainder upon the considered base of CRC [1].

By now the issues of efficient realization of arithmetic operations of summation and deduction using TMC were either unconsidered in the reference literature or this realization was considered by most of researchers theoretically and practically impossible. The realization is made difficult by the fact that it is rather difficult to synthesize the table algorithms for these modular operations while the tables for realization of the modular operations of summation and deduction are different from the point of view of their digital structure. Therefore, they do not possess the symmetric properties inherent to the tables of modular multiplication. However, it is possible to obtain quite different results with the help of investigation of the opportunities of realization of one modular operation using the tables realizing the inverted to it operation and vice versa.

While investigating digital properties of the tables of modular operations of summation and deduction the following analytical correlation is proved

$$\left[\left(\gamma_\alpha,\alpha_i'\right)+\left(\gamma_\beta,\beta_i'\right)\right]+$$

$$+\left\{\left[m_i-\left(\gamma_\alpha,\alpha_i'\right)\right]-\left(\gamma_\beta,\beta_i'\right)\right\}=0\left(\mathrm{mod}\, m_i\right), \quad (6)$$

where

$$\alpha_i=\left(\gamma_\alpha,\alpha_i'\right),\ \beta_i=\left(\gamma_\beta,\beta_i'\right)$$

are the input operands represented in TMC. We shall put down the expression (1) in the form of

$$\left(\gamma_\alpha,\alpha_i'\right)+\left(\gamma_\beta,\beta_i'\right)=$$
$$=m_i-\left\{\left[m_i-\left(\gamma_\alpha,\alpha_i'\right)\right]-\left(\gamma_\beta,\beta_i'\right)\right\}. \quad (7)$$

From the expression (2) it follows that in order to obtain the result of the modular operation of summation in TMC it would be sufficient to know the result of the modular operation of deduction, i.e., there occurs the possibility to efficiently (from the point of view of decreasing of the number of ROM equipment) use TMC for three modular operations – multiplication, summation and deduction.

On the basis of the expression (2) we shall consider the method, by means of which it would be possible to effect performance of any of the three arithmetic operations in CRC - multiplication, summation and deduction.

The operation of modular summation is effected by means of the algorithm described in the expression (2). We shall develop the algorithm for execution of the operation of modular summation with the help of the Table for performance of the modular deduction operation

$$(\alpha_i'-\beta_i')\,\mathrm{mod}\, m_i.$$

In compliance with the expression (2) we consider the method of realization of the modular summation operation

1. The minuend

$$\alpha_i = (\gamma_a - \alpha_i')$$

is inverted upon the module m_i, i.e., we obtain the following expression

$$\overline{\alpha_i} = ((\gamma_a + 1) \bmod 2, \alpha_i').$$

The subtrahend (γ_β, β_i') will be left without changes.

2. By means of ROM realizing the modular deduction operation the result of the operation

$$(\alpha_i' - \beta_i') \bmod m_i$$

is determined upon the input operands α_i' and β_i'. Like for the algorithm of modular multiplication the index γ_i of the result of the modular deduction operation is formed with keeping with the values of the indices of the relevant operands, i.e., in compliance with the values

$$(\gamma_\alpha + 1) \bmod 2$$

and γ_β where

$$\gamma_i = \begin{cases} \overline{\gamma}, \text{ if } (\gamma_\alpha + 1) \bmod 2 \neq \gamma_\beta, \\ \gamma, \text{ if } (\gamma_\alpha + 1) \bmod 2 = \gamma_\beta. \end{cases}$$

Therefore, the result of the modular deduction operation will have the following representation:

$$\left(\gamma_i, \left(\alpha_i' - \beta_i'\right) \bmod m_i\right).$$

3. The obtained result of the modular deduction operation we shall invert upon the module m_i, i.e.,

$$\left((\gamma_i + 1) \bmod 2, \left(\alpha_i' - \beta_i'\right) \bmod m_i\right).$$

Table 1

Table multiplication code

a_i	КТУ		a_i	КТУ	
	γ_a	a_i'		γ_a	a_i'
1	0	1	3	1	2
2	0	2	4	1	1

Table 2

Modular multiplication table

β_i \ a_i	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 3

Modular summation table

β_i \ a_i	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 4

Modular deduction table

β_i \ a_i	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

Table 5

Second quadrant of Table 2

β_i \ a_i		1	2
		4	3
1	4	1	2
2	3	2	4

Table 6

Second quadrant of Table 4

β_i \ a_i		1	2
		4	3
1	4	0	1
2	3	4	0

Table 7

First quadrant of Table 4

β_i \ a_i		2	1
		3	4
1	4	2	3
2	3	1	2

Thus, despite the difference in the digital structure of the tables of modular operations of summation deduction and multiplication there was created a new original table method for realization of arithmetic operations in MA.

On the basis of the method it is possible to synthesize a structurally simple, highly reliable and super-efficient DPS in MA, the basis of which is formed by three separated switches each of them realizing only 0,25 part of the relevant complete table of modular operations of multiplication (Table 2) and deduction (Table 4) (the first switch is the II quadrant of the multiplication table (Table 5); the second and

the third switches are respectively I (Table 7) and II (Table 6) quadrants of the deduction Table 4).

In this sense the table multiplication code obtained a new quality and became the universal table code for performance of the three arithmetic operations in CRC.

Conclusions

The method for realization of public-key cryptographic transformations is considered. The present method is based upon representation and processing of the integer-number digital data. The algorithms for realization of arithmetic operations of summation, deduction and multiplication are developed on the basis of the said method.

The principal advantage of the suggested method lies in the possibility to attain the extra fast action in data processing. Thus, the result of execution of an arithmetic operation by using of the table method can be obtained at the moment of arriving of the input operands for processing in the DPS, i.e., within one cycle, that cannot be executed in standard binary BNS. Therefore, the time for execution of arithmetic operations in TMC is comparable with the clock frequency of TMC that is principally non-attainable for TMC in BNS.

The results of the presented investigations can also be used in the systems and devices for processing of large-size arrays of digital data provided in the form of a non-integer representation in a real time scale. In particular, this method is recommended to use in the systems and devices in order to increase the efficiency of public-key cryptographic transformations.

References

1. Akushskyi I.Ya. Machine arithmetic in residual classes / I.Ya. Akushskyi, D.I. Yuditskyi. – M., 1968. – 440 p.

2. Bleighut R., (1989), Fast algorithms for digital processing of signals / R. Bleighut. – M.: Mir. – 448 p.

3. Kravchenko V.F. Methods and microelectronic devices for digital filtering of signals and images based on the theoretical and numerical transformations / V.F. Kravchenko, A.M. Krot // Foreign radio electronics. Achievements of present-day radio electronics. – 1997. – 6. – P. 3-31.

4. Chervyakov N.I. High-speed digital processing of signals using position-independent arithmetic / N.I. Chervyakov, K.T. Tyncherov, A.V. Veligosha // Radiotekhnika. – 1997. – 10. – P. 23-27.

5. Lavrinenko D.I. Application of fast Fourier transformation in cryptographic transformers / D.I. Lavrinenko // Radiotekhnika. – 2000. – 114. – P. 75-79.

6. Zhikharev V.Ya. Methods and means of data processing in position-independent base notation system in residual classes / V.Ya. Zhikharev, Ya.V. Ilyushko, L.G. Kravets, V.A. Krasnobayev. – Zhytomyr: Volyn, 2005. – 220 p.

7. Zhikharev V.Ya. Methods and algorithms for realization of arithmetic operations in the class of deductions / V.Ya. Zhikharev, Yunes El Handassi, V.A. Krasnobayev // Open information and computer integrated technologies. – 2003. – 20. – P. 84-101.

8. Dolgov V.I. Methods and algorithms for realization of arithmetic operations in the system of remainder classes / V.I. Dolgov, V.A. Krasnobayev, I.V. Kononova // Electron. Modeling. – 1990. – 5. – P. 70-72.

9. Krasnobayev V.A. Algorithms for realization of modular multiplication operation in the system of remainder classes / V.A. Krasnobayev, V.P. Irkhin // Electron. Modeling. – 1993. – 5. – P. 20-26.

10. Krasnobayev V.A. Method for Realization of Transformations in Public-Key Cryptography / V.A. Krasnobayev // Telecommunications and Radio Engineering (USA). – 2007. – Vol. 66, issue 17. – P. 1559-1572.

11. Koshman S.A. Method of Realization of Cryptographic RSA Transformations on the Basis of Application of Modular Number System / S.A. Koshman, V.A. Krasnobayev // Biomedical Soft Computing and Human Sciences. – 2011. – Vol.17, no. 2. – P. 31-36.

Поступила в редколлегию 10.10.2013

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ И ТАБЛИЧНЫЙ МЕТОД РЕАЛИЗАЦИИ МОДУЛЬНЫХ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ ПРИ КРИПТОПРЕОБРАЗОВАНИЯХ В КЛАССЕ ВЫЧЕТОВ

В.А. Краснобаев, А.И. Тыртышников, С.В. Сомов, С.А. Кошман, Г.В. Сокол, Н.В. Рвачова

Рассмотрен метод для реализации криптопреобразований с открытым ключом, которые основаны на использовании непозиционной системы счисления в классе вычетов.

Ключевые слова: *непозиционная система счисления, модулярная система счисления, криптопреобразования.*

МАТЕМАТИЧНА МОДЕЛЬ І ТАБЛИЧНИЙ МЕТОД РЕАЛІЗАЦІЇ МОДУЛЬНИХ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ПРИ КРИПТОПЕРЕТВОРЕННЯХ У КЛАСІ ЛИШКІВ

В.А. Краснобаєв, О.І. Тиртишніков, С.В. Сомов, С.О. Кошман, Г.В. Сокол, Н.В. Рвачова

Розглянуто метод для реалізації криптоперетворень з відкритим ключем, які засновані на використанні непозиційної системи числення у класі лишків.

Ключові слова: *непозиційна система числення, модулярна система числення, криптоперетворення.*