УДК 681. 03

V.A. Krasnobayev[1], O.I. Tyrtyshnikov[1], I.I. Sliusar[1], V.N. Kurchanov[1], S.A. Koshman[2]

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

THE MODEL AND THE METHOD OF IMPLEMENTATION OF INTEGER ARITHMETIC OPERATIONS WITHIN THE RSA CRYPTO ALGORITHMS

The methods of rapid information processing aimed to reduce the time of realization of cryptographic RSA transformations are propounded in the paper. These methods are based on application of the principle of ring shift in the module number system (MNS). MNS application, from point of view of increasing the speed of realization of cryptographic transformations with the open key, proves to be effective in organizing the process of realization of module integer arithmetic operations.

Keywords: *specialized digital devices and systems, base, non-position number system, modular number system, cryptographic transformations.*

Introduction

Currently modern cryptotransformations with the open key are based on transformations of algebraic curves (elliptic curves (EC), hyper elliptic curves (HEC), Picard curves (PC) and superelliptic curves (SEC)) as well as on RSA systems [1 – 3]. The existing trend of development of cryptographic methods of information processing is aimed to increase the keys length that, in turn, results in decreasing the speed of cryptographic transformations with the open key. It is especially crucial for providing the set level of resistance during realization of cryptotransformations on EC in the special systems and devices with existing limitations in memory size and mass sizes, i.e. in those cases, where it is impossible to utilize powerful computers with many digits. This status determines the importance and actuality of development of methods of efficiency increasing, reliability and validity of cryptotransformations [4 – 5].

Sources of authors' research

The analysis of methods of increasing of efficiency of SC in Jacobean of HEC allows to ground theoretically and practically the dependence of efficiency of realization of operations of SC in Jacobean of HEC on the bulk of the following basic characteristics: the type of realization of cryptotransformations (software, hardware or software and hardware); the type of algorithm of SEC divisors; the set base field upon which this curve is set above; the type of curve; values of curve coefficients; the selected system of coordinates, in which divisors of Jacobean of HEC (affinor, projective, weighted and mixed) are presented; the accepted method of arithmetic transformations in Jacobean etc. The known methods of realization of algorithms of SEC (Kantor method of divisors addition, Koblits method, methods of arithmetic transformations of divisors in Jacobean of HEC of the second, third and fourth type, methods of addition of divisors of different weight, Karatsuba method for modular multiplication and reduction in the field of polynominal functions, (the method based on some results of the "Chinese Theorem of Remainders" etc.) do not always meet the requirements of efficiency of cryptotransformations. Meantime, efficiency of application of codes of modular arithmetic, i.e. the modular number system (MNS), is highly appreciated in literature [6, 7] for solving certain tasks of rapid digital information processing (tasks solving of digital filtration, tasks of realization FFT, DPF etc.).

Actual state of the problem and objectives of research

Mentioned above confirms the importance and actuality of development of methods and means for increasing the efficiency, especially of RSA cryptotransformations on the basis of application of MNS. It is connected with the fact that RSA system offered in 1977 is considered to be the most widely used cryptosystem with the open key at present [5, 8].

The objective of the paper is to develop the method of rapid realization of cryptographic transformations with the open key, as well as the structural diagram of operating device (OD) of the special processor of cryptographic information processing (SPCIP) on the basis of MNS application.

According to [7], the influence of basic properties (independence, equality, and low digits existence of remainders presenting an operand) of MNS upon the structure and principles of functioning of SPCIP in MNS is examined. It is emphasized that low digits existence of remainders in presentation of digits in modular arithmetic enables a great choice of variants of system and technical solutions during realization of integer modular arithmetic operations.

It is known that there are four principles of realization of arithmetic operations in MNS: the principle of summation (on the basis of low digits of binary adders in modulus m_i of MNS); tabular principle (on the basis of the use of ROM); direct logical principle of realization of arithmetic operations based on description and realization of module operations at the level of the systems of switch functions, due to which the values of results of module operations are formed (it is better to utilize systole and programmable logical matrices as an element base for technical realization of this principle, as well as PLD); principle of ring shift (PRS) based on the application of ring shift registers (RSR).

The lack of process of transfer between digit remainders presented in MNS (inside the very remainder in modulus m_i between binary digits transfers exist) in the operands processed in SPCIP in the process of cryptotransformations (during realization of module operations) on the basis of PCC is one of main and the most attractive features of MNS.

Applied method of problem solving

In positional number system (PNS), implementation of arithmetic operation needs the sequential processing of digits of operands due to the rules determined by the content of this operation, and it can not be completed until the values of all of intermediate results, with taking into account of all connections between digits, are subsequently determined.

Thus PNS, in which information is obtained and processed in modern SPCIP, has the substantial gap – it has interdigital connections which affect the methods of realization of arithmetic operations, it needs complicated equipment, reduces validity of calculations, and restrict the speed of realization of cryptographic transformations. Therefore, the development of arithmetic which could be characterized by the lack of connections between digits is required. In this case MNS appears to be attractive. The given non-position number system possesses the significant property of independence of remainders from each other according to the accepted system of base. This independence offers wide opportunities in the construction of not only new machine arithmetic but also the principally new scheme of SPCIP realization, which in turn, extends increasingly the application of machine arithmetic. According to many literary sources, the introduction of non-traditional methods of information presenting and processing in digital systems with parallel structure is considered to be one of the means in increasing the efficiency of computer use, particularly, in so-called modular number systems which has maximum level of internal parallelism in the process organization of information processing. The MNS is referred to these systems.

General approach to task solving

We will consider the existing pre-conditions of the effective application of modular number system as the SPCIP system. They are as follows: in SPCIP, digit information processing, like in MNS, is done only with integer numbers; in SPCIP realization only of module arithmetic operations is performed; realization of integer module arithmetic operations in SPCIP is performed in a positive numerical range; basic operations during realization of RSA cryptosystem (more than 95%) are the operations of module multiplication and the operation of numbers squaring in modulus m_i is the most effective (from the point of view of performance speed of module arithmetic operations) realized in MNS; due to increasing the length of one computer word l (the number of computer digits, (embedded processor, processor node) of cryptosystem), which is a special feature of modern development trend of SPCIP of RSA system, efficiency of application of MNS rises; wide use of RSR in SPCIP during realization of RSA cryptotransformations; the gap of the problem solving in PNS of essential increase of efficiency and reliability of SPCIP; positive preliminary results of MNS efficient application for increasing the use efficiency and SPCIP reliability of the real time.

According to findings [9], the principle of realization of integer arithmetic operations is formulated in MNS, i.e. the PRS, which is characterized by a special feature – the result of arithmetic operation $(a_i \pm b_i) \bmod m_i$ with any in modulus m_i of MNS by determined set of base $\{m_j\}$ $(j=\overline{1,n})$, is determined without the calculation of values of sizes of partial sums S_i and values C_i of transfers of binary addares in PNS, but only whereby the cycle shifts of the set digital structure. Indeed, the famous Cayley theorem establishes isomorphism between the elements of eventual abelian group and the elements of the group of transpositions.

It is deduced from Cayley theorem that the influence of elements of abelian group upon the group of all integer numbers is homomorphous. This case allows to organize the process of determination of the result of arithmetic operations in MNS by means of the application of PRS. So, an operand in MNS appears to be a set of n remainders $\{a_i\}$ formed by the successive division of initial number A to n of prime in pairs numbers $\{m_i\}$, for $(i=\overline{1,n})$. In this case the aggregate of remainders $\{m_i\}$ is directly equates with the sum n of Galois simple fields of this kind $\sum_{i=1}^{n} GF(m_i)$.

Due to the method of realization of arithmetic operations in MNS it is convenient and sufficient to consider a variant for the arbitrary eventual Galois field $GF(m_i)$ when i=const, i.e. for the concrete defined system of residues mod m_i. Application of mentioned above properties allows to realize the operations of module addition and subtraction in MNS whereby PRS by means of n ring $M = m_i([\log_2(m_i - 1)] + 1)$, i.e. by bit shift registers.

The arbitrary algebraic system can be presented in the kind of $S = (G, \otimes($ – where G – is not an empty set; $\otimes$ – is the type of operation, defined for any of two elements a_i, $b_i \in G$. Operation $\oplus$ of addition in the set of classes of subtraction *R*, caused by the ideal J, forms a new ring called the ring of classes of subtraction R/J. It can be presented in the kind of Z/m_i, where Z – is a great number of integers 0, ± 1, $\pm 2, \ldots$. (If the base m_i of MNS is a simple number, then Z/m_i is a field). This case determines the possibility of realization of arithmetic operation of addition in MNS without transfers between digits by means of the ring shift of the content of digits.

Methods of realization of cryptographic transformations

On the basis of PRS offered in the paper the method of realization of arithmetic operations in MNS is propounded, i.e. the method of binary presentation of remainders (MBPR). Due to this method, the initial digital structure for every modulus (base) m_i of MNS appears to be as the content of the first line (column) of Cayley Table of module addition (subtraction) $(a_i \pm b_i) \bmod m_i$ of the kind presented in fig. 1.

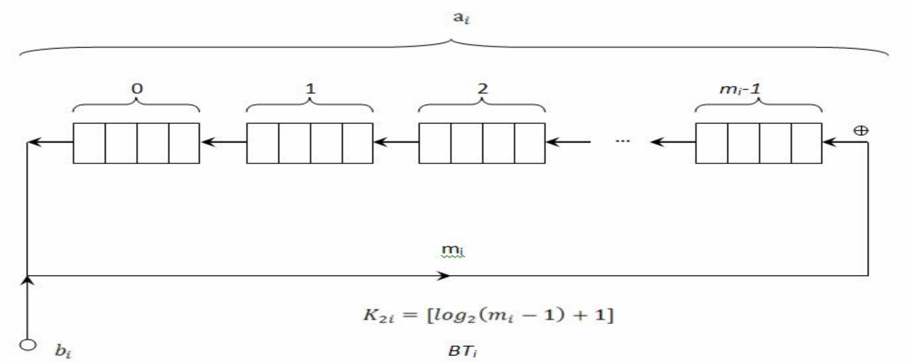

Fig. 1. Adder in modulus m_i in MNS

Initial digital structure of content of RSR for every in modulus m_i can be presented in the kind of (1):

$$P^{(m_i)} = \left[P_0(\alpha_0)\|P_1(\alpha_1)\|\ldots\|P_{m_i-1}(\alpha_{m_i-1})\right]. \quad (1)$$

where $\|$ – is the operation of concatenation (joining, agglutination); $P_v(a_v)$ – k-digital binary code which equals the a_v remainder of $(a_v = \overline{0, m_i - 1})$ number in modulus m_i; $k = [\log_2(m_i - 1) + 1]$.

For the set concrete modulus m_i=5, the initial digital structure of content of RSD looks like:

$$P_{init}^{(5)} = [000\|001\|010\|011\|100].$$

Thus, by means of used ring shift registers in PNS it is easily to realize arithmetic operations in MNS. So degrees of cyclic transpositions due to (1) are determined by the following formulae:

$$\begin{gathered}\left[P_0(\alpha_0)\|P_1(\alpha_1)\|\ldots\|P_{m_i-1}(\alpha_{m_i-1})\right] = \\ = \left[P_z(\alpha_z)\|P_{z+1}(\alpha_{z+1})\|\ldots\|P_0(\alpha_0)\|\ldots\|P_{m_i-1}(\alpha_{m_i-1})\right]^Z,\end{gathered} \quad (2)$$

$$\begin{gathered}\left[P_0(\alpha_0)\|P_1(\alpha_1)\|\ldots\|P_{m_i-1}(\alpha_{m_i-1})\right]^{-Z} = \\ = \left[P_{m_i-1-z}(\alpha_{m_i-1-z})\|\ldots\|P_{m_i-z}(\alpha_{m_i-z1})\| \right. \\ \left. \|\ldots\|P_0(\alpha_0)\|P_1(\alpha_1)\|\ldots\|P_{m_i-z-2}(\alpha_{m_i-z-2})\right].\end{gathered} \quad (3)$$

It should be mentioned that $\left[P_0(\alpha_0)\left(P_1(\alpha_1)\left(\ldots\left(P_{m_i-1}(\alpha_{m_i-1})\right]^{m_i} = \varepsilon\right.\right.\right.$, i.e. if z = m_i then all elements of well-organized set $\{P_j(\alpha_i)\}$ $(j = \overline{0, m_i - 1})$ remain on its initial position.

During technical realization of this method, the first operand a_i determines the number a_{a_i} digit of $P_{a_i}(a_{a_i})$, with the content of the result of module operation in the modulus m_i, and the second operand b_i determines the number of digits of RSR ($b_i k$ – binary digits), which displays how many digits of the RSR content should be shifted (1). Fig. 2 present the chart of possible SPCIP operation device (OD) in MNS.

It is known that time of additional of two remainders $(a_i + b_i) \bmod m_i$ in MNS will be determined by the following mathematical expression:

$$T_{MNS_{m_i}}^{(+)} = K_{1i} \cdot K_{2i} \cdot t_{shift}, \quad (4)$$

where: K_{1i} – is a value of the second b_i element in the sum $(a_i + b_i) \bmod m_i$ (the amount of digits of RSR which is subjected in positive (anticlockwise) direction to initial content shift of RSR), i.e. $K_{1i} = \overline{0, m_i - 1}$; K_{2i} – is amount of binary digits in one RSR digit on modulus m_i, i.e. $K_{2i} = [\log(m_i - 1)] + 1$; $K_{1i} \cdot K_{2i}$ – is the amount of shifted binary digits in positive direction of binary digits of RSR; $t_{shift} = 3 \cdot \tau_{le}$ – is the time of shift of one binary digit; τ_{le} – is the time of switch of one logical element (element And, OR).

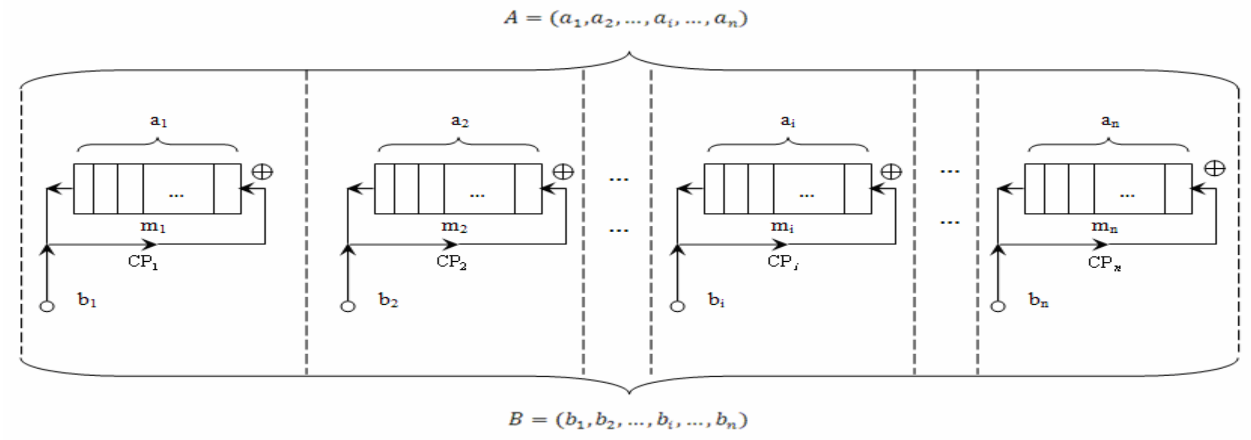

Fig. 2. Chart of operation device of SPCIP for arbitrary MNS

Thus, for the arbitrary modulus m_i of MNS time of addition of two remainders a_i and b_i in modulus equals

$$T^{(+)}_{MNS_{m_i}} = 3 \cdot K_{1i} \cdot \{[\log_2(m_i - 1)] + 1\} \cdot \tau_{le}. \qquad (5)$$

In this case maximally possible value $T^{(+)}_{MNS_{m_i}}$ for the arbitrary module m_i of MNS is equal to

$$T^{(+)}_{MNS_{m_i \max}} = 3 \cdot (m_i - 1) \cdot \{[\log_2(m_i - 1)] + 1\} \cdot \tau_{le}, \qquad (6)$$

but for the given MNS maximal time of addition of two numbers $A = (a_1, a_2, \cdots, a_n)$ and $B = (b_1, b_2, \cdots, b_n)$ equals

$$T^{(+)}_{MNS_{m_n \max}} = 3 \cdot (m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\} \cdot \tau_{le}. \qquad (7)$$

In general, the time of addition of two numbers $A = (a_1, a_2, \cdots, a_n)$ and $B = (b_1, b_2, \cdots, b_n)$ in MNS is determined by the time $T^{(+)}_{MNS_{m_i}}$ of realization of module operation $(a_i + b_i) \bmod m_i$ in computer path (CP_i), i.e. in CIP, for which the case of $K_{1i} \cdot K_{2i} = \max$ is done from all $CP_j (j = \overline{1, n};\ i \neq j)$.

Examples of concrete implementation of operation of addition of two numbers in MNS for one byte $(l = 1)$ processor are propounded. For $l = 1$ MNS base can be as follows: $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ and $m_4 = 7$. The simplified chart of operation device is presented for one byte $(l = 1)$ processor in MNS in fig. 3.

Example 1. If the second operand is equal to $B = (10, 10, 100, 001)$.

Then:

– for $CP_1(m_1 = 3)$ we have $b_1 = 10$, $K_{11} = 2$, $K_{21} = [\log(m_i - 1)] + 1 = 2$, and $K_{11} \cdot K_{21} = 2 \cdot 2 = 4$;

– for $CT_2(m_2 = 4)$ we have $b_2 = 10$, $K_{12} = 2$, $K_{22} = 2$, and $K_{12} \cdot K_{22} = 2 \cdot 2 = 4$;

– for $CP_3(m_3 = 4)$ – $b_3 = 100$, $K_{13} = 4$, $K_{23} = 3$ and $K_{13} \cdot K_{23} = 4 \cdot 3 = 12$;

– for $CP_4(m_4 = 7)$ – $b_4 = 001$, $K_{14} = 1$, $K_{24} = 3$ – and $K_{14} \cdot K_{24} = 1 \cdot 3 = 3$.

It is apparent that the greatest number of shifted binary digits – 12 is occurred in the third computer path (CP_3). Thus, the time of realization of two numbers A and B determined in MNS on the basis of the principle of ring shift, can be defined by the value of the second element B, and equals

$$T^{(+)}_{MNS_{m_3}} = K_{13} \cdot K_{23} \cdot 3 \cdot \tau_{le} = 12 \cdot 3 \cdot \tau_{le} = 36 \cdot \tau_{le}.$$

Example 2. If $B = (10, 11, 001, 001)$. Then we have:

– for $CP_1(m_1 = 3)$, $b_1 = 2(10)$, $K_{11} = 2$, $K_{21} = 2$ and $K_{11} \cdot K_{21} = 2 \cdot 2 = 4$;

– for $CP_2(m_2 = 4)$, $b_2 = 3(11)$, $K_{12} = 3$, $K_{22} = 2$ and $K_{12} \cdot K_{22} = 3 \cdot 2 = 6$;

– for $CP_3(m_3 = 5)$, $b_3 = 1(001)$, $K_{13} = 1$, $K_{23} = 3$ and $K_{13} \cdot K_{23} = 1 \cdot 3 = 3$;

– for $CP_4(m_4 = 7)$, $b_4 = 1(001)$, $K_{14} = 1$, $K_{24} = 3$ and $K_{14} \cdot K_{24} = 1 \cdot 3 = 3$.

Thus, the time of addition of numbers A and B is determined by the time of realization of operation $(a_2 + b_2) \bmod m_2$ in the second expression CP_2 and equals

$$T^{(+)}_{MNS_{m_2}} = K_{12} \cdot K_{22} \cdot 3 \cdot \tau_{le} = 3 \cdot 2 \cdot 3 \cdot \tau_{le} = 18 \cdot \tau_{le}.$$

The comparative analysis of time of realization of operation of addition of two numbers *A* and *B* in PNS and in MNS is presented. The time $T^{(+)}_{PNS}$ of numbers addition A and B in PNS equals

$$T^{(+)}_{PNS} = (2 \cdot \rho - 1) t_s = (16 \cdot 1 - 1) \cdot 3 \cdot \tau_{le}, \qquad (11)$$

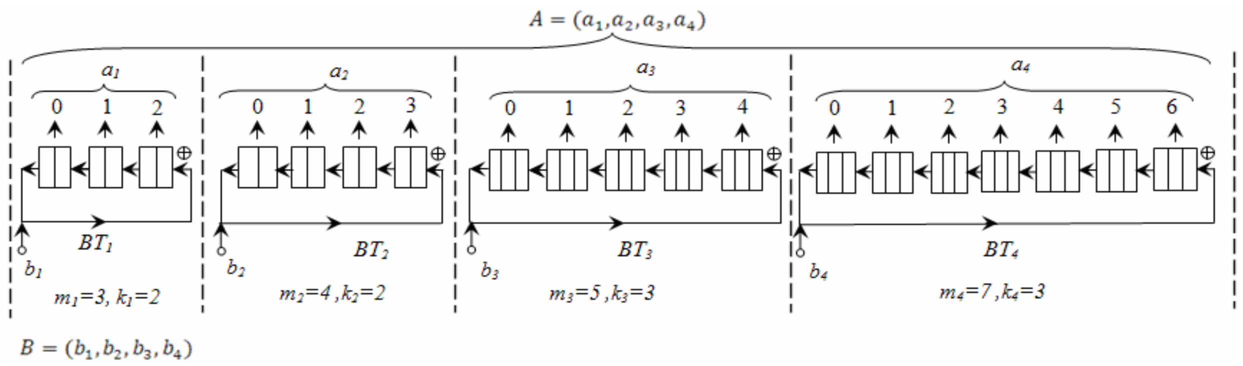

Fig. 3. Simplified chart of operation device in MNS for one byte (l=1) SPCIP

where: $\rho = 8 \cdot 1$ – *l* machine word (number digits of SPCIP for $1 = \overline{1,4}, 8$); $t_S = 3 \cdot \tau_{le}$ – time of summation in $(i+1)$ binary digit of position adder of values $a_{i+1} + b_{i+1} + c_i$, i.e the time of determination of values C_{i+1} and S_{i+1}.

We take into account that due to existing method of two times reduction of maximum time of operation realization of module addition in MNS, we have for PRS:

$$T^{(+)}_{\substack{MNS\\max}} = T^{(+)}_{\substack{MNS\\m_n}} / 2. \qquad (12)$$

We will introduce the coefficient α of relation of time of realization of operation of addition in PNS and in MNS, i.e.

$$\alpha = T^{(+)}_{PNS} / T^{(+)}_{\substack{MNS\\max}} =$$
$$= \frac{(16 \cdot 1 - 1) \cdot 3 \cdot \tau_{le} \cdot 2}{(m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\} \cdot 3 \cdot \tau_{le}} = \qquad (13)$$
$$= \frac{2 \cdot (16 \cdot 1 - 1)}{(m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\}}.$$

Calculation and comparative analysis of time of implementation of arithmetic operations at cryptographic transformations proved high efficiency of application of MBPR which is based on application of PCC, as compared to a method, applied in PNS (tabl. 1).

Table 1

Data of comparative analysis of time of addition operation

$1\ (\rho)$	PNS	MNS			%
	$T^{(+)}_{\Pi CC} / 3 \cdot \tau_B$	m_n	K	$T^{(+)}_{\substack{MCC\\max}} / 3 \cdot \tau_B$	
1 (8)	15	7	3	9	40
2 (16)	31	13	4	24	22

These data are obtained without additional application of existing algorithms, application of which allows to reduce the time of realization of module arithmetic operations. Obtained analytical expressions (4), (5), (6), (7), (9), (10), (13) and the results of time of realization of arithmetic operations in MNS can be used for estimation and comparative analysis of calculable complication of algorithms of RSA of cryptotransformations.

Conclusions of research and perspectives

In this paper new methods of speed increasing of realization of cryptographic transformations in Galois fields are studied, in particular, particularly, the increase of efficiency of RSA of cryptotransformations with the open key. These methods are based on the application of PRS in MNS. The application of fundamental theoretical properties of MNS allows to organize effectively the process of realization of module operations in cryptographic tasks. The method of realization of arithmetic operations in MNS based on PRS, i.e. the method of binary presentation of remainders, is propounded for practical use. The analysis of efficiency of application of these methods and examples of concrete technical realization of module arithmetic operations proves their practicability. Given method of information processing is recommended to be practically used in SPCIP of the real time. Results of the research can be successfully applied in the systems and devices for processing enormous digital information of the real time.

Reference

1. Adibzadeh F. Combination of Multiple Classifiers for Classifying the Diabetic Data / F. Adibzadeh & M.H. Moradi // Biomedical Soft Computing and Human Sciences. – 2009. – Vol. 14, No. 2. – P. 69-80.

2. Iwase, H. Development of General-Purpose Particle and Heavy Ion Transport Monte Carlo Code / H. Iwase, K. Niita, T. Nakamura // Journal of Nuclear Science and Technology. – 2002. – Vol. 39, No. 11. – P. 1142-1151.

3. Automated diagnosis and severity measurement of cyst / A. Banumathi, et al. // Biomedical Soft Computing and Human Sciences. – 2009. – Vol. 14, No. 2. – P. 103-108.

4. Kasami. Theory of encoding / Kasami, Tokura, Ivadari. – M.: Мир, 1978. – 576 c.

5. Shnaier B. Applied Cryptography / B. Shnaier. – M.: Триумф, 2002. – 797 c.

6. Gorbenko I.D. Kriptoanalysis of cryptographic transformations in the groups of points of elliptic curves by the method of Pollarda / I.D. Gorbenko, S.I. Zbitnev, A.A. Polya-

kov // Radioengineering: All-Ukrainian bulletin of science and engineering. – 2001. – Issue 119. – P. 43-50.

7. 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.

8. Akushskiy I.Ya. Machine arithmetic in remainders classes / I.Ya. Akushskiy, D.I. Yuditskiy. – M.: Совю радио, 1968. – 440 с.

9. Kolyada A.A. Modular structures of conveyer method of digital information processing / A.A. Kolyada, I.T. Pak. – Минск: Университет, 1992. – 256 с.

Поступила в редколлегию 3.01.2014

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

МОДЕЛЬ И МЕТОД РЕАЛИЗАЦИИ ЦЕЛОЧИСЛЕННЫХ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ, ВХОДЯЩИХ В КРИПТОАЛГОРИТМЫ RSA

В.А. Краснобаев, А.И. Тыртышников, И.И. Слюсарь, В.Н. Курчанов, С.А. Кошман

С целью уменьшение времени реализации криптографических преобразований RSA в статье рассматриваются методы быстрой обработки информации. Разрабатываемые методы основаны на использовании принципа кольцевого сдвига в модульной системе счисления (МСС). Применение МСС позволило эффективно, с точки зрения повышения быстродействия реализации криптографических преобразований с открытым ключом, организовать процесс реализации модульных целочисленных арифметических операций.

Ключевые слова: *специализированные цифровые устройства и системы, позиционная система счисления, непозиционная система счисления, модулярная система счисления, криптографические преобразования.*

МОДЕЛЬ І МЕТОД РЕАЛІЗАЦІЇ ЦІЛОЧИСЕЛЬНИХ АРИФМЕТИЧНИХ ОПЕРАЦІЙ, ЩО ВХОДЯТЬ ДО КРИПТОАЛГОРИТМІВ RSA

В.А. Краснобаєв, О.І. Тиртишніков, І.І. Слюсарь, В.М. Курчанов, С.О. Кошман

З метою зменшення часу реалізації криптографічних перетворень RSA у статті розглядаються методи швидкої обробки інформації. Методи, що розробляються, засновані на використанні принципу кільцевого зсуву у модулярній системі числення (МСЧ). Застосування МСЧ дозволило ефективно, з точки зору збільшення швидкодії реалізації криптографічних перетворень з відкритим ключем, організувати процес реалізації модульних цілочисельних арифметичних операцій.

Ключові слова: *спеціалізовані цифрові пристрої і системи, позиційна система числення, непозиційна система числення, модулярна система числення, криптографічні перетворення.*