Scientific Issues
Jan Długosz University
in Częstochowa
Mathematics XXI (2016)
123–133
DOI http://dx.doi.org/10.16926/m.2016.21.11

APPLICATION OF MODULAR COMPUTING TECHNOLOGY TO NONLINEAR ENCRYPTION IN CRYPTOGRAPHIC SYSTEMS OF INFORMATIONAL SECURITY

MIKHAIL SELIANINAU

Abstract

In the present paper, we deal with the methodology of nonlinear encryption on the basis of parallel modular computing structures. The use of the minimal redundant modular number system and the interval-modular form of representation of an integer number defined by its modular code creates the computer-arithmetical basis of a cryptographic procedure under consideration. The proposed encryption algorithm is based on the index method of realization of the modular multiplicative operations.

1. Introduction

The creation of effective and secure information systems is one of the priority directions of constructing the protected, dynamically developing information space which covers all the fields of the state activity. Solving the problems of creation of new information security technologies, it is necessary to combine, on the one hand, the high processing rate and transmissions of large volumes of information, and on the other hand, access restrictions to it, providing the required information protection level [1 - 5].

However, in modern information and communication systems the most of the known algorithms of cryptographic information security do not allow performing real time encoding of big data streams. This is substantially caused by the fact that the conventional methods of implementation of these algorithms on the basis of arithmetic of positional number system are insufficiently effective owing to their sequential internal structure.

One of the perspective directions of developing modern cryptography systems of information security (CSIS) consists in the use of nonconventional methods of information processing on the basis of application of the modular computing structures (MCS) possessing the maximum level of internal

parallelism [6 - 10]. In the present article, the implementation of the nonlinear encryption algorithm in modular number systems (MNS) is discussed. The possibility of employing the index representation of Galois fields elements and minimal redundant modular coding of information is considered to increase the speed of cryptographic transformations.

2. The index method of realization of multiplicative operations

The computing algorithms used in the modern CSIS are characterized by the increased content of multiplicative arithmetical operations (modular multiplication and exponentiation of elements of finite fields) in the case of relatively small amount of additive operations. In such systems the index representation of nonzero elements of Galois fields is the most convenient tool for implementation of cryptographic transformations.

The main idea underlying the index data representation (or as it also called "discrete log representation") consists in the possibility of reducing the modular multiplication operation of residues to the modular addition operation [11].

Let us define some prime module p. A set of the smallest non-negative residues of the division of all integer numbers by p forms a complete residue system modulo p, i.e. a set $Z_p = \{0, 1, \ldots, p-1\}$.

Let us designate a set containing nonzero elements of a ring $\mathbf{Z}_p$ as $\mathbf{Z}_p^* = \{1, 2, \ldots p-1\}$. The set $\mathbf{Z}_p^*$ is the reduced system of residues modulo p and represents a cyclic group with respect to multiplication modulo p. This means that there is a generating element g such that any element $\chi \in \mathbf{Z}_p^*$ can be obtained as some degree of an element g, i.e. the set $\{|g^0|_p, |g^1|_p, \ldots, |g^{p-2}|_p\}$ coincides with the set Z_p^* accurate within the permutation of its elements.

The isomorphism of the multiplicative group $\mathbf{Z}_p^*$ and the additive group $\mathbf{Z}_{p-1} = \{0, 1, \ldots, p-2\}$ set by the mapping $\mathbf{G} : \mathbf{Z}_p^* \to \mathbf{Z}_{p-1}$ which assigns to each element $\chi \in \mathbf{Z}_p^*$ the unique element $G(\chi) = \mathrm{ind}_g \chi$ from $\mathbf{Z}_{p-1}$ satisfying the equality

$$|g^{\mathrm{ind}_g \chi}|_p = \chi, \tag{1}$$

plays a significant part in practical realization of the idea of the index method for organization of modular calculations. Here, g is a primitive root modulo p defined as an element of Abelian group $\langle \mathbf{Z}_p^*, \times \rangle \subset \langle \mathbf{Z}_p, + \rangle$ with the order $N = \phi(p) = p - 1$; $\phi(p)$ is the Euler function (the number of nonzero residues of the ring $\mathbf{Z}_p$ mutually prime to p); the element $\mathrm{ind}_g \chi$ of the group $\mathbf{Z}_{p-1}$ is called an index (or a logarithm) of an integer χ to the base g modulo p.

The index representation of the nonzero elements of the field $GF(p)$ is suitable for performance of multiplicative operations as well as operations inverse to them [6]. According to (1), in the case of prime p for any $\alpha, \beta \in \mathbf{Z}_p^*$ the following relation is true

$$|\alpha\beta|_p = |g^{\operatorname{ind}_g |\alpha\beta|_p}|_p = |g^{|ind_g\alpha + \operatorname{ind}_g \beta|_{p-1}}|_p. \tag{2}$$

Thus, the multiplication modulo a prime p can always be reduced to modular addition because of the isomorphism of multiplicative group $\mathbf{Z}_p^*$ and additive index group $\mathbf{Z}_{p-1}$. According to (2), in order to obtain $|\alpha\beta|_p$ it is enough to determine the indices $\operatorname{ind}_g \alpha$ and $\operatorname{ind}_g \beta$ of the operands α and β, add them modulo $p-1$ and then transform the resulting residue $\operatorname{ind}_g |\alpha\beta|_p = |\operatorname{ind}_g \alpha + \operatorname{ind}_g \beta|_{p-1}$ to the desired product $|\alpha\beta|_p$.

For small value of the module p, the direct and inverse transformations of the residues χ and $\operatorname{ind}_g \chi$ ($\chi \in \mathbf{Z}_p$) corresponding to the mappings $\mathbf{G} : \chi \to \operatorname{ind}_g \chi$ and $\mathbf{G}^{-1} : \operatorname{ind}_g \chi \to \chi$ in practice are easily carried out by the look-up table method. Since the volume of the tables required for transformations is about 10 times less than it is for the table of residue multiplication modulo p, then a considered method of modular multiplication with the use of indices appears more efficient than a direct table method, especially with increase of the value of module p. At the same time, the permitted values of the chosen MNS bases are majorized by a threshold allowing the application of tables, for example, by 2^{16}.

In recent years, the comprehensive use of the algebraic systems defined in Galois' fields is one of the most perspective directions in the development of modern CSIS. Therefore, the index method of organization of the modular computation (see (2) and (3)) is of the special interest from the practical point of view, first of all, for effective realization of cryptological procedures in the MNS.

3. The computer-arithmetical basis of modular computing technology

At the present time exists a situation when a conventional data representation and the use of conventional arithmetic of position number systems cease to meet the increased requirements for the CSIS performance. One of the ways to improve a CSIS is the transition to the unconventional computing arithmetic, i.e. by performing all the computations using a MNS [6–10]. The unique property of MNS to carry out the intrinsic decomposition of basic algebraic systems into components of smaller complexity independent from each other caused the wide use of modular arithmetic (MA) in modern computer science and its applications as effective mathematical tool for

mapping of computing processes to high-speed parallel pipeline architectures [6, 7, 12–17].

A classic MNS on the set of integers $\mathbf{Z}$ is determined by means of pairwise relatively prime modules $m_1, m_2, \ldots, m_k$ $(k \geq 2)$. In the given MNS, the number $X \in \mathbf{Z}$ is represented as $X = (\chi_1, \chi_2, \ldots, \chi_k)$, where $\chi_i = |X|_{m_i}$; we shall designate through $|x|_m$ the element of the set $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$ that is congruent to x modulo m. In the nonredundant MNS with the bases $m_1, m_2, \ldots, m_k$ it is possible to code at most $M_k = \prod_{i=1}^{k} m_i$ integers. At the same time, the set $\mathbf{Z}_{M_k} = \{0, 1, \ldots, M_k - 1\}$ is usually used as a range of MNS.

In the MNS with the bases $m_1, m_2, \ldots, m_k$ the modular operations (addition, subtraction and multiplication without overflow check) on any two integers A and B, represented by means of modular codes (MC): $A = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, $B = (\beta_1, \beta_2, \ldots, \beta_k)$ $(\alpha_i = |A|_{m_i}, \beta_i = |B|_{m_i}, i = 1, 2, \ldots, k)$, are carried out independently for each base, i.e. by the rule

$$A \circ B = (\alpha_1, \alpha_2, \ldots, \alpha_k) \circ (\beta_1, \beta_2, \ldots, \beta_k) =$$

$$= (|\alpha_1 \circ \beta_1|_{m_1}, |\alpha_2 \circ \beta_2|_{m_2}, \ldots, |\alpha_k \circ \beta_k|_{m_k}) \quad (\circ \in \{+, -, \times\}. \tag{3}$$

The natural internal parallelism of MNS caused by the lack of interdigit carry propagation during performance of modular operations (3) holds a central position in all the advantages of MA.

The decoding mapping $\mathbf{\Phi}_{MNS} : \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \ldots \times \mathbf{Z}_{m_k} \to \mathbf{D}$ for the MNS with a range $\mathbf{D} = \mathbf{Z}_{M_k}$ which associates the MC $(\chi_1, \chi_2, \ldots, \chi_k)$ with an element $X \in \mathbf{D}$ can be realized according to the Chinese Remainder Theorem [6, 7] by means of the relation

$$X = \sum_{i=1}^{k-1} M_{i,k-1} |M_{i,k-1}^{-1} \chi_i|_{m_i} + I(X) M_{k-1}, \tag{4}$$

where $M_{i,k-1} = M_{k-1}/m_i$, $M_{k-1} = \prod_{i=1}^{k-1} m_i$; $I(X)$ is an integral characteristic of MC called an interval index (II) of a number X with respect to the modules $m_1, m_2, \ldots, m_k$; $|c^{-1}|_m$ designates the multiplicative inversion of an integer c modulo m which is defined as an element d of a ring $\mathbf{Z}_m$ such that $|cd|_m = 1$. For any c relatively prime to m the value $d = |c^{-1}|_m$ always exists and is unique. The expression (4) is called an interval-modular form (IMF) of an integer X [6, 7] .

In the classical MNS the calculation of an II $I(X)$ demands the application of the general algorithm for generating the integral characteristics of MC which is quite difficult and labor-consuming [7, 18]. As is generally known, it is possible to improve significantly the arithmetic properties of MNS and to optimize the algorithms of MA by introducing the so-called minimal additional redundancy which is carried out by some reduction of

the effective range of MNS [6, 7, 12, 13]. The minimal redundant modular coding $\mathbf{\Phi}_{MRMNS} : \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \ldots \times \mathbf{Z}_{m_k} \to \mathbf{D}$ provides the use of the range $\mathbf{D}$ with a cardinal number $|\mathbf{D}| < M_k$.

For many computer applications including also most of modern cryptological algorithms it is enough to use as basic the version of minimal redundant MA (MRMA) oriented on operating only with non-negative integers. In this case, for the redundant MNS a set $\mathbf{Z}_M = \{0, 1, \ldots, M-1\}$ is usually applied as a range $\mathbf{D}$, where $M = m_0 M_{k-1}$, m_0 is a fixed natural number.

The required configuration of minimum redundant MNS (MRMNS) is achieved by the choice of the kth module m_k satisfying a condition $m_k \geq m_0 + \rho$, where

$$\rho = \left\lfloor \sum_{i=1}^{k-1} \frac{m_i - 1}{m_i} \right\rfloor = k - 1 - \left\lceil \sum_{i=1}^{k-1} \frac{1}{m_i} \right\rceil \leq k - 2 \tag{5}$$

represents the maximum value of the rank characteristic $\rho_{k-1}(X)$ determined by the equality

$$|X|_{M_{k-1}} = \sum_{i=1}^{k-1} M_{i,k-1} |M_{i,k-1}^{-1} \chi_i|_{m_i} + \rho_{k-1}(X) M_{k-1}$$

(the designations $\lfloor x \rfloor$ and $\lceil x \rceil$ are used for the nearest to x integers at the left and at the right, respectively). The minimal redundancy is attained in the case when the equality $m_k - m_0 - \rho = |m_k - \rho|_2$ holds [7, 12, 13].

At the same time, the calculation of the II $I(X)$ of a number $X \in \mathbf{D}$ becomes extremely simple since its value is completely defined by the so-called computer II $\hat{I}_k(X) = |I(X)|_{m_k}$ and is reduced to summation of a set of k residues modulo m_k. The following relation is true:

$$I(X) = \begin{cases} \hat{I}_k(X) & \text{if } \hat{I}_k(X) < m_0; \\ \hat{I}_k(X) - m_k & \text{if } \hat{I}_k(X) \geq m_k - \rho, \end{cases} \tag{6}$$

where the residue $\hat{I}_k(X)$ is determined according to the calculation relations

$$\hat{I}_k(X) = \left| \sum_{i=1}^{k} R_{i,k}(\chi_i) \right|_{m_k}; \tag{7}$$

$$R_{i,k}(\chi_i) = \left| -\frac{\chi_{i,k-1}}{M_{k-1}} \right|_{m_k} (i \neq k), \quad R_{k,k}(\chi_k) = \left| \frac{\chi_k}{M_{k-1}} \right|_{m_k}. \tag{8}$$

A redundancy of modular coding is specified by the relation

$$R_{MNS} = 1 - \frac{\log |\mathbf{Z}_M|}{\log |\mathbf{Z}_{M_k}|} = 1 - \frac{\log M}{\log M_k} = \frac{\log (m_k / m_0)}{\log M_k}.$$

Taking into account (5), the lower bound of the input redundancy is assigned by the formula

$$R_{MNS,min} = \frac{\log\left(m_k/(m_k - k + 2)\right)}{\log M_k}$$

and approaches zero with the increase of cardinality of the MNS range.

In spite of the fact that the input additional redundancy is very small, just it allows us to simplify significantly the algorithms of performance of nonmodular operations, first of all, the operations of transformation and expansion of MC. It is seen from the relations (6)–(8) that in comparison with conventional (nonredundant) configurations of the MA a minimal redundant modular coding allows us to attain an essentially new level of optimization of nonmodular procedures on such qualitative characteristics as performance and computational burden. This is caused by the fact that the nonmodular procedures synthesized on the basis of IMF (4) use an interval index which is calculated by means of the simple relations and is formed precisely, without an error inherent in the calculation of the rank characteristic [6, 7]. The main advantages of applied modular computing technology for the construction of CSIS are determined by the reason mentioned above, and a MRMA represents an effective computer-arithmetical basis for the realization of various cryptographic tasks.

4. The nonlinear algorithm of symmetric encryption in the MNS

Let us consider the realization of nonlinear encryption of a high-speed data flow with the use of minimal redundant modular coding and index representation of nonzero elements of Galois fields.

The input sequence represented by a set of binary digits is divided into blocks. Thus, each such a block of length L represents some non-negative integer number A from the range $[0, 2^L)$, $A = (a_{L-1}\ a_{L-2}\ \ldots\ a_1\ a_0)_2$, where $a_j \in \mathbf{Z}_2$ $(j = 0, 1, \ldots, L-1)$.

Let us set the basic MRMNS with the bases $m_1, m_2 \ldots, m_k$ and the range $\mathbf{Z}_M$. At the same time the modules m_i $(i = 1, 2, \ldots, k)$ are chosen to satisfy the relation $M > 2^L$. A primitive element $g_i \in \mathbf{Z}_{m_i}$, i.e. the generator of degree $m_i - 1$, is chosen for each basis m_i. Thus, a set of all primitive elements over the bases of the MRMNS can be interpreted as the MC $(g_1, g_2, \ldots, g_k)$ of some number $G \in \mathbf{Z}_M$ $(g_i = |G|_{m_i}, i = 1, 2, \ldots, k)$ which will be called a primitive number of MRMNS. The combination of the chosen modules of MRMNS and the primitive number represent the confidential information in the CSIS.

The number $A \in \mathbf{Z}_{2^L}$ corresponding to the information block is uniquely coded in the MRMNS by the set of residues $\alpha_i = |A|_{m_i}$ modulo m_i $(i =$

$1, 2, \ldots, k)$, i.e. $A = (\alpha_1, \alpha_2, \ldots, \alpha_k)$. Transformation of the positional code of an integer A to the minimal redundant MC (MRMC) is carried out within the parallel and pipelined MCS of look-up table type [6, 7]. Further, a procedure for the encryption is applied to the block represented in MRMC. For this purpose, at first, the L-bit key sequence B has to be generated by means of pseudorandom sequence generator.

The process of encrypting represents the imposition of key sequence over the information block in MRMNS. This procedure can be considered as realization of some transformation $C = |F(A, B)|_{M_k}$ which is carried out in parallel over the bases $m_1, m_2, \ldots, m_k$. In the MRMNS the various types of linear and nonlinear cryptographic functions and their combinations can be realized, for example $C = |A + B|_{M_k}$, $C = |A \cdot B|_{M_k}$, $C = |A^B|_{M_k}$. The resulting cryptogram is of the form $C = (\gamma_1, \gamma_2, \ldots, \gamma_k)$, $\gamma_i = |C|_{m_i}$ $(i = 1, 2, \ldots, k)$, $C \in \mathbf{Z}_M$.

Let us consider the realization of the procedure of encrypting the open data block with the use of multiplicative and exponentiation operations over the elements of finite fields in MRMNS. The choice of such a cryptographic procedure is determined by the fact that it is not linear and a decryption of the received information requires calculation of a discrete logarithm that is very labor-consuming task.

Let the nonlinear cryptographic transformation be set by the relationship $C = |A \cdot G^B|_{M_k}$, where A is the coded data block, B is the key sequence, G is the chosen predetermined primitive number. Then the MRMC of the cryptogram C is formed according to the expression

$$\gamma_i = |A \cdot G^B|_{m_i} = |\alpha_i \cdot g_i^B|_{m_i} \ (i = 1, 2, \ldots, k). \tag{9}$$

Since $(g_i, m_i) = 1$, then according to Fermat's theorem from the number theory [11] we have $|g_i^B|_{m_i} = |g_i^{|B|_{m_i - 1}}|_{m_i}$.

Therefore,

$$\gamma_i = |\alpha_i \cdot g_i^{\beta_i}|_{m_i}, \tag{10}$$

where $\beta_i = |B|_{m_i - 1}$ $(i = 1, 2, \ldots, k)$.

To calculate the residues γ_i we will use the index method of realization of multiplicative operations in the ring $\mathbf{Z}_{m_i}$. If the residue α_i is nonzero, then in accordance with (1) and (2) we receive

$$\gamma_i = |g_i^{\operatorname{ind}_{g_i} \gamma_i}|_{m_i} = |\alpha_i \cdot g_i^{\beta_i}|_{m_i} = |g_i^{\operatorname{ind}_{g_i} \alpha_i} \cdot g_i^{\beta_i}|_{m_i} =$$

$$= |g_i^{\operatorname{ind}_{g_i} \alpha_i + \beta_i}|_{m_i} = |g_i^{|\operatorname{ind}_{g_i} \alpha_i + \beta_i|_{m_i - 1}}|_{m_i}.$$

Thus, a nonlinear encrypting in the MRMNS is reduced to calculation of an index

$$\operatorname{ind}_{g_i} \gamma_i = |\operatorname{ind}_{g_i} \alpha_i + \beta_i|_{m_i - 1} \tag{11}$$

and its following conversion to the residue γ_i $(i = 1, 2, \ldots, k)$.

If the tables of indices and anti-indices are previously created by the rules $TInd_i[\chi] = \operatorname{ind}_{g_i} \chi$ $(\chi \in \mathbf{Z}^*_{m_i})$ and $TAInd_i[s] = |g_i{}^{|s|_{m_i-1}}|_{m_i}$ $(s = 0, 1, \ldots, 2(m_i - 2))$, respectively, then according to (11) an encrypting procedure modulo m_i requires one reading the table $TInd_i$ for the specification of an index $\operatorname{ind}_{g_i} \alpha_i$, calculation of the sum $s = \operatorname{ind}_{g_i} \alpha_i + \beta_i$ and receiving the resulting residue γ_i by the table $TAInd_i$.

The considered operations are performed in parallel over all the modules of the MRMNS. The resulting MRMC $(\gamma_1, \gamma_2, \ldots, \gamma_k)$ of the cryptogram C enters into a communication channel.

Let us consider a decrypting procedure which is also carried out in the MRMNS. It follows from (9) that for decrypting the cryptogram C it is necessary to create the inverse key $B^{-1} = (\beta_1^{-1}, \beta_2^{-1}, \ldots, \beta_k^{-1})$ by the known key B which is represented by a set of residues $(\beta_1, \beta_2, \ldots, \beta_k)$ (see (10)). Each value of β_i^{-1} $(i = 1, 2, \ldots, k)$ is calculated based on the following congruence condition $|g_i^{\beta_i} \cdot g_i^{\beta_i^{-1}}|_{m_i} = 1$. Thus, $|\beta_i + \beta_i^{-1}|_{m_i-1} = 0$, i.e. $\beta_i^{-1} = m_i - 1 - \beta_i$. The component of the MRMC of the information block A is decoded according to the formula

$$\alpha_i = |\gamma_i \cdot g_i^{\beta_i^{-1}}|_{m_i} \ (i = 1, 2, \ldots, k). \tag{12}$$

Therefore, similar to operation of nonlinear encrypting, the decrypting operation is reduced to calculation of the index

$$\operatorname{ind}_{g_i} \alpha_i = |\operatorname{ind}_{g_i} \gamma_i + \beta_i^{-1}|_{m_i-1} \tag{13}$$

and its following conversion to the residue α_i.

The positional code of a number A can be computed by its MRMC $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ according to the formula (4) within the parallel and pipelined MCS of the table type [6, 7]. Thus, the proposed multiplicative encrypting algorithm for the CSIS allows us to attain the essential increase in efficiency at the acceptable volume of the tabular memory due to the code parallelism and the tabular nature of the MA, the performance of realization of nonmodular operations of code conversions as well as simplicity of calculating the index of a finite field element.

5. The realization of the modular model of CSIS

The choice of the type of cryptographic protection for the concrete information system depends significantly on its features and should base on the comprehensive analysis of requirements imposed on the CSIS. The realization of cryptographic algorithms can be carried out by means of the software, hardware or firmware. The main advantage of the software realization is its flexibility, i.e. the possibility of fast modification of cryptographic

algorithms. The main shortcoming consists in the essential smaller performance in comparison with the hardware; however this difference decreases with the development of computer technologies. The firmware combines the advantages of thesoftware and hardware realization.

The designed algorithm of nonlinear encrypting is characterized by the maximum level of unloading of the real time computing process from the labor-consuming calculations which can be realized by means of the look-up tables formed at a stage of preliminary calculations. This gives the possibility to use an extremely simple table-summation configuration of the CSIS which only extracts residues from tabular memory and sums them over the bases of the MRMNS.

The complete private key of the introduced cryptological algorithm consists of the standard private key (the generated pseudorandom sequence) and the secure algorithm information formed by all the possible choice alternatives for operational bases of the MRMNS and the primitive elements corresponding to them. A cryptographical security of the described algorithm is determined by all possible choices of total keys.

For the cryptological algorithm given above the process of creation of the CSIS includes three associated subsystems, namely: generation of total private keys, encryption of the message and decryption of the cryptogram.

The following main procedures are realized in a subsystem of generation of total keys:

1. The choice and storing of the sets of operational bases $m_1, m_2, \ldots, m_k$ for coding the data block of the required length.

2. The choice and storing of the sets of primitive roots $(g_1, g_2, \ldots, g_k)$.

3. The generation of the key $B = (\beta_1, \beta_2, \ldots, \beta_k)$ for encrypting on the basis of the generated pseudorandom sequence.

4. The determining and storing the key $B^{-1} = (\beta_1^{-1}, \beta_2^{-1}, \ldots, \beta_k^{-1})$ inverse to B.

5. The recording of the total keys in the database (the concrete combinations of the optional bases, the corresponding primitive elements, and the keys B and B^{-1}). The separate storage of the selected sets of the operational bases $m_1, m_2, \ldots, m_k$, the primitive roots $(g_1, g_2, \ldots, g_k)$ as well as the keys B and B^{-1} allows us to set up the different combinations of the total keys.

The computation of the MRMC of the information block and its encrypting is implemented in the encryption subsystem. The decryption of the received ciphered block by means of the inverse key and the following conversion of its MRMC to the binary code is performed in the decryption subsystem. The use of the different variants of total private keys allows us to construct the flexible and simply transformed CSIS that permits us

to implement different models of encrypting with the use of the modular principles of information processing.

References

[1] J. Buchmann, *Introduction to Cryptography*. Springer, New York, 2004.

[2] N. Koblitz, *Algebraic Aspects of Cryptography*. Springer, New York, 2004.

[3] D.R. Stinson, *Cryptography. Theory and Practice*. Chapman & Hall/CRC Press, Boca Raton, 2006.

[4] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, Boca Raton, 2008.

[5] W. Mao, *Modern Cryptography. Theory and Practice*. Prentice Hall PTR, Upper Saddle River, NJ, 2003.

[6] A.A. Kolyada, I.T. Pak, *Modular Structures of Pipeline Digital Information Processing*. University Press, Minsk, 1992 (in Russian).

[7] A.F. Chernyavsky, V.V. Danilevich, A.A. Kolyada, M.Y. Selyaninov, *High-speed Methods and Systems of Digital Information Processing*. Belarusian State University Press, Minsk, 1996 (in Russian).

[8] P.V. Ananda Mohan, *Residue Number Systems: Algorithms and Architectures*. Kluwer Academic Publishers, 2002.

[9] A. Omondi, B. Premkumar, *Residue Number Systems: Theory and Implementation*. Imperial College Press, London, 2007.

[10] P. Kornerup, D.W. Matula, *Finite Precision Number Systems and Arithmetic*. Cambridge University Press, Cambridge, 2010.

[11] I.M. Vinogradov, *Fundamentals of Number Theory*. Nauka, Moscow, 1981 (in Russian).

[12] M. Selyaninov, *Modular technique of parallel information processing*. Scientific Issues of Jan Długosz University in Częstochowa, Mathematics **XIII** (2008), 43–52.

[13] M. Selyaninov, *Construction of modular number system with arbitrary finite ranges*. Scientific Issues of Jan Długosz University in Częstochowa, Mathematics **XIV** (2009), 105–115.

[14] M. Selianinau, *High- speed modular structures for parallel computing in the space of orthogonal projections*. Scientific Issues, Jan Długosz University of Czestochowa, Ser. Technical and IT Education, **V**, (2010), 87-96.

[15] M. Selianinau, *Modular principles of high-speed adaptive filtration of discrete signals*. Scientific Issues, Jan Długosz University of Czestochowa, Ser. Technical and IT Education, **VI**, (2011), 75-84.

[16] M. Selyaninov, *Modular technique of high-speed parallel computing on the sets of polynomials*. Scientific Issues of Jan Długosz University in Częstochowa, Mathematics **XVII** (2012), 69-76.

[17] M. Selyaninov, *Application of modular computing technique for high-speed implementation of cyclic convolution*. Scientific Issues of Jan Długosz University in Częstochowa, Mathematics **XIX** (2014), 213-222.

[18] A.A. Kolyada, M.Y. Selyaninov, *On the formation of the integral characteristics of the codes of residue number systems with the symmetrical range*. Cybernetics **4** (1986), 20–24 (in Russian).

Received: May 2016

Mikhail Selianinau
Jan Długosz University in Częstochowa,
Institute of Technical Education and Safety,
al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
E-mail address: m.selianinov@ajd.czest.pl