NEW DEVELOPMENTS in CIRCUITS, SYSTEMS, SIGNAL PROCESSING, COMMUNICATIONS and COMPUTERS

Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015)

Vienna, Austria
March 15-17, 2015

NEW DEVELOPMENTS in CIRCUITS, SYSTEMS, SIGNAL PROCESSING, COMMUNICATIONS and COMPUTERS

Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015)

Vienna, Austria
March 15-17, 2015

All papers of the present volume were peer reviewed by no less than two independent reviewers. Acceptance was granted when both reviewers' recommendations were positive.

Series: Recent Advances in Electrical Engineering Series | 45

ISSN: 1790-5117
ISBN: 978-1-61804-285-9

NEW DEVELOPMENTS in CIRCUITS, SYSTEMS, SIGNAL PROCESSING, COMMUNICATIONS and COMPUTERS

Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015)

Vienna, Austria
March 15-17, 2015

Modification of the cryptographic algorithms, developed on the basis of nonpositional polynomial notations

Rustem G. Biyashev, Saule E. Nyssanbayeva, Yenlik Ye. Begimbayeva, Miras M. Magzom

***Abstract* —** Cryptographic systems, developed on the basis of nonpositional polynomial notations (NPNs), are called nonconventional, nonpositional or modular. In this paper, models of modified nonconventional encryption systems and digital signature are described. The creation of the model of block encryption system includes the development of a modified nonpositional block encryption algorithm using the analogue of Feistel system and application mode of this modified algorithm. The model of a digital signature based on the scheme of the Digital Signature Algorithm (DSA) and NPNs. Application of NPNs allows creating effective cryptographic systems of high reliability, which enables the confidentiality, authentication and integrity of stored and transmitted information. Synonyms of NPNs – classical notations in residue number system (RNS), polynomial notations systems in RNS, modular arithmetic.

***Keywords* —** cipher mode, digital signature, encryption, nonpositional polynomial notations.

I. INTRODUCTION

THE basis for the creation of the proposed models of cryptosystems are nonconventional systems of encryption and digital signature. These systems are developed on the algebraic approach base, using nonpositional polynomial notations (NPNs) or polynomial notations in residue classes (polynomial RNS). Classical RNS (modular arithmetic) is based on the Chinese remainder theorem, which states that any number can be represented by their remainders (residues) from its division by the base numbers systems, which are formed pairwise coprime numbers [1]-[2]. Then in RNS a positive integer is represented by a sequence of remainders or residues

$$A = \alpha_1, \alpha_2, ..., \alpha_n \qquad (1)$$

The conducting research is funded by the Ministry of Education and Science of the Republic of Kazakhstan (MES RK).

R. G. Biyashev is with the Institute of Information and Computational Technologies of MES RK, 125 Pushkin str., Almaty, 050010, Republic of Kazakhstan. (e-mail: brg@ipic.kz).

S. E. Nyssanbayeva is with the Institute of Information and Computational Technologies of MES RK, 125 Pushkin str., Almaty, 050010, Republic of Kazakhstan (phone: +77017743730, e-mail: sultasha1@mail.ru, snyssanbayeva@gmail.com).

Ye. Ye. Begimbayeva is with the Institute of Information and Computational Technologies of MES RK, 125 Pushkin str., Almaty, 050010, Republic of Kazakhstan (e-mail: enlikb89@gmail.com).

M. M. Magzom is with the Institute of Information and Computational Technologies of MES RK, 125 Pushkin str., Almaty, 050010, Republic of Kazakhstan (e-mail: magzomzn@gmail.com).

from dividing this number by the given positive integer numbers $p_1, p_2, \ldots, p_n$, which are called bases of the system. Numbers α_i are formed in the following way:

$$\alpha_i = A - \left[A / p_i\right] p_i, \; i = \overline{1,n}, \qquad (2)$$

where $\left[A / p_i\right]$ denotes the integer part of the division A by p_i. From (2) follows, that the number α_i of i-th digit of A is the smallest positive remainder of division A by p_i, and $\alpha_i < p_i$. In this case, the formation of each digit number performed independently. According to the Chinese remainder theorem, representation of A in the form of (1) is unique, in case numbers p_i are pairwise coprime. The range of representable numbers in this case is $P = p_1 p_2 \cdots p_n$. Here, similar to a positional number system, the range of representable numbers growing as the product of base numbers, and the digit capacity of the number is growing as the sum of the digit capacity of the same base numbers.

In NPNs (polynomial RNS) bases are used as irreducible polynomials over field $GF(2)$ [3]-[4]. Using NPNs allows reducing the length of the key, to improve durability and efficiency of nonpositional cryptographic algorithms [4]-[5]. Improving the efficiency is provided by the rules of NPNs in which all arithmetic operations can be performed in parallel to the base module NPNs. In developed nonconventional cryptographic algorithms the encryption and formation of digital signature is carried out for an electronic message of the given length. In nonpositional cryptosystems as a criterion of cryptostrength is used cryptostrength of algorithms of encryption and formation of digital signature, which is characterized by a complete secret key. Cryptostrength in this case depends not only on the length of a key sequence, but also on choice of a system of polynomial bases. With the growth of the order of irreducible polynomials with binary coefficients, their number also grows rapidly. Therefore, a wide choice of polynomial bases is possible. Cryptostrength of proposed encryption algorithm which using NPNs significantly increases with the length of the electronic message.

In [3] the arithmetic of nonpositional number systems with polynomial bases and its application to problems of improving reliability are developed. As it is shown, the algebra of polynomials over a field in modulus of the irreducible polynomial over this field is a field and the representation of

the polynomial in the nonpositional form is the only (analogous to the Chinese remainder theorem for polynomials). The rules of performing arithmetic operations in NPNs and restoring the polynomial by its residues are defined. According to the Chinese remainder theorem, all working base numbers should be different.

II. Nonpositional polynomial notations

A. Constructing of NPNs

The process of forming of NPNs for an electronic message M of the given length N bits is as follows. Polynomial bases with binary coefficients are selected

$$p_1(x), p_2(x),\ldots, p_S(x), \quad (3)$$

where $p_i(x)$ - irreducible polynomial with binary coefficients of degree m_i respectively, $i=\overline{1,S}$. These bases are called working base numbers. The main working range in NPNs is a polynomial $P(x)=p_1(x)\,p_2(x)\cdots p_S(x)$ of the degree $m=m_1+m_2+\ldots+m_S$. According to the Chinese remainder theorem, all the base numbers must be different even if their degrees are equal.

In NPNs any polynomial $F(x)$, which degree is less than m, has a unique nonpositional representation in a form of sequence of residues of its division by the working base numbers $p_1(x), p_2(x),\ldots, p_S(x)$:

$$F(x)=(\alpha_1(x),\alpha_2(x),\ldots,\alpha_S(x)), \quad (4)$$

where $F(x)=\alpha_i(x)\left(mod\, p_i(x)\right)$, $i=\overline{1,S}$.

In NPNs a message (or its block) of the given length N bits is represented as follows. It is interpreted as a sequence of remainders of division of some polynomial (let us denote it as $F(x)$) by working base numbers $p_1(x), p_2(x),\ldots, p_S(x)$ of degree not greater than N, that is, in the form of (4). Each working base number should have a degree not exceeding value of N. These base numbers are selected from all irreducible polynomials with degrees varying from m_1 to m_S, providing that the following equation is satisfied [6]:

$$k_1m_1+k_2m_2+\ldots+k_Sm_S=N. \quad (5)$$

Here $0\le k_i\le n_i$ are unknown coefficients and the number of selected irreducible polynomials of degree m_i. One certain set of these coefficients is one of the solutions of (5) and specifies one system of working base numbers, n_i is the number of all irreducible polynomials of degree m_i, $1\le m_i\le N$, $S=k_1+k_2+\ldots+k_S$ is a number of selected working base numbers. In the system of working bases the order of these bases is also taken into account.

Equation (5) defines the number S of working bases, which produce residues that covers the length N of the given message. Complete residue systems modulo polynomials of degree m_i include all polynomials with the degree not exceeding m_i-1. The representation of polynomials of degree m_i-1 requires m_i bits.

As shown in Table I, with growth of degrees of irreducible polynomials, their amount rapidly increases, and, as a result, the number of solutions of (5) also considerably increases.

Calculations for finding irreducible polynomials were conducted in two ways: by dividing a particular polynomial to other polynomials and using analog of the sieve method for finding prime numbers. The results of these calculations matched by both quantitative and qualitative composition.

The properly checked table of irreducible polynomials over field $GF(2)$ for the degrees from 1 to 15 was published in [7].

TABLE I. Dependence of number of irreducible polynomials on their degree

Degree of Irreducible Polynomials	Number of Irreducible Polynomials
1	1
2	1
3	2
4	3
5	6
6	9
7	18
8	30
9	56
10	99
11	186
12	335
13	630
14	1161
15	2182
16	4080
17	7710
18	14532
19	27594
20	52377

Remainders $\alpha_1(x),\alpha_2(x),\ldots,\alpha_S(x)$ are selected in the way where binary coefficients of reminder $\alpha_1(x)$ correspond to the first l_1 bits of the message, the next binary coefficients of reminder $\alpha_2(x)$ correspond to the next l_2 bits, etc., and binary coefficients of reminder $\alpha_S(x)$ correspond to the last l_S binary bits.

ISBN: 978-1-61804-285-9

The positional representation of $F(x)$ is reconstructed from its form (4) [3]-[4]:

$$F(x)=\sum_{i=1}^{S}\alpha_i(x)B_i(x),\ B_i(x)=\frac{P_S(x)}{p_i(x)}M_i(x),\ i=\overline{1,S}. \qquad (6)$$

Polynomials $M_i(x)$ are chosen so as to satisfy the congruence in (6).

B. Hashing an electronic message in NPNs

In NPNs it is possible to hash (compress) an electronic message of the given length N to the length of N_k bits [3]-[4]. This is done by introducing redundancy, that is, the message in NPNs is expanded by redundant bases $p_{S+1}(x), p_{S+2}(x),\ldots, p_{S+U}(x)$. The system of redundant bases is formed independently of the choice of working base numbers $p_1(x), p_2(x),\ldots, p_S(x)$. Note that some bases among the U redundant bases may coincide with some of the working base numbers.

Selection of redundant bases is carried out by analogy with a choice of working bases. These bases are chosen randomly from all irreducible polynomials of degree not exceeding the value of N_k. Denote the degree and the number of irreducible polynomials used in their selection as $a_1, a_2,\ldots, a_U$ and $d_1, d_2,\ldots, d_U$ respectively. The number of selected redundant bases in this case is determined from the equation (the analogue of (5)):

$$t_1a_1+t_2a_2+\ldots+t_Ua_U=N_k, \qquad (7)$$

where $0\le t_j\le d_j$, $0\le a_j\le N_k$, $j=\overline{1,U}$, t_j - the number of selected redundant bases of degree a_j, $U=t_1+t_2+\ldots+t_U$ – the number of selected redundant bases, which produce residues that covers the hash value of length N_k. Solution of the (7) defines a single system of redundant bases.

Further redundant residues (remainders) $\alpha_{S+1}(x),\alpha_{S+2}(x),\ldots,\alpha_{S+U}(x)$ are calculated by dividing reconstructed polynomial $F(x)$ by redundant bases $p_{S+1}(x), p_{S+2}(x),\ldots, p_{S+U}(x)$. Then the hash value $h(F(x))$ of length N_k bits can be interpreted as a sequence of these residues:

$$h(F(x))=(\alpha_{S+1}(x),\alpha_{S+2}(x),\ldots,\alpha_{S+U}(x)), \qquad (8)$$

where $h(F(x))\equiv\alpha_{S+j}(x)\,mod\,(p_{S+j}(x))$, $j=\overline{1,U}$. The sum of the lengths of redundant residues is the length of hash value.

III. Nonconventional symmetric encryption algorithm

The encryption algorithm of an electronic message of the given length N bits based on NPNs includes the following steps. Initially nonpositional polynomial number system is formed (this procedure is described in Subsection A). Then a key (pseudo-random) sequence is generated, and the plaintext is encrypted.

Suppose that for encryption from the set of all irreducible polynomials of degree not exceeding N a system of working base numbers (3) is selected. The message of length N bits is represented as a sequence of residues (4) from the division of a polynomial on the working bases.

Then the encryption key length of N bits is also interpreted as a system of residues $\beta_1(x),\beta_2(x),\ldots,\beta_S(x)$, but from division of other polynomial $G(x)$ by the same working base numbers:

$$G(x)=(\beta_1(x),\beta_2(x),\ldots,\beta_S(x)), \qquad (9)$$

where $G(x)\equiv\beta_i(x)(mod\ p_i(x))$, $i=\overline{1,S}$.

After encrypting the message $F(x)$ using the key $G(x)$ a cryptogram is obtained. This cryptogram is considered as a function $H(x)$:

$$H(x)=(\omega_1(x),\omega_2(x),\ldots,\omega_S(x)), \qquad (10)$$

where $H(x)\equiv\omega_i(x)(mod\ p_i(x))$, $i=\overline{1,S}$. In (10) the first l_1 bits of cryptogram are assigned to binary coefficients of remainder $\omega_1(x)$, l_2 bits of cryptogram are assigned to binary coefficients of remainder $\omega_2(x)$, etc. The last l_s bits of cryptogram are assigned to binary coefficients of the last remainder $\omega_s(x)$.

In software implementation of this nonconventional algorithm of encryption of the message the nonconventional method will be used [8]. The usage of different methods allows obtaining different encryption models.

Key length is one of the system strength indicators. In nonconventional encryption the strength of cryptographic algorithm characterized by complete (private) key is used as a cryptostrength criterion. In this algorithm a complete key is the polynomial $G(x)$ and the certain set of working base numbers chosen from the set of irreducible polynomials whose degree does not exceed N [9].

Statement 1. The cryptostrength of an encryption algorithm developed on the basis of NPNs is determined by total number of possible and distinct from each other variants of choice of key sequences and systems of working base numbers.

To prove the above fact, the combination number of choice of base numbers for each base number degree determined by the (5) is calculated. Then the number of combinations of

system forming from S base numbers with the degrees $m_1, m_2, ..., m_S$ with allowance for their arrangement is determined by expression

$$(k_1 + k_2 + ... + k_S)!C_{n_1}^{k_1} C_{n_2}^{k_2} \cdots C_{n_S}^{k_S}.$$

The encryption is performed by imposing on the message of the generated key sequence of the same length N bits. Therefore for encryption the choice of one system from S base numbers is defined by the formula:

$$(k_1 + k_2 + ... + k_S)!C_{n_1}^{k_1} C_{n_2}^{k_2} \cdots C_{n_S}^{k_S}. \quad (11)$$

Then the encryption cryptostrength of the message of length N bits is determined as the inverse value for (11):

$$p_{kr} = 1/(2^N \sum_{k_1, k_2, ..., k_S} (k_1 + k_2 + ... + k_S)!C_{n_1}^{k_1} C_{n_2}^{k_2} \cdots C_{n_S}^{k_S}). \quad (12)$$

In expression (12) the summation is performed over all possible combinations of coefficients $k_1, k_2, ..., k_S$ satisfying the (5).

Nontraditional method in which the elements of the sequence of residues $\omega_1(x), \omega_2(x), ..., \omega_S(x)$ in the cryptogram are the smallest remnants of division of products $\alpha_i(x)\beta_i(x)$ by respective bases $p_i(x)$ is used for encryption if multiplication operation is used as the function $H(F(x), G(x))$ [8]:

$$\alpha_i(x)\beta_i(x) \equiv \omega_i(x) (\text{mod } p_i(x)),\ i = \overline{1, S}. \quad (13)$$

For deciphering cryptogram by the known key $G(x)$ for each value $\beta_i(x)$ the calculation of the reverse (inverse) polynomial $\beta_i^{-1}(x)$ is made as follows from (13) provided that the following equation is satisfied:

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1 (\text{mod } p_i(x)),\ i = \overline{1, S}. \quad (14)$$

The result is the polynomial $G_i^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \ldots, \beta_S^{-1}(x))$ inverse to the polynomial $G(x)$. Then the elements of the sequence of residues (4) in accordance with (13) and (14) are restored as compared with:

$$\alpha_i(x) \equiv \beta_i^{-1}(x)\omega_i(x) (\text{mod } p_i(x)),\ i = \overline{1, S}.$$

Thus, in the present model of the encryption algorithm of electronic message of the specified length N bits in NPNs, the complete key is:

- the chosen system of polynomial working bases $p_1(x), p_2(x), \ldots, p_S(x)$;
- the key $G(x) = (\beta_1(x), \beta_2(x), \ldots, \beta_S(x))$;
- the key $G_i^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \ldots, \beta_S^{-1}(x))$ needed for deciphering and inverse to $G(x)$.

Examples of determination of cryptostrength by the formula (12).

1. Key length equals 100 bits: system of base numbers includes 6 irreducible polynomials of degree 16 and 1 irreducible polynomial of degree 4. S=7. For this system of base numbers we obtain $p_{kr} \approx 10^{-53}$.

2. Key length equals 200 bits: system of base numbers includes 12 irreducible polynomials of degree 16 and 1 irreducible polynomial of degree 8. S=13. $p_{kr} \approx 10^{-106}$.

3. Key length equals 128 bits: system of base numbers includes 8 polynomials of degree 16. S=8. $p_{kr} \approx 10^{-69}$.

4. Key length equals 256 bits: system of base numbers includes 16 polynomials of degree 16. S=16. $p_{kr} \approx 10^{-135}$.

Cryptostrength of AES standard for the keys of length 128 and 256 bits is $2^{-128} \approx 10^{-38}$ and $2^{-256} \approx 10^{-77}$, respectively. Cryptostrength of encryption algorithms is also by tens of orders greater (examples 3 and 4).

The State Standard of the Republic of Kazakhstan ST RK 1073-2007 specifies the 1st, 2nd, 3rd and 4th security levels for the means of cryptographic protection of information. Key length of symmetric algorithms for these levels should be at least 60, 100, 150 and 200 bits respectively [10]. Minimum cryptostrength values for the keys of 100 and 200 bits equal to $2^{-100} \approx 10^{-29}$ and $2^{-200} \approx 10^{-60}$, respectively. As is seen from examples 1 and 2, the cryptostrength of nonconventional encryption is by tens of orders greater.

Thus, use of NPNs in creation of symmetric encryption algorithms help to achieve the required levels of reliability specified by the Standard ST RK 1073-2007 with significantly shorter secret key lengths. Nonpositional nature of notations also helps to provide high performance and prevent propagation of errors.

IV. Modeling of the System of Nonconventional Block Encryption

Developed nonconventional encryption algorithm is the basis for solving the problems of cryptography.

For the purpose of its practical application, the scientific research is carried out on the development of:

- modified algorithm based on a Feistel network to improve the statistical characteristics of the nonpositional cryptogram (10) - (13);
- models of operation modes of the modified nonconventional encryption algorithm are performed.

A. Modification using the Feistel encryption scheme

If the length of the full key encryption in NPNs larger, then there are more choices of systems of working base numbers. In this regard, one can use several models of Feistel scheme.

Models could differ by the number of sub-blocks as well as by the number of rounds (or iterations). The functions of cryptographic transformation of sub-blocks in scheme models may also be different.

The input data block may be divided into different even number of sub-blocks according to its length. On each step of the iteration the possible variants of key sequences using and systems of working base numbers will be researched.

In computer modeling, the cryptostrength of the developed modified algorithms will be analyzed.

B. Operating modes of the modified block cipher

There is a potential possibility of information leaks about recurring parts of data which encrypted on the one and the same key, in view of the fact that the block ciphers encrypt data by fixed-size blocks [2]-[6], [11]. Therefore, for using block cipher algorithms various modes are developed [12]. Encryption modes in the process of cryptographic transformations are used to provide the required conditions for encrypted messages. The main condition is that the encryption result of each block must be unique regardless of the encrypted data.

It is supposed to consider one of the cipher operation modes models - the Cipher Block Chaining (CBC) mode. In CBC mode, each block of plaintext is XORed with the previous block of the cryptogram and then the result is being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. Moreover, for computing the first ciphertext block is using a random initialization vector (IV). It is necessary to guarantee the uniqueness of IVs for each encryption in order to identical two messages is not encrypted identically. The message that encrypted in CBC mode can only sequentially decrypt, starting with the first block. IVs are also needed to decrypt the data.

The modification of the CBC mode is Propagating cipher-block chaining (PCBC). The main difference of this mode from the CBC is that changes in the ciphertext propagate to all blocks when decrypting, as well as when encrypting. Changing one bit of plaintext affects all subsequent blocks of ciphertext. Distortion of one bit in the cryptogram leads to damage of all subsequent plaintext blocks.

Software implementation of the proposed models of the CBC mode allows choosing the required operating mode of the modified algorithm based on NPNs.

V. Asymmetric System of Digital Signature Based on NPNs

The ElGamal digital signature (DS) scheme is based on the complexity of the problem of computing discrete logarithms in the finite field [13]-[14]. On the basis of this scheme the standards of digital signature DSS (Digital Signature Standard, USA, 1994) and GOST R 34.10-94 (Russian, 1994) are constructed [15]-[16]. Standard DSS based on the hashing algorithm SHA and formation algorithm of the digital signatures DSA (Digital Signature Algorithm). This algorithm has been accepted in 1994 as the USA standard of digital signature and is the variation of a digital signature of the ElGamal scheme and K. Schnorr. The length of the signature in DSA system is 320 bits.

DSA algorithm is a "classic" example of DS scheme based on the using of hash functions and asymmetric encryption algorithm. The strength of the system in general depends on complexity of finding discrete logarithms in the finite field.

The essence of DSA electronic signature scheme is the following.

Let sender and recipient of the electronic document in computation of digital signature use large prime integers p and q: $2^{L-1} < p < 2^L$, $512 \le L \le 1024$, L multiple of 64, $2^{159} < q < 2^{160}$, q - prime divisor of $(p-1)$ and $g = h^{(p-1)/q} mod\ p$, where h - arbitrary integer, $1 < h < p-1$ such that $h^{\frac{p-1}{q}} (mod\ p) > 1$.

Key b is randomly selected from the range $1 \le b \le q$ and keeping in secret. Calculated value $\beta = g^b mod\ p$. The algorithm parameters p, q, g are the public key and published for all users of the information exchange system with DS.

Consider the formation of the DS for the message M.

Determine hash value h from the signed message M: $h = h(M)$.

Choose integer r by some random method, where $1 \le r \le q$. This number stored in secret and varies for each signature.

Calculate: $\gamma = (g^r mod\ p) mod\ q$.

By using the private key of the sender $\delta = (r^{-1}(h + b\gamma)) mod\ q$ is calculated, where r^{-1} satisfies the condition $(r^{-1} r) mod\ q = 1$.

Digital signature for the message M is the pair of numbers (γ, δ), which passed along with the message by open communication channels.

Verification of DS. Let denote M', δ', γ' obtained by the addressee version of M, δ, γ.

Checking the conditions $0 < \delta < q$ and $0 < \gamma < q$. Reject the signature if any one of the conditions of the digital signature is not satisfied.

Calculate hash value $h_1 = h(M')$ from the received message M'.

Calculate value $v = (\delta')^{-1} mod\ q$.

Calculate the expressions: $z_1 = (h_1 v) mod\ q$ and $z_2 = (\gamma' v) mod\ q$.

Calculate value: $u = ((g^{z_1} \beta^{z_2}) mod\ p) mod\ q$.

The DS is valid if $\gamma' = u$, i.e. in the transfer process the integrity of the message was not compromised: $M' = M$. At

default of equality DS is invalid.

Cryptostrength of DSA scheme against "brute force" attacks is primarily dependent on the size of the parameters p and q. Accordingly, cryptostrength against "brute force" attacks on the parameter p in case of 512 and 160 bits is equal 2^{160}. A successful attack on the parameter q is only possible, if the attacker can calculate discrete logarithms in Galois field $GF(2^{512})$.

One of the theoretically possible attacks on DSA scheme is a compromise of the parameter r. For each signature is required a new value of r, which should be chosen randomly. If the attacker finds the value of r, then the secret key b may be disclosed. Another possible embodiment - two signatures were generated on the same value of r. In this case, the attacker is also able to recover b. Consequently, one of the factors that increase the safety of using DS schemes is the existence of a reliable random number generator.

In DSA length conversion module is approximately 1024 bits. To the same length increased key lengths. In this regard, increasing the computational complexity of cryptographic transformations, but decreases the computational speed. Reducing the key length and increasing computing speed, possible in the development of the modifying of this DS scheme on the basis of NPNs.

The modular system of DS with the public key, in creation that will be used a modified algorithm of DSA based on NPNs are be developed. Initially DSA algorithm written as, in which no number q and all calculations are performed only in one modulo p. Then developed a modification of the scheme on the basis of NPNs.

The formation process of NPNs for electronic message M of the given length N bits and calculating the hash value for this message given in Section II.

The modification of DSA digital signature scheme based on NPNs is carried out as follows.

The digital signature computation. Let formed NPNs with working base numbers $p_1(x), p_2(x),\ldots, p_S(x)$. For each of the working base numbers the corresponding generating elements (polynomials) $g_1(x), g_2(x),\ldots, g_S(x)$ are selected. Generating polynomials are analogous to primitive elements in finite field modulo prime number.

The sender's secret key b in the range $[1, 2^m]$ is chosen.

Calculates the value of the public key $\beta(x)$:

$$\beta(x) = (\beta_1(x), \beta_2(x),\ldots, \beta_S(x)).$$

In the modified DS algorithm based on NPNs, the procedure for calculating the hash value will be used in the NPNs.

The random integer r from a range of $\left[1, 2^m\right]$ is selected.

In NPNs polynomials $\gamma(x)$and $\delta(x)$ has nonpositional representation in the form of sequence of residues from its division by the base numbers of:

$$\gamma(x) = \left(\gamma_1(x), \gamma_2(x),\ldots, \gamma_s(x)\right),$$

$$\delta(x) = \left(\delta_1(x), \delta_2(x),\ldots, \delta_s(x)\right).$$

Digital signature for the message M is a pair of polynomials $\left(\gamma(x), \delta(x)\right)$.

Verification of the digital signature is carried out by analogy of the given DSA verification.

Using algebraic approach based on NPNs will reduce the key length for digital signature without significantly lowering its cryptostrength.

VI. Conclusion

Cryptostrength of the developed modified encryption systems and digital signature based on NPNs is characterized by the full secret key. This key is dependent not only on key length (pseudorandom sequence), but also on the chosen system of polynomial bases of NPNs, and also on the number of all possible permutations of bases in the system.

Research and application of encryption modes is aimed at eliminating potential vulnerabilities in the processing of large blocks of messages. In connection with this, models, that applicate CBC cipher mode, will be considered. This mode allows to eliminate the disadvantages of using a single key for encryption all plaintext blocks without significantly reducing the speed of its capacity, as the delay in executing of XOR operation is small. The developed modified system of digital signature, based on DSA algorithm and NPNs, is characterized by improvement of the basic characteristics of the digital signature. Computer modelling of the modified cryptosystems based on NPNs will allow developing recommendations for their secure usage and generation of full secret keys.

References

[1] I. Ya. Akushskii, D. I. Juditskii, “Machine Arithmetic in Residue Classes [in Russian],” Moscow: Sov. Radio, 1968.

[2] W. Stallings, “*Cryptography and Network Security* (4th Edition),” Prentice Hall, 2005.

[3] R. G. Biyashev, “Development and investigation of methods of the overall increase in reliability in data exchange systems of distributed ACSs,” Doctoral Dissertation in Technical Sciences, Moscow, 1985.

[4] R. G. Biyashev, S. E. Nyssanbayeva, “Algorithm for Creation a Digital Signature with Error Detection and Correction,” *Cybernetics and Systems Analysis*, 4, 489-497, 2012.

[5] R. Biyashev, S. Nyssanbayeva, N. Kapalova, “The Key Exchange Algorithm on Basis of Modular Arithmetic,” *International Conference on Electrical, Control and Automation Engineering (ECAE2013)*, Hong Kong – Monami,S. 2014. – P.501-505, December 1-2, 2013.

[6] Gr. C. Moisil, “Algebraic Theory of Discrete Automatic Devices,” [Russian translation]. Inostr. Lit., Moscow, 1963.

[7] N. A. Kapalova, S. E. Nyssanbayeva, R. A. Khakimov, “Irreducible polynomials over the field GF (2n),” Proceedings of Scientific and Technical Society "KAKHAK" , Almaty, Kazakhstan, № 1. P. 17-28, 2013.

[8] R. K. Nyssanbayev, “Cryptographical method on the basis of polynomial bases,” Herald of the Ministry of Science and Higher Education and National Academy of Science of the Republic of Kazakhstan, 5, 63-65, 1999.

[9] R. Biyashev, M. Kalimoldayev, N. Kapalova, R. Khakimov, S. Nyssanbayeva, “Program Modeling of the Cryptography Algorithms on Basis of Polynomial Modular Arithmetic,” *Proceedings. The 5th International Multi-Conference on Complexity, Informatics, and*

Cybernetics. The 5th International Conference on Society and Information Technologies (IMCIC'14 - ICSIT 2014). – Orlando, Florida, U.S.A. 2014. – P. 49-54.

[10] ST RK 1073-2007 "Means of cryptographic protection of information. General technical requirements", Astana: 2009.

[11] N. Ferguson, B. Schneier, T. Kohno, "Cryptography Engineering: Design Principles and Practical Applications," Wiley Publishing Inc, 2010.

[12] Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. 2001 Edition.

[13] W. Diffie, M. Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proc. of the IEEE [Russian Translation]. 3, 71–109, 1979.

[14] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, v. IT-31, n. 4, 1985. P. 469-472.

[15] FIPS PUB 186. Digital Signature Standard (DSS).

[16] Information technology. Cryptographic protection of information. Hash function GOST 4.11-94, State Standard of the Russian Federation, Moscow, 1994. Available: ftp://ftp.wtc-ural.ru/pub/ru.crypt/ ГОСТ 34.11/: 10.01.2015.