EURASIAN JOURNAL OF MATHEMATICAL AND COMPUTER APPLICATIONS
ISSN 2306–6172
Volume 4 , Issue 2 (2016) 33 – 38

MODIFICATION OF THE DIGITAL SIGNATURE, DEVELOPED ON THE NONPOSITIONAL POLYNOMIAL NOTATIONS

M.N.Kalimoldayev, R.G.Biyashev, S.E.Nyssanbayeva, Ye.Ye.Begimbayeva

Abstract Modification of the digital signature, based on nonpositional polynomial notations is developed. The signature algorithm model is based on the scheme of the Digital Signature Algorithm and nonpositional polynomial notations (NPNs). Application of NPNs allows creating effective cryptographic systems for high reliability, which enables the confidentiality, authentication and integrity of stored and transmitted information. Classical notations in residue number system (RNS), polynomial notations systems in RNS, modular arithmetic are the synonyms of NPNs.

Key words: digital signature, nonpositional polynomial notations, cross-border exchange

AMS Mathematics Subject Classification: 94A60

1 Introduction

The basis for the creation of the proposed model of asymmetric system of the digital signature (DS) are nonconventional systems [1-3]. These systems are developed on the algebraic approach base, using nonpositional polynomial notations (NPNs) or polynomial notations in residue classes (polynomial RNS). In the classical notations in residue number system the bases are prime numbers, and RNS 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]. In NPNs bases are irreducible polynomials over $GF(2)$ [3]. Usage of NPNs allows reducing the key length, increasing the strength and efficiency of the nonpositional cryptographic algorithms [4]. Increased efficiency is ensured by the NPNs rules in which all arithmetic operations can be performed in parallel on NPNs base module.

The developed unconventional cryptographic algorithm of the DS formation is performed for a predetermined length of an electronic message. In these cryptosystems as the cryprtostrength criterion used cryptographic strength of DS formation algorithm themselves, which is characterized by the full private key [3-5].

The NPNs arithmetic with polynomial bases and its application to problems of increasing reliability are developed in [3]. It is shown that the algebra of polynomials over a field be the irreducible polynomial modulo over this field is the field and polynomial presentation in nonpositional is unique. The rules of arithmetic operations in NPNs and the polynomial recovery by its residues are defined. According to the Chinese remainder theorem all working bases should be different.

2 Nonpositional polynomial notations

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

$$p_1(x), p_2(x), ..., p_S(x), \tag{1}$$

where $p_i(x)$-irreducible polynomial with binary coefficients of degree m_i respectively, $i = \overline{1, S}$. These bases are called working bases. The main working range in NPNs is a polynomial $P_S(x) = \prod_{i=1}^{S} p_i(x)$ of the degree $m = \sum_{i=1}^{S} m_i$. All the selected working base should be different from each other (according to the Chinese remainder theorem), even if they are irreducible polynomials of one degree.

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

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)), \tag{2}$$

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

In NPNs a message of the given length N is interpreted as a sequence of remainders from division by some polynomial (let us denote it as $F(x)$ by working base numbers $p_1(x), p_2(x), ..., p_S(x)$ of degree not higher than N, that is, in the form of (2). Bases are selected from all irreducible polynomials with degrees varying from m_1 to m_S, providing that the following equation is satisfied [6]:

$$k_1 m_1 + k_2 m_2 + ... + k_S m_S = N. \tag{3}$$

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 (3) and specifies one system of working bases, n_i is the number of all irreducible polynomials of degree m_i, $1 \le m_i \le N$, $S = \sum_{i=1}^{S} k_i$ is a number of selected working bases. Equation (3) 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.

With growth of irreducible polynomials degrees, their amount rapidly increases [7] and as a result, the number of solutions of (3) 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 [8].

The positional representation of $F(x)$ is reconstructed from its form (2) [3-4]:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) B_i(x), B_i(x) = \frac{P_S(x)}{p_i(x)} M_i(x), i = \overline{1, S}. \quad (4)$$

Polynomials $M_i(x)$ are chosen so as to satisfy the congruence in (4).

B. Hashing an electronic message in NPNs

For hashing the message M of length N to the length of N_k bits the redundant bases $p_{S+1}(x), p_{S+2}(x), ..., p_{S+U}(x)$ are entered. These bases are selected randomly from all irreducible polynomials, degree not higher than N_k . System of redundant bases is formed independently from working bases selecting. Note that some bases among the U redundant bases may coincide with some of the working bases. Denote the degree and the number of irreducible polynomials used in their selection as $a_1, a_2, ..., a_U$ and $d_1, d_2, ..., d_U$ respectively. The number of selected redundant bases in this case is determined from the equation (the analogue of (3)):

$$t_1 a_1 + t_2 a_2 + ... + t_U a_U = N_k, \quad (5)$$

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, $U = \sum_{j=0}^{U} t_j$ – the number of selected redundant bases, which produce residues that covers the hash value of length N_k. Solution of the (5) defines a single system of redundant bases.

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

$$h(F(x)) = (\alpha_{S+1}(x), \alpha_{S+2}(x), ..., \alpha_{S+U}(x)), \quad (6)$$

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.

3 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 [9-10]. 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 [11-12]. 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: $2^{L-1} < p < 2^L$, $512 \leq L \leq 1024$, L multiple of 64, $2^{159} < q < 2^{160}$, q- prime divisor of $(p-1)$ and $g = h^{\frac{p-1}{q}} mod\ p$, 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 $1 \leq b \leq q$ and keeping in secret. Value $\beta = g^b mod\ p$ is calculated. 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 $1 \leq r \leq q$. This number stored in secret and varies for each signature.

Value $\gamma = (g^r mod\ p) mod\ q$ is calculated.

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

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 $M^{'}$,$\delta^{'}$,$\gamma^{'}$ obtained by the addressee version of M, δ, γ.

Checking the conditions $0 < \delta, \gamma < q$. 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 $\nu = (\delta^{'})^{-1} mod\ q$.

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

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.

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.

Let formed NPNs with working bases $p_1(x), p_2(x), ..., p_S(x)$. For each of the working bases the corresponding generating elements (polynomials) $g_1(x), g_2(x), ..., g_S(x)$ 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 $\beta(x)$: $\beta(x) = (\beta_1(x), \beta_2(x), ..., \beta_S(x))$.

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 $[1, 2^m]$ 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 bases of: $\gamma(x) = (\gamma_1(x), \gamma_2(x), ..., \gamma_S(x))$, $\delta(x) = (\delta_1(x), \delta_2(x), ..., \delta_S(x))$.

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

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.

4 Conclusion

Cryptostrength of the developed modified 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.

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.

It is also will be used in development of the technology of secure cross-border information exchange [13].

References

[1] Akushskii, I.Ya., Juditskii, D.I., *Machine Arithmetic in Residue Classes [in Russian]*, Sov. Radio, Moscow (1968).

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

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

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

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

[7] Biyashev R.G., Nyssanbayeva S.E., Begimbayeva Ye.Ye., Magzom M.M. *Building modified modular cryptographic systems*, International Journal of Applied Mathematics and Informatics. Vol. 9, 2015. P. 103–109

[8] 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, N 1. P. 17–28, 2013..

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

[10] 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.

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

[12] 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.

[13] Biyashev R.G., Nyssanbayeva S.E., Begimbayeva Ye.Ye. *Formation of the secure cross-border information exchange in the integrated system*, Proceedings of international sc.-pract. conf. “Informational security in light of the Strategy “Kazakhstan-2050”. – Astana, 2015, – p. 87-91.

Maksat N. Kalimoldayev,
Institute of Information and Computational Technologies of MES RK,
125 Pushkin str., Almaty, 050010, Republic of Kazakhstan,
Email: mnk@ipic.kz.

Rustem G. Biyashev,
Institute of Information and Computational Technologies of MES RK,
125 Pushkin str., Almaty, 050010, Republic of Kazakhstan,
Email: brg@ipic.kz.

Saule E. Nyssanbayeva,
Institute of Information and Computational Technologies of MES RK,
125 Pushkin str., Almaty, 050010, Republic of Kazakhstan,
Email: sultasha1@mail.ru.

Yenlik Ye. Begimbayeva,
Institute of Information and Computational Technologies of MES RK,
125 Pushkin str., Almaty, 050010, Republic of Kazakhstan,
Email: enlik_89@mail.ru

Received 10.06.2016, Accepted 27.06.2016