Капилова Н.А.

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени АЛЬ-ФАРАБИ

ИНСТИТУТ ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ
СИБИРСКОГО ОТДЕЛЕНИЯ РАН

ISSN 1560-7534
ISSN 1563-0285

СОВМЕСТНЫЙ ВЫПУСК

по материалам международной научной конференции
"Вычислительные и информационные технологии в науке, технике и образовании"
(CITech-2015)
(24-27 сентября 2015 года)

ВЫЧИСЛИТЕЛЬНЫЕ ТЕХНОЛОГИИ

Том 20

ВЕСТНИК КАЗНУ им. АЛЬ-ФАРАБИ

Серия математика, механика и информатика № 3 (86)

ЧАСТЬ I

АЛМАТЫ – НОВОСИБИРСК, 2015

The Modified Digital Signature Algorithm Based on Modular Arithmetic

Rustem Biyashev, Saule Nyssanbayeva and Yenlik Begimbayeva

Institute of Information and Computational Technologies of MES RK,
125 Pushkin str., Almaty, 050010, Republic of Kazakhstan {sultasha1,enlik89}@mail.ru
http://ipic.kz

Abstract. In this paper the model of unconventional asymmetric system of digital signature is described. Cryptosystems, developed on the basis of nonpositional polynomial notations (NPNs), are called nonconventional, nonpositional or modular. The model of signature is created on the basis of digital signature scheme the Digital Signature Algorithm (DSA) and NPNs. Application of NPNs allows increasing the cryptostrength of the cryptosystem and reducing the key length

Keywords: digital signature, asymmetric scheme, nonpositional polynomial notations, cryptostrength.

1 Introduction

Unconventional systems are basis for creation of the proposed model of asymmetric system of the digital signature (DS) on the basis of DSA algorithm [1-3]. In the classical notations in residue number system the bases are prime numbers, and 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 algorithms of the DS formation are performed for a predetermined length of an electronic message. In these cryptosystems as the cryprtostrength criterion used cryptographic strength of DS formation algorithms themselves, which is characterized by the full private key [3-5].

In [3] developed the NPNs arithmetic with polynomial bases and its application to problems of increasing reliability. 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 Formation of NPNs

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

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

where $p_i(x)$-irreducible polynomials over the field $GF(2)$ of degree m_i respectively, $i = \overline{1,S}$. The main working range of NPNs represented by polynomial $P_S(x) = \prod_{i=1}^{S} p_i(x)$ of 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 $F(x)$, the degree of which is less than m, has nonpositional representation as a sequence of residues from its division into base $p_1(x), p_2(x), \ldots, p_S(x)$ respectively, and it is unique:

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

where $F(x) \equiv (\alpha_i(x)(mod\ p_i(x)), i = \overline{1,S}$. By the form (2) recovering positional representation of the polynomial $F(x)$ [3,4]:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x) B_i(x), B_i(x) = \frac{(P_S(x))}{(p_i(x))} M_i(x) \equiv 1(mod\ (p_i(x)), i = \overline{1,S}. \tag{3}$$

Polynomials $M_i(x)$ are selected such as to satisfy the comparison in (3).

In NPNs the electronic message of length N bits is interpreted as a sequence of remainders of division of some polynomial (denote it also as $F(x)$) according to the working base $p_1(x), p_2(x), \ldots, p_S(x)$ degree not higher than N, ie in the form (2). Bases are selected from the number of all irreducible polynomials of degree from m_1 to m_S from the execution condition of the equation [6]:

$$k_1 m_1 + k_2 m_2 + \cdots + k_S m_S = N. \tag{4}$$

In equation (4) $0 \le k_i \le n_i$, $i = \overline{1,S}$ - the unknown coefficients and the number of selected irreducible polynomials of degree m_i. One concrete set of these coefficients is one of the solutions (4) and defines one system of working bases, n_i - the number of irreducible polynomials of degree m_i. $1 \le m_i \le N$, $S = \sum_{i=1}^{S} k_i$ - the number of selected working bases. Equation (4) defines the number of S working bases, residues that cover the length N of the given messages. The full system of residues by polynomials modulo of degree m_i include all polynomials of degree not higher than $m_i - 1$, to record requiring m_i bit [4-5].

In the NPNs to obtain DS the hash value is used from the signed message.

3 Hashing an electronic message in NPNs

For hashing the message M of length N bits to N_k bits the redundant bases

$$p_{S+1}(x), p_{S+2}(x), ..., p_{S+U}(x). \tag{5}$$

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. Among U redundant bases may coincide with some of the working bases. Let denote $a_1, a_2, \ldots, a_U$ and $d_1, d_2, \ldots, d_U$ degree and the number of irreducible polynomials, respectively, used in their selection. The number of selected redundant bases in this case determined from the equation:

$$t_1 a_1 + t_2 a_2 + \cdots + t_U a_U = N_k, \tag{6}$$

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. $U = t_1 + t_2 + \cdots + t_U$ - number of selected redundant bases, recording of the residues which covers the hash value of length N_k. The solution of equation (6) defines one system of redundant bases.

The next stage of calculations of the hash value is to calculate the redundant residues

$$\alpha_{S+1}(x), \alpha_{S+2}(x), ..., \alpha_{S+U}(x) \quad (7)$$

by dividing the reduced polynomial $F(x)$ to redundant bases (5). Then, the hash value is interpreted as a sequence of residues:

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

where $h(F(x)) \equiv \alpha_{S+j}(x) mod\ p_{S+j}(x))$, $j = \overline{1,U}$. The sum of length of the redundant residues (7) is the length of the hash value and the DS.

The nonpositional asymmetric DS system is constructed to obtained hash value.

4 Asymmetric digital signature based on NPNs

Digital Signature Algorithm (DSA) - this is the digital signature scheme [7], which was adopted in 1994, as the US standard, and acting until 2001. This scheme is the variation of a digital signature of the ElGamal scheme and K. Schnorr. DSA reliability is based on the practically insoluble of the particular case of the problem of calculating the discrete logarithm.

The essence of DSA electronic signature scheme is the following. The sender and recipient of the electronic document in computation use large prime integers p and q, in the range $2^{L-1} < p < 2^L$, $512 \leq L \leq 1024$, 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 $h^{\frac{p-1}{q}}(mod\ p) > 1$.

The private key b is kept in secret and randomly selected from the range $1 \leq b \leq q$. Calculated value $\beta = g^b mod\ p$. The parameters (p, q, g) - are the public keys, which published for all users of the information exchange system with DS.

The formation process of the DS for the message M consists of the following steps:

1. determine hash value h from the signed message $M : h = h(M)$;

2. choose random integer r, which is keeping in secret, in range $1 \leq r \leq q$ and its varying from one sign to another;

3. calculate value: $\gamma = (g^r mod\ p) mod\ q$;

4. calculate $\delta = (r^{'}(h + b\gamma)) mod\ q$, where $r^{'}$ satisfies the condition $(r^{'}r) mod\ q = 1$;

5. DS for the message M is the pair of numbers (γ, δ). They are passed along with the message by open communication channels.

The process of verification of DS M is consists of the following steps: (Let denote $M^{'}$,$\delta^{'}$,$\gamma^{'}$ obtained by the addressee version of M, δ, γ).

1. checking the conditions $0 < \delta, \gamma < q$. Reject the signature if any one of the conditions of the DS is not satisfied these conditions.

2. calculate hash value $h_1 = h(M^{'})$ from the received message $M^{'}$.

3. calculate value $\nu = (\delta^{'})^{-1} mod\ q$.

4. calculate value: $z_1 = (h_1 v) mod\ q$ and $z_2 = (\gamma^{'}\nu) mod\ q$.

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

6. the DS is valid if $\gamma^{'} = u$. It means that in the transfer process the integrity of the message was not compromised. Otherwise, the signature is invalid.

In the construction of nonpositional asymmetric system of DS initially made modification of the DSA algorithm: excluded the second module q, because for the DS calculation will use the obtained above hash value in NPNs. Then, for the constructed DSA algorithm by one module p the nonpositional system of digital signature of length N_k will be developed.

The obtained electronic document (hash value) of length N_k (8) is considered in nonpositional polynomial notation, which nonpositional asymmetric system of DS be developed. For this NPNs polynomial bases

$$\eta_1(x), \eta_2(x), ..., \eta_W(x) \tag{9}$$

are selected similar as the choice of working bases in section 2. Let denote $q_1, q_2, ..., q_W$ and $l_1, l_2, ..., l_W$ degree and the number of irreducible polynomials, respectively, used in their selection. The number of selected redundant bases in this case is determined from the analog equations (4) and (6).

Then, for bases (9) respective generating elements (polynomials) $g_1(x), g_2(x), ..., g_W(x)$ are found, which are analogous to primitive elements in the algorithm DSA.

The private key of the sender b is selected also in range $[1, 2^q]$, where q is the sum of the degrees $q_1, q_2, ..., q_W$.

Calculate value of the public key $\beta(x)$: $\beta(x) = (\beta_1(x), \beta_2(x), ..., \beta_W(x))$ by bases modulo (7).

Next, choose a random integer r in range $[1, 2^q]$.

Polynomials $\gamma(x)$ and $\delta(x)$ in the modified DSA algorithm by one module p presented in nonpositional form as a sequence of residues from their division on the bases (9).

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

5 Conclusion

The feature of formation of nonpositional asymmetric system of DS using the DSA algorithm and NPNs is that not all parameters can be used as indicators of the degree. This applies to polynomial bases of NPNs. Computer modeling of the modified cryptosystems based on NPNs will allow developing recommendations for their reliable use and generation of full secret keys.

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. FIPS PUB 186. *Digital Signature Standard (DSS).*