ISSN 2347 - 3983

Volume 8. No. 7, July 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter47872020.pdf

https://doi.org/10.30534/ijeter/2020/47872020

Redundant Modular Codes for Development of Fault-Tolerant Systems of Satellite Identification

Igor Anatolyevich Kalmykov[1], Vladimir Petrovich Pashintsev[1], Aleksandr Pavlovich Zhuk[1],
Maksim Igorevich Kalmykov[1], Aleksandr Anatolyevich Olenev[2]
[1]North-Caucasus Federal University, Stavropol, Russia
[2]Stavropol State Pedagogical Institute, Stavropol, Russia

ABSTRACT

Hydrocarbon production in the Extreme North on unattended facilities is based on **low earth orbit satellite (LEOS) systems for communications.** Their information security can be improved by means of Identification-Friend-or-Foe (IFF) system for satellite. Authentication protocol based on modular codes(MC) makes it possible prior to communicating session to determine satellite status at minimum time consumptions. Such result is achieved due to parallel computations based on **MC**. However, MC can also detect and correct errors. Therefore, development of authentication protocol, where redundant MC are used for correction of errors occurring upon calculation of response to request from identification system, is an urgent problem. This work is aimed at improvement of fault tolerance of satellite identification system by means of the developed authentication protocol, where redundant MC are used for correction of errors occurring upon calculation of response to request from interrogator.

Key words: satellite authentication system, modular codes, residue number system, polynomial residue number system, error correction.

1. INTRODUCTION

Development of deposits in the coastal area of the Arctic Ocean is impossible without **low earth orbit satellite (LEOS) systems for communications,** their constellation should be comprised of at least 60 satellites [1]. While the number of **LEOS** systems used by companies upon development of resources of the Extreme North increases, the chance of imposing tapped and delayed control command for unattended facilities of hydrocarbon production increases. This could lead to environmental disaster.

In order to prevent forced relaying interference of LEOS systems, some researchers [2, 3] propose to use Identification-Friend-or-Foe (IFF) system onboard the satellites. Herewith, in order to reduce time required for computation of satellite status, [4] developed authentication protocol on the basis of modular codes(MC). However, MC due to redundancy can detect and correct computational errors. Therefore, development of authentication protocol, where redundant MC are used for correction of errors occurring upon calculation of response to request from identification system, is an urgent problem.

2. LITERATURE REVEIW

2.1. Modular codes of residue number system

In order to increase the rate of mathematical operations, [5, 6] propose to use MC. Depending on the base type, the following MC are highlighted:

- residue number system (RNS);

- polynomial residue number system (PRNS).

In the **RNS** codes, the bases m_i, $i = 1, 2, \dots, k$ are the co-prime numbers, for which the following is valid:

$$m_1 < m_2 < m_3 < \dots < m_k . \quad (1)$$

Multiplication of the bases determines operating range:

$$M = \prod_{i=1}^{k} m_i \,. (2)$$

Then, the **RNS** code of integer W, for which $W < M$, is as follows:

$$W = (w_1, w_2, \dots, w_k)\,, (3)$$

where $w_i \equiv W \bmod m_i$; $i = 1, 2, \dots, k$.

Arithmetic operations in **RNS**, using Eq. (3), are performed for residues:

$$W + Y = \left(\left|w_1 + y_1\right|^{+}_{m_1}, \left|w_2 + y_2\right|^{+}_{m_2}, \dots, \left|w_k + y_k\right|^{+}_{m_k} \right) \quad , \quad (4)$$

$$W - Y = \left(\left|w_1 - y_1\right|^{+}_{m_1}, \left|w_2 - y_2\right|^{+}_{m_2}, \dots, \left|w_k - y_k\right|^{+}_{m_k} \right), \quad (5)$$

$$W \cdot Y = \left(\left|w_1 \cdot y_1\right|^{+}_{m_1}, \left|w_2 \cdot y_2\right|^{+}_{m_2}, \dots, \left|w_k \cdot y_k\right|^{+}_{m_k} \right), \quad (6)$$

where $Y \equiv y_i \bmod m_i$; $i = 1, 2, \dots, k$.

Analysis of Eqs. (4)-(6) demonstrates that modular operations are performed in parallel with regard to the bases, independently of one another for short residues. As a consequence, the RNS codes are characterized by higher performance in comparison with positional codes. This property of RNS codes determines the scope of their application. Application of RNS codes for specialized signal digital processing was described in [7, 8, 9]. Since the basic operation of digital filtration is the sum of binary products, then [10, 11] described digital filters operating in RNS**.** Application of RNS codes for detection and correction of errors occurring during computations was described in [7, 12]. It is proposed in [13] to apply **RNS** codes for error correction upon transfer of well telemetric data. Application of protocols of payments and E-money withdrawal implemented in RNS code is described in [14, 15].

A new scope of application of **RNS** codes is satellite identification systems using authentication protocols with zero knowledge proof.

2.2. Satellite authentication protocol implemented in RNS code

It is known that zero knowledge proof authentication protocols are characterized by high encryption strength without application of encryption methods. This is achieved by multiple verification of pretender, where the pretender P, while responding to requests, should prove to the verifier V that he possesses certain secret without real disclosure of the statement. It is proposed in [16, 17] to apply from 30 to 40 rounds of authentication, which leads to significant time consumptions. This drawback can be eliminated by the authentication protocol described in [18].

However, in order to provide high encryption strength, this protocol uses high prime number q. Aiming at reduction of time consumptions for determination of satellite status, the authentication protocol was developed implemented in **RNS** codes. In the protocol, the **RNS** bases are selected according to Eq. (1). Herewith, the range, using Eq. (2), should satisfy the condition $M > q$. According to (3), we obtain the satellite secret key $U = (U_1, ..., U_k)$, the session key $S(j) = (S_1(j), S_2(j),..., S_k(j))$, the parameter for verification of double use S(j) of key $T(j) = (T_1(j), T_2(j),..., T_k(j))$. This is aided by converter from positional code to **RNS** code. The authentication protocol is shown in Table 1.

Table 1: Satellite identification protocol

<table>
<tr><th colspan="4">Preliminary stage</th></tr>
<tr><td></td><td>P (pretender)</td><td colspan="2">Trusted center</td></tr>
<tr><td>1
2</td><td>$U = (U_1, ..., U_k)$ - secret key,
S, T – random numbers;
$S = (S_1, S_2,..., S_k)$, $T = (T_1, T_2,..., T_k)$</td><td colspan="2">Selection of bases $m_1 < m_2 < m_3 < ... < m_k$.
g – generating element of multiplicative group m_i,.</td></tr>
<tr><th colspan="4">Operating stage</th></tr>
<tr><td></td><td>P (pretender)</td><td></td><td>V (verifier)</td></tr>
<tr><td>1</td><td>Computation of session key in <b>RNS</b>
$S_i(j) = F(S_i(j-1), U_i)$;
Computation of verifying parameter in <b>RNS</b>
$T_i(j) = F(T_i(j-1), U_i)$
F – pseudo-random function.</td><td></td><td></td></tr>
<tr><td>2</td><td>Real status is computed
$C_i(j) = g^{U_i} g^{S_i(j)} g^{T_i(j)} \bmod m_i$, $i = 1, 2,..., k$</td><td></td><td></td></tr>
<tr><td>3</td><td>Noise contamination
$U_i^* = (U_i + \Delta U_i(j)) \bmod \varphi(m_i)$,
$S_i^*(j) = (S_i(j) + \Delta S_i(j)) \bmod \varphi(m_i)$,
$T_i^*(j) = (T_i(j) + \Delta T_i(j)) \bmod \varphi(m_i)$.
where $\{\Delta U_i(j), \Delta S_i(j), \Delta T_i(j)\} < m_i$</td><td></td><td></td></tr>
<tr><td>4</td><td>Noisy status is computed
$C_i^*(j) = g^{U_i^*} g^{S_i^*(j)} g^{T_i^*(j)} \bmod m_i$. $i = 1, 2,..., k$</td><td></td><td></td></tr>
</table>

Satellite authentication			
1			Random request number is selected $d(j)=(d_1(j), d_2(j),..., d_k(j))$
2	Response to request «d(j)» $r_i^1(j)=(U_i(j)-d_i(j)U_i) \bmod \varphi(m_i)$, $r_i^2(j)=(S_i^*(j)-d_i(j)S_i(j)) \bmod \varphi(m_i)$, $r_i^3(j)=(T_i^*(j)-d_i(j)T_i(j)) \bmod \varphi(m_i)$		
			Response is received $\left(C_i(j) \parallel C_i^*(j) \parallel r_i^1(j) \parallel r_i^2(j) \parallel r_i^3(j)\right)$
Verification of response to request d(j)			
1			Verification of responses to request $Y_i(j)=C_i(j)^{d_i(j)} g^{r_i^1(j)} g^{r_i^2(j)} g^{r_i^3(j)} \bmod m_i$
			$Y_i(j)=C_i^*(j)$ – friend $Y_i(j) \neq C_i^*(j)$ – foe

However, this protocol, while reducing time consumptions for satellite verification, cannot detect and correct errors occurring during identification. Moreover, the converter from positional code to RNS code makes the structure of identification system more complicated. This drawback can be eliminated by the developed authentication protocol based on redundant PRNS codes.

3. METHODS

3.1 Codes of polynomial residue number system

If irreducible polynomials $p_i(x)$, $i=1, 2,..., k$ are selected as bases, then the MC are arranged in polynomial ring [6]. In order to obtain PRNS codes, the binary code of W is presented in the polynomial form W(x). Then, the polynomial W(x) is divided by the bases $p_i(x)$, $i=1, 2,..., k$. As a consequence, we obtain PRNS code.

$$W(x)=(w_1(x), w_2(x),..., w_k(x)), \quad (7)$$

where $w_i(x) \equiv W(x) \bmod p_i(x)$; $i=1, 2,..., k$.

The operating range of PRNS code is determined as follows:

$$P(x)=\prod_{i=1}^{k} p_i(x). \quad (8)$$

Since the operations are carried out in the polynomial ring, then according to [19], the following is valid:

$$Y(x) \oplus W(x)=\left(\left|y_1(x) \oplus w_1(x)\right|_{p_1(x)}, ..., \left|y_k(x) \oplus w_k(x)\right|_{p_k(x)}\right)$$

, (9)

$$Y(x) \cdot W(x)=\left(\left|y_1(x) \cdot w_1(x)\right|_{p_1(x)}, ..., \left|y_k(x) \cdot w_k(x)\right|_{p_k(x)}\right)$$

,(10)

where $Y(x) \equiv y_i(x) \bmod p_i(x)$; $i=1, 2,..., k$.

Analysis of Eqs. (9) and (10) demonstrates that they are similar to Eqs. (4)-(6). Thus, the PRNS codes are characterized by computation rate comparable with RNS codes. Herewith, in order to execute Eq. (9), it is possible to use XOR elements, which would allow to reduce network consumptions in comparison with LUT tables in RNS.

One of the important elements of authentication protocol is correct response to request from interrogator. If an error occurs during response computation, then the interrogator after invalid response would not allow communication session of its satellite. This drawback can be eliminated by the developed authentication protocol implemented in **PRNS.**

3.2 Authentication protocol allowing to correct response to request from identification system based on redundant PRNS

Let us take single module protocol [18] as prototype for authentication protocol. At preliminary stage, the following parameters are determined: the set of bases of PRNS code $p_i(x)$, $i=1, 2,..., k$, generating element $g=x$, satellite secret key K, session key for the j-th session S(j), additional verification parameter T(j) identified as:

$$\log_2\{К, S(j), T(j)\} < \deg P(x), \quad (11)$$

where $\deg P(x)$ is the degree of polynomial P(x) determined by Eq. (8).

Taking into account the digits of bases of **PRNS**, the blocks are selected: $К_i=\deg p_i(x)$, $S_i^j=\deg p_i(x)$, $T_i^j=\deg p_i(x)$, where $i=1, 2,..., k$. Then we have:

$\mathrm{K} = (\mathrm{K}_1 \parallel \mathrm{K}_2 \parallel ... \parallel \mathrm{K}_k)$, $S^j = (S_1^j \parallel S_2^j \parallel ... \parallel S_k^j)$, $T^j = (T_1^j \parallel T_2^j \parallel ... \parallel T_k^j)$, (12)

At the first stage of the protocol, the responder computes real spacecraft status:

$$C^j(x) = \left(\left| g(x)^{\mathrm{K}_1} g(x)^{S_1^j} g(x)^{T_1^j} \right|^+_{p_i(x)}, ..., \left| g(x)^{\mathrm{K}_k} g(x)^{S_k^j} g(x)^{T_k^j} \right|^+_{p_i(x)} \right). \quad (13)$$

At the second stage, the responder determines noisy parameters. On the basis of the generated values $\{\Delta\mathrm{K}_i, \Delta S_i^j, \Delta T_i^j\} < L$, where $L = 2^{\deg p_i(x)} - 1$, the result is as follows:

$$\tilde{\mathrm{K}}_i^j = \left| \mathrm{K}_i + \Delta\mathrm{K}_i^j \right|^+_L, \; \tilde{S}_i^j = \left| S_i^j + \Delta S_i^j \right|^+_L,$$

$$\tilde{T}_i^j = \left| T_i^j + \Delta T_i^j \right|^+_L \quad (14)$$

At the third stage, the responder obtains the value of spacecraft noisy status:

$$\tilde{C}^j(x) = \left(\left| g(x)^{\tilde{\mathrm{K}}_1^j} g(x)^{\tilde{S}_1^j} g(x)^{\tilde{T}_1^j} \right|^+_{p_i(x)}, ..., \left| g(x)^{\tilde{\mathrm{K}}_k} g(x)^{\tilde{S}_k^j} g(x)^{\tilde{T}_k^j} \right|^+_{p_i(x)} \right). \quad (15)$$

At the fourth stage, the interrogator generates random number-request $d^j = (d_1^j, d_2^j, ... d_k^j)$ where $d_i^j \equiv d^j \bmod L$, $L = 2^{\deg p_i(x)} - 1$, $i = 1, 2, ..., k$, which is transferred to satellite.

At the fifth stage, the responder, using Eqs. (3)-(4), computes responses to the request:

$$r_i^1(j) = \left| \tilde{\mathrm{K}}_i^j - d_i^j - \mathrm{K}_i^j \right|^+_L, \; r_i^2(j) = \left| \tilde{S}_i^j - d_i^j - S_i^j \right|^+_L, \; r_i^3(j) = \left| \tilde{T}_i^j - d_i^j - T_i^j \right|^+_L. \quad (16)$$

Then the satellite response is as follows:

$$\left\{ (C_1^j(x), ..., C_k^j(x)), (\tilde{C}^j(x), ..., \tilde{C}_k^j(x)), (r_1^1, ..., r_k^1), (r_1^2, ..., r_k^2), (r_1^3, ..., r_k^3) \right\}.$$

At the sixth stage of the authentication, the interrogator verifies responses:

$$Y_i^j(x) = \left| C_i^j(x) g(x)^{r_i^1} g(x)^{r_i^2} g(x)^{r_i^3} g^{3d_i} \right|^+_{p_i(x)}. \quad (17)$$

"Friend" status will be assigned to spacecraft when the following is valid:

$$\left\{ Y_1^j(x) = \tilde{C}_1^j(x), \; Y_2^j(x) = \tilde{C}_2^j(x), ..., \; Y_k^j(x) = \tilde{C}_k^j(x) \right\}$$

Obviously, the satellite authentication depends firstly on correct responses to interrogator requests which are computed onboard the satellite. In the developed protocol, the responses $r_i^1(j), r_i^2(j), r_i^3(j)$ are computed with respect to the base $L = 2^{\deg p_i(x)} - 1$. Then, classical approaches to detection and correction of errors cannot be applied in MC. This disadvantage can be eliminated by the developed algorithm of weighted convolution of code, where two reference residues are computed for error correction in one residue. Thus, upon generation of number-request $d^j = (d_1^j, d_2^j, ... d_k^j)$, the interrogator computes two residues:

$$d_{k+1}^j = \sum_{i=1}^{k} d_i^j \bmod 2_i^{\deg p_i(x)} - 1, \quad d_{k+2}^j = \sum_{i=1}^{k} 2^{i-1} d_i^j \bmod 2_i^{\deg p_i(x)} - 1. \quad (18)$$

The result is redundant combination $d^j = (d_1^j, d_2^j, \dots d_k^j, d_{k+1}^j, d_{k+2}^j)$. Similarly, residues are computed for arguments participating in Eq. (16):

$$K_{k+1}^j = \sum_{i=1}^{k} K_i^j \bmod 2_i^{\deg p_i(x)} - 1, \quad K_{k+2}^j = \sum_{i=1}^{k} 2^{i-1} K_i^j \bmod 2_i^{\deg p_i(x)} - 1. \quad (19)$$

$$S_{k+1}^j = \sum_{i=1}^{k} S_i^j \bmod 2_i^{\deg p_i(x)} - 1, \quad S_{k+2}^j = \sum_{i=1}^{k} 2^{i-1} S_i^j \bmod 2_i^{\deg p_i(x)} - 1. \quad (20)$$

$$T_{k+1}^j = \sum_{i=1}^{k} T_i^j \bmod 2_i^{\deg p_i(x)} - 1, \quad T_{k+2}^j = \sum_{i=1}^{k} 2^{i-1} T_i^j \bmod 2_i^{\deg p_i(x)} - 1. \quad (21)$$

$$\tilde{K}_{k+1}^j = \sum_{i=1}^{k} \tilde{K}_i^j \bmod 2_i^{\deg p_i(x)} - 1, \quad \tilde{K}_{k+2}^j = \sum_{i=1}^{k} 2^{i-1} \tilde{K}_i^j \bmod 2_i^{\deg p_i(x)} - 1. \quad (22)$$

$$\tilde{S}_{k+1}^j = \sum_{i=1}^{k} \tilde{S}_i^j \bmod 2_i^{\deg p_i(x)} - 1, \quad \tilde{S}_{k+2}^j = \sum_{i=1}^{k} 2^{i-1} \tilde{S}_i^j \bmod 2_i^{\deg p_i(x)} - 1. \quad (23)$$

$$\tilde{T}_{k+1}^j = \sum_{i=1}^{k} \tilde{T}_i^j \bmod 2_i^{\deg p_i(x)} - 1, \quad \tilde{T}_{k+2}^j = \sum_{i=1}^{k} 2^{i-1} \tilde{T}_i^j \bmod 2_i^{\deg p_i(x)} - 1. \quad (24)$$

During computation of three responses, Eq. (16), we obtain the reference residues:

$$r_{k+1}^1 = \tilde{K}_{k+1}^j - d_{k+1}^j - K_{k+1}^j, \qquad r_{k+2}^1 = \tilde{K}_{k+2}^j - d_{k+2}^j - K_{k+2}^j. \quad (25)$$

$$r_{k+1}^2 = \tilde{S}_{k+1}^j - d_{k+1}^j - S_{k+1}^j, \qquad r_{k+2}^2 = \tilde{S}_{k+2}^j - d_{k+2}^j - S_{k+2}^j. \quad (26)$$

$$r_{k+1}^3 = \tilde{T}_{k+1}^j - d_{k+1}^j - T_{k+1}^j, \qquad r_{k+2}^3 = \tilde{T}_{k+2}^j - d_{k+2}^j - T_{k+2}^j. \quad (27)$$

Then, on the basis of data residues of responses, the following is computed:

$$\dddot{r}_{k+1}^u(j) = \sum_{i=1}^{k} r_i^u(j) \bmod 2_i^{\deg p_i(x)} - 1, \quad \dddot{r}_{k+2}^u(j) = \sum_{i=1}^{k} 2^{i-1} r_i^u(j) \bmod 2_i^{\deg p_i(x)} - 1, \quad (28)$$

where $u = 1, 2, 3.$

In order to verify the responses, the error syndrome is computed:

$$\sigma_{k+1}^u(j) = r_{k+1}^u(j) - \dddot{r}_{k+1}^u(j) \bmod 2_i^{\deg p_i(x)} - 1, \quad \sigma_{k+2}^u(j) = r_{k+2}^u(j) - \dddot{r}_{k+2}^u(j) \bmod 2_i^{\deg p_i(x)} - 1. \quad (29)$$

If the error syndrome is zero, then the responses are correct. Otherwise, the response contains error. Herewith, using the syndrome value, it is possible to determine the erroneous response and to correct it.

4. RESULTS AND DISCUSSION

Let in the PRNS code the following bases are selected: $p_1(x) = x^5 + x^4 + x^3 + x + 1$, $p_2(x) = x^5 + x^4 + x^3 + x^2 + 1$, $p_3(x) = x^5 + x^3 + x^2 + x + 1$. Then the range is $P(x) = \prod_{i=1}^{3} p_i(x) = x^{15} + x^{11} + x^{10} + x^2 + 1$. On the basis of Eq. (11), we select the secret key $K = 31063$, the parameters $S = 12002$, $T = 24001$. Using Eq. (12), we present them in binary code which is subdivided into 5-bit blocks.

$$K = 31063_{10} = 11110\ 01010\ 10111_2 = 30_{10} \parallel 10_{10} \parallel 23_{10} = K_1 \parallel K_2 \parallel K_3.$$

$$S = 12002_{10} = 01011\ 10111\ 00010_2 = 11_{10} \parallel 23_{10} \parallel 2_{10} = S_1 \parallel S_2 \parallel S_3.$$

$$T = 24001_{10} = 10111\ 01110\ 00001_2 = 23_{10} \parallel 14_{10} \parallel 1_{10} = T_1 \parallel T_2 \parallel T_3.$$

1. Determination of spacecraft real status according to Eq. (13):

$$C_1^j(x) = \left| g(x)^{K_1} g(x)^{S_1^j} g(x)^{T_1^j} \right|^+_{p_1(x)} = \left| x^{30} \cdot x^{11} \cdot x^{23} \right|^+_{p_1(x)} = \left| x^2 \right|^+_{p_1(x)} = 00100 = 4,$$

$$C_2^j(x) = \left| x^{10} \cdot x^{23} \cdot x^{14} \right|^+_{p_2(x)} = \left| x^{16} \right|_{p_2(x)} = 01011 = 11\ ,$$

$$C_3^j(x) = \left| x^{23} \cdot x^{2} \cdot x^{1} \right|^+_{p_3(x)} = \left| x^{26} \right|^+_{p_3(x)} = 10100 = 20.$$

2. In order to determine noisy parameters, let us use Eq. (14). Then, at selected $\Delta K = 3332, \Delta S = 10353, \Delta T = 2441$ we obtain:

$$\tilde{K}^j = \left(|30+3|^+_{31} \parallel |10+8|^+_{31} \parallel |23+4|^+_{31} \right) = (2 \parallel 18 \parallel 27) = \left(\tilde{K}_1 \parallel \tilde{K}_2 \parallel \tilde{K}_3 \right),$$

$$\tilde{S}^j = \left(|11+10|^+_{31} \parallel |23+3|^+_{31} \parallel |17+2|^+_{31} \right) = (21 \parallel 26 \parallel 19) = \left(\tilde{S}_1 \parallel \tilde{S}_2 \parallel \tilde{S}_3 \right),$$

$$\tilde{T}^j = \left(|23+2|^+_{31} \parallel |14+12|^+_{31} \parallel |1+9|^+_{31} \right) = (25 \parallel 26 \parallel 10) = \left(\tilde{T}_1 \parallel \tilde{T}_2 \parallel \tilde{T}_3 \right).$$

3. Determination of spacecraft noisy status according to Eq. (15):

$$\tilde{C}_1^j(x) = \left| g(x)^{\tilde{K}_1} g(x)^{\tilde{S}_1^j} g(x)^{\tilde{T}_1^j} \right|^+_{p_i(x)} = \left| x^{2} \cdot x^{21} \cdot x^{25} \right|^+_{p_1(x)} = \left| x^{17} \right|_{p_1(x)} = 01011_2 = 11,$$

$$\tilde{C}_2^j(x) = \left| x^{18} \cdot x^{26} \cdot x^{26} \right|^+_{p_2(x)} = \left| x^{8} \right|_{p_2(x)} = 11100 = 28,$$

$$\tilde{C}_3^j(x) = \left| x^{27} \cdot x^{19} \cdot x^{10} \right|^+_{p_3(x)} = \left| x^{25} \right|_{p_3(x)} = 01010 = 10.$$

4. Interrogator transfers number-request $d^j = 00111 \| 00100 \| 10110 = 7 \parallel 4 \parallel 22$.

5. Responder determines responses to the request using Eq. (16). Then, for the first base we have:

$$r_1^1(j) = \left| \tilde{K}_1^j - d_1^j - K_1 \right|^+_{31} = 27,\ r_1^2(j) = |21-7-11|^+_{31} = 3,\ r_1^3(j) = |25-7-23|^+_{31} = 26.$$

For the second base, the responses to the request will be as follows:

$$r_2^1(j) = \left| \tilde{K}_2 - d_2^j - K_2 \right|^+_{31} = 4,\ r_2^2(j) = |26-4-23|^+_{31} = 30,\ r_2^3(j) = |26-4-14|^+_{31} = 8.$$

For the third base, the responses to the request will be as follows:

$$r_3^1(j) = \left| \tilde{K}_3^j - d_3^j \cdot K_3 \right|^+_{31} = 13,\ r_3^2(j) = |19-22-2|^+_{31} = 26,\ r_3^3(j) = |10-22-1|^+_{31} = 18.$$

The responder transfers two presented statuses and responses.

6. Interrogator, using Eq. (17), determines the satellite status:

$$Y_1^j(x) = \left|x^2 \cdot x^{27} \cdot x^3 \cdot x^{26} \cdot x^{7\cdot 3}\right|^+_{p_1(x)} = \left|x^{17}\right|^+_{p_1(x)} = 01011$$

,

$$Y_2^j(x) = \left|(x^3 + x + 1)x^4 x^{30} x^8 x^{12}\right|^+_{p_2(x)} = 11100,\ Y_3^j(x) = \left|\left(x^4 + x^2\right)x^{17} x^6 x^{19} x^{66}\right|^+_{p_3(x)} = 01010.$$

Since $\left\{Y_i^j(x) = \tilde{C}_i^j(x)\right\}$, then the "friend" status is assigned to the satellite.

Let us consider implementation of error correction algorithm. With this aim, let us compute two reference residues of the request d^j = (7, 4, 22) according to Eq. (18). We obtain:

$$d_4^j = \left|\sum_{i=1}^{3} d_i^j\right|^+_{31} = \left|7 + 4 + 22\right|^+_{31} = 2,\ d_5^j = \left|\sum_{i=1}^{3} 2^{i-1} d_i^j\right|^+_{31} = \left|7 + 2\cdot 4 + 4\cdot 22\right|^+_{31} = 10.$$

Let us compute two reference residues K_j = (30, 10, 23) according to Eq. (19). We obtain:

$$K_4^j = \left|\sum_{i=1}^{3} K_i^j\right|^+_{31} = \left|30 + 10 + 23\right|^+_{31} = 1,\ K_5^j = \left|\sum_{i=1}^{3} 2^{i-1} K_i^j\right|^+_{31} = \left|20 + 2\cdot 10 + 4\cdot 23\right|^+_{31} = 18.$$

Let us compute two reference residues S^j = (11, 23, 2) according to Eq. (20). We obtain:

$$S_4^j = \left|\sum_{i=1}^{3} S_i^j\right|^+_{31} = \left|11 + 23 + 2\right|^+_{31} = 5,\ S_5^j = \left|\sum_{i=1}^{3} 2^{i-1} S_i^j\right|^+_{31} = \left|11 + 2\cdot 23 + 4\cdot 2\right|^+_{31} = 3.$$

Let us compute two reference residues T^j = (23, 14, 1) according to Eq. (21). We obtain:

$$T_4^j = \left|\sum_{i=1}^{3} T_i^j\right|^+_{31} = \left|23 + 14 + 1\right|^+_{31} = 7,\ T_5^j = \left|\sum_{i=1}^{3} 2^{i-1} T_i^j\right|^+_{31} = \left|23 + 2\cdot 14 + 4\cdot 1\right|^+_{31} = 24.$$

Similarly, using Eqs. (22)-(24), we have:

$$\tilde{K}^j = (2, 18, 27, 16, 22),\ \tilde{S}^j = (21, 26, 19, 6, 27),\ \tilde{T}^j = (25, 26, 10, 30, 24).$$

Then, according to Eqs. (25)-(27), we have as follows:

$$r^1(j) = \left|\tilde{K}^j - d^j - K^j\right|^+_L = (2, 18, 27, 16, 22) - (7, 4, 22, 12, 10) - (30, 10, 23, 1, 18) =$$
$$= (27, 14, 13, 13, 25).$$

$$r^2(j) = \left|\tilde{S}^j - d^j - S^j\right|^+_{31} = (5, 30, 26, 30, 14),\ r^3(j) = \left|\tilde{T}^j - d^j - T^j\right|^+_{31} = (26, 8, 18, 21, 21).$$

On the basis of Eq. (28), we have:

$$\dddot{r}_4^1(j) = \left|27 + 14 + 13\right|^+_{31} = 13,\ \dddot{r}_5^1(j) = \left|\sum_{i=1}^{3} 2^{i-1} r_i^1(j)\right|^+_{31} = \left|27 + 2\cdot 14 + 4\cdot 13\right|^+_{31} = 25.$$

$$\ddot{r}_4^{2}(j)=\left|5+30+26\right|_{31}^{+}=30,\ \ddot{r}_5^{2}(j)=\left|\sum_{i=1}^{3}2^{i-1}r_i^{2}(j)\right|_{31}^{+}=\left|5+2\cdot 30+4\cdot 26\right|_{31}^{+}=14.$$

$$\ddot{r}_4^{3}(j)=\left|26+8+18\right|_{31}^{+}=21,\ \ddot{r}_5^{3}(j)=\left|\sum_{i=1}^{3}2^{i-1}r_i^{3}(j)\right|_{31}^{+}=\left|26+2\cdot 8+4\cdot 18\right|_{31}^{+}=21.$$

In this case, using Eq. (29), we obtain the error syndrome:

$$\sigma_4^1(j)=\left|r_4^1(j)-\ddot{r}_4^{1}(j)\right|_{31}^{+}=\left|13-13\right|_{31}^{+}=0\,,\ \sigma_5^1(j)=\left|r_5^1(j)-\ddot{r}_5^{1}(j)\right|_{31}^{+}=\left|25-25\right|_{31}^{+}=0.$$

$$\sigma_4^2(j)=\left|r_4^2(j)-\ddot{r}_4^{2}(j)\right|_{31}^{+}=\left|30-30\right|_{31}^{+}=0\,,\ \sigma_5^2(j)=\left|r_5^2(j)-\ddot{r}_5^{2}(j)\right|_{31}^{+}=\left|14-14\right|_{31}^{+}=0.$$

$$\sigma_4^3(j)=\left|r_4^3(j)-\ddot{r}_4^{3}(j)\right|_{31}^{+}=\left|21-21\right|_{31}^{+}=0\,,\ \sigma_5^3(j)=\left|r_5^3(j)-\ddot{r}_5^{3}(j)\right|_{31}^{+}=\left|21-21\right|_{31}^{+}=0.$$

Since the error syndrome is zero, then the responses have no error. Let the error with the depth of $\Delta K_1^j = 29$ occur upon reading of noisy key image. The erroneous residue is $K_1^j=\left|K_1^j+\Delta K_1^j\right|_{31}^{+}=\left|30+29\right|_{31}^{+}=28^{*}$. Then:

$$\hat{r}^1(j)=\left(2,18,27,16,22\right)-\left(7,4,22,12,10\right)-\left(28^{*},10,23,1,18\right)=\left(25^{*},14,13,13,25\right).$$

Let us compute the reference residues by data residues. Then:

$$\ddot{r}_4^{1}(j)=\left|25+14+13\right|_{31}^{+}=11,\ \ddot{r}_5^{1}(j)=\left|\sum_{i=1}^{3}2^{i-1}d_i^{j}\right|_{31}^{+}=\left|25+2\cdot 14+4\cdot 13\right|_{31}^{+}=23.$$

Thus, the error syndrome for the first response is:

$$\sigma_4^1(j)=\left|\hat{r}_4^1(j)-\ddot{r}_4^{1}(j)\right|_{31}^{+}=\left|13-11\right|_{31}^{+}=2\,,\ \sigma_5^1(j)=\left|\hat{r}_5^1(j)-\ddot{r}_5^{1}(j)\right|_{31}^{+}=\left|25-23\right|_{31}^{+}=2.$$

Since the error syndromes coincided, then the error took place in the first residue and its vector was $\bar{e}(j)=\left(29,\,0,\,0,\,0,\,0\right)$. We obtain the following:

$$r^1(j)=\hat{r}^1(j)-\bar{e}(j)=\left(25^{*},14,13,13,25\right)-\left(29,0,0,0,0\right)=\left(27,14,13,13,25\right).$$

The error is corrected.

The described algorithm makes it possible to correct error in the code comprised of residues with regard to one base. Herewith, for implementation of the given example, in addition to six LUT tables required for computation of response, additional 4 LUT tables are required for computation of two reference residues, two LUT tables – for computation of error syndrome, and one LUT table – for storage of error vector. In the case of triplex reservation, 18 LUT tables would be required to compute the response. Therefore, the developed algorithm requires 1.38 time less network consumptions than the error correction with "2 out of 3" correction method.

5. CONCLUSION

This article has discussed the method of development of spacecraft identification system for LEOS constellation using polynomial MC. The importance of correction of distorted responses to requests from onboard interrogator is described. In order to solve this problem, the error correction algorithm was developed based on convolution of information residues. The presented example demonstrated efficiency of the developed algorithm for a code where all residues were obtained with respect to one base concerning detection and correction of single error. Herewith, the developed algorithm using three **PRNS** data bases requires 1.38 time less network consumptions than the error correction with "2 out of 3" correction method.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Basic Research, project No. 18–07-01020.

REFERENCES

1. What Is Iridium NEXT? Available at:http://www.argo.ucsd.edu/sat_comm_AST13.pdf
2. I.A. Kalmykov, V.P. Pashintsev, P.A. Zhuk. **Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication**.*International Journal of Mechanical Engineering and Technology*, Vol. 9, No 5, pp. 958–965, 2018.
3. M. Lapina, I. Provornov. **Development of Imitation-resistable Authentication Protocol for Low-orbital Space Satellite Communication System**. Young Scirntist's. Third International Workshop on Trends in Information Processing (YSIP-2019), Stavropol, September 17-20, 2019. Available at:http://ceur-ws.org
4. I.A. Kalmykov, V.P. Pashintsev, P.A. Zhuk. **Development of Satellite Authentication System for Low Earth Orbit Satellite Communication System on the Basis of Polynomial Residue Number System**.*International Journal of Engineering and Advanced Technology*, Vol. 8, No 5, pp. 2557-2562, 2019.
5. A. Omondi, B. Premkumar. **Residue Number Systems: Theory and Implementation**. Imperial College Press, London, UK,2007, 296 p. https://doi.org/10.1142/p523
6. A. Mohan. **Residue Number Systems. Theory and Applications**. Springer International Publishing, Cham, Switzerland, 2016.
7. E.P. Stepanova, A.V. Makarova. **The use of redundant modular codes for improving the fault tolerance of special processors for digital signal processing**. CEUR Workshop Proceedings. 1837, 2017, 418 p.
8. A.V. Veligosha, D.I. Kaplun, D.M. Klionskiy. **Parallel-pipeline implementation of digital signal processing techniques based on modular codes**. Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM 2016. 7519731, pp.213-214, 2016.
9. K.A. Katkov, L.I. Timoshenko, A.V. Dunin. **Application of Modular Technologies in the Large-Scale Analysis of Signals**. *Journal of Theoretical and Applied Information Technology*, Vol. 80, No 3, pp. 391-400, 2015.
10. N.I. Chervyakov, A.V. Veligosha. **Digital filters in a system of residual classes**.*Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika*, Vol. 38, No 8, pp. 11-20, 1995.
11. A.V. Veligosha, D.I. Kaplun, D.V. Bogaevskiy. **Adjustment of adaptive digital filter coefficients in modular codes**. Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, pp. 1167-1170, 2018.
12. D.I. Kaplun, D.M. Klionskiy, D.V.Bogaevskiy. **Error correcting of digital signal processing devices using non-positional modular codes**.*Automatic Control and Computer Sciences*,Vol. 51, No 3, pp.167-173, 2017.
13. K.T. Tyncherov, N.I. Chervyakov. **Method of increasing the reliability of telemetric well information transmitted by the wireless communication channel**.*Bulletin of the Tomsk Polytechnic University, Geo Assets Engineering,* Vol. 329, No 3, pp. 36-43, 2018.
14. D.A. Yurdanov, D.B. Gostev. **The implementation of information and communication technologies with the use of modular codes**. CEUR Workshop Proceedings 1837, 418 p., 2017.
15. M. Lapina, N. Kononova, M. Kalmikov. **Development of the protocol "Electronic Cash" with inspection correction rules of the electronic e-cash number for e-Commerce systems**. CEUR Workshop Proceedings 2254, pp. 147-153, 2018.
16. D. Unruh. **Post-quantum security of Fiat-Shamir**. In: "Advances in Cryptology – ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science", vol. 10624, Part I (editors: T. Takagi, T. Peyrin), Springer, Cham. pp. 65–95, 2017.
17. E. Kiltz, V. Lyubashevsky, C. Schaffner. **A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model**. In: Advances in Cryptology – EUROCRYPT 2018. EUROCRYPT 2018. Lecture Notes in Computer Science, vol. 10822 (editors: J. Nielsen, V. Rijmen), Springer, Cham. pp. 552-586, 2018.
18. V.P. Pashentsev, A.V. Lyakhov. **Application of a noise-tolerant authentication protocol for a spacecraft for a low-orbit satellite communications system**. *Infocommunication Technologies*, Vol. 2,pp. 183-190, 2015. https://doi.org/10.18469/ikt.2015.13.2.11
19. E.P. Stepanova, E.V. Toporkova, R.A. Katkov. **Application of the codes of a polynomial residue number system, aimed at reducing the effects of failures in the AES cipher**. *Journal of Digital Information Management*, Vol. 14, No 2, pp. 114-123, 2016.