Developing method for constructing modular turbo code for anti-jam satellite authentication system

I A Kalmykov\textsuperscript{1,2}, V Sh Mukhametshin\textsuperscript{2}, K T Tyncherov\textsuperscript{2} and M V Selivanova\textsuperscript{2}

\textsuperscript{1}North-Caucasus Federal University, Stavropol, Russian Federation
\textsuperscript{2}Ufa State Petroleum Technological University, Branch of the University in the City of Oktyabrsky, Oktyabrsky, Republic of Bashkortostan, Russian Federation

E-mail: kia762@yandex.ru, info@of.ugntu.ru

Abstract. Low-earth orbit (LEO) satellite communication systems must have anti-jam property, which is based on information, structural and energy secrecy as well as immunity to jamming. One of the directions associated with increasing information secrecy is based on the use of a satellite identification system. This system is designed to prevent the imposition of foreign content on the subscriber through the use of an authentication protocol built on proof with zero knowledge. To reduce the time of applicant identification, a number of works propose to use modular codes (MC), which allow parallelizing the computational process in the protocol. It is known that MCs can improve the fault tolerance of the identification system since they are able to eliminate the consequences of faults and failures during operation. However, they can also be used to improve the immunity of LEO satellite communication systems to jamming. Thus, the use of a unified algebraic system when constructing MCs capable of correcting errors caused not only by faults and failures during the operation of the identification system but also by interference in the communication channel will enable to abandon concatenated codes. Therefore, the development of a method for constructing a modular turbo code for an anti-jam satellite authentication system is an urgent task.

1. Introduction
The increased interest in low-earth orbit (LEO) satellite communication systems, which has appeared in the last decade, is associated with the development and implementation of many global projects related to the development of the Arctic Ocean and its coastal zone. This includes the development of the Northern Sea Route, the search and commissioning of hydrocarbon deposits located beyond the Arctic Circle. This means that such LEO satellite communication systems should have immunity to jamming, which is based on information, structural and energy secrets, as well as on the immunity of the data transmission system to jamming [1,2]. A number of works [3,4] propose to use a satellite identification system to increase the information secrecy of the LEO satellite communication systems. One of the methods aimed to reduce the time for applicant’s status calculation is the implementation of the satellite authentication protocols in modular code (MC). Since modular codes are arithmetic, they are widely used to improve the fault tolerance of high-speed computing systems [5-7]. Thus, the introduction of two control bases allows the MC to correct a burst of errors within one remainder in a codeword. It is possible to increase the efficiency of modular codes by developing new principles for constructing MC. Therefore, the purpose of the article is to increase the immunity of the satellite authentication system to jamming through the use of a modular turbo code.
2. Materials and methods

2.1 Principles of constructing modular codes

It is stated in [8,9], that the integer Y in MC is represented as a tuple of remainders

\[ Y = (y_1, y_2, \ldots, y_k) \]

which are obtained by dividing Y by the selected co-prime numbers being the bases \( m_i \), \( m_2, \ldots, m_k \), where \( \text{gcd}(m_i, m_j) = 1 \). In this case, the bases set the following working range

\[ \hat{M} = \prod_{i=1}^{k} m_i. \]

Using MC, it is possible to represent arithmetic operations in the following form

\[ Y \circ D = \left\{ y_1 \circ d_1 \left[ \mod m_1 \right], y_2 \circ d_2 \left[ \mod m_2 \right], \ldots, y_k \circ d_k \left[ \mod m_k \right] \right\}, \]

where \( \circ \) denotes the operations of addition, subtraction, multiplication; \( d_i \equiv D \mod m_i \);

\[ y_i \equiv Y \mod m_i. \]

Analysis of expression (3) has showed that these modular operations can be replaced by parallel and independent operations of addition, subtraction and multiplication with low-discharge remainders. Therefore, MCs are used in high-speed computing systems. Thus, in [10] modular codes are used to construct an adaptive digital filter. In [11], it is proposed to use MC for error correction in the AES encryption algorithm.

In order to reduce the time of satellite identification, a spacecraft (SC) authentication protocol based on MC has been developed. In this protocol, U is the secret key of the SC, \( S \) is the session key of the SC, \( T \) is an additional number that is used in the equation enabling to obtain the public key of the SC when the secondary use of \( S \), which must satisfy \( \{ U, S, T \} \), \( < \hat{M} \).

Afterwards, they are transferred to MC. As a result, we get \( U = (u_1, u_2, \ldots, u_k) \), \( S = (S_1, S_2, \ldots, S_k) \), \( T = (T_1, T_2, \ldots, T_k) \), where \( u_i = \mod m_i \), \( S = S \mod m_1 \); \( T = T \mod m_1 \); \( i = 1, 2, \ldots, k \).

1. To conduct the \( j \)-th communication session, the transponder calculates the true status of the satellite

\[ C_j = (C_{j1}, C_{j2}, \ldots, C_{jk}) \]

where \( C_{ji} = \left\{ g^n \cdot g^{S_i} \cdot g^{T_i} \right\} \mod m_i \); \( g \) is a cyclic parent; \( i = 1, 2, \ldots, k \).

2. Afterwards, the transponder makes random changes \( \{ \Delta u_1, \Delta S_1, \Delta T_1 \} \)

\[ \tilde{u}_i = (u_i + \Delta u_i) \mod \phi(m_i), \tilde{S}_i = (S_i + \Delta S_i) \mod \phi(m_i), \tilde{T}_i = (T_i + \Delta T_i) \mod \phi(m_i), \]

where \( \{ \Delta u_1, \Delta S_1, \Delta T_1 \} < \phi(m_i) \); \( \phi(m_i) \) is Euler function of the base \( m_i \); \( i = 1, 2, \ldots, k \).

3. Thereafter, the noisy status of the spacecraft is determined using the MC

\[ \tilde{C}_j = (\tilde{C}_{j1}, \ldots, \tilde{C}_{jk}) = \left\{ g^{\tilde{u}_{i1}} \cdot g^{\tilde{S}_{i1}} \cdot g^{\tilde{T}_{i1}} \left[ \mod m_i \right], \ldots, g^{\tilde{u}_{ik}} \cdot g^{\tilde{S}_{ik}} \cdot g^{\tilde{T}_{ik}} \left[ \mod m_i \right] \right\}. \]

4. At the authentication stage, the interrogator generates a random number and represents it as \( d_j = (d_{j1}, d_{j2}, \ldots, d_{jk}) \), where \( d_{ji} = d_j \mod m_i \) and then passes it to the transponder.

5. Having received \( d_j = (d_{j1}, d_{j2}, \ldots, d_{jk}) \), the transponder answers the interrogator’s question regarding

\[ r_{j1} = \left[ \tilde{u}_{i1} - d_{j1} \cdot u_{1i} \right] \mod m_i, r_{j2} = \left[ \tilde{S}_{i1} - d_{j1} \cdot S_{1i} \right] \mod m_i, r_{j3} = \left[ \tilde{T}_{i1} - d_{j1} \cdot T_{1i} \right] \mod m_i. \]

6. The transponder transmits \( \{ C_{j1}, \ldots, C_{jk}, (\tilde{C}_{j1}, \ldots, \tilde{C}_{jk}), (r_{j1}, \ldots, r_{j3}), (r_{j2}, \ldots, r_{j3}), (r_{j3}, \ldots, r_{j3}) \} \).
7. Having received the transponder’s signal, the transponder calculates the status of the spacecraft

\[ Y_i^j = \left[ C_i^j \cdot g_i \cdot g_i^2 \cdot g_i^3 \right] \mod 2. \tag{8} \]

The interrogator assigns the status “friend” to the satellite if

\[ \{ Y_i^1 = \tilde{C}_i^1, Y_i^2 = \tilde{C}_i^2, ..., Y_i^j = \tilde{C}_i^j \}. \]

If the transmitted signal is affected by interference in the process of authentication, then the “friend” satellite will be perceived as “foe”, and it will not receive a communication session. Let us consider a method for constructing a turbo code for an anti-jamming satellite authentication system.

In the developed protocol, the interrogator receives the transponder’s signal, which consists of five parts. Therefore, the developed modular turbo code must contain at least five remainders. For ease, we will use a single type of remainder \( \alpha \), i.e.

\[ (C_i^1, C_i^2, C_i^3, C_i^4, C_i^5), \]

\[ (\tilde{C}_i^1, \tilde{C}_i^2, \tilde{C}_i^3, \tilde{C}_i^4, \tilde{C}_i^5), \]

\[ (r_i^1, r_i^2, r_i^3, r_i^4, r_i^5), \]

\[ (r_i^2, r_i^3, r_i^4, r_i^5), \]

\[ (r_i^3, r_i^4, r_i^5). \]

\[ \Rightarrow A_{COK} = \{ \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}, \alpha_{17} \} \]

\[ \alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24}, \alpha_{25}, \alpha_{26}, \alpha_{27} \]

\[ \alpha_{31}, \alpha_{32}, \alpha_{33}, \alpha_{34}, \alpha_{35}, \alpha_{36}, \alpha_{37} \]

\[ \alpha_{41}, \alpha_{42}, \alpha_{43}, \alpha_{44}, \alpha_{45}, \alpha_{46}, \alpha_{47} \]

\[ \alpha_{51}, \alpha_{52}, \alpha_{53}, \alpha_{54}, \alpha_{55} \]. \tag{9}

\[ \text{COK – RNS} \]

It is possible to correct a single error in the MC using two control bases \( m_{k+1}m_k < m_{k+1}m_{k+2} \) [7,8]. As a result, we get the full range of MC

\[ M = \prod_{i=1}^{k+2} m_i = \tilde{M} \prod_{i=k+1}^{k+2} m_i. \tag{10} \]

In this case, the extended MC combination does not contain an error only when executing

\[ Y = (y_1, y_2, ..., y_{k+2}) < \tilde{M}. \tag{11} \]

In this case, the modular turbo code has the following form:

\[ A_{MKK} = \left\{ \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}, \alpha_{17} \right\} \]

\[ \alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24}, \alpha_{25}, \alpha_{26}, \alpha_{27} \]

\[ \alpha_{31}, \alpha_{32}, \alpha_{33}, \alpha_{34}, \alpha_{35}, \alpha_{36}, \alpha_{37} \]

\[ \alpha_{41}, \alpha_{42}, \alpha_{43}, \alpha_{44}, \alpha_{45}, \alpha_{46}, \alpha_{47} \]

\[ \alpha_{51}, \alpha_{52}, \alpha_{53}, \alpha_{54}, \alpha_{55} \]. \tag{12}

In this case, the horizontal control remainder are calculated according to

\[ \alpha_{v0} = \sum_{i=1}^{5} \alpha_{vi}B_i \mod \tilde{M} \mod m_6, \]

\[ \alpha_{v7} = \sum_{i=1}^{5} \alpha_{vi}B_i \mod \tilde{M} \mod m_7, \tag{13} \]

where \( v = 1, 2, 3, 4, 5 \); \( B_i = h_i M m_6^{-1} \) is orthogonal base; \( h_i \) is orthogonal base weight.

In this case, the vertical control residues, with \( j=6, 7 \), are calculated according to
\[
\alpha^2_i = \left[\alpha_{11}B_1 + \alpha_{22}B_2 + \alpha_{33}B_3 + \alpha_{54}B_4 + \alpha_{55}B_5\right] \mod \hat{M}_{m_i}^+, \\
\alpha^2_j = \left[\alpha_{21}B_1 + \alpha_{32}B_2 + \alpha_{43}B_3 + \alpha_{44}B_4 + \alpha_{25}B_5\right] \mod \hat{M}_{m_j}^+, \\
\alpha^2_l = \left[\alpha_{31}B_1 + \alpha_{12}B_2 + \alpha_{53}B_3 + \alpha_{24}B_4 + \alpha_{15}B_5\right] \mod \hat{M}_{m_l}^+, (14) \\
\alpha^2_j = \left[\alpha_{41}B_1 + \alpha_{52}B_2 + \alpha_{13}B_3 + \alpha_{14}B_4 + \alpha_{35}B_5\right] \mod \hat{M}_{m_j}^+, \\
\alpha^2_l = \left[\alpha_{51}B_1 + \alpha_{42}B_2 + \alpha_{23}B_3 + \alpha_{34}B_4 + \alpha_{55}B_5\right] \mod \hat{M}_{m_l}^+.
\]

To correct errors, we use a positional characteristic being the interval

\[
S_6 = \left[\frac{A}{M}\right]_{m_6}^{+} = \sum_{i=7}^{7} \alpha_i R_i + \hat{r} \mod \hat{M}_{m_i}^+, \\
S_7 = \left[\frac{A}{M}\right]_{m_7}^{+} = \sum_{i=7}^{7} \alpha_i R_i + \hat{r} \mod \hat{M}_{m_i}^+, (15)
\]

where \(B_i = R_i \hat{M} + \hat{B}_i \hat{B}_i^T\) and \(\hat{r} = \sum_{i=1}^{5} \hat{B}_i / \hat{M}\) are orthogonal base and rank in the non-redundant RNS.

If the combination \(A = (\alpha_1,...,\alpha_7) < \hat{M}\), then it does not contain an error and \(P X S_i = 0\).

The developed method for constructing a modular turbo code enables to correct all double errors arising in one MC combination. As such, we take the first combination \(A_1\), in which the remainders \(\alpha^*_{11}\) and \(\alpha^*_{13}\) with the error depth \(\Delta\alpha_{11}\) and \(\Delta\alpha_{13}\), respectively, are erroneous. Then we get such a combination

\[
A^*_1 = (\alpha^*_{11}, \alpha^*_{12}, \alpha^*_{13}, \alpha^*_{14}, \alpha^*_{15}, \alpha^*_{16}, \alpha^*_{17}) = \left[\alpha_{11} + \Delta\alpha_{11}, \alpha_{12}, \alpha_{13} + \Delta\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha^*_{16}, \alpha^*_{17}\right].
\]

We will use the Chinese remainder theorem to translate the positional code

\[
A^*_1 = A + \left[\Delta\alpha_{11} \right]_{m_1}^{+} B_1 + \left[\Delta\alpha_{13} \right]_{m_3}^{+} B_3 \mod M, (16)
\]

Let us use the expression (19). Then the interval of this combination is as follows

\[
S^*_{16} = \left[\frac{A^*_1}{M}\right] \mod m_6 = S^*_{16} + S^*_{13} \mod m_6, \\
S^*_{17} = \left[\frac{A^*_1}{M}\right] \mod m_7 = S^*_{11} + S^*_{13} \mod m_7, (17)
\]

where \(S^*_{11}, S^*_{13}\) are the numbers of the intervals with MC when one-time errors \(\alpha^*_1 = (\alpha_{11} + \Delta\alpha_{11}) \mod m_1\) and \(\alpha^*_3 = (\alpha_{13} + \Delta\alpha_{13}) \mod m_3\) occur.

It is known that MC cannot correct a double error when using two control bases. However, the developed method enables to eliminate this drawback. After all, erroneous residues \(\alpha^*_1\) and \(\alpha^*_3\) are used in calculations \((S^*_{16}, S^*_{17})\), \((S^*_{16}, S^*_{17})\).

3. Results and Discussion

We choose the modules \(m_1 = 7, m_2 = 11, m_3 = 13, m_4 = 19, m_5 = 29\) for MC. Then the working range is \(\hat{M} = \prod_{i=1}^{5} m_i = 551551\). Let the redundant modules be \(m_6 = 37, m_7 = 43\). Then the full range is \(M = 877517641\) [13]. We have a transponder signal presented in MC \(C^1 = (2, 2, 15, 17, 4, 14)\).
\[
\tilde{C}^1 = (2, 4, 7, 3, 26, 12, 1), \quad r^1 = (1, 3, 7, 1, 6, 8, 9), \quad r^2 = (5, 10, 0, 12, 20, 25, 5), \quad r^3 = (1, 7, 8, 1, 5, 29, 42).
\]

Let there be errors with depth \( \Delta \alpha_{11} = 3 \) and \( \Delta \alpha_{13} = 4 \) when transmitting the true status of the satellite. Then we get \( \alpha_{11}^* = \left( \alpha_{11} + \Delta \alpha_{11} \right) \mod m_1 = 2 + 3 \mod 5 = 5 \), \( \alpha_{13}^* = \left( \alpha_{13} + \Delta \alpha_{13} \right) \mod m_1 = 2 + 4 \mod 5 = 6 \). Then,

\[
\Lambda_1^* = (\alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}, \alpha_{17}) = (5^*, 2, 6^*, 15, 17, 4, 14).
\]

Let us calculate the values of the interval for this erroneous combination

\[
S_{16}^1 = \left[ \alpha_{11}^* R_1 + \alpha_{12}^* R_2 + \alpha_{13}^* R_3 + \alpha_{14}^* R_4 + \alpha_{15}^* R_5 + \alpha_{16}^* R_6 + \alpha_{17}^* R_7 + \tilde{t} \right] \mod m_6 = 34.
\]

Then the interval is as follows

\[
S_{17}^1 = \left[ \alpha_{11}^* R_1 + \alpha_{12}^* R_2 + \alpha_{13}^* R_3 + \alpha_{14}^* R_4 + \alpha_{15}^* R_5 + \alpha_{16}^* R_6 + \alpha_{17}^* R_7 + \tilde{t} \right] \mod m_7 = 34.
\]

However, this interval does not correspond to the one-time error interval. Therefore, the decoder, when receiving the interval \((S_{16}^1, S_{17}^1)\) is unable to correct an error in the code. The application of the developed method eliminates this disadvantage. Let us calculate \((S_{16}^2, S_{17}^2)\).

\[
S_{16}^2 = \left[ \alpha_{11}^* R_1 + \alpha_{12}^* R_2 + \alpha_{13}^* R_3 + \alpha_{14}^* R_4 + \alpha_{15}^* R_5 + \alpha_{16}^* R_6 + \alpha_{17}^* R_7 + \tilde{t} \right] \mod m_6 = \|137\|_37 = 27.
\]

The resulting interval corresponds to the error \(\alpha_{11}^*\) with the depth \(\Delta \alpha_{11} = 3\). In this case, the erroneous remainder \(\alpha_{13}^*\) is used in calculations \((S_{26}^2, S_{27}^2)\). Then the interval is as follows

\[
S_{26}^2 = \left[ \alpha_{41}^* R_1 + \alpha_{52}^* R_2 + \alpha_{13}^* R_5 + \alpha_{14}^* R_4 + \alpha_{15}^* R_5 + \alpha_{26}^* R_6 + \alpha_{27}^* R_7 + \tilde{t} \right] \mod m_9 = \|490\|_37 = 9.
\]

The resulting interval corresponds to the error \(\alpha_{13}^*\) with the depth \(\Delta \alpha_{13} = 4\). Correction of the codogram is performed according to

\[
A_1 = \Lambda_1^* - \tilde{c} = (5^*, 2, 6^*, 15, 17, 4, 14) - (3, 0, 4, 0, 0, 0, 0, 0) = (2, 2, 2, 15, 17, 4, 14).
\]

To assess the effectiveness of the method for constructing a modular turbo code, a software package enabling to simulate a communication channel with impulse noise was created. It was compared with the RNS code having four control bases \(m_6 = 37, m_7 = 43, m_8 = 47, m_9 = 53\), and fixes double errors. The results of the research are shown in the figure.

The analysis of the figure shows that the application of the developed method for constructing the modular turbo code benefits the increase of the immunity of the identification system to jamming. Thus, with the signal-to-noise ratio \(E_b/N_0 = 13\) dB, the probability of a system error with the developed method is \(P_{err} = 3 \cdot 10^{-5}\), while for the classical RNS it is \(P_{err} = 8.6 \cdot 10^{-5}\). This means that the developed method increases the immunity of the identification system to jamming by 2.86 times in comparison with the classical method of constructing correcting RNS codes.
4. Conclusion
The article shows the relevance of the development of modular compositional code. An algorithm for searching and correcting multiple errors in a modular compositional code is considered. An example of the implementation of a modular turbo code is presented. It is shown that for the signal-to-noise ratio $E_b/N_0 = 13\text{dB}$, the system error probability with the developed method is $P_{err} = 3 \cdot 10^{-5}$, while for the classical RNS it is $P_{err} = 8.6 \cdot 10^{-5}$. Thus, the developed method increases the immunity of the identification system to jamming by 2.86 times in comparison with the classical method of constructing correcting RNS codes.

References
[1] Gorbenko I D, Zamula A A, Morozov V L 2017 Telecommunications and Radio Engineering 76 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30
[2] Pashintsev V P, Peskov M V, Zhuk A P A 2018 International Journal of Civil Engineering and Technology 9(13) 44-61
[3] Kalmykov I A, Pashintsev V P, Zhuk A P, Chistousov N K 2019 International Journal of Engineering and Advanced Technology (IJET) 8(5) 2557-2562
[4] Pashintsev V P, Zhuk A P, Rezenkov D N 2018 International Journal of Mechanical Engineering and Technology (IJMET) 9(5) 958-965
[5] Tyncherov K T, Mukhametshin V Sh and Rakhimov N R 2021 Theoretical basis for constructing special codes for a noise-resistant downhole telemetry system Journal of Physics: Conference Series (IPDME-2020 – International Conference on Innovations, Physical Studies and Digitalization in Mining Engineering) 1753 012081 1-5 DOI: 10.1088/1742-6596/1753/1/012081
[6] Makarova A V, Stepanova E P, Toporkova E V 2017 The use of redundant modular codes for improving the fault tolerance of special processors for digital signal processing 2017 CEUR Workshop Proceedings 1837 115-122
[7] Kaplun D I, Klionskiy D M, Bogaevskiy D V 2017 Error correction of digital signal processing
devices using non-positional modular codes *Automatic Control and Computer Sciences* **51**(3) 167-173

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

[9] Mohan P V 2016 *Residue Number Systems: Theory and Applications* (New York: Springer)

[10] Veligosha A V, Kaplun D I, Bogaevskiy D V 2018 Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2018) 1167-1170

[11] Stepanova E P, Toporkova E V, Rezenkov D N 2016 *Journal of Digital Information Management* **14**(2) 114-123

[12] Mohan P V 2002 *Residue Number Systems: Algorithms and Architectures* (London: Kluwer Academic Publishers)

[13] Tyncherov K T, Mukhametshin V Sh and Rakhimov N 2021 Selection and justification of efficiency parameters of a noise-resistant downhole telemetry system *IOP Conference Series: Materials Science and Engineering (International Conference on Mechanical Engineering, Automation and Control Systems (MEACS 2020))* **1064** 012072 1-6 DOI:10.1088/1757-899X/1064/1/012072