Science and Technology City Hall
KRASNOYARSK, RUSSIA

«MIST: Aerospace-IV 2021»

«Application of modular turbo codes in authentication systems»

N.K. Chistousov, I.A. Kalmykov, D.V. Dukhovnyj, I.D. Efremenkov, N.I. Kalmykova

Problem statement

The main goal is to use principles of turbo codes and modular codes in order to:

- increase the noise immunity of satellite communication systems;
- provide an authentication procedure for space crafts;
- use the same kind of code for both calculations during the execution of authentication protocol and forwarding information over communication channel.

Solution methods

- Turbo codes

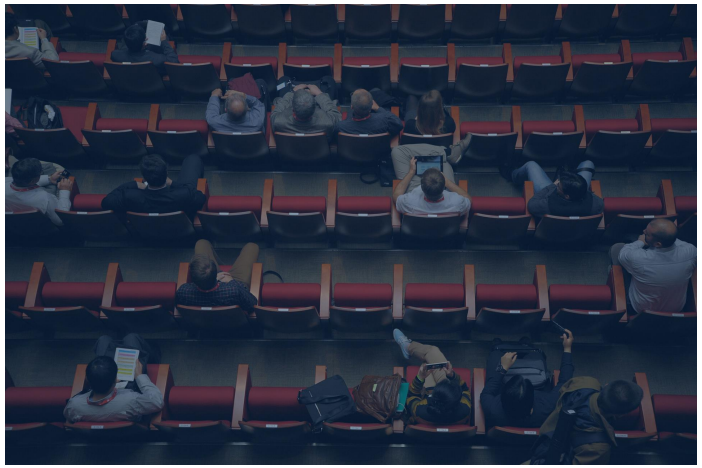
$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & h_{11} & h_{12} & \dots & h_{1k} \\ a_{21} & a_{22} & \dots & a_{2n} & h_{21} & h_{22} & \dots & h_{2k} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & h_{n1} & h_{n2} & \dots & h_{nk} \\ v_{11} & v_{21} & \dots & v_{n1} & c_{11} & c_{12} & \dots & c_{1k} \\ v_{12} & v_{22} & \dots & v_{n2} & c_{21} & c_{22} & \dots & c_{2k} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ v_{1k} & v_{2k} & \dots & v_{nk} & c_{k1} & c_{k2} & \dots & c_{kk} \end{pmatrix}$$

- Modular codes

$$\gcd(m_i, m_j) = 1 \; \forall \; i \neq j$$

$$\widehat{M} = \prod_{i=1}^{n} m_i \, , M = \prod_{i=1}^{n+k} m_i = \widehat{M} \prod_{i=1}^{k} m_{n+i} \, ;$$

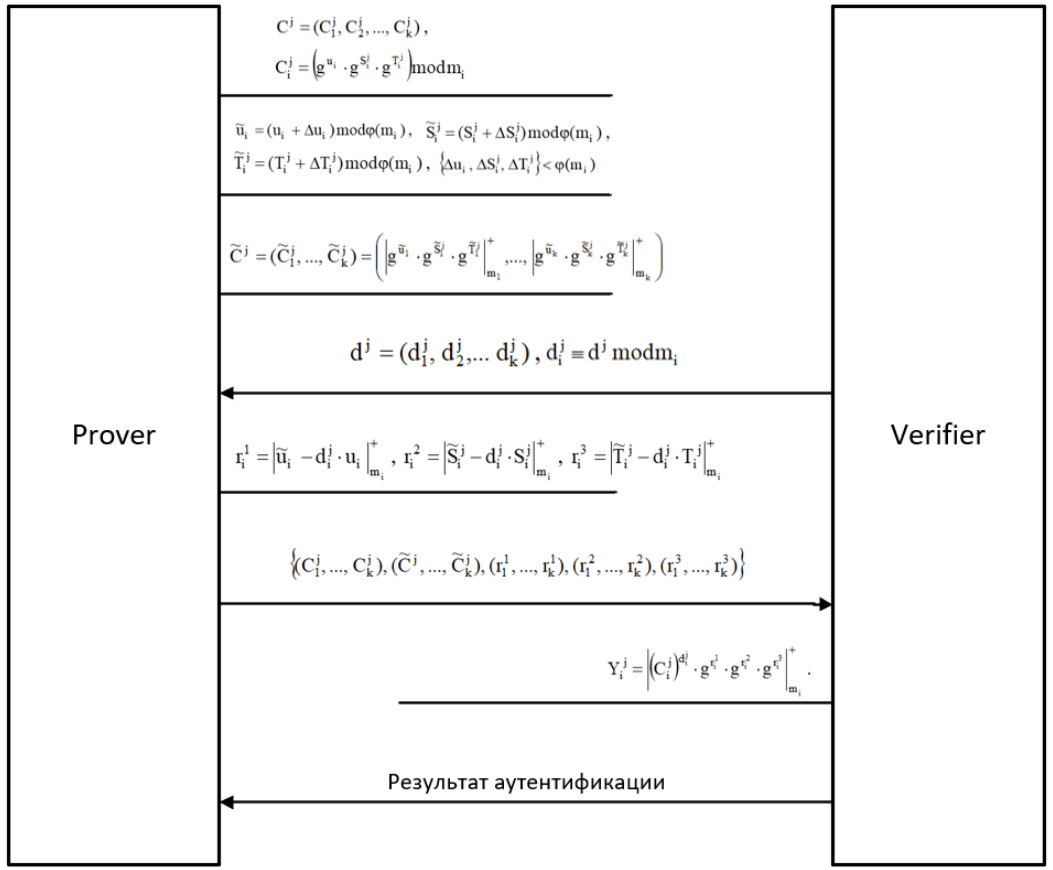
$$Y = (y_1, y_2, \dots, y_n, y_{n+1}, y_{n+2}, \dots, y_{n+k}), y_i = Y \bmod m_i.$$

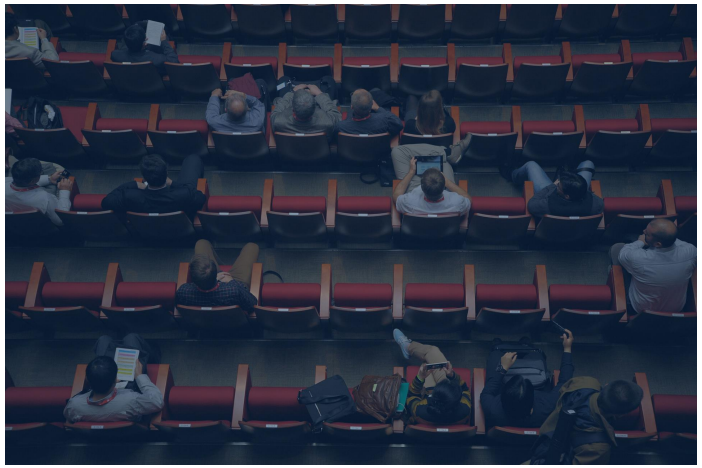


Science and Technology City Hall
KRASNOYARSK, RUSSIA

Solution methods

- Authentication protocol with usage of modular codes





Science and Technology City Hall
KRASNOYARSK, RUSSIA

Solution methods

- Structure of the developed modular turbo code

$$\begin{matrix}(C_1^j, C_2^j, C_3^j, C_4^j, C_5^j),\\ (\widetilde{C}_1^j, \widetilde{C}_2^j, \widetilde{C}_3^j, \widetilde{C}_4^j, \widetilde{C}_5^j),\\ (r_1^1, r_2^1, r_3^1, r_4^1, r_5^1),\\ (r_1^2, r_2^2, r_3^2, r_4^2, r_5^2),\\ (r_1^3, r_2^3, r_3^3, r_4^3, r_5^3).\end{matrix} \Rightarrow A_{RNS} = \begin{cases}(\alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15})\\ (\alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24}, \alpha_{25})\\ (\alpha_{31}, \alpha_{32}, \alpha_{33}, \alpha_{34}, \alpha_{35})\\ (\alpha_{41}, \alpha_{42}, \alpha_{43}, \alpha_{44}, \alpha_{45})\\ (\alpha_{51}, \alpha_{52}, \alpha_{53}, \alpha_{54}, \alpha_{55})\end{cases}$$

- Calculation of residues

$$\alpha_{v6}^1 = \left(\sum_{i=1}^{5} \alpha_{vi} B_i \bmod \hat{M}\right) \bmod m_6, \alpha_{v7}^1 = \left(\sum_{i=1}^{5} \alpha_{vi} B_i \bmod \hat{M}\right) \bmod m_7$$

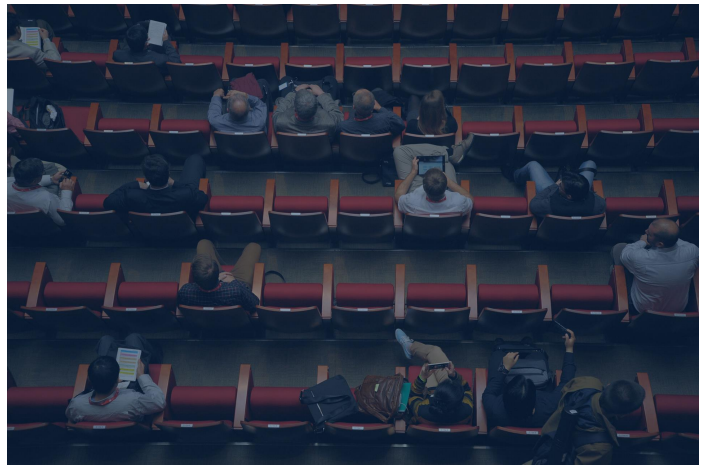
$$\alpha_{1j}^2 = \left|\left(\alpha_{11}B_1 + \alpha_{22}B_2 + \alpha_{33}B_3 + \alpha_{54}B_4 + \alpha_{55}B_5\right) \bmod \hat{M}\right|_{m_j}^+,$$

$$\alpha_{2j}^2 = \left|\left(\alpha_{21}B_1 + \alpha_{32}B_2 + \alpha_{43}B_3 + \alpha_{44}B_4 + \alpha_{25}B_5\right) \bmod \hat{M}\right|_{m_j}^+,$$

$$\alpha_{3j}^2 = \left|\left(\alpha_{31}B_1 + \alpha_{12}B_2 + \alpha_{53}B_3 + \alpha_{24}B_4 + \alpha_{15}B_5\right) \bmod \hat{M}\right|_{m_j}^+,$$

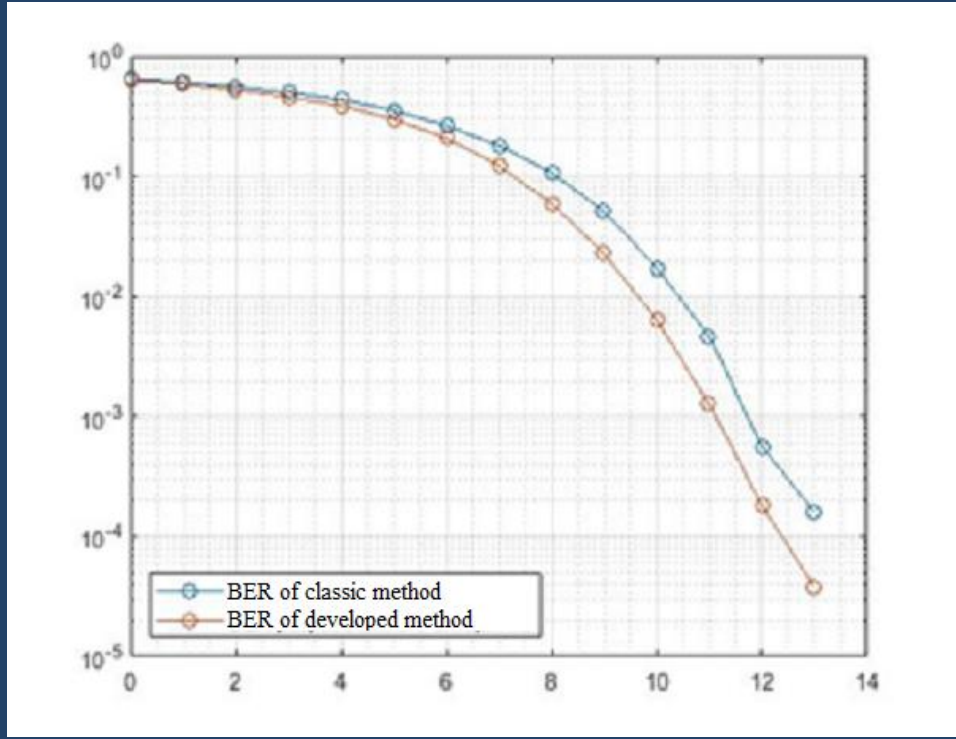
$$\alpha_{4j}^2 = \left|\left(\alpha_{41}B_1 + \alpha_{52}B_2 + \alpha_{13}B_3 + \alpha_{14}B_4 + \alpha_{35}B_5\right) \bmod \hat{M}\right|_{m_j}^+,$$

$$\alpha_{5j}^2 = \left|\left(\alpha_{51}B_1 + \alpha_{42}B_2 + \alpha_{23}B_3 + \alpha_{34}B_4 + \alpha_{55}B_5\right) \bmod \hat{M}\right|_{m_j}^+.$$



Science and Technology City Hall
KRASNOYARSK, RUSSIA

Conclusions



Bit error rates comparison

- Program simulation was created to compare the noise immunity of system for two cases: using not modified authentication protocol and using developed modular turbo code.
- When a signal-to-noise ratio is 13 dB, the probability of a system error using the developed method is $3 \cdot 10^{-5}$ while for the classic RNS it is $8.6 \cdot 10^{-5}$. It means an increase of noise immunity of the system in 2.86 times.

Contacts

N.K. Chistousov, I.A. Kalmykov, D.V. Dukhovnyj, I.D. Efremenkov, N.I. Kalmykova
North Caucasus Federal University, Stavropol
E-mail: kia762@yandex.ru