Developing “friend or foe” protocol in residue number system code for satellite authentication

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, 1, Pushkina St., Stavropol, 355017 Russian Federation
\textsuperscript{2}Ufa State Petroleum Technological University, Branch of the University in the City of Oktyabrsky, 54a, Devonskaya St., Oktyabrsky, Republic of Bashkortostan, 452607, Russian Federation

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

Abstract. Low-earth orbit (LEO) satellite communication systems are successfully used in control and monitoring systems for the production and transportation of hydrocarbons from fields located beyond the Arctic Circle. As the number of countries engaged in the development of such fields expands, the number of groupings of LEO satellite communication systems grows as well. To prevent the possibility of intercepting and imposing a delayed command to control the intruder satellite, it is necessary to use the “friend or foe” identification system for the LEO satellite communication systems. At the same time, it is proposed to use authentication protocols with zero knowledge to ensure high imitation resistance in such systems. To increase their efficiency, the article proposes to use the codes of the residual number system (RNS). The novelty of this idea lies in the fact that the use of parallel RNS codes will reduce the time spent on performing arithmetic operations implemented in authentication protocols. This will reduce the likelihood of an intruder satellite picking up the correct response signal. Therefore, the development of an authentication protocol for LEO satellite communication systems based on RNS codes, the use of which will reduce the time for satellite identification, is an urgent task.

1. Introduction

At present, only low-earth orbit (LEO) satellite communication systems are able to organize effective management of the production and transportation of hard-to-recover hydrocarbons [1] at unattended facilities located beyond the Arctic Circle. However, an increase in the number of countries engaged in the development of deposits in the Arctic Ocean entails an increase in the number of groupings of LEO satellite communication systems. To prevent the possibility of intercepting and imposing a delayed command to control the intruder satellite, it is necessary to increase the information secrecy of the LEO satellite communication systems. Therefore, the development of a “friend or foe” identification system for the LEO satellite communication systems is an urgent task. It is known that the authentication protocols with zero knowledge increase the mimic resistance of the satellite identification system without secret keys [1–3]. However, these protocols are iterative in nature. To reduce the time spent on determining the satellite status, it is necessary to use parallel computations implemented in the code of the residual number system (RNS). The novelty of this idea lies in the fact that the use of parallel RNS codes will reduce the time spent on performing arithmetic operations implemented in authentication protocols. And this, in turn, will lead to an increase in the information secrecy of the LEO satellite.
communication systems. Thus, the likelihood of the correct response signal selection by the intruder satellite decreases. Therefore, the purpose of the article is to develop a LEO satellite communication systems authentication protocol based on RNS codes as their use will reduce the time for satellite identification.

2. Materials and methods

2.1 Principles of constructing modular codes

RNS codes refer to arithmetic codes used for calculations with integers [4-6]. For this, numbers that become the base of the code \( m_1, m_2, \ldots, m_k \), where \( \text{GCD}(m_i, m_j) = 1, \ i \neq j \) are selected. The product of these bases gives the operating range of the RNS

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

Then the number \( A \), has the following form in the RNS code if it is less than the working range:

\[
A = (a_1, a_2, \ldots, a_k) ,
\]

where \( a_i \equiv A \mod m_i ; i = 1, \ldots, k \).

Since the RNS codes are implemented in a ring of integers, the following equality holds true:

\[
A * C = ((a_1 * c_1) \mod m_1, (a_2 * c_2) \mod m_2, \ldots, (a_k * c_k) \mod m_k) ,
\]

where * denotes addition, subtraction and multiplication operations; \( c_i \equiv C \mod m_i ; i = 1, \ldots, k \).

The analysis of equality (3) showed that the use of RNS codes enables to reduce the time spent on performing modular operations. This is determined by the low bit depth of the RNS code remainders, as well as the parallel execution of these operations on the basis of the code. Therefore, RNS codes are widely used in real-time systems. Thus, the work [7] shows the implementation of a digital filter in the RNS. The work [8] presents a method of increasing the reliability of telemetric well information transmitted by the wireless communication channel. The work [9] shows the use of RNS codes when performing Fourier-like orthogonal transformations of signals.

However, RNS codes can be used in authentication protocols based on zero knowledge proofs. These protocols provide high imitation strength of authentication without the use of encryption systems. In [10], a new authentication scheme based on the Fiat-Shamir protocol was developed for the exchange of confidential information in the Internet of Things technology. The works [11,12] show the application of the Feige-Fiat-Shamir authentication protocol for machine authentication in the integration of external networks and the Internet of vehicles (IoV). However, these protocols cannot be used in a friend or foe system for satellites since the identification process requires 20 to 40 times of authentication. Therefore, an analysis enabling to identify authentication protocols that have one stage of recognition was carried out. These include the Guillou-Quisquater and Shnor protocols [13, 14]. However, analysis of these protocols has showed that the authentication stage includes four steps required to determine the status of the applicant. The authentication protocol described in [15] enables to reduce the number of such steps. In this protocol, the identification procedure is reduced to three steps being as follows: the question of the examiner, the calculation of the answer by the applicant and the verification of the correctness of the answer. However, this protocol uses a large prime number to perform authentication. And all the calculations are performed with regards to its modulus. Let us develop this protocol in the RNS code.

2.2. Preliminary stage of the protocol

1. The applicant has a secret key \( W \) being an initial parameter \( C \) for calculating the \( n \)-th session key \( C(n) \), where \( n = 1, 2, \ldots \) is the number \( B \), with which the argument \( B(n) \) is iteratively calculated and which allows determining the fact of double use of the session key. These parameters are represented in the
RNS code \((W_1(n), W_2(n), ..., W_k(n))\), \((C_1(n), C_2(n), ..., C_k(n))\), \((B_1(n), B_2(n), ..., B_k(n))\). In this case, the bases of the RNS code having the same generating element \(a_1 = a_2 = ... = a_k\) are chosen.

2. Before the start of the communication session the applicant calculates the initial status of the satellite

\[
U_1(n) = (a_1^{W_1(n)}a_1^{C_1(n)}a_1^{B_1(n)}) \mod m_1, \\
\vdots \\
U_k(n) = (a_k^{W_k(n)}a_k^{C_k(n)}a_k^{B_k(n)}) \mod m_k.
\] (4)

3. The applicant chooses the following numbers \(\Delta W(n), \Delta C(n), \Delta B(n) \leq \prod_{i=1}^{k} \phi(m_i) - 1\) and then calculates

\[
W'_i(n) = (W_i + \Delta W_i(n)) \mod \phi(m_i), \\
C'_i(n) = (C_i(n) + \Delta C_i(n)) \mod \phi(m_i), \\
B'_i(n) = (B_i(n) + \Delta B_i(n)) \mod \phi(m_i).
\] (5)

4. The applicant calculates the modified status of the spacecraft

\[
U'_1(n) = (a_1^{W'_1(n)}a_1^{C'_1(n)}a_1^{B'_1(n)}) \mod m_1, \\
\vdots \\
U'_k(n) = (a_k^{W'_k(n)}a_k^{C'_k(n)}a_k^{B'_k(n)}) \mod m_k.
\] (6)

2.3. Applicant authentication stage

1. The relying party chooses a random number \(H = (H_1(n), H_2(n), ..., H_k(n))\). This “question” is passed on to the applicant.

2. Having received the question, the applicant, calculates the answers

\[
Q'_1(n) = (W'_1(n) - H_1W_1(n)) \mod \phi(m_1), \\
\vdots \\
Q'_i(n) = (W'_i(n) - H_kW_k(n)) \mod \phi(m_k). \\
Q'_k(n) = (C'_k(n) - H_kC_k(n)) \mod \phi(m_k). \\
Q'_1(n) = (B'_1(n) - H_1B_1(n)) \mod \phi(m_1), \\
\vdots \\
Q'_i(n) = (B'_i(n) - H_kB_k(n)) \mod \phi(m_k).
\] (7, 8, 9)

The applicant sends the following signal \(U(n), U'(n), Q^1(n), Q^2(n), Q^3(n)\) to the relying party.

3. The relying party checks the correctness of the answers to the question

\[
R_1(n) = (U_1^{H_1(n)}a_1^{Q_1(n)}a_1^{Q'_1(n)}a_1^{Q_1(n)}) \mod m_1, \\
\vdots \\
R_k(n) = (U_k^{H_k(n)}a_k^{Q_k(n)}a_k^{Q'_k(n)}a_k^{Q_k(n)}) \mod m_k.
\] (10)

If \((R_1(n), R_2(n), ..., R_k(n)) = (U'_1(n), U'_2(n), ..., U'_k(n))\) is obtained after checking, then the relying party assigns the applicant the “friend” status. Let us carry out a comparative analysis of the considered authentication protocols implemented in the RNS code.
### 3. Results and Discussion

1. The applicant chooses the following RNS bases: \( m_1 = 19, m_2 = 29, m_3 = 39 \), since they have a generating element \( a_1 = a_2 = a_3 = 2 \). Considering the range of code \( M_3 = \prod_{i=1}^{3} m_i = 21489 \) [15], we choose the secret key \( W = 10102 = (13, 10, 1) \), session key \( C(1) = 365 = (2, 17, 32) \) and the number \( B(1) = 452 = (15, 17, 8) \).

2. Before starting the first data exchange session the applicant calculates the initial status of the spacecraft according to (4):

   \[
   U_1(I) = (a_1 W_1(a_1) C_1(a_1))_1 \mod m_1 = 2^{13} \cdot 2^2 \cdot 2^{15} \mod 19 = 2^{12} \mod 19 = 11,
   
   U_2(I) = (a_2 W_2(a_2) C_2(a_2))_2 \mod m_2 = 2^{10} \cdot 2^{17} \cdot 2^{17} \mod 29 = 2^{16} \mod 29 = 25,
   
   U_3(I) = (a_3 W_3(a_3) C_3(a_3))_3 \mod m_3 = 2^4 \cdot 2^{32} \cdot 2^8 \mod 37 = 2^5 \mod 37 = 32.
   
3. The applicant chooses the numbers \( \Delta W(n) = 221 = (5, 25, 5), \quad \Delta C(n) = 101 = (11, 17, 29), \quad \Delta B(n) = 58 = (4, 2, 22) \), and changes the parameters \( W, C(n), B(n) \) according to (5):

   \[
   W^*(n) = (\lceil |3 + 5|^* |10 + 25|^* |5 + 5|^* \rceil, \lceil |0 + 25|^* |1 + 5|^* \rceil) = (0, 7, 6),
   
   C^*(n) = (\lceil |4 + 1|^* |17 + 17|^* |32 + 29|^* \rceil) = (15, 6, 25),
   
   B^*(n) = (\lceil |5 + 4|^* |7 + 2|^* |8 + 22|^* \rceil) = (1, 19, 30).
   
4. The applicant calculates the changed status of the spacecraft according to (6):

   \[
   U_1^*(I) = (a_1 W_1^*(a_1) C_1(a_1))_1 \mod m_1 = 2^0 \cdot 2^{15} \cdot 2^2 \mod 19 = 2^{16} \mod 19 = 5,
   
   U_2^*(I) = (a_2 W_2^*(a_2) C_2(a_2))_2 \mod m_2 = 2^7 \cdot 2^{16} \cdot 2^{19} \mod 29 = 2^4 \mod 29 = 16,
   
   U_3^*(I) = (a_3 W_3^*(a_3) C_3(a_3))_3 \mod m_3 = 2^6 \cdot 2^{25} \cdot 2^{30} \mod 37 = 2^{25} \mod 37 = 20.
   
#### 3.1. Applicant authentication stage

1. The relying party chooses the “question” \( H = 367 = (6, 19, 34) \), which passes to the applicant.

2. Having received the question, the applicant calculates the answers according to (7)-(9):

   \[
   Q_1^1(I) = \left| W_1^*(I) - H_1 W_1(I) \right|_{\mp_{(m_1)}} = \lceil 0 - 9 \cdot 3 \rceil_{18} = 12,
   
   Q_2^1(I) = \left| W_2^*(I) - H_2 W_2(I) \right|_{\mp_{(m_2)}} = \lceil 7 - 9 \cdot 10 \rceil_{28} = 13,
   
   Q_3^1(I) = \left| W_3^*(I) - H_3 W_3(I) \right|_{\mp_{(m_3)}} = \lceil 6 - 14 \cdot 1 \rceil_{36} = 8.
   
   \]
   
   \[
   Q_1^2(I) = \left| C_1^*(I) - H_1 C_1(I) \right|_{\mp_{(m_1)}} = \lceil 5 - 6 \cdot 4 \rceil_{18} = 9,
   
   Q_2^2(I) = \left| C_2^*(I) - H_2 C_2(I) \right|_{\mp_{(m_2)}} = \lceil 6 - 19 \cdot 17 \rceil_{28} = 19,
   
   Q_3^2(I) = \left| C_3^*(I) - H_3 C_3(I) \right|_{\mp_{(m_3)}} = \lceil 25 - 34 \cdot 32 \rceil_{36} = 17.
   

\[
\begin{align*}
Q_1^1(l) &= B_1^1(l) - H_1 B_1^1(l)_{\text{mod}(m_j)} = 1 - 6 \cdot 15^+_{18} = 1, \\
Q_2^2(l) &= B_2^2(l) - H_2 B_2^2(l)_{\text{mod}(m_j)} = 19 - 19 \cdot 17^+_{28} = 4, \\
Q_3^3(l) &= B_3^3(l) - H_3 B_3^3(l)_{\text{mod}(m_j)} = 30 - 34 \cdot 8^+_{36} = 10.
\end{align*}
\]

The applicant sends \((U(n) || U^+(n) || Q^1(n) || Q^2(n) || Q^3(n))\) to the relying party.

3. The relying party checks the answers in accordance with (10)

\[
\begin{align*}
R_1(l) &= U_1^H(n) a_1^Q(n) a_1^Q(n) a_1^Q(n)_{\text{mod}(m_j)} = 1^6 \cdot 2^{12} \cdot 2^9 \cdot 2^4_{19} = 5, \\
R_2(l) &= U_2^H(n) a_2^Q(n) a_2^Q(n) a_2^Q(n)_{\text{mod}(m_j)} = 2^{519} \cdot 2^{12} \cdot 2^{19} \cdot 2^4_{29} = 16, \\
R_3(l) &= U_3^H(n) a_3^Q(n) a_3^Q(n) a_3^Q(n)_{\text{mod}(m_j)} = 3^2 \cdot 2^8 \cdot 2^17 \cdot 2^{10}_{37} = 20.
\end{align*}
\]

As a result of the check, we get \((R_1(l), R_2(l), R_3(l)) = (U_1^1(l), U_2^1(l), U_3^1(l)) = (5, 16, 20)\). In this case, the relying party assigns the applicant the “friend” status.

In order to conduct a comparative analysis of the developed authentication protocols implemented in RNS codes, a hardware design of the structural model of the authentication system has been created using the FPGA FPLD Xilinx Virtex-7. The bit depth of the RNS code base has been chosen to be 32. When implementing the hardware design of the system, the environment Vivado HLS 2019.2 has been used. The clock frequency of the FPLD was 250 MHz. Comparative analysis has shown that 3.7 ms was required for one round of the authentication stage using the Guillou-Quisquater protocol, 3.1 ms for the Shnor protocol, and 1.2 ms for the developed protocol. The greatest time expenditure for the Guillou-Quisquater protocol has been associated with the fact that at the authentication stage it is necessary to perform two exponentiation operations in it. In the authentication protocol Shnor, at this stage, one exponentiation operation is performed to modulo. However, in the developed protocol, there is no such operation. Based on the data obtained, it can be concluded that the use of the developed authentication protocol implemented in the RNS codes enables to increase the information secrecy of the LEO satellite communication systems by 2.58 times compared to the Shnor protocol and 3.08 times compared to the Guillou-Quisquater protocol.

4. Conclusion

To ensure the information secrecy of the LEO satellite communication systems and to prevent the possibility of imposing a intercepted and delayed control command, it is proposed to use the “friend or foe” identification system for satellites. To reduce the likelihood of selecting the correct response signal by the intruder satellite, that is, to further increase information secrecy, it is proposed to implement authentication protocols in RNS codes. The novelty of this idea lies in the fact that the use of parallel RNS codes will reduce the time spent on performing arithmetic operations implemented in authentication protocols. In order to carry out a comparative analysis of the developed authentication protocols implemented in RNS codes, a hardware design of the structural model of the authentication system with a base width of 32 bits was developed. The results obtained showed that the use of the developed authentication protocol implemented in RNS codes enables to increase the information secrecy of the LEO satellite communication systems by 2.58 times compared to the Shnor protocol and 3.08 times compared to the Guillou-Quisquater protocol.

References

[1] Polyakov V N, Chizhov A P, Kotenev Yu A and Mukhametshin V Sh 2019 Results of System Drilling Techniques and Completion of Oil and Gas Wells IOP Conference Series: Earth and Environmental Science (IPDME 2019 – International Workshop on Innovations and Prospects
of Development of Mining Machinery and Electrical Engineering) 378(1) 012119 1–7 DOI: 10.1088/1755-1315/378/1/012119

[2] Kalmykov I A, Pashintsev V P, Zhuk A P, Chistousov N K 2019 Development of an error correction algorithm to improve the fault tolerance of the identification-friend-or-foe International Journal of Engineering and Advanced Technology (IJEAT) 8(5) 2557-2562

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

[4] Katkov K A, Timoshenko L I, Dunin A V 2015 Application of modular technologies in the large-scale analysis of signals Journal of Theoretical and Applied Information Technology 80(3) 391-400

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

[6] Veligosha A V, Kaplun D I, Bogaevskiy D V 2018 Adjustment of adaptive digital filter coefficients in modular codes Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2018) 1167-1170

[7] Tyncherov K T, Chervyakov N I, Selivanova M. V 2018 Method of increasing the reliability of telemetric well information transmitted by the wireless communication channel Bulletin of the Tomsk Polytechnic University Geo Assets Engineering 329(3) 36-43

[8] Yurdanov D, Gostev D 2017 CEUR Workshop Proceedings 1837 206-212

[9] Francisco Martín-Fernández, Pino Caballero-Gil and Cándido Caballero-Gil 2016 Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Thing Sensors 16(1) doi:10.3390/s16010075

[10] Dua F, Kumar N, Das A, Susilo W 2018 IEEE Trans. Veh. Technol. 67(5) 4359–4373.

[11] Shao J, Lin X, Lu R, Zuo C 2016 IEEE Trans. Veh. Technol. 65(3) 1711–1720

[12] Kusnardi K, Gunawan D 2019 TELKOMNIKA 17(2) 826-834 DOI: 10.12928/TELKOMNIKA.v17i2.1175413

[13] Ambroze M, Stengel I, Tomlinson M 2019 2nd Scientific Conference of Computer Sciences (SCCS) DOI: 10.1109/SCCS.2019.8852614

[14] Kalmykov I, Lapina M, Provornov I, Voloshin E 2019 CEUR Workshop Proceedings 3rd International Workshop on Young Scientist's Trends in Information Processing YSIP3 2019 2500 1548072500

[15] 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