International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Development of Satellite Authentication System for Low Earth Orbit Satellite Communication System on the Basis of Polynomial Residue Number System

Igor Anatolyevich Kalmykov, Vladimir Petrovich Pashintsev, Aleksandr Pavlovich Zhuk, Nikita Konstantinovich Chistousov, Aleksandr Anatolyevich Olenev

Abstract: ***Low Earth orbit satellite (LEOS) communication system can be successfully applied in automated systems of remote monitoring and control of hydrocarbons production and transportation in the Extreme North. Herewith, continuous communications are possible if LEOS communication system is comprised of up to 60 satellites. With the increase in number of countries exploring deposits of Arctic shelf, the number of LEOS systems will also increase. This could lead to such situation when an alien satellite being in the radio coverage zone of receiver installed on terminal station of unattended object can impose previously tapped control command. As a consequence, the unattended facility of hydrocarbon production and transportation can fail. In order to prevent such situation, it is proposed to apply identification-friend-or-foe (IFF) systems for satellite. High information security in such systems is provided by zero-knowledge proof of knowledge (ZKPK) authentication protocol. Aiming at improvement of satellite identification rate, it is proposed to apply polynomial residue number system (PRNS), since arithmetic operations in such codes are executed independently and in parallel by bases. This work is aimed at reduction of time of satellite authentication by IFF system due to the use of PRNS codes.***

Index Terms: ***information security, modular codes, polynomial residue number system, satellite authentication system,zero-knowledge proof of knowledge authentication protocols.***

I. INTRODUCTION

LEOS communication systemsarewidely applied in such global projects as exploration of the Northern Sea Route, development of information telemetric systems of air and land transport in high latitudes [1], [2]. Special attention is paid to the exploration projects of Arctic ocean shelf. In this case **LEOS communication systems**are included into automated systems of remote monitoring and control of hydrocarbons production and transportation. Communication systems are comprised of from 48 to 60 satellites.

Since the number of countries and companies involved in exploration of Arctic increases, the number of **LEOS systems** will also grow. Hence, it could be possible that an alien satellite being in the radio coverage zone of receiver installed on terminal station of unattended object can impose previously tapped and delayed control command. As a consequence, the unattended facility of hydrocarbon production and transportation can fail.

Such situation can be eliminated by improvement of LEOS information security using **IFF system for satellite** [3]. Satellite authentication rate can be increased by using parallel calculations. Peculiar position among integral algebraic structures of Galois fields is occupied by **modular codes(MC)** of **PRNS**. Application of these codes allows to parallelize calculations at the level of arithmetic operations. Thus, development of **IFF system for satellite** is an urgent task.

II. LITERATURE REVIEW

A. Analysis of IFF system for satellite

As a rule, the **IFF system** is widely applied for authentication of both of civil and military aircrafts [4], [5]. In [6] in order to improve cryptographic security of IFF system, it is proposed to use 256-element pseudo-random sequences. In [7] it is proposed to apply encrypted 64-bit code for identification of object status which should be modified every 24 hours. The main drawback of the IFF system is the necessity to use secure channel for transfer of correct identifier to objects. The performed analysis of major principles of data arrangement of IFF system has demonstrated that they cannot perform satellite authentication and cannot be used in LEOS.

B. Analysis of authentication protocols

It is obvious that efficiency of information security of **LEOS communication systems**is defined by authentication protocol used in **IFF system for satellite.** It was revealed in [8], [9] that numerous authentication protocols could be subdivided into three groups.

Manuscript published on 30 June 2019.
* Correspondence Author (s)
Igor Anatolyevich Kalmykov, North-Caucasus Federal University Stavropol, Russian Federation.
Vladimir Petrovich Pashintsev, North-Caucasus Federal University Stavropol, Russian Federation.
Aleksandr Pavlovich Zhuk, North-Caucasus Federal University Stavropol, Russian Federation.
Nikita Konstantinovich Chistousov, North-Caucasus Federal University Stavropol, Russian Federation.
Aleksandr Anatolyevich Olenev, Stavropol State Pedagogical Institute. Stavropol, Russian Federation.
This work was supported by the Russian Foundation for Basic Research, project No. 18–07-01020.

The first group is comprised of password authentication protocols. However, these authentication protocols cannot be used for satellite identification since their cryptographic security is low. The second group is based on request/response authentication protocols. According to [10], these protocols widely apply encrypting algorithms. However, these protocols cannot be used in **IFF systems for satellite**, since it is required to store secret keys not only at satellites but also at unattended controlled facilities.

This drawback is absent in **zero knowledge proof** authentication protocols which form the third group [10], [11]. In these protocols, the verifier V generates random requests which should by responded by the pretender P. In the frames of this protocol, the pretender should assure the verifier V that the known statement is valid. If the pretender is the authorized user, that is, his statement is true, then upon increase in the number of verification stages, the probability of correct statement should tend to unity. Otherwise, when the pretender's statement is false, the probability of correct statement would be close to zero.

However, possessing high cryptographic security, these protocols are characterized by low authentication rate. In general, these protocols require for 20-40 authentication cycles, each comprised of three stages for pretender identification. Therefore, such protocols cannot be used for satellite authentication.

III. METHODS

A. Two stage zero knowledge proof authentication protocol

This drawback can be eliminated by the protocol described in [12]. In this protocol, two stages are sufficient for authentication of the pretender P. With this aim, the protocol uses the satellite secret key U, the session key S(j), and the parameter for verification of dual use of the session key T(j). It is shown in Table I.

Table 1. Satellite identification protocol

	Preliminary stage		
	P (pretender)	Trusted center	V (verifier)
1 2	U – secret key, U = {1, 2,…, q - 1}; S, T – random numbers; (S, T) = {1, 2, …, q - 2}.	q – prime number g – primitive element of group q	
	Operational stage		
	P (pretender)		V (verifier)
1	Calculation of session key S(j) = F(S); S(j) = {1, 2,…, q - 2}; Calculation of verification parameter T(j) = F(T); T(j) = {1, 2,…, q - 2}; F – pseudo-random function.		
2	True status is calculated $C(j) = g^{U} g^{S(j)} g^{T(j)} \bmod q$		
3	Noise masking of parameters $U(j) = (U + \Delta U(j)) \bmod \varphi(q),$ $S^{*}(j) = (S + \Delta S(j)) \bmod \varphi(q),$ $T^{*}(j) = (T + \Delta T(j)) \bmod \varphi(q)$ where {ΔU, ΔS, ΔT } = {1, 2,…, q - 2}.		
4	Noised status is calculated $C^{*}(j) = g^{U} g^{S^{*}(j)} g^{T^{*}(j)} \bmod q.$		
	Satellite authentication		
1			Request is selected d(j) = {1, 2,…, q - 2}.
2	Response to request «d(j)» $r_1(j) = (U(j) - d(j)U) \bmod \varphi(q),$ $r_2(j) = (S^{*}(j) - d(j)S(j)) \bmod \varphi(q),$ $r_3(j) = (T^{*}(j) - d(j)T(j)) \bmod \varphi(q)$		
			Acquiring parameters (C(j), C*(j), r_1(j), r_2(j), r_3(j))

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Verification of response to request d(j)			
1			Verification of responses to request $Y(j) = C(j)^{d(j)} g^{r_1(j)} g^{r_2(j)} g^{r_3(j)} \bmod q$
			Y(j) = C*(j) – friend Y(j) ≠ C*(j) – foe

The main drawback of this protocol is the use of one module q. According to [13], high spoofing resistance of authentication protocol requires that $\log_2 q \geq 128$ digits. Therefore, in order to perform multiplicative operations with respect to base q, high time consumption is required. This drawback can be eliminated by development of satellite authentication based on PRNS modular codes.

B. Modular codes. Satellite authentication protocol implemented in PRNS modular codes

Two types of modular codes are possible. The first type is comprised of codes of **residue number system** where an integer number U is presented in the form of residues $U = (u_1, u_2, ..., u_k)$, where $u_i \equiv U \bmod m_i$, m_i are the modular codes coprime basis, $i = 1, 2, ..., k$ [3] and [14]. Then, the arithmetic operations in modular codes can be presented as follows:

$$U + Z = ((u_1 + z_1) \bmod m_1, ..., (u_k + z_k) \bmod m_k), \quad (1)$$

$$U - Z = ((u_1 - z_1) \bmod m_1, ..., (u_k - z_k) \bmod m_k), \quad (2)$$

$$U \cdot Z = ((u_1 \cdot z_1) \bmod m_1, ..., (u_k \cdot z_k) \bmod m_k), \quad (3)$$

where $Z \equiv z_i \bmod m_i$; $i = 1, 2, ..., k$.

The modular codes increase the rate of arithmetic operations since the calculations are performed in parallel. Due to these properties the modular codes are applied in digital systems of signal processing [15],[16]. The researchers [17], [18] analyzed the principles of development of digital filters based on modular codes. The researchers [19], [20] demonstrated error corrections using modular codes. Application of modular code in ATM cash withdrawal protocol has been demonstrated in [21]. Application of modular codes for reliability improvement of borehole information has been demonstrated in [22].

The second group is comprised of modular codes of **PRNS.** In these codes irreducible polynomials $p_i(x)$, i = 1, …, k are used as bases. Then, the integer number U should be initially presented in the form of polynomial H(x) and then in the form of residues $Y(x) = (y_1(x), y_2(x), ..., y_k(x))$, where $y_i(x) \equiv Y(x) \bmod p_i(x)$ [23]. Then, for PRNS code the following equations are valid:

$$Y(x) \oplus Z(x) = (|y_1(x) \oplus z_1(x)|_{p_1(x)}, ..., |y_k(x) \oplus z_k(x)|_{p_k(x)}), \quad (4)$$

$$Y(x) \cdot Z(x) = (|y_1(x) \cdot z_1(x)|_{p_1(x)}, ..., |y_k(x) \cdot z_k(x)|_{p_k(x)}), \quad (5)$$

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

The product of PRNS code bases determines the operational range:

$$P(x) = \prod_{i=1}^{k} p_i(x). \quad (6)$$

Conversion from PRNS to position code is performed using the Chinese remainder theorem, according to which:

$$Y(x) = \left(\sum_{i=1}^{k} y_i(x) m_i(x) M_i(x) \right) \bmod P(x), \quad (7)$$

where $M_i(x) = P(x)/p_i(x)$; $m_i(x) M_i(x) \equiv 1 \bmod p_i(x)$; $m_i(x)$ is the weight of orthogonal basis.

Let us apply single module protocol of satellite identification described in [12]. The protocol involves participation of the responder at the satellite and the requester at the controlled object. Let us implement the protocol in PRNS modular code. Let us select parameters satisfying the condition:

$$\log_2 \{U, S(j), T(j)\} < \deg P(x). \quad (8)$$

Let us concatenate the secret key $U = (u_1 \| u_2 \| ... \| u_k)$, the j-th session key $S^j = (S_1^j \| S_2^j \| ... \| S_k^j)$ and the parameter for verification of dual use of the session key $T^j = (T_1^j \| T_2^j \| ... \| T_k^j)$, where $u_i = \deg p_i(x)$, $S_i^j = \deg p_i(x)$; $T_i^j = \deg p_i(x)$; $i = 1, 2, ..., k$; $\deg p_i(x)$ is the polynomial degree.

Preliminary stage at the j-th communication session:

1. The responder calculates the true satellite status in PRNS:

$$C^j(x) = (C_1^j(x), C_2^j(x), ..., C_k^j(x)), \quad (9)$$

where $C_i^j(x) = \left| g(x)^{u_i} g(x)^{S_i^j} g(x)^{T_i^j} \right|_{p_i(x)}^{+}$; g(x) = x; $i = 1, 2, ..., k$.

2. The responder modifies secret parameters:

$$\tilde{u}_i = (u_i + \Delta u_i) \bmod G_i, \quad (10)$$

$$\tilde{S}_i^j = (S_i^j + \Delta S_i^j) \bmod G_i, \quad (11)$$

$$\tilde{T}_i^j = (T_i^j + \Delta T_i^j) \bmod G_i, \quad (12)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

where $\{\Delta u_i, \Delta S_i^j, \Delta T_i^j\} < G_i$ are random numbers; $G_i = 2^{\deg p_i(x)} - 1; i = 1, 2, ..., k$.

3. The responder determines the satellite noisy status using PRNS:

$$\tilde{C}^j(x) = (\tilde{C}_1^j(x), \tilde{C}_2^j(x), ..., \tilde{C}_k^j(x)), \quad (13)$$

where $\tilde{C}_i(x) = \left| g(x)^{\tilde{u}_i} g(x)^{\tilde{S}_i^j} g(x)^{\tilde{T}_i^j} \right|_{p_i(x)}^{+}$.

Satellite authentication:

1. The requester transfers to the satellite random number $d^j = (d_1^j, d_2^j, ... d_k^j)$, where $d_i^j \equiv d^j \bmod G_i$; $G_i = 2^{\deg p_i(x)} - 1$; $i = 1, 2, ..., k$.

2. The responder receiving $d^j = (d_1^j, d_2^j, ... d_k^j)$ calculates responses as follows:

$$r_i^1 = (\tilde{u}_i - d_i^j \cdot u_i) \bmod G_i, \quad (14)$$

$$r_i^2 = (\tilde{S}_i^j - d_i^j \cdot S_i^j) \bmod G_i, \quad (15)$$

$$r_i^3 = (\tilde{T}_i^j - d_i^j \cdot T_i^j) \bmod G_i, \quad (16)$$

where $G_i = 2^{\deg p_i(x)} - 1$; $i = 1, 2, ..., k$.

The satellite transfers to the requester the following data:

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

Verification of responses:

1. The requester verifies the responses to the request $d^j = (d_1^j, d_2^j, ... d_k^j)$.

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

The "friend" status is assigned to the satellite if the following is valid:

$$\{Y_1^j(x) = \tilde{C}_1^j(x), Y_2^j(x) = \tilde{C}_2^j(x), ..., Y_k^j(x) = \tilde{C}_k^j(x)\}. \quad (18)$$

Analysis of the developed authentication protocol has demonstrated that it can be used for satellite identification at higher rate since the authentication is comprised of two stages. In order to estimate efficiency of the developed authentication protocol, it was compared with the Fiat–Shamir protocol and the Schnorr protocol. The analysis has demonstrated that the developed protocol performs authentication in two stages, that is, by 30 times faster than the Fiat–Shamir protocol and by 1.5 faster than the Schnorr protocol.

IV. RESULTS AND DISCUSSION

Let us exemplify the development of the **IFF system for satellite.** The given bases of modular code are $p_1(x) = x^5 + x^2 + 1$, $p_2(x) = x^5 + x^3 + 1$; $p_3(x) = x^5 + x^3 + x^2 + x + 1$. The operating range of the code is $P = \prod_{i=1}^{3} p_i(x) = x^{15} + x^4 + x^3 + x^2 + x + 1$. Then, the size of the secret key U, the parameters S and T should not exceed 15 digits. Let U = 19521, S = 5900, and T = 737. Let us present them in binary code and concatenate them. We obtain:

$$U = (u_1 \| u_2 \| u_3) = (10011_2 \| 00010_2 \| 00001_2) = (18_{10} \| 2_{10} \| 1_{10}),$$

$$S^j = (S_1^j \| S_2^j \| S_3^j) = (00101_2 \| 11000_2 \| 01100_2) = (5_{10} \| 24_{10} \| 12_{10}),$$

$$T^j = (T_1^j \| T_2^j \| T_3^j) = (00000_2 \| 10111_2 \| 00001_1) = (0_{10} \| 23_{10} \| 1_{10}).$$

Preliminary stage at the j-th communication session:

1. The responder calculates the true satellite status in PRNS according to Eq. (9):

$$C_1^j(x) = \left| g(x)^{u_1} g(x)^{S_1^j} g(x)^{T_1^j} \right|_{p_1(x)}^{+} = \left| x^{18} \cdot x^5 \cdot x^0 \right|_{x^5+x^2+1}^{+} = x^3 + x^2 + x + 1,$$

$$C_2^j(x) = \left| g(x)^{u_2} g(x)^{S_2^j} g(x)^{T_2^j} \right|_{p_2(x)}^{+} = \left| x^2 \cdot x^{24} \cdot x^{23} \right|_{x^5+x^3+1}^{+} = x^4 + x^3 + 1,$$

$$C_3^j(x) = \left| g(x)^{u_3} g(x)^{S_3^j} g(x)^{T_3^j} \right|_{p_1(x)}^{+} = \left| x^1 \cdot x^{12} \cdot x^1 \right|_{x^5+x^2+1}^{+} = x^3 + x^2.$$

2. The responder modifies the secret parameters according to Eqs. (10)-(13)

$$\tilde{u}_1 = \left| u_1 + \Delta u_1 \right|_{31}^{+} = \left| 18 + 19 \right|_{31}^{+} = 6,$$

$$\tilde{u}_2 = \left| 2 + 22 \right|_{31}^{+} = 24, \ \tilde{u}_3 = \left| 1 + 25 \right|_{31}^{+} = 26.$$

$$\tilde{S}_1^j = \left| S_1^j + \Delta S_1^j \right|_{31}^{+} = \left| 5 + 29 \right|_{31}^{+} = 3, \ \tilde{S}_2^j = \left| 24 + 8 \right|_{31}^{+} = 5,$$

$$\tilde{S}_3^j = \left| 12 + 7 \right|_{31}^{+} = 19.$$

$$\tilde{T}_1^j = \left| T_i^j + \Delta T_i^j \right|_{31}^{+} = \left| 0 + 26 \right|_{31}^{+} = 26,$$

$$\tilde{T}_2^j = \left| 23 + 9 \right|_{31}^{+} = 1, \ \tilde{T}_3^j = \left| 1 + 4 \right|_{31}^{+} = 5.$$

3. The responder determines the satellite noisy status using Eq. (13):

$$\tilde{C}_1^j(x) = \left| g(x)^{\tilde{u}_1} g(x)^{\tilde{S}_1^j} g(x)^{\tilde{T}_1^j} \right|_{p_1(x)}^{+} = \left| x^6 \cdot x^3 \cdot x^{26} \right|_{x^5+x^2+1}^{+} = x^4,$$

$$\tilde{C}_2^j(x) = \left| g(x)^{\tilde{u}_2} g(x)^{\tilde{S}_2^j} g(x)^{\tilde{T}_2^j} \right|_{p_2(x)}^{+} = \left| x^{24} \cdot x^5 \cdot x^1 \right|_{x^5+x^3+1}^{+} = x^4 + x^2,$$

$$\tilde{C}_3^j(x) = \left| g(x)^{\tilde{u}_3} g(x)^{\tilde{S}_3^j} g(x)^{\tilde{T}_3^j} \right|_{p_1(x)}^{+} = \left| x^{26} \cdot x^{19} \cdot x^5 \right|_{x^5+x^2+1}^{+} = x^4 + x^3 + x.$$

Satellite authentication:

1. The requester transfers to the satellite a random number $d^j = (4, 4, 4)$.

2. The responder, receiving $d^j = (4, 4, 4)$, calculates responses according to Eqs. (14)-(16):

$$r_1^1 = \left| \tilde{u}_1 - d_1^j u_1 \right|_{31}^{+} = \left| 6 - 72 \right|_{31}^{+} = 27,$$

$$r_1^2 = \left| \tilde{S}_1^j - d_1^j S_1^j \right|_{31}^{+} = \left| 3 - 20 \right|_{31}^{+} 14,$$

$$r_1^3 = \left| \tilde{T}_1^j - d_1^j T_1^j \right|_{31}^{+} = 26.$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

$$r_2^1 = \left|\tilde{u}_2 - d_2^j u_2\right|_{31}^{+} = \left|24-8\right|_{31}^{+} = 16 \quad ,$$

$$r_2^2 = \left|\tilde{S}_2^j - d_2^j S_2^j\right|_{31}^{+} = \left|5-96\right|_{31}^{+} = 2 \quad ,$$

$$r_2^3 = \left|\tilde{T}_2^j - d_2^j T_2^j\right|_{31}^{+} = 2.$$

$$r_3^1 = \left|\tilde{u}_3 - d_3^j u_3\right|_{31}^{+} = \left|26-4\right|_{31}^{+} = 22 \quad ,$$

$$r_3^2 = \left|\tilde{S}_3^j - d_3^j S_3^j\right|_{31}^{+} = \left|19-48\right|_{31}^{+} = 2 \quad ,$$

$$r_3^3 = \left|\tilde{T}_3^j - d_3^j T_3^j\right|_{31}^{+} = 1.$$

The satellite transfers to the requester the following data in binary code:

- true status

$$C^j(x) = (C_1^j(x), C_2^j(x), C_3^j(x)) = \{x^3+x^2+x+1, x^4+x^3+1, x^3+x^2\},$$

- noisy status

$$\tilde{C}^j(x) = (\tilde{C}_1^j(x), \tilde{C}_2^j(x), \tilde{C}_3^j(x)) = \{x^4, x^4+x^2, x^4+x^3+x\},$$

- responses $r^1 = (r_1^1, r_2^1, r_3^1) = (27, 16, 22)$,

$$(r_1^2, r_2^2, r_3^2) = (4, 2, 2),\ (r_1^3, r_2^3, r_3^3) = (26, 2, 1).$$

Verification of responses:

1. The requester verifies the responses to the request according to Eq. (17)

$$Y_1^j(x) = \left|(x^3+x^2+x+1)^4 \cdot x^{27} \cdot x^{14} \cdot x^{26}\right|_{x^5+x^2+1}^{+} = x^4,$$

$$Y_2^j(x) = \left|(x^4+x^3+1)^4 \cdot x^{16} \cdot x^2 \cdot x^2\right|_{x^5+x^3+1}^{+} = x^4+x^2,$$

$$Y_3^j(x) = \left|(x^3+x^2)^4 \cdot x^{22} \cdot x^2 \cdot x^1\right|_{x^5+x^2+1}^{+} = x^4+x^3+x.$$

The verification result coincides with the satellite noisy status:

$$\left\{Y_1^j(x) = \tilde{C}_1^j(x),\ Y_2^j(x) = \tilde{C}_2^j(x),\ Y_3^j(x) = \tilde{C}_3^j(x)\right\}.$$

Hence, the "friend" status is assigned to the satellite. Now it can start data exchange with unattended facility. If Eq. (18) is not valid, then the "foe" status is assigned to the satellite, and communication session is rejected.

Let us compare efficiency of the developed method with the previously considered one. It is known that raising of m to the power n requires $N = 2\left|\log_2 n\right|$ multiplications. It has been demonstrated in [24] that for multiplication of two 128 digit number, T_{MUL} = 7 **CPU cycles** are required. In this case the length of raising to the power with respect to base will be:

$$T_1(n) = NT_{MUL}T_{CPU} = 2\left|\log_2 n\right|T_{MUL}T_{CPU} = 14\left|\log_2 n\right|T_{CPU}. \quad (19)$$

Let the bit depth with respect to base q is 120 bit. Then according to Eq. (19), the length of raising to the power with respect to base will be $T_1(n=100) = 14\left|\log_2 q\right| = 98$ **CPU cycles**. If the authentication processor speed is F = 333 MHz, then the tact duration is $T_{CPU} = 3 \cdot 10^{-9}$ s. Then the length of raising to the power with respect to base will be $T_1(n=100) = 274$ ns .

While using PRNS codes, the adders and multipliers with respect to base can be substituted with LUT tables. In this case the execution time of operation will equal to the time of data read out from LUT table. For this example, it is required to select ten modules $p_i(x)$, for which $\deg p_i(x) = 12$. Then, it is possible to select **ROM** Series 1645 (128K×16), its data access time is $T_2(n=10) = 100$ ns . Therefore, application of the developed **IFF system for satellite** increases the satellite authentication rate by 2.74 times.

V. CONCLUSION

With the increase in the number of countries exploring Arctic deposits, the number of ***LEOS communication systems*** between central station and unattended facilities of hydrocarbon production and transportation will also increase.This could lead to such situation when an alien satellite could impose previously tapped control command. As a consequence, the unattended facility of hydrocarbon production and transportation can fail. In order to prevent such situation, it is proposed to apply **IFF system**.

The performed analysis of development of **IFF systems** has demonstrated that they cannot be used for satellite authentication in ***LEOS* communication systems.** Aiming at development of **IFF system for satellite,** the main authentication protocols were also analyzed. On the basis of the obtained results, the use of **zero knowledge proof** authentication protocols was substantiated.

This article presented the development of **IFF system for *LEOS* systems**based on modular codes of **PRNS**. Application of this method has made it possible to develop **zero knowledge proof** spoof resistant authentication protocol which is able to determine satellite status at lower time consumptions.

Comparative analysis has demonstrated that the developed **IFF system for satellite** increased satellite authentication rate by 2.74 times using ten 12-digit PRNS modules in comparison with single module protocol.

REFERENCES

1. "Iridium Satellite Communication". Available: https://www.iridium.com/services/iridium-certus/
2. "What Is Iridium NEXT?". Available: http://www.argo.ucsd.edu/sat_comm_AST13.pdf
3. R.N.Rezenkov, V.P.Pashintsev, P.A.Zhuk, and M.I.Kalmykov, "Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication".International Journal of Mechanical Engineering and Technology (IJMET),vol. 9(5), 2018, pp. 958–965
4. "MK-XII/A IFF Interrogators. Defense and security in five continents". Available: https://www.indracompany.com/sites/default/files/MK-XIIA%20IFF%20INTERROGATORS.pdf
5. "THE MARK XII IFF SYSTEM".Available: https://www.telinstrument.com/avionics-news/industry-articles/20-the-mark-xii-iff-system.html
6. Patent US 8325081 B2."Identification friend or foe (IFF) system". 2003.
7. Patent US 5745575 A. "Identification friend or foe (IFF) system using variable codes". 1996.
8. N.Ferguson, B.Schneier, and T. Kohno, "Cryptography Engineering". New York: John Wiley & Sons, 2010.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

9. R.Smith, "Authentication: From Passwords to Public Keys". New York: Addison-Wesley Publishing Company, Inc., 2002.
10. N.Ferguson, and B.Schneier, "Practical Cryptography". New York: John Wiley & Sons, 2003.
11. Sh. Goldwasser, and Y.Kalai, "On the (In) security of the Fiat-Shamir Paradigm". Proceedings of the 44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA,pp. 102-114
12. V.P.Pashentsev, and A.VLyakhov, "Primeneniepomekhoustoichivogoprotokolaautentifikatsiikosmicheskogoapparatadlyanizkoorbital'noisistemysputnikovoisvyazi" ["Noise immune authentication protocol of spacecraft for low Earth orbit satellite communication systems"].Infokommunikatsionnyetekhnologii, vol. 2,2015, pp. 183-190.
13. ISO/IEC 9798-5:2009 Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques.
14. A.Omondi, and B.Premkumar,"Residue Number Systems: Theory and Implementation". UK:Imperial College Press, 2007.
15. A. V.Veligosha, D. I.Kaplun,D. M. Klionskiy, and V. V.Gulvanskiy, "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. 7519731,2016, pp.213-214.
16. K. A.Katkov, L. I.Timoshenko, A. V.Dunin, andT. A.Gish, "Application of Modular Technologies in the Large-Scale Analysis of Signals". Journal of Theoretical and Applied Information Technology, vol. 80(3),2015, pp. 391-400
17. N. I.Chervyakov, A. V.Veligosha, and P. E.Ivanov, "Digital filters in a system of residual classes".IzvestiyaVysshikhUchebnykhZavedenij. Radioelektronika, vol. 38(8), 1995, pp. 11-20.
18. A.V.Veligosha, D.I.Kaplun, and 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, ElConRus 2018, 2018, pp. 1167-1170.
19. D. I.Kaplun, D. M.Klionskiy, and D. V.Bogaevskiy, "Error correcting of digital signal processing devices using non-positional modular codes".Automatic Control and Computer Sciences, vol. 51(3),2017, pp.167-173.
20. E. P.Stepanova, and 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.
21. D. A.Yurdanov, and D. B.Gostev, "The implementation of information and communication technologies with the use of modular codes. CEUR Workshop Proceedings 1837, 2017.
22. K.T.Tyncherov, N.I.Chervyakov, M.V.Selivanova, and I.A.Kalmykov, "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(3), 2018, pp. 36-43
23. E. P.Stepanova, E. V.Toporkova, R. A.Katkov, D. N.Rezenkov, "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(2) 2016, pp. 114-123.
24. "Lists of instruction latencies, throughputs and micro-operation breakdowns for Intel, AMD and VIA CPUs". 2018. Available: https://www.agner.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)