Algorithms of the Intelligent System for Ensuring Cybersecurity of on-board Equipment Supersonic Passenger Aircraft

Irina Mishchenko[1,*], *Vladislav* Kosyanchuk[1,†], *Evgeny* Zybin[1,‡] , *Maxim* Lelikov[1,§] and *Georgy* Platoshin [1,**]

[1]State Research Institute of Aviation Systems, Moscow, Russia

Abstract. This paper discusses the principles of forming a cyber-safe complex of on-board equipment for a supersonic passenger aircraft (SPA). The article discusses two-level protection of the on-board network against unauthorized access. The possibility of using algorithms based on blockchain and block encryption for the future protection of SPA from external and internal threats is being investigated.

1 Introduction

The aviation industry is undergoing a stage of digital transformation and automation of processes in the field of maintenance and creation of aircraft avionics complexes in order to increase economic efficiency. The introduction of advanced technologies into the on-board systems of an aircraft and into the infrastructure of airports leads to the transformation of the information space and an increase in the risk of potential vulnerabilities. Existing practices currently do not have operational ways to restrict unauthorized access by third parties to critical aircraft systems, which increases the likelihood of accidental or intentional impact on the information security of the aircraft in order to carry out aviation incidents leading to economic and social destabilization. In the conditions of intensive digitalization and global information interaction, an integrated approach is required to consider the issues of safe operation of a supersonic passenger aircraft on the ground and in the air.

The process of forming a cybersecurity complex of on-board equipment and supersonic passenger aircraft (SPA) systems begins with the elaboration of an approach to assessing the functional requirements and recommendations for information security systems and identifying cyber risks based on them. The identified factors that weaken the information security of the on-board information and computing network (OICN) allow a more targeted approach to the application of technical measures to detect threats and focus special attention on methods of protecting aircraft from cyber-attacks.

* Corresponding author: mishchenko_ib@gosniias.ru
† Corresponding author: vvk@gosniias.ru
‡ Corresponding author: zybin@gosniias.ru
§ Corresponding author: malelikov@2100.gosniias.ru
** Corresponding author: pga@gosniias.ru

To date, OICN should have several measures of technical and procedural protection of aircraft, which can be conditionally divided into two types according to the level of access:
- Protection from external threats. External threats include everything that is not inside the aircraft.
- Protection from internal threats. In this case, an attempt to obtain unauthorized access is carried out directly from the aircraft.

A promising technological solution in the field of information protection of the SPA from potential cyber incidents is the use of cryptographic algorithms considered in this paper. When studying methods of combating external threats, the sun is regarded as a material point-a subscriber exchanging with other subscribers of the global digital network of the single sky. It is proposed to implement guaranteed protection with data decentralization by using blockchain-based algorithms. Similarly, to protect against internal threats, it is proposed to use block encryption, which allows converting information data into a sequence of blocks with encrypted data.

2 The algorithm of the intelligent cybersecurity system based on blockchain

Blockchain technology is a mechanism of information exchange of a distributed system, built according to certain rules of a continuous sequential chain of cryptographically linked blocks (a linked list). A block is a data structure that includes any amount of information over which a hash function is transformed to obtain a unique set of fixed-size characters, called a hash sum. Each block contains its own hash sum and the hash sum of the previous block, which establishes a connection between the blocks. Compromising the data of one block will change its hash sum and reflect this action in subsequent blocks, while the previous blocks are not affected. Copies of block chains are stored on many different computing devices on the network. Thus, full transparency of information exchange between all participants and rapid detection of data manipulation is ensured [1]. One of the most well-known and frequently used hashing algorithms currently is SHA-256, which creates 256-bit strings (i.e., 256 consecutive 1s and 0s).

In addition to the hash function, blockchain technology uses another of the main forms of cryptography - asymmetric encryption (public key cryptography) [2]. In this method, each user uses a public and private key. The public key is visible to everyone, while the private key is known only to its owner. The keys are interconnected – information encrypted with a public key can only be disclosed by the private key associated with it.

The most common algorithms for asymmetric encryption are RSA (an abbreviation of the names of the creators of the algorithm: Rivest, Shamir and Adleman), DSA (Digital Signature Algorithm) and ECC (Elliptic Curve Cryptography). ECC-based algorithms combine reliable protection and high performance, based on discrete logarithm in a group of elliptic curve points and the use of short keys (for example, 224-bit ECC keys provide the same protection as a 2048-bit RSA key).

ECC is used both for creating digital signatures using ECDSA (Elliptic Curve Digital Signature Algorithm) (Fig. 1) and for key exchange via ECDH (Elliptic Curve Diffie-Hellman).

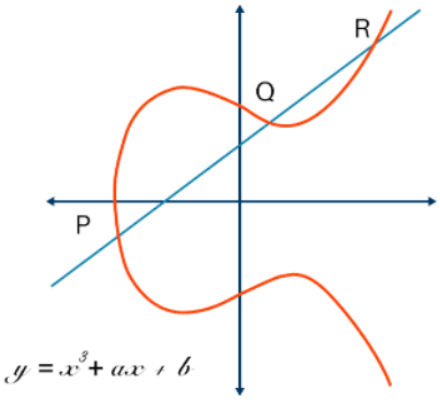

Fig. 1. Elliptic Curve Diffie-Hellman.

The ECDSA algorithm, similar in structure to DSA, but defined unlike it not over a field of integers, but over a finite field of elliptic curve points. One of the forms of elliptic curves are the Weierstrass curves (1), which look like a symmetrical curve parallel to the x axis when plotting:

$$y^2 = x^3 + ax + b \qquad (1)$$

In the context of this algorithm, a finite simple field can be represented as a predefined set of positive numbers in which the result of each calculation should be rendered (2).

$$y^2 = x^3 + ax + b \ (mod\ p) \qquad (2)$$

Among the fixed parameters of the elliptic curve for cryptographic algorithms, the equation of the curve, the value of the field modulus, the base point on the curve and the order of the base point are distinguished. This parameter is selected specifically and is a very large prime number [3].

The ECDSA algorithm is based on a one-way property that allows calculations to be performed in one direction, and does not allow obtaining results in reverse calculation without knowing some initial value. Thus, the line of the elliptic curve passes through three points (P, Q and R) and knowing only two of the points (P and Q), you can easily get a third point (R), but at the same time, having only one point (R), the other two (P and Q) cannot be calculated. This property is aimed at eliminating the possibility of falsifying the authenticity of the signature, which also provides a significantly high stability of the algorithm [4].

The scope of blockchain technology in the cybersecurity of aviation systems is limitless due to its unique properties such as reliability, accessibility, high adaptability, economic efficiency and profitability.

3 Algorithm of operation of an intelligent cybersecurity system based on block encryption

The "Grasshopper" algorithm is supposed to be used as a block algorithm — a symmetric block encryption algorithm with a block size of 128 bits and a key length of 256 bits, using an SP network to generate round keys [5].

The algorithm is based on the so-called SP network - substitution-permutation network (Substitution-Permutation network) (Fig. 2). The cipher based on the SP network receives a block and a key as input and performs several alternating rounds consisting of substitution stages and permutation stages.

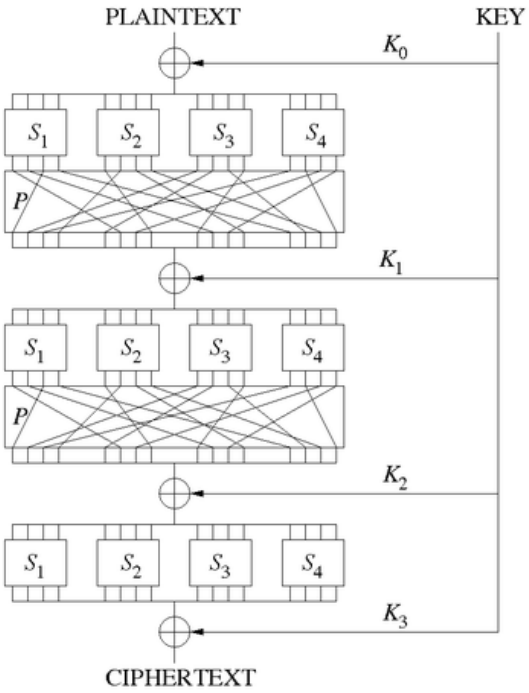

Fig. 2. Substitution-Permutation network.

In the "Grasshopper" nine full rounds are performed, each of which includes three consecutive operations:

The operation of superimposing the round key or bitwise XOR of the key and the input data block.

Non-linear transformation, which is a simple replacement of one byte with another according to the table. The nonlinear transformation is given by substitution (3):

$$S = \mathrm{Bin8}\, S' \,\mathrm{Bin8} - 1, \qquad (3)$$

where S' = (S'(0), S'(1), …, S'(255)).

Linear transformation. Each byte from the block is multiplied in the Galois field by one of the coefficients of the series, depending on the byte sequence number.

The last tenth round is not complete; it includes only the first XOR operation. All data blocks are encrypted with a single key, so there is no need to transmit it with each message and perform additional calculations that affect the speed of data processing. The form of implementation of the algorithm is possible both software and hardware. The "Grasshopper" algorithm is a stream cipher that is resistant to all currently known types of attacks on block ciphers.

4 Conclusion

In the aviation industry, increased attention is paid to cybersecurity by the airborne complex of the Air Force, since unauthorized interference and changes in flight parameters can lead to negative consequences at the same time. As a promising protection of the SPA from external and internal threats, the possibility of using algorithms based on blockchain and block encryption is being investigated. These measures help to increase the probability of detecting and preventing a cyber incident, increase the degree of data protection and limit access to information computing systems.

This work is partially supported by Ministry of Science and Higher Education of the Russian Federation under the agreement № 075-15-2022-1024.

References

1. Blockchain [Electronic resource]: Material from Wikipedia free Encyclopedia: May 9, 2023 / Wikipedia authors, Wikipedia, free Encyclopedia. Electron. dan. San Francisco: Wikimedia Foundation, 2023. Access mode: https://ru.wikipedia.org/?curid=5677831&oldid=130331890
2. S.P. Panasenko, *Encryption algorithms,* A special reference book (St. Petersburg: BHVPeterburg, 2009)
3. Recommendations on standardization: information technology. Cryptographic protection of information: parameters of elliptic curves for cryptographic algorithms and protocols (Moscow, Standartinform, 2016)
4. Mathematical foundations of Bitcoin Blockchain on May 9, 2023, Blog Collection Habr.com, Bitfury Group Russia, 2023. Access mode: https://habr.com/ru/companies/bitfury/articles/340378/
5. Grasshopper (cipher), Wikipedia. [2023]. Update date: 09.03.2023. URL: https://ru.wikipedia.org/?curid=5333163&oldid=129121257 (accessed: 09.03.2023)