МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ / MATHEMATICAL SOFTWARE FOR COMPUTERS, COMPLEXES AND COMPUTER NETWORKS

DOI: https://doi.org/10.60797/IRJ.2024.150.121

DEVELOPMENT OF CONTROL SCHEMES FOR BASIC CRYPTOGRAPHIC TRANSFORMATION OPERATIONS PERFORMED BY A PROGRAMMABLE LOGIC INTEGRATED CIRCUIT

Research article

Lukin M.V.[1, *]

[1] ORCID : 0009-0009-4472-6042;

[1] Central Research Institute of the Air Force (Ministry of Defense of the Russian Federation), Moscow, Russian Federation

* Corresponding author (maxim[at]vishnin.ru)

Abstract

This article discusses the procedure for developing control schemes for the basic operations of cryptographic transformation of information performed by a programmable logic integrated circuit that is part of the control system of an autonomous technical means. The purpose of the research is to analyze the basic logical operations used by various algorithms for cryptographic transformation of information, as well as to develop a mathematical apparatus for monitoring the correctness of these operations. The control of the execution of logical operations is carried out inside a programmable logic integrated circuit in parallel with the main algorithm of cryptographic transformation of information. In the future, the developed control schemes can be used in the development of an algorithm for technical diagnostics of programmable logic integrated circuits with localization of the location and cause of the malfunction.

Keywords: technical control, programmable logic integrated circuit, modular arithmetic, cryptographic transformation of information, technical diagnostics, autonomous technical tool.

РАЗРАБОТКА СХЕМ УПРАВЛЕНИЯ БАЗОВЫМИ ОПЕРАЦИЯМИ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ, ВЫПОЛНЯЕМЫМИ ПРОГРАММИРУЕМОЙ ЛОГИЧЕСКОЙ ИНТЕГРАЛЬНОЙ СХЕМОЙ

Научная статья

Лукин М.В.[1, *]

[1] ORCID : 0009-0009-4472-6042;

[1] Центральный научно-исследовательский институт Военно-воздушных сил (Министерства обороны Российской Федерации), Москва, Российская Федерация

* Корреспондирующий автор (maxim[at]vishnin.ru)

Аннотация

В данной статье рассматривается процедура разработки схем управления основными операциями криптографического преобразования информации, выполняемыми программируемой логической интегральной схемой, входящей в состав системы управления автономным техническим объектом. Целью исследования является анализ основных логических операций, используемых различными алгоритмами для криптографического преобразования информации, а также разработка математического аппарата для контроля корректности выполнения этих операций. Управление выполнением логических операций осуществляется внутри программируемой логической интегральной схемы параллельно с основным алгоритмом криптографического преобразования информации. В дальнейшем разработанные схемы управления могут быть использованы при разработке алгоритма технической диагностики программируемых логических интегральных схем с локализацией места и причины неисправности.

Ключевые слова: технический контроль, программируемая логическая интегральная схема, модульная арифметика, криптографическое преобразование информации, техническая диагностика, автономное техническое средство.

Introduction

Cryptographic transformation of information (hereinafter referred to as KPI) is the process of changing information that depends on the parameter being changed, and has the property that it is impossible to restore the original information from the transformed one, without knowing the current key, with a labor intensity less than the specified one.

Currently, KPI is implemented by software, hardware, and software-to-hardware tools. At the same time, in the case of even a minimal error of one bit, the information recovery process becomes impossible.

Especially relevant is the problem of error occurrence during KPI on autonomous technical means (hereinafter referred to as PBX) that operate at a long distance from the technical operator and transmit cryptographically transformed information to the processing object via radio channels.

In this regard, there is a need for autonomous monitoring of the implementation of KPI on the PBX in order to determine the error in advance and, if possible, eliminate the malfunction of the device that performs KPI.

The main computing device that performs KPI is currently a programmable logic integrated circuit. This computing tool is the most versatile for implementing various KPI algorithms.

The most cryptographic algorithms are based on four basic logical operations:

– modulo 2 addition operation.
– modulo 2^16 addition operation;
– cyclic shift operation.
– substitution operation.

Control of these logical operations will allow you to most fully determine the technical condition of the FPGA performed by the KPI on the PBX.

Consider numerical control of arithmetic operations modulo. The construction of control schemes is based on two theorems [1].

Theorem 1. The sum of numbers is comparable modulo q with the sum of the residuals r of the same numbers, i.e. [2]

$$\sum_{i=1}^{n} A_i = \sum_{i=1}^{n} r_{ai} \bmod q. \quad (1)$$

Theorem 2. The product of numbers is comparable modulo q with the product of the residuals r of the same numbers, i.e. [2]

$$\prod_{i=1}^{n} A_i = \prod_{i=1}^{n} r_{ai} \bmod q. \quad (2)$$

Let us consider control schemes for the following transformations: summation modulo 2, summation modulo 2^{16}, substitution and cyclic shift operation [3], [4], [5].

Results and Discussion

Development of an algorithm for controlling the modulo summation operation. The control scheme for adding numbers modulo 2 is shown in Fig. 1.

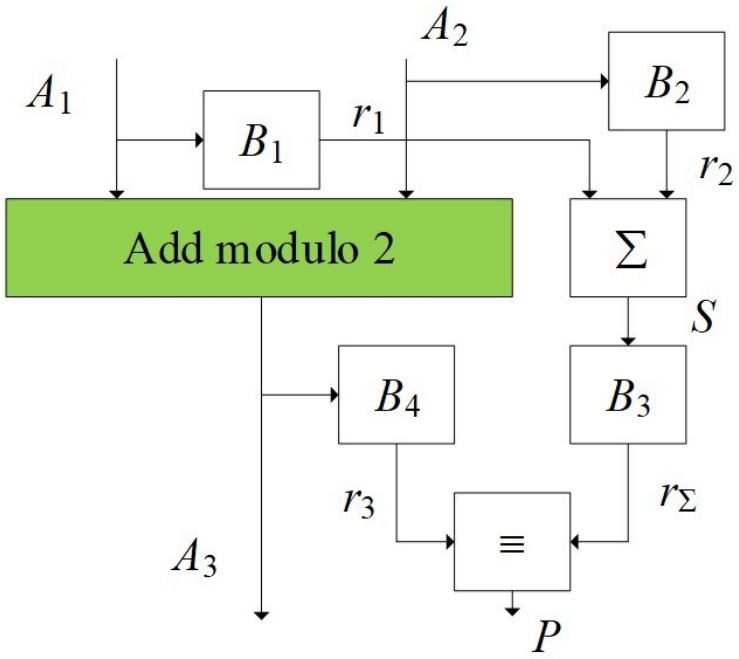

Figure 1 - Control of the value of binary numbers modulo 2
DOI: https://doi.org/10.60797/IRJ.2024.150.121.1

In general, the operation of this scheme can be described in the following way.

The result of summing two numbers A_1 and A_2 is the number A_3. In blocks B_1 and B_2, the residuals r_1 and r_2 numbers A_1 and A_2 before conversion, respectively. Then, in block S, the resulting residuals are summed up. Since the sum of the residuals can be greater than the modulus, then at the output of the adder, it is necessary to perform the operation of finding the remainder again using the conversion in block B_3. As a result, the remainder r_{A3} obtained from the number A_3 is compared with the sum of the remainder of the numbers A_1 and A_2 – r_{Σ} in the comparison module (≡) with the formation of the "norm" sign (P) in the form of a logical unit and zero – otherwise. It should be noted that the P-value is an additional feature (parameter) of the subsystem functioning and diagnostics model, i.e. $P \in \Omega_{\zeta}$.

The functioning of the presented control scheme can be divided into several stages:

1. At the initial stage, the numbers involved in the addition operation modulo 2 are obtained. After that, the remainder of the terms r_1, r_2 and their sum ($S = r_1 + r_2$) are found.

2. In the next step, we determine the remainder r_3 of the sum of the residuals S and the remainder r_4 of the sum of the terms A_1 and A_2.

3. At the last stage, a report is generated about whether the summation is correct (output P_1) or not (output P_2).

From a formal point of view, these stages can be represented as a set of the following maps [6]:

$$B_1 : A_1 \rightarrow r_1, \tag{3}$$

where B_1 is an operator that characterizes getting the remainder r_1 from a number A_1.

$$B_2 : A_2 \rightarrow r_2, \tag{4}$$

where B_2 is an operator that characterizes getting the remainder r_2 from a number A_2.

$$S : \sum_{i=1}^{2} r_i \rightarrow s, s \in \mathrm{S} \tag{5}$$

where S is the operator for finding the sum of balances r_1 and r_2.

$$B_3 : S \rightarrow r_3, \tag{6}$$

where B_3 is an operator that characterizes obtaining the remainder r_3 from the sum of the remainder r_1 and r_2.

$$P : r_3 \vee r_4 \rightarrow p, p \in \{1, 0\}, \tag{7}$$

where P is an operator that characterizes obtaining the solution p.

When controlling addition modulo 2^16, the scheme is simplified, taking into account the fact that the remainder of two numbers is calculated in the transformation itself (Fig. 2).

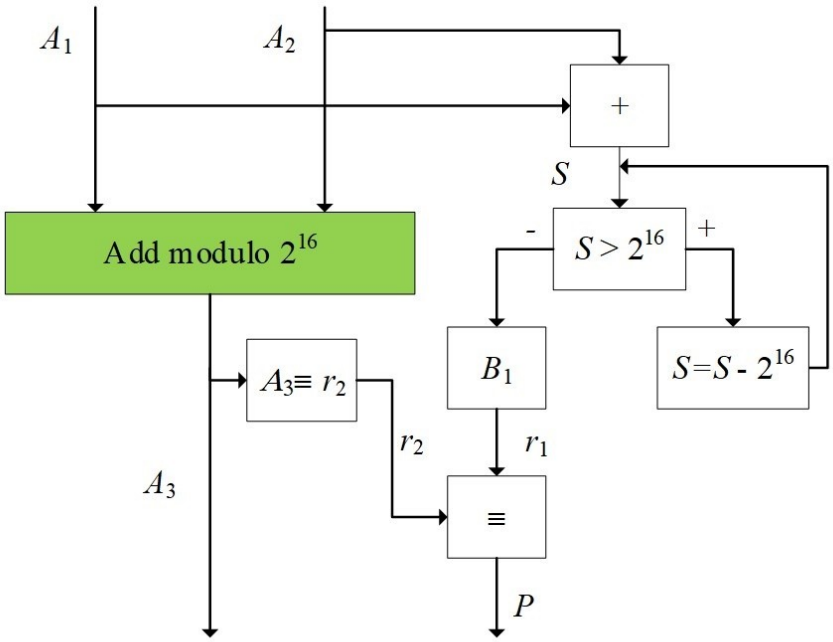

Figure 2 - Control of the position of binary numbers modulo 2^16

DOI: https://doi.org/10.60797/IRJ.2024.150.121.2

The functioning of the presented control scheme can be divided into several stages:

1. At the initial stage, the addition of numbers is performed. After that, the sum is compared with the number 2^16. If the value is exceeded, the difference is calculated $S > 2^{16} \Rightarrow S = S - 2^{16}$.

2. In the next step, we define the remainder r_1 of the sum of the numbers S and the remainder r_2 as a number A_3 ($A_3 \equiv r_2$).

3. At the last stage, a report is generated about whether the summation is correct (output P_1) or not (output P_2).

Basic analytical relations [7]:

$$B_1 : S \rightarrow r_1, \tag{8}$$

where B_1 is an operator that characterizes getting the remainder r_1 from a number S.

$$P : r_1 \vee r_2 \rightarrow p, p \in \{1, 0\}, \tag{9}$$

where P is an operator that characterizes obtaining the solution p.

The control scheme of the shift operation is shown in Fig. 3.

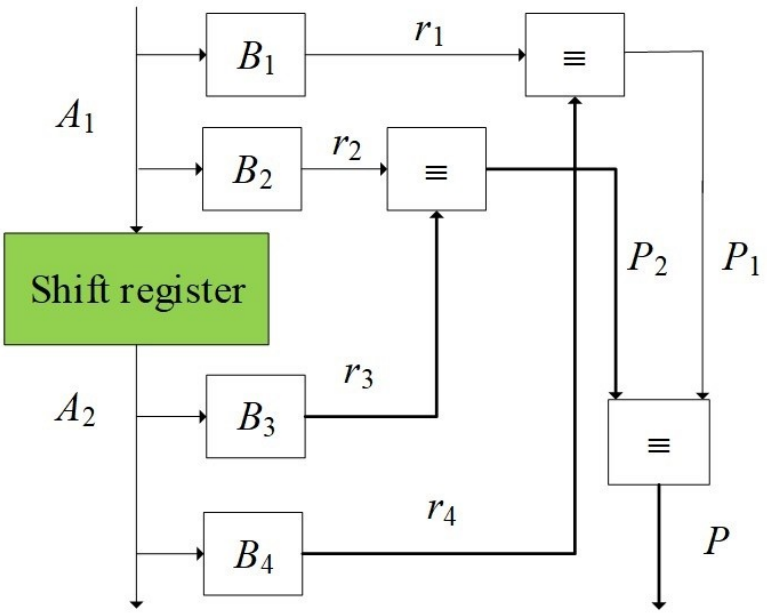

Figure 3 - Control scheme for the shift operation
DOI: https://doi.org/10.60797/IRJ.2024.150.121.3

The functioning of the presented control scheme can be divided into several stages:

1. At the initial stage, the number is represented A_1 as two numbers relative to the number of clock cycles of the shift towards the highest digit. The residuals of the indicated numbers are calculated. Similarly, the component numbers are determined A_2 and the residuals are calculated.
2. In the next step, the remainder of the numbers before and after the shift is compared.
3. At the last stage, a report is generated about whether or not the number shift (P) is correct.

Basic analytical relations [8], [9]:

$$B_1 : A_1 \rightarrow r_1$$
$$B_2 : A_1 \rightarrow r_2 \quad (10)$$

where B_1, B_2 are operators that characterize obtaining residuals r_1 and r_2 from a number A_1.

$$B_3 : A_2 \rightarrow r_3$$
$$B_4 : A_2 \rightarrow r_4 \quad (11)$$

where B_3, B_4 are operators that characterize obtaining residuals r_3 and r_4 from a number A_2.

Comparing numbers before and after the shift

$$r_1 \equiv r_4 : P_2$$
$$r_2 \equiv r_3 : P_1 \quad (12)$$

where P_1, P_2 are the results of comparing the residuals r_3 and r_4.

$$P : P_1 \vee P_2 \rightarrow p, p \in \{1, 0\}, \quad (13)$$

where P is an operator that characterizes obtaining the solution p.

The control scheme for substitution operations is shown in Figure 4.

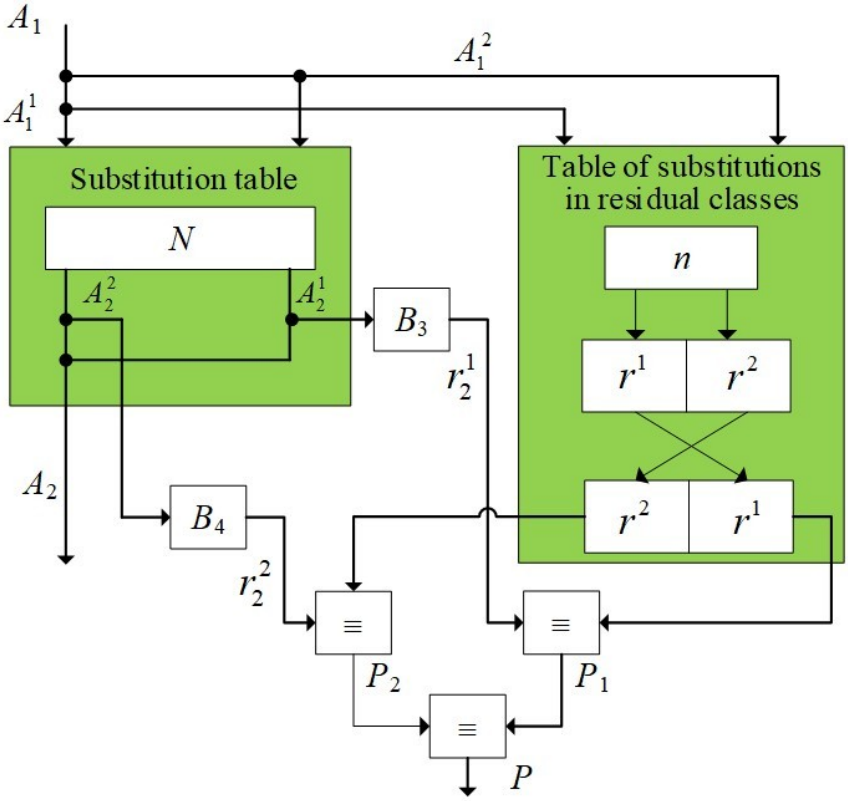

Figure 4 - Control scheme for the substitution operation
DOI: https://doi.org/10.60797/IRJ.2024.150.121.4

The functioning of the presented control scheme can be divided into several stages:

The functioning of the presented control scheme can be divided into several stages:

1. At the initial stage, the division of the numbers A_1 and A_2 by the corresponding numbers is carried out, and the definition of the numbers $A_1 = \langle A_1^1, A_1^2 \rangle$ and $A_2 = \langle A_2^2, A_2^1 \rangle$.

2. From the table of residuals n, select the residuals r_1 and r_2.

3. The remainder (r_2^1 and r_2^2) of the numbers are generated after performing the substitution operation and compared with the remainder from the remainder table.

4. At the last stage, a report is generated about whether the substitution is correct or not (P).

Basic analytical relations [10]:

$$B_3 : A_2^1 \rightarrow r_2^1, \tag{14}$$

where B_3 is an operator that characterizes getting the remainder r_2^1 from a number A_2^1 .

$$B_4 : A_2^2 \rightarrow r_2^2 \tag{15}$$

where B_4 is an operator that characterizes getting the remainder r_2^2 from a number A_2^2 .

Comparing numbers before and after the shift

$$\begin{aligned} r_2^2 \equiv r^2 : P_2 \\ r_2^1 \equiv r^1 : P_1 \end{aligned} \tag{16}$$

where P_1, P_2 are the results of comparing the residuals r_2^1 and r_2^2 .

$$P : P_1 \vee P_2 \rightarrow p, p \in \{1, 0\}, \tag{17}$$

where P is an operator that characterizes obtaining the solution p.

Conclusion

Thus, we have developed control schemes for the main operations of cryptographic transformation, namely addition modulo 2,modulo 2 ^ 16, shift and substitution. Many additional parameters of the technical diagnostics process have been formed. It is necessary to make adjustments to the functioning model of the encoder, taking into account the process of its technical diagnostics, based on the obtained parameters.

Конфликт интересов

Не указан.

Рецензия

Маняшин А.В., Тюменский Индустриальный университет, Тюмень, Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2024.150.121.5

Conflict of Interest

None declared.

Review

Manyashin A.V., Tyumen Industrial University, Tyumen, Russian Federation
DOI: https://doi.org/10.60797/IRJ.2024.150.121.5

Список литературы / References

1. Поликарповский О.И. Использование системы счисления остатков в качестве математической основы для программно определяемой радиосвязи / О.И. Поликарповский, Л.О. Ковтун, Л.В. Карпова // Вестник Национального технического университета Украины. Серия "Радиотехника". Создание радиоаппаратуры. — 2019. — № 76. — С. 21–28. DOI: 10.20535/RADAP.2019.76.21-28.

2. Гладков А.В. Модификация алгоритма обнаружения и локализации ошибок в системе остаточных классов / А.В. Гладков, В.А. Кучуков, М.Г. Бабенко // Труды Института системного программирования Российской академии наук. — 2022. — № 34. — С. 75–78. DOI: 10.15514/ISPRAS-2022-34(3)-6.

3. Проворнов И.А. Роль и место приближенного метода выполнения немодульных операций в системе остаточных классов / И.А. Проворнов, Е.А. Волошин, Е.М. Гринев // Технологическое развитие науки: тенденции, проблемы и перспективы. — 2018. — № 1. — С. 50–52.

4. Волошин Е.А. Быстрое теоретико-числовое преобразование в системе остаточных классов / Е.А. Волошин, К.Т. Тунчеров, М.В. Селиванова // Материалы 47-й Всероссийской научно-технической конференции молодых ученых, аспирантов и студентов с международным участием. — 2020. — № 1. — С. 716–718.

5. Валуева М.В. Разработка аппаратной реализации нейросетевого классификатора визуальных образов с использованием вычислений в системе остаточных классов / М.В. Валуева // Сборник тезисов участников форума "Наука будущего – наука молодых". — 2017. — № 12(14). — С. 107–108.

6. Калита Д.И. Применение системы остаточного класса в энергосберегающих приложениях цифровой обработки сигналов / Д.И. Калита, Н.И. Червяков // Информационно-коммуникационные технологии в науке, производстве и образовании. — 2014. — № 1. — С. 227–235.

7. Малофей А.О. Математическое моделирование параллельных каналов связи для передачи данных в системе остаточных классов / А.О. Малофей, А.А. Смирнов // Математические методы и информационно-технические средства : материалы XIII Всероссийской научно-практической конференции. — 2017. — № 1. — С. 165–169.

8. Джурабаев А.Е. Реализация параллельных вычислений с большими разрядными числами на основе системы остаточных классов / А.Е. Джурабаев, М.А. Дерябин // Естественные науки – основа настоящего и фундамент будущего : материалы VII ежегодной научно-практической конференции Северо-Кавказского федерального университета "Университетская наука для региона". — 2019. — № 1. — С. 16–18.

9. Гранкин В.В. Обзор методов расширения базы системы остаточных классов / В.В. Гранкин, М.С. Карамышева // Новая наука: Теоретический и практический взгляд. — 2016. — № 1(2). — С. 120–122.

10. Ляхов П.А. Стохастический криптоанализ системы разделения секретов в системе остаточных классов / П.А. Ляхов, В.И. Теплицкий // Естественные науки – основа настоящего и фундамент будущего : материалы VI ежегодной научно-практической конференции Северо-Кавказского федерального университета "Университетская наука для региона". — 2018. — № 1. — С. 35–38.

Список литературы на английском языке / References in English

1. Polikarpovskiy O.I. Ispol'zovaniye sistemy schisleniya ostatkov v kachestve matematicheskoy osnovy dlya programmno opredelyayemoy radiosvyazi [Using the Remainder System as a Mathematical Basis for Software-Defined Radio] / O.I. Polikarpovskiy, L.O. Kovtun, L.V. Karpova // Vestnik Natsional'nogo tekhnicheskogo universiteta Ukrainy. Seriya "Radiotekhnika". Sozdanie radioapparatury [Bulletin of the National Technical University of Ukraine. Series "Radio Engineering". Creation of Radio Equipment]. — 2019. — No. 76. — P. 21–28. DOI: 10.20535/RADAP.2019.76.21-28. [in Russian].

2. Gladkov A.V. Modifikatsiya algorita obnaruzheniya i lokalizatsii oshibok v sisteme ostatkovykh klassov [Modification of the Error Detection and Localization Algorithm in the Remainder Class System] / A.V. Gladkov, V.A. Kuchukov, M.G. Babenko // Trudy Instituta sistemnogo programmirovaniya Rossiyskoy akademii nauk [Proceedings of the Institute of System Programming of the Russian Academy of Sciences]. — 2022. — No. 34. — P. 75–78. DOI: 10.15514/ISPRAS-2022-34(3)-6. [in Russian].

3. Provornov I.A. Rol' i mesto priblizhennogo metoda vypolneniya nemodul'nykh operatsiy v sisteme ostatkovykh klassov [The Role and Place of the Approximate Method of Performing Non-Modular Operations in the Remainder Class System] / I.A. Provornov, E.A. Voloshin, E.M. Grinev // Tekhnologicheskoe razvitie nauki: tendentsii, problemy i perspektivy [Technological Development of Science: Trends, Problems, and Perspectives]. — 2018. — No. 1. — P. 50–52. [in Russian].

4. Voloshin E.A. Bystroye teoretiko-chislovoe preobrazovaniye v sisteme ostatkovykh klassov [Fast Theoretical-Numerical Transformation in the Remainder Class System] / E.A. Voloshin, K.T. Tuncherov, M.V. Selivanova // Materialy 47-y Vserossiyskoy nauchno-tekhnicheskoy konferentsii molodykh uchenykh, aspirantov i studentov s mezhdunarodnym uchastiyem [Proceedings of the 47th All-Russian Scientific and Technical Conference of Young Scientists, Postgraduates, and Students with International Participation]. — 2020. — No. 1. — P. 716–718. [in Russian].

5. Valuyeva M.V. Razrabotka apparatnoy realizatsii neyrosetevogo klassifikatora vizual'nykh obrazov s ispol'zovaniem vychisleniy v sisteme ostatkovykh klassov [Development of Hardware Implementation of a Neural Network Visual Image Classifier Using Computations in the Remainder Class System] / M.V. Valuyeva // Sbornik tezisov uchastnikov foruma "Nauka budushchego – nauka molodykh" [Proceedings of the Forum "Science of the Future – Science of the Young"]. — 2017. — No. 12(14). — P. 107–108. [in Russian].

6. Kalita D.I. Primenenie sistemy ostatkovogo klassa v energosberegayushchikh prilozheniyakh tsifrovoy obrabotki signalov [Application of the Remainder Class System in Energy-Saving Applications of Digital Signal Processing] / D.I. Kalita, N.I. Chervyakov // Informatsionno-kommunikatsionnye tekhnologii v nauke, proizvodstve i obrazovanii [Information and Communication Technologies in Science, Industry, and Education]. — 2014. — No. 1. — P. 227–235. [in Russian].

7. Malofey A.O. Matematicheskoye modelirovaniye parallel'nykh kanalov svyazi dlya peredachi dannykh v sisteme ostatkovykh klassov [Mathematical Modeling of Parallel Communication Channels for Data Transmission in the Remainder Class System] / A.O. Malofey, A.A. Smirnov // Matematicheskie metody i informatsionno-tekhnicheskie sredstva [Mathematical Methods and Information-Technical Means] : proceedings of the XIII All-Russian Scientific and Practical Conference. — 2017. — No. 1. — P. 165–169. [in Russian].

8. Dzhurabaev A.E. Realizatsiya parallel'nykh vychisleniy s bol'shimi razryadnymi chislami na osnove sistemy ostatkovykh klassov [Implementation of Parallel Computations with Large Bit-Length Numbers Based on the Remainder Class System] / A.E. Dzhurabaev, M.A. Deryabin // Estestvennye nauki – osnova nastoyashchego i fundament budushchego [Natural Sciences – the Basis of the Present and the Foundation of the Future] : proceedings of the VII Annual Scientific and Practical Conference of the North-Caucasus Federal University "University Science for the Region". — 2019. — No. 1. — P. 16–18. [in Russian].

9. Grankin V.V. Obzor metodov rasshireniya bazy sistemy ostatkovykh klassov [Overview of Methods for Expanding the Remainder Class System Base] / V.V. Grankin, M.S. Karamysheva // Novaya nauka: Teoreticheskiy i prakticheskiy vzglyad [New Science: Theoretical and Practical Perspective]. — 2016. — No. 1(2). — P. 120–122. [in Russian].

10. Lyakhov P.A. Stokhasticheskiy kriptoanaliz sistemy razdeleniya sekretov v sisteme ostatkovykh klassov [Stochastic Cryptoanalysis of the Secret Sharing System in the Remainder Class System] / P.A. Lyakhov, V.I. Teplitskiy // Estestvennye nauki – osnova nastoyashchego i fundament budushchego [Natural Sciences – the Basis of the Present and the Foundation of the Future] : proceedings of the VI Annual Scientific and Practical Conference of the North-Caucasus Federal University "University Science for the Region". — 2018. — No. 1. — P. 35–38. [in Russian].