ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ
Қ. И. Сәтпаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Х А Б А Р Л А Р Ы

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный исследовательский технический университет им. К. И. Сатпаева

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
Kazakh national research technical university named after K. I. Satpayev

SERIES
OF GEOLOGY AND TECHNICAL SCIENCES

2 (434)

MARCH – APRIL 2019

THE JOURNAL WAS FOUNDED IN 1940

PUBLISHED 6 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series of geology and technical sciences scientific journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of News of NAS RK. Series of geology and technical sciences in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of geology and engineering sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабарлары. Геология және техникалық ғылымдар сериясы" ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабарлары. Геология және техникалық ғылымдар сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді геология және техникалық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия геологии и технических наук» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Известия НАН РК. Серия геологии и технических наук в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по геологии и техническим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары. Геология мен техникалық ғылымдар сериясы».
ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)

Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.).
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 30.04.2010 ж. берілген **№10892-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Мерзімділігі: жылына 6 рет.
Тиражы: 300 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
http://www.geolog-technical.kz/index.php/en/

Редакцияның мекенжайы: Қазақстан, 050010, Алматы қ., Қабанбай батыра көш., 69а.
Қ. И. Сәтбаев атындағы геология ғылымдар институты, 334 бөлме. Тел.: 291-59-38.

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Известия НАН РК. Серия геологии и технических наук».
ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)
Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№10892-Ж,** выданное 30.04.2010 г.

Периодичность: 6 раз в год
Тираж: 300 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел.: 272-13-19, 272-13-18, http://nauka-nanrk.kz /geology-technical.kz

---

Адрес редакции: Казахстан, 050010, г. Алматы, ул. Кабанбай батыра, 69а.
Институт геологических наук им. К. И. Сатпаева, комната 334. Тел.: 291-59-38.

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

News of the National Academy of Sciences of the Republic of Kazakhstan. Series of geology and technology sciences.
ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of information and archives of the Ministry of culture and information of the Republic of Kazakhstan N 10892-Ж, issued 30.04.2010

Periodicity: 6 times a year
Circulation: 300 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18, http://nauka-nanrk.kz/geology-technical.kz

Editorial address: Institute of Geological Sciences named after K.I. Satpayev
69a, Kabanbai batyr str., of. 334, Almaty, 050010, Kazakhstan, tel.: 291-59-38.

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
SERIES OF GEOLOGY AND TECHNICAL SCIENCES
ISSN 2224-5278
Volume 2, Number 434 (2019), 199 – 205 **https://doi.org/10.32014/2019.2518-170X.55**

UDC 004.056
IRSTI 81.93.29

M. Kalimoldayev[1], S. Tynymbayev[1], S. Gnatyuk[2], M. Ibraimov[3], M. Magzom[1]

[1]Institute of Information and Computational Technologies, Almaty, Kazakhstan,
[2]National aviation university, Kyiv, Ukraine,
[3]Al-Farabi Kazakh national university, Almaty, Kazakhstan.
E-mail: mnk@ipic.kz, s.tynym@mail.ru, s.gnatyuk@nau.edu.ua,
margulan.ibraimov@kaznu.kz, magzomxzn@gmail.com

THE DEVICE FOR MULTIPLYING POLYNOMIALS MODULO AN IRREDUCIBLE POLYNOMIAL

Abstract. In this paper a design of the polynomial multiplier by modulo of irreducible polynomial with coefficients in GF(2) is described. The main advantages of using the non-positional notations and the main directions of the development of the modular number systems are described. The work is implemented in the framework of a reseach on the hardware implementation of encryption algorithm based on polynomial residue number system.

Keywords: hardware encryption, binary polynomials, residue number system, hardware multiplier.

Introduction. As a result of the search for ways of increasing the efficiency of electronic computing devices, methods for detecting and correcting errors and creating highly reliable computer systems, research began in the field of nonpositional notation systems in the middle of the 20th century.

In the classical positional number system, the value of each digit in the number designation depends on its position. In contrast, in nonpositional numeration systems, the designation of numbers is based on other principles.

An example of a nonpositional system widely used in computing technologies is the residual number system (RNS) [1]. In RNS an multi-valued integer in the positional notation is represented as a sequence of several positional numbers of a small digit.

The first thought about the possibility of using RNS in computing technology was expressed by Valach and Svoboda [2]. In 1968 Akushsky and Yuditsky published the book "Machine arithmetic in residual classes" [3], a fundamental work on new machine arithmetic. They took an active part in the implementation of a specialized electronic computer based on the RNS. In parallel, Garner published a paper that describes the system of residual classes and arithmetic operations in it [4].

From the mid-1970s, theoretical developments began to be applied in technological developments. More than 150 papers were published in the period from the mid-1970s to the mid-1980s in this direction, in the same period the first patents and books on RNS were obtained. Initially, the main scope of RNS was digital signal processing. Juan built and tested a matched filter in a two-dimensional RNS capable of operating 20 million operations per second [5].

In [6] an implementation of RNS with arrays of lookup tables placed with high density in read-only memory is considered. The implementation of such a system is limited to the operations of addition, subtraction, multiplication and scaling by a predefined constant. Particular attention is paid to the scaling algorithm, and the developed two scaling algorithms are described.

Currently, RNS is often used in the development of efficient and high-performance special-purpose processors [7]. For instance, some applications of nonpositional number systems considered for neural networks processing [8], which may have a high potential in our country for the implementation of high-performance and protected artificial intelligence based systems [9], as well as for highly-parallel multi-agent computing systems [10].

RNS is widely used in cryptography. For example, modular arithmetic allows creating an effective hardware implementation of cryptographic systems [11]. The use of a nonpositional number system allows us to speed up slow computations in asymmetric encryption algorithms and increase their reliability. For example, RNS is widely used in the hardware implementation of RSA and ECC algorithms [12, 13].

In polynomial RNS in GF(2), addition and subtraction operations are performed via bitwise XOR, so that no overflow problem occurs. In other words, a modular reduction is not necessary for operations of addition and subtraction. However, coercion to the module is still necessary for multiplication.

In [14-17] described approaches to the development of a block symmetric encryption algorithm based on polynomial RNS, where secrecy is determined by the so-called "full key", which consists of a secret key (pseudo-random) sequence and the selected moduli system. Resistance against exhaustive search in this case depends not only on the length of the secret sequence but also on the composition of selected system of polynomial bases, and on the number of possible permutations of bases in that system [18]. That is, the reliability of the encryption algorithm is increased by introducing additional secret parameters in the form of a base system of a polynomial RNS. This allows creating encryption systems with customized cryptographic strength, balanced between computing performance and security for different use cases.

In [19-22], various architectures and variants of the implementation of multipliers in the RNS are presented from the point of view of application in public-key cryptographic systems.

This article discusses the multiplier version of polynomials modulo irreducible polynomial for the previously described symmetric cryptosystems based on polynomial RNS, with the possibility of using base systems of arbitrary length and composition.

The developed device of modular polynomials multiplier. Consider the design of a device for multiplying the polynomial A(x) by the polynomial B(x) modulo an irreducible polynomial P(x) with calculating the remainder R by the formula:

$$R = [A(x) * B(x)] mod\ P(x),$$

where A (x) is a polynomial-multiplicand (further multiplicand), B (x) is a polynomial-multiplier (further multiplier), where P (x) is a polynomial-module (further module), where A(x) < P(x) and B(x) < P (x).

The multiplication of polynomials modulo is performed in stages. The number of the binary representation of the multiplier - N, determines the number of stages of multiplication. At each stage, a partial remainder R_i is formed. The remainder calculated at the last stage R_{N-1} is the result of multiplying polynomials modulo. The formation of each partial remainder R_i in turn is performed in three sub-steps. In the first sub-step, the multiplicand A(x) is logically multiplied by the binary coefficient b_i of the multiplier B(x) starting from the highest bit. In the second sub-step, A(x)*b_i is summed modulo 2 with the previous intermediate partial remainder R_{i-1} shifted by one bit to the higher order and the value $C_i = A(x) * b_i \oplus 2R_{i-1}$ is calculated, in the third sub-step partial remainder R_i by reducing C_i modulo P (x).

Figure 1 shows a block diagram of a device for multiplying polynomials modulo an irreducible polynomial. The device consists of four blocks and one delay line 5. The register block - 1 consists of register RgP(x) for storing the module P(x), register RgA(x) for storing the multiplicand A(x), register RgB(x) for storing the multiplier B(x). The block 2 consists of N AND gates ($And_0 \div And_{N-1}$). The block 3 consists of adders modulo 2 ($Add2_1 \div Add2_{N-1}$). The block 4 consists of partial remainder formers - 4 ($PRF_1 \div PRF_{N-1}$).

At input 6, a polynomial is accepted - the module P (x). Input 7 is designed to receive a polynomial - multiplicand A(x). Input 8 is used to receive a polynomial – multiplier B(x). The signal "Start" is fed through the input 9. 10 - is the output of the device.

The information outputs of register RgP(x) are connected by the first information inputs of all ($PRF_1 \div PRF_{N-1}$). The information outputs of register RgA(x) are connected to the information inputs of the ($And_0 \div And_{N-1}$) circuits, and the control inputs of the ($And_0 \div And_{N-1}$) circuits are fed from the outputs of the RgB(x) register, respectively, the values of the bits $b_{N-1}, b_{N-2},.., b_1, b_0$ of the multiplier B(x). The information outputs of the circuits And_0 and And_1 are supplied respectively to the first and second information inputs of the first modulo 2 adder $Add2_1$. The informational outputs of the $Add2_1$ are connected to the second inputs PRF_1.

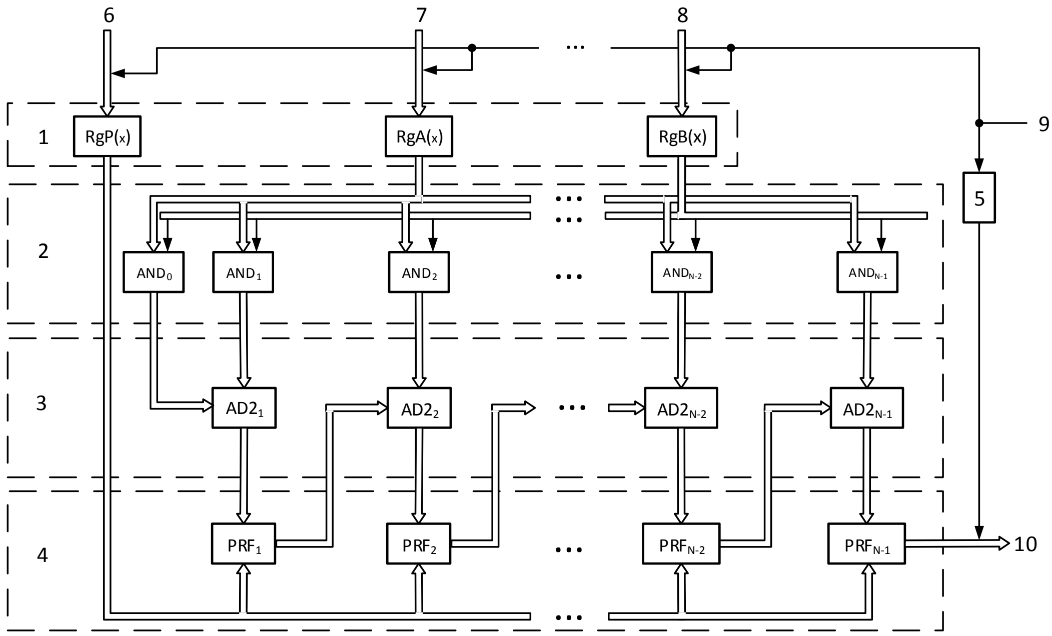

Figure 1 – Block diagram of the developed multiplier of polynomials by irreducible polynomial

The information outputs of the $And_2, And_3, \dots, And_{N-2}, And_{N-1}$ circuits are connected to the second information inputs of Add2$_2$, Add2$_3$,..,$Add2_{N-2}, Add2_{N-1}$. To the first inputs of which are fed from the information outputs $PRF_1, PRF_2, .., PRF_{N-2}, PRF_{N-1}$, respectively. Information outputs Add2$_2$, Add2$_3$, ..., $Add2_{N-2}, Add2_{N-1}$are connected to the second information inputs $PRF_1, PRF_2, .., PRF_{N-2}, PRF_{N-1}$, respectively. Information outputs PRF_1 is connected to the output of device 10. A device for multiplying polynomials modulo an irreducible polynomials works as follows.

After applying the "Start" signal to input 9, binary representation of the polynomials P(x), A(x) and B(x) from inputs 6, 7, 8, are respectively accepted into registers RgP(x), RgA(x) and RgB(x). From the outputs of register RgP(x), binary representation of the module P(x) are fed to the first inputs $PRF_1 \div PRF_{N-1}$. Binary representation of the multiplicand polynomial A(x) are fed to the information inputs of the $And_1 \div And_{N-1}$ circuits. From the information outputs of register RgB(x), bits b_{N-1}, b_{N-2},.., b_1, b_0 of the binary representation of the multiplier are fed to the control inputs of the $And_0 \div And_{N-1}$ circuits. If $b_{N-1} = 1$, then the code A(x) is generated at the output of the And_0 circuit. Since A(x)<P(x), the output $R_0 = A(x)$ is formed at the output of And_0 , which is fed to the second inputs of the adder modulo two $Add2_1$, to the first input the result of the multiplication $A(x) * b_{N-2}$comes from the outputs And_1. At the output $Add2_1$, we obtain $C_1 = R_0 \oplus A(x) * b_{N-2}$, which in turn is fed to the second input PRF_1. At the output, the first partial remainder $R_1 = C\ mod\ P(x)$ is formed, which is shifted by one bit towards the higher bit$(2 * R_1)$ is fed to the first input of the adder $Add2_2$ to the second input, which is fed from the output And$_2$ the result is logically multiplied by $A(x) * b_{N-3}$. The output $Add2_2$ forms the values $C_2 = A(x) * b_{N-3} * 2R_1$, which is fed to the second inputs PRF, where $R_2 = C\ mod\ P(x)$ is formed. Similarly, C_3, C_4,..,. C_{N-1} and R_3, R_4,..,. R_{N-1} are formed. The delayed signal "Start" on delay lines - 5 outputs the result to the output 10 of the device. The magnitude of the delay on delay line 5 determined by the time of formation of the result.

Figure 2 shows a fragment of the functional diagram of the device, where partial remainders R_0 и R_1 are formed.

The binary representations of the polynomial A(x) and the bit b_{N-1} and b_{N-2} of the multiplier B(x) are fed to the information inputs of the And_0, And_1 gates. When b_{N-1}=$b_{N-2} = 1$, $A(x) = R_0$ is formed at the output of the And_0 and we get A(x) at the output of the And_1. A (x) is fed to the inputs of the adder modulo 2 $Add2_1$ and calculates the value C$_1$, which is fed to the inputs $Add2_1$ and inputs of the circuit And$_2$, which are part of PRF_1. The highest bit C_1 is fed to the control input of the circuit And$_1$ and through the inverter NOT to the control input of the circuit And_2 PRF_1. When $C_{highest} = 1$, the result of summing

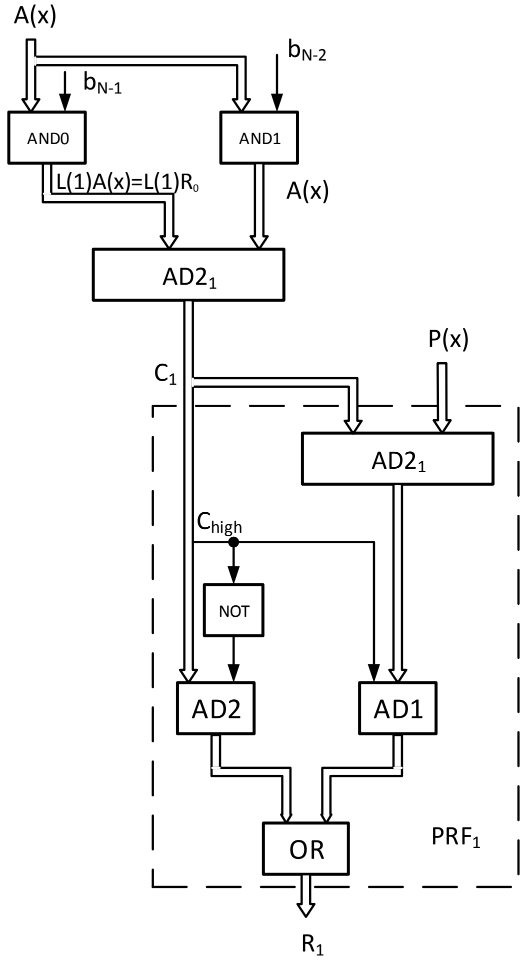

Figure 2 – Functional diagram of the partial residue Ri former

C_1 with P(x) modulo 2 from the output $Add2_1$ through the circuits And_1 and OR is transmitted to the output PRF_1 forming R_1 (with $C_1 > P(x)$).

Consider the operation of the multiplication device of polynomials A(x) and B(x) modulo irreducible polynomials P(x) with a specific example.

Let $A(x)=x^7 + x^5 + x^2 + x$, the binary representation: A(x) = 10100110; $B(x)=x^7 + x^6 + x^5 + x + 1$, binary representation: B(x) = 11100011; P(x) = $P(x)=x^8 + x^4 + x^3 + x + 1$, binary representation: P(x) = 100011011;

Since A(x) <P(x), the zero partial product (remainder) - r_0=10100110.

The procedure for calculating residues is given in table 1.

Check example shown in figure 3.

$$(x^4 + x + 1)(x^4 + x^2 + 1) = x^8 + x^6 + x^5 + x^3 + x^2 + x + 1.$$

$$\oplus \frac{\begin{array}{l} x^8 + x^6 + x^5 + x^3 + x^2 + x + 1 \\ x^8 + x^5 + x^3 \end{array}}{\oplus \frac{\begin{array}{l} x^6 + x^2 + x + 1 \\ x^6 + x^3 + x \end{array}}{R(x) = x^3 + x^2 + 1,}} \quad \begin{array}{|l} x^5 + x^2 + 1 \\ \hline x^3 + x \end{array}$$

Figure 3 – Example of the modular multiplication

The result corresponds to the binary representation - 01101.

Stages of hardware multiplication on the developed design

Stages	b_i	$2R_{i-1}, A(x) * b_i$	CM2	ФЧО
1	$b_0 = 1$ $b_1 = 0$	$R_0 = A(x) * b_0 = 10011$ $2R_0$ = 100110 $A(x)*b_1$ = 0	$C_1 = 2R_0 \oplus A(x) * b_1 = 2R_0 \oplus 0 = 100110$	R_1 = C_1modP(x) C_1 = ⊕ 100110 P(x) = 100101 R_1 = 00011
2	$b_2 = 1$	$2R_1$ = 000110 $A(x)*b_2$ = 10011	$C_2 = 2R_1 \oplus A(x) * b_2$ $2R_1$ = ⊕ 000110 $A(x)$ = 10011 C_2 = 010101	R_2 = C_2modP(x) C_2 = ⊕ 010101 P(x) = 100101 R_2 = 010101
3	$b_3 = 0$	$2R_2$ = 101010 $A(x)*b_3$ = 0	$C_3 = 2R_0 \oplus 0$ C_3 = 101010	R_3 = C_3modP(x) C_3 = 101010 P(x) = ⊕ 100101 R_3 = 001111
4	$b_4 = 1$	$2R_3$ = 011110 $A(x)*b_4$ = 10011	$C_4 = 2R_0 \oplus A(x)$ $2R_1$ = ⊕ 011110 $A(x)$ = 10011 C_2 = 001101	R_4 = C_4modP(x) C_4 = ⊕ 001101 P(x) = 100101 R_4 = 01101

Results. From the considered device of modular multiplication of polynomials it is not difficult to notice that at each stage of multiplication for calculating the partial remainder the polynomials are processed on two modulo-two adders in which there are no carry bit transfer, which allows constructing high-speed modulus multipliers.

In the proposed multiplication scheme, if the obtained remainder R(x) is multiplied by the inverse value of $B^{-1}(x)$, then the value of the polynomial A(x) can be restored. This makes it possible to implement on such multipliers high-speed devices for encrypting and decrypting data.

Conclusion. As was shown above, the main advantages of using the nonpositional number system are the absence of transfer of bits in the operations of addition and multiplication, and, consequently, the possibility of parallel execution of operations on each of the bases of the system, which significantly speeds up the calculation process. For the most effective implementation of computing devices based on the residual class system, it is required to develop non-standard circuit solutions that effectively perform calculations in the nonpositional number system.

The developed modular multiplier is to be used as a main computation unit in hardware implementation of the considered symmetric encryption system built on polynomial RNS.

Acknowledgement. This research has been supported by the Science Comittee, the Ministry of Education and Science, Republic of Kazakhstan (Institute of Information and Computational Technologies, project no. AP05132469 “Development of software-hardware facilities for cryptosystems based on the nonpositional number system”).

М. Н. Калимолдаев[1], С. Т. Тынымбаев[1], С. Гнатюк[2], М. К. Ибраимов[3], М. М. Мағзом[1]

[1]Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан;
[2]Ұлттық авиациялық университеті, Киев, Украина,
[3]Аль-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

КЕЛТІРІЛМЕЙТІН КӨПМҮШЕЛІКТЕР МОДУЛІ БОЙЫНША КӨПМҮШЕЛІКТЕРДІ КӨБЕЙТУ ҚҰРЫЛҒЫСЫ

Аннотация. Мақалада коэффициенттері GF(2) келтірілмейтін көпмүшеліктер модулі бойынша көпмүшеліктерді көбейту құрылғысының құрылысы баяндалады. Бейпозициялық санақ жүйесін қолданудың негізгі артықшылықтары және модульдік сандар жүйесін дамытудың негізгі бағыттары сипатталған. Жұмыс полиномиальды қалдық кластар сандық жүйесі негізінде құрылған шифрлау алгоритмін аппараттық түрде іске асыру бойынша зерттеулер шеңберінде жүзеге асырылады.

Түйін сөздер: аппараттық шифрлау, екілік көпмүшеліктер, қалдық кластар жүйесі, аппараттық көбейткіш.

М. Н. Калимолдаев[1], С. Т. Тынымбаев[1], С. Гнатюк[2], М. К. Ибраимов[3], М. М. Мағзом[1]

[1]Институт информационных и вычислительных технологий, Алматы, Казахстан,
[2]Национальный авиационный университет, Киев, Украина,
[3]Казахский национальный университет имени Аль-Фараби, Алматы, Казахстан

УСТРОЙСТВО УМНОЖЕНИЯ ПОЛИНОМОВ ПО МОДУЛЮ НЕПРИВОДИМЫХ ПОЛИНОМОВ

Аннотация. В статье описывается устройство умножения полиномов по модулю неприводимых полиномов с коэффициентами над GF(2). Описаны основные преимущества использования непозиционных систем счисления и основные направления развития модульных систем счисления. Работа выполняется в рамках исследований по аппаратной реализации алгоритма шифрования, построенного на базе полиномиальной системы остаточных классов.

Ключевые слова: аппаратное шифрование, бинарные полиномы, система остаточных классов, программный умножитель**.**

Information about authors:

Kalimoldayev Maksat, Director general of Institute of Information and Computational Technologies, Doctor of sciences, professor, academician member of the National Academy of Science of the Republic of Kazakhstan, Almaty, Kazakhstan; mnk@ipic.kz; https://orcid.org/0000-0003-0025-8880

Tynymbayev Sakhybay, Chief researcher, Candidate of Technical Sciences, Institute of Information and Computational Technologies, Almaty, Kazakhstan; s.tynym@mail.ru; https://orcid.org/0000-0002-9326-9476

Sergiy Gnatyuk, Doctor of sciences, Associate Professor, Leading Researcher in Cybersecurity R&D Lab, Executive Secretary of Ukrainian Scientific Journal of Information Security, Scientific Adviser of Engineering Academy of Ukraine, IEEE Member, National Aviation University, Kyiv, Ukraine; s.gnatyuk@nau.edu.ua; https://orcid.org/0000-0003-4992-0564

Ibraimov Margulan, Lead researcher, PhD, Head of Department of Physics and Technology, Al-Farabi Kazakh National University, Almaty, Kazakhstan; margulan.ibraimov@kaznu.kz; https://orcid.org/0000-0002-8049-3911

Magzom Miras, Senior researcher, PhD, Institute of Information and Computational Technologies, Almaty, Kazakhstan; magzomxzn@gmail.com; https://orcid.org/0000-0002-9380-1469

REFERENCES

[1] Garner H.L. The residue number system // IRE Transactions on Electronic Computers. 1959. Vol. 8, 2. P. 140–147. A. Omondi, B. Premkumar, "Residue Number Systems: Theory and Implementation", Advances in Computer Science and Engineering: Texts, Imperial College Press, 2007.

[2] Valach M. Vznik kodu a ciselne soustavy zbytkovych trid // Stroje Na Zpracovani Informaci, Sbornik III. 1955. A. Svoboda, M. Valach, Operatorove obvody, Stroje Na Zpracovani Informaci // Sbornik III. 1955.

[3] Sinkov M.V., Sinkova T.V., Fedorenko A.V., Chapor A.A. Unconventional system of residual classes and its founder I. Ya. Akushsky [Online]. Available: http://www.icfcst.kiev.ua/Symposium/Proceedings2/Sinkov.rtf

[4] Taylor F.J. Residue arithmetic: a tutorial with examples // IEEE Comput. 1988. 17. P. 50-62.

[5] Huang C.H., Taylor F.J. A memory compression scheme for modular arithmetic // IEEE Trans. Acoust. Speech Signal Process. ASSP-27. 1979. P. 608-611.

[6] Jullien G.A. Residue number scaling and other operations using rom arrays // IEEE Trans. Comput. C-27(4). 1978. P. 325-336.

[7] Rooju Chokshi, Krzysztof S. Berezowski, Aviral Shrivastava, Stanisław J. Piestrak, Exploiting Residue Number System for Power-Efficient Digital Signal Processing in Embedded Processors // Proceedings of the CASES '09. Grenoble, France. P. 19-28.

[8] Nakahara, Hiroki & Sasao, Tsutomu. (2015). A deep convolutional neural network based on nested residue number system. 1-6. 10.1109/FPL.2015.7293933.

[9] Kalimoldayev M.N., Pak I.T., Baipakbayeva S.T., Mun G.A., Shaltykova D.B., Suleimenov I.E. Methodological basis for the development strategy of artificial intelligence systems in the Republic of Kazakhstan in the Message of the President of the Republic of Kazakhstan dated October 5, 2018 // News of the National academy of sciences of the Republic of the Kazakhstan. Series of geology and technical sciences. 2018. Vol. 6, N 431. P. 47-54 (in Eng.). https://doi.org/10.32014/2018.2518-170X.34

[10] Samigulina G.A., Nyusupov A.T., Shayakhmetova A.S. Analytical review of software for multi-agent systems and their applications // News of the National academy of sciences of the Republic of the Kazakhstan. Series of geology and technical sciences. 2018. Vol. 3, N 429. P. 173-181 (in Eng.).

[11] Schinianakis D., Stouraitis T. Residue Number Systems in Cryptography: Design, Challenges, Robustness // Secure System Design and Trustable Computing, Springer. 2016.

[12] Schinianakis D., Fournaris A., Michail H., Kakarountas A., Stouraitis T. An RNS implementation of an Fp elliptic curve point multiplier // IEEE Trans. Circuits Syst. I 56(6). 2009. P. 1202-1213.

[13] Sousa L., Antão S., Martins P. Combining residue arithmetic to design efficient cryptographic circuits and systems // IEEE Circuits and Systems Magazine. 2016.

[14] Biyashev R.G., Nyssanbayeva S.E., Begimbayeva Ye.Ye., Magzom M.M. Modification of the cryptographic algorithms developed on the basis of nonpositional polynomial notations // Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015). Vienna, Austria, 2015. P. 170-176.

[15] Kalimoldayev M., Nyssanbayeva S., Magzom M. Model of nonconventional encryption algorithm based on nested Feistel network // Open Engineering. 2016. 6. P. 225-227.

[16] Biyashev R., Kalimoldayev M., Nyssanbayeva S., Magzom M. Development of an encryption algorithm based on non-positional polynomial notations // Proceedings of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). Chiang Mai, Thailand, 2016. P. 243-245.

[17] Kapalova N., Dyusenbayev D. Security analysis of an encryption scheme based on nonpositional polynomial notations // Open Engineering. 2016. 6. P. 250-258.

[18] Biyashev R., Nyssanbayeva S., Kapalova N. Secret keys for nonpositional cryptosystems. Development, investigation and implementation. Lambert Academic Publishing, 2014. 136 p.

[19] Schinianakis D., Stouraitis T. // A RNS Montgomery multiplication architecture//IEEE International Symposium on Circuits and Systems (ISCAS). 2011. P. 1167-1170.

[20] Chu J., Benaissa M. GF(2m) multiplier using Polynomial Residue Number System // IEEE Asia Pacific Conference on Circuits and Systems. 2008. P. 1514-1517.

[21] Urbano-Molano F., Trujillo-Olaya V., Velasco-Medina J. Design of an elliptic curve cryptoprocessor using optimal normal basis over GF(2ˆ233) // IEEE Fourth Latin American Symposium on Circuits and Systems. 2013. P. 1–4.

[22] Aitkhozhayeva E.Zh., Tynymbayev S.T. Aspects of hardware reduction modulo in asymmetric cryptography [Aspektyi apparatnogo privedeniya po modulyu v asimmetrichnoy kriptografii] // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. 2014. Vol. 5. P. 88-93. ISSN 1991-349421. DOI 10.32014/2018.2518-1467 (in Rus.).

Publication Ethics and Publication Malpractice in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-170X (Online), ISSN 2224-5278 (Print)

http://www.geolog-technical.kz/index.php/en/

Верстка *Д. Н. Калкабековой*

Подписано в печать 12.04.2019.
Формат 70x881/8. Бумага офсетная. Печать – ризограф.
15,2 п.л. Тираж 300. Заказ 2.

Национальная академия наук РК
050010, Алматы, ул. Шевченко 28, т. 272-13-19, 272-13-18