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

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

ХАБАРЛАРЫ

ИЗВЕСТИЯ

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

NEWS

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), 238 – 248 **https://doi.org/10.32014/2019.2518-170X.60**

UDK 004.056
MRNTI 81.93.29

S. Tynymbayev[1], S. A. Gnatyuk[2], Y. Zh. Aitkhozhayeva[3],
R. Sh. Berdibayev[1], T. A. Namazbayev[4]

[1]Almaty University of Power Engineering and Telecommunication, Almaty, Kazakhstan,
[2]National Aviation University, Kyiv, Ukraine,
[3]Kazakh National Research Technical University after K. I. Satpayev, Almaty, Kazakhstan,
[4]Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: s.tynym@mail.ru, s.qnatyuk@nau.edu.ua, ait_djam@mail.ru, r.berdybaev@aues.kz, tirnagog@mail.ru

MODULAR REDUCTION BASED ON THE DIVIDER BY BLOCKING NEGATIVE REMAINDERS

Abstract. The hardware implementation of a time-critical one of the basic operations of asymmetric cryptosystems – mod reduction is considered. An accelerated remainder determination method by an arbitrary modulus of number and the method implementation device based on a divider are proposed. The idea of the negative remainders blocking during division without restoring the remainder is used. The mod reduction device, possessing the raised speed is developed. A step-by-step description of the operation of the device and illustrative examples are provided. The efficiency of the proposed circuit solution is verified on the Artix-7 FPGA from Xilinx for reducible numbers of different bit (2, 16, 32, 64). Identified and presented in the form of graphs for the dependence of the spent resources (Look-Up Table, Flip - Flop, Input/Output) of the FPGA Artix-7 on the capacity of the reducible number A.

Key words: asymmetric cryptoalgorithm, cryptosystems hardware implementation, modular reduction.

Introduction. High performance is one of the significant advantages of hardware encryption compared to software encryption [1]. In addition, the hardware implementation of cryptoalgorithm ensures its integrity, and encryption and storage of keys is carried out in the encoder board itself, and not in the computer's RAM. Thus, the implementation of the algorithm itself is protected, which is also an important advantage. These and other advantages of hardware encryption have led to interest in the hardware implementation of cryptosystems, especially asymmetric (with public key), since the widespread application of asymmetric cryptosystems with secure distribution of public keys is constrained by their low performance. The asymmetric cryptosystems are applied as independent protection mean for transferring or storing data as a means of users authentication and as a means of distributing symmetric cryptosystems keys. The algorithm is based on cryptosystems public-key of such irreversible transformations as the large numbers expansion into prime factors, the calculation of the logarithm in a finite field, the calculation of the algebraic equations roots. Procedures for encryption and decryption in asymmetric crypto algorithms use complex and cumbersome mathematical calculations over very large numbers. Therefore, encryption and decryption operations are performed much more slowly than in symmetric crypto algorithms. Speed operating units development for the crypto hardware asymmetric encryption is a critical, despite their high cost. The most time-critical basic operation in asymmetric crypto algorithms is reduction mod (obtaining the remainder from division a number by a module P), which is repeated many times. For a hardware implementation reduction mod different number-theoretic methods are applied to calculate the remainder when divided by a modulus P, which leads to various devices structures [2-15].

More rapid among the classical algorithms for integer division of numbers is division without restoring the remainder. The division process itself upon hardware implementation reduces to multiple operation of algebraic addition on the adder, and shift the dividend and divisor. In this case, depending on the remainder sign, the divider is fed to the inputs of the adder either in the forward (with a negative sign of the remainder) or in the one's complement (with a positive sign of the remainder). To do this, "XOR" circuits are included in the "divider-adder register" path, which must function as control inverters. The inclusion of such circuits into the composition of the division block leads to its complication and introduces a certain delay in the transfer chains of the operand.

Modular reduction based on the divider by blocking negative remainders. Consider the division algorithm by shifted dividend which enables to exclude circuit "XOR" from the divider device.

Supposing, from one left to the left of the previous remainder $2r_{i-1}$ divisor R is subtracted. If this remainder is formed with a positive sign (Sgn=0) at the adder output, then its one's complement value ($\overline{Sgn}$ =1) the positive remainder code r_i is transmitted to the remainder register. If, as a result of this calculation, the remainder of (Sgn=0) is formed with a negative remainder (Sgn=1), then its one's complement value ($\overline{Sgn}$=0) is blocked and a negative transmission of the remainder of the remainder register inputs. In the next division step the "old" positive remainder is shifted one bit to the left, then the divider is subtracted from that remainder. Thus, producing a division by blocking negative remnants axes, division operation is reduced to only implement shift operations and subtractions. In this case, the operation of adding the divider to the partial remainder is not required. This makes it possible to exclude from the logic circuitry device's "XOR".

Given that it is not required to form the partial of dividing, the functional device driving circuit of the mod reduction number is represented in Figure 1.

Figure 1 shows that the registers RgA and RgP are used to store the reducible number A and the module P, that the numbers A and P enter through the AND1, OR1 and AND2 gates, respectively, according to the "Start" signal. There are no "XOR" between the RgP register and the CM adder, and the blocking of the negative remainder ($2r_{i-1}$-P) is performed by the signal $\overline{Sgn}$=0, which is fed to the control inputs of the block of AND4 gates, the information inputs of which are fed bits from the outputs of the adder. The AND5 gates is used to output the calculated remainder from RgA by the signal "End of operation". The adder, the NOR gates, and the AND gates block form the partial remainders generator (PRG), where the partial remainders r_i=$2r_{i-1}$-P are sequentially calculated. The schematic shown in figure 1 is called a sequential action number reduction device. In this circuit, the partial remainders calculated at each step of bringing mod r_i are received in the upper bits of the register RgA, which in the next step are shifted one bit to the left.

Matrix scheme of the device for reduction of numbers on the module with a shift by one bit in the direction of the high bit. When constructing matrix schemes for reducing the number modulo the partial remainders from the output of the next partial remainders generator is transmitted with a shift of one bit to the left by the inputs of the next partial remainders generator (PRG_{i+1}). In this case, the structure of the partial remainders generator i has the form shown in figure 2.

If T (transfer) $2r_{i-1} \geq P$, the transfer will be formed from the adder sign T=1 and wherein Sgn=0. By the signal T=1, the positive difference $2r_{i-1} - P$ (i.e. r_i) from the output of the transmitter is transmitted through the AND2 gate to the outputs of the partial remainders generator. If $2r_{i-1} < P$, then the value $2r_{i-1}$ from the input is transferred unchanged to the outputs of the partial remainders generator through the AND1 gate, by means of the signal Sgn = 1. The AND1, AND2 and OR gates form the multiplexer MS.

Figure 3 shows the matrix diagram of the device for modifying the numbers with a shift by one bit in the direction of the high bit of the number given. The device contains the register RgP for storing the N-bit module P, the register RgA for storing the 2N-bit reducible number A, N of the formers of partial residuals PRG.1 ÷ PRG.N, the delay element DL.

The information outputs of the register RgP are connected with the information inputs of the PRG.1 ÷ PRG.N / 2 for transmitting the values of $\overline{P}$. The information outputs of the RgA register of the number A are connected with the inputs of all the PRG.1. ÷ PRG.N.

Initially, the remainder R_0 is determined by the N high bits of the 2N-bit number A. The remainder R_0 shifted by one bit to the left is $2R_0$. $2R_0$ together with the bits attached to it, following the low bits of R_0 from the register RgA, represent the number $A_1 = (R_0 + a_{n-1})$. The PRG.1 defines the remainder R_1 modulo P of the number A_1.

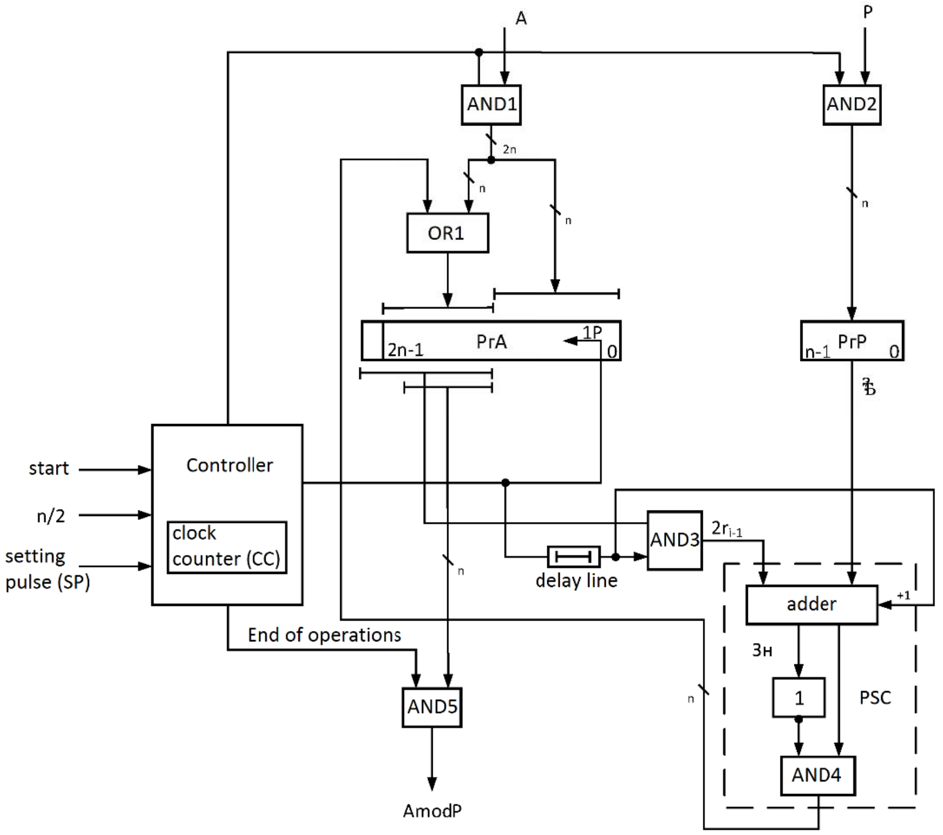


Figure 1 – The device of reduction of number A on P module on the basis of the divider with blocking of the negative remainders

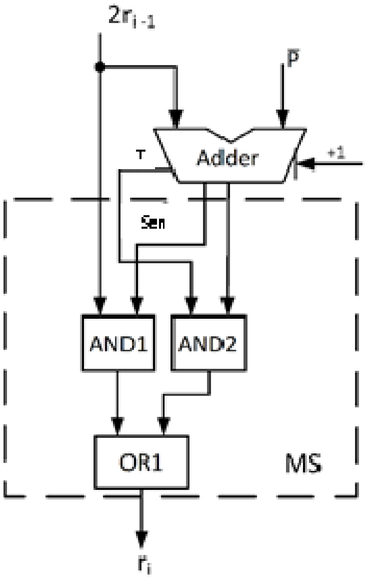


Figure 2 – Functional diagram of the partial remainders generator (PRG)
(T - transfer from the sign bit of the adder, 3n-sign of the remainder)

The formation of the number A_i ($i = 1 \div N$), which is sent to the PRG.i to determine the remainder R_i modulo P, is carried out similarly. The resulting remainder $R_{(i-1)}$ from the output of the PRG.i-1 is shifted left by one bit towards the high-order bits and the next bit of the low-order bit of the number A is added to it, which follows the bit used in the previous step to form A_{i-1}).

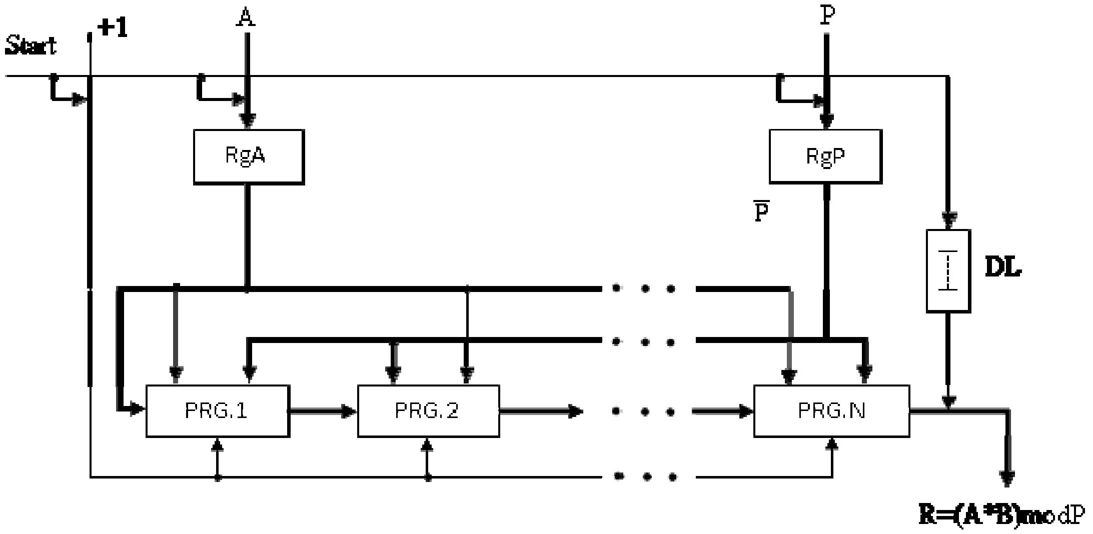


Figure 3 – Matrix scheme of the device for reduction of numbers on the module with a shift one bit to the left

Ultimately, the inputs a_0 of the number A and the partial remainder $4R_{(N-1)}$ from the outputs of the PRG.N-1 are fed to the inputs of the PRG.N from the register RgA. At the outputs of the PRG.N the final result is formed $R_{N-1} = R$.

Consider the operation of the device to reduction 2N-bit number A on the N-bit module R.

At the signal "Start", which is sent to the input device, and the value of P is taken in the register RgP. The value of the number A from the input is taken into the RgA register. Level +1 is sent to PRG.1 ÷ PRG.N.

The value of $\overline{P}$ from the outputs of the register RgP is sent to the inputs of all PRG.1 ÷ PRG.N/2. At the same time, the N high bits of the number A (ie, R_0) from the outputs of the PRG register of the number A with a shift of one bit to the left in the direction of the higher bits are sent to the inputs of the PRG.1. In this case, the low bit of the shifted code R_0 from the register RgA is appended to the bit a_{n-1} of the number A, forming the number A_1. At the output of PRG.1, a partial remainder R_1 modulo P of the number A_1 is formed. Next, the value of R_1 with a shift by one bit in the direction of the higher bit, as well as the bits a_{n-2} of the number A from the register PRG form A_2 and are sent to the inputs of the PRG.2. In this case, at the output of the PRG.2, a partial remainder R_2, etc. At the final stage, the partial remainder $R_{(N-1)}$ from the outputs of the previous PRG.N-1 is shifted by one bit towards the most significant bit and the bit a_0 of the number A from the RgA register is sent to the inputs of the PRG.N and the remainder R_N is formed at its outputs. The “End of operations” signal, which is formed at the output of the delay element DL, the remainder $R_{(N/2)}$ is output to the device.

The time of formation of the result T_{fr} is determined by the total time of the signal passing through the PRG, i.e. $T_{fr} = N/2 * T_{PRG}$.

The following is an example of a 2N-bit reduction of the number A by the N-bit module P.

$$\text{Let } A = 894_{10} = \begin{cases} a_{11}a_{10}a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0 \\ 0\ \ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \end{cases}$$

N=12; $P = 35_{10} = 100011_2$.

The high 6 bits of the binary code of the number A determine the value $R_0 = 001101_2 = 13_{10}$. By shifting the remainder R_0 to the left by one bit, appending the next bit a_5 of A, we get $A_1 = L\ (1)\ R_0 + a_5 = 2R_0 + a_5 = 27_{10}$.

For clarity, all calculations by definition of the remainder R = A mod P are given in table 1 in the decimal number system.

Table 1 – The order of calculation of R = A mod P

1 stage PRG$_1$	$A_1 = L(1)R_0 + a_5 = 26_{10} + 1_{10} = 27_{10}$	R_1=$27mod35 = 27_{10}$
2 stage PRG$_2$	$A_2 = L(1)R_1 + a_4 = 54_{10} + 1_{10} = 55_{10}$	R_2=$55mod35 = 20_{10}$
3 stage PRG$_3$	$A_3 = L(1)R_2 + a_3 = 40_{10} + 1_{10} = 41_{10}$	R_3=41mod35 = 16_{10}
4 stage PRG$_4$	$A_4 = L(1)R_3 + a_2 = 12_{10} + 1_{10} = 13_{10}$	R_4=13mod35 = 13_{10}
5 stage PRG$_5$	$A_5 = L(1)R_4 + a_1 = 26_{10} + 1_{10} = 27_{10}$	R_5=$27mod35 = 27_{10}$
6 stage PRG$_6$	$A_6 = L(1)R_5 + a_0 = 54_{10} + 0_{10} = 54_{10}$	R_6=$54mod35 = 19_{10}$ R=19_{10}

For check R = 894 mod 35 = 19_{10}.

Matrix scheme of the device to reduction the numbers on the module with a shift by two bits to the high bit. Figure 4 shows the functional diagram PRG$_i$, which consists of three binary adders Adder1, Adder2, Adder3, four groups of circuits AND1, AND2, AND3, AND4, and a group of circuits OR. The left inputs of the adders are supplied with the number A$_i$, formed from the partial remainder R$_{(i-1)}$, shifted two bits to the left high bit with the addition of two bits a$_{(n-2i+1)}$) a$_{(n-2i)}$ of the number A from the register RgA.

The $3\overline{P}$ value from the Rg3P register is sent to the right-hand inputs of the Adder3, and twice the 2P value of the registers is sent to the right-hand inputs of the Adder2. The value of $\overline{P}$ from the outputs of the register RgP is sent to the right inputs of Adder1. The lowest inputs of all adders send a level +1, which translates $3\overline{P}$, $2\overline{P}$ and $\overline{P}$ from the return code to an additional one, which allows from (4R$_{(i-1)}$ + a$_{(n-2i+1)}$ a$_{(n-2i)}$) simultaneously subtract $\overline{P}$, $2\overline{P}$ and $3\overline{P}$ on the adders Adder1, Adder2, Adder3, respectively. At the same time, the T3, T2 and T1 transfer signals, and the values of the signs Sgn3, Sgn2 and Sgn1, are generated at the outputs Adder1, Adder2, Adder3, which are sent to the control inputs of the group of circuits AND4, AND3, AND2, AND1 allowing the issuance of the partial balance R$_i$ the input of a group of circuits OR from the outputs of the corresponding adder.

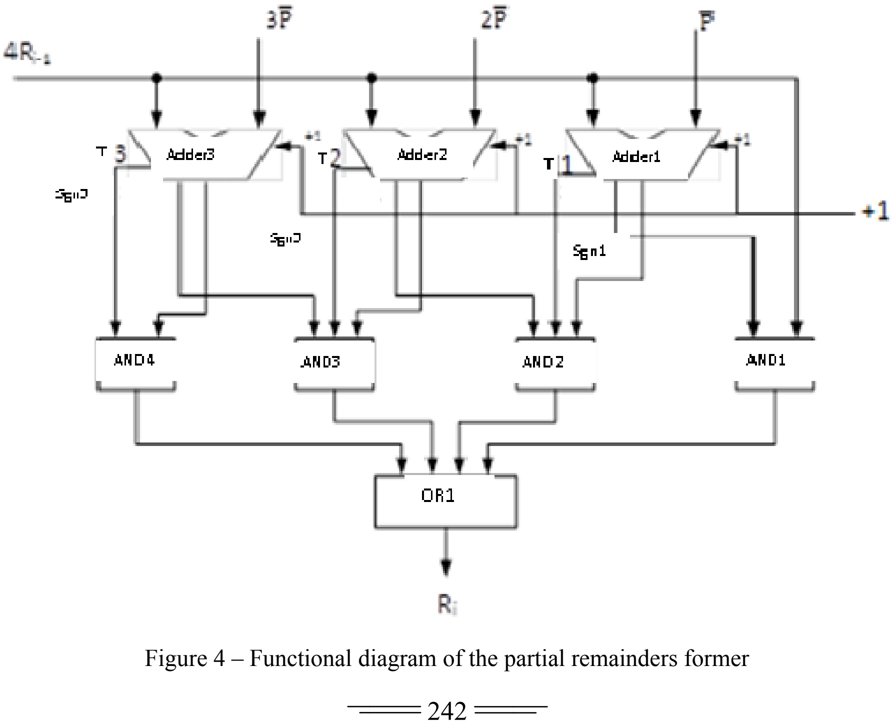


Figure 4 – Functional diagram of the partial remainders former

Figure 5 shows a diagram of the device for modifying numbers. The device contains the register RgP for storing the N-bit module P, the register Rg3P for storing the tripled module 3P, the register RgA for storing the 2N-bit reducible number A, N / 2 of partial formers of the residual frequency generator PRG.1. .3.

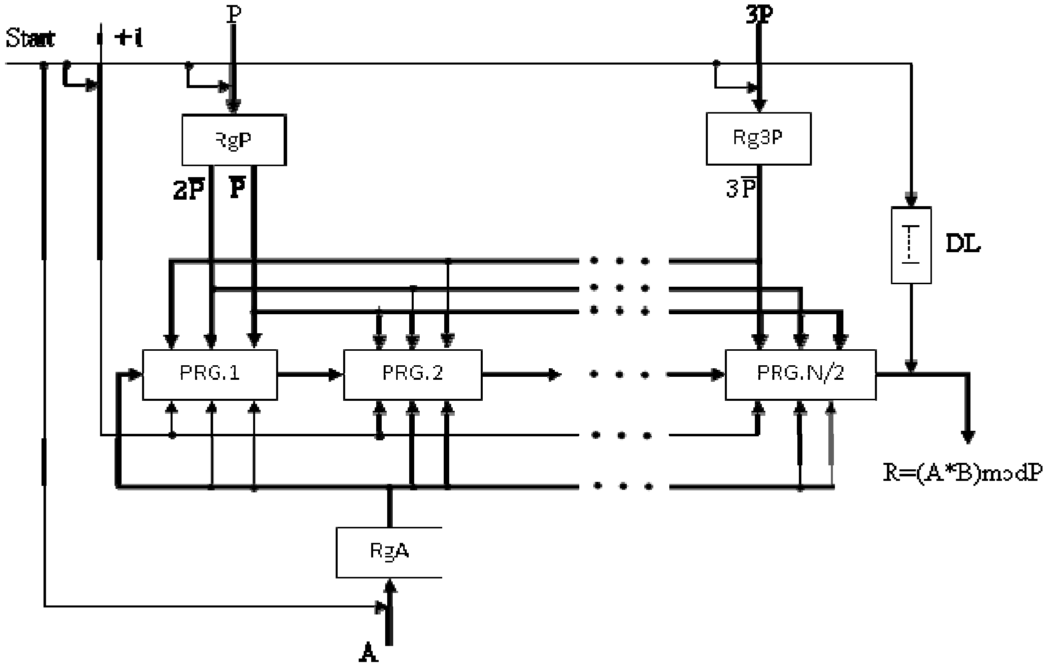


Figure 5 – Matrix scheme of the device to reduction the numbers on the module with a shift of two bits to the left

The information outputs of the register RgP are connected with the information inputs of PRG.1 ÷ PRG.N/2 for transmitting the values $\overline{P}$ and $2\overline{P}$. The value of $2\overline{P}$ is formed by transferring $\overline{P}$ with a shift of one bit to the left. The information outputs of the Rg3P register are also connected to the inputs of the PRG.1 ÷ PRG.N/2. By this connection, the value of the tripled module $3\overline{P}$ перед is transmitted. The information outputs of the RgA register of the number A are connected with the inputs of all the PRG.1. ÷ PRG.N/2.

Initially, the remainder R_0 is determined by the N bits of the 2N-bit number A. The remainder R_0 shifted two bits to the left is $4R_0$. $4R_0$ together with the two bits attached to it, following the lower bits of R_0 from the register RgA, represent the number $A_1 = (4R_0 + a_{(n-1)}\ a_{(n-2)})$. The PRG.1 defines the remainder R_1 modulo P of the number A_1.

The formation of the number A_i (i = 1 ÷ N/2), which is sent to the PRG.i to determine the remainder R_i modulo P, is carried out in a similar way. The resulting remainder $R_{(i-1)}$ from the output of the PRG.i-1 is shifted to the left by two bits towards the high-order bits, and the next two lower bits of the number A are added to it, which follow the two bits used in the previous step to form A_{i-1}.

$$A_i = L(2)R_{i-1} + a_{n-2i+1}a_{n-2i}=4R_{i-1} + a_{n-2i+1}a_{n-2i}$$

Ultimately, the inputs a_1 and a_0 of number A and the partial remainder $4R_{(N/2-1)}$ from the outputs of the PRG.N/2-1 are sent to the inputs of the PRG.N/2 from the register of RgA. At the outputs of the PRG.N/2, the final result is $R_{N/2} = R$.

Consider the operation of the device to reduction 2N-bit number A on the N-bit module R.

At the signal "Start", which is sent to the input of the device, the value of 3P is taken to the register Rg3P, and the value of P is taken to the register of RgP. The value of the number A from the input is taken into the RgA register. Level +1 is sent to PRG.1 ÷ PRG.N/2.

The value of $3\overline{P}$ from the outputs of the register Rg$3\overline{P}$, $2\overline{P}$ and $\overline{P}$ from the outputs of the register of RgP is fed to the inputs of all PRG.1 ÷ PRG.N/2. At the same time, the N high bits of the number A (i.e., R_0) from the outputs of the RgA register of the number A with a shift of two bits to the left in the direction of the higher bis are sent to the inputs of the PRG.1. At the same time, the $a_{(n-1)}\ a_{(n-2)}$ of the number A are joined to the low-order bits of the shifted code R_0 from the register RgA, forming the number A_1. At the output of PRG.1, a partial remainder R_1 modulo P of the number A_1 is formed. Further, the value of R_1 with a shift of two bits in the direction of the high bit, as well as the bits $a_{(n-3)}$ $a_{(n-4)}$ of the number A from the register RgA form A_2 and are sent to the inputs of the PRG.2. In this case, at the output of the PRG.2, a partial remainder R_2, etc. At the final stage, the partial remainder $R_{N/2-1}$ from the outputs of the previous PRG.N/2-1 with a shift of two bits towards the most high bit and the bits a_1 a_0 of the number A from the RgA register send to the inputs of the PRG.N/2 and at its outputs, the remainder $R_{N/2}$ is formed. The "End of operations" signal, which is formed at the output of the delay element DL, the remainder $R_{N/2}$ is output to the device.

The time of formation of the result T_{fr} is determined by the total time of the signal passing through the PRG, i.e. $T_{fr} = N/2 * T_{PRG}$.

Table 2 shows the conditions for the formation of the smallest positive remainder R_i at the outputs of the adders depending on the values of the transfers T3, T2, T1 and signs Sgn3, Sgn2 and Sgn1.

Table 2 – The order of formation of the partial remainder R_i

Transfers			Signs			Formation R_i at the outputs of adders			A_i
T3	T2	T1	Sgn3	Sgn 2	Sgn 1	Adder3	Adder2	Adder1	
1	1	1	0	0	0	R_i	–	–	–
0	1	1	1	0	0	–	R_i	–	–
0	0	1	1	1	0	–	–	R_i	–
0	0	0	1	1	1	–	–	–	$R_i = A_i$

There is an example of a 2N - bit number A reduction according to an N - bit module P.

$$\text{Let } A = 894_{10} = \begin{cases} a_{11}a_{10}a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0 \\ 0\ \ 0\ \ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \end{cases}$$

N=12; N/2=6;

P = 35_{10}=100011_2; 2P=70_{10} и 3P=105_{10}.

The higher RgP bits of the binary code of the number A determine the value $R_0 = 001101_2 = 13_{10}$. By shifting the remainder R_0 to the left two bits, by adding the following bits a_5 a_4 of number A, we get $A_1 = L(2)R_0 + (a_5a_4) = 4 \cdot R_0 + (a_5a_4) = 52_{10} + 3_{10} = 55_{10}$.

For clarity, all calculations by definition of the remainder R = A mod P are given in table 3 in the decimal number system.

Table 3 – The order of calculation of R = A mod P

1 stage
PRG_1
	$A_1 = L(2)R_0 + a_5a_4 = 52_{10} + 3_{10} = 55_{10}$
	Adder3: _ 55 / 105 / –50
	Adder2: _ 55 / 70 / –25
	Adder1: _ 55 / 35 / +20
		T3=T2=0
		T1=1
		Sgn2= Sgn 3=1
		Sgn1=0
		R_1=20_{10}

2 stage
PRG_2
	$A_2 = L(2)R_1 + a_3a_2 = 80_{10} + 3_{10} = 83_{10}$
	Adder3: _ 83 / 105 / –22
	Adder2: _ 83 / 70 / +13
	Adder1: _ 83 / 35 / +48
		T3=0
		T1=T2=1
		Sgn3=1
		Sgn1= Sgn2=0
		R_2=13_{10}

3 stage
PRG_3
	$A_3 = L(2)R_2 + a_1a_0 = 4 \cdot 13_{10} + 2_{10} = 54_{10}$
	Adder3: _ 54 / 105 / –51
	Adder2: _ 54 / 70 / –16
	Adder1: _ 54 / 35 / +19
		T3=T2=0
		T1=1
		Sgn2= Sgn3=1
		Sgn1=0
		R_3=R=19_{10}

For check R = 894 mod 35 = 19_{10}.

Implementation on FPGA. Checking the algorithm for reducing the number mod on the basis of a divider with the blocking of negative remainders was carried out on Field Programmable Gate-Array (FPGA). Unlike conventional digital microcircuits, the logic of the FPGA is not determined in the manufacture, but is set at the design stage of a particular device, through the appropriate programs.

For design, a debugging environment is used that allows you to set the desired structure of the digital device in the form of a program in special languages for describing the equipment Verilog, VHDL, AHDL, etc. To do this, the Nexys 4 Board of the programmable logic integrated circuit Artix-7 from the company Xilinx (figure 6). To describe the scheme of reducing the number by modulus, the language Verilog is chosen [16-20].

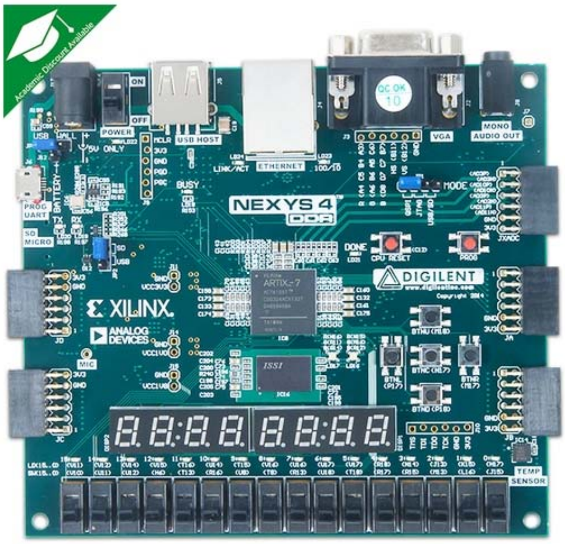


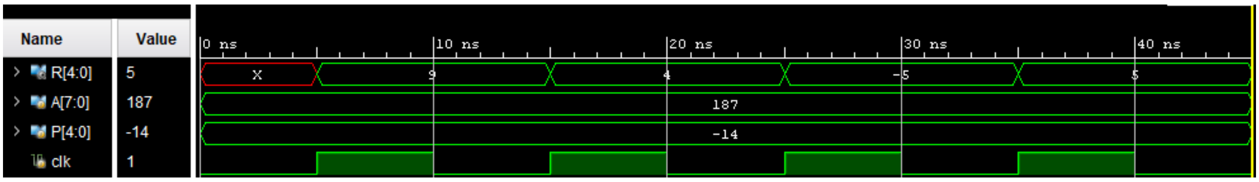
Figure 6 – Nexys FPGA Board

Table 4 shows the number of basic resources FPGA Artix-7 (XC7A100T-1CSG324C).

Table 4 – FPGA Artix-7 Resources

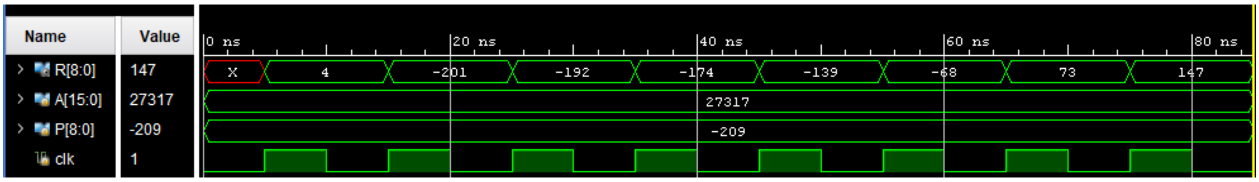
Resource	Number
LUT (Look-Up Table)	63400
FF (Flip-Flop),	126800
IO (Input / Output)	210
BUFG (architecture-independent global buffer)	32

To enter input data and a visual display of intermediate results FPGA Board is provided by all essential ports and peripheral device, the main ones are 16 switches, 16 LEDs, as well as USB-UART bridge, DDR2 128MB and others. Figure 7 shows a time diagram of the operation of the number reducing device $A_{a7\div a0} = 187_{10} = 10111011_2$ with 8 module with $P = 14_{10} = 1110_2$ a capacity of 4. The highest bits of the number A are $r_0 = 11_{10} = 1011_2$. According to the figure 7, on the rising edge of the clock pulse CP1, the contents of register A are shifted to the left by one bit and the register is formed $(2r_0 + a_3) = 23$. Partial remainder is formed $r_2 = 18 - P = 4$, which is transferred to register A. In the following clock pulse CP2 feed the contents of register A is shifted left by one bit and the register is formed ($2r_1$ + a_2) = 18. Partial remainder r_2 = 18 – P = 4 is formed, which is transferred to register A. In the next clock pulse CP3, the contents of register A are shifted to the left by one bit and the register is ($2r_2$ + a_1) = 9 formed. Partial remainder r_3 = 9 – P = –5, while transmission r_3 in register A is blocked and in it the old remainder (9) is saved. With the last clock pulse CP4, the contents of register A are shifted to the left by one bit and the register is formed ($2r_3$ + a_0) = 19, partial remainder r_4 = R = 19 – P = 5.



Name	Value
R[4:0]	5
A[7:0]	187
P[4:0]	-14
clk	1

Figure 7 – The diagram for an 8 - bit number algorithm



Name	Value
R[8:0]	147
A[15:0]	27317
P[8:0]	-209
clk	1

Figure 8 – The diagram for a 16-bit number algorithm

The figure 8 shows a similar diagram for the reducible number $A = 27317_{10}$ with a resolution of 16 mod $P = 209_{10}$ with the bit 8. The clock pulses CP1 - CP8 forms $r_1 = 4$, $r_2 = –201$, $r_3 = –192$, $r_4 = –174$, $r_5 = –139$, $r_6 = –68$, $r_7 = 73$ and $r_8 = 147 – 209 = –62$, respectively. Thus R= 27317 mod 209 = 147.

Also remainder values were calculated for the number of A with the bit 32 and 64. Figure 9 shows the dependence of resources expended FPGA Artix-7 driven on the bit number A. In this figure, LUT (Look-Up Table) – conversion table, FF (Flip-Flop) - triggers, IO (Input/Output) - inputs/outputs.

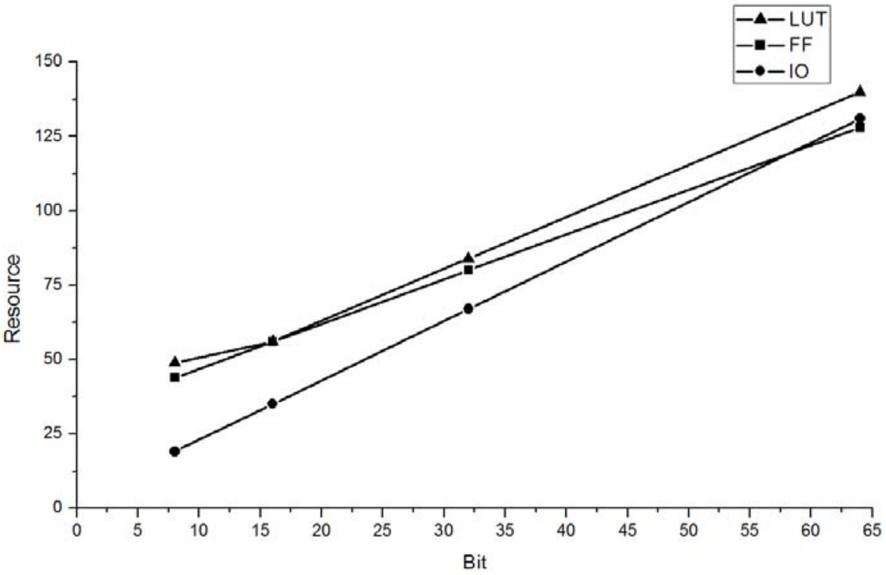


Figure 9 – Number of resources expended

The number of used resources LUT and FF does not exceed even 1% of the resources Artix-7. This allows you to use this FPGA for numbers greater bit spine than 64.

To determine the speed of the process of reducing the number module, an internal FPGA generator with a frequency of 100 MHz was used. It is known that the running time of the algorithm is directly proportional to half the length of the input bit. Knowing these data, you can calculate the elapsed time for reducing the number to a module:

$$t = \left(k/2\right)/f \,, \tag{1}$$

where k is the bit of the reducible number A, *f* – frequency of the FPGA. For example, you can determine the speed for a 16-bit number, which will be 80 ns.

Conclusion. Number reduction mod is based on divider with blocking negative remainder to optimize the structure of the device for reducing number mod. Implementation of the device on FPGA Artix-7 (XC7A100T-1CSG324C). It shows the possibility of the applicability of divider with blocking negative balances to bring the numbers mod.

Acknowledgement. The work was carried out by the authors within the framework of program-targeted financing of the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (BR053236757 "Development of software and hardware and software for cryptographic protection of information during its transmission and storage in infocommunication systems and general purpose networks").

С. Тынымбаев[1], С. А. Гнатюк[2], Е. Ж. Айтхожаева[3], Р. Ш. Бердибаев[1], Т. А. Намазбаев[3]

[1]Алматы энергетика және байланыс университеті, Алматы, Қазақстан,
[2]Ұлттық авиациялық университеті, Киев, Украина,
[3]Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан,
[4]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

ТЕРІС ҚАЛДЫҚТАРДЫ БҰҒАТТАЙТЫН БӨЛУ ҚҰРЫЛҒЫСЫ НЕГІЗІНДЕ САНДЫ МОДУЛЬГЕ КЕЛТІРУ

Аннотация. Асимметриялық криптожүйелердің уақыт бойынша күрделі негізгі операцияларлар бірі болып табылатын модулге келтіру операциясының аппаратты түрде жүзеге асырлыуы қарастырылды. Кез-келген модуль бойынша қалдықты табу әдісі және теріс қалдықтарды бұғаттайтын бөлу құрылғысы негізінде әдісті жүзеге асыратын құрылғысы ұсынылады. Жоғары жылдамдықпен модулге келтіру құрылғысы беріледі: атап айтқанда, әр түрлі жекелеген қалдықтарды құрастырушылар негізіндегі бір және екі бірлікке келтірілетін санды жылжытатын матрицалық модульге келтіру құрылғылары. Ұсынылған тізбекті шешімдердің тиімділігі Xilinx-ден Artix-7 FPGA-да әртүрлі разрядты (2, 16, 32, 64) келтірілетін сандар үшін тексерілді. Artix-7 FPGA -ның жұмсалған аппараттар қоры (Look-Up Table, Flip-Flop, Input/Output) мен келтірілетін сан разрядтылығы бойынша тәуелділігі графиктер түрінде анықталып келтірілген.

Түйін сөздер: асимметриялық криптоалгоритмдер, криптожүйелерді аппаратты жүзеге асыру, модульге келтіру.

С. Тынымбаев[1], С. А. Гнатюк[2], Е. Ж. Айтхожаева[3], Р. Ш. Бердибаев[1], Т. А. Намазбаев[3]

[1]Алматинский университет энергетики и связи, Алматы, Казахстан,
[2]Национальный авиационный университет, Киев, Украина,
[3]Казахский национальный исследовательский технический университет им. К. И. Сатпаева,
Алматы, Казахстан,
[4]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан

ПРИВЕДЕНИЕ ЧИСЛА ПО МОДУЛЮ НА ОСНОВЕ ДЕЛИТЕЛЬНОГО УСТРОЙСТВА С БЛОКИРОВКОЙ ОТРИЦАТЕЛЬНЫХ ОСТАТКОВ

Аннотация. Рассматривается аппаратная реализация критичной по времени одной из базовых операций асимметричных криптосистем - приведения по модулю. Предлагается метод определения остатка по произвольному модулю от числа и устройство реализации метода на основе делительного устройства с блокировкой отрицательных остатков. Приводится устройство приведения по модулю, обладающее повышенным быстродействием: а именно, матричные устройства приведения чисел по модулю со сдвигом приводимого числа на один и два разряда на основе различных формирователей частичных остатков. Приводятся пошаговые описания работ устройств и иллюстрационные примеры. Работоспособность предложенных схемных решения проверен на ПЛИС Artix-7 от Xilinx для приводимых чисел различной разрядности (2, 16, 32, 64). Выявлены и приведены в виде графиков зависимости затраченных ресурсов (Look-Up Table, Flip-Flop, Input/Output) ПЛИС Artix-7 от разрядности приводимого числа А.

Ключевые слова: асимметричный криптоалгоритм, аппаратная реализация криптосистем, приведение по модулю.

Information about authors:

Tynymbayev Sakhybay, Professor of the Department of Information security systems, Candidate of Technical Sciences, Almaty University of Power Engineering and Telecommunication, Almaty, Kazakhstan; s.tynym@mail.ru; https://orcid.org/0000-0002-9326-9476

Gnatyuk Sergiy, Associated Professor, Doctor of Science, National Aviation University, Kyiv, Ukraine; s.qnatyuk@nau.edu.ua; https://orcid.org/0000-0003-4992-0564

Aitkhozhayeva Yevgeniya, Associated Professor of the Department of Department of Cybersecurity, data storage and processing, Candidate of Technical Sciences, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; ait_djam@mail.ru; https://orcid.org/0000-0002-5961-8556

Berdibayev Rat, Head of the Department of Information security systems, Candidate of Political Sciences, Almaty University of Power Engineering and Telecommunication, Almaty, Kazakhstan; r.berdybaev@aues.kz; https://orcid.org/0000-0002-8341-9645

Namazbayev Timur, Senior Lecturer of the Department of Solid state physics and Nonlinear Physics, Master of Engineering Science, al-Farabi Kazakh National University, Almaty, Kazakhstan; tirnagog@mail.ru; https://orcid.org/0000-0002-2389-2262

REFERENCES

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

[2] Pankratova I.A. (2009). Number-theoretical methods of cryptography: tutorial [Teoretiko-chislovye metody kriptografii: Uchebnoe posobie]. [Tomsk State University] Tomsk. 120 p. (In Rus.).

[3] Tenca A.F., Tawalbeh L.A. (2003). Algorithm for Unified Modular Division in GF(p) and GF(2n) Suitable for Cryptographic Hardware. Electronics Letters // Electronics Letters. 2003. Vol. 40. P. 304-306. https://doi.org/10.1049/el:20040233.

[4] Nedjah N., L de Macedo Mourelle (2006). A review of modular multiplication methods and respective hardware implementations // Informatica. 2006. Vol. 30, N 1. P. 111-129.

[5] Sadiq M., Ahmed J. (2006). Complexity analysis of multiplication of long integers // Asian Journal of Information Technology. 2006. Vol. 5. P. 111-112. http://medwelljournals.com/abstract/?doi=ajit.2006.111.112.

[6] Yang W., Hseih P., Laih C. (2004). Efficient squaring of large integers. IEICE Transactions on Fundamentals of Electronics // Communications and Computer Sciences. 2004. Vol. E87-A, N 5. P. 1189-1192.

[7] Jahani S., Samsudin A., Subramanian K.G. (2014). Efficient Big Integer Multiplication and Squaring Algorithms for Cryptographic Applications // Journal of Applied Mathematics. 2014. P. 1-9. https://doi.org/10.1155/2014/107109.

[8] Petrenko V.I., Kuz'minov J.V. (2007). Modulus multiplexer [Umnojitel' po modulu]. Patent of the Russian Federation. No. 2299461. (In Rus.).

[9] Kopytov V.V., Petrenko V.I., Sidorchuk A.V. (2011). Device for generating remainder from arbitrary modulus of number [Ustroystvo dlya formirovaniya ostatka po proizvol'nomu modulu ot chisla]. Patent of the Russian Federaton. No. 2445730. (In Rus.).

[10] Orlov S.A., Tsilker B.J. (2014). Organization of computers and systems [Organizaciya EHVM i sistem], 3rd ed. SPb.: Peter. ISBN 978-5-496-01145-7. (In Rus.).

[11] Zakharov V., Stolov E., Shalagin S. (2011). Device for forming the remainder from specified module [ustrojstvo dlya formirovaniya ostatka po zadannomu modulyu]. Patent of the Russian Federation, No. 2421781. (In Rus.).

[12] Pisek E., Henige T.M. (2013). Method and apparatus for efficient modulo multiplication. Patent US No. 8417756 B2.

[13] Lambert R.J. (2014). Method and apparatus for modulus reduction. Patent US No.08862651 B2.

[14] Ivashov I.V., Kapovsky B.R., Plyasheshnik P.I., Pchelkina V.A., Iskakova E.L., Nurmukhanbetova D.E. (2018). Mathematical simulation of one-stage grinding of products frozen in blocks // News of the National Academy of Sciences of the Republic of Kazakhstan. Series of geology and technical sciences. 2018. Vol. 5, N 431. P. 48-65. https://doi.org/10.32014/2018.2518-170X.9 ISSN 2518-170X (Online). ISSN 2224-5278 (Print).

[15] Kalimoldayev M.N., Pak I.T., Baipakbayeva S.T., Mun G.A., Shaltykova D.B., Suleimenov I.E. (2018). 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 National Academy of Sciences of the Republic of Kazakhstan. Series of geology and technical sciences. 2018. Vol. 6, N 432. P. 47-54. https://doi.org/10.32014/2018.2518-170X.34. ISSN 2518-170X (Online). ISSN 2224-5278 (Print).

[16] Dubey R. (2009). Introduction to Embedded System Design Using Field Programmable Gate Arrays. Springer-Verlag London Limited. ISBN 978-1-84882-015-9.

[17] Palchaudhuri A., Chakraborty R.S. (2016). High Performance Integer Arithmetic Circuit Design on FPGA, Springer India, India. https://doi.org/10.1007/978-81-322-2520-1. ISSN 978-81-322-2519-5.

[18] Chu P.P. (2008). FPGA Prototyping by Verilog Examples, John Wiley & Sons, Inc. New Jersey. https://doi.org/10.1002/9780470374283. ISBN 978-0-470-18532-2.

[19] Deschamps J.P., Sutter G. (2007). Comparison of FPGA Implementation of the Mod M Reduction, Latin American Applied Research. 2007. Vol. 37. P. 93-97.

[20] Zhanabaev Z., Kozhagulov Y., Zhexebay D. (2016). FPGA implementations of scale-invariant models of neural networks // Turkish Journal of Electrical Engineering & Computer Sciences. 2016. Vol. 24, N 6. P. 5090-5099. https://doi.org/10.3906/elk-1504-204.

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.
15,75 п.л. Тираж 300. Заказ 2.

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