ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

ХАБАРШЫСЫ

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

PUBLISHED SINCE 1944

2

MARCH – APRIL 2019

ALMATY, NAS RK

Clarivate
Analytics

NAS RK is pleased to announce that Bulletin of NAS RK 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 Bulletin of NAS RK in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential multidiscipline content to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабаршысы" 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. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабаршысының Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді мультидисциплинарлы контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Вестник НАН РК» 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 Вестника НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному мультидисциплинарному контенту для нашего сообщества.

«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5551-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

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

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

«Вестник Национальной академии наук Республики Казахстан».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Собственник: РОО «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 **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

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

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2518-1467 (Online),
ISSN 1991-3494 (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 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

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

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

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 2, Number 378 (2019), 220 – 225 **https://doi.org/10.32014/2019.2518-1467.59**

UDC 004.056
IRSTI 81.93.29

Y. Zh. Aitkhozhayeva[1], S. Tynymbayev[1], N. A. Seilova[2], L. A. Tereikovska[3], A. Zh. Imanbayev[2]

[1]«Almaty University of Power Engineering and Telecommunications» NPJSC, Almaty, Kazakhstan,
[2]«KazNRTU after K. I. Satbayev» NPJSC, Almaty, Kazakhstan,
[3]Kyiv National University of Construction and Architecture, Kyiv, Ukraine.
E-mail: ait_djam@mail.ru, s.tynym@mail.ru, seilova_na@mail.ru, terejkowski@ukr.net, azekeee_92@mail.ru

METHOD AND DEVICE FOR MODULUS REDUCTION

Abstract. Is considered the possibility of accelerating one of the basic time-critical operations for the asymmetric cryptographic algorithm RSA - modulus reduction. The method for fast determination of residue of number by modulus and its implementation offered. Is used the idea of increased module. Alternative methods of modulus reduction are known, they require large hardware cost. Is developed device for modulus reduction, characterized by high speed with optimal costs hardware. For the calculations used combinational circuits that are characterized by high speed and low cost hardware. Is considered the step by step the work of device and the illustrative examples. Device can be used in cryptoprocessors, in digital computing systems to accelerate the division operation, for formation elements of finite fields, in computing systems using modular arithmetic.

Keywords: hardware encryption, asymmetric cryptoalgorithms, modular reduction.

Introduction. According to the leading world experts, by 2020 a quarter of the world economy will be digital. Social networks and mobile applications are actively used in education and for communication of people in society. The share of Internet users and ICT, and in Kazakhstan, too, is steadily growing [1, 2].

But these new technologies bring not only new opportunities with them, but also new problems of ensuring information security. One of the most reliable ways to ensure the protection of information stored in electronic form is cryptographic protection. Cryptographic algorithms (symmetric and asymmetric) provide transform plaintext into ciphertext by encrypting source text.

Using asymmetric encryption algorithms easier compared with symmetric encryption algorithms, since there is no need to transmit the secret key. However, their use limited by low speed, as the encryption and decryption algorithms of asymmetric cryptographic procedures employ more complex and cumbersome mathematical calculations than symmetric cryptographic algorithms [3].

To increase the speed of cryptographic systems, it is necessary to use a hardware implementation of cryptographic algorithms, which increases the speed of cryptographic algorithms by 60 times compared with the software implementation, and provides better protection. This is not the only advantage of hardware encryption [4]. The keen interest in hardware realization of asymmetric cryptoalgorithms, in particular an algorithm of RSA that used in the majority of international and national standards on protection and safety of information.

For a hardware implementation of RSA encryption and decryption developed special processors. These processors, implemented on ultra-large integrated circuits (VLSI), allows perform RSA operations associated with the exponentiation of large numbers in a very large degree modulo P in a relatively short time.

However, the RSA hardware implementation performs encryption and decryption operations about 1000 times slower than the hardware implementation of the DES - symmetric cryptographic algorithm. Such a significant difference in speed arises from the fact that RSA uses the exponentiation of multi-digit numbers (numbers with the order of 10^{309}) to a very large degree modulo *P*. RSA laboratory recommends to use keys of size 1024 bits for common tasks, and for more important tasks keys 2048 bits and more. For example, a key with a length of 4000 bits to achieve the 3rd level of security and a key with a length of 8000 bits to achieve the 4th level of security by the standard of the Republic of Kazakhstan ST RK 1073-2007 is prescribed [5].

One approach to improve the performance of public-key cryptosystems is to accelerate the performance of basic operations of asymmetric cryptoalgorithms, such as multiplication, exponentiation and reduction modulo.

Patents and articles offer various circuit solutions of devices for modulus reduction - the most complex basic operation. The devices implement various methods for obtaining modulo residue. Most of the methods are based on the polynomial representation of the reducible number *A* in binary number system. Various approaches are used to obtain the remainder R_i modulo *P*: preliminary obtaining multiples of the module *P* with their subsequent parallel subtraction from the given number *A*; obtaining residues modulo *P* from the weights of the digits 2^i, followed by their summation modulo *P* depending on the corresponding coefficient a_i of the reducible number *A*; use of preliminary calculations with preservation of results (Montgomery method); Barrett's algorithm; tabular calculators; conveyors for subtracting the module *P* from the reducible number of *A* and others [6-18].

The majority of high-speed devices is characterized by large hardware costs that are directly proportional to the quantity of bits of used numbers. Therefore, their use is problematic when applying multi-digit numbers.

Formulation of the problem. The goal of this work is to find ways to increase the speed of the hardware implementation of asymmetric cryptosystems by accelerating the most complex basic operation - reduction modulo using the idea of an increased module *P* [19].

The task is to accelerate the determination of the remainder of the number for arbitrary modulus with the optimization of hardware costs. Below we propose a method for obtaining a modulo residue for a high-speed device that allows to perform reduction modulo with optimal hardware costs.

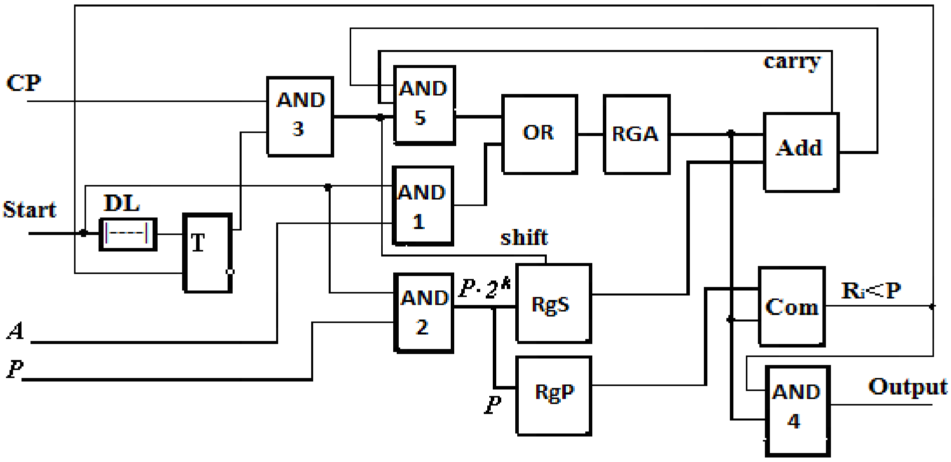
Methods. The proposed method is based on the classical iterative division method with a divider shift characterized by minimal hardware costs and low speed, which was adapted to produce a residue and modified to accelerate the production of a residue.

The method of obtaining the modulo residue, implemented in the device, is based on the fact that when the remainder *R* is obtained from dividing the initial number *A* by an arbitrary module *P*, successive subtraction from the number of the module $R = ((... ((AP) -P) - P) - ...) -P)$, is replaced by subtracting the increased module $P \times 2^k$ (using an additional code), where *k* is the difference between the digit capacity of the number *A* (excluding the leading zero bits) and the number *P*. Then from received partial remainders R_i, the values of $P \times 2^{k-i}$ $(i = 1,2, ... k)$ are subtracted. These values obtained by shifting the increased module to the right by one digit at each iteration (halving) until the next residual R_i will not be less than *P*. The subtraction of $R_{i+1} = R_i - (P \times 2^{k-i})$ is performed at each iteration. If the remainder R_{i+1} is negative, then it is not used. Otherwise, the previous residue R_i is replaced by the resulting residue R_{i+1}. The analysis of the obtained residue R_{i+1} eliminates negative residues and ends the reduction process modulo at $R_i < P$ on any iteration, which speeds up the generation of the remainder.

Results. Figure shows a structural scheme of a device in which the method proposed above is used to determine the modulo residue. This device is a modification of the device for the formation of a residue by arbitrary module patented in the Republic of Kazakhstan [19]. Description of the device is given below.

The *Start* signal allows the initial number *A* to be written through the *AND1* circuit group and the *OR* circuit group in the *RgA* register (in the register *RgA* is initially the *A* number, then the remainder R_i), the module *P* is written through the *AND2* circuit group in the *RgP* register and in the upper bits of the shift register *RgS* (in the shift register is initially $P \times 2^k$, after the shift $P \times 2^{k-i}$). The same *Start* signal with a delay sets the trigger *T* to one state via the delay element *DL*. A single potential from the direct output of the trigger *T* is fed to the circuit *AND3*, allowing further passage of the clock pulses from the *CP* input through the circuit *AND3* for clocking the operation of the device. The initial number *A* is considered as the zero residue of R_0. The residual R_i codes (initially $R_i = A$) from the *RgA* register and the *P* module from the *RgP* register are sent to the comparison circuit *Com*. Determined by $R_i < P$ or not.

The *Start* signal allows the initial number *A* to be written through the *AND1* circuit group and the *OR* circuit group in the *RgA* register (in the register *RgA* is initially the *A* number, then the remainder R_i), the module *P* is written through the *AND2* circuit group in the *RgP* register and in the upper bits of the shift



Structure of the device

register *RgS* (in the shift register is initially $P \times 2^k$, after the shift $P \times 2^{k-i}$). The same *Start* signal with a delay sets the trigger *T* to one state via the delay element *DL*. A single potential from the direct output of the trigger *T* is fed to the circuit *AND3*, allowing further passage of the clock pulses from the *CP* input through the circuit *AND3* for clocking the operation of the device. The initial number *A* is considered as the zero residue of R_0. The residual R_i codes (initially $R_i = A$) from the *RgA* register and the *P* module from the *RgP* register are sent to the comparison circuit *Com*. Determined by $R_i < P$ or not.

If $R_i < P$, then at the output of the comparison circuit *Com*, a signal "1" is generated, which, through the group of schemes *AND4*, allows the output of the number R_i from the output of the register *RgA* to the output of the result. The same signal zeroes the trigger *T*, the passage of the clock pulse is prohibited, the formation of the remainder is completed. Otherwise, the process of finding the remainder continues since at the same time, the residual R_{i+1} is formed on the combinational adder *Add* by subtracting R_i - ($P \times 2^{k-i}$). In the first step, the remainder of R_i is equal to *A*, *i* is equal to "0". When subtracting, a carry signal from the most significant bit of the combinational adder, equal to "0" or "1" will be generated.

The value of the carry signal depends on the ratio between R_i and ($P \times 2^{k-i}$).

If $R_i <$ ($P \times 2^{k-i}$), then the remainder R_{i+1} will be negative. In this case, the carry signal from the high-order combinational adder *Add* is "0" and the resulting residue R_{i+1} is not used.

If the remainder R_{i+1} is positive, then the carry signal "1" is generated from the combinational adder *Add* ($R_i \geq$ ($P \times 2^{k-i}$)). These signal allows the previous residue R_i in *RgA* to be replaced with the resulting residue R_{i+1}. With the arrival of the clock pulse *CP* from the output of the *AND3* circuit, this carry signal allows transferring the received remainder R_{i+1} from the outputs of the combinational adder *Add* via the *AND5* circuit group and the *OR* circuit group to the *RgA* register. The resulting residue R_{i+1} is written to the *RgA* register. The same clock pulse from the output of the *AND3* circuit is arrive to the shift input of the shift register *RgS*, performing a shift of the increased module *($P \times 2^{k-i}$)* in the shift register *RgS* to the right by one bit, reducing at half.

Further operation of the device is carried out similarly. The process continues until the next residue R_i becomes less than *P* *($R_i < P$).*

For each clock pulse, if a carry signal "1" is present from the high-order bit of the combinational adder *Add*, it is allowed to write into the *RgA* register the next R_{i+1} residue from the outputs of the combinational adder *Add* instead of the previous R_i and shift the increased module in the shift register *RgS* to the right by one bit. Therefore, the delay time of the *Start* signal on the delay element *DL* to set the trigger *T* to one state, allowing the passage of clock pulses, and the period of clock pulses must exceed the sum of the signal propagation time through the elements *AND1 (AND5), OR*, the write time in the register *RgA*, the subtraction time on the combinational adder *Add*. The shift time in the shift register *RgS* of the $P \times 2^{k-i}$ value is not taken into account, since the shift is performed simultaneously with the signal propagation through the elements *AND1 (AND5)*, *OR*, and with the writing to the *RgA* register. The response time of the comparison circuit *Com* is also not taken into account, since the comparison is performed simultaneously with the subtraction operation on the combinational adder *Add*.

Examples. Example 1. The following is an example of the operation of a modular device for the case when A=111_{10}=1101111_2, P=13_{10}=1101_2, k=7-4=3, $P\times2^k$= $P\times2^3$=1101000_2=104_{10}.

In this case, the capacity of *RgA, RgS* and *Add* is equal 7 bit.

By the *Start* signal, the binary code of the number *A* (1101111) is written into *RgA*, the binary code of the *P* module (number 1101) is written into *RgP*, $P \times 2^3$ (number 1101000) is written into *RgS*. The same Start signal with a delay, since it passes through the delay element *DL*, will set the trigger *T* to the state "1".

In the *Com* comparison circuit, numbers *A* and *P* are compared. Since *A*>*P*, the signal “1” is not generated at the output of the *Com* comparison circuit. There is no permission to issue a code from *RgA* to the output of the device, the process continues.

At the same time, on the combinational adder *Add*, subtraction R_1 = *A*- ($P \times 2^3$) is performed using the additional code (a.c.) of the increased module $P \times 2^3$ located in *RgS*:

$$R_1 = 1101111\text{-}1101000 = 1101111\text{+}0011000_{\text{a.c.}} = (1)\ 0000111.$$

The carry from the higher order bit in this example is presented in parentheses for clarity. The carry signal is equal to "1", since the remainder of R_1 is positive (0000010_2 = 2_{10}), and it will be used.

Through the *AND3* circuit, the first clock pulse goes to the third (enable) inputs of the *AND5* circuit group, the first (informational) inputs of the *AND5* circuit group come from the output of the combinational adder *Add* calculated residue R_1. To the second (enable) inputs of the AND5 group of circuits, the signal “1” is received (the carry from the high-order bit of the combination adder Add).. The remainder R_1 is written to *RgA*. The value of *RgA* will change and become equal to 0000111. This same clock pulse shifts the content of *RgS* to the right by one digit: $P \times 2^3$ decreases twice and becomes equal to $P \times 2^2$ = 0110100.

The process is repeated. On comparator circuit compares the obtained residue R_1 and *P*.

Since R_1<*P*, then the output of the comparison circuit generates a signal equal to "1", which through the *AND4* circuit group allows the output of the number R_1 (00000111) from the output of the *RgA* register to the output of the device. The same signal zeroes the trigger *T* (the passage of the *CP* clock signals is prohibited). The formation of the residue is completed; the residue is 00000111_2 = 7_{10}. To calculate the remainder, one clock pulse was required.

Using the classic fast division method without restoring the remainder, seven clock pulses would be required to calculate the remainder.

Example 2. Below is an example of the operation of the device for determining the remainder of the number for arbitrary modulus for the case when A=234_{10}=11101010_2, P=19_{10}=10011_2, k=8-5=3, $P\times2^k$= $P\times2^3$=10011000_2=152_{10}.

In this case, the capacity of *RgA, RgS* and *Add* is equal 8 bit.

Intermediate results and the final result for each clock pulse are shown in table (for compactness, the results are recorded in the 10th number system).

Calculation Results

Clock pulse	*Start*	1	2
RgA	234	82	6
RgP	19	19	19
RgS	152	76	38
Result at the output of the comparison circuit *Com*	0	0	1
Result at output of Combinational adder *Add*	234-152 = 82 carry = 1	82-76 = 6 carry = 1	6-38 = -32 carry = 0
Result at the device output *Output*	0	0	6

The formation of the residue is complete, the residue is 000000110_2 = 6_{10}. Calculation of the remainder required two clock pulses. Using the classic fast division method without restoring the remainder, eight clock pulses would be required to calculate the remainder.

Conclusion. When using the classic fast division method without restoring the remainder the obtaining remainder requires *m* clock pulses, where *m* is the digit capacity of *A*. When using the division acceleration method with simultaneous determination of two partial quotients, the obtaining remainder requires *m/2* clock pulses.

When using the proposed algorithm and device to obtain the remainder of dividing the number *A* by the module *P*, one to *k* clock pulses are required (depending on the ratio of the values of the number *A* and the module *P*). Always $m>k$ is, then the time benefit will be for any ratios of the values of the number *A* and the module *P*.

In the proposed device for determining the residual from the number for arbitrary modulus combinational circuits are used, which are characterized by high speed and low hardware costs.

The practical application of this device allows you to speed up the reduction modulo in cryptoprocessors. The device can also be used in digital computing systems to accelerate the operation of division, in systems for the formation of elements of finite fields, in computing systems operating in the SRC (system of residual classes).

Е. Ж. Айтхожаева[1], С. Т. Тынымбаев[1], Н. А. Сейлова[2], Л. А. Терейковская[3], А. Ж. Иманбаев[2]

[1]«Алматы энергетика және байланыс университеті» КЕАҚ, Алматы, Қазақстан,
[2]«Қ. И. Сәтбаев атындағы ҚазҰТЗУ» КЕАҚ, Алматы, Қазақстан,
[3]Киев Ұлттық Құрылыс және Сәулет Университеті, Киев, Украина

ЖЫЛДАМДЫҒЫ ЖОҒАРЫ МОДУЛЬГЕ КЕЛТІРУ ҚҰРЫЛҒЫСЫ

Аннотация. Криптожүйелерді аппартты жолмен іске асыру олардың жылдамдығын арттыруға мүмкіндік береді. Алайда асиммериялық криптоалгортмдердің төмен жылдамдығы олардың қолданылуын шектейді. Көп қолданысқа ие асимметриялық криптоалгоритм RSA шифрлау алгоритмі болып табылады. Модульге келтіру операциялар ішіндегі RSA алгортмін іске асыруды баяулататын уақыт бойынша ең қиыны болып табылады. Қалдықты екі разрядқа солға жылжытатын бөлу әдісінің түрөзгерсі қолданылатын жылдамдығы жоғары модульге келтіру құрылғысының құрылмы ұсынылады. Бұл қалдық алуды екі есеге жылдамдатуға мүмкіндік береді.

Түйін сөздер: аппаратты шифрлау, асимметриялық криптоалгоритмдер, модульге келтіру.

Е. Ж. Айтхожаева[1], С. Т. Тынымбаев[1], Н. А. Сейлова[2], Л. А. Терейковская[3], А. Ж. Иманбаев[2]

[1]НАО «Алматинский университет энергетики и связи», Алматы, Казахстан,
[2]НАО «КазНИТУ им. К. И. Сатпаева», Алматы, Казахстан,
[3]Киевский Национальный Университет Строительства и Архитектуры, Киев, Украина

МЕТОД И УСТРОЙСТВО ДЛЯ ПРИВЕДЕНИЯ ЧИСЕЛ ПО МОДУЛЮ

Аннотация. Рассматривается возможность ускорения критичной по времени одной из базовых операций асимметричного криптоалгоритма RSA - приведения по модулю. Предлагается метод ускоренного определения остатка по произвольному модулю от числа и устройство реализации метода. Используется идея увеличенного модуля. Разрабатывается устройство приведения по модулю, обладающее повышенным быстродействием при оптимальных аппаратных затратах. Для вычислений используются комбинационные схемы, которые характеризуются высоким быстродействием и малыми аппаратными затратами. Приводится пошаговое описание работы устройства и иллюстрационные примеры. Устройство приведения по модулю может применяться в криптопроцессорах, цифровых вычислительных устройствах для ускорения операции деления, в устройствах для формирования элементов конечных полей, в вычислительных устройствах, использующих модулярную арифметику.

Ключевые слова: аппаратное шифрование, асимметричные криптоалгоритмы, приведение по модулю.

Information about authors:

Aitkhozhayeva Yevgeniya Zhamalkhanovna, associated professor of the Department of Cybersecurity, information processing and storage, 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

Seilova Nurgul Abadullaevna, assistent professor of the Department of Cybersecurity, information processing and storage, Candidate of Technical Sciences, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; seilova_na@mail.ru; https:// orcid.org/0000-0003-3827-179X

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

Tereikovska Liudmyla Alekseevna, associate professor of the Department Cybersecurity and computer engineering, Candidate of Technical Sciences, Kyiv National University of Construction and Architecture, Kyiv, Ukraine; terejkowski@ukr.net; https://orcid.org/0000-0002-8830-0790

Imanbayev Azamat Zhanatuly, lecturer of the Department of Cybersecurity, information processing and storage, Master of Technical Sciences, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; azekeee_92@mail.ru; https://orcid.org/0000-0003-3719-4091

REFERENCES

[1] Kushzhanov N.V., Balginova K.M., Maydangalieva Z.A., Satygalieva G.B., Dashqin Mahammadli (2018). The digital Kazakhstan. The developmemt of human resourses in education // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. 2018. Vol. 6, N 376. P. 82-94. ISSN 2518-1467 (Online). ISSN 1991-3494 (Print). https://doi.org/10.32014/2018.2518-1467.31.

[2] Kenzhebayeva Zh.E., Yeskendirova D.M., Abdurakhmanova A.A., Bainazarova R.M., Sarieva A.M., Pestvenidze T.K. (2018). System analysis, management and processing of information // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. 2018. Vol. 5, N 375. P. 124-128. ISSN 2518-1467 (Online),. ISSN 1991-3494 (Print). https://doi.org/10.32014/2018.2518-1467.16.

[3] Shangin V.F. (2014). Information security and information protection [Informacionnaya bezopasnost i zashchita informacii] [DMK Press]. Moscow. 702 p. (in Rus.).

[4] Aitkhozhayeva E.Zh., Tynymbayev S.T. (2014). 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. Vol. 5. P. 88-93. ISSN 2518-1467 (Online). ISSN 1991-3494 (Print).

[5] ST RK 1073-2007. Means of cryptographic information protection. General technical requirements [Sredstva kriptograficheskoy zashshity informacii. Obshchie tekhnicheskie trebovaniya] [Gosstandart]. Astana, Kazakhstan, 2007 (in Rus.).

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

[7] Kovtun M., Kovtun V. (2017). Review and classification of algorithms for dividing and modulating large integers for cryptographic applications [Obzor i klassifikaciya algoritmov deleniya i privedeniya po modulyu bolshih celyh chisel dlya kriptograficheskih prilozheniy] [Kompaniya Sayfer] [http://docplayer.ru/30671408-Obzor-i-klassifikaciya-algoritmov- deleniya-i-privedeniya-po-modulyu-bolshih-celyh-chisel-dlya-kriptograficheskih-prilozheniy.html] (in Rus.).

[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] Zakharov V.M., Stolov E.L., Shalagin S.V. (2011). Device for forming the remainder from specified module [Ustroystvo dlya formirovaniya ostatka po zadannomu modulyu]. Patent of the Russian Federaton No. 2421781 (in Rus.).

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

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

[13] Bockes M., Pulkus J. (2015). Method for arbitrary-precision division or modular reduction. Patent US No. 9042543 B2 (in Eng.).

[43] Skryabin I., Sahin Y.H. (2013). Support operations for encryption algorithms with public key and their implementation in the microprocessor "Elbrus" [Operatsii podderzhki algoritmov shifrovaniya s otkryitym klyuchom i ih realizatsiya v mikroprotsessore «Elbrus»] [http://www.myshared.ru/slide/213088] (in Rus.).

[15] Hars L. (2004). Long Modular Multiplication for Cryptographic Applications. In: Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004. Lecture Notes in Computer Science, vol 3156. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-540-28632-5_4 (in Eng.).

[16] Yu H., Bai G., Hao H. (2015). Efficient Modular Reduction Algorithm Without Correction Phase. In: Wang J., Yap C. (eds) Frontiers in Algorithmics. FAW 2015. Lecture Notes in Computer Science, vol 9130. Springer, Cham. DOI: 10.1007/978-3-319-19647-3_28 (in Eng.).

[17] Tynymbayev S.T., Aitkhozhayeva E.Zh., Adilbekyzy S. (2018). High speed device for modular reduction of numbers [Ustroystvo bystrogo privedeniya chisel po modulyu]. Certificate of state registration of rights to the object of copyright of the MOJ of the RK [Svidetel'stvo MYU RK o gosudarstvennoj registracii prav na ob"ekt avtorskogo prava] No.1422 (IS 2562) (in Rus.).

[18] Tynymbayev S.T., Aitkhozhayeva Y.Zh., Adilbekkyzy S. (2018). High speed device for modular reduction // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. 2018. Vol. 6, N 376. P. 147-152. ISSN 2518-1467 (Online). ISSN 1991-3494 (Print). https://doi.org/10.32014/2018.2518-1467.38.

[19] Aytkhozhaeva E.Zh., Tynymbaev S.T. (2016). Generator remainder from arbitrary modulus of number [Formirovatel' ostatka po proizvolnomu modulyu ot chisla]. Patent of the Republic Kazakhstan [Patent Respubliki Kazakhstan]. No. 30983 (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 2518-1467 (Online), ISSN 1991-3494 (Print)

http://www.bulletin-science.kz/index.php/en/

Редакторы *М. С. Ахметова, Т. М. Апендиев, Д. С. Аленов*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 12.04.2019.
Формат 60х881/8. Бумага офсетная. Печать – ризограф.
16,0 п.л. Тираж 500. Заказ 2.

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