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

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

6

АЛМАТЫ
АЛМАТЫ
ALMATY

2018

ҚАРАША
НОЯБРЬ
NOVEMBER

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,
www: nauka-nanrk.kz, bulletin-science.kz

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 6, Number 376 (2018), 147 – 152 **https://doi.org/10.32014/2018.2518-1467.38**

UDC 004.056
IRSTI 81.93.29

S. Tynymbayev[1], Y. Zh. Aitkhozhayeva[2], S. Adilbekkyzy[3]

[1]Institute of Information and Computational Technologies, Almaty, Kazakhstan;
[2]Kazakh National Research Technical University named after K. I. Satpayev
(Satbayev University), Almaty, Kazakhstan;
[3]Universiti Tenaga Nasional (UNITEN), Kajang, Selangor, Malaysia.
E-mail: s.tynym@mail.ru, ait_djam@mail.ru, sairan.02.95@mail.ru

HIGH SPEED DEVICE FOR MODULAR REDUCTION

Abstract. It points to the advantages of hardware implementation of encryption. Hardware implementation of cryptosystems allows to increase their speed. But the low-speed of asymmetric cryptosystems, in comparison with symmetric cryptosystems, even with hardware implementation limits their application. The most used asymmetric crypto algorithm is the RSA encryption algorithm. Modular reduction is a time-critical operation that slows down the implementation of the RSA algorithm. The structure of a fast modular reduction device is proposed, in which a modified division method with a shift of the remainders by two bit positions to the left is used. This allows to speed up the receipt of the remainder twice.

Keywords: hardware encryption, asymmetric cryptoalgorithms, modular reduction.

Introduction. Cryptographic methods of information protection are indispensable in the transfer of confidential information through communication channels, establishing the authenticity of transmitted messages, storing information on storage media. Hardware implementation of cryptographic algorithms allows you to perform data encryption much faster and safer than software implementation. The development of modern microelectronics allows you to place the cryptoprocessor on a single chip [1-3].

Specialized hardware devices of cryptographic protection are not only more reliable and productive in comparison with software encryption. The list of advantages of hardware encoders that realize both symmetric and asymmetric crypto algorithms is much wider [4].

In practical implementation, the problem of high-speed symmetric cryptosystems (systems with a secret key) is the problem of key distribution. To solve this problem, asymmetric cryptosystems (two-key systems with a public key) were proposed. Asymmetric cryptosystems, in comparison with symmetric cryptosystems, have a lower speed, but there is no problem of transferring and confirming the authenticity of secret keys. Cryptography with public keys is better corresponds for key management and for protocols.

Algorithm of RSA encryption. From asymmetric cryptoalgorithms, the RSA encryption algorithm (Rivest, Shamir and Adleman, 1978), which is based on an irreversible transformation (decomposition of large numbers into prime factors), is most widely used in practice. RSA is part of ISO 9796, it is used as a public key encryption standard in the banking sector of France and Austria. Currently, the RSA algorithm is used in many protocols and programs, including:

– the S/MIME (Secure/Multipurpose Internet Mail Extensions) application layer protocol for encrypting and signing in e-mail using a public key;

– the SSH application layer protocol, in which the algorithms for the digital signature of RSA (DSA) is used for server authentication;

– the TLS (Transport Layer Security) presentation layer protocol and its predecessor SSL (Secure Sockets Layer), which are the basis of HTTPS (Hyper Text Transfer Protocol Secure);

– a set of IPSec (IP Security) network layer protocols, including authentication, integrity check and encryption of IP packets;

– the STT (Stateless Transport Tunneling) tunneling protocol for network virtualization;

– the PGP (Pretty Good Privacy) program that allows you to perform encryption and digital signature operations for messages, files and other information presented in electronic form, including transparent data encryption on storage devices, for example, on a hard disk;

– a family of standards PKCS (Public Key Cryptography Standards) designed for secure information exchange on the Internet using PKI (Public Key Infrastructure).

Therefore, many studies are focused at improving the performance of crypto-algorithm RSA.

Hardware solutions for modular reduction. To develop a high-speed RSA cryptoprocessor, it is necessary to develop fast-acting blocks of hardware implementation of algorithm operations. The basic operation of the RSA algorithm is the modular exponentiation of integers (a^xmod p). This operation is realized through multiplication, squaring and modular reduction. One of the approaches to improve the performance of public key cryptosystems is the acceleration of these operations. The most complex of them is the modular reduction operation, since it is the calculation of the remainder from dividing the number by the module P, and the division operation is the most complex of the arithmetic operations.

Theoretical and practical questions of high-speed integer multipliers and quadrants for a different class of computing systems are well developed, which cannot be said about the modular reduction. The high-speed hardware solution of the modular reduction operation is a key problem in the hardware implementation of asymmetric cryptoalgorithms that use the modular exponentiation of numbers, including RSA.

There are many different methods of calculating the remainder when dividing by the module *P* [5-10]. When using the binary (usual) representation of integers, it is possible to distinguish three types of device structures of modular reduction depending on the principle of remainder formation.

In the first type of devices blocks of formation of multiple modules *P*i (i = 1, 3, ..., k)* are used. Then these values are simultaneously (in parallel) subtracted from the reducible number *A* on *K* adders. The least positive remainder $C_i=A-P*i$ is the result [11]. This type of device has a high speed, but with increasing values of *A* and *P*, the complexity of circuits and hardware costs increase. RSA uses numbers of the order of 10^{309}, which makes it impossible to use this type of device in the practical implementation of RSA.

The second type of devices uses the method of forming the remainders (r_i) of the bit weights of the binary number (2^i) from division by module *P*. The calculated remainders modulo 2^i *(i = 0, 1, ..., k-1)* are summed if the coefficients of the corresponding weights of the number A_i are equal to 1. The summation is carried out successively on *K-1* modulo adders *P* [12]. It is implemented by the formula: $A \bmod P = (\sum_0^{k-1}(2^i \bmod P)A_i) \bmod P$. Sequential summation on *K-1* adders for large digits (*k-1*) has a negative effect on the speed of the device.

The third type of devices uses various modified methods of a machine algorithm for binary division, which leads to a wide variety of structures. When division is used with a divisor shift to the right, it is possible to obtain various device structures, one of which is given in [13].

Device structure for modular reduction. In this paper, we consider a device for fast modular reduction of a number with a shift of the remainder to the left. At each step of the calculation, the value of either tripled *(3p)* or doubled *(2p)* or single value of the module *(p)* is subtracted from the remainder r_{i-1} that shifted by two bit positions to the left. This allows to accelerate the calculation of reducing the *2n*-bit number *A* by the *n*-bit module *P* twice.

The binary representation (*2p* and *3p*) and ones' complement ($2\bar{p}$ *and* $3\bar{p}$) of the doubled and tripled module are precomputed. Then, previous remainder r_{i-1} multiplied by the four, i.e. $4r_{i-1}$ is compared on the comparators with the values *3p, 2p, p* and it is determined which of the following operations must be performed in order to compute the value of the next remainder r_i: $r_i = 4r_{i-1} - p$, or $r_i = 4r_{i-1} - 2p$, or $r_i = 4r_{i-1} - 3p$. In the adder all operations are performed in the two's complement, so $r_i = 4r_{i-1} + \bar{p} + 1$, or $r_i = 4r_{i-1} + 2\bar{p} + 1$ or $r_i = 4r_{i-1} + 3\bar{p} + 1$ is determined and formed.

A functional diagram of such a device is shown in figure 1.

The device consists of a (2n+2)-bit register *RgA*, where the reducible number *A* is stored and shifted by two bit positions to the left, the register *RgP* for storing the n-bit module *P*, the adder *Add1* for calculating the ones' complement of the tripled module value $3\bar{p}$ (by summing $2\bar{p}$ with $\bar{p}$).

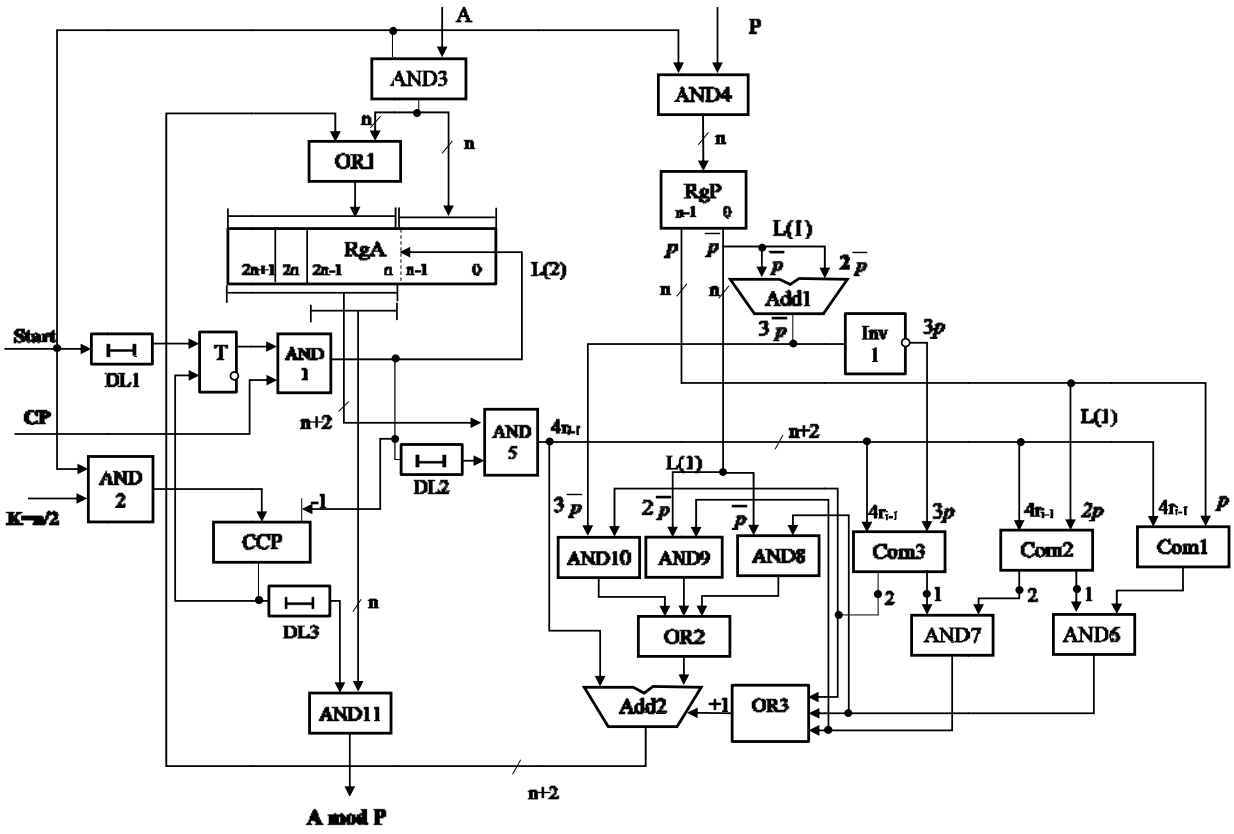

Figure 1 – High speed device for modular reduction

Values of $3p$ are formed by inverting the output bits of *Add1* on the block of inverters *Inv1*. In the comparator *Com1*, the codes $4r_{i-1}$ and p are compared.

If $4r_{i-1} < p$, then a *"0"* signal is generated at its output. Conversely, if $4r_{i-1} \geq p$, then the signal *"1"* is generated at the output of this circuit.

The *Com2* compares the value $4r_{i-1}$ with the value of the module $2p$. If $4r_{i-1} < 2p$, then at the output 1 of this circuit, the signal *"1"* is set. If $4r_{i-1} \geq 2p$, output 1 is set to *"0"* and at the output 2 is signal *"1"*.

The *Com3* compares the codes $4r_{i-1}$ and $3p$. If $4r_{i-1} < 3p$, then at the output 1 of this circuit a *"1"* signal is formed and *"0"* is set at the output 2. In case, $4r_{i-1} \geq 3p$, at the output 1 is formed by the signal *"0"* and at the output 2 the signal *"1"* is set.

Table 1 shows the executable operations, depending on the ratios of $4r_{i-1}$ with different values of the modules p, $2p$ и $3p$.

Table 1 – Executable operations for different ratios $4r_{i-1}$ with p, $2p$, $3p$

Ratios	Executable operations
$4r_{i-1} < p$	$r_i = 4r_{i-1}$
$p \leq 4r_{i-1} < 2p$	$r_i = 4r_{i-1} + \bar{p} + 1$
$2p \leq 4r_{i-1} < 3p$	$r_i = 4r_{i-1} + 2\bar{p} + 1$
$3p \leq 4r_{i-1}$	$r_i = 4r_{i-1} + 3\bar{p} + 1$

According to this table, when $4r_{i-1} < p$, the value $4r_{i-1}$ with *OR1* gates is written without changes to *RgA*.

With the ratios $p \leq 4r_{i-1} < 2p$, a signal *"1"* is generated at the output of the *AND6* gates, which is simultaneously fed to the inputs of *OR3* and *AND8* gates, the second input of the *AND8* gates are supplied

with bits $\bar{p}$. Output *AND8* gates are fed to the right inputs of the adder *Add2* via the *OR2* gates. On the left inputs *Add2*, the codes of the value $4r_{i-1}$ are fed, and through *OR3* the signal *"+1"* is fed to the input of the lowest order bit position of this adder, the operation $r_i = 4r_{i-1} + \bar{p} + 1$ is performed. The result through the block of *OR1* gates is transmitted to the highest order bit positions of the register *RgA*.

When conditions $4r_{i-1} \geq 2p$ and $4r_{i-1} < 3p$ are satisfied, a signal *"1"* is generated at the output of the *AND7* gates, which is fed to the input of the *OR3* gate and the block of the *AND9* gates. At the second data inputs of *AND9* are fed the bits of module $2\bar{p}$. Output *AND9* gates through the block of OR2 gates are fed to the right inputs of the *Add2*, and the code *"+1"* is supplied to the input of the lowest order bit position and the operation $r_i = 4r_{i-1} + 2\bar{p} + 1$ is performed in the adder. The result through the block of *OR1* gates is transmitted to the highest order bit positions of the register *RgA*.

With the ratios $4r_{i-1} \geq 3p$ from output 2 of the comparator *Com3*, a signal *"1"* is applied to the input of the *OR3* gate and to the control inputs of the *AND10* gates. At the data inputs of *AND10* gates are fed with bits of the module *p* multiplied by three $(3\bar{p})$ from the outputs of the adder *Add1*. Codes $3\bar{p}$ through the block of *OR2* gates are transmitted to the right inputs of the *Add2*, to the left inputs of this adder bits of code $4r_{i-1}$ are fed. In this case, the operation $4r_{i-1} + 3\bar{p} + 1$ is performed in the adder. The result of the operation through the block of *OR1* gates is written to the highest order bit positions of the register *RgA*.

The high speed modular reduction device works as follows.

With the signal *"Start",* the reducible number *A* and the module *P* by means of the blocks *AND3* and *AND4* gates, respectively, are received in the registers *RgA* and *RgP*. From the true outputs of the register the value of the true representation of the module *p* is transferred to the right inputs of the comparator *Com1* and shifted to the left by one bit (*2p*) is fed to the right inputs of the comparator *Com2*. From the complementary outputs of *RgP*, a ones' complement module $\bar{p}$, which is fed to the data inputs of the block of *AND8* gates and to the left inputs of the adder *Add1*. The value $3\bar{p}$ from output *Add1* is fed to the left inputs of *AND10* gates. The value $3\bar{p}$ is inverted by the inverters block *Inv1*, forming the value *3p*, which is fed to the right inputs of the comparator *Com3*.

Also, with the signal *"Start"* through the block of *AND2* gates the binary code of the number of cycles K = *n*/2 is received in the subtracting counter of the clock pulses (*CCP*). In addition, the *"Start"* signal, the delayed on delay line *DL1* for the time of recording information in *RgA* and *RgP*, is fed to the one-input of the flip-flop *T*. Flip-flop is set of to the one condition. The one condition of the trigger permits the passage of the first clock pulse *CP1* to the output of the *AND1* gate. Further, *CP1* arrives at the input of the shift register *RgA* and shifts it two bit positions to the left, increasing the contents of *RgA* by four. At the same time, the value of the counter decreases by one by the pulse *CP1*. During shift of information in *RgA CP1* is delayed on *DL2*. After this, the shifted by two bit positions content of *RgA* through the block of the *AND5* gates is transferred to the left inputs of the adder *Add2, Com3, Com2, Com1.*

Further, depending on the ratio of the $4r_{i-1}$ code and the values of the modules *3p, 2p* and *p*, a signal *"1"* is generated either at the output of the *AND*6 or *AND*7 gates, or at the output 2 of the comparator *Com3*. According to the generated signal *"1"*, the calculation r_i is performed with reference to table 1. The resulting partial remainder r_i by the block *OR1* gates is transmitted to the register *RgA*, being memorized in the highest order bit positions of the register *RgA*. At this point, the circuit receives a second clock pulse *CP2*, which passes through the block of *AND*1 gate and shifts *RgA* another two bit positions to the left, forming the value $4r_i$. Simultaneously, *CP2* arrives at the subtracting input of the *CCP* and reduces its state by one. The value $4r_i$ from the outputs of the *AND*5 gates goes to the inputs *Add2, Com3, Com2, Com1*. In the adder *Add2* the intermediate remainder r_{i+1} is calculated, which is transmitted to the highest order bit positions of the register *RgA*.

After the $n/2^{th}$ clock pulse arrives in the *CCP*, a zero code is set and the signal *"End of operation"* is generated, which is fed to the zero-input of the flip-flop T and blocks the passage of the next clock pulse to the output of the AND1 gate. The last clock pulse calculates the last remainder $r_{n/2}$, which is stored in the highest order n-bit positions of the register *RgA*, which is the result of the calculation. The result from *RgA*, on the signal *"End of Operation",* which was delayed on *DL3*, is output by the block the *AND11* gates to the output.

Results. The presented device allows to accelerate the calculation by reducing the *2n*-bit number *A* modulo *P* by two times. The number of cycles necessary to reducing any number A modulo P is defined as $K = n/2$, where *n* is bits of the module P. For this device, a certificate of authorship has been obtained [14].

Conclusion. When processing a large amount of data on the same algorithm, the most productive are the pipeline structures. When encrypting data, the modular reduction operation is performed for a large amount of different numbers. Therefore, to increase the speed, it is advisable to use pipeline structures. When pipelining, the whole process is divided into a sequence of completed steps. Each of the stages of the division procedure is computed at its stage pipeline, with all stages running in parallel.

On the base of the modification of the above device, it is possible to construct a pipelined device for formation of the remainders by arbitrary module *P* of the number *A*.

REFERENCES

[1] Dhir Amit (2000) Data Encryption using DES/Triple-DES Functionality от Spartan-II FPGAs. [XILINX] [https://www.slideshare.net/bekicotngamuk/data-encryption-standard-40727964] (In Eng.).

[2] Rodionov A.Y. (2014) Efficient Hardware Implementation of the GOST R 34.10-2001, GOST R 34.10-2012 by FPGA [O sozdanii effektivnoy apparatnoy realizacii GOST R3410-2001, GOST R 34.10-2012 na osnove PLIS] [RusKripto 2014] [http://docplayer.ru/45820534-O-sozdanii-effektivnoy-apparatnoy-realizacii-gost-r-gost-r-na-osnove-plis-rodionov-a-yu-ruskripto-2014.html] (In Rus.).

[3] Qasem Abu Al-Haija, Mahmoud Smadi, Monther Al-Ja'fari and Abdullah Al-Shua'ibi. (2014) Efficient FPGA Implementation of RSA Coprocessor Using Scalable Modules. Procedia Computer Science 34 (2014), P. 647-654. DOI: 10.1016/j.procs.2014.07.092 (In Eng.).

[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] 5 (2014): 88-93. ISSN 1991-349421. DOI 10.32014/2018.2518-1467 (In Rus.).

[5] 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.).

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

[7] 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 otkryityim klyuchom i ih realizatsiya v mikroprotsessore «Elbrus»] [http://www.myshared.ru/slide/213088] (In Rus.).

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

[9] 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.).

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

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

[12] 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.).

[13] Aitkhozhayeva E.Zh., Tynymbayev S.T. (2016) The remainder generator by an arbitrary modulus of the number [Formirovatel ostatka po proizvolnomu modulyu ot chisla]. Patent of the RK. No. 30983 (In Rus.).

[14] Tynymbayev S.T., Aitkhozhayeva E.Zh., Adilbekyzy S. (2018) High speed device for modular reduction [Ustrojstvo 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.).

С. Т. Тынымбаев[1], Е. Ж. Айтхожаева[2], С. Әділбекқызы[3]

[1]Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан,
[2]Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан,
[3]Universiti Tenaga Nasional (UNITEN), Kajang, Selangor, Malaysia

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.

С. Т. Тынымбаев[1], Е. Ж. Айтхожаева[2], С. Әділбекқызы[3]

[1]Институт информационных и вычислительных технологий, Алматы, Казахстан,
[2]Казахский национальный исследовательский технический университет им. К. И. Сатпаева, Алматы, Казахстан,
[3]Universiti Tenaga Nasional (UNITEN), Kajang, Selangor, Malaysia

БЫСТРОДЕЙСТВУЮЩЕЕ УСТРОЙСТВО ДЛЯ ПРИВЕДЕНИЯ ЧИСЕЛ ПО МОДУЛЮ

Аннотация. Аппаратная реализация криптосистем позволяет повысить их быстродействие. Но низкое быстродействием ассиметричных криптосистем ограничивает их применение. Самым используемым асимметричным криптоалгоритмом является алгоритм шифрования RSA. Приведение по модулю является критичной по времени операцией, замедляющей реализацию алгоритма RSA. Предлагается структура устройства быстрого приведения по модулю, в котором используется модифицированный метод деления со сдвигом остатков на два разряда влево. Это позволяет ускорить получение остатка в два раза.

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

Information about authors:

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

Aitkhozhayeva Yevgeniya – associated professor of the Department of Information Security, 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

Adilbekkyzy Sairan – master's dergree student Universiti Tenaga Nasional, Kajang, Selangor, Malaysia, Almaty, Kazakhstan; sairan.02.95@mail.ru; https://orcid.org/0000-0002-3929-7070

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/ru/

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

Подписано в печать 29.11.2018.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
16,5 п.л. Тираж 500. Заказ 6.