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

4

JULY – AUGUST 2020

ALMATY, NAS RK

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 CitationIndex, 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 Ақпарат және коммуникациялар министрлігінің Ақпарат комитетінде 12.02.2018 ж. берілген **№ 16895-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: «NurNaz GRACE», Алматы қ., Рысқұлов көш., 103.

«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 Министерства информации и коммуникаций и Республики Казахстан **№ 16895-Ж**, выданное 12.02.2018 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.
http://www.bulletin-science.kz/index.php/en/

Адрес типографии: «NurNazGRACE», г. Алматы, ул. Рыскулова, 103.

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 periodical printed publication in the Committee of information of the Ministry of Information and Communications of the Republic of Kazakhstan No. **16895-Ж**, issued on 12.02.2018.

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

Address of printing house: «NurNaz GRACE», 103, Ryskulov str, Almaty.

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ISSN 1991-3494

Volume 4, Number 386 (2020), 13 – 20 **https://doi.org/10.32014/2020.2518-1467.98**

UDC 004.056
IRSTI 81.93.29

**M. Kalimoldayev[1], S. Tynymbayev[2], M. Ibraimov[3],
M. Magzom[1], Y. Kozhagulov[3], T. Namazbayev[3]**

[1]Institute of Information and computational technologies, Almaty, Kazakhstan;
[2]Almaty University of Power Engineering and Telecommunication, Almaty, Kazakhstan;
[3]Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: mnk@ipic.kz, s.tynym@mail.ru, margulan.ibraimov@kaznu.kz,
magzomxzn@gmail.com, kazgu.kz@gmail.com, tirnagog@mail.ru

PIPELINE MULTIPLIER OF POLYNOMIALS MODULO WITH ANALYSIS OF HIGH-ORDER BITS OF THE MULTIPLIER

Abstract. Among public-key cryptosystems, cryptosystems built on the basis of a polynomial system of residual classes are special. Because in these systems, arithmetic operations are performed at high speed. There are many algorithms for encrypting and decrypting data presented in the form of polynomials. The paper considers data encryption based on the multiplication of polynomials modulo irreducible polynomials. In such a multiplier, the binary image of a multiply polynomial can serve as a fragment of encrypted text. The binary image of the multiplier polynomial is the secret key and the binary representation of the irreducible polynomial is the module.

Existing sequential polynomial multipliers and single-cycle matrix polynomial multipliers modulo do not provide the speed required by the encryption block. The paper considers the possibility of multiplying polynomials modulo on a Pipeline in which architectural techniques are laid in order to increase computing performance.

In the conclusion of the work, the time gain of the multiplication modulo is shown by the example of the multiplication of five triples of polynomials. Verilog language was used to describe the scheme of the Pipeline multiplier. Used FPGA Artix-7 from Xilinx companies.

The developed Pipeline multiplier can be used for cryptosystems based on a polynomial system of residual classes, which can be implemented in hardware or software.

Key words: Polynomial system of remainder classes, irreducible polynomials, remainder former, Pipeline modular multiplier.

Introduction. There are two approaches to multiplying polynomials modulo. At the first approach, multiplying modulo in two stages is performed [1, 2]. At the first stage, polynomials are multiplied, at the second stage, polynomials multiple by irreducible polynomials modulo. If at the first stage of multiplication polynomials are possible to accelerate on matrix circuits, then the accelerated of them multiplying modulo is difficult. At the second approach, process of multiplying modulo is divided into steps, and at each step of the multiplication polynomials is combined with the operation of reduction irreducible polynomials modulo. While, of multiplying polynomials are performed on a sequential circuit starting with the analysis of high-order [3] or left-most [4] bits of the polynomial multiplier.

To improve performance, one-clock multipliers of polynomials modulo with a matrix structure were developed [5-7].

The matrix structures of parallel multipliers have the potential improving performance - the possibility of pipelining, which is a prospective architectural technique [8].

Main part. During pipelining, the multiplying operation is divided into a finite number of sub-operations, and each sub-operation is performed at its own Pipeline stage, with all Pipeline stages are working of parallel. The results obtained at the *i*-th stage are transferred for further processing to the (*i*+1)-th Pipeline stage. Transmit of information from stage to stage is through the buffer memory located between them.

A stage that have accomplished of its sub-operation remember the result in the buffer memory and can start processing the next portion of the sub-operation data, while the next Pipeline stage uses the data stored in the buffer memory located at its output. Synchronization of the Pipeline is provided by clock pulses, the period of which is determined by the slowest Pipeline stage and the delay in the buffer memory element.

In a Pipeline multiplier of N stages, the multiplying data modulo can be input with an interval of N times less than for a matrix multiplier. Output results appear at the same pace.

A diagram of an N-stage of the Pipeline for multiplying a polynomial-multiplicand A(x) by a polynomial-multiplier B(x) modulo an irreducible polynomial P(x) shown in figure 1.

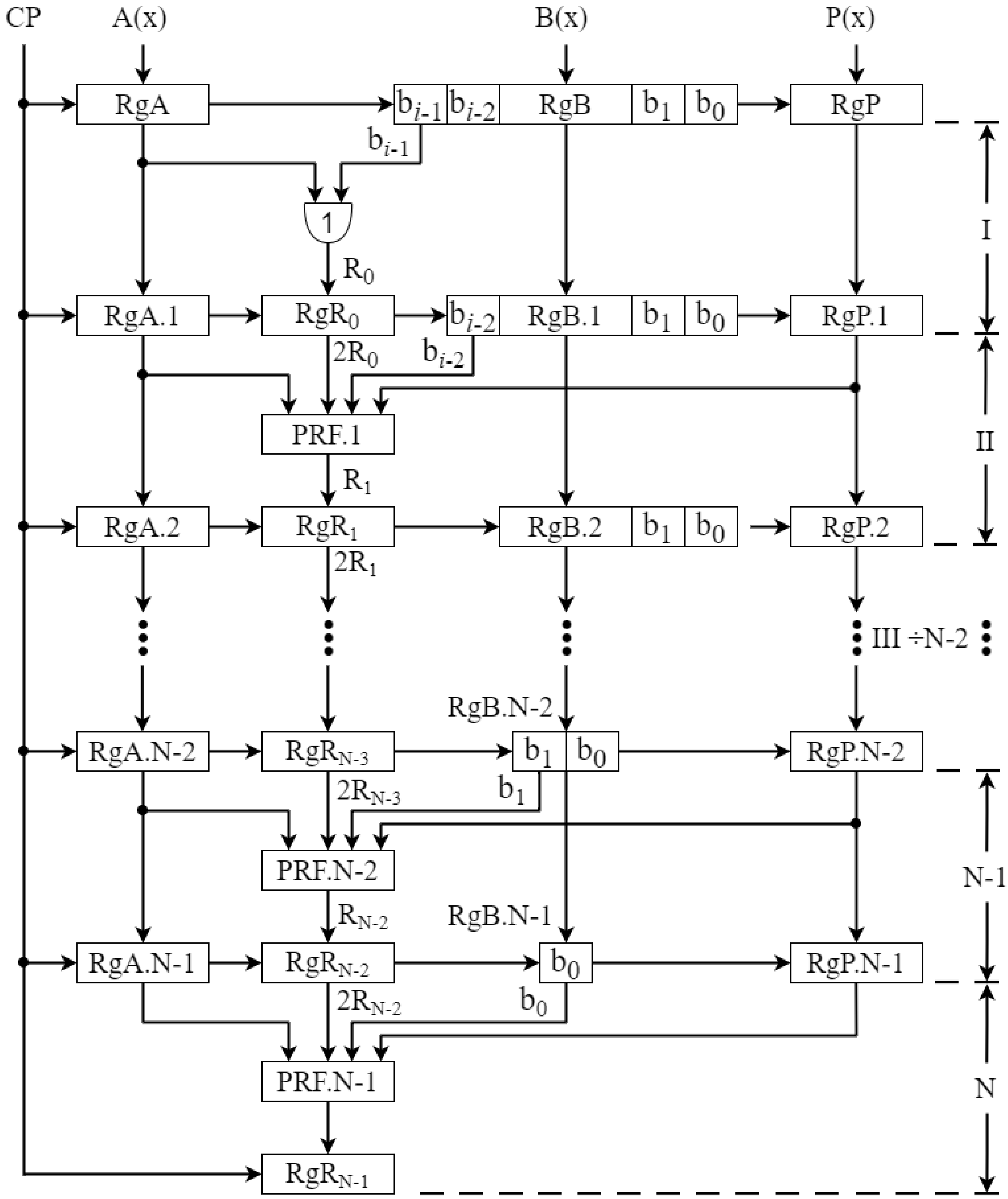


Figure 1 – Pipeline multiplier of polynomials modulo starting with analysis of high-order bit of the multiplier

The first Pipeline stage contains logical block diagram AND1 and buffer registers RgA.1, RgR_0, RgB.1and RgP.1. The second and next Pipeline stages contain logical blocks-former of partial remainders ($PRF_N \div PRF_{N-1}$). The second and other Pipeline stages have individual buffer registers. For example, the buffer registers of the second Pipeline stage are the registers RgA.2, RgR_1, RgB.2 and RgP.2. The buffer register of the N-stage is the Rg.N-1 register, in this diagram the registers RgA, RgB and RgP are the input Pipeline registers, where before the start of operations on the next triples of polynomials $A(x)_i$, $b(x)_i$ and $P(x)_i$, the *i*-th triple of polynomials is accepted.

Upon the first clock pulse CP1 is provided, the first triple of polynomials A, B, P from the input registers are transferred to the first stage of buffer registers. In the process this transfer, the contents input register RgA logical are multiplied by the high-order bit b_{i-1} polynomial-multiplier $B_1(x)$. The result of operations $A_1(x)\&b_{i-1}=R_0$ written to the first stage of buffer register RgR_0, and $A_1(x)$, $P_1(x)$ are accepted in the RgA.1 and RgP.1 registers.

According to the clock signal CP1, the second triple of polynomials A2(x), B2(x) and P2(x) are received to place of the first triples $A_1(x)$, $B_1(x)$ and $P_1(x)$ in the input registers. Upon the signal CP2 is provided, the contents of the input registers are transferred to the first stage of buffer registers, the contents of the first stage are transferred to the second stage of buffer registers RgA.2, RgR_1, RgB.2 and RgP.2. While, in the first Pipeline stage operation $A_2(x)\ \&b_{i-1} = R_0$ is performed, reaches in RgR register. The buffer registers RgA.1, RgP.1 will receive the corresponding contents of RgA (A_2) and RgP (P_2).

During the action of the second pulse of CP2 in PRF.1, the operation and the calculation of the remainder $R_1 = (2R_0 \oplus A_1\&b_{i-2}) \bmod P_1$ saved in the buffer register RgR_1 are performed.

The clock signal CP2 into the input registers receives the polynomials of the third triples of polynomials $A_3(x)$, $B_3(x)$ and $P_3(x)$. Upon the third clock signal CP3 is provided, the third triples of polynomials $A_3(x)$, $B_3(x)$ and $P_3(x)$, will be processed by the logical blocks of the first stage (AND1), the second triples of polynomials $A_2(x)$, $B_2(x)$, and $P_2(x)$, will be processed by the logical blocks of the second stage PRF.1, the logic blocks of the third stage PRF.2 will process the first triples of polynomials $A_1(x)$, $B_1(x)$ and $P_1(x)$.

Upon the N-clock pulse CP.N is provided, the contents of the input registers polynomials $A_N(x)$, $B_N(x)$ and $P_N(x)$ will reaches to the first stage buffer registers, the contents of the first stage buffer registers to the second stage buffer registers, etc.

The results of processing the polynomials $A_1(x)$, $B_1(x)$ and $P_1(x)$ from the N-1 stage buffer registers will moved to the N-stage buffer register – Rg.N-1, while in PRF.N-1 $R_{N-1} = [(2R_{N-1} \oplus A_1(x)\&b_0)]\mathit{mod}P_1$ is calculated, which is the result of multiplying modulo $[A_1(x)*B_1(x)]\mathit{mod}P_1(x)$. The input registers receive the triples of polynomials $A_{N+1}(x)$, $B_{N+1}(x)$ and $P_{N+1}(x)$ with a clock signal CP.N.

Upon the clock pulses N+1, N+2, N+3, etc. is provided on the output Pipeline register Rg.N-1, the results of multiplying of triples of polynomials will be formed:

$$\begin{aligned} R_{N-1} &= [A_{N+1}(X) * B_{N+1}(X)] \bmod P_{N+1} \\ R_{N-1} &= [A_{N+2}(X) * B_{N+2}(X)] \bmod P_{N+2} \\ &\vdots \\ R_{N-1} &= [A_{N+k}(X) * B_{N+k}(X)] \bmod P_{N+k} \end{aligned}$$

The results of the sum modulo of two $2R_{i-1} \oplus A(x)b_i$ is provided to the left inputs is performed by the adder modulo of two Add.1. The value of P (x) is provided to the right inputs of Add.2. If, at the same time $C = 2R_{i-1} \oplus A(x)b_i > P(x)$ then in the high-order bit of the sum C the value $C_h = 1$ is formed. With this signal, block of diagram AND3, the result of adding $C \oplus P(x)$ at the output of Add.2 forming R_i is output. If $C = 2R_{i-1} \oplus A(x)b_i < P(x)$, $C_h = 0$. Then the value $C = 2R_{i-1} \oplus A(x)b_i$ by the signal $C_h = 1$ by the block of diagram AND2 the output is $C = R_i$.

Figure 2 shows the structure of the PRF_i. The central adder modulo 2 is the Add.2 adder.

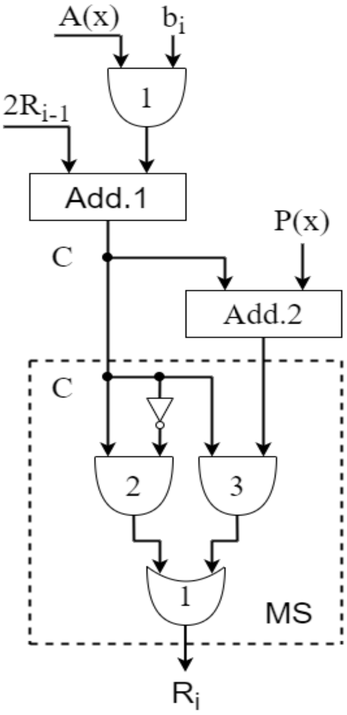
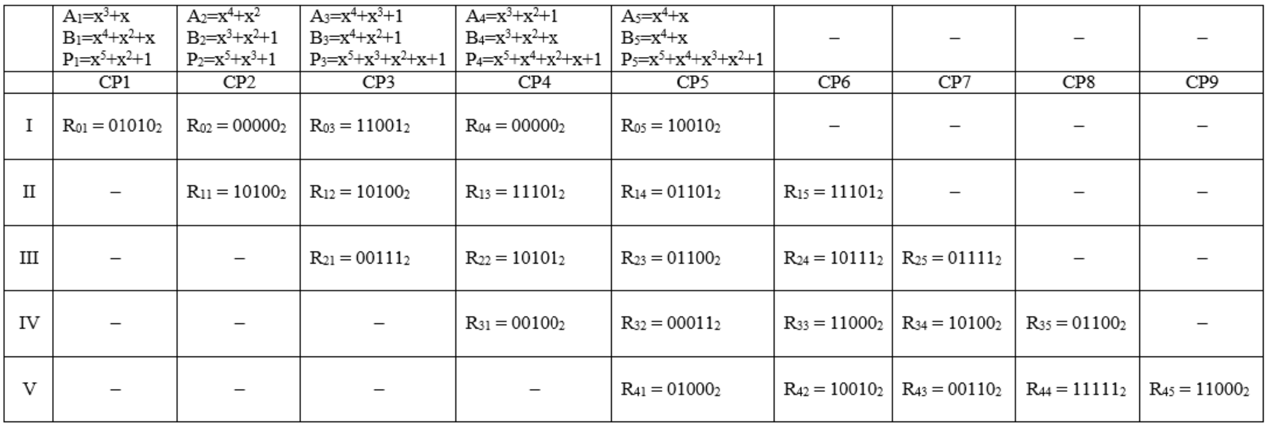


Figure 2 – PRF*i* structure

Consider the example of multiplying polynomials modulo on a five-stage Pipeline. Let:

$A_1 = x^3+x = 01010_2$; $B_1 = x^4+x^2+x = 10110_2$; $P_1 = x^5+x^2+1 = 100101_2$;
$A_2 = x^4+x^2 = 10100_2$; $B_2 = x^3+x^2+1 = 01101_2$; $P_2 = x^5+x^3+1 = 101001_2$;
$A_3 = x^4 + x^3 + 1 = 11001_2$; $B_3 = x^4 + x^2 + 1 = 10101_2$; $P_3 = x^5+x^3+x^2+x+1 = 101111_2$;
$A_4 = x^3 + x^2 + 1 = 01101_2$; $B_4 = x^3 + x^2 + x = 01110_2$; $P_4 = x^5 + x^4 + x^2 + x + 1 = 110111_2$;
$A_5 = x^4 + x = 10010_2$; $B_5 = x^4 + x = 10010_2$; $P_5 = x^5 + x^4 + x^3 + x^2 + 1 = 111101_2$.

The results of multiplying polynomials $A_1(x) \div A_5(x)$ by $B_1(x) \div B_5(x)$ modulo $P_1(x) \div P_5(x)$ are shown in figure 3.



	$A_1=x^3+x$ $B_1=x^4+x^2+x$ $P_1=x^5+x^2+1$	$A_2=x^4+x^2$ $B_2=x^3+x^2+1$ $P_2=x^5+x^3+1$	$A_3=x^4+x^3+1$ $B_3=x^4+x^2+1$ $P_3=x^5+x^3+x^2+x+1$	$A_4=x^3+x^2+1$ $B_4=x^3+x^2+x$ $P_4=x^5+x^4+x^2+x+1$	$A_5=x^4+x$ $B_5=x^4+x$ $P_5=x^5+x^4+x^3+x^2+1$	–	–	–	–
	CP1	CP2	CP3	CP4	CP5	CP6	CP7	CP8	CP9
I	$R_{01} = 01010_2$	$R_{02} = 00000_2$	$R_{03} = 11001_2$	$R_{04} = 00000_2$	$R_{05} = 10010_2$	–	–	–	–
II	–	$R_{11} = 10100_2$	$R_{12} = 10100_2$	$R_{13} = 11101_2$	$R_{14} = 01101_2$	$R_{15} = 11101_2$	–	–	–
III	–	–	$R_{21} = 00111_2$	$R_{22} = 10101_2$	$R_{23} = 01100_2$	$R_{24} = 10111_2$	$R_{25} = 01111_2$	–	–
IV	–	–	–	$R_{31} = 00100_2$	$R_{32} = 00011_2$	$R_{33} = 11000_2$	$R_{34} = 10100_2$	$R_{35} = 01100_2$	–
V	–	–	–	–	$R_{41} = 01000_2$	$R_{42} = 10010_2$	$R_{43} = 00110_2$	$R_{44} = 11111_2$	$R_{45} = 11000_2$

Figure 3 – The results of multiplying polynomials $A_1(x) \div A_5(x)$ by $B_1(x) \div B_5(x)$ modulo $P_1(x) \div P_5(x)$

From this figure 3

$R_{41} = [A_1(x) \cdot B_1(x)]$ *mod* $P_1 = 01000_2$, is corresponds to a polynomial: $R_{41} = x^3$;
$R_{42} = [A_2(x) \cdot B_2(x)]$ *mod* $P_2 = 10010_2$, is corresponds to a polynomial: $R_{42} = x^4 + x$;
$R_{43} = [A_3(x) \cdot B_3(x)]$ *mod* $P_3 = 00110_2 = x^2 + x$;
$R_{44} = [A_4(x) \cdot B_4(x)]$ *mod* $P_4 = 11111_2 = x^4 + x^3 + x^2 + x + 1$;
$R_{45} = [A_5(x) \cdot B_5(x)]$ *mod* $P_5 = 11000_2 = x^4 + x^3$.

In this figure 3, R_{ij} are the numbers of intermediate remainders $i(i = 0 \div 4)$ and the numbers of triples of numbers j, where $j = 1 \div 5$.Consider the time value. The multiplying time of polynomials without a Pipeline is determined by the formula:

$$T_{w.c} = NKT_K\,,$$

where K – the number of triples of polynomials to be multiplying, N – The number of Pipeline stages, T_K – the duration of the clock period, which is determined by the ratio $T_K = T_{PRF} + T_{BRg}$, where T_{PRF} – partial remainder formation time, T_{BRg} – time of recording of the processing results to buffer registers.

The runtime of operations on K input polynomial streams (triples of polynomials) at N Pipeline stages or with a clock period T_K is determined by the ratio [9]:

$$T_{NK} = (N + (K-1))T_K\,.$$

The time value is determined by the formula:

$$C = (NK - (N + K - 1))T_K\,.$$

For our example,

$$C = (NK - (N + K - 1))T_K = (25 - 9)T_K = 16T_K\,.$$

The timing diagram and the results of the multiplying modulo the above triples of numbers on a five-stage Pipeline are shows in figure 4. Verilog HDL is used to describe the circuit of the Pipeline multiplier. Artix-7 from Xilinx as the Field Programmable Gate Array (FPGA) was chosen.

As shown in the figure 4, the first triple of polynomials $A_1(x)$, $B_1(x)$, $P_1(x)$ from the Pipeline input registers to the buffer registers of the first stage with the first clock signal CP1 are transferred. In this case, the partial remainder $R_{01} = 01010_2$ is calculated by the logical block of the first stage.

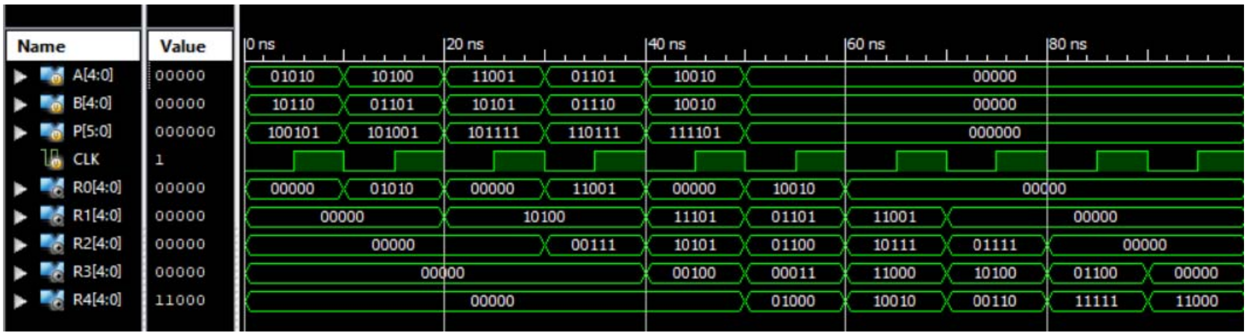


Figure 4 – The timing diagram of the Pipeline circuit

During the action of the second clock signal CP2, the second triple of polynomials $A_2(x)$, $B_2(x)$, $P_2(x)$ from the Pipeline input registers are transferred to the first stage buffer register, the contents of the first stage buffer registers are transferred to the second stage buffer registers. In this case, at the first stage $R_{02} = 00000_2$, at the second stage of the Pipeline, the remainder $R_{11} = 10100_2$ is calculated.

Upon the third clock pulse CP3 is provided from the Pipeline input registers, the triple of polynomials $A_3(x)$, $B_3(x)$, $P_3(x)$ are transferred to the first stage buffer registers, the contents of the first stage buffer registers are transferred to the second stage buffer registers, also the contents of the second stage buffer registers are transferred to the third stage buffer registers. While, a partial remainder $R_{03} = 11001_2$ is formed in the first stage of the Pipeline, $R_{12} = 10100_2$ and $R_{21} = 00111_2$ respectively are formed in the second and third stages of the Pipeline.

After the fourth clock pulse CP4 is provided, triple of polynomials $A_4(x)$, $B_4(x)$, $P_4(x)$ enter the inputs of the first stage of the Pipeline, the partial remainder $R_{04} = 00000_2$ is calculated of the first stage of the Pipeline, the remaining residues $R_{13} = 11101_2$, $R_{22} = 10101_2$, $R_{31} = 00100_2$ are formed on the other three stages.

Upon the fifth pulse CP5 is provided, triple of polynomials $A_5(x)$, $B_5(x)$, $P_5(x)$ enter the inputs of the first stage of the Pipeline, and at the first, second, third and fourth stages partial remainders $R_{05} = 10010_2$, $R_{14} = 01101_2$, $R_{23} = 01100_2$, $R_{32} = 00011_2$, $R_{41} = 01000_2$ are formed.

Upon the sixth pulse CP6 is provided to the inputs of the first stage of the Pipeline, polynomials are not provided and the remainders $R_{15} = 11101_2$, $R_{24} = 10111_2$, $R_{33} = 11000_2$, $R_{42} = 10010_2$ are formed on the corresponding 2, 3, 4, 5 stages of the Pipeline.

After the seventh pulse CP7 is provided the remainders $R_{25} = 01111_2$, $R_{34} = 10100_2$, $R_{43} = 00110_2$ in the 3, 4, 5 stages of the Pipeline are calculated.

The eighth clock pulse CP8 the remainders $R_{35} = 01100_2$, $R_{44} = 11111_2$ in stages 4, 5 are formed.

The ninth clock pulse CP9 completes the work of the Pipeline and in the fifth stages of the Pipeline the remainder R_{45} is calculated, which is the result $R_{45} = [A_5(x) * B_5(x)] \bmod P_5(x)$.

Conclusion. Considered pipeline scheme and calculation examples show that pipeline allows you to process a stream of three polynomials increasing the data encryption performance, which allows you to build a high-performance cipher process.

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

М. Н. Калимолдаев[1], С. Тынымбаев[2], М. К. Ибраимов[3],
М. М. Мағзом[1], Е. Т. Кожагулов[3], Т. А. Намазбаев[3]

[1]Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан;
[2]Алматы энергетика және байланыс университеті, Алматы, Қазақстан;
[3]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

КӨБЕЙТКІШТІҢ ЖОҒАРҒЫ РАЗРЯДТАРЫН ТАЛДАУ НЕГІЗІНДЕ ПОЛИНОМДАРДЫҢ МОДУЛЬ БОЙЫНША КОНВЕЙЕРЛІ КӨБЕЙТУ ҚҰРЫЛҒЫСЫ

Аннотация. Ашық кілтті криптожүйе ішінде қалдықтар жүйесінің көпмүшелік негізінде құрылған криптожүйелерінің алатын орны бөлек. Өйткені мұндай жүйеде арифметикалық амалдар жоғары жылдамдықпен орындалады. Көпмүшелік түрінде берілген мәліметтерді шифрлаудың тиімді тәсілі ретінде полиномдарды модульмен көбейту амалын алуға болады. Мұндай тәсілде көбейгіш ретінде шифрланатын мәтіннің белгілі бір фрагменті болып саналатын көпмүшеліктің екілік бейнесі алынса, ал көбейткіш ретінде құпия кілт болып табылатын көпмүшеліктің екілік бейнесі алынады. Модуль ретінде көбейтілетің көпмүшеліктің келтірілмейтін көпмүшеліктерінің бірі таңдалады.

Полиномдарды модульмен көбейтетін құрылғылардың ішінен жылдамдығы жоғары болып келетін матрицалық көбейту құрылғыларын атауға болады. Бірақ мұндай құрылғылардың өзі шифрлау жылдамдығын күрт өсіре алмайды. Шифрлау жылдамдығын арттыру үшін статьяда полиномдарды модульмен көбейтетін конвейер сұлбасының құрамы, логикалық құрылғылары, олардың ішкі ақпараттық байланыстары қаралады. Үштік полиномдар тізбегін конвейерде өңдеу ретіне мысалдар көрсетілген.

Жұмыстың қорытындысында бес сатылы конвейер арқылы полиномдардың бес үштігін (көбейгіш, көбейткіш, модуль) модульмен көбейтетін конвейер сұлбасының программаланатын логикалық интегралдық сұлбада (ПЛИС) Verilog тілінде іске қосылу жағдайы қарастырылды. Конвейер жұмысының уақыт диаграммасы мен модульмен көбейту нәтижелері келтірілген. ПЛИС ретінде Xilinx фирмалық өнімі Artix-7 таңдап алынған.

Алынған конвейер сұлбасы қалдықтар жүйесінің көпмүшелік негізінде құрылған криптожүйеде жылдамдығы жоғары шифрлау блогын құру үшін қолдануға болады.

Түйін сөздер: қалдық кластарының полиномдық жүйесі, келтірілмейтің полиномдар, қалдық құрастырушы, модуль бойынша конвейерлі көбейту құрылғысы.

**М. Н. Калимолдаев[1], С. Тынымбаев[2], М. К. Ибраимов[3],
М. М. Мағзом[1], Е. Т. Кожагулов[3], Т. А. Намазбаев[3]**

[1]Институт информационных и вычислительных технологий, Алматы, Казахстан;
[2]Алматинский университет энергетики и связи, Алматы, Казахстан;
[3]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан

КОНВЕЙЕРНЫЙ УМНОЖИТЕЛЬ ПОЛИНОМОВ ПО МОДУЛЮ С АНАЛИЗОМ СТАРШИХ РАЗРЯДОВ МНОЖИТЕЛЯ

Аннотация. Среди криптосистем с открытым ключом особое место занимают криптосистемы, построенные на базе полиномиальной системы остаточных классов. Потому что в таких системах арифметические операции выполняются с высокой скоростью. Существует множество алгоритмов шифрования и расшифрования данных, представленных в виде многочленов. В работе рассматривается шифрование данных, основанных на умножении полиномов по модулю неприводимых полиномов. В таком умножителе двоичное изображение полинома-множимого может служить фрагментом шифруемого текста, двоичное изображение полинома-множителя является секретным ключом, а двоичное представление неприводимого полинома –модулем.

Существующие умножители полиномов последовательного действия и однотактные матричные умножители полиномов по модулю не обеспечивают ту скорость, которая требуется от блока шифрования. В работе рассматривается возможность умножения полиномов по модулю на конвейере, в котором заложены архитектурные приемы для повышения производительности вычисления.

В заключении работы приведен выигрыш по времени умножения по модулю на примере умножения пяти троек полиномов. Для описания схемы конвейерного умножителя был использован язык Verilog. В качестве ПЛИС выбран Artix-7 от компании Xilinx.

Разработанный конвейерный умножитель может быть использован для криптосистем на базе полиномиальной системы остаточных классов, которые могут быть реализованы программно-аппаратным или аппаратным способами.

Ключевые слова: полиномиальная система остаточных классов, неприводимые полиномы, формирователь остатков, конвейерный умножитель по модулю.

Information about authors:

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

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

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

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

Kozhagulov Yeldos, Lead researcher, PhD, Lecturer of Department of Physics and Technology, al-Farabi Kazakh national university, Almaty, Kazakhstan; kazgu.kz@gmail.com; https://orcid.org/0000-0001-5714-832X

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, e-mail: tirnagog@mail.ru; https://orcid.org/0000-0002-2389-2262

REFERENCES

[1] Magzom M. Development and research of cryptosystems for information security in decentralized networks. PhD Dissertation [Razrabotka i issledovanie kriptosistem zashchity informatsii v detsentralizovannykh setiakh. PhD Dissertation]. Almaty, 2017 (in Russ.).

[2] Tynymbayev S., Kapalova N. Polynomial multipliers on the module of irreducible polynomials sequential action [Umnozhitel' polinomov po moduliu neprivodimykh polinomov posledovatel'nogo deistviia]. Materials of the 2nd international scientific-practical conference “Informatics and applied mathematics”. Almaty 2017 (in Russ.).

[3] Kalimoldayev M., Tynymbaev S., Magzom M., Ibraimov M., Khokhlov S., Sydorenko V. Polynomials Multiplier under Irreducible Polynomial Module for High-Performance Cryptographic Hardware Tools. Proc. Of 15th International Conference on ICT in Education, Research and Industrial Applications // Integration, Harmonization and Knowledge Transfer. Kherson, Ukraine, June 12-15, 2019. P. 729-757.

[4] Kalimoldayev M., Tynymbayev S., Kapalova N. Polynomial multipliers on the module of irreducible polynomials // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. Vol. 4, N 368 (2017). P. 48-53.

[5] Kalimoldayev M., Tynymbayev S., Gnatyuk S., Ibraimov M., Magzom M. The device for multiplying polynomials modulo an irreducible polynomial // News of The National Academy of Sciences of the Republic of Kazakhstan Series of Geology and Technical Sciences. Vol. 2, N 434 (2019). P. 199-205. DOI: 10.32014/2019.2518-170X.55

[6] Kalimoldayev M., Tynymbayev S., Gnatyuk S., Khokhlov S., Magzom M., Kozhagulov Y. Matrix multiplier of polynomials modulo analysis starting with the lower order digits of the multiplier // News of The National Academy of Sciences of the Republic of Kazakhstan Series of Geology and Technical Sciences. Vol. 4, Issue 436 (2019). P. 181-187. DOI: 10.32014/2019.2518-170X.113

[7] Tynymbayev S., Berdibayev R., Omar T., Gnatyuk S., Namazbayev T., Adilbekkyzy S. Devices for multiplying modulo numbers with analysis of the lower bits of the multiplier // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. Vol. 4, N 380 (2019). P. 38-45. DOI: 10.32014/2019.2518-1467.90.

[8] Tsil'ker B.Ia., & Orlov S.A. (2011) Organization of computers and systems: A textbook for high schools [Organizatsiia EVM i sistem: Uchebnik dlia vuzov]. SPb.: Piter, 2011. 688 p. (in Russ.).

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, Д. С. Аленов, А. Ахметова*
Верстка на компьютере *Д. А. Абдрахимовой*

Подписано в печать 14.08.2020.
Формат 60х881/8. Бумага офсетная. Печать – ризограф.
21,6 п.л. Тираж 500. Заказ 4.

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