N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
SERIES OF GEOLOGY AND TECHNICAL SCIENCES
ISSN 2224-5278
Volume 3, Number 441 (2020), 102 – 109 **https://doi.org/10.32014/2020.2518-170X.60**

UDC 004.056
IRSTI 81.93.29

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

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

THE DEVICE FOR MULTIPLYING POLYNOMIALS MODULO WITH ANALYSIS OF TWO LEAST SIGNIFICANT BITS OF THE MULTIPLIER PER STEP

Abstract. We consider a device for multiplying polynomials modulo where two bits of the polynomial multiplier are analyzed per multiplication step. Such a device can serve as the basic unit for building cryptosystems based on non-positional polynomial number systems, where the binary representation of the polynomial multiplicand can show a fragment of the encrypted text, and the binary representation of the polynomial multiplier can serve as a secret key. The module is a binary representation of the irreducible polynomial of these two polynomials.

Key words: cryptosystem based on a polynomial number system, irreducible polynomials, polynomial multiplier modulo irreducible polynomials, remainders.

Introduction. Modern computing devices mainly operate in a positional number system. In such devices, when performing arithmetic operations on multi-bit numbers, it becomes necessary to take into account inter-bit transfers, which significantly slows down the calculation speed and complicates the structure of the computer.

In order to significantly improve the performance of computing devices, it is necessary to use number systems devoid of the disadvantages of a positional number system. Today, such a number system is the so-called "non-positional number systems", one of which is the "system of residual classes (RNS)" [1]. The use of RNS is an effective way of performing with a large discharge data. In particular, the use of RNS allows increasing the speed of the operation due to the lack of transfer. These features provide significant advantages of the RNS over the positional number system when performing modular operations of addition, subtraction and multiplication. This is especially true if multi-bit numbers act as operands. In this case, the multi-bit number is grouped into smaller blocks and each block is processed in parallel, which leads to faster execution of operations on the multi-bit number.

In Kazakhstan, the The Institute of Information and Computational Technologies (of the Ministry of Education and Science of the Republic of Kazakhstan conducts research and implementations of cryptographic information protection algorithms based on the non-positional polynomial number system (NPNS) [2–5]. In particular, algorithms for block symmetric data encryption based on the NPNS were developed and implemented. Of particular interest are the hardware-software and hardware methods for implementing NPSS, which can significantly accelerate the process of encryption and decryption of data due to parallel processing at the level of individual modules and bits inside the module, and key generation allows for integrity.

The main hardware/software and hardware cryptosystems are polynomial multipliers modulo irreducible polynomials, where routine calculations are performed to encrypt and decrypt data. In [6–11], multipliers of polynomials modulo irreducible polynomials were considered, where at each step of multiplication, the least significant or most significant bit of the polynomial multiplier was analyzed.

In this paper, we consider a device for multiplying polynomials modulo with an analysis of two bits of a polynomial multiplier, which allows to accelerate the process of multiplication.

Main part. The functional diagram of the considered polynomial multiplier is shown in figure 1. The device includes:

a shift register RgB that shifts two bits in the direction of the least significant bit;

a register RgP for storing the module P(x);

partial remainder formers PRF1 and PRF2;

a register of partial remainders of the RgPR;

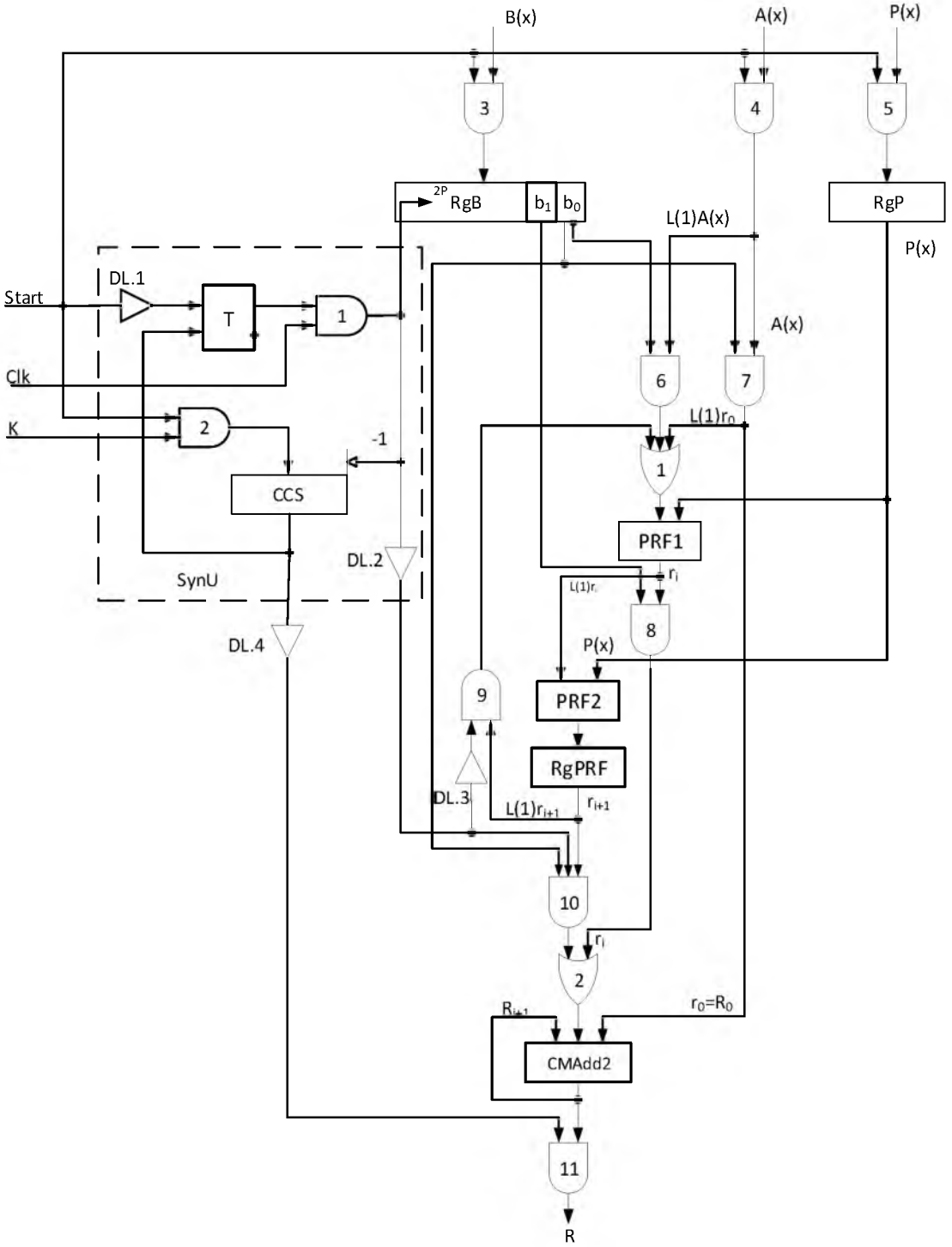

Figure 1 – The device for multiplying polynomials modulo with analysis of two bits of the polynomial multiplier per step

logical circuits And3 ÷ And11 gates;
logical circuits OR1 and OR2 gates;
delay lines DL.3, DL.4;
cumulative adder modulo two (CMAdd2);
a synchronization unit (SynU), which contains a flip-flop T, a counter of clock signals of the CCS, logical circuits And2 gates, delay lines DL.1 and DL.2.

The "Start" signal, the clock signals Clk, and the binary representation of the number of shifts K are fed to the SynU inputs. The polynomial of the multiplier B(x) is fed to the input of the RgB register through the block of circuits And3, the polynomial of the multiplicand A(x) through the block of circuits And4, and the irreducible polynomial P(x) is fed through a block of circuits And5.

Figure 2 shows the structure of the PRF, which consists of an modulo adder two and a multiplexer MS, containing blocks of circuits And1', And2' and OR', the inverter NOT of which is input to the most significant bit order bit (MS) of the doubled value of the remainder r_{i-1}. The inverter NOT output is connected to the control input of the block of circuits And2' and the control bit of the circuit block And1' is supplied with the most significant bit MS, the value of the doubled remainder $2r_{i-1}$, without inversions. The information inputs of the block of circuits And2'are supplied with the bits of the doubled remainder $2r_{i-1}$, and the information inputs of the block of circuits And1' are connected to the outputs of MAdd2.

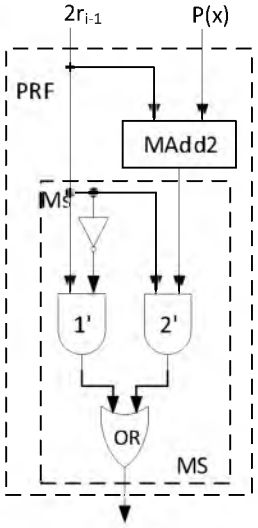

Figure 2 – Functional diagram of PRF

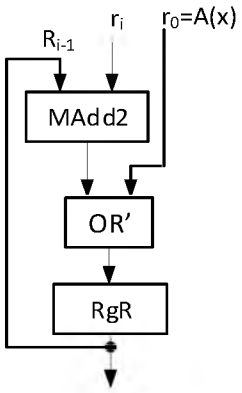

Figure 3 – Functional diagram CMAdd2

When M_S = 1 ($2r_{i-1}$>P(x)), the result of summing $2r_{i-1} \oplus P(x)$ is fed through And1'to the output of the block OR'. In this case, a partial remainder $r_i = 2r_{i-1} \bmod P(x) = 2r_{i-1} \oplus P(x)$ is formed. At M_S= 0 ($2r_{i-1}$ < P(x)), the value $2r_{i-1}$ is output through the blocks of And2' and OR'circuits, a partial remainder $r_i = 2r_{i-1}$ is formed.

The structure of the cumulative adder modulo two (CMAdd2) is shown in figure 3, which consists of an adder modulo two (MAdd2), an intermediate remainder register RgR, where the values $R_i = R_{i-1} \oplus r_i$ are stored. As well as the values r_0=A(x), which is formed by the "Start" level at b_0 = 1 (where b_0-bit of the binary representation of the polynomial multiplier B (x)).

The operation of the multiplication begins with the input to the input SynU signal "Start". By this signal, the polynomial multiplier B(x) is received in the RgB register through the And3 circuit block, and the binary representations of the polynomial-irreducible polynomial module P(x) are received into the RgP register through the And5 circuit block. The binary representations of the polynomial A(x) are received through the block of circuits And4. The "Start" signal also writes the binary representations of the number of shifts – K to the CCS. After receiving the binary representations of the polynomial B(x) in the least significant bits of the register RgB, the values of the representations b_1 and b_0 are fixed. The positive output of the flip-flop, where the value of the bits b_0 is fixed, is connected to the inputs of the blocks of circuits And7 and And10, and the inverse output of this flip-flop is connected to the input of the block of

circuits And6. The positive output of the flip-flop, where the value of bit b_1 is recorded, is connected to the inputs of the block of circuits And8. The value of the multiplicand A(x) with a shift by one bit in the direction of the most significant bits (L(1) A(x)) is fed to the inputs of the block of circuits And6 and without a shift, it is fed to the inputs of the block And7. With a value of $b_0 = 1$, the binary representations of the polynomial A(x) without a shift is fed to the input of the register RgR CMAdd2 and with a shift by one bit in the direction of the most significant bit, it is fed to the moves of the block of circuits OR1. The outputs of OR1 are connected to the first inputs of the PRF1, and to its second inputs are fed binary coefficients of the polynomial P(x). At the same time, the value of the first partial remainder r_1 is formed at the outputs of PRF1. With a value of $b_1 = 1$, the value of r1 is fed to the inputs of the CMAdd2 through the blocks of circuits And8 and OR23. At the same time, at the its outputs, the value of the intermediate remainder $R_1 = R_0 \oplus r_1$ is formed, which is stored in the register RgR.

In parallel with the formation of the intermediate remainder R_1, the value of the partial remainder r_1 with a shift by one bit in the direction of the most significant bit one is fed to the inputs of the PRF2. The value of the remainder r_2 is generated at the outputs of the PRF2, which is stored in the register RgPRF2. Since the time of formation and r_1 fixations in RgPRF2 is longer than the time of formation and fixations of the intermediate remainder R_1, the delay time on the DL.1 of the "Start" signal is determined by the total delay of PRF1, PRF2 and the registers RgB and RgPRF2. Thus, before the "Start" signal arrives at the input of the flip-flop T from the output DL.1, the partial remainder r_2 is fixed in the register RgPRF2, and the intermediate remainder R_1 is registered in the register RgR CMAdd2.

After the formation of r_2 and R_1, the "Start" signal from the output of DL.1 is fed to the input of flip-flop T and puts it in a single state, which allows the first clock signal Clk11 to go to output And1. Clk1 from the output of And1 is fed to the input of the RgB register and shifts it by two bits to the right, and in its lower bits the value of bits b_3 and b_2 of the polynomial B(x) is fixed. At the same time, the Clk1 decreases the value of the counter by one. Clk1, after a delay by the time of shifting the register RgB, the element DL.2 is fed to the input of the block of circuits And10. At $b_2 = 1$ the value r_2 from the outputs of RgPRF2is supplied through the blocks of circuits OR3 to the inputs of the circuit CMAdd2, where the value of the intermediate remainder $R_2 = R_1 \oplus r_2$ is calculated and it is stored in RgR CMAdd2.

At the same time, the partial remainder r_2 is shifted by one bit toward the higher one with the clock signal Clk1 through the block of circuits And9 with a delay for the time of writing R2 in RgR in DL.3 is fed to the inputs of the PRF1 through the block of circuits OR1. At the outputs of PRF1, a partial remainder $r_3 = 2r_2 mod P(x)$ is formed, which with a value of $b_3 = 1$ is fed through the blocks of circuits And8 and OR3 to the inputs of CMAdd2, where an intermediate remainder $R_3 = R_2 \oplus r_3$ is formed. During the formation of intermediate remainder R_3, the value of the remainder r_3 from the outputs of the PRF1 with a shift by one bit to the higher side is fed to the inputs of the PRF2 and the intermediate remainder forms the output of which $r_4 = 2r_3 mod P(x)$, which is stored in the register RgPRF2. Thus, before entering the next pulse of Clk2 in the circuit in the register RgPRF2 we have a partial remainder r_4, in the register RgR CMAdd2 the value of the intermediate remainder R_3.

Other remainders are similarly formed in RgR and RgPRF2. After the last clock signal is supplied to RgR, the final result $R_{\frac{N-1}{2}}$ is generated. At the same time, the CCS generates a signal "End of operations", which is delayed by the DL.4 elements for the time the remainder $r_{\frac{N-1}{2}}$ and $R_{\frac{N-1}{2}}$ are PRFs, we are able to increase the speed.

Consider the example of multiplication of polynomials modulo.

Let $A(x) = x^5+x^4+x+1$; $B(x) = x^5+x^3+x^2+1$; $P(x) = x^6+x+1$. Binary representations of these polynomials: $A = 110011_2$ $B=101101_2$ and $P=1000011_2$. The calculation results are given in table1.

To implement the device "for multiplying polynomials modulo with analysis of two bits of the polynomial multiplier per step" was used FPGAs from the company Xilinx, family Artix-7. Table 2 shows the total number of Artix 7 FPGAs (xc7a100t). The work of this device for polynomials with a power of m = 6 ÷ 12 was tested on it.

Figure 4 shows the timing diagram of the device for polynomials $A(x) = 110011_2$, $B(X) = 101101_2$ and $P(x) = 1000011_2$, which implement the operation R(x) = A(x)*B(x)mod P(x) with power m = 6. As can be seen from the timing diagram, the output data are the values of partial remainders (r_i, r_{i+1}) and

Table 1 – The sequence of operations

Clock signals	Start	Clk1	Clk2
b_i	b_1=0, b_0=1	b_2=1, b_3=1	b_5=1, b_4=0
PRF1	$r_0=b_0*A(x)=110011$; $r_1=2r_0 \bmod P(x)=$ 1100110 ⊕ 1000011 0100101 $r_1>P(x)$	$r_3=2r_2 \bmod P(x)=$ 0010010 ⊕ 1000011 0010010 $r_3<P(x)$	$r_5=2r_4 \bmod P(x)=$ 1001000 ⊕ 1000011 0001011 $r_5>P(x)$
PRF2 RgPRF2	$r_2=2r_1 \bmod P(x)=$ 1001010 ⊕ 1000011 0001001 $r_2>P(x)$	$r_4=2r_3 \bmod P(x)=$ 0100100 ⊕ 1000011 0100100 $r_4<P(x)$	$r_6=2r_5 \bmod P(x)=$ 0010110 ⊕ 1000011 0010110 $R_6<P(x)$
CMAdd2	$R_0=0⊕r_0=110011$ $R_1=R_0⊕(r_1*b_1)=$ 110011 ⊕ 000000 110011	$R_2=R_1⊕(r_2*b_2)=$ 001001 ⊕ 110011 111010 $R_3=R_2⊕(r_3*b_3)=$ 111010 ⊕ 010010 101000	$R_4=R_3⊕(r_4*b_4)=$ 101000 $R_5=R_4⊕(r_5*b_5)=$ 101000 ⊕ 001011 100011

Checking:

$(x^5+x^4+x+1)*(x^5+x^3+x^2+1)= x^{10}+x^9+x^8+x^2+x+1;$

$x^{10}+x^9+x^8+x^2+x+1 \;\big|\; x^6+x+1$

⊕

$x^{10}+x^5+x^4 \;\big|\; x^4+x^3+x^2$

$x^9+x^8+x^5+x^4+x^2+x+1$

⊕

$x^9+x^4+x^3$

$x^8+x^5+x^3+x^2+x+1$

⊕

$x^8+x^3+x^2$

x^5+x+1, which corresponds to 100011_2

Table 2 – Total number of Artix 7 FPGA resources (xc7a100t)

Resources	Number
LUT	63 400
FF	126 800

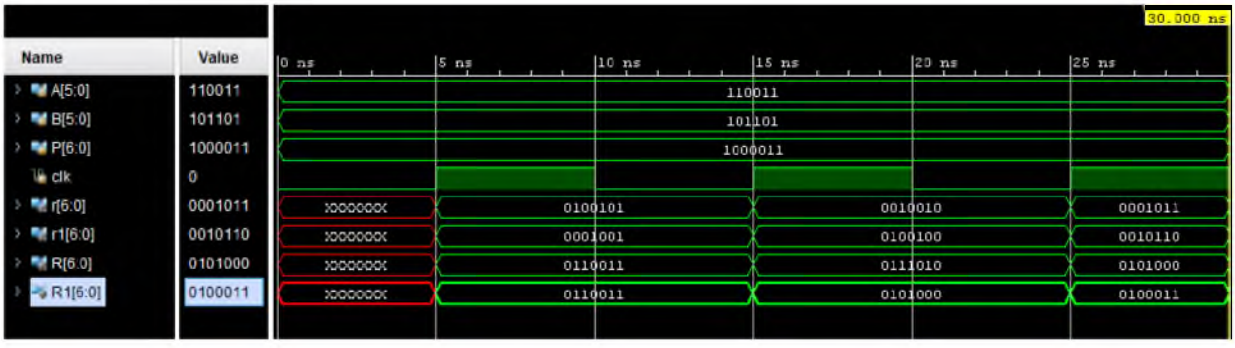

Figure 4 – Diagrams of the formation of intermediate remainders for polynomials with power m = 6

intermediate remainders (R_i, R_{i+1}). In this case, after applying the "Start" level, the value $r_0 = A(x)$ with the value $b_0 = 1$ through the block of circuits And7 is recorded in PrR CMAdd2 as $r_0=R_0=110011$. At the same time, the value of r0 with a shift by one bit to the left is fed to the input of PRF1 and r1 = 0100101 is formed at the output of PRF1. With a value of b1 = 1, the value r1 is fed to the input of CMAdd2, where the operation is performed then R1=R0⊕r1*b1)=110011. Then, at the same time, r1 with a shift by one bit to the left is fed to the input of PRF2 at the output of which an intermediate remainder r2=2r1modP(x)=0001001 is formed, which is stored in RgPRF2. This ends the action of the "Start" signal. With a clock signal Clk1 with a value of b2 = 1, the contents of RgPRF2 are transmitted to the inputs of CMAdd2. Where R2=R1⊕r2*b2)=111010 is formed. At the same time, r2 from the outputs of RgPRF2 with a left shift by one bit is fed to the input of the PRF1 at the output of which a partial remainder r3=2r2modP(x)=0010010 is generated, which is fed to the inputs of CMAdd2, forming R3=R2⊕r3*b3)=101000. At the same time, r3 with a shift by one bit to the left is fed to the inputs of the PRF2, forming r4=2r3modP(x)=0100100, which is stored in RgPRF2. After applying the clock signal Clk2 as the value is b4 = 0, then R4=R3⊕r4*b4)=101000. Also the signal Clk2 doubles the value r4 is transmitted to the inputs of the filter 1 at the output of which the value r5=2r4modP(x)=0001011, which is fed to the inputs of CMAdd2, where the final balance R5 = R4⊕r5 * b5) = 100011 is formed.

Table 3 – The amount of resources spent

m, bit	LUT	%	FF	%
6	202	0.32	130	0.10
8	271	0.43	185	0.15
10	398	0.63	252	0.20
12	591	0.93	332	0.26

Table 3 shows the amount of the main resources LUT and FF used and their percentage of the total for polynomials with power m = 6 ÷ 12.

Conclusion. As can be seen from the considered the device for multiplying polynomials modulo with analysis of two bits of the polynomial multiplier per step, the multiplication process can be accelerated almost twice. Similarly, to accelerate the multiplication of polynomials modulo per step of multiplication, you can analyze more than two bits of the multiplier.

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[1], С. Ғнатюк[2], М. К. Ибраимов[3], М. М. Мағзом[1]

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

ҚАДАМ САЙЫН КӨБЕЙТКІШТЕРДІҢ ЕКІ РАЗРЯДТАРЫН ТАЛДАУ АРҚЫЛЫ ПОЛИНОМДАРДЫ МОДУЛЬ БОЙЫНША КӨБЕЙТЕТІН ҚҰРЫЛҒЫ

Аннотация. ҚР БжҒМ ҒК қарасты Ақпараттық және есептеуіш технолоғиялар институтында бейпозициялық көпмүшеліктер есептеу жүйесі (БКЕЖ) негізінде деректерді шифрлаудың симметриялық алгоритмі жасалынып, ол программалық жолмен іске қосылған. Деректерді шифрлау және кері шифрлау жылдамдығын арттыру үшін аталған криптожүйе программалық-аппараттық немесе аппараттық жолмен іске қосылуы мүмкін. Мұндай БКЕЖ негізінде құрылған криптожүйеде деректерді шифрлау жылдамдығының өсірілуі оның құрамындағы аппараттық модульдердің параллель жұмыс жасауымен байланысты. БКЕЖ-ге сүйенін құрылған криптожүйелердің негізгі блоғына көпмүшеліктері келтірілмейтін көпмүшеліктер модулі арқылы көбейтетін құрылғылар жатады. Мұндай құрылғыларда деректерді шифрлауға және кері шифрлауға қажет арифметикалық амалдар орындалады.

Аталған көбейту құрылғысында көбейгіш ретінде шифрланатын мәтіннің бір бөлігі болып табылатын көпмүшеліктің екілік коэффициенттері, ал көбейткіш ретінде құпия кілт рөлін атқаратын көпмүшеліктің екілік коэффициенттері бола алады. Модуль ретінде жоғарыдағы көпмүшеліктегі келтірілмейтін көпмүшеліктерінің бірінің екілік коэффициенттері алынады.

Көпмүшеліктерді модуль бойынша көбейтудің екі тәсілі бар. Біріншісінде көпмүшеліктердің екілік коэффициенттерін бір-біріне көбейтіп, одан соң көбейтіндіні модульге келтіреміз. Мұнда көбейту уақыты көпмүшеліктерді көбейтуге кететін уақытпен және оны модульге келтіру уақыттарымен анықталады. Оның үстіне көбейтінді разрядтары модуль разрядтары санынан асып кетеді. Мұндай жағдайда көбейту құрылғысының құрамы күрделіленеді.

Екінші тәсілінде көпмүшеліктерді модуль бойынша көбейту үстінде көбейту амалы бірнеше қадам арқылы орындалады. Қадам саны көбейткіш болып табылатын көпмүшеліктің екілік коэффициенттерінің санымен (разрядтарымен) анықталады.

Көбейтудің әр қадамында бұрынғы алынған жекеленген ri-1 қалдық жоғары разрядқа қарай бір разрядқа жылжытылып (ягни екіге көбейтіліп), жекелеген қалдық қалыптастырғыш (ЖҚҚ) кірісіне беріледі. ЖҚҚ екіге көбейтілген 2ri-1 қалдықты модульге келтіріп ri қалдығын қалыптастырады. Одан әрі ri қалдығы одан бұрын алынған аралық Ri-1 қалдығына екілік модульмен қосындыланып, Ri аралық қалдығын қалыптастырады. Жоғарыдан көрініп тұргандай, көбейтудің әр қадамында қалдықтарды жекеленген қалыптастыру үстінде көпмүшеліктерді көбейту және оларды модульге келтіру операциялары бір қадамда орындалады.

Мақалада көбейтудің әр қадамында көбейткіш көпмүшеліктерінің екі разрядтарын талдау арқылы көпмүшеліктерді модуль бойынша көбейтетін құрылғы қаралады. Көбейту құрылғысының құрылымдық сұлбасы, оның жұмыс жасау реті, көбейту құрылғысының құрамына кіретін жекеленген қалдықтар қалыптастырғышы, құрамында жинақтағышы бар екі модульмен жұмыс жасайтын қосындылағышы қаралады. Қаралған көпмүшеліктерді модульмен көбейту құрылғысының жұмысы Xilinx компаниясының ПЛИС-ін (Artix-7) іске қосу арқылы тексерілген.

Түйін сөздер: бейпозициялық көпмүшеліктер есептеу жүйесі, келтірілмейтін көпмүшеліктер, көпмүшеліктерді келтірілмейтін көпмүшеліктер арқылы көбейту, қалдықтар қалыптастырғышы.

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

[1]Институт информационных и вычислительных технологий, Алматы, Казахстан;
[2]Национальный авиационный университет, Киев, Украина;
[3]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан

УСТРОЙСТВО УМНОЖЕНИЯ ПОЛИНОМОВ ПО МОДУЛЮ С АНАЛИЗОМ ЗА ШАГ ДВУХ МЛАДШИХ РАЗРЯДОВ МНОЖИТЕЛЯ

Аннотация. В Институте информационных и вычислительных технологий КН МОН РК разработаны и программно реализованы алгоритмы блочного симметричного шифрования данных на базе непозиционной полиномиальной системы счисления (НПСС). Особый интерес представляют программно-аппаратные и аппаратные способы реализация НПСС, которые позволяют существенно ускорить процесс шифрования и расшифрования данных за счет параллельной обработки данных на уровне отдельного модуля и разрядов внутри каждого модуля.

При программно-аппаратной и аппаратной реализаций криптосистем на базе НПСС основным блоком является умножитель полиномов по модулю неприводимых полиномов, где производятся сложные вычисления по шифрованию и расшифрованию данных. В таких умножителях в качестве множимого выступает фрагмент шифрируемого текста, а множителем является полином, который служит секретным ключом, а модуль выбирается из множества неприводимых полиномов.

Существует два подхода к умножению полиномов по модулю. В первом подходе двоичные коэффициенты полиномов множителя и множимого умножаются на устройстве умножения полиномов, затем это произведение приводится по модулю неприводимого полинома. При таком подходе время умножения полиномов по модулю складывается из времени умножения полиномов и времени приведения произведения полиномов по модулю неприводимого полинома. Кроме этого, результат умножения полиномов выходит за разрядной сеткой модуля, что усложняет структуру устройства умножения.

Во втором подходе умножение полиномов по модулю операция разбивается на шаги, число которых определяется числом двоичных коэффициентов (разрядностью) полинома – множителя. При этом на каждом шаге предыдущий частичный остаток ri-1 передается со сдвигом на один разряд в сторону старшего разряда этого остатка (ri-1 умножается на два) на входы следующего формирователя частичных остатков (ФЧО) и производится его приведение по модулю неприводимого модуля, формируя частичный остаток ri. Остаток ri при единичном значении анализируемого разряда множителя подается на входы накапливающего сумматора по модулю два, где вычисляется промежуточный остаток путем сложения по модулю два частичного остатка ri с промежуточным остатком Ri-1. При этом подходе умножения нетрудно заметить, что при формировании очередного частичного остатка операция умножения полиномов совмещается с операцией приведения по модулю.

В данной работе рассматривается умножитель полиномов по модулю, где на каждом шаге умножения анализируется два разряда полинома – множителя, что позволяет ускорить процесс умножения. В работе приводятся функциональные схемы умножителя и его компонентов, пример умножения. В заключении приводится реализация рассмотренного устройства умножения на ПЛИС фирмы Xilinx (семейства Artix-7). Работа предложенного устройства умножения опробирована для полиномов, имеющих степень m=6÷12, и определено для них количество затраченных ресурсов.

Ключевые слова: криптосистема на основе полиномиальной системы счисления, неприводимые полиномы, умножитель полиномов по модулю неприводимых полиномов, формирователи остатков.

Information about authors:

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

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

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

REFERENCES

[1] Akushsky I.Ya., Yuditsky D.I. (1968) Machine arithmetic in residual classes [Mashinnaya arifmetika v ostatochnykh klassakh]. Moscow: Soviet Radio. P. 440 (in Russ.).

[2] Amerbaev V.M., Biyashev R.G., Nysanbaeva S.E. (2005) Application of non-positional number system in cryptographic information protection [Primeneniye nepozitsionnoy sistemy schisleniya pri kriptograficheskoy zashchite informatsii]. News of The National Academy of Science of The Republic of Kazakhstan, Series of physical and mathematical. Vol. 3 (2005). P. 9-12 (in Russ.).

[3] Nysanbaev R.K. (1999) Cryptographic method based on polynomial foundations [Kriptograficheskiy metod na osnove polinomial'nykh osnoviy]// Bulletin of the Ministry of Science and Higher Education and Nat. Acad. Science of the Republic of Kazakhstan - Almaty: Gylym, 1999. N 5. P. 63-65 (in Russ.).

[4] Biyashev R., Kalimoldayev M., Nysanbaeyeva S., Magzom M. (2016) Development of an encryption algorithm based on nonpositional polynomial notations //Proceeding of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). Chiang Mai; Thailand, 2016. P.243-245. https://doi.org/10.2991/amsee-16.2016.64

[5] Kalimoldayev, M.N., Biyashev, R.G., Nyssanbayeva, S.E., Begimbayeva, Y.Y. (2016). Modification of the digital signature, developed on the nonpositional polynomial notations. Eurasian Journal of Mathematical and Computer Applications. ISSN 2306-6172, Vol. 4, Issue 2 (2016), P. 33-38

[6] Kalimoldayev M., Tynymbayev S., Gnatyuk S., Ibraimov M., Magzom M. (2019) The device for multiplying polynomials modulo an irreducible polynomial // News of The National Academy of Science of The Republic of Kazakhstan Series of Geology and Technical Sciences, ISSN 2224-5278, Vol. 2, N 434 (2019), P. 199-205 https://doi.org/10.32014/2019.2518-170X.55 ISSN 2518-170X (Online), ISSN 2224-5278 (Print)

[7] Kalimoldayev M., Tynymbayev S., Magzom M., Ibraimov M., Khokhlov S., Abisheva A., Sydorenko V. Polynomials multiplier under irreducible polynomials module for high-performance cryptographic hardware tools (2019) CEUR Workshop Proceedings, 2393. P. 729., https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069432716&partnerID=40&md5=35074925faba10fc9a96dd780cc09c63 (15.08.2019)

[8] Kalimoldayev M., Tynymbayev S., Gnatyuk S., Khokhlov S., Magzom M., Kozhagulov V. Matrix Multiplier of Polynomials module Analysis Starting with the Lower order Digits of the Multiplier, News of The National Academy of Science of The Republic of Kazakhstan Series of Geology and Technical Sciences, Vol. 4, N 436 (2019), P. 181-187 (Scopus, Cite Score Tracker 0.06, SJR 0.142 Web of Science, IF 0.118 by KazBS). https://doi.org/10.32014/2019.2518-170X.113 ISSN 2518-170X (Online), ISSN 2224-5278 (Print)

[9] Kalimoldayev M.N., Tynymbayev S., Magzom M., Namazbaev T. (2019) // Multiplier of polynomials modulo sequential action [Umnozhitel' polinomov po modulyu posledovatel'nogo deystviya], Materials IV International scientific-practical conference "Informatics and applied mathematics" Part 2, P. 607-615, Almaty, from September 25 to 29, 2019 (in Russ.).

[10] Kalimoldayev M.N., Tynymbayev S., Magzom M.M., Ibraimov M.K., Kozhagulov E.T. (2019) Device for multiplying polynomials modulo irreducible polynomials [Ustroystvo umnozheniya polinomov po modulyu neprivodimykh polinomov], Patent (19) KZ (13) B (11) 33810, G06F 7/72 (2006.01), G06F 7/523 (2006.01) G06F 7/52 (2006.01), Bull. No 31 on 08/02/2019 (in Russ.).

[11] Apendiyev T.A., Asylbekova Z.M., Abdukadyrov N.M., Satov E.Z. (2016) A historical picture of German resettlement to Kazakhstan (End of the 19th Century–Beginning of the 20th Century) // Herald of the Russian Academy of Sciences. 86 (6), 534–536. https://doi.org/10.1134/s1019331616060174

[12] Apendiyev T.A., Abdukadyrov N.M., Kubeyev R.D. (2019) History of German Diaspora in Kazakhstan in the Context of Migration System // Bulletin of the Georgian National Academy of Sciences. 2019. Vol. 13, Issue 4. P. 127-134.