

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

4

АЛМАТЫ
АЛМАТЫ
ALMATY

2017

JULY
ИЮЛЬ
ШІЛДЕ

Б а с р е д а к т о р ы

х. ғ. д., проф., ҚР ҰҒА академигі

М. Ж. Жұрынов

Р е д а к ц и я а л қ а с ы:

Абиев Р.Ш. проф. (Ресей)
Абишев М.Е. проф., корр.-мүшесі (Қазақстан)
Аврамов К.В. проф. (Украина)
Аппель Юрген проф. (Германия)
Баймуқанов Д.А. проф., корр.-мүшесі (Қазақстан)
Байпақов К.М. проф., академик (Қазақстан)
Байтулин И.О. проф., академик (Қазақстан)
Банас Иозеф проф. (Польша)
Берсимбаев Р.И. проф., академик (Қазақстан)
Велихов Е.П. проф., РҒА академигі (Ресей)
Гашимзаде Ф. проф., академик (Әзірбайжан)
Гончарук В.В. проф., академик (Украина)
Давлетов А.Е. проф., корр.-мүшесі (Қазақстан)
Джрбашян Р.Т. проф., академик (Армения)
Қалимолдаев М.Н. проф., академик (Қазақстан), бас ред. орынбасары
Лаверов Н.П. проф., академик РАН (Россия)
Лупашку Ф. проф., корр.-мүшесі (Молдова)
Мохд Хасан Селамат проф. (Малайзия)
Мырхалықов Ж.У. проф., академик (Қазақстан)
Новак Изабелла проф. (Польша)
Огарь Н.П. проф., корр.-мүшесі (Қазақстан)
Полещук О.Х. проф. (Ресей)
Поняев А.И. проф. (Ресей)
Сагиян А.С. проф., академик (Армения)
Сатубалдин С.С. проф., академик (Қазақстан)
Таткеева Г.Г. проф., корр.-мүшесі (Қазақстан)
Умбетаев И. проф., академик (Қазақстан)
Хрипунов Г.С. проф. (Украина)
Якубова М.М. проф., академик (Тәжікстан)

«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

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2017

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

Г л а в н ы й р е д а к т о р
д. х. н., проф. академик НАН РК
М. Ж. Журинов

Р е д а к ц и о н н а я к о л л е г и я:

Абиев Р.Ш. проф. (Россия)
Абишев М.Е. проф., член-корр. (Казахстан)
Аврамов К.В. проф. (Украина)
Апель Юрген проф. (Германия)
Баймуканов Д.А. проф., чл.-корр. (Казахстан)
Байпаков К.М. проф., академик (Казахстан)
Байтулин И.О. проф., академик (Казахстан)
Банас Иозеф проф. (Польша)
Берсимбаев Р.И. проф., академик (Казахстан)
Велихов Е.П. проф., академик РАН (Россия)
Гашимзаде Ф. проф., академик (Азербайджан)
Гончарук В.В. проф., академик (Украина)
Давлетов А.Е. проф., чл.-корр. (Казахстан)
Джрбашян Р.Т. проф., академик (Армения)
Калимолдаев М.Н. академик (Казахстан), зам. гл. ред.
Лаверов Н.П. проф., академик РАН (Россия)
Лунашку Ф. проф., чл.-корр. (Молдова)
Мохд Хасан Селамат проф. (Малайзия)
Мырхалыков Ж.У. проф., академик (Казахстан)
Новак Изабелла проф. (Польша)
Огарь Н.П. проф., чл.-корр. (Казахстан)
Полещук О.Х. проф. (Россия)
Поняев А.И. проф. (Россия)
Сагиян А.С. проф., академик (Армения)
Сатубалдин С.С. проф., академик (Казахстан)
Таткеева Г.Г. проф., чл.-корр. (Казахстан)
Умбетаев И. проф., академик (Казахстан)
Хрипунов Г.С. проф. (Украина)
Якубова М.М. проф., академик (Таджикистан)

«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

© Национальная академия наук Республики Казахстан, 2017

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

E d i t o r i n c h i e f

doctor of chemistry, professor, academician of NAS RK

M. Zh. Zhurinov

E d i t o r i a l b o a r d:

Abiyev R.Sh. prof. (Russia)
Abishev M.Ye. prof., corr. member. (Kazakhstan)
Avramov K.V. prof. (Ukraine)
Appel Jurgen, prof. (Germany)
Baimukanov D.A. prof., corr. member. (Kazakhstan)
Baipakov K.M. prof., academician (Kazakhstan)
Baitullin I.O. prof., academician (Kazakhstan)
Joseph Banas, prof. (Poland)
Bersimbayev R.I. prof., academician (Kazakhstan)
Velikhov Ye.P. prof., academician of RAS (Russia)
Gashimzade F. prof., academician (Azerbaijan)
Goncharuk V.V. prof., academician (Ukraine)
Davletov A.Ye. prof., corr. member. (Kazakhstan)
Dzhrbashian R.T. prof., academician (Armenia)
Kalimoldayev M.N. prof., academician (Kazakhstan), deputy editor in chief
Laverov N.P. prof., academician of RAS (Russia)
Lupashku F. prof., corr. member. (Moldova)
Mohd Hassan Selamat, prof. (Malaysia)
Myrkhalykov Zh.U. prof., academician (Kazakhstan)
Nowak Isabella, prof. (Poland)
Ogar N.P. prof., corr. member. (Kazakhstan)
Poleshchuk O.Kh. prof. (Russia)
Ponyaev A.I. prof. (Russia)
Sagiyani A.S. prof., academician (Armenia)
Satubaldin S.S. prof., academician (Kazakhstan)
Tatkeyeva G.G. prof., corr. member. (Kazakhstan)
Umbetayev I. prof., academician (Kazakhstan)
Khripunov G.S. prof. (Ukraine)
Yakubova M.M. prof., academician (Tadjikistan)

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>

© National Academy of Sciences of the Republic of Kazakhstan, 2017

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

M. N. Kalimoldayev, S. T. Tynymbayev, N. A. Kapalova

Institute of information and computational technologies CS MES RK, Almaty, Kazakhstan.
E-mail: mnk@ipic.kz, s.tynym@mail.ru, nkapalova@mail.ru

POLYNOMIAL MULTIPLIERS ON THE MODULE OF IRREDUCIBLE POLYNOMIALS

Abstract. In cryptographic information protection the most important role is played by approaches to their implementation. According to researchers, the task of optimizing the operation of encryption algorithms is in demand and is relevant at the present time. Hardware has a number of significant advantages over software, for example, it has better speed characteristics, ensures the cryptographic algorithm integrity, and allows to optimize many mathematical operations used in encryption algorithms. But software implementations of encryption algorithms are usually cheaper than hardware ones. Given the advantages list of these approaches, it is possible to solve the problem of encryption algorithms optimization by software and hardware means. It gives the user configuration flexibility and high data security. Hardware and software cryptographic system consists of an electronic device that connects to a personal computer and software to operate with the device. In such systems, the functions that are not critical to the speed and security of the work are shifted to software, thereby reducing their cost.

The developed encryption algorithm on the basis of non-positional polynomial notations is intended for software, hardware, and also software and hardware implementation. The main hardware-implemented device in non-positional algorithm of the cryptographic transformation is a device for multiplication of polynomials on the module of the irreducible polynomials, which produces routine calculations on data encryption.

This paper considers the classical approach to construction of the multipliers on the module of irreducible polynomials, where at the first stage the product of two polynomials is computed, and at the second stage the obtained result is given on the module of irreducible polynomials.

Key words: cryptography, encryption algorithms, non-positional polynomial notations, software and hardware implementation.

УДК 004.056.5

М. Н. Калимолдаев, С. Т. Тынымбаев, Н. А. Капалова

Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан

УМНОЖИТЕЛИ ПОЛИНОМОВ ПО МОДУЛЮ НЕПРИВОДИМЫХ ПОЛИНОМОВ

Аннотация. В криптографической защите информации важнейшую роль играют подходы к их реализации. Также, по мнению исследователей, задача оптимизация работы алгоритмов шифрования является востребованной и актуальной в настоящее время. Аппаратные средства имеют ряд существенных преимуществ перед программными, например, обладают лучшими скоростными характеристиками, гарантируется целостность криптографического алгоритма, и позволяют оптимизировать многие математические операции, применяемые в алгоритмах шифрования. Но программные реализации алгоритмов шифрования, как правило, дешевле аппаратных. Учитывая перечень достоинств этих подходов, можно решить задачу оптимизации работ алгоритмов шифрования программно-аппаратным способом. Он предоставляет пользователю гибкость настройки и высокую защищенность данных. Программно-аппаратная криптосистема состоит из электронного устройства, которое подключается к персональному компьютеру и программного обеспечения для работы с устройством. В таких системах выполнение функций, некритичных к скорости работы и безопасности, перекладывается на программное обеспечение, что способствует снижению их стоимости.

Разработанный алгоритм шифрования на базе непозиционных полиномиальных систем счисления предназначен для программной, аппаратной и программно-аппаратной реализации. Основным аппаратно реализуемым устройством в непозиционном алгоритме криптографического преобразования является устройство для умножения полиномов по модулю неприводимых полиномов, где производятся рутинные вычисления по шифрованию данных.

В работе рассматривается классический подход к построению умножителей полиномов по модулю неприводимых полиномов, где на первом этапе вычисляется произведение двух полиномов, а втором этапе – полученное произведение приводится по модулю неприводимых полиномов.

Ключевые слова: криптография, алгоритмы шифрования, непозиционные полиномиальные системы счисления, программно-аппаратная реализация.

Криптография играет ключевую роль в обеспечении защиты информации в вычислительной технике и средствах коммуникации. Последние десятилетия криптография интенсивно развивается, этому способствуют такие факторы как бурное развитие вычислительной техники и ее повсеместное использование. То же самое касается и разработки криптографических алгоритмов. Известно множество алгоритмов шифрования, разработанных научными институтами, один из подходов построения алгоритма блочного симметричного шифрования исследуется в Институте информационных и вычислительных технологий КН МОН РК.

В разработанных непозиционных системах шифрования в качестве критерия криптостойкости используется не длина ключа, а криптостойкость самих криптоалгоритмов. Обусловлено это применением арифметики непозиционных систем, т.е. систем счисления в остаточных классах (СОК). В отличие от классических СОК предлагаемые криптографические нетрадиционные алгоритмы рассматриваются в полиномиальных системах счисления в остаточных классах, в которых основаниями служат не простые числа, а неприводимые многочлены над полем $GF(2)$, т.е. с двоичными коэффициентами. Так, полным ключом в нетрадиционном алгоритме шифрования являются ключевая последовательность и система полиномиальных оснований, которая выбирается из всего множества неприводимых многочленов степени не выше значения длины блока с учетом порядка распределения выбранных оснований. Использование непозиционных полиномиальных систем счисления (НПСС) позволяет также повысить эффективность алгоритмов, так как в соответствии с правилами НПСС все арифметические операции могут выполняться параллельно по модулям оснований НПСС [1-4].

Проводятся работы по эффективной программной реализации разработанных алгоритмов в виде модулей, объединенных в систему криптографической защиты информации (СКЗИ)[5]. Также планируется построение программно-аппаратной и аппаратной реализации симметричных криптографических алгоритмов защиты информации на базе НПСС. Так как программно-аппаратная и аппаратная реализация имеют ряд существенных преимуществ перед программными аналогами, аппаратная реализация обладает лучшими скоростными характеристиками, гарантируется целостность криптографического алгоритма и позволяют оптимизировать многие математические операции, применяемые в алгоритмах шифрования. При программно-аппаратной реализации разработанных алгоритмов часть процедур реализуется аппаратно.

Основным устройством в НПСС является устройство для умножения полиномов по модулю неприводимых полиномов, где производятся рутинные вычисления по шифрованию данных.

В работе рассматривается классический подход к построению умножителей полиномов по модулю неприводимых полиномов, где на первом этапе вычисляется произведение двух полиномов, а втором этапе - полученное произведение приводится по модулю неприводимых полиномов.

Рассмотрим организацию умножителей на примере умножения полиномов A и B . Пусть коэффициенты A и B представлены в двоичной системе:

$$A = \{a_{n-1}a_{n-2} \dots a_1a_0\} \text{ и } B = \{b_{n-1}b_{n-2} \dots b_1b_0\}$$

Матрица частичных произведений полиномов с разрядностью n приведена на рисунке 1. Суммируя каждый столбец этой матрицы по модулю два получим двоичное представление $AxB = C$, где $C = \{C_{2n-1}C_{2n-2} \dots C_1C_0\}$. Здесь сдвинутые относительно друг друга строки матрицы последовательно суммируются по модулю два.

Тогда $C = 2^{n-1} A \cdot b_{n-1} \oplus 2^{n-2} A \cdot b_{n-2} \oplus \dots \oplus 2^1 A \cdot b_1 \oplus 2^0 A \cdot b_0$, где 2^i разрядные веса полиномов ($i = 0, (n-1)$), b_i значения разрядов полинома B ($b_i = \{0,1\}$).

Умножение полиномов осуществляется по методу, где умножение начинается с анализа старшего разряда множителя со сдвигом на каждом шаге умножения суммы частичного произведения вправо (в сторону младшего разряда) на один разряд. При таком методе умножения на каждом шаге умножения анализируется i -й старший разряд множителя (b_i) начиная со старшего. И если при этом $b_i = 1$, то двоичные коэффициенты полинома A суммируются по модулю два с предыдущей суммой частичного произведения или они не суммируются, если $b_i=0$. После этого полученная сумма частичного произведения и разряды множителя сдвигаются вправо на один разряд. Количество таких шагов определяется разрядностью двоичных коэффициентов полинома множителя.

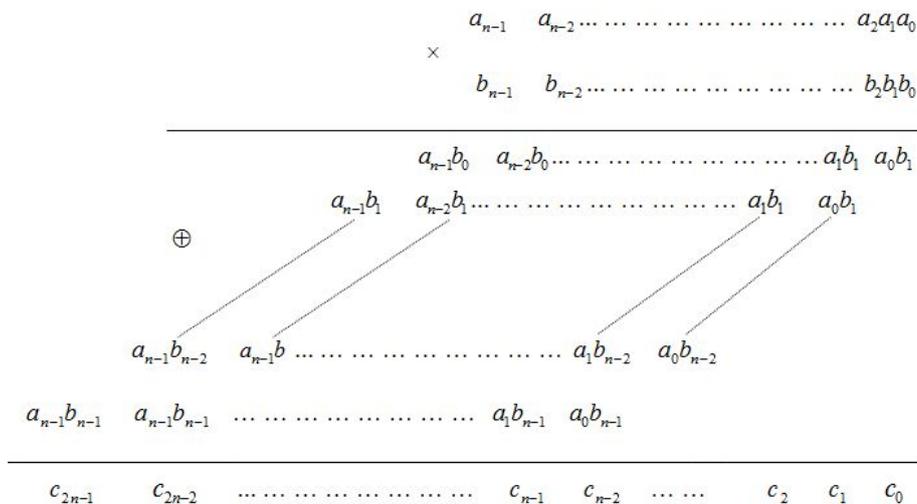


Рисунок 1 – Схема перемножения полиномов A и B

На рисунке 2 приведена структурная схема умножителя полиномов A и B последовательного действия. Умножитель состоит из регистров коэффициентов полинома A (PrA), полинома B (PrB), регистра частичного произведения (PrЧП), сумматора по модулю два (далее СМ), блока синхронизаций (БС), который в своем составе имеет вычитающий счетчик тактовых импульсов (СчТИ).

Согласно выбранному методу умножения в регистр PrB старшие разряды полинома $B - b_{n-2}, b_{n-1} \dots$ принимаются младшие разряды регистра B , а младшие разряды полинома $B - b_0, b_1 \dots$ принимаются старшие разряды регистра B .

Разряды PrЧП связаны с левыми входами СМ через схему И1 правые входы СМ связаны с выходами регистра полинома A (множимое) через схему И2. На третий вход схемы И2 подается значение (очередного старшего разряда полинома B , выдача содержимого регистра PrЧП – на выходы схемы И1 управляется тактовым импульсом ТИ, выдача содержимого PrA на выходы схемы И2 управляется тактовым импульсом также значения младшего разряда регистра PrB - b_i . Результаты сложения по модулю два с выходов СМ передаются на входы регистра PrЧП, где они запоминаются до подачи сдвигающего тактового импульса. Работа умножителя начинается с подачи сигнала «Пуск», который поступает на БС, где в счетчик записывается код числа сдвигов $K = \log_2 n$ (n -разрядность регистра PrB) кроме того сигналом «Пуск» осуществляет прием коэффициентов полиномов регистрами PrA и PrB.

После этого БС выдает тактовые импульсы ТИ в схему умножителя. Каждым тактовым импульсом суммируется по модулю два содержимое регистров PrЧП и PrA и результаты сложения записываются в регистр PrЧП и задержанным на линии задержки (ЛЗ.) тактовым импульсом содержимое регистров PrЧП и PrB сдвигается вправо на один разряд. После подачи n -го тактового импульса в регистрах PrЧП и PrB и дополнительном разряде – Д регистра PrB формируется

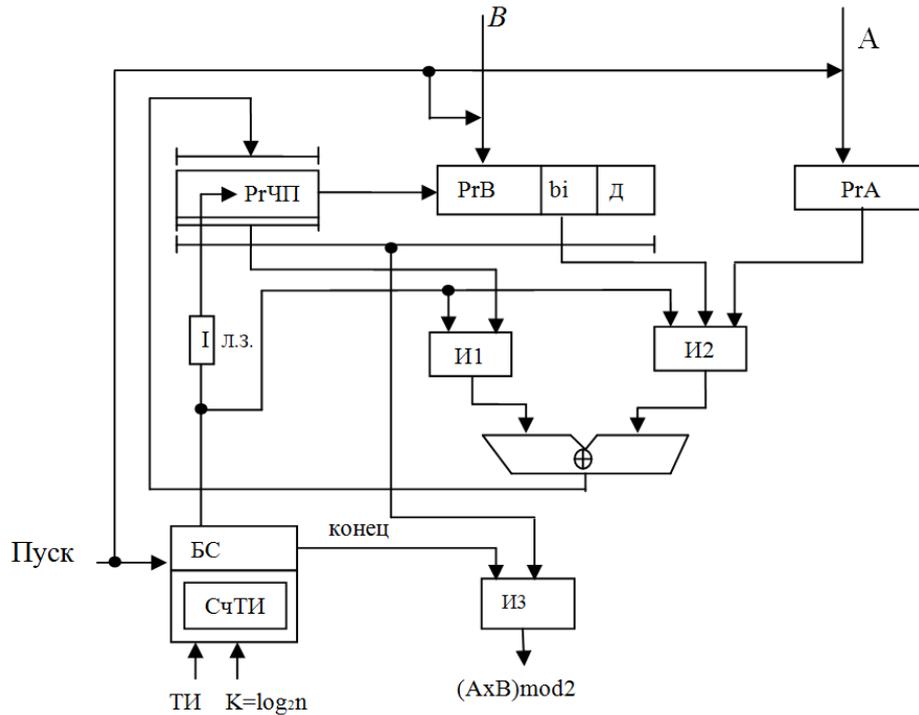


Рисунок 2 – Умножитель полиномов последовательного действия

значение произведения – С. Последний n-ый тактовый импульс установит СчТИ в нулевое состояние, при этом вырабатывается сигнал «Конец операций», который выдает содержимое PrЧП и PrB с дополнительным разрядом со сдвигом влево на один разряд логической схемой ИЗ. Кроме этого сигналом «Конец операций» блокируется поступление тактового импульса в устройство.

Теперь перейдем к рассмотрению второго этапа – приведению по модулю P. Для этого рассмотрим пример умножения полиномов A и B по модулю P.

Пусть $A(x) = x^3 + x + 1$ и $B(x) = x^3 + 1$; $P(x) = x^4 + x + 1$

Тогда $L(x) = (x^3 + x + 1)(x^3 + 1) \bmod (x^4 + x + 1) = (x^6 + x^4 + x + 1) \bmod (x^4 + x + 1) = x^3 + x^2$

Двоичное представление $C = A(x)B(x) = x^6 + x^4 + x + 1 = 1010011$

Двоичное представление $P = 10011$;

Тогда для вычисления $C \bmod P$ требуется следующие вычисления (рисунок 3).

$L(x) = 01100$ соответствует полиному $x^3 + x^2$.

C	10100	11	
P	⊕ 10011		$x^4 + x^2 > x^4 + x + 1$ поэтому
r_0	00111	11	$r_0 = 10100 \oplus 10011 = 00111$
$2r_0$	01111	1	сдвиг влево на один разряд
P	⊕ 10011		$2r_0 < P$ поэтому $r_1 = 01111$
$r_1 = 2r_0$	01111		сдвиг влево r_1 на один разряд
$2r_1$	11111		
P	⊕ 10011		
L(x)	01100		результат

Рисунок 3 – Пример умножения полиномов

Из рассмотренного примера видно, что блок формирования частичного остатка должен выдать на выход $2r_i$ при условии, если $2r_i < P$, иначе результат сложения $2r_i \oplus P$. Следует заметить, что перед вычислением очередного остатка r_i предыдущий остаток r_{i-1} сдвигается влево на один разряд, т.е. формируется удвоенное значение $2R_{i-1}$.

Из рассмотренного примера видно, что формирователь частичного остатка должен выдать на его выход $2r_{i-1}$ (где $2r_{i-1}$ сдвинутый на один разряд влево предыдущий остаток r_{i-1}), если $2r_{i-1} < P$, иначе результат сложения $2r_{i-1} \oplus P$.

Тогда структура формирователя частичного остатка (ФЧО) имеет вид, как это показано на рисунке 4.

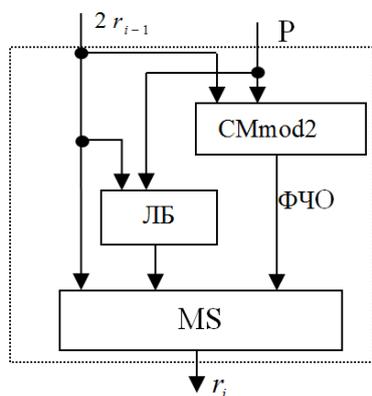


Рисунок 4 – Структура ФЧО

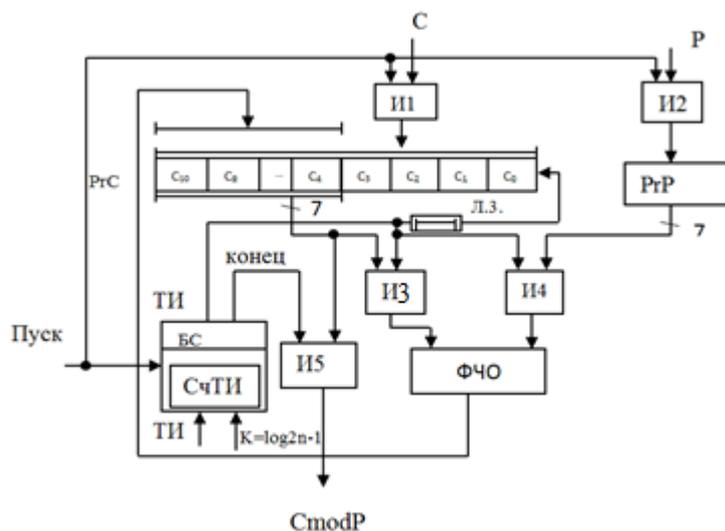


Рисунок 5 – Схема устройства приведения по модулю CmodP

Как видно из рисунка 4, ФЧО состоит из сумматора по модулю и мультипликатора (MS), логического блока (ЛБ), который коммутирует на выход мультипликатора либо код удвоенного предыдущего частичного остатка $2r_{i-1}$ или выход сумматора по модулю, где была вычислена $2r_{i-1} \oplus P$ в зависимости от соотношения $2r_{i-1}$ и P .

Приведение произведения полиномов – С по модулю можно осуществить с помощью одного ФЧО или на множестве ФЧО. На рисунке 4 приведена схема устройства приведения, по модулю последовательного типа на одном ФЧО. Пусть $C = c_{10}c_9...c_1c_0$ где коэффициенты полиномов А и В имеют по 5 разрядов, а для таких полиномов разрядность неприводимых полинома $n=5$. Схема устройства приведения по модулю с помощью одного ФЧО приведена на рисунке 5.

На этой схеме значения С и Р принимаются через схему И1 и И2 в регистр PrC и регистр PrP сигналом «Пуск». После этого с блока синхронизаций первый тактовый импульс ТИ, который подается на входы логических схем И3 и И4, тем самым содержимое регистра PrC $[C_8 \div C_4]$ поступает на левые входы ФЧО, а на правый вход, ФЧО подается содержимое PrP. В зависимости от соотношения входного кода и неприводимого полинома на выходах ФЧО формируется частичный остаток, который подается на входы регистра PrC $[C_8 \div C_4]$. Задержанный первый ТИ на линии задержки Л.З. поступает на вход PrC и сдвигает его содержимое формируя $2r_{i-1}$.

Вторым тактовым импульсом на входы ФЧО подаются $2r_{i-1}$ и P. После этого формируется частичный остаток r_i , который принимается в PrC $[C_8 \div C_4]$. И задержанным вторым тактовым

импульсом ТИ содержимое PnC сдвигается влево, на один разряд формируя следующий удвоенный остаток.

Процесс формирования остатков заканчивается после подачи $n-1$ тактового импульса. При этом $SчТИ=0$ и счетчик вырабатывает сигнал «Конец операции». Этим сигналом блокируется передача тактового импульса в схему и содержимое регистра $PnC[C_8 \div C_4]$ передается на выход через схему И5.

Таким образом, в работе рассмотрен классический подход к построению умножителя полиномов по модулю неприводимых полиномов, где на первом этапе вычисляется произведение двух полиномов, а втором – полученное произведение приводится по модулю.

REFERENCES

- [1] Biyashev R.G. Razrabotka i issledovaniye metodov skvoznogo povysheniya dostovernosti v sistemakh obmena dannyimi raspredelennykh ASU: diss. dokt. tekhn. nauk: 05.13.06: zashchishchena 09.10.1985: utv. 28.03.1986. - M., 1985. (in Russ.)
- [2] Amerbayev V.M., Biyashev, R.G., Nysanbayeva S.Ye. Primeneniye nepozitsionnykh sistem schisleniya pri kriptograficheskoy zashchite // Izv. Nats. akad. Nauk Respubliki Kazakhstan. - Ser. fiz.-mat. - Almaty: Gylym, 2005. - № 3. - S. 84-89. (in Russ.)
- [3] Biyashev R., Kalimoldayev M., Nyssanbayeva S., Kapalova N., Khakimov R. (2014). Program Modeling of the Cryptography Algorithms on Basis of Polynomial Modular Arithmetic / The 5th International Conference on Society and Information Technologies, Orlando, Florida, USA, P. 49-54
- [4] Kapalova N., Dyusenbayev D. (2016) Security analysis of an encryption scheme based on nonpositional polynomial notations, Journal Open Engineering, 1:250-25. DOI: 10.1515/eng-2016-0034.
- [5] Biyashev, S. Nyssanbayeva, N. Kapalova, A. Haumen, Modified symmetric block encryption-decryption algorithm based on modular arithmetic (2016) Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016), Chiang Mai, Thailand, P. 263-265.

М. Н. Қалимолдаев, С. Т. Тынымбаев, Н. А. Капалова

Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан

КЕЛТІРІЛМЕЙТІН КӨПМҮШЕЛІКТЕР МОДУЛІ БОЙЫНША КӨПМҮШЕЛІКТЕРДІ КӨБЕЙТУ

Аннотация. Ақпаратты криптографиялық қорғауда оларды жүзеге асыру жолдары аса маңызды рөл атқарады. Сондай-ақ, зерттеушілердің ойынша, шифрлеу алгоритмдерінің жұмыс істеуін тиімдету есептері қазіргі таңда қажетті және өзекті. Аппараттық құралдар бағдарламалыққа қарағанда айтарлықтай ерекшеліктері бар, мысалы, олар жақсы жылдамдық сипаттарына ие, криптографиялық алгоритмнің тұтастығын кепілдік және де шифрлеу алгоритмдерінде қолданылатын көптеген математикалық амалдарды тиімдетуге мүмкіндік береді. Бірақ та шифрлеу алгоритмдерін бағдарламалық жүзеге асыру аппараттыққа қарағанда арзандау. Осы әдістердің ұтымды жақтарын ескере отырып, шифрлеу алгоритмінің жұмысын тиімдету есебін бағдарламалық-аппараттық жолмен шешуге болады. Ол қолданушыға икемді баптау мен хабардың жоғары қорғанысын қамтамасыз етеді.

Бағдарламалық-аппараттық криптожүйелер дербес компьютерге қосылған электрондық құрылғы мен онымен жұмыс істеуге арналған бағдарламалық қамтудан тұрады. Бұндай жүйелерде, жұмыс жылдамдығы мен қауіпсіздігі жағынан сынды емес, функциялар бағдарламалық қамтуға жүктеледі, бұл олардың құнының төмендеуіне ықпал етеді.

Құрылған позициялық емес полиномды санау жүйесіне негізделген, шифрлеу алгоритмін бағдарламалық, аппараттық және бағдарламалық-аппараттық жүзеге асыруға болады. Позициялық емес криптографиялық өзгерту алгоритмінде негізгі аппараттық жүзеге аырылатын құрал болып, ақпаратты шифрлеу кезіндегі қиын есептеулерді орындайтын, келтірілмейтін полиномдар модулі бойынша полиномдарды көбейту құрылғысы саналады.

Бұл жұмыста келтірілмейтін полиномдар модулі бойынша полиномдарды көбейту құрылғысын құрудың классикалық әдіс қарастырылған, бірінші этапта екі полиномның көбейтіндісі орындалады, ал екінші этапта көбейтіндінің мәнінен келтірілмейтін көмүшелік бойынша модуль алынады.

Түйін сөздер: криптография, шифрлеу алгоритмі, позициялық емес полиномдық санау жүйесі, бағдарламалық-аппараттық жүзеге асыру.

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

Подписано в печать 21.07.2017.

Формат 60x881/8. Бумага офсетная. Печать – ризограф.
11,75 п.л. Тираж 2000. Заказ 4.