**REPORTS OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN**
ISSN 2224-5227
Volume 5, Number 5 (2014), 20 – 26

HARDWARE METHODS IMPLEMENTATION FOR BASIC OPERATIONS OF ASYMMETRIC CRYPTOALGORITHMS

Tynymbaev S.T., Aythozhaeva E.Zh.
Kazakh national technical university named after K.I.Satpayev, Almaty

Key words: hardware encryption, asymmetric cryptoalgorithms, exponentiation to the power with reduction modulo.

Abstract. A comparative analysis of different hardware methods of performing basic operations exponentiation to the power with reduction modulo - integer multiplication and squaring, on speed and hardware cost is presented. Devices are analyzed for the most critical operation of exponentiation to the power of numbers modulo - reduction modulo.

УДК 681.322

АППАРАТНЫЕ МЕТОДЫ РЕАЛИЗАЦИИ БАЗОВЫХ ОПЕРАЦИЙ АСИММЕТРИЧНЫХ КРИПТОАЛГОРИТМОВ

С.Т. Тынымбаев, Е.Ж. Айтхожаева
Казахский национальный технический университет им. К.И.Сатпаева, г. Алматы

Ключевые слова: аппаратные средства шифрования, асимметричные криптоалгоритмы, возведение чисел в степень по модулю.

Аннотация. Рассматриваются преимущества и разновидности аппаратных средств шифрования. Указывается на низкое быстродействие асимметричных криптоалгоритмов в связи с громоздкими арифметическими вычислениями над числами с повышенной разрядностью (возведение в степень по модулю) и вытекающую из этого проблему ускорения возведения чисел в степень по модулю. Проводится сравнительный анализ различных аппаратных методов выполнения базовых операций возведения чисел в степень по модулю - целочисленного умножения и возведения в квадрат, по быстродействию и аппаратным затратам. Анализируются устройства для выполнения наиболее критичной операции возведения чисел в степень по модулю – приведения по модулю. Определяется направление разработки оптимальных устройств приведения по модулю.

Способы хранения информации на современном этапе развития компьютерных технологий динамично совершенствуются. Связано это с упрощением ее хранения в вычислительных системах и несравнимо высокой скоростью доступа к ней. В настоящее время информация представляет собой специфический товар, который можно купить, продать, обменять на что-то другое и т.д. Информация является стратегическим ресурсом государства. Поэтому защита информации от несанкционированного доступа, кражи, уничтожения и других преступных действий является актуальной проблемой [1, 2].

Одним из наиболее надежных способов обеспечения защиты информации, хранящейся в электронной виде, является криптографическая защита. Криптография связана с шифрованием и

расшифровыванием конфиденциальных данных в каналах коммуникаций. Она также применяется для того, чтобы исключить возможность искажения информации или подтвердить ее происхождение. Криптографические преобразования информации обеспечивают недоступность ее для лиц, не имеющих ключа, и поддерживают с требуемой надежностью обнаружение несанкционированных искажений. Криптографические средства составляют отдельную группу формальных средств защиты, которые обеспечивают превращение открытого текста в шифртекст путем шифрования исходного текста с помощью криптографических алгоритмов [2]. Они могут быть реализованы в виде программных, аппаратных и программно-аппаратных средств защиты.

Аппаратные средства шифрования представляют собой специализированное оборудование. Они дороже программных шифраторов и сложнее в реализации, но имеют ряд существенных преимуществ перед программными средствами: высокая производительность, простота, защищенность и т.д. [3].

Аппаратные средства шифрования информации имеют три разновидности:

- шифровальные модули (они самостоятельно выполняют всю работу с ключами),
- блоки шифрования в каналах связи,
- шифровальные платы расширения для установки в персональные компьютеры.

Большинство устройств первого и второго типа являются узкоспециализированными. Платы расширения для персональных компьютеров являются более универсальным средством аппаратного шифрования и обычно могут быть легко сконфигурированы таким образом, чтобы шифровать всю информацию, которая записывается на жесткий диск компьютера, а также все данные, пересылаемые на его гибкий диск и в последовательные порты. Большая часть устройств для аппаратного шифрования реализована в виде PCI плат расширения или приборов типа USB-ключ.

На современном этапе развития криптографии особое внимание привлекают асимметричные криптоалгоритмы [4]. Использование в ассиметричном шифровании пары ключей (в сравнении с симметричным шифрованием, у которого используется только один ключ) повышает сложность криптоанализа для злоумышленника.

Главным недостатком асимметричных криптоалгоритмов является низкое быстродействие, так как в процедурах шифрования и дешифрования используются громоздкие арифметические вычисления над числами с повышенной разрядностью (возведение в степень по модулю). Поэтому главная проблема асимметричных криптоалгоритмов – это проблема ускорения возведения чисел в степень по модулю. Одним из путей решения этой проблемы является использование аппаратных средств для выполнения базовых операций быстрого возведения чисел в степень по модулю – целочисленного умножения, возведения в квадрат, приведения по модулю.

К настоящему времени накоплен большой опыт в разработке быстродействующих целочисленных умножителей и квадраторов, использующих различные методы ускорения умножения. Методы ускорения умножения делятся на аппаратные и логические.

Более быстродействующими являются аппаратные методы ускорения умножения. Ускорение операции умножения в этом случае достигается за счет:

- параллельного формирования частичного произведения (ЧП);
- минимизации количества сложений;
- уменьшения времени распространения переносов при формировании ЧП.

Параллельное вычисление ЧП присутствует во всех умножителях, где умножение реализовано аппаратно. В зависимости от реализации операции суммирования они подразделяются на матричные и древовидные. В обоих случаях суммирование осуществляется с помощи массива взаимосвязанных одноразрядных сумматоров.

В матричных структурах сумматоры организованы в виде матрицы, а в древовидных – в виде дерева того или иного вида.

При матричном умножении результат C перемножения двух n-разрядных двоичных чисел A и B без знака можно описать выражением:

$$\mathrm{C} = \mathrm{A} * \mathrm{B} = \left(\sum_{i=0}^{n-1} a_i * 2^i\right) * \left(\sum_{j=0}^{n-1} b_j * 2^j\right) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j * 2^{i+j};$$

Умножение сводится к параллельному формированию битов из n – разрядных частичных

произведений с последующим их суммированием с помощью матриц сумматоров. Такая схема известна как умножитель Брауна.

Сократить задержку в матричных умножителях удается в схемах, построенных по древовидной структуре. Если в матричных умножителях для суммирования n частичных произведении требуется n-строк сумматоров, то в древовидных схемах количество ступеней сумматоров пропорционально log2n. Это приводит к сокращению времени вычисления суммы ЧП. Однако при реализации таких умножителей требуются дополнительные связи для объединения разрядов, имеющих одинаковый вес, из-за чего площадь, занимаемая схемой на кристалле, может увеличиться.

В настоящее время наибольшее распространение получили три древовидные схемы получения суммы ЧП: дерево Уоллеса, дерево Дадда и перевернутое ступенчатое дерево [5,6].

Схема Уоллеса является наиболее быстрой, но ее структура наименее регулярна, из-за чего предпочтение отдается иным древовидным структурам. Схема в основном используется для быстрого перемножения чисел большой разрядности. При умножении чисел небольшой разрядности чаще используется схема Дадда. В основе этого умножителя лежит дерево Уоллеса с меньшим числом сумматоров. Схемы Уоллеса и Дадда имеют общий недостаток – нерегулярность структуры. Схема перевернутой лестницы (overturnedstairs) является одной из попыток сделать древовидную структуру более регулярной, что позволяет облегчить ее реализацию в интегральном исполнении.

К умножителям, реализующим аппаратные методы ускорения, относятся также ведические умножители, построенные на основе ведической математики [7,8]. Ведическая математика основывается на ведическом знании и состоит из 16 словоформул, которые известны как сутры (sutras). Ведическую математику исследовал Шри Барати Кришна Тиртха (1984-1960, философ, санскрит, математик и историк). Барати Кришна, опираясь на древнеиндийские письменные наследия, доказал, что словесные сутры являются не чем иным, как математическими формулами.

Рассмотрим алгоритм умножения чисел в десятичной системе на основе ведической математики, где используется словесная сутра UrdhvaTiryagbhyam (вертикально и крест на крест). Пусть A=123 и B=456. Необходимо найти произведение A*B=C.

Шаг-1

1 2 3

| Результат 3*6=18

4 5 6 Перенос =0

8 18

Шаг-2

1 2 3

Результат 12+15=27

4 5 6 Перенос =1

88 28

Шаг-3

1 2 3

| Результат 12+6+10=28

4 5 6 Перенос =2

088 30

Шаг-4

1 2 3

Результат 8+5=13

4 5 6 Перенос =3

6088 16

Шаг-5

1 2 3

| Результат =4

4 5 6 Перенос =1

56088 5

Конечный результат C=123*456=56088.

Аналогичным способом можно вычислить C=A2.

В таблице 1 приведено сравнение ведического умножителя 16*16 бит с другими умножителями по количеству используемых логических элементов [8].

Таблица 1 – Результаты сравнений по количеству логических элементов

Ведический умножитель	Матричный умножитель	Умножитель на дереве Уоллеса	Умножитель Бута
799	559	762	905

Из таблицы 1 видно, что по числу используемых логических элементов самым экономичным является матричный умножитель, затем умножитель на дереве Уоллеса.

Для сравнительного анализа на рисунках 1 и 2 приведены времена задержки различных умножителей и квадраторов, соответственно, в условных единицах. По рисункам 1 и 2 нетрудно заметить, что самыми быстродействующими являются ведические умножители и квадраторы.

Аппаратные умножители имеют ограничение на число разрядов вводимых чисел. Умножитель повышенной разрядности можно получить из модулей меньшей разрядности, выстраивая, так называемую, рекурсивную декомпозицию операции умножения [5]. Например, для построения умножителя 8*8 бит можно использовать четыре модуля 4*4 и для формирования окончательного результата потребуются дополнительные сумматоры. Модули можно реализовать па ПЗУ. Тогда такие умножители называют таблично-алгоритмическими умножителями. Если дополнительные сумматоры встроены внутри модуля, то их называют множительно-суммирующими блоками (МСБ) [9].

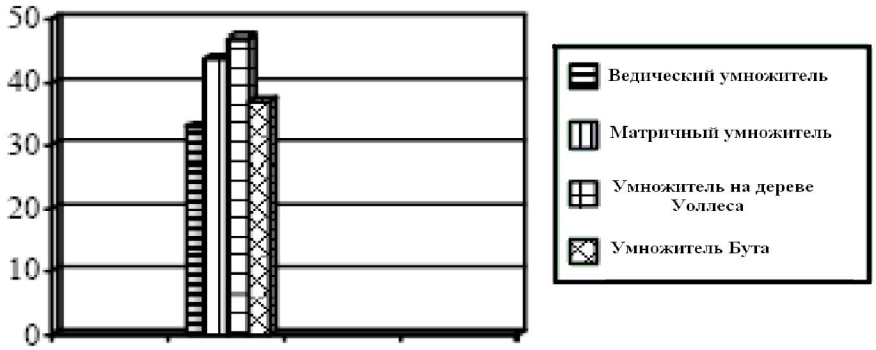

Рисунок 1. Диаграммы сравнения различных типов умножителей

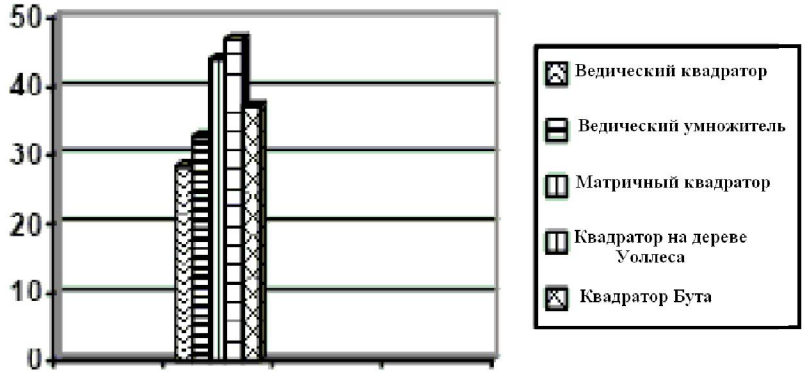

Рисунок 2. Диаграммы сравнения различных типов квадраторов

В матричных и древовидных умножителях заложен еще один потенциал производительности – возможность конвейеризации. При конвейерной организации процесс умножения разбивается на последовательность законченных этапов. Каждый из этапов умножения выполняется на своей ступени конвейера, причем все ступени работают параллельно. Результаты, полученные на i-ступени, передаются на дальнейшую обработку в (i+1) ступень конвейера. Передача информации со ступени на ступень происходит через буферную память, размещаемую между ними. Схема конвейера легко может быть применена к матричным и древовидным умножителям.

Рассмотренные выше различные подходы к реализации умножителей и квадраторов повышенной разрядности позволяют ускорить выполнение операций умножения и возведения в квадрат, которые являются базовыми операциями ассиметричных криптоалгоритмов.

Следующей базовой операцией асимметричных криптоалгоритмов является приведение по модулю P.

В работе [3] на основе выявленных характерных признаков были предложены следующие типы классификации устройств приведения по модулю:

- параллельные и последовательные;
- однотактные и многотактные;
- по наличию или отсутствию управляющего блока (в том числе микропрограммного);
- по используемой системе счисления.

На рисунке 3 приведена схема устройства приведения по модулю, где остаток определяется после формирования произведения двух чисел путем многократного вычитания модуля из исходного приводимого числа Z. Все вычитания реализуются на одном и том же узле. Устройство является последовательным (*), многотактным (**) циклическим, микропрограммным, используется двоичная система счисления. Операция производится над числами под управлением микропрограммы. В качестве Z может выступать произведение чисел Z=X*У или Z=X2. После приема в регистры РгZ и РгР соответственно операнда Z и модуля Р, они сравниваются на схеме сравнения (СС). Если при этом Z<P (X2=1), то в качестве результата на выход схемы выдается содержимое РгZ. При Z>=P из Z вычитается Р на сумматоре SM: с инверсных выходов РгР поступает –Р и на третий вход младшего разряда сумматора подается +1. При этом выполняется микрооперация РгZ:=РгZ+(-РгР)д.к., т.е. вычитание заменяется сложением (-Р) в дополнительном коде и остаток записывается в РгZ.

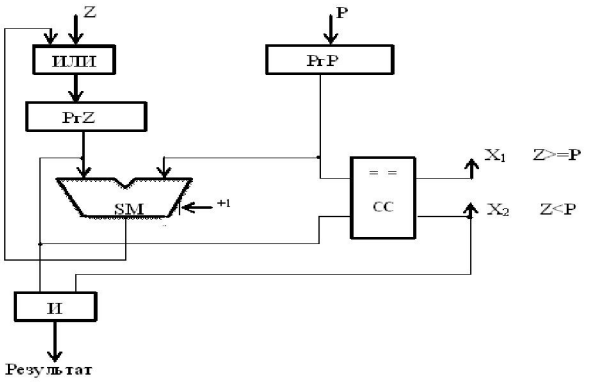

Рисунок 3. Схема приведения по модулю с последовательным вычитанием модуля

Затем новое значение РгZ сравнивается с содержимым РгР. И все циклически повторяется до тех пор, пока значение РгZ не станет меньше значения РгР (X2=1). Количество вычитаний зависит от соотношения чисел Z и Р. Например, при Р=33 и Z=1080, количество вычитаний составляет 32. Схема является оптимальной по аппаратным затратам, но медленнодействующей.

Для получения быстродействующего однотактного устройства приведения по модулю можно одновременно вычислять Z–P, Z-2P, Z-3P, Z-4P и т.д. Пусть Р=710=0001112 и Z=3310=1000012. Тогда целая часть от деления Z на P div=4 и необходимо выполнить следующие вычитания:

C1= Z - P =3310-710=0.1000012-0.0001112=0.1000012+1.111001=10.0110102=+2610;

C2= Z -2P =3310-1410=0.1000012-0.0011102=0.1000012+1.1100102=10.0100112= +1910;

C3= Z -3P =3310-2110=0.1000012-0.0101012=0.1000012+1.1010112=10.0011002= +1210;

C4= Z -4P =3310-2810=0.1000012-0.0111002=0.1000012+1.1001002=10.0001012=+510;

C5= Z -5P =3310-3510=0.1000012-0.1000112=0.1000012+1.0111012=01.1111102=--210.

Полученные значении C1÷C4 необходимо сравнивать с модулем Р и при Ci<P необходимо передать Ci на выход схемы в качестве результата приведения по модулю. Это требует включения в состав устройства одновременно работающих четырех схем сравнения. Для исключения четырех схем сравнения дополнительно вычисляется C5. Из примера видно, что при вычислении C1, C2, C3, C4 получен положительный результат. При этом из знаковых разрядов возникают переносы П1=П2=П3=П4=1. При вычислении C5 получается отрицательное число (–210) и перенос из знакового разряда П5=0. С помощью сигнала П5 имеется возможность значение C4, которое является результатом, передать на выход блока приведения по модулю.

Схема однотактного блока приведения по модулю, в котором используется данный подход, изображена на рис.4 [10]. Значение кратных Р (2P, 3P, 4P, 5P) формируются на формирователях (Ф2Р, Ф3Р, Ф4Р, Ф5Р). Для получения инверсных значении Р, 2P, 3P, 4P, 5P потребуются инверторы ИНВ1, ИНВ2, ИНВ3, ИНВ4, ИНВ5. Вычитание Z-iP производится на двоичных

сумматорах SM1÷SM5, на первые входы которых подается значение Z, а на вторые входы инверсные значения P, 2P, 3P, 4P, 5P.

В момент суммирования на младшие разряды сумматоров подается +1 (для получения дополнительного кода –P). По окончанию суммирования на выходе каждого сумматора формируются переносы П1, П2…П5 и остатки.

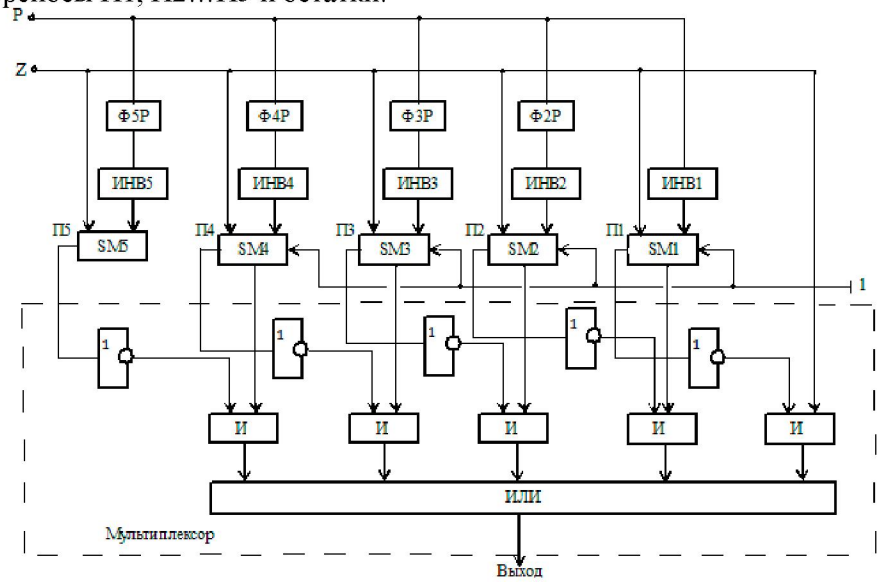

Рисунок 4. Схема однотактного блока приведения по модулю

Если остаток Ci= Z-iP>P, то Пi=1, иначе Пi=0. На выходе каждого сумматора SMi имеется схема, на входы которой подаются Ci, Пi и Пi+1. Инвертированный положительный сигнал Пi+1 разрешает прохождение на выход результат Ci при условии, что Пi=1. Для этого используются схемы И. Выходы схем И объединяются схемой ИЛИ и на ее выходе формируется значение остатка – результата приведения по модулю. Инверторы, схемы И, схема ИЛИ на выходе образуют мультиплексор. При P>Z на выходе SM1 сигнал П1=0 и соответственно через схему И0 значение Z передается на выход мультиплексора.

Данная схема является быстродействующей и очень эффективной при малых значениях соотношений Z и P. При больших соотношениях Z и P сложность схемы резко возрастает. Например, при Z=3020 и P=55, div=54. Для реализации блока приведения по модулю потребуется 54 схемы получения значение i*P и 55 двоичных сумматоров для выполнения операции Ci= Z-iP.

Анализ первой рассмотренной схемы приведения по модулю показывает, что схема очень проста и не требует больших аппаратных затрат, но быстродействие очень низкое. Вторая схема быстродействующая, но при этом аппаратные затраты очень высокие. Отсюда нетрудно заметить направление исследования по дальнейшему усовершенствованию блоков приведения по модулю .

В первой схеме необходимо увеличить быстродействие путем введения в состав блока аппаратной избыточности в разумных пределах, а во второй схеме необходимо минимизировать аппаратные затраты. Для этого необходимо разработать новые алгоритмы приведения по модулю и новые схемотехнические решения, реализующие эти алгоритмы.

ЛИТЕРАТУРА

[1] Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2012. 592 с.

[2] Рябко Б.Я, Фионов А.И. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004. 173 с.

[3] Айтхожаева Е.Ж., Тынымбаев С.Т. Аспекты аппаратного приведения по модулю в асимметричной криптографии. Журнал Вестник НАН РК, №5 (2014).- Алматы: Наука, 2014. С.88-93.

[4] Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. – СПб.: Профессионал, 2005. 490 с.

[5] Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. 2-е изд. -Спб.: Питер, 2011. 688 с.

[6] New Mou, Z.,Sutand F. Overturned stairs.Adder Trees and Multiplier Design. IEEE Transaction on Computers, c-41, Apr.1992. - pp 940-948.

[7] Sethi K., Panda R. An improved squaring circuits for binary numbers. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.3, No.2. 2012. pp. 111-116.
[8] Kumar A., Kumar D., Siddhi. Hardware Implementation of 16*16 bit Multiplier and Square using Vedic Mathematics. International Conference on Signal, Image and Video Processing (ICSIVP). 2012. pp.309-314.
[9] Угрюмов Е.П. Цифровая схемотехника. – СПБ.: БХВ – Петербург, 2005. – 800 с.
[10] Петренко В.И., Кузьминов Ю.В. Умножитель по модулю. Патент РФ RU 2299461. Бюллетень № 14. Опубликован 20.05.07.

REFERENCES

[1] Shan'gin V.F. M.: DMK Press, 2007. 592 s. (in Russ.).
[2] Ryabko B.Ya., Fionov A.I. M.: Nauchnyy Mir, 2004. 173 s. (in Russ.).
[3] Aithozhaeva E.Zh., Tynymbaev S.T. Jurnal Vestnik NAN RK, №5 (2014). Almaty: Nauka, 2014. (in Russ.). pp.88-93.
[4] Rostovtsev A.G., Makhovenko E.B. SPb.: Professional, 2005. 490 s. (in Russ.).
[5] TSil'ker B.Ya., Orlov S.A. SPb.: Piter, 2011. 688 s. (in Russ.).
[6] New Mou Z., Sutand F. IEEE Transaction on Computers, c-41, Apr.1992. pp. 940-948.
[7] Sethi K., Panda R. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.3,No.2, 2012. pp. 111-116.
[8] Kumar A., Kumar D., Siddhi. International Conference on Signal, Image and Video Processing (ICSIVP). 2012. pp.309-314.
[9] Ugrumov E.P. SPb.: BHV – Peterburg, 2005. 800 s. (in Russ.).
[10] Petrenko V.I., Kuz'minov U.V. Patent RF RU 2299461. Bulleten' № 14. Opublikovan 20.05.07 (in Russ.).

Асимметриялық криптоалгоритмдердегі базалық операцияларды аппараттық жүзеге асыру тәсілдері

Тынымбаев С.Т., Айтхожаева Е.Ж.

Тірек сөздер: шифрлаудың аппараттық жабдықтары, ассиметриялық криптоалгоритмдер, сандарды модуль бойынша дәрежесіне шығару.

Аннотация. Сандарды модуль бойынша дәрежесіне шығарудың базалық операцияларын (яғни бүтін сандық көбейтулерді және квадраттауды) орындаудың әртүрлі аппараттық әдестерін шапшаңдығы және аппараттық шығымдары бойынша салыстырмалы талдау жүргізілген. Сандарды модуль бойынша дәрежеге шығарудың ең сынды болып табылатын операциясын (яғни модульге келтіру) орындауға арналған құрылғылар талданған.

С.Т. ТЫНЫМБАЕВ профессор к.т.н., Е.Ж. АЙТХОЖАЕВА профессор к.т.н.
Казахский национальный технический университет им. К.И.Сатпаева, г. Алматы

Поступила 11.10.2014 г.