ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Սաղաթելյան Աննա Կարպիսի

ՄՈԴՈՒԼՅԱՐ ԹՎԱԲԱՆՈՒԹՅԱՆ ԲԼՈԿՈՒՄ ԹՎԱԲԱՆԱԿԱՆ ՍԱՐՔԵՐԻ ՆԱԽԱԳԾՄԱՆ ՄԵԹՈԴՆԵՐԻ ՄՇԱԿՈՒՄ ԵՎ ՀԵՏԱԶՈՏՈՒՄ

Ե 13.03 - «Հաշվողական մեքենաներ, համալիրներ, համակարգեր, ցանցեր, դրանց տարրերը և սարքավորումները» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման

ՍԵՂՄԱԳԻՐ

Երևան 2015

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Сагателян Анна Карписовна

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДОВ ПРОЕКТИРОВАНИЯ АРИФМЕТИЧЕСКИХ УСТРОЙСТВ В БЛОКЕ МОДУЛЯРНОЙ АРИФМЕТИКИ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.03– “Вычислительные машины, комплексы, системы, сети, их элементы и устройства”

Ереван 2015

Ատենախոսության թեման հաստատվել է Հայաստանի ազգային պոլիտեխնիկական համալսարանում (ՀԱՊՀ)

Գիտական ղեկավար՝ տ.գ.դ. Գ.Տ. Կիրակոսյան

Պաշտոնական ընդդիմախոսներ՝ տ.գ.դ., Ա.Թ. Քուչուկյան

ֆ.-մ.գ. թ. Վ.Ա. Վարդանյան

Առաջատար կազմակերպություն՝ ՍԻՆՈՓՍԻՍ ԱՐՄԵՆԻԱ ՓԲԸ

Ատենախոսության պաշտպանությունը տեղի կունենա 2015թ.դեկտեմբերի 8-ին, ժ.15:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 "Ինֆորմատիկա և հաշվողական համակարգեր" մասնագիտական խորհրդի նիստում, (հասցե՝ 0014, Երևան, Պ. Սևակի փ. 1):

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ -ի գրադարանում:

Սեղմագիրն առաքված է 2015թ. նոյեմբերի 7-ին:

037 Մասնագիտական խորհրդի
գիտական քարտուղար, ֆ.-մ.գ. դ. Հ.Գ. Սարուխանյան

Тема диссертации утверждена в Национальном политехническом университете Армении (НПУА)

Научный руководитель: д.т.н. Г.Т. Киракосян

Официальные оппоненты: д.т.н. А.Т. Кучукян

к.ф.-м.н. В.А. Варданян

Ведущая организация: "СИНОПСИС АРМЕНИЯ" ЗАО

Защита диссертации состоится 8 декабря 2015г. в 15:00 часов на заседании Специализированного совета 037 "Информатика и вычислительные системы" в Институте проблем информатики и автоматизации НАН РА (адрес: 0014, г. Ереван, ул. П. Севака 1).

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.

Автореферат разослан 7-го ноября 2015г.

Ученый секретарь
Специализированного совета 037, д.ф.-м. н. А.Г. Саруханян

ԱՇԽԱՏԱՆՔԻ ՀԱՄԱՌՈՏ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Թեմայի արդիականությունը: Ատենախոսությունը նվիրված է մոդուլյար թվաբանության կիրառմամբ բարդ ֆունկցիոնալ բլոկների (ԲՖ բլոկներ) նախագծման մեթոդների մշակմանը և հետազոտմանը:

Թվային սարքերին միշտ ներկայացվում են արագագործության բարձրացման պահանջներ, որոնք կարելի է նաև իրականացնել մոդուլյար թվաբանության օգնությամբ: Մոդուլյար թվաբանության մնացորդների հետ գործողությունների զուգահեռ կատարման շնորհիվ հնարավորություն է տալիս էականորեն բարձրացնել թվաբանական հաշվարկների արագագործությունը:

Մասնագիտացված թվային սարքերի նախագծման արտադրողականության բարձրացման հիմնական մեթոդներից է ԲՖ բլոկների բազմակի օգտագործումը, ուստի թվային սարքերի ապարատային իրագործման նոր մեթոդների որոնումը արդիական գիտատեխնիկական խնդիր է: Ատենախոսությունը նվիրված է հենց այդ արդիական խնդրին՝ մոդուլյար թվաբանության բլոկի կիրառմամբ թվային ԲՖ բլոկների նախագծման մեթոդների հետազոտմանը և մշակմանը:

Հետազոտման օբյեկտը: Հետազոտման օբյեկտը մոդուլյար թվաբանական բլոկում թվաբանական սարքերի նախագծման մեթոդներն են, ԲՖ բլոկների օգնությամբ սինթեզման արդյունքում դրանց վերլուծությունը, համեմատումը և գնահատումը, ինչպես նաև մասնագիտացված մոդուլյար թվային սարքերի կառուցվածքի մոդելավորման ալգորիթմական և ծրագրային ապահովման միջոցները:

Աշխատանքի նպատակը և խնդիրները: Ատենախոսության նպատակն է՝ հետազոտել և մշակել մոդուլյար թվաբանության բլոկում մասնագիտացված ԲՖ բլոկների միջոցով նախագծման մեթոդները և միավորել դրանք մեկ ավտոմատացված համակարգում, որի օգնությամբ հնարավոր է իրականացնել թվային սարքերի օպտիմալ կառուցվածքների մոդելավորում, սիմուլյացիա, սինթեզում և գնահատում:

Նշված նպատակին հասնելու համար ձևակերպվել և լուծվել են հետևյալ խնդիրները.

- Հետազոտել թվային սարքերի նախագծման ժամանակակից մեթոդները և դրանց կիրառման առանձնահատկությունները:
- Մշակել տարբեր մեթոդներով մոդուլյար գումարիչների, բազմապատկիչների և մոդուլով աստիճան բարձրացնելու սարքերի ԲՖ բլոկների միջոցով ապարատային իրականացումները, ինչպես նաև գնահատել դրանց արագագործությունը և ապարատային ծախսերը:
- Վերլուծել մոդուլյար ԲՖ բլոկների կառուցվածքները՝ կախված մոդուլի արժեքից և կիրառման ոլորտից:

- Մշակել մոդուլյար թվաբանության բլոկում մասնագիտացված ԲՖ բլոկների միջոցով նախագծման մեթոդների միավորված ավտոմատացված համակարգը:

<u>Հետազոտման մեթոդները</u>: Ատենախոսությունում օգտագործվել են թվային սարքերի կառուցվածքների մշակման տեսական և գործնական մեթոդները և գործիքամիջոցները: Որպես հետազոտության հիմնական բազա՝ օգտագործվել են մոդուլյար թվային սարքերի նախագծման տեխնոլոգիաների վերաբերյալ հրատարակված գիտական և մասնագիտական աշխատանքները:

<u>Գիտական նորույթը:</u> Հետազոտության արդյունքում ստացվել են հետևյալ գիտական արդյունքները.

- Մշակվել են տարբեր մեթոդներով մոդուլյար գումարիչների, բազմապատկիչների և մոդուլով աստիճան բարձրացնելու թվային սարքերի ԲՖ բլոկների միջոցով ապարատային իրականացումները:
- Գնահատվել են նախագծված մասնագիտացված մոդուլյար թվային սարքերի արագագործությունը և ապարատային ծախսերը՝ կախված մուտքային թվերի ու մոդուլի արժեքի կարգայնությունից:
- Առաջարկվել են մոդուլյար թվաբանության բլոկում թվաբանական սարքերի նախագծման օպտիմալ մեթոդի ընտրության մոտեցումները:
- Մշակվել է մոդուլյար թվաբանության բլոկում մասնագիտացված թվային սարքերի ԲՖ բլոկների միջոցով նախագծման մեթոդների միավորված ավտոմատացված համակարգը:

<u>Պաշտպանության ներկայացվում են հետևյալ արդյունքները</u>.

1. Մոդուլյար գումարիչների կառուցման տարբեր մեթոդներ և այդ մեթոդների կիրառման արդյունավետությունը՝ կախված մուտքային թվերի և մոդուլի արժեքի կարգայնությունից:
2. Մոդուլյար բազմապատկիչների կառուցման տարբեր մեթոդներ և այդ մեթոդների կիրառման արդյունավետությունը՝ կախված մուտքային թվերի և մոդուլի արժեքի կարգայնությունից:
3. Մոդուլով աստիճան բարձրացումը իրականացնող սարքերի կառուցման տարբեր մեթոդներ և այդ մեթոդների կիրառման արդյունավետությունը՝ կախված մուտքային թվերի և մոդուլի արժեքի կարգայնությունից:
4. Մոդուլյար թվաբանության բլոկում մասնագիտացված թվային սարքերի ԲՖ բլոկների միջոցով նախագծման մեթոդների միավորված ավտոմատացված համակարգը:

<u>Գիտական հիմնադրույթների հավաստիությունը</u> պայմանավորված է տեսական, հետազոտական և ժամանակակից վերլուծության մեթոդներով, օգտագործված և մշակված մաթեմատիկական ու ծրագրային ապահովմամբ, ինչպես նաև գործնական կիրառման արդյունքներով:

Աշխատանքի գործնական արժեքը և ներդրումը: Ատենախոսությունում ստացված արդյունքները կարող են կիրառվել մասնագիտացված բարդ թվային սարքերի (ազդանշանների թվային մշակման, գաղտնագրման և կոդերի հսկման համակարգերը), ինչպես նաև մոդուլյար թվաբանության վրա հիմնված այլ թվային սարքերի նախագծման համար:

Մշակված մեթոդների կիրառումը հնարավորություն կընձեռի բարձրացնել մասնագիտացված բարդ թվային սարքերի և համակարգերի նախագծման արդյունավետությունը, ինչպես նաև զգալիորեն կկրճատի գործողությունների կատարման ժամանակային ծախսերը:

Մշակված RSA ալգորիթմով գաղտնագրման մասնագիտացված բարդ թվային սարքը ներդրվել և օգտագործվել է "Երևանի կապի միջոցներ" ԳՀ ՓԲԸ–ում և "Ֆեմբոքս" ՍՊԸ-ում, իսկ "Ծրագրավորվող տրամաբանական սարքեր" մեթոդական ցուցումներով մշակվել են լաբորատոր աշխատանքներ և ներդրվել ՀԱՊՀ Քոմփյութերային համակարգեր և ցանցեր ամբիոնում:

Աշխատանքի ապրոբացիան: Ատենախոսության հիմնական գիտական ու կիրառական դրույթները և արդյունքները զեկուցվել ու քննարկվել են ՀԱՊՀ տարեկան գիտաժողովներում (2010թ., 2012թ., 2014թ.), ՀԱՊՀ-ի ՔՀևՑ ամբիոնի գիտական սեմինարներում (2012թ., 2013թ., 2014թ., 2015թ.):

Հրապարակումները: Ատենախոսության հիմնական դրույթները տպագրվել են յոթ գիտական հոդվածներում, որոնք բերված են սեղմագրի վերջում:

Ատենախոսության կառուցվածքը և ծավալը: Աշխատանքը բաղկացած է ներածությունից, 4 գլխից, հիմնական արդյունքներից 107 անուն օգտագործված գրականության ցանկից և 4 հավելվածից:

Աշխատանքի ընդհանուր ծավալը 142 էջ է և ներառում է 42 նկար և 10 աղյուսակ: Աշխատանքը գրված է հայերեն լեզվով:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածությունում հիմնավորվել է թեմայի արդիականությունը, ձևակերպվել են ատենախոսական աշխատանքի հիմնական նպատակը, խնդիրները, գիտական նորույթը, պաշտպանության ներկայացված հիմնական դրույթները և կիրառական նշանակությունը:

Առաջին գլուխը նվիրված է մոդուլյար թվաբանության բլոկում թվային սարքերի նախագծման ժամանակակից մեթոդների և գործիքամիջոցների հետազոտմանը և վերլուծությանը, մոդուլյար թվաբանության հիմնադրույթների, հիմնական օրենքների և սկզբունքների հետազոտմանը, ինչպես նաև դիտարկված մեթոդների, դրանց հիման վրա նախագծվող թվային սարքերի կիրառման ոլորտներին և զարգացման ուղղություններին: Հետազոտման արդյունքում բացահայտվել են մոդուլյար թվաբանության բլոկի առավելությունները և թերությունները: Առանձին դիտարկվել են թվային սարքերի նախագծման

ժամանակակից գործիքամիջոցները և կիրառման առանձնահատկությունները, ժամանակակից ինտեգրալային սխեմաների բազան, որի կիրառմամբ մշակվել և նախագծվել են մոդուլյար թվաբանության բլոկում թվաբանական սարքերը, վերլուծվել և համակարգվել են ինտեգրալային սխեմաների նախագծման մոտեցումներն ու առկա մեթոդները:

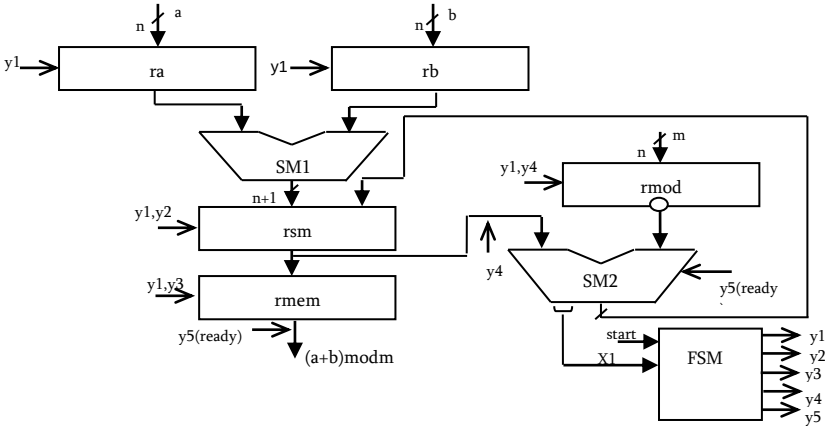
Երկրորդ գլխում մշակվել են մոդուլյար թվաբանության բլոկում թվաբանական սարքերի (գումարիչներ, բազմապատկիչներ, աստիճան բարձրացման գործողություն կատարող սարք) կառուցման և նախագծման նոր մեթոդներ:

Մշակված մոդուլյար գումարիչի սխեման գերադասելի է մոդուլի մեծ արժեքների դեպքում, բացի դրանից, եթե նախագծումն իրագործվում է FPGA-ների (Field-Programmable Gate Array) օգնությամբ, ապա վերջիններս ունեն սահմանափակ քանակով ներկառուցված տրամաբանություն և անհամեմատ ավելի շատ քանակով տրիգերներ, հետևաբար ղեկավարող ավտոմատի առկայությունը նույնպես առավելություն է:

Առանց LUT (Look-Up-Table) աղյուսակի օգտագործման մոդուլյար գումարման թվային սարքի կառուցվածքային սխեման, ըստ արտահայտություն (1)-ի, որտեղ օգտագործվում է արդյունքի ընտրման համար մուլտիպլեքսոր և 2 գումարիչ, համալրված է ղեկավարող ազդանշաններով (նկ. 1):

$$(a+b)\text{mod}m = \begin{cases} (a+b), & 0 \le a+b \le m, \\ a+b - km, & a+b > m, \end{cases} \qquad (1)$$

որտեղ $k = 1, 2, 3, \ldots, (a+b)/m$:

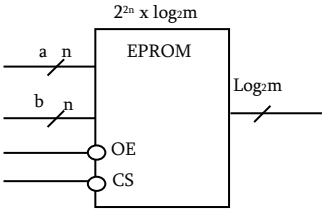


Նկ.1. Մոդուլյար գումարման սարքի կառուցվածքային սխեման:

Կատարվել է տարբեր մեծության թվերի և առանձին մոդուլների կիրառմամբ մոդուլյար գումարիչների կառուցման մշակված մեթոդների համեմատական վերլուծություն: Մշակվել են նաև 2^n+1 և 2^n-1 մոդուլներով

արագագործ մոդուլյար գումարիչներ, որոնք առաջարկվում է նախագծել՝ կիրառելով երկուական լուծումների դիագրամների տեխնոլոգիան, որը լայնորեն կիրառվում է մոդուլյար թվաբանության բլոկում թվային սխեմաների կառուցման համար:

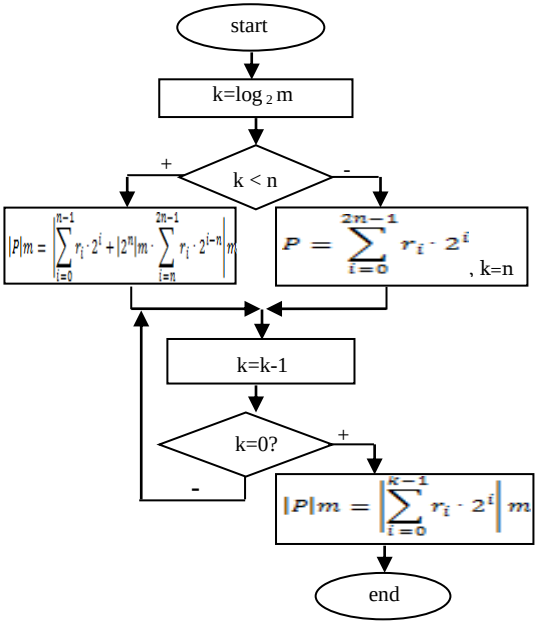
Մշակված են նաև մոդուլյար բազմապատկիչների նախագծման նոր մեթոդներ, որոնք մասամբ հիմնված են նախագծման առկա մեթոդների վրա (օրինակ՝ ինդեքսային մեթոդի հիման վրա), $m=2^k$ մոդուլով մոդուլյար բազմապատկիչներ և Բուտի ալգորիթմի ու դիրքային բազմապատկիչի հիման վրա $(2^n\pm1)$ մոդուլների համար բազմապատկման սարքեր:



Նկ. 2. EPROM-ի միջոցով մոդուլյար բազմապատկիչի իրագործումը:

Մշակված թվային սխեման (նկ. 2.) հնարավորություն է տալիս ստանալ (axb) mod m արտահայտության արժեքը EPROM (Erasable Programmable Read-Only-Memory) տիպի հիշող սարքի միջոցով:

Ատենախոսությունում մշակվել է մոդուլյար բազմապատկիչներ, երբ մոդուլի արժեքը հավասար է 2^k,: $m=2^k$ մոդուլով մոդուլյար բազմապատկիչների կառուցման համար կարող է օգտագործվել այն մոտեցումը, որը հիմնված է մոդուլյար թվաբանության և դասական բուլյան հանրահաշվի հատկությունների միավորման վրա: Շնորհիվ մոդուլյար թվաբանության հատկանիշների, 2^k մոդուլով մոդուլյար բազմապատկիչների իրագործումը կարելի է իրականացնել ատենախոսությունում մշակված ալգորիթմով (նկ. 3):

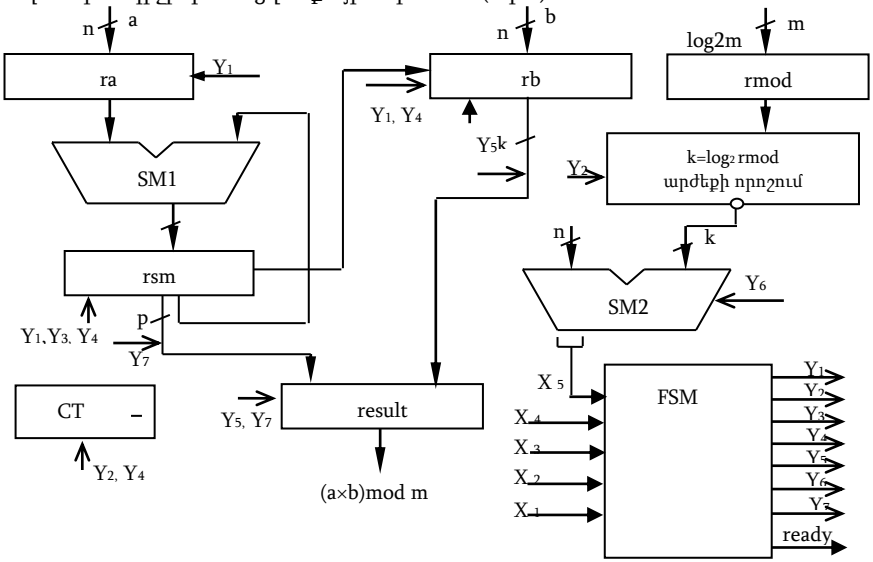


Նկ. 3. $m=2^k$ մոդուլով բինար մեթոդով մոդուլյար բազմապատկման ալգորիթմի բլոկ-սխեման:

Երկու դրական a և b թվերի P=a×b արտադրյալը ներկայացվում է երկուական թվաբանության հայտնի բանաձևով (2), որտեղ r_i –ն a և b թվերի բազմապատկման i-րդ բիթն է:

$$P = \sum_{i=0}^{2n-1} r_i \cdot 2^i \qquad (2)$$

Համաձայն ալգորիթմի բլոկ-սխեմայի՝ $m=2^k$ մոդուլով մոդուլյար բազմապատկիչը a և b դրական թվերի սովորական երկուական բազմապատկիչն է, որից որպես վերջնական արժեք՝ վերցված են ընդհանուր P=axb արտադրյալի ցածր k բիթերը: Նկ. 3-ում պատկերված ալգորիթմի հիման վրա ատենախոսությունում մշակված է $m=2^k$ մոդուլով մոդուլյար բազմապատկիչի կառուցվածքային սխեման (նկ. 4)

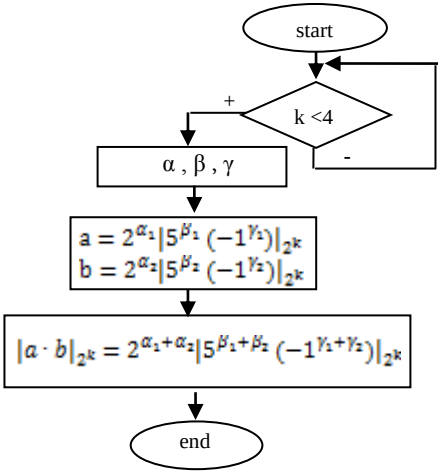


Նկ. 4. 2^k մոդուլով մոդուլյար բազմապատկիչի կառուցվածքային սխեման:

Հարկ է նշել, որ $m=2^k$ մոդուլով մոդուլյար բազմապատկիչները կարող են կիրառվել նաև $m=2^k+1$ և $m=2^k-1$ մոդուլներով կոդերի հսկում իրականացնող մասնագիտացված սարքերում, իսկ այն մասնավոր դեպքերում, երբ $m=2^k+1$ և $m=2^k-1$ պարզ թվեր են (օրինակ՝ $2^4+1=17$, $2^8+1=257$, $2^5-1=31$, $2^8-1=127$ և այլն), ապա այդպիսի բազմապատկիչները կարող են կիրառվել նաև որոշ ալգորիթմներով (RSA գաղտնագրման, Դիֆֆի-Հելլմանի գաղտնագրման բանալիների գեներացման ալգորիթմներ) գաղտնագրման սարքերի կառուցման դեպքում:

2^k մոդուլով մոդուլյար բազմապատկման թվային սարքի իրականացումը նույնպես հնարավոր է, եթե k>3, մոդուլյար թվաբանության հայտնի ինդեքսային մեթոդով, արտահայտություն 3-ի կիրառմամբ

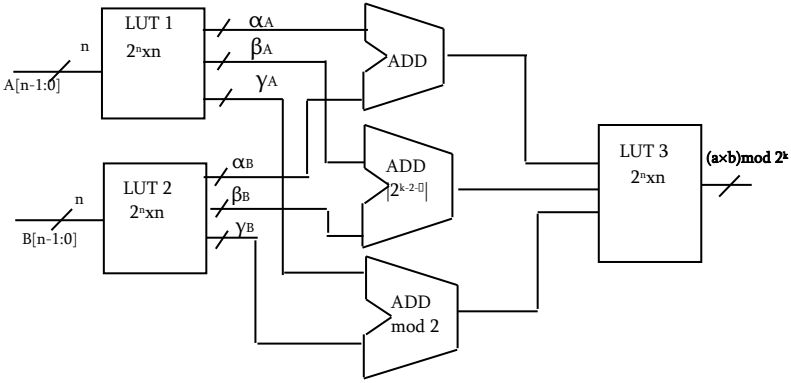
$$a = 2^{\alpha} |5^{\beta} (-1^{\gamma})|_{2^k} \qquad (3)$$



Նկ. 5. $m=2^k$ մոդուլով մոդուլյար բազմապատկման ալգորիթմի բլոկ-սխեման:

Ցանկացած $k>3$ պայմանին բավարարող k թվի համար $\pm5^1$, $\pm5^2$, $\pm5^2$,....,$\pm5^{k-2}$ ամբողջ թվերը հանդիսանում են 2^k մոդուլով բոլոր մնացորդները: Այսինքն, ցանկացած a կենտ թիվ $A\in[1, 2^k -1]$ միջակայքից կարելի է ներկայացնել մոդուլյար ինդեքսային ձևով, (α, β, γ) ինդեքսների եռյակի միջոցով: Ատենախոսությունում մշակվել 2^k մոդուլով ինդեքսային մեթոդով մոդուլյար բազմապատկման ալգորիթմի բլոկ-սխեման պատկերված է նկ. 5-ում:

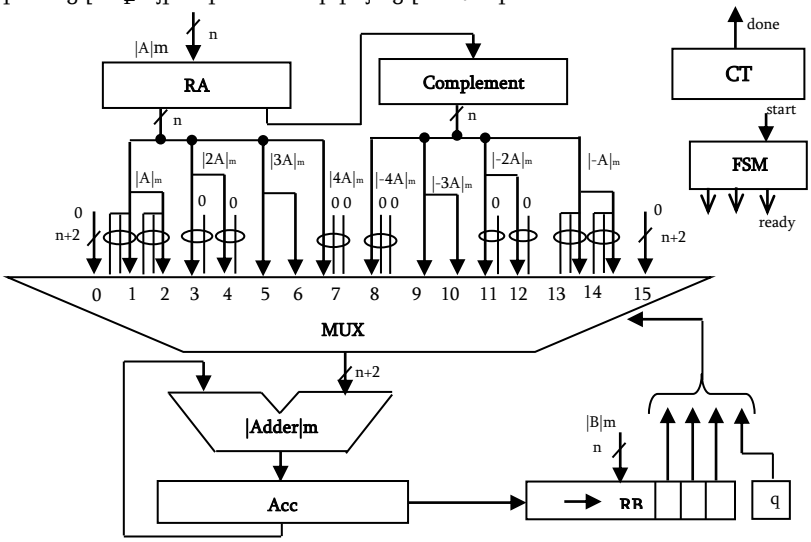
Վերոհիշյալ ալգորիթմի հիման վրա մշակվել է LUT աղյուսակների կրառմամբ $m=2^k$ մոդուլով ինդեքսային մեթոդով մոդուլյար բազմապատկիչի կառուցվածքային սխեման, պատկերված նկ. 6-ում:



Նկ. 6. 2^k մոդուլով ինդեքսային մեթոդով մոդուլյար բազմապատկիչի սխեման:

Ատենախոսությունում մշակվել է Բուտի ալգորիթմի հիման վրա մոդուլյար բազմապատկիչների նախագծման մեթոդ, երբ մասնակի արտադրյալները որոշվում են ոչ թե կոմբինացիոն կամ ծառանման բազմապատկիչների (կախված թվերի կարգայնությունից) միջոցով, այլ Բուտի վերակոդավորման գործողություններից հետո մասնակի արտադրյալների գումարը իրականացվում է մոդուլյար գումարիչների միջոցով: Բազմապատկումը կատարվում է n տակտերի ընթացքում, որտեղ n-ը բազմապատկիչի կարգերի քանակն է:

Մշակված Բուտի մոդիֆիկացված ալգորիթմով (չորս բիթերի վերլուծությամբ) մոդուլյար բազմապատկման թվային սարքի նախագծված կառուցվածքային սխեման ներկայացված է նկ. 7-ում:



Նկ. 7. Բուտի մոդիֆիկացված ալգորիթմով (չորս բիթի վերլուծությամբ) մոդուլյար բազմապատկման սարքի կառուցվածքային սխեմա:

Բուտի մոդիֆիկացումներով (Radix4, Radix 8, Radix 16 և Radix 32) նախագծված թվային սարքերի արագագործությունը և ապարատային ծախսերը բերված են աղյ. 1-ում:

Աղյուսակ 1. Բուտի մոդիֆիկացումներով թվային սարքերի արագագործությունը և ապարատային ծախսերը:

Մոդիֆի-կացում	Արագագոր-ծություն	Ապարատային ծախսեր		
Radix 4	n տակտ	1 հատ 4_1MX	n կարգ. հաշվիչ	n+1 կարգ. Գումարիչ
Radix 8	n/2 տակտ	1 հատ 8_1MX	n/2 կարգ. հաշվիչ	n+2 կարգ. Գումարիչ
Radix 16	n/3 տակտ	1 հատ 16_1MX	n/3 կարգ. հաշվիչ	n+3 կարգ. Գումարիչ
Radix 32	n/4 տակտ	1 հատ 32_1MX	n/4 կարգ. հաշվիչ	n+4 կարգ. Գումարիչ

Եթե բազմապատկման գործողությունը իրականացնենք նույն ալգորիթմներով հաջորդող բաժանման գործողությամբ, և ոչ թե մոդուլյար բլոկում, ապա բազմապատկումից (2n տակտ միայն բազմապատկման համար) հետո բաժանման գործողությունը կատարվում է.

- 2n-m տակտ՝ նորմալացման համար,
- 2n-m+1 տակտ՝քանորդի կարգերի որոշման համար,

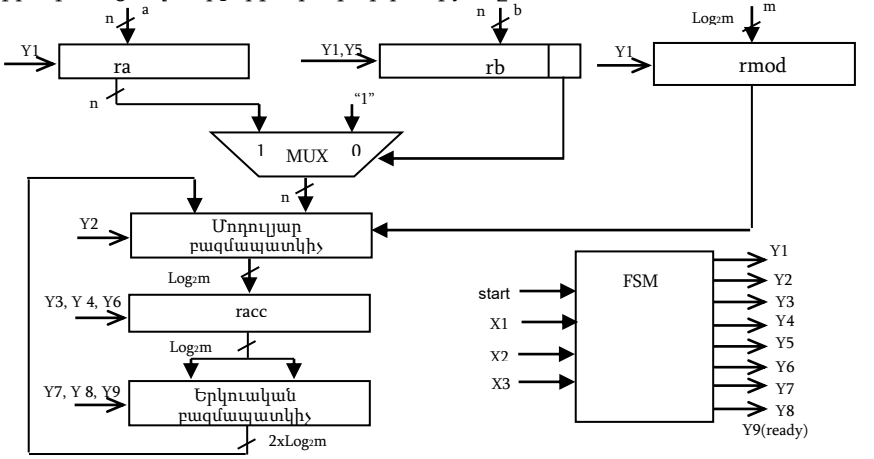
- 2n-m տակտ՝ վերջմնական մնացորդի տեղաշարժի համար, հետևաբար զուտ բաժանման գործողության վրա ծախսվում է 3n-3m+1 ժամանակ:

Բուտի ալգորիթմի մոդիֆիցացումների հիման վրա մոդուլյար թվաբանության բլոկում նախագծված և երկուական թվաբանությունում առկա թվային սարքերի արագագործությունների արդյունքները ներկայացված են աղյ. 2-ում:

Աղյուսակ 2: Բուտի մոդիֆիկացված ալգորիթմների մոդուլյար և երկուական թվաբանություններում սարքերի արագագործությունը:

	Բուտի ալգորիթմի մոդիֆիկացումները			
	Radix 4	Radix 8	Radix 16	Radix 32
Մոդուլյար բլոկում Բուտի ալգորթմով նախագծված բազմապատկիչներ	n տակտ	n/2 տակտ	n/3 տակտ	n/4 տակտ
Բուտի ալգորիթմով բազմապատկում և հաջորդող բաժանում	2n +6n-3m +1	n/2+6n-3m +1	n/3+6n-3m +1	n/4+6n-3m +1

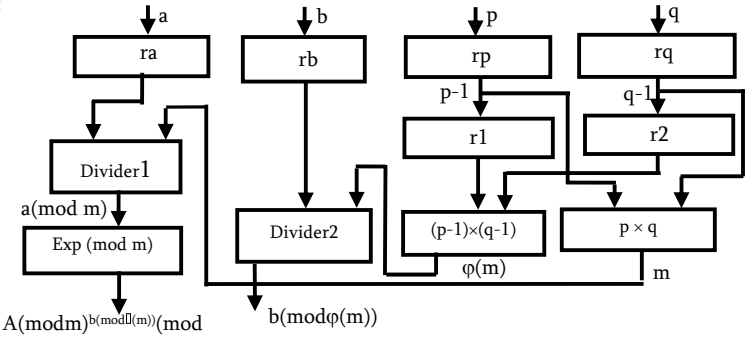
Աղյ. 2-ում բերված արդյունքների համեմատությունը ցույց է տալիս, որ բոլոր մոդիֆիկացումների համար մոդուլյար թվաբանության բլոկում Բուտի ալգորիթմով նախագծված բազմապատկիչների արագագործությունը գերազանցում է Բուտի ալգորիթմով բազմապատկում և հաջորդող բաժանում իրականացնող սարքերի արագագործությունը:



Նկ. 8. "Քառակուսի բարձրացման - բազմապատկման" ալգորիթմի աստիճան բարձրացնելու թվային սարքի կառուցվածքային սխեմա:

Ատենախոսությունում մշակված են տարբեր ալգորիթմներով աստիճան բարձրացման գործողություն կատարող թվային սարքերի նախագծման մեթոդներ, այդ սարքերից մեկի կառուցվածքային սխեման ներկայացված է նկ. 8-ում, որտեղ բազմապատկիչների և հաջորդող բաժանման թվային սարքերի փոխարեն կիրառվել է նախագծված մոդուլյար բազմապատկիչ:

Էյլերի ֆունկցիայի կիրառմամբ մոդուլով աստիճան բարձրացնելու թվային սարքի նախագծված կառուցվածքային սխեման ներկայացված է նկ. 9-ում: Տվյալ մշակված մեթոդով նախագծման դեպքում մեծանում է թվային սարքի արագագործությունը մուտքային թվերի կարգայնության փոքրացման հետևանքով, քանի որ և աստիճանը հաշվարկվում է մոդուլ φ(m)-ով, իսկ արդյունքը՝ մոդուլ m-ով:



Նկ. 9. Էյլերի ֆունկցիայի կիրառմամբ մոդուլով աստիճան բարձրացնելու թվային սարքի կառուցվածքային սխեմա:

Երրորդ գլխում զետեղված են բոլոր մեթոդներով մշակված թվային սարքերի ISE Design Suite ավտոմատ նախագծման համակարգի միջոցով ստացված սինթեզման արդյունքների վերլուծությունները Spartan-3E ընտանիքի FPGA-ի օգտագործմամբ: Վերլուծությունը կատարվել է FPGA-ում սինթեզված տեխնոլոգիական սխեմաներում LUT աղյուսակների քանակի, FPGA-ի սեկցիաների (Slice-րի) օգտագործման տեսակետից, և ձևավորվել են առաջարկներ՝ կախված մուտքային թվերի և մոդուլի արժեքի կարգայնություններից նախագծման նախընտրելի մեթոդի ընտրման նպատակով:

Նախագծված թվային սարքերի սինթեզման հաշվետվութան օրինակը ներկայացված է աղյ. 3-ում:

Աղյուսակ 3: Նախագծված թվային սարքերի սինթեզման հաշվետվություն:

N	Օգտագործված տրամաբանություն	FPGA ռեսուրսների օգտագործման հաշվետվություն				
		n=8	n=16	n=32	n=64	
		Used	Used	Used	Used	Ընդ.
1.	Քառամուտք LUT-ի քանակ	20	34	58	77	9312
2.	Օգտագործ. սեկցիաների (Slices) քանակ	18	22	36	41	4656
3.	Կապակցված տրամ. պարունակող սեկցիաների քանակ	10	10	10	10	10
4.	Օգտագործ.մուտք/ելքերի (IOBs) քանակ	24	48	80	136	190
5.	Արագագործություն	25 նվ	25 նվ	25 նվ	25 նվ	

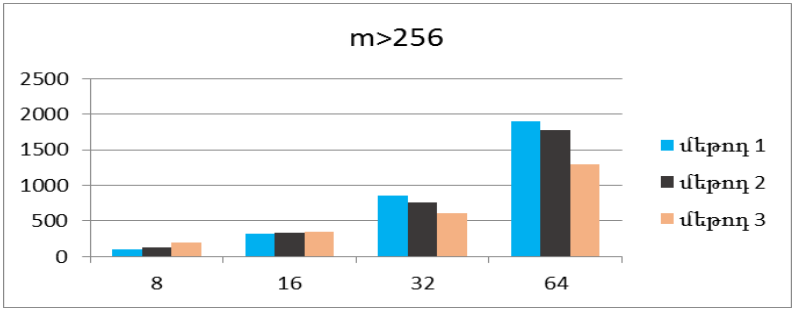
Գնահատումը կատարվել է ոչ միայն ապարատային ծախսերի այլ նաև արագագործության տեսակետից: Մասնագիտացված թվային սարքերի սինթեզ-

ման համար ընտրվել է սինխրոազդանշանի գեներացման ժամանակը՝ 5 նվ, այսինքն՝ Verilog նկարագրումը՝ always #5 clk=~clk: Արագագործությունը գնահատվել է սինթեզվող սարքի աշխատանքի սիմուլյացիայի ժամանակ, որն իրականացվել է ModelSim (Mentor Graphics) փաթեթի միջոցով:

Որպես օգտագործված ռեսուրսներ դիտարկվել են.

- Քառամուտք LUT-աղյուսակները, որոնց ընդհանուր քանակը Spartan-3E FPGA-ում 9312 հատ է: Դիտարկվել է n=8, n=16, n=32 և n=64 կարգանի a և b թվերի գումարման սարքի սինթեզման համար օգտագործված LUT-րի քանակը:
- Օգտագործված սեկցիաները, որոնց ընդհանուր քանակը նույն FPGA-ում 4656 հատ է: Դիտարկվել է նույն սկզբունքով օգտագործված քանակը:
- Կապակցված տրամաբանություն պարունակող սեկցիաներy (Slices), որոնց ընդհանուր քանակը Spartan-3E FPGA-ում 10 հատ է: Դիտարկվել է նույն սկզբունքով օգտագործված քանակը:
- Օգտագործված մուտք/ելքերը, որոնց ընդհանուր քանակը նույն FPGA-ում 190 հատ է: Դիտարկվել է նույն սկզբունքով օգտագործված քանակը:

Աղյ. 3-ից երևում է, որ անկախ a և b թվերի կարգայնությունից մասնագիտացված թվային սարքի արագագործությունը 25նվ է: Այդ արդյունքները ընդհանրացված տեսքով կարելի է ներկայացնել նաև կախվածությունների գրաֆիկի տեսքով (նկ. 10), որտեղ ներկայացված է FPGA ընդհանրացված ռեսուրսների քանակի կախվածությունը օպերանդների կարգայնությունից (n=8, n=16, n=32 և n=64): Տվյալ գրաֆիկը ներկայացնում է FPGA–ի օգտագործված բոլոր տեսակի ռեսուրսների գումարային քանակը՝ կախված թվերի կարգայնությունից, m մոդուլի արժեքը [256 : 1023] միջակայքում:



Նկ. 10. Մոդուլար գումարիչների նախագծման մեթոդների ներկայացումը գրաֆիկի միջոցով, m-ը պատկանում է [256, 1023] միջակայքին:

Գնահատելով սինթեզման արդյունքները, կախված մոդուլի արժեքի մեծությունից և թվերի կարգայնությունից FPGA-ի ռեսուրսների օգտագործման տեսակետից, կարելի է եզրակացնել, որ.

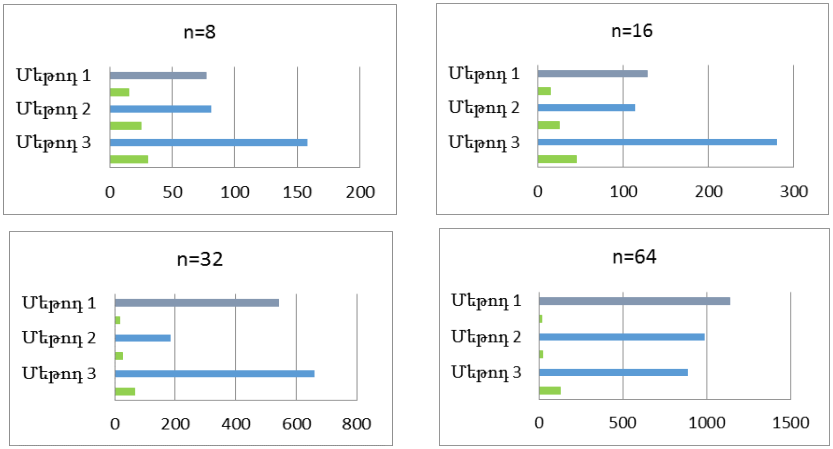
- 1-ին սկզբունքով մոդուլյար գումարիչները նախընտրելի է կառուցել a և b թվերի n<16 կարգայնության և m մոդուլի արժեքի [0 : 255] միջակայքի դեպքում:
- 2-րդ սկզբունքով մոդուլյար գումարիչները նախընտրելի է կառուցել a և b թվերի n>16 կարգայնության և m մոդուլի արժեքի [0 : 255] միջակայքի դեպքում:
- 3-րդ սկզբունքով մոդուլյար գումարիչները նախընտրելի է կառուցել a և b թվերի n>16 կարգայնության և m մոդուլի արժեքի [256 : 1023] միջակայքի դեպքում:

Գնահատելով սինթեզման արդյունքները՝ առաջարկվում է մոդուլյար սարքերի նախագծման արդյունավետ մեթոդ FPGA-ի ռեսուրսների օգտագործման և այդ սարքի աշխատանքի արագագործության տեսակետից: Գնահատումները կատարվել են հետազոտությունների արդյունքում ձևավորված և փորձնականորեն ստացված հետևյալ բանաձևի հիման վրա՝

$$G = \sum_{i=0}^{5} R_i \cdot T, \qquad (4)$$

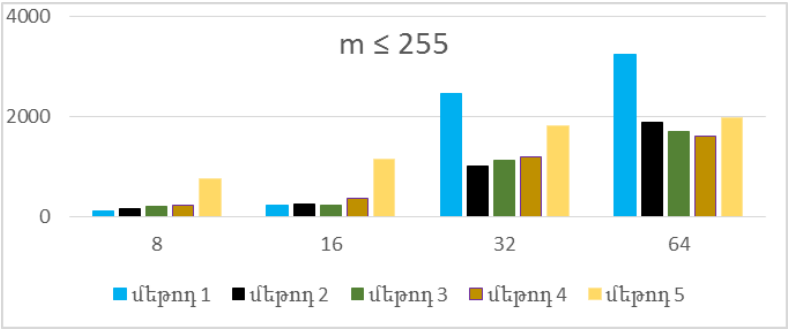
որտեղ G-ն՝ արդյունավետության հայտանիշն է, Ri-ն FPGA-ի բոլոր օգտագործված ռեսուրսները, T-ն՝ սարքի արագագործությունը,:

Նկ. 11-ում ներկայացվել են FPGA ռեսուրսների օգտագործման և մասնագիտացված թվային սարքի արագագործության գնահատումները մոդուլյար գումարիչների նախագծման երեք մեթոդի համար n=8, n=16, n=32 և n=64 կարգայնության թվերի դեպքում:

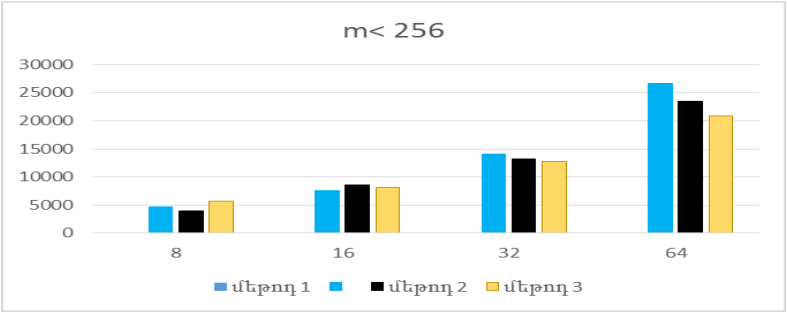


Նկ. 11. Մոդուլյար գումարիչների նախագծման մեթոդների ներկայացումը գրաֆիկի միջոցով, m-ը պատկանում է [256, 1023] միջակայքին:

Նմանատիպ արդյունքներ ստացվել է նաև մոդուլյար բազմապատկիչների (նկ.12) և մոդուլով աստիճան բարձրացնելու սարքերի սինթեզման (նկ. 13) արդյունքները, եթե m մոդուլի արժեքը [0: 255] միջակայքում է:



Նկ.12. Մոդուլյար բազմապատկիչների նախագծման մեթոդների ներկայացումը գրաֆիկի միջոցով, m-ը պատկանում է [0, 255] միջակայքին:



Նկ.13. Մոդուլով աստիճան բարձրացնելու սարքերի նախագծման մեթոդների ներկայացումը գրաֆիկի միջոցով, m-ը պատկանում է [0, 255] միջակայքին:

Մոդուլյար թվաբանության բլոկում թվաբանական սարքերի նախագծման մեթոդների հետազոտման արդյունքների հիման վրա նախագծվել է ModSystem ավտոմատացված երկխոսային բաց համակարգը: ModSystem ավտոմատացված համակարգի նախագծման համար առաջադրվել են հետևյալ պահանջները.

- օգտագործել միայն անվճար և բաց կոդով տարածվող թվային սարքերի նախագծման միջոցներ (XST ISE մոդելավորող և սինթեզող փաթեթը),
- մշակված համակարգը պետք է աշխատի ժամանակակից օպերացիոն համակարգերի միջավայրում և հասանելի լինի շարժական քոմփյութերների համար:

ModSystem ավտոմատացված համակարգը մշակվել է Web տեխնոլոգիայով, ունի կայքի տեսք և գրվել է PHP օբյեկտ-կողմնորոշված ծրագրավորման լեզվով: Անհրաժեշտ տվյալների պահպանման համար օգտագործվել է MySQL տվյալների հենքերի կառավարման համակարգը:

ModSystem ավտոմատացված համակարգը կիրառողին հնարավորություն է տալիս կատարել մոդուլյար թվաբանության բլոկում մասնագիտացված թվային սարքերի նախագծման մեթոդի ընտրություն: Նկ. 14-ում պատկերված է ModSystem ավտոմատացված համակարգի age.php էջը, որի միջոցով կարելի է կատարել ընտրություն՝ կախված նախագծվող մասնագիտացված թվային սարքի տեսակից (մոդուլյար գումարիչներ, բազմապատկիչներ կամ մոդուլով աստիճան բարձրացնելու սարքեր և այլ:

Նկ.14. ModSystem համակարգի կողմից առաջարկվող նախագծվող սարքերի տիպերը:

Ընտրությունը կարելի է կատարել նաև՝ հիմք ընդունելով սարքի մուտքային տվյալները (թվերի կարգայնություն, մոդուլի արժեք ու մեծություն): Նախագծողը ընտրությունը կարող է կատարել ինքնուրույն համակարգում ներկայացված բոլոր նախագծված սարքերի Verilog նկարագրումներից, կամ, օգտվելով այդ նույն սարքերի նախագծման մեթոդի ընտրության առաջարկներից, որոնք արվել են ատենախոսությունում: Քանի որ մասնագիտացված թվային սարքի նախագծման մեթոդի ընտրության առաջարկները կատարվել են սարքերի սինթեզման հաշվետվությունների հիման վրա, իսկ գնահատումները՝ ըստ FPGA-ի ռեսուրների օգտագործման և սարքի արագագործության տեսակետից, ուստի նախագծողը հնարավորություն ունի ընտրել Verilog նկարագրումը՝ կախված թվերի կարգայնությունից և մոդուլի արժեքից կամ մեծությունից:

Չորրորդ գլխում մշակված մասնագիտացված թվային սարքերը ներկայացված են կառուցվածքային սխեմաների տեսքով, ինչպես նաև տրվել են այդ

սարքերի արդյունավետ աշխատանքի կազմակերպման մշակված ալգորիթմները: Որպես մոդուլյար թվաբանության կիրառման ոլորտները դիտարկվել են գաղտնագրման և թվային հսկման համակարգերը: Առանձին մշակված են RSA գաղտնագրման և Դիֆֆի-Հելլմանի գաղտնագրման բանալիների գեներացման ալգորիթմների վրա հիմնված մասնագիտացված թվային սարքերը, որտեղ գաղտնագրման և վերծանման գործողությունների կատարումը արագացնելու համար: Այս սարքերում, ի տարբերություն աստիճան բարձրացնելու գործողության ավանդական ալգորիթմի, օգտագործել է մշակված Էյլերի ֆունկցիայի կիրառմամբ մոդուլով աստիճան բարձրացնելու բլոկը: Տվյալ մեթոդով նախագծված մասնագիտացված թվային սարքի կիրառումը կրճատել է FPGA-ի օգտագործված ռեսուրսները մինչև 18%:

Մշակվել են m=7 և m=9 մոդուլներով ապարատային հսկում իրականացնող մասնագիտացված թվային սարքեր, որոնց կառուցվածքային սխեմաներում ներառվել են ատենախոսությունում մշակված մոդուլյար գումարիչներ: Վերջիններիս կիրառումը կրճատել է FPGA-ի օգտագործված ռեսուրսները 7%-ով:

ԱՏԵՆԱԽՈՍԱԿԱՆ ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

Ատենախոսությունում հետազոտությունների հիման վրա հիմնավորվել է մոդուլյար թվաբանության բլոկում մասնագիտացված թվային սարքերի նախագծման նոր մեթոդների մշակման անհրաժեշտությունը: Հետազոտության հիմնական արդյունքներն են.

1. Մշակվել են մոդուլյար գումարիչների կառուցման տարբեր մեթոդներ և գնահատվել է այդ մեթոդների կիրառման արդյունավետությունը՝ կախված մուտքային թվերի և մոդուլի արժեքի կարգայնությունից, որի արդյունքում կրճատել է FPGA օգտագործված ռեսուրսների 8-10% [1, 4]:
2. Մշակվել են մոդուլյար բազմապատկիչների կառուցման տարբեր մեթոդներ և գնահատվել է այդ մեթոդների կիրառման արդյունավետությունը՝ կախված մուտքային թվերի և մոդուլի արժեքի կարգայնությունից, ինչի արդյունքում կարելի է կրճատել FPGA ներառված ռեսուրսների 7-12% [1, 2, 6, 7]:
3. Մշակվել են մոդուլով աստիճան բարձրացում իրականացնող սարքերի կառուցման տարբեր մեթոդներ և գնահատվել է այդ մեթոդների կիրառման արդյունավետությունը՝ կախված մուտքային թվերի և մոդուլի արժեքի կարգայնությունից, ինչի արդյունքում կարելի է կրճատել FPGA ռեսուրսների ≈15% [3, 5]:
4. Գնահատվել են մոդուլյար բլոկում թվաբանական գործողություններ կատարող սարքերի արագագործությունը և բարդությունները FPGA-ի ռեսուրսների օգտագործման տեսակետից [4]:

5. Հետազոտությունների արդյունքում արվել են առաջարկներ մոդուլյար սարքերի տարբեր մեթոդների նախագծման առավելությունների վերաբերյալ [4, 6]:
6. Մշակվել է մոդուլյար թվաբանության բլոկի համար ավտոմատացված նախագծման Modsystem համակարգը, որում միավորված են մշակված մեթոդները և, որի օգնությամբ կարելի է կատարել մոդուլյար թվաբանության բլոկում մասնագիտացված թվային սարքերի նախագծման մեթոդի ընտրություն [3, 5]:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԹԵՄԱՅԻ ՇՐՋԱՆԱԿՆԵՐՈՒՄ ՀՐԱՊԱՐԱԿՎԱԾ ԱՇԽԱՏՈՒԹՅՈՒՆՆԵՐ

1. Սաղաթելյան Ա.Կ. Արդյունքի ձևավորման փոփոխական ժամանակով ամբողջ թվերի բաժանման արագագործ սարքի կառուցվածքը// ՀՊՃՀ-ի Լրաբեր գիտական և մեթոդական հոդվածների ժողովածու.- Երևան, 2010.- Հատոր 2, № 1.- էջ 236-239:
2. Туманян А.К., Сагателян А.К. Построение схем умножения на основе комбинационных умножителей// Вестник Государственного инженерного университета Армении. Серия “ Моделирование, Оптимизация, Управление”.-2011.- выпуск 14, том 1. - С. 82-91.
3. Սաղաթելյան Ա.Կ., Թումանյան Ա.Կ., Քամալյան Ա.Գ. RSA ալգորիթմի ապարատային իրագործումը // ՀՊՃՀ-ի Լրաբեր գիտական հոդվածների ժողովածու.- Երևան: Ճարտարագետ, 2013.- Մաս 1.-էջ 179-185:
4. Сагателян А.К. Принципы построения модулярных сумматоров // Materiały IX Międzynarodowej naukowi praktycznej konuferencji, Wschodnie partnerstwo. - 2013 Volume 35, Techniczne nauki, Przemyśl Nauka i studia.- С. 41-45:
5. Saghatelyan A.K. The Hardware Implementation of the Cryptographic Key Generation based on Diffie-Hellman algorithm // Proceedings of Engineering academy of Armenia. - 2013. – Vol. 10, № 4. - P. 760-763.
6. Կիրակոսյան Գ.Տ, Սաղաթելյան Ա.Կ. Մնացորդային դասերի համակարգում ինդեքսային մեթոդով բազմապատկման սարքերի նախագծումը// ՀՊՃՀ-ի Լրաբեր գիտական հոդվածների ժողովածու.- Երևան: Ճարտարագետ, 2014.- Մաս 1. - էջ 110-115:
7. Սաղաթելյան Ա.Կ. Մնացորդային դասերի համակարգում $m=2^k$ մոդուլով բազմապատկման սարքերի նախագծում // Հայաստանի գիտությունների ազգային ակադեմիայի և Հայաստանի ազգային պոլիտեխնիկական համալսարանի Տեղեկագիր. Տեխնիկական գիտությունների սերիա. - 2015.- Հատոր 68, № 1. – էջ 44-50:

САГАТЕЛЯН АННА КАРПИСОВНА

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДОВ ПРОЕКТИРОВАНИЯ АРИФМЕТИЧЕСКИХ УСТРОЙСТВ В БЛОКЕ МОДУЛЯРНОЙ АРИФМЕТИКИ

Актуальность темы. Диссертационная работа посвящена разработке и исследованию методов проектирования цифровых устройств, сложных функциональных блоков (СФ- блоки) в блоке (аппарате) модулярной арифметики.
К цифровым схемам всегда предъявляются требования повышения быстродействия, которые можно реализовать с помощью системы остаточных классов (модулярной арифметики). Использование блока модулярной арифметики позволяет значительно повысить быстродействие арифметических вычислений за счет параллельного выполнения операций над остатками.

Одним из основных методов повышения производительности проектирования специализированных цифровых устройств является многократное использование СФ-блоков. Исходя из вышесказанного поиск новых методов аппаратной реализации цифровых устройств является актуальной научно-технической задачей. Диссертационная работа посвящена разработке и исследованию методов проектирования СФ-блоков с применением блока модулярной арифметики.

Объект исследования. Объектом исследования являются методы проектирования арифметических устройств в блоке модулярной арифметики, анализ и сравнение результатов их синтеза с использованием СФ-блоков, а также средства алгоритмического и программного обеспечения разработки структур модулярных устройств.

Методы исследования. В диссертации использованы теоретические и практические методы и инструментальные средства разработки структур цифровых устройств. В качестве основы для исследования использованы опубликованные научные и специализированные работы по технологии проектирования модулярных устройств.

Научная новизна исследования. Научной новизной диссертационной работы является разработка методов проектирования СФ-блоков для реализации основных вычислительных модулярных устройств и их объединение в автоматизированной системе проектирования для блока модулярной арифметики, с помощью которой можно реализовать моделирование, синтез и оценку оптимальной структуры цифрового устройства. Для достижения данной цели были сформулированы и решены следующие задачи:

- исследование современных методов проектирования цифровых устройств и особенностей их применения;
- разработка методов проектирования аппаратных реализаций модулярных сумматоров, умножителей и устройств возведения в степень по модулю с

использованием СФ-блоков, а также оценка их быстродействия и аппаратных затрат;

- оценка быстродействия и аппаратных затрат спроектированных модулярных устройств в зависимости от разрядности операндов и значения модуля;
- предложения способов выбора оптимального метода проектирования арифметических устройств в блоке модулярной арифметики;
- разработатка объединенной автоматизированной системы выбора методов проектирования специализированных СФ-блоков для блока модулярной арифметики.

Основные результаты диссертационной работы:

1. Разработаны разные методы проектирования модулярных сумматоров и произведена оценка эффективности применения этих методов в зависимости от разрядности входных операндов и значения модуля, в результате чего использованные ресурсы FPGA сокращаются на 8-10% [1, 4].
2. Разработаны разные методы проектирования модулярных умножителей и произведена оценка эффективности применения этих методов в зависимости от разрядности входных операндов и значения модуля, в результате чего можно сократить использованные ресурсы FPGA сокращаются на 7 -12% [1, 2, 6, 7].
3. Разработаны разные методы проектирования устройств возведения в степень по модулю и произведена оценка эффективности применения этих методов в зависимости от разрядности входных операндов и значения модуля, в результате чего использованные ресурсы FPGA сокращаются на 15% [3, 5].
4. Произведена оценка быстродействия и сложности реализации на FPGA устройств, выполняющих арифметические операции в блоке модулярной арифметики [4].
5. Обоснованы предложения, сделанные на основе исследований, о выборе оптимального метода проектирования арифметических устройств в блоке модулярной арифметики с использованием FPGA [4, 6].
6. Разработана объединенная автоматизированная система методов проектирования специализированных СФ-блоков для блока модулярной арифметики [3, 5].

SAGHATELYAN ANNA
DEVELOPING AND INVESTIGATING METHODS FOR DESIGNING ARITHMETIC DEVICES IN THE BLOCK OF MODULAR ARITHMETIC

SUMMARY

Urgency of the subject. Digital circuits are always expected to have a high-speed performance which can be reached by means of the Residue Number System (Modular Arithmetic). The application of Residue Number System considerably increases the operating speed of arithmetical calculations due to the parallel execution of operations on the remainders.

It is known that substantial theoretical research has been conducted in the field of modular arithmetic. Nonetheless, this line of research has not been widely explored, mainly on account of the lacking digital equipment, the component foundation.

Nowadays, along with the advancements in the field of the integral Schematics (Circuit Engineering), an opportunity of researching and designing devices in the block of modular arithmetic has presented itself.

This work regards the Residue Number System as an instrument generally applied for increasing the operating speed and the accuracy of calculations.

The study of the unique features of executable operations in the block of modular arithmetic and the application of their results are considered to be a promising research area.

It is important to note, that the existence of the SoC (Systems-on-Chip). with the application of modular arithmetic broadens the field of implementation of the latter (e.g. cryptography, digital data diagnostics and data control, etc.). Hence, one can claim that designing and repeatedly utilizing such SoC, also finding new methods of hardware implementation is considered to be a significant scientific and engineering task. The dissertation is devoted to the specific task: investigating and developing methods for designing SoC with the application of modular arithmetic.

The investigation subjeect. The purpose of this research is developing methods for designing arithmetic devices using modular arithmetic, analyzing and comparing the results of their synthesis by means of SoC and utilizing algorithmic and software tools for modeling the structure of modular devices.

The Scientific Novelty of the Research: The scientific novelty of this research is developing methods for designing SoC for the realization of the main calculating devices and automatic systems of designing for the block of modular arithmetic. The findings are as fallows:

- Up to date design methods for digital devices and peculiarities of thera applicationhave been investigated.

- Hardware implementation of modular adders, multipliers and modular exponention devices by using SoC has been developed, as well as their high-speed and hardware expenditure have been assessed.
- The speed of operation and the hardware expenditure of the designed modular devices have been assessed, depending on the operand widths and the value of the module.
- Means, by which on optimal method for designing arithmetic devices in the block of the modular arithmetic can be selected, have been proposed.
- A united automated system of methods for designing SoC in the block of modular arithmetic has been developed.

The results of the dissertation are:

1. Various methods for designing modular adders and the efficiency of using these methods, depending on the width of the operands and the value of the module have been developed.[1, 4].
2. Various methods for designing modular multipliers and the efficiency of using these methods, depending on the width of the operands and the value of the module have been developed. [1, 2, 6, 7].
3. Various methods of designing modular exponentiation devices and the efficiency of using these methods, depending on the width of the operands and the value of the module have been developed. [3, 5].
4. The speed of operation and the complexity of the devices in the block of modular arithmetic have been assessed from the perspective of using FPGA resources [4].
5. Claims about the value of various design methods of modular devices have been justified [4, 6].
6. A system of automated design for the block of modular arithmetic has been developed [3, 5].