**A.A. KHEMCHYAN, A.K. ASLANYAN, A.H. ARSHAKYAN,
G.H. KHACHATRYAN**

PROTECTION OF COMPUTER CRYPTOGRAPHIC EQUIPMENT AT UNCERTAINTY OF THE FOE CONTROL

The protection of encryption equipment is a fundamental issue in application of different accessibility policies. It is shown that by applying external encryption and decryption equipment working on hard logic, an independent cryptographic system and its main output encrypted information are obtained which will allow the consumers to protect themselves from the actions of malicious programs (embedded devices). It makes possible to use non-standard methods of decryption.

Keywords: malware, encryption system, embedded devices, cryptanalysis.

ՀՏԴ 681.3

Ռ.Հ. ԳԵՂԱՄՅԱՆ, Ա.Կ. ՍԱՂԱԹԵԼՅԱՆ, Ա.Գ. ՔԱՄԱԼՅԱՆ

ԵՌԱՆԿՅՈՒՆԱՉԱՓԱԿԱՆ ՖՈՒՆԿՑԻԱՆԵՐԻ ՀԱՇՎԱՐԿ ԻՐԱԿԱՆԱՑՆՈՂ ՍԱՐՔԻ ԱՊԱՐԱՏԱՅԻՆ ԻՐԱԳՈՐԾՈՒՄԸ

Դիտարկված են արագագործության տեսակետից արդյունավետ եռանկյունաչափական ֆունկցիաների հաշվարկման սարքի նախագծման եղանակը և տրամաբանական սինթեզումը ժամանակակից միջոցների կիրառմամբ:

Առանցքային բառեր. Եռանկյունաչափական ֆունկցիաներ, ապարատային իրագործում, աղյուսակային ընտրում, PROM հիշողություն:

Ուսումնասիրելով եռանկյունաչափության հիմնական ֆունկցիաները և օրենքները՝ կարելի է պնդել, որ լայնորեն կիրառվող և հաշվարկվող ֆունկցիաների դասին են պատկանում sin, cos, tg, ctg պարզ ֆունկցիաները, և այդ ֆունկցիաների արժեքների որոշումն ունի որոշակի պարբերականություն: Եռանկյունաչափական օրենքների հիման վրա կատարելով նաև գումարման/հանման գործողությունը և ունենալով sinα և tgα արժեքները, կարելի է ստանալ համապատասխանաբար cosα և ctgα ֆունկցիաների արժեքները:

Այս ձևափոխումները հիմնված են բերման բանաձևերի և եռանկյունաչափության պարբերականությունը և զույգությունը պահպանող օրենքների վրա:

Որպես սկզբնական տեղեկություն առաջարկվում է ձևավորել 2 աղյուսակ՝ $\sin(0^0)$-$\sin(90^0)$ արժեքները պահող աղյուսակը և $tg(0^0)$-$tg(90^0)$ արժեքները պահող աղյուսակը: Այդ նպատակով օգտագործվում է ծրագրավորվող 2 հիշող սարք (PROM)՝ սինուս (PROM1) և տանգենս (PROM2) արժեքների համար, յուրաքանչյուրը 128x16 ծավալով: Այս որոշումը հիմնված է մշակվող սարքի ապարատային

ծախսերի կրճատման և արագագործության բարձացման սկզբունքների վրա: Իրականում կարելի էր տվյալ խնդիրը լուծել մեկ այլ կերպ՝ ձևավորելով 1 աղյուսակ՝ 128x8 ծավալով, sin(0^0)-sin(90^0) արժեքները պահելու համար, բայց այս դեպքում, բացի բերման բանաձևերից, պետք էր կիրառել նաև տանգենս և կոտանգենս ֆունկցիաների որոշման հիմնական բանաձևերը (tgα=$\frac{sin\alpha}{cos\alpha}$ և ctgα = $\frac{cos\alpha}{sin\alpha}$) [1,2]: Այդ դեպքում պետք կլիներ կառուցվածքային սխեմային ավելացնել բաժանման սարք՝ հաշվարկն իրականացնելու համար, ինչը կհանգեցնի ոչ միայն ապարատային ծախսերի ավելացմանը, այլ նաև արագագործության նվազմանը, քանի որ տանգենս և կոտանգենս ֆունկցիաների հաշվարկը կկատարվեր 2 փուլով՝

1. կոսինուս ֆունկցիայի արժեքի որոշումը սինուս ֆունկցիայի միջոցով՝ հիմնվելով աղյուսակում բերված բանաձևերի վրա,

2. բաժանանման գործողության միջոցով տանգենս և կոտանգենս ֆունկցիաների արժեքների հաշվարկը:

Սակայն եթե առաջարկված եղանակով կիրառում ենք 2 PROM հիշող սարք սինուսի և տանգենսի համար առանձին-առանձին, ապա սինուս և տանգենս ֆունկցիաների արժեքների հաշվարկն իրականացվում է միատակտ աղյուսակային ընտրանքի միջոցով, իսկ կոտանգես և կոսինուս ֆունկցիաների արժեքների հաշվարկն իրականացվում է՝ հիմնվելով հետևյալ օրենքների և բանաձևերի վրա:

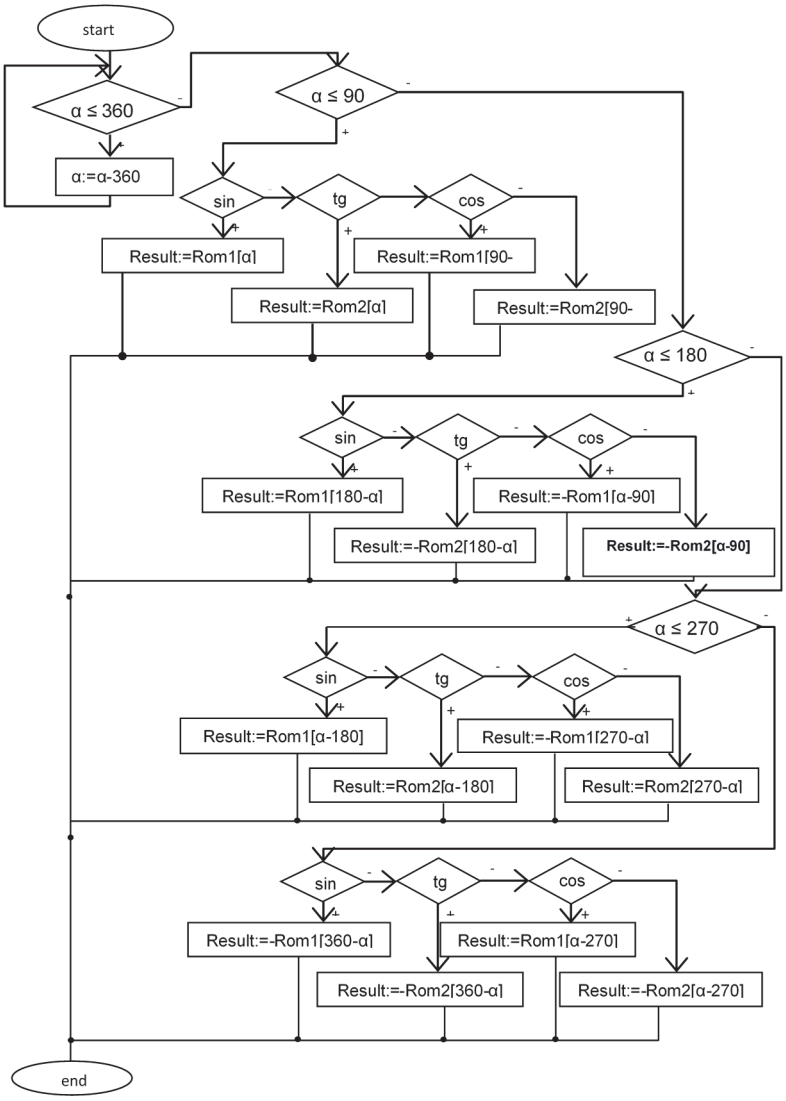
Աղյուսակ

α անկյուն	cosα արժեքը sinα-ի կիրառմամբ	ctgα արժեքը tgα-ի կիրառմամբ
$0^o<\alpha<90^o$	cosα =sin(90^0-α)	ctgα= tg(90^0-α)
$90^o<\alpha<180^o$	cosα =-sin(α -90^0)	ctgα=-tg(α -90^0)
$180^o<\alpha<270^o$	cosα =-sin(270^0-α)	ctgα= tg(270^0-α)
$270^o<\alpha<360^o$	cosα =sin(α -270^0)	ctgα=- tg(α -270^0)

Ելնելով նշված հանգամանքներից՝ մշակել ենք եռանկյունաչափական գործողություններն իրականացնող սարքի ալգորիթմի բլոկ-սխեման (նկ. 1):

Հաշվարկվող անկյան եռանկյունաչափական ֆունկցիան որոշելու համար նախ, անհրաժեշտության դեպքում, ձևավորում ենք անկյան արժեքը 0^o-360^o միջակայքում՝ հիմնվելով պարբերականության օրենքի վրա: Ապա որոշվում է α անկյան քառորդը, և կախված եռանկյունաչափական ֆունկցիայից՝ կամ կատարվում է տվյալ անկյան արժեքի միատակտ ընտրությունը համապատասխան PROM-ից, կամ՝ նախնական հաշվարկ՝ հիմնվելով բերման բանաձևերի վրա,

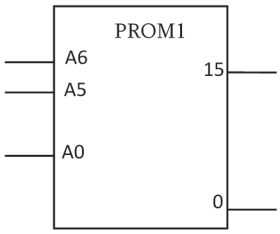
ապա՝ ձևավորված նոր α_1 անկյան արժեքի միատակտ ընտրությունը Rom1-ից, կամ՝ Rom2-ից (ինչպես նշված է ալգորիթմի բլոկ-սխեմայում): Բլոկ-սխեմայից երևում է, որ կախված հաշվարկվող անկյան մեծությունից՝ ալգորիթմը պահպանում է իր պարբերականությունը եռանկյունաչափական ֆունկցիաների որոշման հաջորդականության սկզբունքներում. նախ՝ որոշվում է հաշվարկվող ֆունկցիան, ապա կատարվում որոշակի գործողություն՝ տվյալը PROM-ից ընթերցելու համար:



Նկ. 1. Եռանկյունաչափական գործողություններն իրականացնող սարքի ալգորիթմի բլոկ-սխեման

Սինուս ֆունկցիայի արժեքների ներկայացման համար առանձնացվում է 128x16 ծավալով PROM, քանի որ այն մտապահում է 0^0-90^0 անկյունների սինուս արժեքները, հետևաբար՝ PROM-ը պետք է ունենա նվազագույնը 7-բիթանի հասցեական մուտք ($(90)_{10}=(1011010)_2$) և 16 բիթ երկարություն (նկ. 2) [3,4], պայմանավորված նրանով, որ ցանկացած անկյան սինուսը ≤ 1-ից (կոտորակային թիվ է): Որպեսզի պահպանենք ճշտությունը, իսկ գործողությունները կատարենք ամբողջ թվերով, որոշվեց կոտորակային թվերը մեծացնել 2^{15} անգամ:

Այնուհետև հաշվարկները կատարելուց հետո ստացված արժեքը փոքրացնել 2^{15} անգամ: PROM1 հիշող սարքի հասցեն [addr] համապատասխանում է անկյան արժեքին՝ PROM1[addr]:



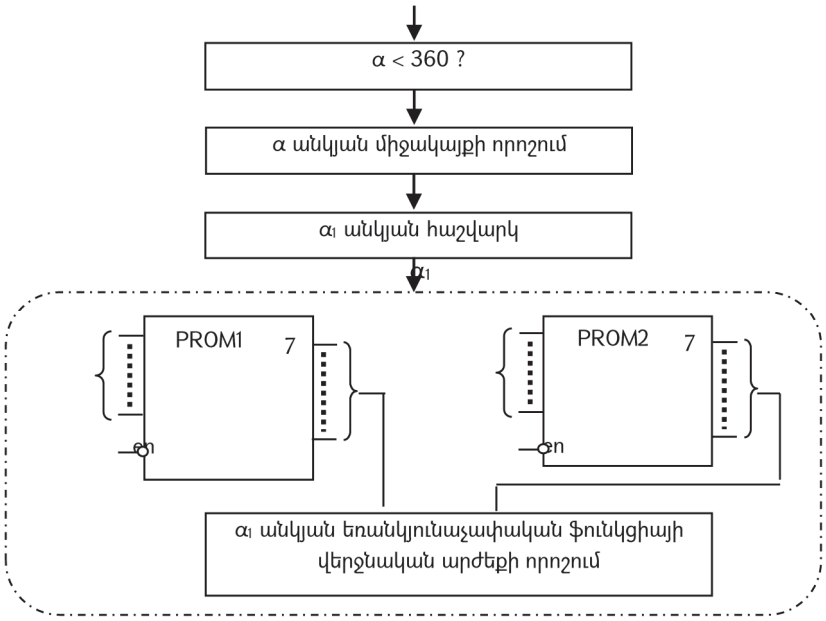
$\sin 1^0 = 0.017452$
$\sin 2^0 = 0.034899$
. . . .
$\sin 89^0 = 0.999848$
$\sin 90^0 = 1.000000$

Rom1[0]=0000000000000000;
Rom1[1]=0000001000000010;
Rom1[2]=0000010000000100;
. . . . . .
Rom1[89]=0111111111111111;
Rom1[90]=1000000000000000

Նկ. 2. Սինուս ֆունկցիայի արժեքների ներկայացման PROM հիշողությունը

Տանգենս ֆունկցիայի արժեքների ներկայացման համար առանձնացվում է 128x16 ծավալով PROM2: PROM2 հիշող սարքը կառուցվում է PROM1-ի տրամաբանությամբ: Սակայն ինֆորմացիայի պահպանումը նույն սկզբունքով, ինչպես PROM1-ում է, չի կարող իրականացվել, քանի որ տանգենս ֆունկցիայի 0^0-90^0 անկյունների արժեքները գտնվում են 0-58 միջակայքում: Այդ պատճառով տարբեր անկյունների դեպքում արժեքները պահվում են տարբեր սկզբունքներով, արժեքները մեծացնելով 2^{15} -ից մինչև 2^8 անգամ, քանի որ դրանք գտնվում են տարբեր միջակայքերում (օրինակ՝ 76^0-82^0 անկյունների տանգենս արժեքները գտնվում են 1-4 միջակայքում):

Մշակված կառուցվածքը, բացի PROM հիշող սարքերից, պետք է ունենա հաշվարկվող անկյան արժեքի որոշման բլոկ, α անկյան միջակայքի որոշման բլոկ, α_1 անկյան հաշվարկման բլոկ և գումարման գործողություն իրականացնող սարք, ինչպես նաև α_1 անկյան եռանկյունաչափական ֆունկցիայի վերջնական արժեքի որոշման բլոկ, որը ներառում է 2^k տեղաշարժող ռեգիստր և նշանի ձևավորման սխեմա (նկ. 3): Հաշվարկվող անկյան արժեքի որոշման բլոկը կատարում է $\alpha \le 360^0$ պայմանի ստուգումը և α անկյան վերահաշվարկը $0 \le \alpha < 360^0$ միջակայքում:



Նկ. 3. Ֆունկցիաների արժեքի որոշման սարքի բլոկների փոխկապակցման սխեման

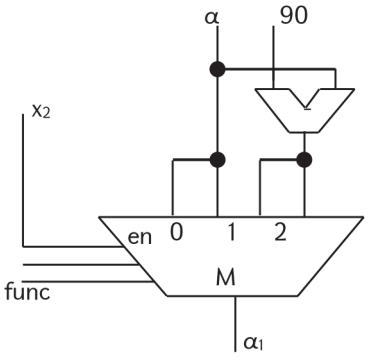
Տվյալ բլոկի կառուցվածքում առկա են կոմպարատոր (CMP), գումարիչ և մուլտիպլեքսոր: Վերահաշվարկված α անկյան միջակայքի որոշման բլոկը ներառում է նախապատվության կոդավորիչ (PrCD) և ներկառուցված տրամաբանություն, որոնց միջոցով ձևավորվում են x_2, x_3, x_4 պայմանների իրականացումները, այսինքն՝ ճշգրիտ որոշվում է α անկյան միջակայքը: α_1 անկյան հաշվարկման բլոկում կատարվում են այն գործողությունները, որոնք նախորդում են նոր ստացված անկյան համապատասխան եռանկյունաչափական ֆունկցիայի արժեքի ընտրությանը PROM1 կամ PROM2 աղյուսիկից:

Այս բլոկը ներառում է 4 հատ 4_1 մուլտիպլեքսոր, որոնց թույլատրման մուտքերն են նախորդ α անկյան միջակայքի որոշման բլոկի ելքում ձևավորված x_2, x_3, x_4 արժեքները: Մուլտիպլեքսորը կատարում է α_1 անկյան արժեքի հաշվարկման գործողությունը՝ համաձայն եռանկյունաչափական օրենքների և մշակված ալգորիթմի բլոկ-սխեմայի: Կախված α անկյան գտնվելու միջակայքից և անհրաժեշտ ֆունկցիայից՝ կատարվում են վերահաշվարկը և նոր α_1 անկյան որոշումը (նկ. 4): 4 ֆունկցիաները (sin, tg, cos, ctg) կոդավորում են 2 բիթով: Եթե $\alpha \le 90^0$ (x_2 պայման) $\sin\alpha_1 = \sin\alpha$ և $\mathrm{tg}\alpha_1 = \mathrm{tg}\alpha$, այսինքն՝ $\alpha_1 = \alpha$, իսկ $\cos\alpha_1 = \sin(90^0-\alpha)$, $\mathrm{ctg}\alpha_1 = \mathrm{tg}(90^0-\alpha)$: Կարելի է նկատել, որ մշակված սխեմաներում օգտագործվում կամ կիրառվում են միայն կոմբինացիոն հանգույցներ (մուլտիպլեքսորներ, կոմպարատոր, նախապատվության կոդավորիչ, գումարիչներ և տարրականան այլ

տրամաբանություն): Այս ամենը հնարավորություն է ընձեռում սարքերի աշխատանքը FPGA-ի միջոցով նախագծելիս օգտագործել վերջինիս ռեսուրսների փոքր քանակություն [5]:

Փաստորեն առաջարկվող եռանկյունաչափական ֆունկցիաներն իրականացնող սարքի հիշողություն պարունակող հանգույցներն են PROM1 և PROM2 հիշող սարքերը և FSM ղեկավարող ավտոմատը: α_1 անկյան հաշվարկման գործողությունն իրականացնելուց հետո անհրաժեշտ է կատարել պահանջվող եռանկյունաչափական ֆունկցիայի արժեքի միատակտ աղյուսակային ընտրությունը PROM1 կամ PROM2 հիշողություններից: Ընտրությունը կախված է պահանջվող եռանկյունաչափական ֆունկցիայից:

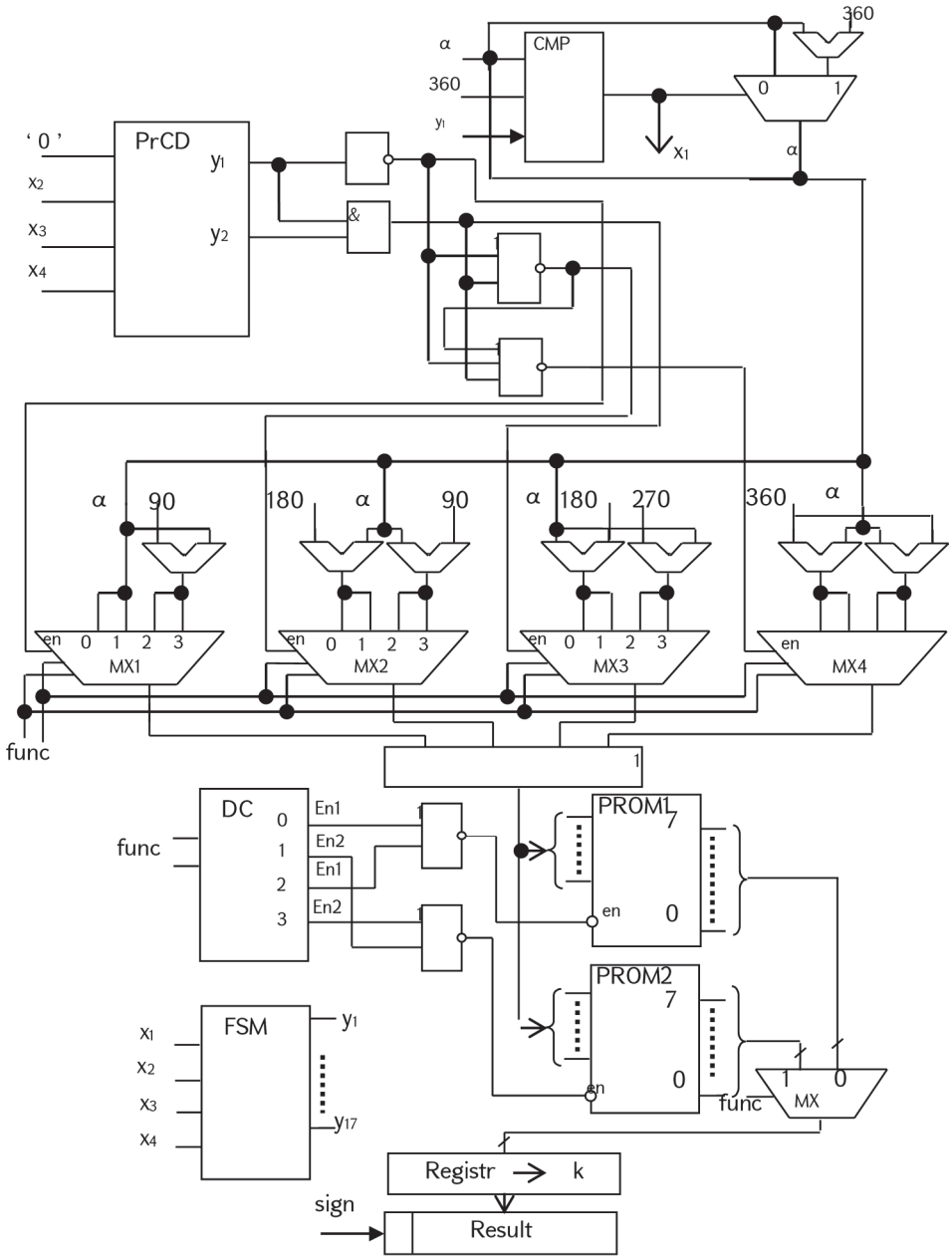
Function	արժեք
sin	00
tg	01
cos	10
ctg	11



Նկ. 4. α_1 անկյան արժեքի հաշվարկման բլոկի կառուցվածքը $\alpha \le 90^0$ միջակայքում

Այդ նպատակով օգտագործվել է վերծանիչ, որի միջոցով վերլուծելով մուտքային եռանկյունաչափական ֆունկցիայի կոդը՝ կատարվում է PROM1 կամ PROM2 ընթերցման թույլատվության (En) մուտքի ակտիվացում և նշանի տեղակայման տեղաշարժող ռեգիստր՝ վերջնական արժեքի ձևավորման համար (նկ.5):

Եզրակացություն: Մշակվել է եռանկյունաչափական գործողություններ իրականացնող ալգորիթմի բլոկ-սխեման, ներկայացվել են PROM հիշող սարքերի ընդհանուր կառուցվածքները, ինչպես նաև առանձին սարքերի ապարատային իրագործումները: Կատարված են բոլոր սարքերի Verilog նկարագրումները և սինթեզումը՝ FPGA-ի օգտագործմամբ [6]: Սինթեզումից հետո ավտոմատ նախագծման համակարգը (ISE DISIGN) տրամադրել է հաշվետվություն FPGA-ի ռեսուրսների օգտագործման վերաբերյալ, համաձայն որի՝ օգտագործվել են տրիգերների քանակի 1%, քառամուտք LUT-երի 55%, սեկցիաների 72% և մուտք-ելքերի 46%:



Նկ. 5. α անկյան եռանկյունաչափական ֆունկցիայի արժեքի որոշմշակված սարքի կառուցվածքը

Այդ բլոկներում կիրառվում են միայն կոմբինացիոն բազային հանգույցներ մասնավորապես՝

- 4 հատ 4_1 մուլտիպլեքսորներ,

- 1հատ կոմպարատոր,
- 1 հատ նախապատվության կոդավորիչ,
- 1 հատ վերծանիչ,
- 8 հատ 9-կարգանի գումարիչներ:

Իսկ առաջարկվող եռանկյունաչափական ֆունկցիաներն իրականացնող սարքի հիշողություն պարունակող հանգույցներն են՝

- PROM1 հիշող սարքը՝ սինուս ֆունկցիայի արժեքների պահման համար,
- PROM2 հիշող սարքը՝ տանգենս ֆունկցիայի արժեքների պահման համար,
- FSM ղեկավարող ավտոմատը:

Ապարատային այս իրագործման առավելությունն այն է, որ սարքի ելքում ձևավորվում է եռանկյունաչափական ֆունկցիաների արժեքների (հիմնականում ≤ 1-ի կոտորակային թվեր) երկուական կոդը, ինչը հնարավոր չէ ստանալ զանգվածային կիրառման առկա հաշվիչների միջոցով:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. http://www.botik.ru/~psi/PSI/disk_20/e-book/e-book/1-4/03-Zakharov-Algoritmy-CORDIC-p-353.pdf
2. http://patents.su/3-1262486-ustrojjstvo-dlya-vychisleniya-trigonometricheskikh-funkcijj.html
3. **Хамахер., Врашневич З., Заки С.** Организация ЭВМ.- 5-е изд.- СПб.: Питер, 2003.-854 с.
4. **Столлингс У.** Структурная организация и архитектура компьютерных систем. - 5-е изд.-М.: Изд.дом “Вильямс”, 2002.-893 с.
5. **Цилькер Б.Я., Орлов С.А.** Организация ЭВМ и систем. –СПб.: Питер, 2006.- 667 с.
6. Макромодули быстродействующих умножителей на ПЛИС Xilinx // Scan Engineering Telecom .- 1998.

Р.А. ГЕГАМЯН, А.К. САГАТЕЛЯН, А.Г. КАМАЛЯН

АППАРАТНАЯ РЕАЛИЗАЦИЯ УСТРОЙСТВА, РЕАЛИЗУЮЩЕГО РАСЧЕТ С ТРИГОНОМЕТРИЧЕСКИМИ ФУНКЦИЯМИ

Рассмотрен эффективный, с точки зрения быстродействия, способ проектирования устройства, вычисляющего тригонометрические функции и его синтез с применением современных средств проектирования.

Ключевые слова: тригонометрические функции, аппаратная реализация, табличная выборка, PROM память.

R.H. GEGHAMYAN, A.K. SAGHATELYAN, A.G. QAMALYAN

HARDWARE IMPLEMENTATION OF THE DEVICE CARRYING OUT CALCULATIONS WITH TRIGONOMETRIC FUNCTIONS

From a standpoint of fast operation, an efficient method for calculating the trigonometric function and its synthesis by applying modern methods of design is considered.

Keywords: trigonometric functions, hardware realization, tabular choice, PROM memory.

ՀՏԴ 530.15

Տ.Ա. ՖԼՋՅԱՆ

ԱՊԱՀՈՎԱԳՐԱԿԱՆ ԸՆԿԵՐՈՒԹՅԱՆ ՔՈՄՓՅՈՒԹԵՐԱՅԻՆ ՑԱՆՑԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԻՋՈՑՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄԸ, ՀԱՄԵՄԱՏԱԿԱՆ ԳՆԱՀԱՏՈՒՄԸ ԵՎ ԲԱՐԵԼԱՎՈՒՄԸ

Հետազոտվել է ապահովագրական ընկերության քոմփյութերային ցանցի կառուցվածքը՝ անվտանգության տեսակետից, դիտարկվել են նրա անվտանգության բարձրացման գործիքամիջոցները, և կատարվել է դրանց հիմնավոր ընտրությունը: Իրականացվել է գործող և առաջարկվող ապահովագրական ընկերության մասնագիտացված քոմփյութերային ցանցի կառուցվածքների աշխատունակության, անվտանգության և արդյունավետության համեմատական գնահատումն ու բարելավումը:

Առանցքային բառեր. քոմփյութերային ցանց, ցանցային անվտանգություն, գործիքամիջոց, ցանցային աշխատունակություն և արդյունավետություն, ապահովագրական ընկերության ցանց:

Ներածություն: Ապահովագրական ընկերության քոմփյութերային ցանցերում անվտանգության ապահովման հիմնախնդիրները միշտ եղել են ուշադրության կենտրոնում և շարունակում են մնալ արդիական, քանի որ այդ ընկերությունների մասնագիտացված քոմփյութերային ցանցերին ներկայացվող անվտանգության պահանջները մշտապես վերանայվում ու խստացվում են [1]: Որպես կանոն, յուրաքանչյուր ապահովագրական ընկերության մասնագիտացված քոմփյութերային ցանցի համար անհրաժեշտ է ունենալ իր եզակի անվտանգության ապահովումը, որպեսզի հնարավոր լինի պատշաճ մակարդակով կազմակերպել ցանցի անվտանգության գործընթացը, հաշվի առնելով կենտրոնական բանկի, արտաքին աուդիտի, հաճախորդների և այլոց պահանջներն ու շահերը [1]: Այսպիսի մասնագիտական քոմփյութերային ցանցում անվտանգության կազմակերպումը և իրականացումը ձևավորվում են հիմնական ռիսկերի գնահատումով, կրի-