ՀՏԴ 681.3

Է.Վ. ԱԼԵՔՍԱՆՅԱՆ, Ա.Կ. ՍԱՂԱԹԵԼՅԱՆ, Է.Վ. ՎԻՐԱԲՅԱՆ

ՓԼԵՅՖԵՐԻ ԾԱԾԿԱԳՐՈՎ ԳԱՂՏՆԱԳՐՈՂ ՍԱՐՔԻ ՄՇԱԿՈՒՄԸ ԵՎ ԱՊԱՐԱՏԱՅԻՆ ԻՐԱԳՈՐԾՈՒՄԸ

Ուսումնասիրվում են Փլեյֆերի ծածկագրով գաղտնագրող սարքի ապարատային իրագործման հարցեր: Նախագծված են սկզբնական և ձևափոխված աղյուսակների մտապահման համար հիշող սարքերի կառուցվածքները և տեքստի ու բանալու տառերի ներմուծման ճշգրտված ալգորիթմի բլոկ-սխեման: Մշակված է Փլեյֆերի ծածկագրով նախագծված սարքի կառուցվածքային սխեման, գնահատված են սարքի արագագործությունը և ապարատային ծախսերը FPGA ռեսուրսների տեսակետից:

Առանցքային բառեր. Փլեյֆերի ծածկագիր, գաղտնագրման սարքի կառուցվածքային սխեմա, ապարատային իրագործում, FPGA ռեսուրսներ:

Փլեյֆերի ծածկագիրը օգտագործում է 5x5 մատրից պարունակող (լատինական այբուբենի համար) գաղտնաբառ (հիմնաբառ) կամ արտահայտություն: Մատրից ստեղծելու և ծածկագիր օգտագործելու համար բավական է հիշել հիմնաբառը և չորս պարզ կանոններ: Բանալին մատրից կազմելու համար, նախևառաջ, անհրաժեշտ է լրացնել մատրիցի դատարկ բջիջները գաղտնաբառի տառերով (առանց գրելու կրկնվող նիշերը), ապա լրացնել մատրիցի մնացած բջիջները այբուբենի նիշերով, որոնք չեն հայտնվում հիմնաբառում (անգլերեն տեքստերում «Q» նիշը սովորաբար բաց է թողնված՝ այբուբենի կրճատման համար, այլ տարբերակներում «I» և «J» միավորվում են մեկ բջիջի մեջ):

Գաղտնաբառը կարող է գրվել մատրիցի վերին շարքում ձախից աջ կամ պարուրաձև՝ վերին ձախ անկյունից դեպի կենտրոն: Այբուբենով լրացված հիմնաբառը կազմում է 5x5 մատրից [1]:

Հաղորդագրությունը ծածկագրելու համար անհրաժեշտ է այն բաժանել բիգրամների (երկու նիշի խմբերի), եթե բիգրամի երկու նիշ համընկնում է (կամ եթե միայն մեկ նիշ է մնացել), ապա առաջին նիշից հետո պետք է ավելացնել «X» և ծածկագրել նոր զույգը: Փլեյֆերի ծածկագրի որոշ տարբերակներում «X»-ի փոխարեն օգտագործվում է «Q» [1 - 3]:

1. Եթե բիգրամի նիշերը հայտնվում են մեկ տողում, ապա այդ նիշերը փոխարինվում են համապատասխան նիշերի աջ կողմում գտնվող մոտակա սյունակներում տեղակայված նիշերով:

2. Եթե բուն տեքստի բիգրամի նիշերը հայտնվում են նույն սյունակում, ապա դրանք փոխարկվում են նույն սյունակի նիշերի, որոնք անմիջապես դրանց տակ են: Եթե նիշը սյունակի ներքևի նիշն է, ապա այն փոխարինվում է նույն սյունակի առաջին նիշով:

3. Եթե բուն տեքստի բիգրամի նիշերը տարբեր սյունակների և տարբեր տողերի մեջ են, ապա դրանք փոխարինվում են նույն գծերի մեջ գտնվող, բայց ուղղանկյան այլ անկյուններին համապատասխանող նիշերով:

2. Եթե նիշը տողի մեջ վերջինն է, ապա այն փոխարինվում է նույն տողի առաջին նիշով: Վերծանման համար անհրաժեշտ է օգտագործել այս չորս կանոնների հակադարձումը՝ մերժելով «X» (կամ «Q») նիշերը, եթե դրանք բնօրինակ հաղորդագրության մեջ իմաստ չունեն [3]:

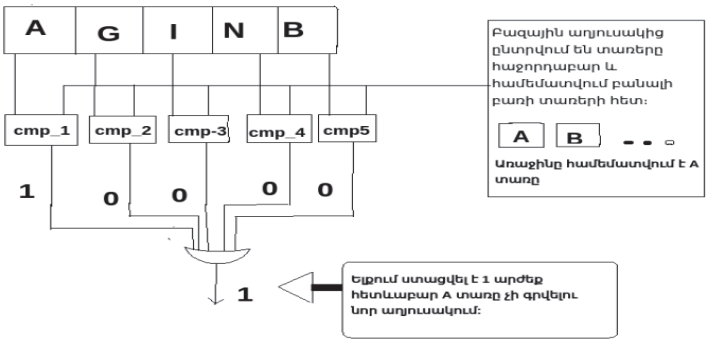
Հետազոտելով Փլեյֆերի շիֆրով աղյուսակը, որը պարունակում է 25 սիմվոլ, որոշվել է այդ տառերի բինար կոդավորման համար օգտագործել 5 բիթ՝ հիմնվելով $\log_2(25) <= 5$ բանաձևի վրա:

Տառերի կոդավորումը 5 բիթերի միջոցով ներկայացված է աղյուսակում:

Աղյուսակ

A=00001;	B=00010;	C=00011;	D=00100;	E=00101;
F=00110;	G=00111;	H=01000;	I=01001;	K=01010;
L=01011;	M=01100;	N=01101;	O=01110;	P=01111;
Q=10000;	R=10001;	S=10010;	T=10011;	U=10100;
V=10101;	W=10110;	X=10111;	Y=11000;	Z=11001;

Տվյալ գործողությունների քայլերը ներկայացնելու և իրականացնելու նպատակով մշակվել է փոփոխված աղյուսակի ձևավորման ալգորիթմի բլոկ-սխեման, ըստ որի՝ մշակվել է այդ աղյուսակը ձևավորող սարքի մշակված կառուցվածքային սխեման, որը պատկերված է նկ. 1-ում:

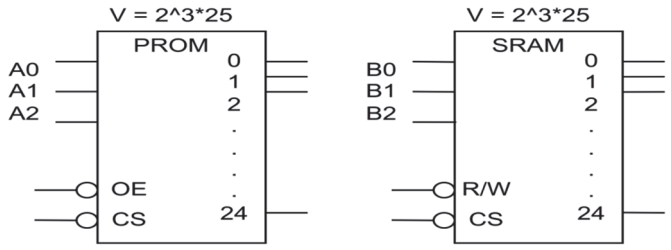


Նկ. 1. Բանալի բառի տառերի համեմատման մշակված պայմանական սխեման

Փլեյֆերի շիֆրով գաղտնագրման սարքի աղյուսակների մտապահման համար առաջարկվում է օգտագործել երկու տարբեր տեսակի հիշող սարքեր [4]:

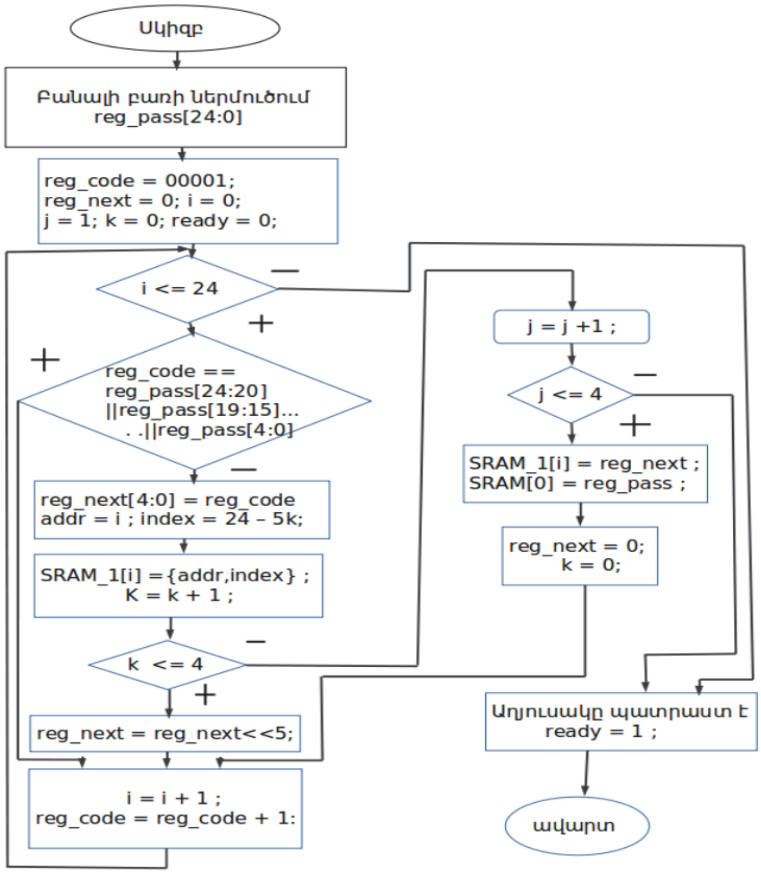
Բազային աղյուսակի մտապահման համար, որտեղ պահվում են 25 լատինական տառերը, կարելի է օգտագործել PROM հիշողություն, իսկ գաղտնաբառի

ներմուծմամբ ձեւափոխված աղյուսակի մտապահման համար՝ SRAM հիշողություն (նկ. 2) [5,6]:



Նկ. 2. Փլեյֆերի ծածկագրի սկզբնական և փոփոխված աղյուսակների մտապահման համար նախագծված սարքերի կառուցվածքները

Տառերի փոխարինման գործընթացի ալգորիթմի մշակված բլոկ-սխեման ներկայացված է նկ. 3-ում:



Նկ. 3. Տառերի փոխարինման գործընթացի ալգորիթմի մշակված բլոկ-սխեման

Հետևելով այս քայլերին, ստանում ենք տեքստը՝ կոդավորված ձևով՝ reg_pass [24:0]; գրանցում ենք բանալու 5 չկրկնվող տառերը: reg_code[4:0] - այստեղ հաջորդաբար գրանցվում են սկզբնական աղյուսակի տառերը համեմատման համար: reg_next[24:0] - գրանցվում են գաղտնաբառին չհամապատասխանող առաջին 5 տառերը, տառերը գրանցվում են հերթով աջից և տեղաշարժվում դեպի ձախ 5 բիթով նոր տառի դեպքում: i – ն՝ բազային աղյուսակի հերթական տառն է, j – ն՝ փոխված աղյուսակի հաջորդ տողերի հասցեները (հասցեներ 1,2,3,4): Աղյուսակի 0-րդ հասցեում գրանցվում է բանալին:

k-ն ցույց է տալիս, թե փոխված աղյուսակի հերթական տողի որ համարի տառն է: Տողում ֆիքսված է 5 տառ: SRAM_1 - առանձին հիշողություն, որտեղ պահվում է ստեղծված աղյուսակի տառերի կոորդինատը, այսինքն որ տողում է՝ addr, և տողի որերորդ բիթն է (index = 5k):

Եթե k = 0, ապա այդ տառը reg_nex-ի ամենաբարձր բիթերն են (24-5k = 24), եթե k = 1՝ 24- 5*1 = 19 և այլն: ready -ն ազդանշան է, որի առկայությունը հավաստում է ձևավորվող աղյուսակի պատրաստ լինելու մասին:

Բանալու տառերը ներմուծվում են հերթով՝

pass_1, pass_2, pass_3...pass_5;

հինգբիթանի ռեգիստրներում, որոնք միավորվում են reg_pass-ում՝

reg_pass={pass_1, pass_2 ... pass_5}:

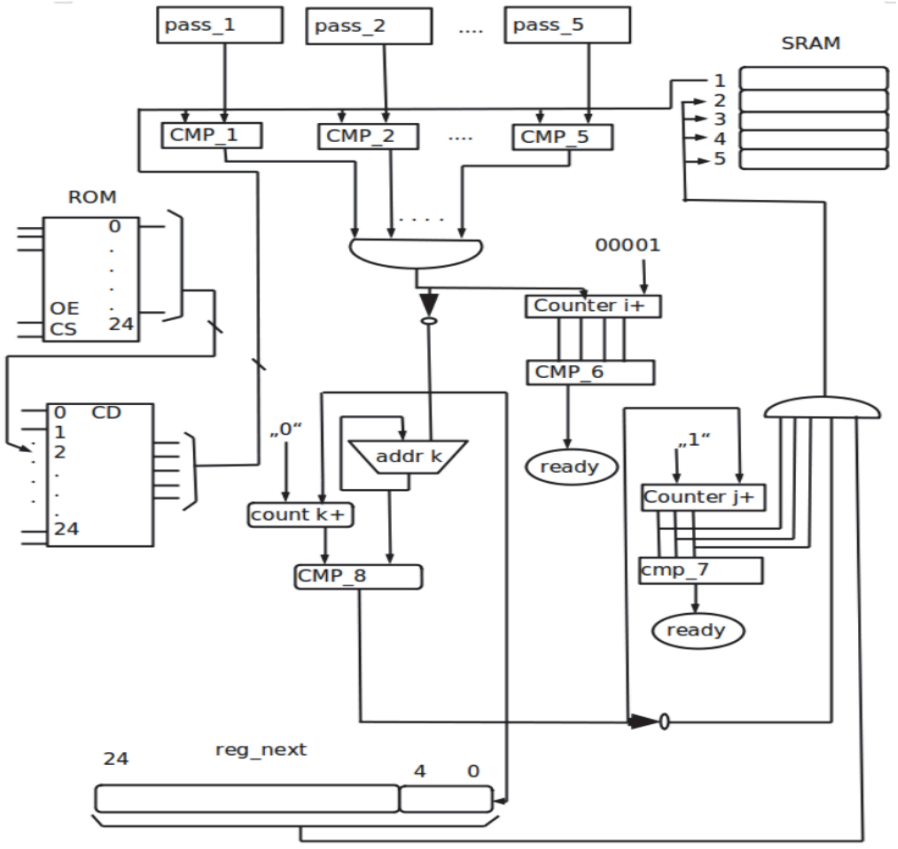
Կարելի է նաև միանգամից ներմուծել 25 բիթանի ռեգիստրում (reg_pass[24:0]):

SRAM հիշողության պարունակությունը ձևափոխող սարքի կառուցվածքային սխեման ներկայացված է նկ. 4-ում: Ըստ մշակված կառուցվածքային սխեմայի՝ գաղտնագրման բանալու 5 տառերից յուրաքանչյուրը պահվում է 5 հատ 5- կարգանի ռեգիստրներում: ROM հիշողությունում պահվում է Փլեյֆերի դասական աղյուսակը, որին կատարվում է դիմում՝ յուրաքանչյուր տառի կոդի հասցեով: ROM հիշողությունում տառերի քանակը 25-ն է, հետևաբար՝ i –ի արժեքով սահմանափակվում են տառերի քանակը և ալգորիթմի ցիկլիկ կազմակերպումը: ROM հիշողությունում տառերի և բանալու բառի տառերի համընկնումները ստուգվում են համեմատման սարքերի՝ կոմպարատորների միջոցով (CMP_1, CMP_2, CMP_3, CMP_4, CMP_5): Համընկնումները վերլուծվում են 5-մուտքանի «Կամ» տարրի միջոցով: Սխեմայում առկա Counter i-ն գումարող հաշվիչ է՝ M=25 հաշվի մոդուլով, դասական աղյուսակում տառերի քանակի վերահսկման համար, այսինքն, երբ Counter i-ի պարունակությունը հավասար է 24-ին, ապա CMP_6-ի միջոցով հաստատվում է տառերի փոխարինման գործընթացի ավարտը: SRAM հիշողության ձևավորման համար կա K արժեքի սահմանափակում, որի միջոցով հսկվում

է ձևափոխված աղյուսակի տողերի քանակը, ինչն իրականացվում է Counter k -ի եւ CMP_8 միջոցով:

Counter j -ի եւ CMP_7 միջոցով վերահսկվում է փոխված աղյուսակի տողերի հասցեների քանակը:

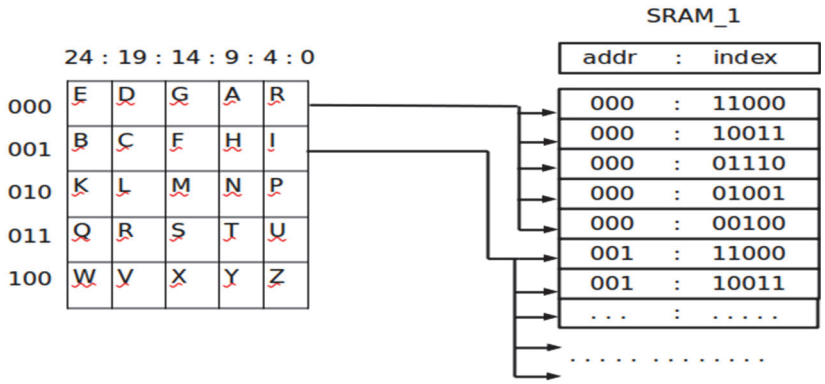
Ինչպես արդեն նշվել է, reg_next[24:0]-ը 25-կարգանի ձախ տեղաշարժող ռեգիստր է, որտեղ գրանցվում են գաղտնաբառին չհամապատասխանող հերթական 5 տառերը, որոնք գրանցվում են հերթով աջից և տեղաշարժվում դեպի ձախ 5 բիթով նոր տառի դեպքում: Ապա SRAM հիշողության հերթական տողում (1,2,3,4 տողերում) գրանցվում է reg_next[24:0] ռեգիստրի ամբողջական լրացված պարունակությունը [7]:



Նկ. 4. SRAM հիշողության պարունակությունը ձևափոխող սարքի մշակված կառուցվածքային սխեման

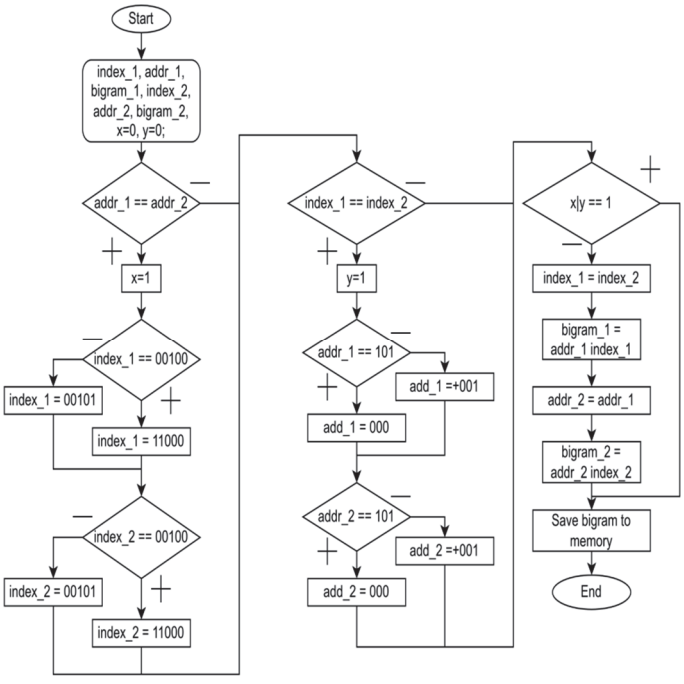
SRAM_1-ի յուրաքանչյուր տողում նշված տառերի կոորդինատները պարունակում են 2 տեսակի տեղեկություն՝ տառի 3-կարգանի հասցեն և 5- կարգանի

դիրքի սկզբնական բիթի համարը: Այդ պատճառով որոշվել է SRAM_1 հիշող սարքի ծավալը՝ V= 2^5 x 8: Նկ.5.-ում ներկայացված են SRAM_1 հիշողության պարունակությունը և կառուցվածքը նշված օրինակի համար (բանալի բառը՝ EDGAR):

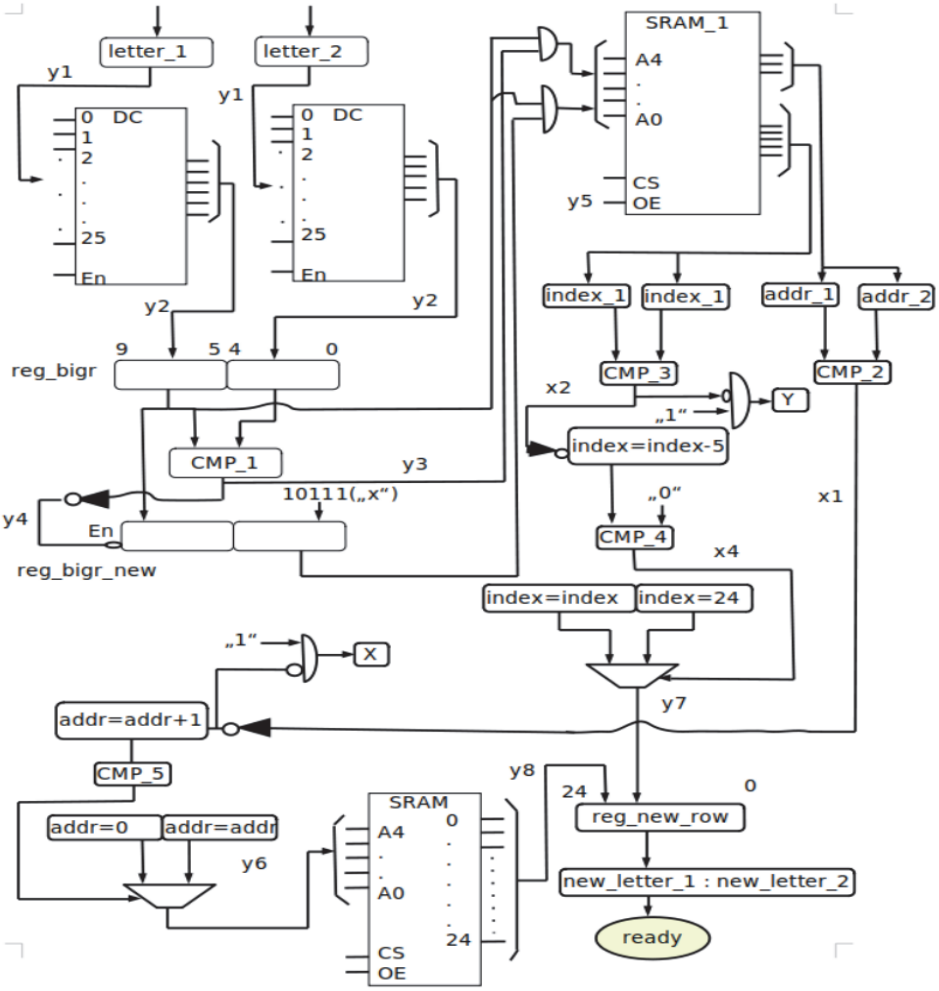


Նկ. 5. SRAM_1 հիշողության պարունակությունը և կառուցվածքը նշված օրինակի համար

Հետազոտելով Փլեյֆերի շիֆրով ձևափոխված աղյուսակի հիման վրա տառերի փոխարինման գործընթացը, մշակվել են այդ պրոցեսը կազմակերպող ալգորիթմի բլոկ- սխեման (նկ. 6) և կառուցվածքային սխեման (նկ. 7):



Նկ. 6. Տառերի փոխարինման գործընթացի ալգորիթմի բլոկ-սխեման



Նկ. 7. Տառերի փոխարինման գործընթացի կառուցվածքային սխեման

Փլեյֆերի ալգորիթմով գաղտնագրումն իրականացնող սարքի ապարատային իրագործումը կատարված է սարքավորումների նկարագրման Verilog HDL նախագծման լեզվի միջոցով [8]: Իսկ սարքերի վերջնական սինթեզումները կատարված են ISE DESIGN ավտոմատ նախագծման համակարգի կիրառմամբ, որի հնարավորությունները թույլ են տալիս վերլուծել և գնահատել նախագծված սարքերի աշխատանքի տևողությունը և ապարատային ծախսերը՝ ծրագրավորվող սարքերի ռեսուրսներ օգտագործման տեսակետից:

Նկարագրության ճշտությունը ստուգվել է Mentor Graphics ընկերության ModelSim փաթեթ-սիմուլյատորի կիրառմամբ, որի հիման վրա կատարվել է Verilog նկարագրման կոմպիլյացիան:

Եզրակացություն: Հետազոտելով և ուսումնասիրելով տառերի փոխարինման եղանակով Փլեյֆերի ալգորիթմի աշխատանքի սկզբունքները, այդ ալգորիթմի իրագործման համար մշակվել են.

1. Երեք տարբեր տեսակի և ծավալների հիշող սարքեր՝ դասական աղյուսակի մտապահման համար PROM հիշող սարքը՝ V=2^3x25 ծավալով, SRAM հիշողությունը՝ V=2^3x25 ծավալով, և տառերի կոորդինատների մտապահման հիշող սարքը՝ V=2^5 x 8 ծավալով:
2. Տառերի փոխարինման գործընթացը կազմակերպող սարքի կառուցվածքային սխեման, որի բարդությունը որոշվում է վերծանիչների կարգայնությամբ, SRAM և PROM հիշող սարքերի ծավալներով և ռեգիստրների քանակով ու կարգայնությամբ:

Վերլուծելով նախագծված սարքի մեկ բիգրամի սիմվոլների փոխաինման գործընթացի տևողությունը գործողության սկզբից մինչև ավարտման մասին ազդարարող ազդանշանը՝ սիմուլյատորի ժամանակային դիագրամի միջոցով, երևում է, որ այն կազմում է 210 նվ: Իսկ ապարատային ծախսերը, համաձայն հաշվետվության, կազմում են ծրագրավորվող սարքի (Spartan-3E, xc6s500e) ռեսուրսների մոտավորապես 9%-ը:

Հաշվարկվել է հիշող սարքերի ծավալների կախվածությունը Փլեյֆերի քառակուսում ընդգրկված սիմվոլների քանակից:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. https://crypto.stackexchange.com/questions/378/what-is-entropy
2. https://www.academia.edu/31794739/Vigenere_Cipher_Trends_Review_and_Possible_Modifications
3. https://crypto.interactive-maths.com/vigenegravere-cipher.html
4. **Крэндалл Р., Померанс К**. Простые числа: Криптографические и вычислительные аспекты/ Пер с англ.; Под ред. и с предисл. В.Н. Чубарикова.-М.: Книжный дом 'ЛИБРОКОМ&#39, 2015.- 664 с.
5. **Столлингс У.** Структурная организация и архитектура компьютерных систем. -5-е изд. –М.: Изд.дом “ Ильамс”, 2002.-893 с.
6. **Цилькер Б.Я., Орлов С.А.** Организация ЭВМ и систем.-СПб.: Питер, 2016.- 667 с.
7. **Saghatelyan A.** The Hardware Implementation of the Cryptographic Key Generation based on Diffie-Hellman algorithm// Հայաստանի ճարտարագիտական ակադեմիայի Լրաբեր. Գիտական հոդվածների ժողովածու.- 2015.- Հատոր 10, N 4. - էջ 760-763:

8. Ծրագրավորվող տրամաբանական սարքեր /**Ա.Թումանյան., Ա.Համազասպյան, Ա.Սաղաթելյան, և ուրիշ.** «Թվային սարքերի նախագծման միջոցներ» առարկայի դասընթացի մեթոդական ցուցումներ/ ՀՊՃՀ.-Եր.: Ճարտարագետ, 2014.- 90էջ:

Э.В. АЛЕКСАНЯН, А.К. САГАТЕЛЯН, Э.В. ВИРАБЯН

РАЗРАБОТКА И АППАРАТНАЯ РЕАЛИЗАЦИЯ КРИПТОУСТРОЙСТВА ПО ШИФРУ ПЛЕЙФЕРА

Исследованы вопросы аппаратной реализации криптоустройства по алгоритму Плейфера. Спроектированы структуры запоминающих устройств для хранения первоначальной и измененной таблиц и уточненной блок-схемы алгоритма загрузки символов текста и криптоключа. Спроектирована структурная схема криптоустройства по алгоритму Плейфера и оценены его быстродействие и аппаратные затраты с точки зрения ресурсов FPGA.

Ключевые слова: шифр Плейфера, структурная схема криптоустройства, аппаратная реализация, ресурсы FPGA.

E.V. ALEXANYAN, A.K. SAGHATELYAN, E.V. VIRABYAN

THE HARDWARE IMPLEMENTATION CRYPTOGRAPHIC DEVICE USING THE PLAYFAIR CODE

The issues on hardware implementation of a cryptodevice based on the Playfair algorithm have been studied. The mathematical substantiation of the algorithm is presented, a permanent memory device for storing the original and modified tables and a block diagram of the algorithm for loading text symbols and a cryptokey are developed. A block diagram of a cryptodevice based on the Playfair algorithm is designed and its performance and hardware costs are estimated from the point of view of FPGA resources.

Keywords: Playfair's cryptoalgorithm, encryption key, block diagram, hardware implementation, FPGA resourses.