ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Խեմչյան Արտակ Արարատի

ՍԽԱԼՆԵՐ ՈՒՂՂՈՂ ԿՈԴԵՐՈՎ ԳԱՂՏՆԻՔԻ ԲԱԺԽՄԱՆ ՄԻՋՈՑՆԵՐԻ ՄՇԱԿՈՒՄԸ

Ե.13.05 – «Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրերի համալիրներ» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

Երևան – 2017

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Хемчян Артак Араратович

РАЗРАБОТКА СРЕДСТВ РАСПРЕДЕЛЕНИЯ СЕКРЕТА НА ОСНОВЕ КОДОВ, ИСПРАВЛЯЮЩИХ ОШИБКИ

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.05 «Математическое моделирование, численные методы и комплексы программ»

Ереван – 2017

Ատենախոսության թեման հաստատվել է Հայաստանի ազգային պոլիտեխնիկական համալսարանում:

Գիտական ղեկավար՝	տեխ.գիտ.թեկնածու	Գ.Ի.Մարգարով
Պաշտոնական ընդդիմախոսներ՝	ֆիզ.-մաթ.գիտ.դոկտոր	Մ.Ե.Հարությունյան
	տեխ.գիտ.թեկնածու	Ա.Կ.Ասլանյան
Առաջատար կազմակերպություն՝	Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ	

Պաշտպանությունը կայանալու է 2017թ. հունիսի 6-ին, ժ. 17:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:
Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ գրադարանում:
Սեղմագիրը առաքված է 2017թ. մայիսի 6-ին:

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

Тема диссертации утверждена в Национальном политехническом университете Армении.

Научный руководитель:	кандидат тех. наук	Г.И.Маргаров
Официальные оппоненты:	доктор физ.-мат. наук	М.Е.Арутюнян
	кандидат тех. наук	А.К.Асланян
Ведущая организация:	Ереванский научно-исследовательский институт средств связи	

Защита состоится 6-ого июня 2017г. в 17:00 на заседании специализированного совета 037 «Информатика» Института проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.
С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.
Автореферат разослан 6-ого мая 2017г.

Ученый секретарь,
Специализированного совета 037
доктор физ.-мат.наук А.Г.Саруханян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Աշխատանքի արդիականությունը: Տեղեկատվական տեխնոլոգիաների արագ զարգացումը բերեց նրան, որ գաղտնի ինֆորմացիայի զգալի մասը պահպանվում է էլեկտրոնային ձևաչափերով, որի կորուստը կամ բացահայտումը կարող է անցանկալի հետևանքներ առաջացնել օգտատիրոջ համար: Դրան զուգահեռ ավելանում է տեղեկատվական համակարգերի վրա հարձակումների հավանականությունը, որոնց նպատակը կարող է լինել ինչպես գաղտնի ինֆորմացիայի բացահայտումը, այնպես էլ նրա վնասումը կամ փոփոխումը: Մյուս կողմից հնարավոր է ինֆորմացիայի կորուստը՝ կապված բնական երևույթների հետ: Նկարագրված դեպքերում կարող են օգտակար լինել գաղտնիքի բաշխման շեմային մեթոդները: Ի սկզբանե, առավել հայտնի գաղտնիքի բաշխման շեմային մեթոդները օգտագործվել են բանալիների բաշխման համար: Այսինքն, գաղտնի ինֆորմացիան գաղտնագրվում է, իսկ գաղտնագրման բանալին բաշխվում: Այս դեպքում լուծվում է գաղտնիության խնդիրը, սակայն չեն լուծվում ամբողջականության և հասանելիության խնդիրները: Եթե գաղտնագրված ինֆորմացիան վնասվի կամ հասանելի չլինի, ապա բանալու վերականգնմամբ հնարավոր չէ վերծանել այն: Ներկայումս տարածում է գտնում ինֆորմացիայի ամբողջական բաշխման տարբերակը, որն արդեն լուծում է հասանելիության և ամբողջականության խնդիրները: Հաշվի առնելով այն, որ գոյություն ունեցող մեթոդները դանդաղ են և ինֆորմացիայի ծավալը օր օրի աճում է, խնդիր է առաջանում մշակել ավելի արագագործ գաղտնիքի բաշխման շեմային մեթոդ: Հետազոտությունները ցույց են տալիս, որ արագագործ գաղտնիքի բաշխման շեմային մեթոդ կարելի է ստանալ սխալներ ուղղող կոդերի օգնությամբ:

Գաղտնիքի բաշխման մեթոդում կարևոր դեր ունի ոչ միայն բաշխման և վերականգնման արագությունը, այլ նաև բաղադրամասերի անվտանգությունը: Այդ իսկ պատճառով, գաղտնիքի բաշխման մեթոդը պետք է օժտված լինի բաղադրամասի ստուգման և անհրաժեշտության դեպքում կորած կամ վնասված բաղադրամասի վերականգնման հնարավորություններով: Այդ հնարավորությունները մեծացնում են ինֆորմացիայի անվտանգ պահպանման ժամանակը:

Աշխատանքի նպատակը կայանում է սխալներ ուղղող կոդերով գաղտնիքի բաշխման արագ միջոցների մշակումը: Այդ նպատակին հասնելու համար դրվել և լուծվել են հետևյալ խնդիրները՝

- մշակել գաղտնիքի բաշխման արագագործ շեմային մեթոդ, որը հնարավորություն կտա բաշխել և վերականգնել մեծ ծավալի ինֆորմացիա:
- մշակել սխալներ ուղղող կոդերով բաշխման դեպքում բաղադրամասի հավաստիության ստուգման մեթոդ:
- մշակել սխալներ ուղղող կոդերով բաշխման դեպքում վնասված կամ կորած բաղադրամասի արագ վերականգնման մեթոդ:

Գիտական նորույթ:

- Մշակվել է գաղտնիքի բաշխման շեմային մեթոդ՝ հիմնված սխալներ ուղղող կոդերի վրա, որն ի տարբերություն գոյություն ունեցողների ավելի արագ է և հնարավորություն է տալիս կատարել մեծ ծավալի ինֆորմացիայի բաշխում՝ ապահովելով ինչպես գաղտնիությունը, այնպես էլ ամբողջականությունն ու հասանելիությունը:
- Առաջարկվել է բաղադրամասի հավաստիության ստուգման արագ մեթոդ, որն ի տարբերություն գոյություն ունեցողների, հնարավորություն է տալիս ստուգել բաղադրամասը սխալներ ուղղող կոդերով բաշխման դեպքում և հայտնաբերել կեղծված կամ վնասված բաղադրամասերը :
- Առաջարկվել է վնասված կամ կորած բաղադրամասի արագ վերականգնման մեթոդ, որն ի տարբերություն գոյություն ունեցողների, հնարավորություն է տալիս օգտագործել այն սխալներ ուղղող կոդերով բաշխման դեպքում և մեծացնում է գաղտնիքի ապահով պահպանման ժամանակը:

Աշխատանքի գործնական նշանակությունը:

- Ստացված գիտական արդյունքների հիման վրա մշակվել է գաղտնիքի բաշխման ECC Sharing համակարգը, որը հնարավորություն է տալիս արագ բաշխել և վերականգնել մեծ ծավալի ինֆորմացիա, կատարել բաղադրամասի ստուգում, վերականգնել կորած կամ վնասված բաղադրամասերը, որի շնորհիվ բաշխման գործընթացը արագացել է 42.3%-ով, իսկ վերականգնմանը՝ 11.95%-ով:
- Ուսումնական նպատակների համար մշակված գաղտնիքի բաշխման մեթոդների հետազոտման ECC Sharing Explore համակարգը հնարավություն է տալիս հետազոտել ինչպես կոդերով, այնպես էլ գոյություն ունեցող այլ բաշխման մեթոդները: Համակարգը հնարավորություն է տալիս համեմատել բաշխման մեթոդները ըստ արագագործության:

Պաշտպանության են ներկայացվում հետևյալ դրույթները:

- Գաղտնիքի շեմային բաշխման արագ մեթոդ, որն աշխատում է սխալներ ուղղող կոդերի հիման վրա և ապահովում է ինչպես գաղտնիությունը, այնպես էլ ամբողջականությունն ու հասանելիությունը:
- Բաղադրամասի հավաստիության ստուգման մեթոդ, որը կիրառելի է սխալներ ուղղող կոդերով բաշխման դեպքում:
- Վնասված կամ կորած բաղադրամասի արագ վերականգնման մեթոդ, որի ընթացքում գաղտնիքի վերականգնում չի կատարվում և որը կիրառելի է սխալներ ուղղող կոդերով բաշխման դեպքում:

Ներդրումները:

Ստենախոսության շրջանակներում մշակված ECC Sharing ծրագրային միջոցը ներդրվել է «ԱՅ ԷՅ ԷՄ Քլաուդ լիմիթեդ» ընկերության Հայաստանյան մասնաճյուղում գաղտնի ինֆորմացիայի ապահով պահպանման նպատակով: Ծրագրային միջոցի կիրառմամբ ընկերությունում կատարվում է գաղտնի ինֆորմացիայի անվտանգ պահուստավորումը և անհրաժեշտության դեպքում արագ վերականգնումը:

Ատենախոսության շրջանակներում մշակված ECC Sharing Explore ծրագրային միջոցը օգտագործվում է ՀԱՊՀ ՏԱԾԱ ամբիոնում լաբորատոր աշխատանքների անցկացման համար:

Աշխատանքի արդյունքները զեկուցվել են. "Հաջորդ սերնդի կիբեռ անվտանգություն" ուսանողական կոնֆերանսում (ԱՊՀ և Ռուսաստան փուլ, 2014թ., ք. Մոսկվա, Ռուսաստան), "Հաջորդ սերնդի կիբեռ անվտանգություն" ուսանողական կոնֆերանսում (եզրափակիչ փուլ, 2014թ., ք. Ստոկհոլմ, Շվեդիա), ՀԱՊՀ տարեկան գիտաժողովում (2015թ., ք. Երևան), "ՆԱՏՕ առաջադեմ հետազոտական աշխատաժողով"-ում (NATO ARW, 2015թ., գ. Աղվերան, ՀՀ), "Քոմփյութերային գիտությունների և տեղեկատվական տեխնոլոգիաների" միջազգային գիտաժողովում (CSIT 2015թ., ք. Երևան), "Գիտության և տեխնոլոգիաների մերձեցում" գիտաժողովում (STC, 2016թ. ք. Երևան), "Միջազգային գիտափորձնական ուսանողների և երիտասարդ գիտնականների գիտաժողով"-ում (Ազգային ավիացիոն համալսարան, 2016թ. ք. Կիև, Ուկրաինա), "XIII միջազգային գիտական և տեխնիկական կոնֆերանսում – նոր ինֆորմացիոն տեխնոլոգիաներ և համակարգեր" (NITaS, 2016թ. ք. Պենզա, Ռուսաստան), "Ինտերնետ անվտանգության համաշխարհային կոնգրես"-ում (WorldCIS-2016, 2016թ. ք. Լոնդոն, Մեծ Բրիտանիա), ՀԱՊՀ ՏԱԾԱ ամբիոնի գիտատեխնիկական սեմինարներում (2014-2017թ., ք. Երևան):

Հրապարակումներ: Ատենախոսության հիմնական արդյունքները տպագրված են 10 գիտական աշխատություններում, որոնք թվարկված են սեղմագրի վերջում:

Աշխատանքի կառուցվածքը և ծավալը: Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, եզրակացությունից և 56 անուն օգտագործված գրականության ցուցակից: Աշխատանքի ընդհանուր ծավալն է 107 էջ՝ ներառյալ 29 նկար: Հավելվածները կազմում են 2 էջ:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածություն: Ներածության մեջ հիմնավորված է թեմայի արդիականությունը, ձևակերպված են աշխատանքի նպատակները, գիտական նորույթները և հիմնական դրույթները, որոնք ներկայացվում են պաշտպանության:

Գլուխ առաջին: Ատենախոսության առաջին գլխում դիտարկված է գաղտնիքի բաշխման գաղափարը, նրա տեսակները և առանձնահատկությունները: Բերված են ներկայում առավել հայտնի բաշխման մեթոդները: Դիտարկվում են գաղտնիքի բաշխման մեթոդներում բաղադրամասի ստուգման, վնասված կամ կորած բաղադրամասի վերականգնման և բաղադրամասերի պարբերական թարմացման հնարավորությունները: Այս գլխում նաև համեմատվում են ինֆորմացիայի գաղտնագրման, այնուհետև գաղտնագրման բանալու բաշխման և ինֆորմացիայի ամբողջական բաշխման տարբերակները, տրվում է նրանց առավելություններն ու թերությունները: Այս գլխում է նկարագրված նաև սխալներ ուղղող կոդերի կառուցվածքային առանձնահատկությունները և կարևոր սահմանումները: Այս գլխում բերված է նաև այլ հեղինակների կողմից՝ սխալներ ուղղող կոդերի հիման վրա գաղտնիքի բաշխման մեթոդների ուղղությամբ կատարված աշխատանքների ներկա վիճակը:

Գլխի վերջում, կատարված հետազոտությունների հիման վրա, ձևավորվել է աշխատանքի նպատակը, և դրվել են այն խնդիրները, որոնք հարկավոր է լուծել այդ նպատակին հասնելու համար:

Գլուխ երկրորդ: Երկրորդ գլխում նկարագրված է սխալներ ուղղող կոդերով աշխատող գաղտնիքի բաշխման շեմային մեթոդը, որը հնարավորություն է տալիս բաշխել և վերականգնել մեծ ծավալի ինֆորմացիա: Հետազոտությունների արդյունքում, որոշվել է գաղտնիքի բաշխման մեթոդը կառուցել հատվածային սխալներ ուղղող կոդերի վրա: Մշակված մեթոդը ճկուն է և կարող է աշխատել այլ երկուական հատվածային կոդերի դեպքում նույնպես: Ալգորիթմի աշխատանքը սկսվում է նրանից, որ գաղտնի ինֆորմացիան կոդավորվում է ընտրված սխալներ ուղղող կոդով: Կոդավորված ինֆորմացիան պայմանական ներկայացվում է նկ.1-ում պատկերված երկչափ զանգվածի տեսքով: Այդ զանգվածում սյուների քանակը կախված է սխալներ ուղղող կոդից (կոդաբառի երկարությունից), իսկ տողերի քանակը կախված է նախնական ինֆորմացիայի ծավալից: Զանգվածի յուրաքանչյուր տող իրենից ներկայացնում է այդ կոդի կոդաբառ: Ալգորիթմը դիտարկենք $(31,21,2)$ երկու սխալ ուղղող կոդի համար: Տվյալ դեպքում k=31: Քանզի այս զանգվածի յուրաքանչյուր տող իրենից ներկայացնում է (31,21,2) կոդի կոդաբառ, իսկ այդ կոդը կարողանում է ուղղել կամայական երկու սխալ, ապա դժվար չէ նկատել, որ կամայական երկու սյան բացակայության դեպքում, հնարավոր է դրանք վերականգնել: Այդ նպատակին հասնելու համար անհրաժեշտ է յուրաքանչյուր տողի համար աշխատացնել այդ կոդի ապակոդավորման ալգորիթմը:

1	2	3	...	k
$V_{1,1}$	$V_{1,2}$	$V_{1,3}$	⋯	$V_{1,k}$
$V_{2,1}$	$V_{2,2}$	$V_{2,3}$	⋯	$V_{2,k}$
$V_{3,1}$	$V_{3,2}$	$V_{3,3}$	⋯	$V_{3,k}$
$V_{4,1}$	$V_{4,2}$	$V_{4,3}$	⋯	$V_{4,k}$
$V_{5,1}$	$V_{5,2}$	$V_{5,3}$	⋯	$V_{5,k}$
...	...	...	...	...
$V_{q,1}$	$V_{q,2}$	$V_{q,3}$	⋯	$V_{q,k}$

Նկ. 1. Կոդավորված գաղտնի ֆայլի կառուցվածքը:

Այժմ, եթե ենթադրենք, որ յուրաքանչյուր սյուն իրենից ներկայացնում է առանձին բաղադրամաս, ապա որոշակի վերապահումներով կարելի է ասել, որ այդ տարբերակով բաշխումը կբերի (29,31) շեմային կառուցվածքի: Սակայն այս տարբերակով ստացված բաղադրամասերը (բաղադրամաս-ֆայլերը) ունեն ավելի փոքր ծավալ, որը և անվտանգության տեսանկյունից է վատ (հատարկումը ավելի արագ կկատարվի) և հակասում է գաղտնիքի բաշխման շեմային մեթոդներին ներկայացվող պահանջներից մեկին (բաղադրամասի և գաղտնիքի ծավալները պետք է լինեն հավասար): Որպեսզի լուծվի այս խնդիրը և ստացվեն նաև այլ շեմային կառուցվածքներ, առաջարկվել է կատարել սյուների խմբավորում՝ որոշակի օրինաչափությամբ: Այդ նպատակի համար գեներացվում են կոնկրետ շեմային կառուցվածքներ ապահովող աղյուսակներ: Օրինակ աղյուսակ 1-ը ապահովում է (4,5) շեմային կառուցվածք (31,21,2) կոդի համար:

Աղյուսակ 1: (31,21,2) կոդով (4,5) շեմային կառուցվածք

Մաս 1	17	23	14	18	13	3	19	26	16	9	12	8	5	15	6	2	10	1	7	4	29
Մաս 2	25	15	5	10	23	17	1	4	22	9	12	13	7	16	3	18	6	8	2	28	30
Մաս 3	15	7	21	17	8	3	27	19	6	23	13	2	16	10	18	4	5	9	24	25	1
Մաս 4	18	14	16	10	26	21	1	4	15	9	11	13	7	6	5	17	2	3	23	8	28
Մաս 5	27	29	30	10	8	3	1	4	6	9	11	13	14	15	16	17	22	24	2	7	5

Աղյուսակում յուրաքանչյուր տող իրենից ներկայացնում է առանձին բաղադրամաս, իսկ այդ տողում նշված են այն սյուների համարները, որոնք տրվելու են այդ բաղադրամասին: Դժվար չէ նկատել, որ կամայական չորս բաղադրամասի միավորումից հավաքվում է 29 սյուն, իսկ դա, ինչպես արդեն նշվեց, բավարար է բացակայող սյուները վերականգնելու համար: Այսինքն այս տարբերակով բաշխման դեպքում ստացվում է (4,5) շեմային կառուցվածք:

Ակնհայտ է, որ խմբավորման աղյուսակները զուգորդություններ են կրկնություններով: Առաջարկվել է խմբավորման աղյուսակների ձևավորման երկու մոտեցում: Առաջին մոտեցման դեպքում բոլոր հնարավոր բաղադրամասերից հատարկման եղանակով ստացվում են խմբավորման աղյուսակները: Բոլոր հնարավոր բաղադրամասերի քանակը որոշվում է հետևյալ բանաձևով՝

$$C_m^k = \frac{m!}{k!\cdot(m-k)!} \quad (1)$$

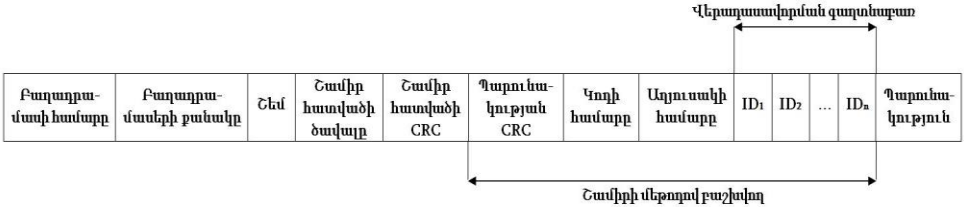
Մյուս մոտեցման դեպքում, որպես (h,n) բաշխման աղյուսակ ընտրվում է $R(n,n-h+1)$ հավասարակշիռ կոդի բոլոր կոդաբառերի աղյուսակից ստացվող աղյուսակը, իսկ այդ աղյուսակին բավարարող կոդը ունի հետևյալ տեսքը՝$(\mathrm{m,k,t})$, որտեղ՝

$$m = \frac{n!}{(h-1)!\cdot(n-h+1)!} + h - n + 1, k = \frac{n!}{(h-1)!\cdot(n-h+1)!} + t,\ t = 1,2,3\ldots \quad (2)$$

Առաջին մոտեցման դեպքում ընտրվում է կոդը, որից հետո ձևավորվում է աղյուսակը, իսկ երկրորդ մոտեցման դեպքում ձևավորվում է աղյուսակը և որոշվում այն կոդի տվյալները, որին բավարարում է այդ աղյուսակը: Երկրորդ մոտեցումը էականորեն արագացնում է աղուսակի ձևավորման գործընթացը և նախատեսված է երկար կոդերի համար:

Այս տարբերակով բաշխումը ապահովում է շեմային կառուցվածքը, սակայն անվտանգության տեսանկյունից ունի բաց կողմ: Շեմային մեթոդներին ներկայացվող պահանջներից մեկն ասում է, որ շեմից պակաս բաղադրամասեր ունեցողը ոչինչ չպետք է կարողանա իմանալ գաղտնի ինֆորմացիայի վերաբերյալ: Այս դեպքում ակնհայտ է, որ պայմանական հակառակորդը, ունենալով նույնիսկ մեկ բաղադրամաս, իմանում է որոշակի սյուների պարունակությունը: Չնայած այն հանգամանքին, որ այդ ճանապարհով գաղտնիքի ամբողջական բացահայտում հնարավոր չէ, այնուամենայնիվ այդ խնդրի լուծման համար առաջարկվում է մի մոտեցում, որը պայմանականորեն կանվանենք վերադասավորում: Վերադասավորում գործողության իմաստը կայանում է նրանում, որ մինչ բաշխման գործընթացը, խմբավորման աղյուսակում կատարվեն որոշակի տեղափոխումներ, որի կատարման ձևի մասին հակառակորդը չպետք է իմանա: Առաջարկվում է խմբավորման աղյուսակում սյուները միմյանց հետ տեղափոխել, որից հետո ձևափոխված աղյուսակով կատարել բաշխում: Այլ կերպ ասած՝ խմբավորման աղյուսակը գաղտնագրվում է վերադասավորման գաղտնագրով: Ակնհայտ է, որ այդ տեղափոխությունը չի խախտում աղյուսակով ստացվող շեմային կառուցվածքը, բայց միևնույն ժամանակ հակառակորդին զրկում է աղյուսակին տիրապետելու հնարավորությունից: Վերադասավորման համար առաջարկվում է գեներացնել որոշակի քանակությամբ սյուների համարներ, որոնք անհրաժեշտ է զույգ առ զույգ տեղափոխել դիրքերով: Գեներացված հաջորդականությունը պայմանական անվանենք վերադասավորման գաղտնաբառ և որն ունի հետևյալ տեսքը՝ $ID_1,ID_2,ID_3,\ldots,ID_n$: Գեներացված սյուների քանակը պետք է լինի զույգ: Բաշխման ժամանակ օգտագործված գաղտնաբառը անհրաժեշտ է նաև վերականգնող կողմին, հակառակ դեպքում հնարավոր չի լինի ստանալ ձևափոխված (գաղտնագրված) աղյուսակը և կատարել գաղտնիքի վերականգնումը: Քանզի այդ գաղտնաբառը բաղադրամասերում (ֆայլերում) բաց տեսքով պահել հնարավոր չէ, այդ պատճառով

առաջարկվում է այն բաշխել կատարյալ գաղտնիություն ապահովող Շամիրի շեմային մեթոդով և ստացված բաղադրամասերը (գաղտնաբառի բաղադրամասերը) կցել ձևավորվող բաղադրամասերին (նոր մեթոդով բաշխվող ինֆորմացիայի բաղադրամասերին): Որպես բաշխման տվյալներ օգտագործվում են նախապես ընտրված շեմային կառուցվածքի տվյալները: Շեմի քանակով բաղադրամասերի միավորումից հետո հնարավոր կլինի վերականգնել վերադասավորման գաղտնաբառը, աղյուսակում կատարել վերադասավորումը և վերականգնել գաղտնիքը: Ձևավորվող բաղադրամաս ֆայլերի կառուցվածքը ներկայացված է նկ. 2-ում:

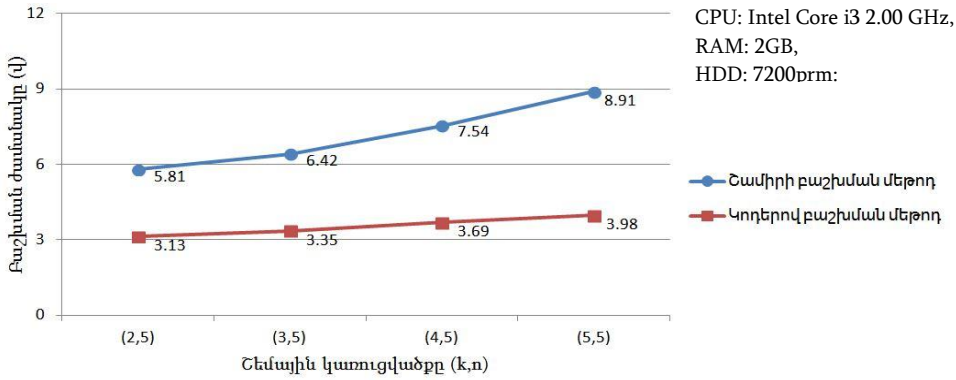


Նկ. 2. Բաղադրամաս ֆայլի կառուցվածքը:

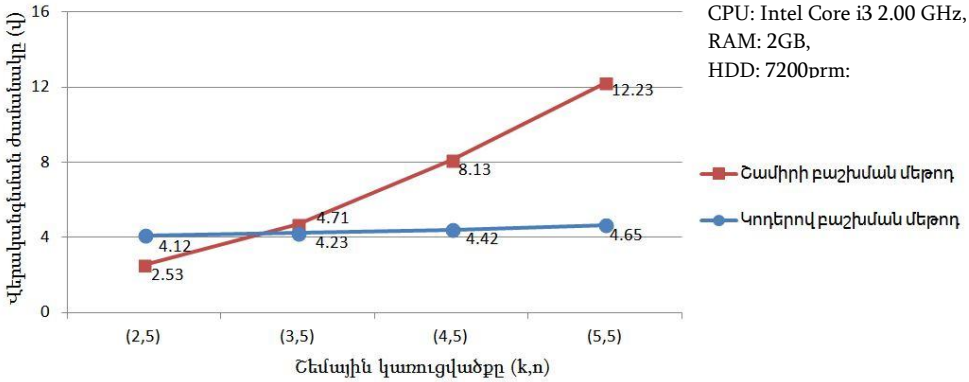
Հաշվի առնելով բաշխման համար ընտրված կոդի և համապատասխան աղյուսակի «անհրաժեշտությունը» հակառակորդին, այդ երկու տվյալը նույնպես կցվում է վերադասավորման գաղտնաբառին և բաշխվում Շամիրի մեթոդով: Հարկավոր է նշել, որ այդ հատվածի ծավալը շատ փոքր է և արագագործության առումով գրեթե չի ազդի մշակված մեթոդի արագագործության վրա (քանզի մեթոդը նախատեսված է մեծ ծավալի ինֆորմացիա բաշխելու համար):

Նկ. 3-ում պատկերված են Շամիրի մեթոդի և մշակված մեթոդի բաշխման արագործությունների գրաֆիկները: Նկ. 4-ում պատկերված է այդ մեթոդների վերականգնման արագագործության գրաֆիկները:

Այս գլխում ներկայացված են այլ փորձնական արդյունքներ նույնպես: Օրինակ 2Gb ծավալով ինֆորմացիա բաշխելու դեպքում մշակված մեթոդը 42.3%-ով ավելի արագ է քան Շամիրի մեթոդը: Վերականգնման դեպքում առավելությունը 11.95% է:



Նկ. 3. Մշակված և Շամիրի մեթոդներով 10Մբ ծավալով ինֆորմացիայի բաշխման արագագործության գրաֆիկները:



Նկ. 4. Մշակված և Շամիրի մեթոդներով 10Մբ ծավալով ինֆորմացիայի վերականգնման արագագործության գրաֆիկները:

Գլուխ երրորդ: Այս գլխում ներկայացվում են սխալներ ուղղող կոդերով բաշխման դեպքում բաղադրամասի հավաստիության ստուգման և կորած կամ վնասված բաղադրամասի վերականգնման մեթոդները: Բաղադրամասի ստուգման մեթոդի հիմքում ընկած է Շամիրի մեթոդում բաղադրամասի ստուգման մեթոդը: Մշակված ալգորիթմում բաղադրամասի ստուգումը հիմնված է **"Շամիրի մեթոդով բաշխվող"** և **"Պարունակություն"** հատվածների ստուգման վրա: Գաղտնիքը բաշխողը բաշխումից առաջ որոշում է Շամիրի մեթոդում օգտագործվող g, q և p թվերը, որից հետո հաշվարկում և հրապարակում է $r_0, r_1, \dots, r_t$-ն: Այնուհետև ընտրում է բաշխման համար սխալներ ուղղող կոդը և այն աղյուսակը, որով պետք է կատարվի գաղտնի ինֆորմացիայի բաշխումը: Հաջորդ քայլում բաշխողը գեներացնում է $ID_1, ID_2, \dots, ID_n$ վերադասավորման գաղտնաբառը, նրան կցում սխալներ ուղղող կոդի և աղյուսակի համարները և համարելով դա որպես S գաղտնիք, կատարում է այդ հատվածի բաշխումը Շամիրի մեթոդով: Որպես բաշխման տվյալներ ընդունվում են այն բաղադրամասերի քանակը և շեմի արժեքը, որը օգտագործվելու է գաղտնի ինֆորմացիայի բաշխման ժամանակ: Այս ամենից հետո կատարվում է գաղտնի ինֆորմացիայի բաշխումը, որից հետո այն ոչնչացվում է: Վերջին քայլում բաշխողի կողմից հաշվարկվում և հրապարակվում են ստացված բաղադրամասերի **«Պարունակություն»** հատվածների CRC32 արժեքները (CRC1,CRC2,…,CRCn): Հաշվի առնելով, որ CRC32-ը միակողմանի ֆունկցիա է, ապա կարող ենք պնդել, որ նրա հրապարակումը ոչինչ չի բացահայտում բաղադրամասի պարունակության վերաբերյալ և հետևաբար անվտանգության տեսանկյունից ոչ մի խնդիր չի առաջացնում: Այսքանով բաշխողի կողմից բաշխման գործընթացն ավարտվում է:

Այժմ դիտարկենք այն գործողությունների հաջորդականությունը, որը պետք է կատարի բաղադրամաս ստացողը, որպեսզի համոզվի, որ իր բաղադրամասը իրական է և փոփոխված չէ:

1. Ստանալով բաղադրամասը, հարկավոր է առանձնացնել **«Շամիրի մեթոդով բաշխվող»** հատվածը և վերը նկարագրված ալգորիթմով ստուգել այդ հատվածի իսկությունը (օգտագործելով բաշխողի կողմից հրապարակված

տվյալները): Եթե այդ հատվածում սխալ չի հայտնաբերվում , ապա հարկավոր է շարունակել ստուգումը և պարզել **«Պարունակություն»** հատվածի իսկությունը: Եթե **«Շամիրի մեթոդով բաշխվող»** հատվածում սխալ է հայտնաբերվում, ապա ստուգումը ավարտվում է, իսկ բաղադրամասը համարվում փոփոխված (կեղծված կամ վնասված):

2. Առաջին կետի ստուգման դրական արդյունքի դեպքում, բաղադրամասի սեփականատերը հաշվարկում է **«Պարունակություն»** հատվածի CRC32 արժեքը և համեմատում այն բաշխողի կողմից հրապարակված համապատասխան CRC32 արժեքի հետ: Համընկնելու դեպքում համարվում է, որ այդ հատվածում փոփոխություն չի կատարվել և սրանով ստուգման գործընթացը ավարտվում է:

Ինչպես տեսանք, ստուգման գործընթացից դուրս մնացին **«Բաղադրամասի համարը»**, **«Բաղադրամասերի քանակը»**, **«Շեմը», «Շամիր հատվածի ծավալը»** և **«Շամիր հատվածի CRC»** հատվածները: Այս հատվածները չստուգելու պատճառը հետևյալն է:

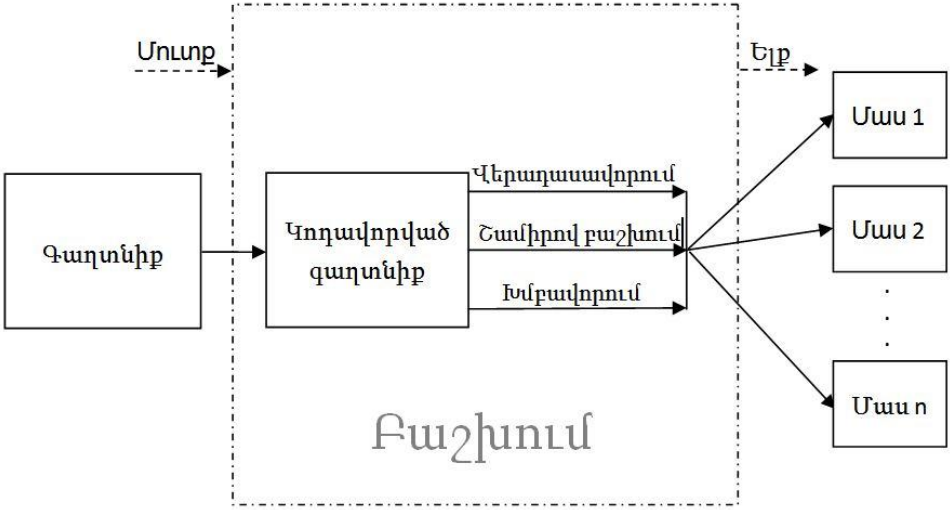
1. **«Բաղադրամասի համարը»**, **«Բաղադրամասերի քանակը»** և **«Շեմը»** տվյալները համարվում են հայտնի և դրանց ստուգման համար լրացուցիչ ալգորիթմական լուծումներ հարկավոր չեն:
2. **«Շամիր հատվածի ծավալը»** և **«Շամիր հատվածի CRC»** հատվածները ստուգելու կարիք չկա, քանզի նրանցից առնվազն մեկի փոփոխությունն արդեն կառաջացնի սխալ **“Շամիրի մեթոդով բաշխվող»** հատվածի ստուգման ընթացքում:

Այսքանով բաղադրամասերի ստուգման գործընթացը կարելի է համարել ավարտված: Այժմ դիտարկենք այս եղանակով բաղադրամասերի ստուգման հավաստիությունը: Հնարավո՞ր է արդյոք “խափել” այս ստուգման մեթոդին: Քանի որ ստուգման գործընթացը բաժանված է երկու մասի, ապա անվտանգության ստուգման համար դիտարկենք նրանցից յուրաքանչյուրն առանձին:

1. **“Շամիրի մեթոդով բաշխվող»** հատվածի անվտանգությունը հիմնված է Շամիրի մեթոդով բաղադրամասերի ստուգման վրա, իսկ այդ մեթոդը համարվում է, որ ապահովում է կատարյալ անվտանգությունը: Հետևաբար այս հատվածի ստուգման իսկությունը կասկած չի հարուցում:
2. **“Պարունակություն”** հատվածի ստուգման ժամանակ օգտագործվում է CRC32, որը կարելի է համարել հեշ ֆունկցիա: Իհարկե հեշ ֆունկցիաների դեպքում գոյություն ունի կոլիզիայի հավանականություն և տեսականորեն հնարավոր է, որ լինի այլ **“Պարունակություն”** հատված, որի դեպքում ստացվի միևնույն CRC32 արժեքը: Սակայն հաշվի առնելով, որ **“Պարունակություն”** հատվածը ունի մեծ ծավալ և այդ ծավալը գաղտնի չէ, ապա հակառակորդի խնդիրը էականորեն բարդանում է: Նա պետք է փորձի գտնել այդ նույն երկարության այլ բիթային հաջորդականություն, որի դեպքում կստացվի նույն CRC32 արժեքը: Չնայած որ այս գործողությունը բավականին բարդ է և ժամանակատար, այնուամենայնիվ անհրաժեշտության դեպքում կարելի է

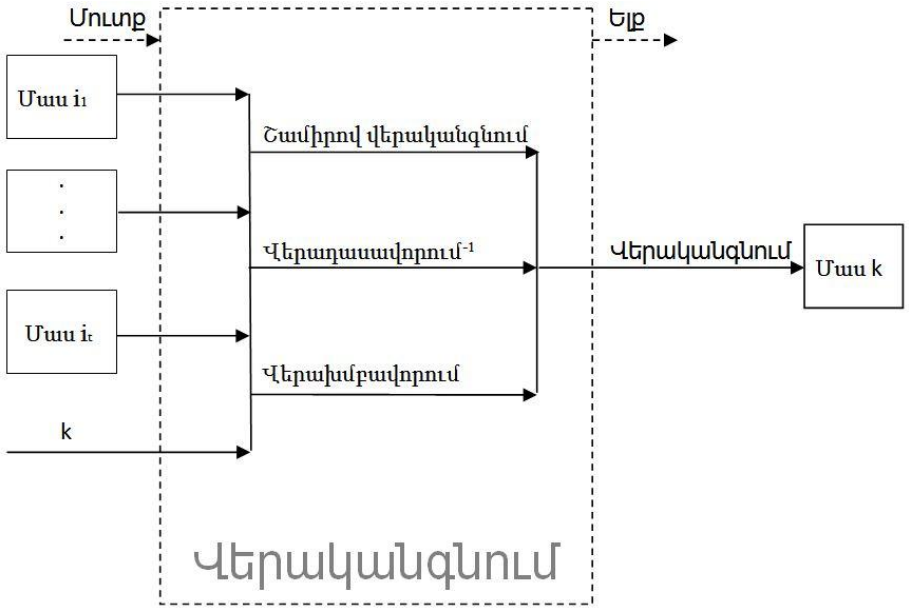
CRC32-ը փոխարինել այլ՝ ավելի երկար հեշ ֆունկցիայով, որի դեպքում շատ ավելի դժվար կլինի գտնել միևնույն հեշ արժեք ունեցող և նույն երկարության բիթային հաջորդականություն: CRC32-ի ընտրությունը պայմանավորված է նրա արագագործությամբ և միաժամանակ փոքր ծավալով:

Այս գլխում նաև նկարագրված է սխալներ ուղղող կոդերով բաշխման համար կորած կամ վնասված բաղադրամասի վերականգնման մեթոդը: Վերականգնման մեթոդը հիմնված է գաղտնիքի միջանկյալ բացահայտման վրա, սակայն այդ գործընթացում բացակայում է վերջնական ապակոդավորման գործողությունը: Մեթոդը էականորեն ավելի արագ է, քան պարզապես գաղտնիքի վերականգնումը և կրկին բաշխումը: Մեթոդի աշխատանքի նկարագրության համար հարկավոր է ներկայացնել բաշխման ալգորիթմի բլոկ-սխեման, որը պատկերված է նկ. 5-ում:



Նկ. 5. Գաղտնիքի բաշխման մեթոդի աշխատանքը:

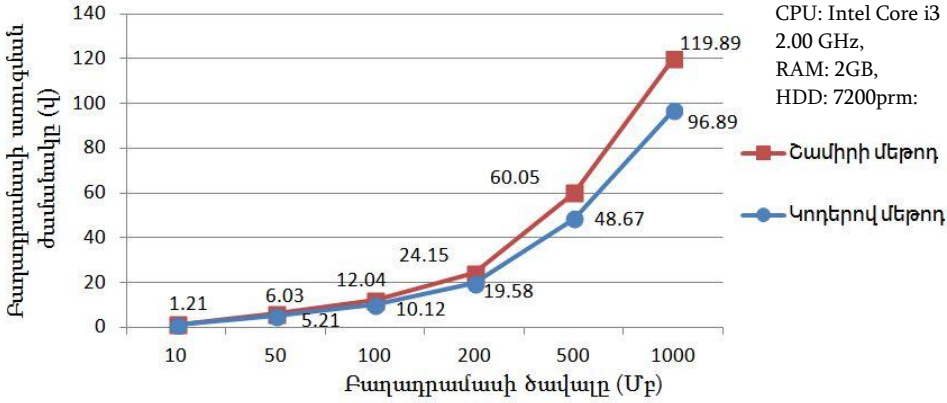
Վերականգնման գործընթացը պատկերված է նկ. 6-ում: Ինչպես տեսնում ենք որպես մուտքային տվյալներ տրվում են t հատ բաղադրամաս և այն բաղադրամասի համարը, որը անհրաժեշտ է վերականգնել: Բաղադրամասի վերականգնման համար նախ անհրաժեշտ է վերականգնել **“Շամիրի մեթոդով բաշխվող»** հատվածը և ստանալ վերադասավորման գաղտնաբառը, սխալներ ուղղող կոդի և աղյուսակի համարները: Ունենալով այդ տվյալները հնարավոր է կատարել վերադասավորման և խմբավորման հակադած գործողությունները: Այս ամենից հետո գաղտնիքի վերականգնման համար անհրաժեշտ է կատարել ապակոդավորման գործողությունը, սակայն բաղադրամասի վերականգնման համար այդ գործընթացը անհրաժեշտ չէ: Վերականգնման համար անհրաժեշտ է ստացված տվյալներից առանձնացնել այն սյուների տվյալները, որոնք օգտագործվել են k-րդ բաղադրամասի ստացման համար:



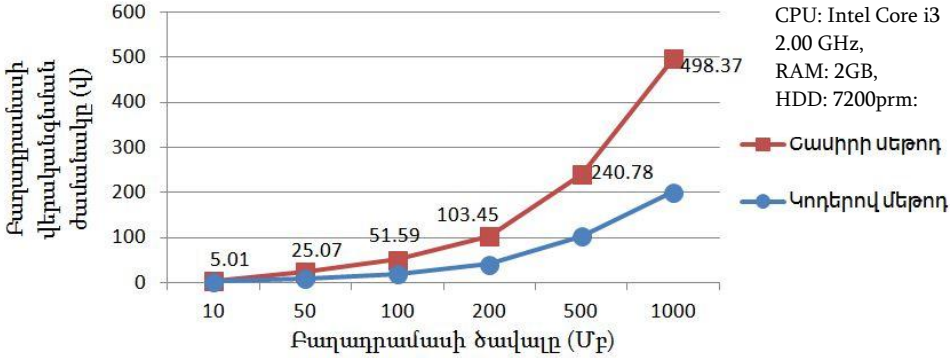
Նկ. 6. Կորած բաղադրամասի վերականգնումը:

Դիտարկենք օրինակ: Ենթադրենք բաշխման համար օգտագործվել է աղյուսակ 1-ը, որն ապահովում է (4,5) շեմային կառուցվածք: Որպես կորած բաղադրամաս դիտարկենք առաջին բաղադրամասը: Այս դեպքում վերականգնման համար որպես մուտքային տվյալներ հարկավոր է տալ 2-5 բաղադրամասերը և 1 թիվը: **“Շամիրով վերականգնում”**, **“Վերադասավորում$^{-1}$”** և **“Վերախմբավորում”** գործողություններից հետո կստանանք այն սյուների տվյալները, որոնք նշված են 2-5 բաղադրամասերի դիմաց: Դժվար չէ տեսնել, որ առաջին բաղադրամասի համար անհրաժեշտ սյուները այդտեղ առկա են: Անհրաժեշտ է վերցնել այդ սյուների տվյալները և ձևավորել առաջին բաղադրամասը: Այս գործընթացից դուրս մնաց ամենաժամանակատար գործողությունը՝ ինֆորմացիայի ապակոդավորումը և բացակայող սյուների վերականգնումը: Նկարագրված մեթոդը չի կարող վերականգնել կորած բաղադրամասը այն դեպքում, երբ $t = n$: Այդ դեպքում հնարավոր չի լինի վերականգնել **“Շամիրով բաշխում”** հատվածը և հետևաբար մնացած գործողություններն արդեն անհնար կլինի կատարել: Այսինքն, կարող ենք փաստել, որ $t = n$ դեպքում բաշխման մեթոդը շատ ռիսկային է և նույնիսկ մեկ բաղադրամասի վնասումը կամ կորուստը կբերի գաղտնիքի կորստին:

Նկ. 7-ում պատկերված են Շամիրի և մշակված մեթոդներում բաղադրամասի ստուգման մեթոդների արագործությունների գրաֆիկները: Նկ. 8-ում պատկերված է այդ մեթոդներում բաղադրամասի վերականգնման մեթոդների արագագործությունների գրաֆիկները: Գրաֆիկները ցույց են տալիս, որ մշակված մեթոդներն ավելի արագ են, քան Շամիրի մեթոդի դեպքում:



Նկ. 7. Շամիրի և մշակված մեթոդներում բաղադրամասի սպուգման մեթոդների արագործությունների գրաֆիկները:



Նկ. 8. Շամիրի և մշակված մեթոդներում բաղադրամասի վերականգնման մեթոդների արագործությունների գրաֆիկները:

Գլուխ չորրորդ: Այս գլխում ներկայացված է ստացված գիտական արդյունքների հիման վրա մշակված գաղտնիքի բաշխման ECC Sharing համակարգը, որը հնարավորություն է տալիս արագ բաշխել և վերականգնել մեծ ծավալի ինֆորմացիա, կատարել բաղադրամասի ստուգում, վերականգնել կորած կամ վնասված բաղադրամասերը: Նաև նկարագրվում է ուսումնական նպատակների համար մշակված՝ գաղտնիքի բաշխման մեթոդների հետազոտման ECC Sharing Explore համակարգը, որը հնարավորություն է տալիս հետազոտել ինչպես կոդերով, այնպես էլ գոյություն ունեցող այլ բաշխման մեթոդները: Համակարգը հնարավորություն է տալիս համեմատել բաշխման մեթոդները ըստ արագագործության: Մանրամասն նկարագրված է այդ ծրագրի աշխատանքը:

ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

- Մշակվել է գաղտնիքի բաշխման շեմային մեթոդ՝ հիմնված սխալներ ուղղող կոդերի վրա, որն ի տարբերություն գոյություն ունեցողների ավելի արագ է և հնարավորություն է տալիս կատարել մեծ ծավալի ինֆորմացիայի բաշխում՝ ապահովելով ինչպես գաղտնիությունը, այնպես էլ ամբողջականությունն ու հասանելիությունը [1, 2, 3, 6, 7, 9]:
- Առաջարկվել է բաղադրամասի հավաստիության ստուգման արագ մեթոդ, որն ի տարբերություն գոյություն ունեցողների, հնարավորություն է տալիս ստուգել բաղադրամասը սխալներ ուղղող կոդերով բաշխման դեպքում և հայտնաբերել կեղծված կամ վնասված բաղադրամասերը [4, 5]:
- Առաջարկվել է վնասված կամ կորած բաղադրամասի արագ վերականգնման մեթոդ, որն ի տարբերություն գոյություն ունեցողների, հնարավորություն է տալիս օգտագործել այն սխալներ ուղղող կոդերով բաշխման դեպքում և մեծացնում է գաղտնիքի ապահով պահպանման ժամանակը [8, 9, 10]:
- Ստացված գիտական արդյունքների հիման վրա մշակվել է գաղտնիքի բաշխման ECC Sharing համակարգը, որը հնարավորություն է տալիս արագ բաշխել և վերականգնել մեծ ծավալի ինֆորմացիա, կատարել բաղադրամասի ստուգում, վերականգնել կորած կամ վնասված բաղադրամասերը, որի շնորհիվ բաշխման գործընթացը արագացել է 42.3%-ով, իսկ վերականգնմանը՝ 11.95%-ով [4, 5, 7]:
- Ուսումնական նպատակների համար մշակված գաղտնիքի բաշխման մեթոդների հետազոտման ECC Sharing Explore համակարգը հնարավություն է տալիս հետազոտել ինչպես կոդերով, այնպես էլ գոյություն ունեցող այլ բաշխման մեթոդները: Համակարգը հնարավորություն է տալիս համեմատել բաշխման մեթոդները ըստ արագագործության [5, 7]:

ՀՐԱՏԱՐԱԿՎԱԾ ԱՇԽԱՏՈՒԹՅՈՒՆՆԵՐԸ

[1] Хемчян А., Арутюнян С. “Система распределения секрета на основе кодов, исправляющих ошибки” // Системный администратор – Москва, Россия, 2014, N4 (137), С. 81-82

[2] Margarov G., Khemchyan A. “Secret sharing based on error-correcting codes” //Proceedings of national polytechnic university of Armenia, information technologies, electronics, radio engineering – Երևան, Հայաստան, 2015, Հ.1, N1, Էջ 62-67

[3] Khemchyan A. “Secret sharing based on BCH error correction code” //Proceedings of the Conference Computer Science and Information Technologies (CSIT-2015) – Yerevan, Armenia, 2015, P. 280-282

[4] Խեմչյան Ա. “Գաղտնիքի բաշխման շեմային սխեմա՝ սխալներ ուղղող Հեմմինգի կոդի հիման վրա” // ՀԱՊՀ Լրաբեր, գիտական և մեթոդական հոդվածների ժողովածու – Երևան, Հայաստան, 2016, Հ.1, Է. 129-137

[5] Хемчян А. “Пороговые схемы разделения секрета и коды исправляющие ошибки” // Тезисы докладов международной научно-практической конференции молодых ученых и студентов – Киев, Украина, 2016, С. 216-217

[6] Хемчян А. “Распределение данных на основе кодов, исправляющих ошибки” // Науковий журнал Безпека інформації – Киев, Украина, 2016, С. 261-264

[7] Khemchyan A. “Distributed Data Storage in Cloud Systems Based on Error Correcting Codes” // Meeting Security Challenges Through Data Analytics and Decision Support. “NATO Science for Peace and Security” Series - D: Information and Communication Security – 2016, Volume 47, P. 287-292

[8] Khemchyan A., Harutyunyan S. “A New (k,n)-Threshold Secret Sharing Scheme Based on Error-Correcting Codes” // Proceedings of the Conference World Congress on Internet security (WorldCIS2016) – London, United Kingdom, 2016, P. 92-96

[9] Hovsepyan V., Khemchyan A., Atayan B. “Data Security and Backup in Cloud Envirement” // Proceedings of the Conference World Congress on Internet security (WorldCIS2016) – London, United Kingdom, 2016, P. 101-105

[10] Хемчян А. “Новая (k,n) пороговая схема распределения секрета на основе кодов, исправляющих ошибки” // Сборник научных статей XIII международной научно-технической конференции Новые информационные технологии и системы ("НИТиС-2016") – Пенза, Россия, 2016, С. 260-262

Khemchyan Artak Ararat

RESEARCH OF METHODS FOR SECRET SHARING BASED ON ERROR-CORRECTING CODES

RESUME

The rapid development of information technology has led to a significant part of the confidential information to be stored in electronic formats, the loss or exposure of which can cause undesirable consequences for the user. In parallel, the risk of possible attacks on information systems increases, the purpose of which may be disclosure of confidential information, its damage or modification. From the other hand, potential data loss is possible due to natural phenomena. For the described cases, secret sharing methods may be useful. The most popular secret sharing threshold methods were originally used for the distribution of keys, i.e the secret information is being encrypted and encryption keys are distributed afterwards. This solves the confidentiality problem, but doesn't address integrity and availability problems, which are open and not solved yet. If encrypted information is not available or is damaged, it is impossible to decipher it with recovered key. Currently, new data sharing method is widely used. It offers new option for entire data sharing rather than only key and solves Integrity and availability problems as well. Given the fact that existing methods are slow and the volume of information is growing day by day, a question arises to develop a faster threshold secret sharing method. Different researches show that the fast threshold secret-sharing method can be achived by using the Error-Correcting Codes.

In secret sharing method not only the distribution and recovery speed, but also the security of components has an important role. Therefore, secret sharing method must have component checking mechanism, and if necessary, the possibility of restoring lost or damaged components. These capabilities increase the safe storage time of information.

Goal and objectives.

The purpose of this research is a development of new secret sharing methods, based on Error-Correcting Codes. To achieve this, following problems are listed and solved:

- develop a high-speed threshold secret sharing method that allows to recover and distribute large volumes of information,
- develop components' verification method for secret sharing based on Error-Correcting Codes,
- develop fast method of damaged or missing component recovery for secret sharing based on Error-Correcting Codes.

The main results are:

- New secret sharing threshold method has been developed, which is based on Error-Correcting Codes. Unlike existing ones, this is faster and enables distribution of large volumes of information, ensures information confidentiality, as well as integrity and availability [1, 2, 3, 6, 7, 9].
- Proposed a fast method of checking the authenticity of components, which, unlike the existing ones, provides an opportunity to check the components shared via Error-Correcting Codes and detect the falsified or damaged components [4, 5].
- Proposed method of rapid recovery of lost or damaged component, which usage during sharing via Error-Correcting Codes, unlike the existing ones, increases safe storage time of the secret [8, 9, 10].
- Based on the results obtained from the research developed, "ECC Sharing" Secrets sharing system has been developed, which allows quick sharing and recovery of large volumes of information, as well as performs component validation, recovers lost or damaged components. From performance improvement point of view it makes the distribution process faster by 42.3% and recovery by 11.95% appropriately [4, 5, 7].
- "ECC Sharing Explore" system, designed for educational purposes, enables the system to research secret sharing methods based on Error-Correcting Codes, as well as to other distribution methods. The system allows also to compare the performance of different sharing methods [5, 7].

ХЕМЧЯН АРТАК АРАРАТОВИЧ

РАЗРАБОТКА СРЕДСТВ РАСПРЕДЕЛЕНИЯ СЕКРЕТА НА ОСНОВЕ КОДОВ, ИСПРАВЛЯЮЩИХ ОШИБКИ

РЕЗЮМЕ

Быстрое развитие информационных технологий привело к тому, что значительная часть секретных данных хранятся в электронном формате, и потеря или раскрытие может привести к нежелательным последствиям для пользователя. Параллельно с этим, увеличивается риск возможных атак на информационные системы, целью которых может быть как раскрытие данных, а также повреждение или модификация. С другой стороны, возможны потери данных из-за природных явлений. В описанных случаях могут быть полезны методы распределения секрета. Наиболее популярные методы порогового распределения секрета первоначально использовались для распределения ключей. То есть, секретная информация шифруется, а ключ шифрования распределяется. В этом случае решается проблема конфиденциальности, но не решены проблемы целостности и доступности. Если шифрованная информация будет повреждена или недоступна, то восстановлением ключа невозможно расшифровать информацию. В настоящее время распространяется метод целостного распределения информации, который уже решает проблему доступности и целостности. Учитывая тот факт, что существующие методы являются медленными, а объем информации растет с каждым днем, появляется необходимость разработки более быстродействующего метода порогового распределения секрета. Исследования показали, что быстродействующий метод порогового распределение секрета можно получить с помощью кодов, исправляющих ошибки.

В методе распределения секрета важную роль играет не только скорость распространения и восстановления, но и безопасность компонентов. Таким образом, метод распределения должен быть наделен возможностями проверки компонента, и, в случае необходимости, восстановления потерянного или поврежденного компонента. Эти возможности увеличивают время безопасного хранения информации.

Целью работы является разработка быстрых средств распределения секрета с помощью кодов, исправляющих ошибки. Для достижения этой цели были поставлены и решены следующие задачи:

- Разработать быстродействующий пороговый метод распределения секрета, который позволит распределить и восстановить информацию большого объема.

- Разработать метод проверки подлинности компонента при распределений с помощью кодов, исправляющих ошибки.
- Разработать метод быстрого восстановления поврежденного или потерянного компонента при распределении с помощью кодов, исправляющих ошибки.

Основные результаты диссертационной работы следующие:

- Разработан пороговый метод распределения секрета, основанный на кодах, исправляющих ошибки, который, в отличие от существующих более быстрый и позволяет распределять большие объемы данных, обеспечивая не только конфиденциальность, а также их целостность и доступность [1, 2, 3, 6, 7, 9].
- Разработан быстрый метод проверки подлинности компонента, который в отличие от существующих позволяет проверить компонент при распределении с помощью кодов, исправляющих ошибки, и обнаружить поддельные или поврежденные компоненты [4, 5].
- Разработан метод быстрого восстановлении поврежденного или отсутствующего компонента, который, в отличие от существующих, позволяет использовать его при распределении с помощью кодов, исправляющих ошибки и увеличивает время безопасного хранения секрета [8, 9, 10].
- На основании полученных научных результатов разработана система «ECC Sharing» распределения секрета, которая позволяет быстро распределять и восстанавливать информацию большого объема, выполнять тестирование компонента, восстанавливать потерянные или поврежденные компоненты, с помощью которых процесс распределения ускорился на 42.3%, а восстановление - на 11.95% [4, 5, 7].
- Система исследования методов распределения секрета «ECC Sharing Explore», разработанный для образовательных целей, дает возможность исследовать как метод на кодах, так и другие существующие методы распределения секрета. Система дает возможность сравнить методы распределения по скорости [5, 7].