ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԻՆՖՈՐՄԱՏԻԿԱՅԻ
ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Մանուկյան Օֆելյա Ալբերտի

«SAFER» և նմանօրինակ ծածկագրման համակարգերում կիրառվող արդյունավետ ալգորիթմների մշակում և իրականացում

Ե.13.05 «Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրերի համալիրներ» մասնագիտությամբ

Տեխնիկական գիտությունների թեկնածուի
գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան 2011

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РЕСПУБЛИКИ АРМЕНИЯ

Манукян Офелия Альбертовна

Разработка и реализация эффективных алгоритмов применимых в “SAFER” и подобных криптосистемах

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.05
“Математическое моделирование, численные методы и комплексы программ”.

Ереван 2011

Ատենախոսության թեման հաստատվել է ՀՀ Գիտությունների Ազգային Ակադեմիայի Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում:

Գիտական ղեկավար՝ ֆ.մ.գ.թ. Մ. Կ. Կյուրեղյան

Պաշտոնական ընդդիմախոսներ՝ ՀՀ ԳԱԱ ակադ., տ.գ.դ., պրոֆ. Գ. Հ. Խաչատրյան
տ.գ.թ. Հ. Վ. Ասցատրյան

Առաջատար կազմակերպություն՝ Հայաստանի Պետական Ճարտարագիտական Համալսարան

Պաշտպանությունը կայանալու է 2011թ.-ի հուլիսի 1-ին, ժամը 15^{00}-ին, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 □Ինֆորմատիկա և հաշվողական համակարգեր□ մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ 0014, Երևան, Պ.Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրը առաքված է 2011թ.-ի հունիսի 1-ին:

037 Մասնագիտական խորհրդի
գիտական քարտուղար, ֆ.մ.գ.դ., պրոֆեսոր Մ. Ե. Հարությունյան

Тема диссертации утверждена в Институте проблем информатики и автоматизации НАН РА.

Научный руководитель: к.ф.м.н. М. К. Кюрегян

Официальные оппоненты: акад. НАН РА, д.т.н., проф. Г. Г. Хачатрян
к.т.н. Г. В. Асцатрян

Ведущая организация: Государственный Инженерный Университет Армении

Защита состоится 1-го июля 2011г., в 15^{00} ч., на заседании специализированного совета N 037 “Информатика и вычислительные системы” Института проблем информатики и автоматизации НАН РА по адресу: 0014, Ереван, ул. П.Севака 1.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.
Автореферат разослан 1-го июня 2011г.

Ученый секретарь
специализированного совета 037,
д.ф.м.н., профессор М.Е.Арутюнян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը

Համակարգչային ցանցերի համատարած ներդրման հետ կապված ինֆորմացիայի պաշտպանության խնդիրը դառնում է առավել կարևոր և արդիական: Ինֆորմացիոն տեխնոլոգիաների և տվյալների փոխանցման միջոցների արագ զարգացման հետ զուգընթաց մեծանում է անհրաժեշտությունը ունենալու տվյալների ծածկագրման ապահով և արագ ծրագրային միջոցներ: Ժամանակակից զարգացման էտապում մեծ ջանքեր են ներդրվում նմանատիպ համակարգերի ստեղծման համար և այս աշխատանքը այդպիսի մի օրինակ է:

Աշխատանքում մասնավորապես նկարագրվում է այն հիմնադրույթների մանրամասն վերլուծությունը, ինչի վրա հիմնվելով կառուցվել է բլոկային ծածկագրման SAFER համակարգերի ընտանիքը և մեր կողմից համալրվել է նոր տարբերակներով: Ցավոք ժամանակակից զարգացման էտապում ծածկագրման համակարգերի լիարժեքության և ապահովության ապացուցումը, ապագայում տվյալների պահպանման հնարավոր բարդությունների գնահատումը բավականին դժվար խնդիր է, այդ իսկ պատճառով շատ կարևոր է տվյալների պահպանման հիմնադրույթների ընտրությունը:

Տվյալների ծածկագրման համար ալգորիթմ ընտրելիս պետք է ստուգել նրա կայունությունը արդեն գոյություն ունեցող հարձակումների տիպերի նկատմամբ: Հարձակումների հնարավոր տիպերի ընտրության գործընթացում գոյություն ունի որոշակի մոտեցում, այն է՝ պարզել, թե հարձակումներից որոնք են առավել բնորոշ տվյալ ալգորիթմի համար և դրանցից որոնք են ամենից շատ կիրառվում նմանատիպ ալգորիթմի վրա գրոհի դեպքում:

Հետազոտությունները ցույց են տվել, որ ներկա դրությամբ բլոկային ծածկագրման համակարգերի համար ամենից վտանգավորը դիֆերենցիալ և գծային ծածկագրավերլուծության եղանակներն են, որոնք այս աշխատանքում ուսումնասիրվող հիմնական առարկաներից են: Այնուամենայնիվ, անկախ նրանից, որ ապացուցվում է ընտրված ծածկագրման համակարգի կայունությունը դիֆերենցիալ և գծային վերլուծությունների նկատմամբ, պետք է հաշվի առնել, որ համակարգը կարող է ապահով չլինել ցանկացած գոյություն ունեցող կամ դեռևս անհայտ հարձակման նկատմամբ:

Ինտերնետի համատարած զարգացման հետ զուգընթաց աճել է բաց չվերահսկվող կապուղով փոխանցվող տվյալների քանակը և ծավալը: Բազմաթիվ գործարար մարդկանց անհրաժեշտ է իրենց գործնական ինֆորմացիան ինչ-որ կերպ պաշտպանել իրենց մրցակիցներից կամ հիմնավորել դրա իրավացիությունը թվային ստորագրության միջոցով: Այլ կերպ ասած, խնդիրը համընդհանուր ցանցում համաձայնության հաստատումն է փոխադարձաբար անվստահելի կողմերի միջև:

Նման խնդիրների լուծումներից է հանդիսանում հասարակական բանալիով ծածկագրման համակարգերի (Public Key Cryptography) օգտագործումը: Գրականության մեջ ընդունված է հասարակական բանալիով ծածկագրման

համակարգերը ներկայացնել որպես գաղտնիությունը պահպանող տեխնիկա: Այն օգտագործվում է նաև թվային ստորագրություններում, որոնք օգտագործողին տալիս են հետևյալ բնութագրիչ հատկությունները՝ իրավացիություն, ամբողջականություն և անժխտելիություն, ինչն անխտիր պահանջվում է էլեկտրոնային կոմերցիայում:

Ծածկագրման ալգորիթմների օգտագործմամբ իրականացվող գործարքների քանակը հետզհետե աճում է, ինչը հանգեցնում է հաշվողական համակարգերի գերբեռնվածության: Խնդիրն, իհարկե, կարելի է որոշակի կերպ լուծել, ավելացնելով հաշվողական համակարգի պրոցեսորների կամ սերվերների քանակը, սակայն դա բավականին թանկարժեք միջոց է:

Բացահայտորեն երևում է, որ հետզհետե անհրաժեշտ կլինի մեծացնել թվերի երկարությունները, իսկ ալգորիթմներում հաշվարկների բարդության կախումը օպերանդների երկարություններից քառակուսային է և, բացի դրանից, մեծանում է կապուղու բեռնվածությունը այդպիսի տվյալներ փոխանցելիս (ինչպես օրինակ թվային ստորագրության փոխանցումը): Խնդրի լուծման տարբերակներից են հետզհետե զարգացող ծածկագրման համակարգերը՝ հիմնված էլիպտիկ կորերի վրա:

Քանի որ վերջին հաշվով բոլոր հայտնի ալգորիթմները իրականացվում են համակարգչի կամ այլ սարքային միջոցներով, ապա նպատակահարմար է ունենալ այնպիսի խմբեր, որոնցում խմբային գործողությունները էլեմենտների միջև լինեն հեշտ իրագործելի: Ընտրություններից մեկը վերջավոր դաշտերի վրա որոշված էլիպտիկ կորին պատկանող կետերի խումբն է, որը հետզհետե դառնում է ավելի կիրառելի: Այս խմբում լուծվում է խնդիրը, կապված օպերանդների երկարությունների մեծացման և կապուղու խնայողաբար օգտագործման հետ:

Այսպիսով, արդիական ու կարևոր խնդիր է մեծ թվերի և շատ մեծ աստիճանի բազմանդամների թվաբանությունն իրականացնող ալգորիթմների մշակումն ու իրականացումը ժամանակակից հաշվողական համակարգերում:

Աշխատանքի մյուս մասը նվիրված է վերջավոր դաշտերի վրա անվերածելի և նորմալ բազմանդամների բացահայտ տեսքով կառուցման խնդրին: Առաջարկված են այդպիսի բազմանդամների կառուցման նոր մեթոդներ, որոնցից մեկի համար կատարվել է ծրագրային իրականացում: Մեր կողմից առաջարկվող ալգորիթմները թույլ են տալիս կառուցել փոքր կշիռ ունեցող անվերածելի բազմանդամներ: Ինչպես հայտնի է, փոքր կշիռ ունեցող անվերածելի բազմանդամի դեպքում վերջավոր դաշտում իրականացվող հիմնական գործողությունները կատարվում են անհամեմատ ավելի արագ:

<u>Աշխատանքի նպատակն է</u> առաջարկել բլոկային ծածկագրման համակարգերի SAFER ընտանիքի նոր տարբերակներ և ցույց տալ, որ դրանք կայուն են դիֆերենցիալ և գծային վերլուծությունների նկատմամբ: Ինչպես նաև, մշակել և իրականացնել արագ ու էֆեկտիվ ալգորիթմներ՝ վերջավոր դաշտերի վրա անվերածելի և նորմալ բազմանդամների բացահայտ տեսքով կառուցման համար, որոնք թույլ են տալիս կառուցել հնարավորինս փոքր կշիռ ունեցող անվերածելի բազմանդամներ:

Հետազոտման օբյեկտ են հանդիսանում ալգորիթմները, որոնք օգտագործվում են ինֆորմացիայի պաշտպանության ժամանակակից ծածկագրաբանական միջոցներում:

Հետազոտման մեթոդները

Աշխատանքում օգտագործվել են թվերի տեսության, վերջավոր դաշտերի տեսության, հավանականությունների տեսության և ծածկագրաբանության մաթեմատիկական մեթոդները:

Արդյունքների գիտական նորույթը

- Մշակվել են SAFER ընտանիքի նոր բլոկային ծածկագրման համակարգեր, որոնք իրենց կայունությամբ և հուսալիությամբ չեն զիջում ինչպես հայտնի SAFER+ և SAFER++, այնպես էլ SAFER ընտանիքի մնացած բոլոր համակարգերին,
- Մշակվել են վերջավոր դաշտերի վրա անվերածելի և նորմալ բազմանդամների բացահայտ տեսքով կառուցման նոր մեթոդներ:

Ստացված արդյունքների կիրառական նշանակությունը

SAFER բլոկային ծածկագրման համակարգերի ընտանիքը համալրվել է լրիվ նոր, նախկինում գոյություն չունեցող տարբերակներով, որոնք իրենց կայունությամբ և հուսալիությամբ չեն զիջում ինչպես SAFER+ և SAFER++, այնպես էլ SAFER ընտանիքի մնացած բոլոր համակարգերին:

Ունենալով SAFER բլոկային ծածկագրման համակարգերի ընտանիքի բազմաթիվ ծածկագրման համակարգերի տարբերակներ՝ ցանկացած պահի կարելի է պատահականորեն ընտրել համակարգերից մեկը և հաղորդակցող կողմերի փոխհամաձայնությամբ օգտագործել այդ համակարգը՝ միմյանց ծածկագրված հաղորդագրություններ ուղարկելու նպատակով: Սա, բնականաբար, ավելի է ամրապնդում հուսալիության աստիճանը՝ դարձնելով գաղտնիությունը երկու բնույթի. առաջինը դա գաղտնի բանալու առկայությունն է, իսկ երկրորդը՝ կիրառված ծածկագրման համակարգի կոնկրետ տարբերակի անհայտ լինելը:

Երկրորդ ուսումնասիրված ուղղությունը անվերածելի և նորմալ բազմանդամների բացահայտ տեսքով կառուցման խնդիրն է: Աշխատանքում առաջարկված են այդպիսի բազմանդամների կառուցման նոր մեթոդներ, որոնցից մեկի համար կատարվել է ծրագրային իրականացում կլաստերային հաշվողական համակարգում:

Մեր կողմից առաջարկվող ալգորիթմները թույլ են տալիս կառուցել փոքր կշիռ ունեցող անվերածելի բազմանդամներ: Այս խնդրի լուծումը սովորաբար բաց է թողնվում հիմնական թեորեմների կողմից, այսինքն թեորեմներն օգտագործում են անվերածելի բազմանդամներ, սակայն չեն տրամադրում դրանց փնտրման կամ կառուցման խնդրի լուծման եղանակներ:

SAFER ընտանիքի բլոկային ծածկագրման համակարգերի սինթեզման նպատակով ստեղծված “DiffLinearAnalyser” ծրագրաշարը և անվերածելի բազմանդամների կառուցման նպատակով ստեղծված “IPG“ ծրագրաշարը կարող են օգտագործվել

ծածկագրաբանության տարբեր ասպարեզներում ինչպես փորձագիտական, այնպես էլ գործնական նպատակներով:

Վերջավոր դաշտի էլեմենտների միջև հանրահաշվական գործողությունների իրականացման օպտիմալացված ծրագրային միջոցները կարող են լայն կիրառություն գտնել նմանատիպ խնդիրներում, որտեղ կարևոր է գործողությունների իրականացման արագությունը և հիշողության ռեսուրսների խնայողաբար հատկացումն ու ժամանակին ազատումը:

Ներդրումներ

"DiffLinearAnalyser" ծրագրաշարը ներդրված է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում տեղադրված զուգահեռ հաշվարկների համար նախատեսված բարձր արտադրողականությամբ ARM Cluster հաշվողական համակարգում: Աշխատանքի մի մասը կատարվել է ISTC A-823 և ISTC A-1453 գրանտների շրջանակներում:

Պաշտպանությանը ներկայացվում են հետևյալ դրույթները.

1. SAFER ընտանիքի նոր բլոկային ծածկագրման համակարգերը՝ կառուցված արդեն գոյություն ունեցող SAFER+ և SAFER++ բլոկային ծածկագրման համակարգերի հիման վրա,
2. Դիֆերենցիալ և գծային ծածկագրավերլուծության եղանակներն ու նրանց կիրառությունը նոր կառուցված բլոկային ծածկագրման համակարգերի վրա,
3. Վերջավոր դաշտերի վրա անվերածելի և նորմալ բազմանդամների կառուցման համար առաջարկված նոր մեթոդները, որոնք թույլ են տալիս կառուցել հնարավորինս փոքր կշիռ ունեցող անվերածելի բազմանդամներ,
4. "DiffLinearAnalyser" ծրագրաշարը, որն իրականացնում է նոր սինթեզված բլոկային ծածկագրման համակարգերի դիֆերենցիալ և գծային վերլուծություն-ները կլաստերային հաշվողական համակարգում,
5. "IPG" ծրագրաշարը, որի օգնությամբ կառուցվում է անվերածելի բազմանդամների հաջորդականություն և փնտրվում է միևնույն աստիճանի հնարավորինս փոքր կշիռ ունեցող անվերածելի բազմանդամներ:

Ապրոբացիա և հրապարակումներ

Աշխատանքում ներկայացված հիմնական արդյունքները զեկուցվել են CSIT'2005 և CSIT'2009 Կոմպյուտերային գիտությանը և ինֆորմացիոն տեխֆոլոգիաներին նվիրված V և VII միջազգային գիտաժողովներում (Երևան 2005, 2009) և ԻԱՊԻ ընդհանուր սեմինարներում:

Ատենախոսության թեմայով հրապարակված են 7 գիտական աշխատանքներ, որոնց ցանկը բերված է սեղմագրի վերջում:

Աշխատանքի կառուցվածքն ու ծավալը

Ատենախոսությունը բաղկացած է առաջաբանից, երեք գլուխներից, օգտագործված գրականության ցանկից և երկու հավելվածներից: Աշխատանքի ծավալը կազմում է

131 էջ, օգտագործված գրականության ցանկն ընդգրկում է 63 անուն:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Առաջաբանում հիմնավորվում է թեմայի արդիականությունը, հետազոտության նպատակն ու հիմնական խնդիրները, ձևակերպվում են ուսումնասիրման օբյեկտն ու հիմնադրույթները, հետազոտությունների գիտական նորույթն ու ստացված արդյունքների կիրառական նշանակությունը:

Առաջին գլխում հակիրճ ձևակերպվում է ինֆորմացիայի պաշտպանության հիմնա-խնդիրը, տրվում է ծածկագրաբանության հասկացությունը և հիմնադրույթները, նկարագրվում է բլոկային ծածկագրման համակարգերի մոդելը: Մասնավորապես, նկարագրվում է SAFER բլոկային ծածկագրման համակարգերի ընտանիքը SAFER+ և SAFER++ համակարգերի օրինակով և այն դրույթները, որոնց վրա հիմնվելով կառուցվել են այդ համակարգերը:

Աշխատանքում նկարագրված նոր բլոկային ծածկագրման համակարգերը կառուցվել են արդեն գոյություն ունեցող SAFER+ և SAFER++ բլոկային ծածկագրման համակարգերի հիման վրա, այսինքն դրանք հանդիսանում են SAFER ընտանիքի համակարգերի նոր տարբերակներ: SAFER+ և SAFER++ բլոկային ծածկագրման համակարգերը առաջարկվել են ՀՀ ԳԱԱ ԻԱՊԻ Տվյալների Կոդավորման բաժնի աշխատակիցներ՝ ՀՀ ԳԱԱ ակադեմիկոս, տեխ.գ.դ. Գուրգեն Խաչատրյանի և ֆ.մ.գ.թ Մելսիկ Կյուրեղյանի կողմից՝ SAFER ծածկագրման համակարգերի ընտանիքի հիմնադիր Ջեյմս Մեսսիի հետ համատեղ աշխատանքի շնորհիվ:

SAFER+ համակարգը 1988թ.-ին ներկայացվել է AES (Advanced Encryption Standard) մրցույթին և անցել է նախընտրական փուլը 14 այլ ծածկագրման ալգորիթմների հետ միասին: Հետագայում համակարգի հիման վրա մշակվել են մի քանի հեղինակային իրավունքով պաշտպանված ալգորիթմներ, որոնք ընդունվել են օգտագործման Bluetooth ստանդարտի ինքնության ճանաչման (message authentication codes called E1) և բանալու գեներացման (key derivation called E21 and E22) սխեմաներում:

Առավել նոր տարբերակը՝ SAFER++-ը հանդիսանում է SAFER+ համակարգի հետագա զարգացումը, ինչն էլ արտացոլվել է նրա անվանման մեջ: SAFER++-ը մասնակցել է NESSIE (New European Schemes for Signature Integrity and Encryption) ստանդարտների մրցույթին և եզրափակիչ փուլում ճանաչվել է 21-րդ դարի երեք լավագույն ազատ օգտագործման բլոկային ծածկագրման համակարգերից մեկը:

SAFER+ և SAFER++ ծածկագրման ալգորիթմներում օգտագործվում է “Armenian Shuffle” 16 բայթ երկարությամբ կոորդինատային տեղափոխությունը, որը փոխարինում է SAFER ընտանիքի ծածկագրման նախորդ համակարգերում օգտագործվող “Hadamard Shuffle” տեղափոխությանը: “Armenian Shuffle” 16-բայթ երկարությամբ կոորդինատային տեղափոխությունը ապահովում է SAFER+ և SAFER++ ծածկագրման համակարգերում ավելի արագ ծածկագրման դիֆուզիա (համակարգերի դիֆուզիան կլինի ապահովված, երբ չնչին փոփոխությունները ռաունդի մուտքում

բերեն զգալի փոփոխությունների ռաունդի ելքում): Դա թույլ է տալիս նվազեցնել ռաունդների քանակն ու մեծացնել ծածկագրման արագությունը, միաժամանակ ապահովել նրանց բարձր կայունությունը դիֆերենցիալ վերլուծության նկատմամբ:

SAFER+ և SAFER++ բլոկային ծածկագրման համակարգերից յուրաքանչյուրի համար որոշակիորեն ընտրված են “Armenian Shuffle” կոորդինատային տեղափոխություններ, այն է՝ [9, 12, 13, 16, 3, 2, 7, 6, 11, 10, 15, 14, 1, 8, 5, 4] SAFER+ համակարգի համար և [9, 6, 3, 16, 1, 14, 11, 8, 5, 2, 15, 12, 13, 10, 7, 4] SAFER++ համակարգի համար, ըստ որոնց առաջին ելքային բայթը երկու համակարգերի համար էլ հանդիսանում է իններորդ մուտքային բայթը, երկրորդ ելքային բայթը՝ տասներկուերորդ մուտքային բայթը SAFER+-ում և վեցերորդ մուտքային բայթը SAFER++-ում, և այլն:

Երկրորդ գլխում նկարագրվում են նոր բլոկային ծածկագրման համակարգերի նկատմամբ կիրառված դիֆերենցիալ և գծային վերլուծությունների եղանակները և այն մոտեցումները, որոնց հիման վրա փնտրվել են “Armenian Shuffle” կոորդինատային տեղափոխությունները:

Գլխի 2.1 ենթամասում նկարագրվում է նոր բլոկային ծածկագրման համակարգերի սինթեզման ընթացակարգը:

Գլխի 2.2 ենթամասում հակիրճ նկարագրվում են ծածկագրման համակարգերի ծածկագրավերլուծության հիմնադրույթները:

Գլխի 2.3 ենթամասում մանրամասն նկարագրվում են նոր բլոկային ծածկագրման համակարգերի նկատմամբ կիրառված դիֆերենցիալ վերլուծության արդյունքները:

Բերենք հակիրճ նկարագրությունը. դիֆերենցիալ վերլուծությունը ուսումնասիրում է, թե ինչպիսի ազդեցություն կունենան և ինչ փոփոխությունների կբերեն մուտքային տվյալների տարբերությունները ելքային տվյալների տարբերությունների վրա: Բլոկային ծածկագրման համակարգերի դեպքում այն դիտարկում է ձևափոխությունների միջով անցնող մուտքային տվյալների տարբերությունները հետևելու մի շարք տեխնիկաներ, որպեսզի հայտնաբերի այն միջակայքերը, որտեղ համակարգը դրսևորում է ոչ-պատահական վարվելակերպ (non-random behaviour): Օգտվելով համակարգի նմանատիպ անորակ հատկություններից՝ վերլուծողը կարող է որոնել և գտնել գաղտնի բանալին մասամբ կամ ամբողջությամբ:

Սահմանենք դիֆերենցիալ վերլուծության եղանակում կիրառվող բայթային դիֆերենցիալները և բայթային քվազի-դիֆերենցիալները: Յուրաքանչյուր ռաունդի սկզբում համակարգը բայթ-առ-բայթ զուգակցում է $X=[X_1, X_2, \ldots, X_{16}]$ 16 բայթ երկարությամբ մուտքային վեկտորը $Z_a=[Z_{a1}, Z_{a2}, \ldots, Z_{a16}]$ ռաունդի 16 բայթ երկարությամբ առաջին ենթաբանալու հետ՝ ստանալով $T=[T_1, T_2, \ldots, T_{16}]$ 16 բայթ երկարությամբ մուտքային վեկտոր ոչ-գծային ձևափոխության համար: X և Z_a վեկտորների զուգակցումը կատարվում է հետևյալ օրենքով՝

$$T = X \otimes Z_a,$$

որտեղ $\otimes = [\oplus,+,+,\oplus,\oplus,+,+,\oplus,\oplus,+,+,\oplus,\oplus,+,+,\oplus]$: Այստեղ $\oplus$-ով նշանակված է բայթերի բիթ-առ-բիթ ըստ mod2-ի գումարման գործողությունը (XOR), իսկ +-ով նշանակված է սովորական բայթային գումար գործողությունը, այսինքն բայթ-առ-բայթ գումարումը ըստ mod256-ի: Այժմ $S = [S_1, S_2, \ldots, S_{16}]$-ով նշանակենք գծային ձևափոխության 16 բայթ երկարությամբ մուտքային վեկտորը, որը որոշվում է հետևյալ կերպ՝

$$S_j = 45^{(X_j \otimes Z_{aj})} + Z_{bj}, \quad j \in \{1,4,5,8,9,12,13,16\},$$

որտեղ Z_a և Z_b ռաունդի երկու ենթաբանալիներն են: Այսպիսով, 1, 4, 5, 8, 9, 12, 13, 16 բայթերը կդիտարկվեն որպես աստիճանական բայթեր: Նմանապես, ունենք, որ

$$S_j = \log_{45}(X_j + Z_{aj}) \oplus Z_{bj}, \quad j \in \{2,3,6,7,10,11,14,15\},$$

և 2, 3, 6, 7, 10, 11, 14, 16 բայթերը կդիտարկվեն որպես լոգարիթմական բայթեր:

16 բայթ երկարությամբ V և V^* վեկտորների ΔV տարբերությունը սահմանենք այսպես՝

$$\Delta V = [V_1 \oplus V_1^*, V_2 - V_2^*, V_3 - V_3^*, V_4 \oplus V_4^*, V_5 \oplus V_5^*, V_6 - V_6^*, V_7 - V_7^*, V_8 \oplus V_8^*,$$

$$V_9 \oplus V_9^*, V_{10} - V_{10}^*, V_{11} - V_{11}^*, V_{12} \oplus V_{12}^*, V_{13} \oplus V_{13}^*, V_{14} - V_{14}^*, V_{15} - V_{15}^*, V_{16} \oplus V_{16}^*],$$

իսկ $\tilde{\Delta} V$ քվազի-տարբերությունը այսպես՝

$$\tilde{\Delta} V = [V_1 - V_1^*, V_2 - V_2^*, V_3 - V_3^*, V_4 - V_4^*, V_5 - V_5^*, V_6 - V_6^*, V_7 - V_7^*, V_8 - V_8^*,$$
$$V_9 - V_9^*, V_{10} - V_{10}^*, V_{11} - V_{11}^*, V_{12} - V_{12}^*, V_{13} - V_{13}^*, V_{14} - V_{14}^*, V_{15} - V_{15}^*, V_{16} - V_{16}^*]$$

$(a, r) = (\Delta X_j, \Delta S_j)$ թվազույգը անվանենք աստիճանական բայթային դիֆերենցիալ, երբ $j \in \{1,4,5,8,9,12,13,16\}$ և լոգարիթմական բայթային դիֆերենցիալ, երբ $j \in \{2,3,6,7,10,11,14,15\}$: Աստիճանական բայթային դիֆերենցիալներից ավելի հետաքրքիր տարբերակ են աստիճանական բայթային քվազի-դիֆերենցիալները, որոնցում XOR գործողությամբ որոշված ելքային ΔS_j տարբերության փոխարեն դիտարկվում է $\tilde{\Delta} S_j$ տարբերությունը՝ որոշված տարբերության գործողությամբ ըստ mod256-ի: Քանի որ $S = [S_1, S_2, \ldots, S_{16}]$ հանդիսանում է գծային ձևափոխության մուտքային վեկտորը, ապա ռաունդի $Y = [Y_1, Y_2, \ldots, Y_{16}]$ ելքային վեկտորը կորոշվի $Y = SM$ հավասարմամբ, որտեղ բոլոր հանրահաշվական գործողությունները կատար-վում են ըստ mod256-ի: Հետևաբար, երբ $\tilde{\Delta} S$ վեկտորի բոլոր անդամները հաշվարկվում են ըստ mod256-ի, այսինքն $\tilde{\Delta} S = S_j - S_j^*$, կունենանք, որ

$$\tilde{\Delta} Y = SM - S^* M = (\tilde{\Delta} S) M$$

Այս պարզ առընչությունից երևում է, որ SAFER բլոկային ծածկագրման համակարգերի դիֆերենցիալ վերլուծությունը կատարելիս ավելի նպատակահարմար է բայթային դիֆերենցիալների փոխարեն օգտագործել բայթային քվազի-դիֆերենցիալներ:

Այսպիսով, եթե ΔV և $\widetilde{\Delta} V$ տարբերությունները որոշվում են բայթ-առ-բայթ տարբերության գործողությամբ ըստ mod256-ի, ապա X և X^* վեկտորների տեղափոխությունը չեզոքացնում է տարբերությունը, միևնույն դեպքում ոչ մի ազդեցություն չի ունենում ΔV տարբերության վրա, որը որոշված է XOR գործողությամբ: Հետևաբար, լոգարիթմական բայթային դիֆերենցիալների համար, երբ մուտքային և ելքային տարբերությունները որոշվում են բայթ-առ-բայթ տարբերության գործողությամբ ըստ mod256-ի, ճիշտ է հետևյալը հավանականային հավասարությունը՝

$$P(\Delta S = \tau \mid \Delta X = \alpha) = P(\Delta S = -\tau \mid \Delta X = -\alpha).$$

Նմանապես, աստիճանական բայթային քվազի-դիֆերենցիալների համար, երբ միայն ելքային տարբերություններն են որոշվում բայթ-առ-բայթ տարբերության գործողությամբ ըստ mod256-ի, ճիշտ է հետևյալ հավանականային հավասարությունը՝

$$P(\Delta S = \tau \mid \Delta X = \alpha) = P(\Delta S = -\tau \mid \Delta X = \alpha).$$

Դիֆերենցիալ վերլուծության հիմնական նպատակն է գտնել քվազի-դիֆերենցիալներ՝ r ռաունդների համար մեծ անցումային հավանականությամբ: SAFER ընտանիքի մեր կողմից սինթեզված նոր բլոկային ծածկագրման համակարգերի դիֆերենցիալ ամբողջական վերլուծությունը՝ իրականացված ծրագրային միջոցներով, ցույց է տվել, որ $r = 5$ ռաունդից սկսած բոլոր դիֆերենցիալ շղթաների անցումային հավանականությունները փոքր են 2^{-128}-ից, ինչը նշանակում է, որ նոր բլոկային ծածկագրման համակարգերը 6 և ավելի (սակայն ոչ քիչ) ռաունդների դեպքում ապահով և կայուն են դիֆերենցիալ վերլուծության նկատմամբ: Նշենք, որ դիֆերենցիալ վերլուծության գրոհի միջոցով $r = 6$ ռաունդով նոր բլոկային ծածկագրման համակարգերի գաղտնի բանալին գտնելու փորձերը համարժեք կլինեն, կամ կպահանջեն նույնքան հաշվարկներ, որքան բանալու համապարփակ որոնումը՝ բոլոր հնարավոր բանալիների փորձարկմամբ (brute force attack):

Գլխի 2.4 ենթամասում մանրամասն նկարագրվում են նոր բլոկային ծածկագրման համակարգերի նկատմամբ կիրառված գծային վերլուծության արդյունքները:

Բերենք հակիրճ նկարագրությունը. գծային վերլուծությունը ստատիկ, բաց տեքստերի ընտրմամբ գրոհի (chosen plaintext attack) եղանակ է, որն էֆեկտիվ է այնպիսի համակարգերի համար, որտեղ ենթաբանալիները ստացվում են ըստ mod2-ի գումարման գործողության միջոցով: Բլոկային ծածկագրման համակարգերի գծային վերլուծության ուսումնասիրության առարկան գծային առընչություններն են՝ կազմված սկզբնական բաց տեքստի (plaintext), ծածկագրի (ciphertext) և ենթաբանալու (subkey) բիթերի միջև: Իդեալական համակարգերում նման գծային առընչությունները տեղի ունեն $1/2$ հավանականությամբ: Գծային առընչություններին անվանում են նաև գծային մոտարկումներ կամ ապրոքսիմացիաներ, քանի որ գծային վերլուծությունը կապված է այնպիսի հավասարումների հետ, որոնք բնութագրվում են հավանականություններով:

Յուրաքանչյուր համակարգ ունի գծային մոտարկումների կառուցման յուրահատուկ եղանակ: Մեծմասամբ, գծային մոտարկումները բլոկային ծածկագրման

համակարգերի համար ստացվում են յուրաքանչյուր ռաունդի մոտարկումները միավորելու արդյունքում:

Դիցուք $X_i = (x_n, x_{n-1}, \ldots, x_2, x_1)$ կամայական i-րդ ռաունդի n-բիթանի մուտքն է, $R(X_i)$-ն՝ ելքը, իսկ K_i-ն ռաունդի ենթաբանալին: Այդ դեպքում նրանց միջև գծային առընչությունը կարելի է արտահայտել հետևյալ կերպ՝

$$X_i \cdot \Gamma I \oplus R(X_i) \cdot \Gamma O = K_i \cdot \Gamma K_i \qquad (1)$$

որտեղ ΓI, ΓO և ΓK_i-ն n-բիթանի ծածկույթներ են (mask), որոնք որոշում են X_i-ի, $R(X_i)$-ի և K_i-ի այն բիթերը, որոնք ներառված են գծային առընչության մեջ: Օրինակ՝ $X_i \cdot \Gamma = X \cdot 45_x = x_1 \oplus x_3 \oplus x_7$ ('x' ստորին ինդեքսը նշանակում է թվի արժեքը 16-ական համակարգում): (1) առընչության ձախ մասը տալիս է նրա աջ մասում ենթաբանալու XOR-գումարման գնահատականը: Առանց խախտելու ընդհանրությունը, կարելի է (1) առընչությունը ներկայացնել ավելի պարզեցված տեսքով՝

$$X_i \cdot \Gamma I \oplus R(X_i) \cdot \Gamma O = 0 \qquad (2)$$

(2) առընչությունը կարող է բնութագրվել երկու թվային մեծություններով, որոնցից մեկը $p = \frac{P(X_i \cdot \Gamma I = R(X_i) \cdot \Gamma O))}{2^n}$ է, որը արտահայտում է (2) առընչության տեղի ունենալու հավանականությունը, և երկրորդը՝ (2) առընչության հավասարակշռության շեղումը պատահական բաշխվածությունից, այն է $p' = p - \frac{1}{2}$: Պարզ է, որ $-\frac{1}{2} \le p' \le \frac{1}{2}$, իսկ մոտարկումն արդյունավետ է, երբ $p' \neq 0$: $\varepsilon = |p'|$ բացարձակ արժեքը կոչվում է շեղում: Որքան մեծ է շեղումը, այնքան ավելի արդյունավետ է գծային առընչությունը, այսինքն, որքան առավել շեղված է (2) առընչությունը պատահական բաշխվածությունից, այնքան ավելի քիչ ծավալով բաց տեքստ անհրաժեշտ կլինի գնահատելու (առավել մեծ ճշտությամբ) $K_i \cdot \Gamma K_i$ մեծությունը:

$p' < 0$ դեպքում $K_i \cdot \Gamma K_i$-ի համար տեղի ունի հետևյալը՝ $\overline{K_i \cdot \Gamma K_i} = (K_i \cdot \Gamma K_i) \oplus 1$: Բլոկային ծածկագրման համակարգի մեկ ռաունդի երկարժեք գծային առընչությունը ներկայացնելու համար կատարենք հետևյալ նշանակումը՝

$$\Gamma = (\Gamma I, \Gamma O, \varepsilon)$$

Միառաունդ գծային առընչությունները կարելի է միավորել կամ կապակցել՝ ավելի շատ ռաունդների մոտարկումները ստանալու համար: Եթե $\Gamma_1 = (\Gamma X_1, \Gamma Y_1, \varepsilon_1)$ և $\Gamma_2 = (\Gamma X_2, \Gamma Y_2, \varepsilon_2)$ համապատասխանաբար r_1 ռաունդի և r_2 ռաունդի անկախ գծային առընչություններն են, իսկ $\Gamma Y_1 = \Gamma X_2$, ապա այս առընչությունները կարելի է միավորել՝ $(r_1 + r_2)$ ռաունդի $\varepsilon = 2 \cdot \varepsilon_1 \cdot \varepsilon_2$ շեղումով գծային առընչությունը ստանալու համար:

Այժմ մեկ ռաունդի համար սահմանենք I/O (մուտքային/ելքային) գումար $S^{(i)}$-ն:

Սահմանում 2.1: *Մեկ ռաունդի համար I/O գումար $S^{(i)}$-ն իրենից ներկայացնում է բալանսավորված երկարժեք f_i ֆունկցիայի ռաունդի $Y^{(i-1)}$ մուտքի և բալանսավորված երկարժեք g_i ֆունկցիայի ռաունդի $Y^{(i)}$ ելքի գումարը ըստ mod2-ի, այն է՝*

$$S^{(i)} = f_i(Y^{(i-1)}) \oplus g_i(Y^{(i)}):$$

Սահմանում ՀԿՄ 2.3 (Harpes-Kramer-Massey]: *f_i և g_i ֆունկցիաները կոչվում են $S^{(i)}$ I/O (մուտք/ելք) գումարի համապատասխանաբար մուտքային և ելքային ֆունկցիաներ: Հաջորդական ռաունդների համար I/O գումարները կկոչվեն կապակցված, եթե յուրաքանչյուր I/O գումարի ելքային ֆունկցիան, բացառությամբ վերջինի, համընկնում է իրեն հաջորդող I/O գումարի մուտքային ֆունկցիայի հետ՝ $g_i = f_{i+1}$: Այն դեպքում, երբ $S^{(1)}, S^{(2)}, ..., S^{(r)}$ կապակցված են,նրանց գումարը նույնպես I/O գումար է՝*

$$S^{(1...r)} = \oplus_{i=1}^{r} S^{(i)} = f_0(Y^{(0)}) \oplus g_r(Y^{(r)}),$$

և կոչվում է r ռաունդների I/O գումար:

Աշխատանքում ուսումնասիրվել են նկարագրված I/O գումարները և իրականացվել է ընդհանրացված գծային վերլուծություն SAFER ընտանիքի նոր տարբերակների նկատմամբ: Կատարվել են ծրագրային հետազոտություններ, որոնք թույլ են տալիս ուսումնասիրել կապակցված մուտք/ելք գումարների գոյության հարցը՝ փնտրելով էֆեկտիվ հոմոմորֆ I/O գումարներ ավելի քան մեկ ռաունդի համար: Հետազոտությունների արդյունքում ունենում ենք հետևյալ թեորեմը՝

Թեորեմ 2.2: Էֆեկտիվ հոմոմորֆ I/O գումարներ գտնող եղանակը SAFER-ի երկու կես-ռաունդներից կազմված հաջորդականության համար չի գտնում որևէ I/O գումար ոչ-զրոյական դիսբալանսով, որը ներառում է ամենաքիչը երկու PHT-շերտ:

Հետևաբար, փնտրվող կապակցված գումարների բացակայությունը վկայում է ուսումնասիրվող բլոկային ծածկագրման համակարգերի կայունության մասին գծային վերլուծության նկատմամբ:

Գլխի 2.5 ենթամասում ներկայացվում են կատարված տեսական հետազոտություն-ների արդյունքում հնարավորինս էֆեկտիվորեն մշակված և իրականացված ալգորիթմները՝ կլաստերային հաշվողական համակարգում SAFER բլոկային ծածկագրման համակարգերի ընտանիքի նոր տարբերակների դիֆերենցիալ և գծային վերլուծությունների ծրագրային իրականացման համար:

Ստեղծվել են “DiffLinearAnalyser” և “PrmTest (Permutation Testing)” զուգահեռ հաշվարկների ծրագրային փաթեթները, որոնք գրվել են C++ ծրագրավորման լեզվով, իսկ կլաստերային հաշվողական համակարգում զուգահեռացումը իրականացվել է ինֆորմացիայի ցանցային փոխանցման համար օգտագործվող MPI (Message Passing Interface) համակարգի միջոցով: Այժմ մանրամասն նկարագրենք փաթեթներից յուրաքանչյուրը:

1. PrmTest (Permutation Testing) – փաթեթը նախատեսված է 16 բայթ երկարությամբ տեղադրությունների վերլուծությունը կլաստերային հաշվողական միջավայրում իրականացնելու համար: Դիտարկվում են բոլոր հնարավոր P տեղադրությունները, որոնց քանակն է $16! \approx 2.1 \cdot 10^{13}$:

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ p_1 & p_2 & p_3 & p_4 & p_5 & p_6 & p_7 & p_8 & p_9 & p_{10} & p_{11} & p_{12} & p_{13} & p_{14} & p_{15} & p_{16} \end{pmatrix}$$

Այս տեղադրությունների համար ստուգվում են SAFER ծածկագրման համակարգին անհրաժեշտ և կայունություն ապահովող որոշակի պայմաններ՝

1.1 տեղադրության կենտ դիրքերում պետք է լինեն կենտ ինդեքսներ, իսկ զույգ դիրքերում՝ զույգ ինդեքսներ՝

$$p1, p3, p5, p7, p9, p11, p13, p15 (\mathrm{mod}\ 2) = 1$$
$$p2, p4, p6, p8, p10, p12, p14, p16 (\mathrm{mod}\ 2) = 0$$

1.2 գծային ձևափոխությունների $M(P)$ մատրիցը չպետք է պարունակի զրոյական էլեմենտ՝

$$M(P)[i][j] \neq 0, \ (i, j = 1,2,...,16):$$

Նշված պայմանների ստուգման արդյունքում ընտրվում են տեղադրությունները, որոնք հետագայում ենթարկվելու են դիֆերենցիալ և գծային վերլուծությունների, ընդ որում նշված պայմանների ստուգումը զգալիորեն կրճատում է վերլուծության ենթակա տեղադրությունների քանակը, այն դարձնելով մոտավորապես $8! \cdot 8! \approx 1.6 \cdot 10^9$: Ծրագրի աշխատանքի արդյունքում ունենում ենք “Armenian Shuffle” կոորդինատային տեղափոխությունների մի ցուցակ՝ ենթակա հետագա հետազոտությունների:

2. DiffLinearAnalyser (Differential-Linear Analyser) – ծրագրային փաթեթը նախատեսված է SAFER+ և SAFER++ բլոկային ծածկագրման համակարգերին համարժեք նոր ծածկագրման համակարգերի դիֆերենցիալ և գծային վերլուծությունները կլաստերային հաշվողական միջավայրում իրականացնելու համար: Վերլուծության նպատակով դիտարկվում են PrmTest ծրագրային փաթեթի աշխատանքի արդյունքում ստացված “Armenian Shuffle” կոորդինատային տեղափոխությունները:

“DiffLinearAnalyser” ծրագրաշարում գործողությունների զուգահեռացումը կատարվել է հնարավորինս էֆեկտիվ եղանակով: Ծրագիրը կլաստերային համակարգին հարցում է կատարում՝ որոշակի քանակի պրոցեսորների պահանջով: Ստանալով իրեն անհրաժեշտ քանակի պրոցեսորները՝ խնդրի գործողությունները իրականացնում է հետևյալ կերպ. դիտարկում է պրոցեսներից մեկը որպես գլխավոր (Proc_0), որը բաշխում է տեղադրությունները պրոցեսների միջև (Proc_1…Proc_n), վերահսկում է բոլոր պրոցեսների աշխատանքը և գրանցում է կատարված վերլուծությունների արդյունքները: Մյուս պրոցեսները ստանում են տեղադրութ-յունները, իրականացնում են դիֆերենցիալ ու գծային վերլուծությունները և արդյունքների մասին հայտնում են գլխավոր պրոցեսին, այն

է՝ գլխավոր պրոցեսին են ուղարկում վերլուծությունները դրական արդյունքով անցած “Armenian Shuffle” կոորդինատային տեղափոխությունները: Դիֆերենցիալ և գծային վերլուծությունների նկատմամբ կայունություն ցուցաբերած “Armenian Shuffle” կոորդինատային տեղափոխությունները համարվում են հուսալի հիմք՝ SAFER բլոկային ծածկագրման համակարգերի ընտանիքի նոր տարբերակների սինթեզման համար:

Գլխի 2.6 ենթամասում բերված է եզրակացություն. ամփոփելով կատարված հետազոտությունների արդյունքները՝ նշենք, որ թվով մոտ **6300** “Armenian Shuffle” կոորդինատային տեղափոխություններ ցուցաբերել են կայունություն ծածկագրավերլուծությունների նկատմամբ և համարվում են հուսալի հիմք՝ SAFER բլոկային ծածկագրման համակարգերի ընտանիքի նոր տարբերակների սինթեզման համար: Այդ “Armenian Shuffle” տեղափոխությունների մի մասը բերված է ատենախոսության վերջում՝ “Հավելված1“ բաժնում:

Հետազոտության սահմաններում լուծվել է նաև հետևյալ խնդիրը՝ ապացուցվել է, որ SAFER ընտանիքի ցանկացած բլոկային ծածկագրման համակարգի համար կայունություն ապահովող ռաունդների մինիմալ քանակը 6 է: Այսինքն, SAFER ընտանիքի նոր բլոկային ծածկագրման համակարգ, որի ռաունդների քանակն ավելի քիչ է, քան SAFER+ և SAFER++ համակարգերում ընտրված ռաունդների քանակն է, գոյություն չունի:

Երրորդ գլխում նկարագրվում են մեր կողմից մշակված ալգորիթմները՝ վերջավոր դաշտերի վրա անվերածելի և նորմալ բազմանդամների բացահայտ տեսքով կառուցման համար:

Գլխի 3.1 ենթամասում նկարագրվում է խնդրի դրվածքը, կիբառական նշանակությունը և առաջարկված ալգորիթմների հիմնական առավելությունները նմանատիպ ալգորիթմների նկատմամբ:

Գլխի 3.2 ենթամասում նկարագրվում է վերջավոր դաշտերի վրա անվերածելի բազման-դամների կառուցման մեթոդը՝ Վարշամովի օպերատորի օգտագործմամբ, որի համար կատարվել է ծրագրային իրականացում:

Առաջարկվող մեթոդը թույլ է տալիս նախապես ընտրված պրիմիտիվ և անվերածելի բազմանդամների օգտագործմամբ բացահայտ տեսքով կառուցել բարձր աստիճանի անվերածելի բազմանդամներ: Այս մեթոդի հիման վրա մշակվել է էֆեկտիվ ալգորիթմ՝ կլաստերային հաշվողական համակարգում մեթոդի ծրագրային իրականացման համար: Հիշողության ռեսուրսների բաշխումը՝ հիշողության հատկացումն ու ժամանակին ազատումը կատարվել են խնայողաբար, քանի որ հաշվարկների ընթացքում տվյալների երկարությունները շատ արագ աճում են: Կլաստերային հաշվողական համակարգում ծրագրի զուգահեռացումը կատարվել է ըստ տվյալների, այսինքն տվյալները բաշխվում են պրոցեսորների միջև, բոլոր պրոցեսորները աշխատում են միևնույն ծրագրով և յուրաքանչյուրը կառուցում է հերթական անվերածելի բազմանդամը: Արդյունքում ստանում ենք անվերածելի բազմանդամների հաջորդականություն և բացի այդ փնտրում ենք միևնույն աստիճանի հնարավորինս փոքր կշիռ ունեցող անվերածելի բազմանդամը:

Նկարագրվելիք մեթոդը թույլ է տալիս կառուցել և՛ կենտ և՛ զույգ աստիճանի անվերածելի բազմանդամներ, բացի այդ կառուցում ենք համեմատաբար փոքր կշռով անվերածելի բազմանդամներ: Այսպես, կառուցվելիք անվերածելի բազմանդամը կունենա $n\cdot\prod_{i=1}^{\sigma}(2^{n_i}-1)$ աստիճանը, որտեղ $n,n_1,n_2,...,n_\sigma(n_i>1)$ փոխադարձաբար պարզ թվերը հանդիսանում են նախապես ընտրված անվերածելի և պրիմիտիվ բազմանդամների աստիճանները: Կախված նրանից, կենտ աստիճանի բազմանդամ ենք ուզում կառուցել, թե զույգ, կարող ենք ընտրել այնպիսի բազմանդամներ, որոնց դեպքում $n\cdot\prod_{i=1}^{\sigma}(2^{n_i}-1)$ թիվը կլինի զույգ կամ կենտ, ըստ մեր ցանկության, հետևաբար բացահայտ տեսքով կկառուցենք համապատասխան աստիճանի բազմանդամը:

Դիցուք $L^\theta f(x)$-ը Վարշամովի օպերատորն է, որը սահմանվում է հետևյալ կերպ՝

$$L^\theta f(x)=\frac{1}{\theta(x)}\sum_{u=0}^{m}\sum_{v=0}^{n}\theta_u a_v x^{uq^v}$$

որտեղ $f(x)=\sum_{u=0}^{n}a_u x^u$ և $\theta(x)=\sum_{v=0}^{m}a_v x^v$, $a_u,\theta_v\in F_2$:

Դիտարկենք $n_1,n_2,...,n_\sigma(n_i>1)$ փոխադարձաբար պարզ աստիճաններով պրիմիտիվ բազմանդամների $\Sigma_\sigma=\{f_1(x),f_2(x),...,f_\sigma(x)\};\sigma\geq 1$ բազմությունը և n աստիճանի $\varphi(x)$ անվերածելի բազմանդամը F_2 վերջավոր դաշտի վրա: Դիցուք $T=\prod_{i=1}^{\sigma}(2^{n_i}-1)$ և տեղի ունի հետևյալ պայմանը՝ $\gcd(n,T)=1$ (gcd - greatest common divisor/ամենամեծ ընդհանուր բաժանարար): Դիտարկենք նաև G_σ բազմությունը, որը հանդիսանում է σ երկարությամբ բոլոր հնարավոր $\varepsilon=(\varepsilon_1,\varepsilon_2,...,\varepsilon_\sigma);\varepsilon_i=\overline{0,1}$ բինար վեկտորների բազմությունը (կբացառենք $\varepsilon=(0,0,...,0)$-ի դեպքը): Յուրաքանչյուր $\varepsilon\in G_\sigma\setminus(00...0)$ հաջորդականության համար կատարենք հետևյալ նշանակումները՝

$$f(x,\varepsilon,\Sigma_\sigma)=L^x\prod_{i=1}^{\sigma}f_i(x)^{\varepsilon_i},$$

$$xf(x,\varepsilon,\Sigma_\sigma)\equiv R^{(\varepsilon)}(x)(\mathrm{mod}\ \varphi(x)),$$

և $\psi^{(\varepsilon)}(x)=\sum_{u=0}^{n}\psi_u^{(\varepsilon)}x^u$, որտեղ $\psi_u^{(\varepsilon)}(x)$-ը հետևյալ առընչության ոչ-տրիվյալ լուծումն է՝

$$\sum_{u=0}^{n}\psi_u^{(\varepsilon)}(R^{(\varepsilon)}(x))^u\equiv 0(\mathrm{mod}\ \varphi(x)):$$

Այս պայմանների դեպքում տեղի ունի հետևյալ թեորեմը, որն առաջարկել է Կյուրեղյանն իր աշխատանքներից մեկում՝

Թեորեմ 3.2.1: Հետևյալ բազմանդամները՝

$$F(x)=(\varphi(x))^{(-1)^{\sigma}}\frac{\prod_{\substack{\varepsilon\in G_\sigma \\ 2|(\sigma-|\varepsilon|)}}\psi^{(\varepsilon)}(xf(x,\varepsilon,\Sigma_\sigma))}{\prod_{\substack{\varepsilon\in G_\sigma \\ 2\dagger(\sigma-|\varepsilon|)}}\psi^{(\varepsilon)}(xf(x,\varepsilon,\Sigma_\sigma))}$$

և $\psi^{(\nu)}(x)$, որտեղ $|\varepsilon|=\sum_{i=1}^{\sigma}\varepsilon_i$ և $\nu\in G_\sigma$, համապատասխանաբար nT և n աստիճանի անվերածելի բազմանդամներ են F_2 վերջավոր դաշտի վրա:

Անվերածելի բազմանդամների կառուցման նկարագրված մեթոդի ծրագրային իրականացման համար հնարավորինս էֆեկտիվորեն մշակվել է IPG (Irreducible Polynomial Generator) ծրագրային փաթեթը: IPG Ծրագրի աշխատանքի արդյունքում կառուցվել են մինչև **1.560.000** աստիճանի ավերածելի բազմանդամներ՝ հնարավորինս փոքր կշիռներով. յուրաքանչյուր բազմանդամ ունի իր երկարության կեսին մոտ կամ ավելի փոքր կշիռ: Մասնավորապես, ծրագիրը հնարավորություն է տալիս նաև կառուցելու մինիմալ կշռով՝ երեք կամ հինգ կշիռ ունեցող բազմանդամներ:

Ծրագրային փաթեթում կառուցվող բազմանդամների աստիճանների վրա սահմանափակում դրված չէ և այն հնարավորություն է տալիս կառուցելու նաև ավելի բարձր աստիճանի բազմանդամներ: Փորձերը ցույց են տվել, որ մինչև **95000** աստիճանի բազմանդամների կառուցումը կատարվում է ակնթարթորեն՝ մեկ վայրկյանից փոքր ժամանակում, իսկ ավելի բարձր՝ մինչև **1559814** աստիճանի բազմանդամները կառուցվում են վայրկյանների ընթացքում՝ առավելագույնը 156 վայրկյան:

Աղյուսակ 1-ում բերված է ծրագրի աշխատանքի արդյունքներն արտացոլող աղյուսակ: Աղյուսակի առաջին սյունակում նշված են կառուցված անվերածելի բազմանդամների աստիճանները, երկրորդ սյունակում նշված են նախապես ընտրված $\varphi(x)$ անվերածելի բազմանդամի և $\Sigma_\sigma=\{f_1(x),f_2(x),...,f_\sigma(x)\};\sigma\geq 1$ պրիմիտիվ բազմանդամների աստիճանները, երրորդ սյունակում՝ բազմանդամի կառուցման ժամանակը վայրկյաններով, իսկ վերջին սյունակում՝ կառուցված անվերածելի բազմանդամի կշիռը:

Աղյուսակ 1

Անվերածելի բազմանդամի աստիճանը	$\varphi(x)$ **և** $\Sigma_\sigma=\{f_1(x),f_2(x),...,f_\sigma(x)\}$ **բազմանդամների աստիճանները**	**1 CPU Dual Core 4GHz վրկ.**	**Անվերածելի բազմանդամի կշիռը**
105	7, 4	0.0047	41
1020	4, 8	0.0053	545
2044	4, 9	0.0055	1083
4092	4, 10	0.0075	2183
6132	4, 2, 9	0.0155	3121
13335	7, 4, 7	0.0231	6427
40005	5, 6, 7	0.1415	19399

661416	8, 2, 3, 5, 7	68.0165	330843
909447	11, 2, 3, 5, 7	156.7333	455217
1332597	7, 2, 5, 11	71.8381	665457
1559814	6, 7, 11	81.1987	773343

Մշակվել է ալգորիթմ՝ կառուցելու մինիմալ (երեք կամ հինգ) կշռով անվերածելի բազմանամներ՝ հիմնվելով Թեորեմ 3.2.1-ի միջոցով կառուցված անվերածելի բազմանամների վրա:

Աղյուսակ 2-ում բերված են երեք և հինգ կշիռ ունեցող որոշ անվերածելի բազմանդամներ:

Աղյուսակ 2

Անվերածելի բազմանդամի աստիճանը	$\varphi(x)$ և $\Sigma_\sigma = \{f_1(x), f_2(x),..., f_\sigma(x)\}$ բազմանդամների աստիճանները	Անվերածելի բազմանդամի կշիռը	Անվերածելի Բազմանդամը
12	4, 2	3	X^12+x^3+1
15	5, 2	3	X^15+x^1+1
24	8, 2	5	X^24+x^4+x^3+x^1+1
28	4, 3	3	X^28+x^1+1
30	10, 2	3	X^30+x^1+1
60	4, 4	3	X^60+x^1+1
105	5, 2, 3	3	X^105+x^4+1

Դիցուք $F(x)$-ը n աստիճանի անվերածելի բազմանդամ է F_2 վերջավոր դաշտի վրա՝ կառուցված վերը նկարագրված եղանակով: Այժմ n աստիճանի անվերածելի բազմանդամի կշիռը մինիմալի հասցնելու նպատակով կիրառվում է հետևյալ մեթոդը. որպես հիմք վերցվում է այս $F(x)$ բազմանդամը և դիտարկվում է հետևյալ առընչությունը՝

$$\sum_{u=0}^{n} \psi(R(x))^u \equiv 0 (\mathrm{mod}\ F(x)) : \qquad (1)$$

Այստեղ $R(x)$-ը որոշվում է $x^r \equiv R(x) (\mathrm{mod}\ F(x))$ արտահայտությունից, որտեղ r-ը $2^n - 1$-ի բաժանարար չէ: (1) առընչության $\psi(x)$ ոչ-տրիվյալ լուծումը ևս հանդիսանում է n աստիճանի անվերածելի բազմանդամ F_2 վերջավոր դաշտի վրա: Այսպիսով, դիտարկելով (1) առընչությունը բոլոր այն r-երի համար, երբ r-ը $2^n - 1$-ի բաժանարար չէ և $2 \le r < 2^n - 1$՝ կգտնենք n աստիճանի մինիմալ կշռով անվերածելի բազմանդամը:

Գլխի 3.3 ենթամասում նկարագրվում են հաշվողական տեսակետից հեշտ եղանակներ՝ կենտ բնութագրիչով վերջավոր դաշտերի վրա անվերածելի և գծորեն

անկախ արմատներով բազմանդամների կառուցման համար: Դիտարկվում են հետևյալ տիպի քառակուսային ձևափոխությունները $F_q[x]$ օղակում՝

$$P(x) \to (dx^2 + rx + h)^n P\left(\frac{ax^2 + bx + c}{dx^2 + rx + h}\right),$$

որտեղ q -ն կենտ պարզ թիվ է: Այն թույլ է տալիս կառուցել ավելի բարձր կարգի անվերածելի բազմանդամներ՝ հիմնվելով որոշակիորեն ընտրված $P(x)$ անվերածելի բազմանդամի վրա, որն ունի առնվազն մեկ գործակից՝ $a_{2i+1} \neq 0, (0 \le i \le \lfloor n/2 \rfloor)$ պայմանին բավարարող:

Մինչ մեթոդների նկարագրությանն անցնելը տանք որոշ հիմնական գաղափարների սահմանումները: Դիցուք F_q -ն $q = p^s$ կարգն ունեցող Գալուայի դաշտն է՝ իր F_q^* մուլտիպլիկատիվ խմբով, որտեղ p -ն կենտ պարզ թիվ է, իսկ s -ը բնական թիվ է: Ենթադրենք, որ $F(x)$ -ը F_q դաշտի վրա անվերածելի n աստիճանի նորմավորված բազմանդամ է և β -ն նրա արմատն է, հետևաբար $F_q(\beta) = F_{q^n}$ դաշտը F_q դաշտի n -չափանի ընդլայնումն է: F_{q^n} -ի Գալուայի խումբը F_q -ի վրա ցիկլիկ է և գեներացված է Ֆրոբենիուսի արտապատկերմամբ՝ $\sigma(\alpha) = \alpha^q, \alpha \in F_{q^n}$:

F_{q^n} -ի նորմալ բազիս F_q -ի վրա կոչվում է $N = \left\{\alpha, \alpha^q \ldots, \alpha^{q^{n-1}}\right\}$ բազիսը, այսինքն դա բազիս է՝ կազմված որոշակի ֆիկսված $\alpha \in F_{q^n}$ էլեմենտի հանրահաշվական համալուծներից: Այդպիսի α -ին կանվանենք նորմալ բազիսի ծնիչ էլեմենտ: Մյուս կողմից, $\alpha \in F_{q^n}$ -ին կանվանենք F_{q^n} -ի նորմալ էլեմենտ F_q -ի վրա այն և միայն այն դեպքում, երբ նրա հանրահաշվական համալուծներից կազմված $\{\alpha, \alpha^q \ldots, \alpha^{q^{n-1}}\}$ բազմությունը կազմում է F_{q^n} -ի նորմալ բազիս F_q -ի վրա: Ապացուցելու համար, որ $\alpha \in F_{q^n}$ -ը նորմալ էլեմենտ է, Meyn-ը իր աշխատանքում դիտարկել է F_{q^n} -ը որպես $F_q[x]$ օղակի մոդուլ $\left(\sum_k a_k x^k\right) \circ \alpha = \sum_k a_k \sigma^k(\alpha)$ գործողության նկատմամբ, որտեղ $\sigma : \alpha \to \alpha^q$ արտապատկերումը Ֆրոբենիուսի ավտոմորֆիզմն է: $\alpha \in F_{q^n}$ էլեմենտի աղիտիվ կարգ (annihilator) կանվանենք այն $g(x)$ բազմանդամը և կնշանակենք՝ $Ord_q(\alpha) = g(x)$, որի համար տեղի ունի հետևյալ պայմանը՝ $g(x) \circ \alpha = 0$ և $\frac{g(x)}{h(x)} \circ \alpha \neq 0,$ $g(x)$ -ի բոլոր նորմավորված $h(x)$ բաժանարարների համար:

Յուրաքանչյուր α -ի համար $Ord_q(\alpha)$ -ն բաժանվում է $x^n - 1$ բազմանդամի վրա և α -ն կոչվում է նորմալ էլեմենտ այն և միայն այն դեպքում, երբ $Ord_q(\alpha) = x^n - 1$: Այն

դեպքում, երբ α նորմալ էլեմենտի հանրահաշվական համալուծները F_{q^r} -ի վրա կազմում են F_{q^n} -ի F_{q^r} վեկտորական տարածության բազիս n -ի յուրաքանչյուր r բաժանարարի համար, այդ α -ին անվանում են F_{q^n} -ի կատարյալ նորմալ էլեմենտ F_q -ի վրա:

Նորմավորված $F(x) \in F_q[x]$ անվերածելի բազմանդամը կանվանենք նորմալ կամ N -բազմանդամ, եթե նրա արմատները F_q դաշտի վրա գծորեն անկախ են: Ցանկացած էլեմենտի մինիմալ բազմանդամը $N = \left\{\alpha, \alpha^q \ldots, \alpha^{q^{n-1}}\right\}$ նորմալ բազիսում հետևյալն է՝ $m(x) = \prod_{i=0}^{n-1} (x - \alpha^{q^i}) \in F_q[x]$, որը F_q -ի վրա անվերծելի բազմանդամ է: Նորմալ բազիսի էլեմենտները որոշակի N -բազմանդամի արմատներն են, հետևաբար N -բազմանդամը նորմալ բազիսի նկարագրման մեկ այլ եղանակն է: Հայտնի է, որ նման բազիս միշտ գոյություն ունի և N -ի յուրաքանչյուր էլեմենտ նաև N -ի ծնիչ էլեմենտ է:

Գլխի 3.3.1 ենթամասում նկարագրվում է անվերածելի բազմանդամների կառուցման մի մեթոդ և ապացուցվում է հետևյալ թեորեմը՝

<u>Թեորեմ 3.3.1.1</u> Դիցուք q -ն կենտ պարզ թիվ է, $P(x) = \sum_{u=0}^{n} a_u x^u \in F_q[x] \quad n > 1$ աստիճանի անվերածելի բազմանդամ է, որի առնվազն մեկ գործակցի համար բավարարված է հետևյալ պայմանը՝ $a_{2i+1} \neq 0, (0 \le i \le \lfloor n/2 \rfloor)$: Դիցուք $ax^2 + 2hx + ahd^{-1}$ և $dx^2 + 2ax + h$ փոխադարձաբար պարզ բազմանդամներ են, որտեղ $a, d, h \in F_q^*$ և $a \neq hd$: Ենթադրենք, որ $(hd^{-1})^n$ -ը ոչ-զրոյական քառակուսային էլեմենտ է F_q -ում, իսկ $(hd - a^2)^n g_0\left(\frac{h}{d}\right)$ -ն, որտեղ $g(x) = (-1)^n \sum_{\substack{0 \le j \le n \\ u+v=2j,\, v<u \le n}} ((-1)^n 2a_u a_v + (-1)^j a_j^2) x^j$ ոչ-քառակուսային էլեմենտ է F_q -ում: Սահմանենք $t_k = n2^k$ աստիճանի $F_k(x)$ բազմանդամների հաջորդականությունն այսպես՝

$$\begin{cases} F_0(x) = P(x) \\ F_k(x) = H_{k-1}(a,d)^{-1} (dx^2 + 2ax + h)^{t_{k-1}} F_{k-1}\left(\frac{ax^2 + 2hx + ahd^{-1}}{dx^2 + 2ax + h}\right); k \ge 1 \end{cases},$$

որտեղ $H_{k-1}(a,d) = d^{t_{k-1}} F_{k-1}\left(\frac{a}{d}\right)$: Այդ դեպքում յուրաքանչյուր $k \ge 1$ -ի համար $F_k(x)$ -ը $t_k = n2^k$ աստիճանի անվերածելի բազմանդամ է F_q -ի վրա:

Գլխի 3.3.2 ենթամասում նկարագրվում է անվերածելի բազմանդամների կառուցման մեկ այլ մեթոդ, ապացուցվում է հետևյալ թեորեմը՝

Թեորեմ 3.3.2.1 Դիցուք q-ն կենտ պարզ թիվ է, $P(x)=\sum_{u=0}^{n}a_u x^u \in F_q[x] \quad n>1$ աստիճանի անվերածելի բազմանդամ է, որի առնվազն մեկ գործակցի համար բավարարված է հետևյալ պայմանը՝ $a_{2i+1}\neq 0,(0\le i\le \lfloor n/2 \rfloor)$: Ենթադրենք, որ $a,c\in F_q^*$, $(ac)^n$-ը քառակուսային էլեմենտ է F_q-ում, իսկ $(-1)^n g_0\left(\frac{c}{a}\right)$-ն, որտեղ

$$g(x)=(-1)^n \sum_{\substack{0\le j\le n \\ u+v=2j, v<u\le n}}((-1)^n 2a_u a_v+(-1)^j a_j^2)x^j,$$

ոչ-քառակուսային էլեմենտ է F_q դաշտում: Սահմանենք $t_k=n2^k$ աստիճանի $F_k(x)$ բազմանդամների հաջորդականությունն այսպես՝

$$\begin{cases} F_0(x)=P(x) \\ F_k(x)=(2x)^{t_{k-1}}F_{k-1}\left(\dfrac{ax^2+c}{2ax}\right); k\ge 1 \end{cases}:$$

Այդ դեպքում յուրաքանչյուր $k\ge 1$-ի համար $F_k(x)$-ը $t_k=n2^k$ աստիճանի անվերածելի բազմանդամ է F_q-ի վրա:

Հիմնական դրույթներն ու եզրահանգումները

- Մշակվել են նոր բլոկային ծածկագրման համակարգեր՝ կառուցված արդեն գոյություն ունեցող SAFER+ և SAFER++ բլոկային ծածկագրման համակարգերի հիման վրա, որոնք ևս հանդիսանում են SAFER ընտանիքի նոր տարբերակներ [3]:
- SAFER ընտանիքի մեր կողմից սինթեզված նոր բլոկային ծածկագրման համակարգերի դիֆերենցիալ ամբողջական վերլուծությունը՝ իրականացված ծրագրային միջոցներով, ցույց է տվել, որ $r=5$ ռաունդից սկսած բոլոր դիֆերենցիալ շղթաների անցումային հավանականությունները փոքր են 2^{-128}-ից, ինչը նշանակում է, որ նոր բլոկային ծածկագրման համակարգերը 6 և ավելի (սակայն ոչ քիչ) ռաունդների դեպքում ապահով և կայուն են դիֆերենցիալ վերլուծության նկատմամբ:
- Ապացուցվել է, որ SAFER ընտանիքի ցանկացած բլոկային ծածկագրման համակարգի համար կայունություն ապահովող ռաունդների մինիմալ քանակը 6 է: Այսինքն, SAFER ընտանիքի նոր բլոկային ծածկագրման համակարգ, որի ռաունդների քանակն ավելի քիչ է, քան SAFER+ և SAFER++ համակարգերում ընտրված ռաունդների քանակն է, գոյություն չունի: Թվով մոտ **6300** "Armenian Shuffle" կոորդինատային տեղափոխություններ ցուցաբերել են կայունություն ծածկագրավերլուծությունների նկատմամբ և համարվում են հուսալի հիմք՝ SAFER բլոկային ծածկագրման համակարգերի ընտանիքի նոր տարբերակների սինթեզման համար [3,7]:

- F_2 վերջավոր դաշտի վրա անվերածելի բազմանդամների կառուցման համար նկարագրվել և իրականացվել է մեթոդ, որի օգնությամբ կառուցվել են մինչև **1.560.000** աստիճանի ավերածելի բազմանդամներ՝ հնարավորինս փոքր կշիռներով: Մասնավորապես, մեթոդը հնարավորություն է տալիս նաև կառուցելու մինիմալ կշռով՝ երեք կամ հինգ կշիռ ունեցող բազմանդամներ [5,6]:
- Ներկայացվել է հաշվողական տեսակետից հեշտ եղանակ՝ կենտ բնութագրիչով վերջավոր դաշտերի վրա նորմավորված անվերածելի և նորմալ բազմանդամների հաջորդականությունների կառուցման համար [1,2,4]:

<u>Ատենախոսության թեմայի շրջանակներում հրապարակված աշխատությունների ցանկ</u>

1. M. K. Kyureghyan, M. M. Kyureghyan, O. A. Manukyan, "Completely Normal Elements in Iterated Quadratic Extentions of Finite Fields of Odd Characteristics", Proceedings of the International Conference on Computer Science and Information Technologies CSIT"2005, September 19-23, Yerevan, Armenia, pp. 172-178, 2005.
2. O. A. Manukyan, "Methods for Constructing Irreducible Polynomials over Finite Fields", Proceedings of the International Conference on Computer Science and Information Technologies CSIT"2005, September 19-23, Yerevan, Armenia, pp. 178-182, 2005.
3. M. K. Kyureghyan, O. A. Manukyan, "Differential Cryptanalysis of Block Ciphers in the Cluster Computational Environment", Proceedings of the International Conference on Computer Science and Information Technologies CSIT"2005, September 19-23, Yerevan, Armenia, pp. 447-451, 2005.
4. M. K. Kyureghyan, O. A. Manukyan, "Completely Normal Elements in Iterated Quadratic Extentions of Finite Fields of Odd Characteristics", Mathematical Problems of Computer Science 31, 16-27, 2008.
5. O. A. Manukyan, "Explicit Construction of Irreducible Polynomials over Finite Field F_2 in Cluster Computational Environment", Proceedings of the International Conference on Computer Science and Information Technologies CSIT"2009, September, 28 - October 2, Yerevan, Armenia, pp. 167-168, 2009.
6. O. A. Manukyan, M. K. Kyureghyan, "Construction of Explicit Irreducible Polynomials over F_2 In Cluster Computational Environment", Mathematical Problems of Computer Science 33, 144-149, 2010.
7. O. A. Manukyan, M. K. Kyureghyan, E. Harutyunyan, "Linear Cryptanalysis of Block Ciphers in the Cluster Computational Environment", Mathematical Problems of Computer Science 33, 121-126, 2010.

Ofelya Manukyan

Design and Implementation of Effective Algorithms Applicable in SAFER type Cryptosystems

RESUME

The aim of the thesis is to propose new versions of block ciphers of SAFER family and to prove their crypto-resistance against both differential and linear cryptanalysis. Further, research was focused on computationally easy and efficiently implementable iterative techniques to construct irreducible and normal polynomials over finite fields that still remain a subject of interest both from mathematical theory, as well as practical applications such as coding theory and cryptosystems using finite fields.

The SAFER family of block ciphers has increased with several new versions of block ciphers that are as strongly secure against crypto-attacks as the more-recent members - SAFER+ and SAFER++, and offer substantial improvment in speed over the previous ciphers in SAFER family. Availability of a great variety of versions of SAFER family block ciphers allows the user to choose randomly one of these versions and employ it for exchanging encrypted messages between communicating parties by the mutual acceptance of all communicating sides. Due to these option the security level of the cryptosystem is considerable enhanced, since now it is based on two components: the private key and the secrecy of cryto-algorithm version.

The second area of the research has been the problem of construction of irreducible and normal polynomials over finite fields in explicit form. Different algorithms and techniques of construction of such polynomials are proposed and a software realization of one of these methods is presented. The considered techniques of construction allow constructions of low weight irreducable polynomials (the weight of a polynomial is the number of nonzero coefficients of the polynomial). Usage of low weight irreducible polynomials allows faster implementation of basic operations over finite fields.

Generally, the problem of constructing or finding irreducible and normal polynomials over finite fields remains almost open in basic theorems of cryptography, since they mainly address to the problem of irreducibility itself, while the issues of constructing or finding such polynomials fall out of the range of their consideration.

The software packages: "*DiffLinearAnalyser*", intended for construction of new block ciphers and "*IPG*", provided for construction of irreducible polynomials, may currently serve as a complete, practical software tool for conducting an integrated, comprehensive research in many fields of cryptography.

The software tools providing effective calculation of finite field operations can be widely used in similar applications, where the implementation power and allocation and distribution of memory resources is drastically important.

"*DiffLinearAnalyser*" software package is installed in Arm Cluster computational environment at the Institute of Information and Automation problems of NAS RA. The main part of the research was carried out within the framework of ISTC A-823 and ISTC A-1453 projects.

The following aspects are provided in the thesis:

1. Design of versions of block ciphers of SAFER family on the basic of existing block ciphers SAFER+ and SAFER++.
2. Differential and linear cryptanalyses and their applications against the newly-designed versions of block ciphers
3. Proposition of new methods of construction of irreducible and normal polynomials over finite fields which allow constructions of low weight irreducable polynomials (the weight of a polynomial is the number of nonzero coefficients of the polynomial)
4. Design of "*DiffLinearAnalyser*" software package intended for performing differential and linear crypto-analyses of newly- created block ciphers in the cluster computational environment.
5. Design of "*IPG*" program paskage provided for construction of sequences of irreducible polynomials and search of low weight irreducable polynomials.

The main results are:

- Several new versions of block ciphers of SAFER family have been proposed, which by their crypto-characteristics proved to be similar to the more-recent members of the family: SAFER+ and SAFER++ and offer substantial improvment in speed over the previous ciphers in SAFER family. This means that such new "Armenian Shuffle" coordinate permutations have been found for these newly–created versions that also provide the best possible diffusion and are similarly strongly secure against differential and linear cryptanalyses.
- "*DiffLinearAnalyser*" parallel software package intended for performing differential and linear cryptanalyses of newly-created block ciphers may currently serve as a complete, practical software tool for conducting an integrated, comprehensive research in many fields of designing new versions of SAFER family cryptosystems.
- New methods have been suggested for constructing irreducible and normal polynomials over finite fields. One of the methods based on Varshamov's operator allows constructions of sequences of irreducible polynomials of higher degree over F_2 in explicit form starting from a given irreducible polynomial and a primitive polynomial. "*IPG*" software package provided for construction of sequences of irreducible polynomials as well as for finding low weight irreducable polynomials of have been developed.

Манукян Офелия Альбертовна

Разработка и реализация эффективных алгоритмов применимых в “SAFER” и подобных криптосистемах

ЗАКЛЮЧЕНИЕ

Целью данной работы является построение новых блочных шифров семейства SAFER и доказательство их криптостойкости относительно дифференциального и линейного криптоанализа, а так же проведение ряда исследований по разработке эффективных и быстро-реализуемых итеративных методов построения неприводимых и нормальных полиномов над конечными полями, имеющие решающее значение в разных областях криптографии.

Семейство блочных шифров SAFER пополнилось новыми, не имеющими аналогов вариантами, которые по своей криптостойкости и быстродействию не уступают как криптосистемам SAFER+ и SAFER++, так и всем предшествующим представителям данного семейства. Наличие нескольких вариантов блочных шифров семейства SAFER позволяет пользователю произвольно выбирать одну из версий криптоалгоритма и применять ее для передачи кодированных сообщений между передающей и принимаюшей сторонами по их обоюдному согласию. Возможность такого выбора усиливает криптоустойчивость шифра, при этом сектерность шифра обеспечивается двумя составляющими: первое – наличие секретного ключа и второе - случайный выбор определенной версии криптоалгоритма.

Вторым направлением исследований является задача построения неприводимых и нормальных полиномов над конечными полями. В данной работе предложены новые методы построения таких полиномов, один из которых представлен в программной реализации. Рассмотренные нами алгоритмы дают возможность получить неприводимые полиномы с малым весом. Обычно, решение задачи построения неприводимых полиномов не учитывается основными теоремами по той причине, что в большинстве случаев они обращены к самой проблеме неприводимости полиномов, а предоставление методов построения или нахождения таких полиномов остается за пределами их рассмотрения.

В ходе работы над диссертацией были разработаны программные пакеты “DiffLinearAnalyser” и “IPG”. “DiffLinearAnalyser”, предназначенные для построения блочных криптоалгоритмов семейства SAFER. “IPG” предназначен для построения неприводимых полиномов. Эти пакеты могут применяться как программное средство для решения как практических, так и экспериментальных задач в разных областях криптографии.

Программные средства, обеспечивающие оптимальную реализацию алгебраических операций над элементами конечных полей могут найти широкое применение при решении аналогичных задач, в которых скорость реализации операций, а также эффективное распределение и размещение ресурсов памяти играют определяющую роль.

Программный пакет “DiffLinearAnalyser” внедрен в Институте Проблем Информатики и Автоматизации НАН РА, в вычислительной среде ARM Cluster, которая

является высокоэффективной, быстродействующей инфраструктурой, поддерживающей параллельные вычисления.

На защиту выносятся следующие положения:

1. Новые версии семейства блочных шифров SAFER, созданные на основе блочных шифров SAFER+ и SAFER++ .
2. Методы дифференциального и линейного криптоанализа и их применение к предложенным разновидностям блочных шифров.
3. Новые методы построения неприводимых и нормальных полиномов над конечными полями, позволяющие получать неприводимые полиномы с наименьшим весом.
4. Программный пакет “DiffLinearAnalyser”, который предназначен для проведения дифференциального и линейного криптоанализа блочных шифров семейства SAFER в кластерной вычислительной среде.
5. Программный пакет “IPG”, который предназначен для построения последовательности неприводимых полиномов и нахождения неприводимых полиномов с наименее возможным весом.

Основные результаты:

- Разработаны новые версии блочных шифров, которые по своим криптохарактеристикам равносильны криптоалгоритмам SAFER+ и SAFER++, т.е. для них найдены такие координатные перестановки “Armenian Shuffle”, которые также обеспечивают наилучшую возможную диффузию криптосистемы, тем самым усиливая ее криптостойкость к криптоанализу. Новые версии блочных шифров аналогично быстродействены, как и вышеназванные шифры, благодаря меньшему числу раундов шифрования.
- Проведен дифференциальный и линейный криптоанализ вновь разработанных версий блочных шифров семейства SAFER. Доказана криптостойкость данных версий к атакам дифференциального и ленейного криптоанализа. Спроектировано параллельное программное средство “DiffLinearAnalyser”, предназначенное для проведения дифференциального и линейного криптоанализа вновь разработанных версий блочных шифров SAFER+ и SAFER++. Оно представляется целостным средством, которое поддерживает эффективные исследования в области разработки новых криптоалгоритмов аналогичных SAFER+ и SAFER++.
- Предложены новые методы построения неприводимых и нормальных полиномов над конечными полями. Один из рассмотренных методов, основанный на операторе Варшамова, позволяет получать последовательности неприводимых полиномов высоких степеней над полем F_2 в явном виде, исходя из имеющихся неприводимого и примитивного полиномов. Разработан программный пакет “IPG”, который позволяет получать неприводимые полиномы в явном виде, а также находить полиномы с наименее возможным весом среди полиномов одной и той же степени.