ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Կյուրեղյան Քնարիկ Մարտինի

SAFER ԸՆՏԱՆԻՔԻ 256 ԲԻԹԱՅԻՆ ԾԱԾԿԱԳՐԱԿԱՆ ՀԱՄԱԿԱՐԳԻ ՄՇԱԿՈՒՄ ԵՎ ԻՐԱԿԱՆԱՑՈՒՄ

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

ՍԵՂՄԱԳԻՐ

ԵՐԵՎԱՆ 2017

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Кюрегян Кнарик Мартиновна

РАЗРАБОТКА И РЕАЛИЗАЦИЯ 256 БИТНОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ СЕМЬИ SAFER

АВТОРЕФЕРАТ

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 ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում

Գիտական ղեկավար՝ ֆիզ. մաթ. գիտ. թեկնածու Մ.Կ. Կյուրեղյան

Պաշտոնական ընդդիմախոսներ՝ ֆիզ. մաթ. գիտ. դոկտոր Լ.Հ. Ասլանյան
տեխ. գիտ. թենածու Ա.Հ. Ջիվանյան

Առաջատար կազմակերպություն՝ Հայաստանի ազգային պոլիտեխնիկական համալսարան

Պաշտպանությունը կայանալու է 2017թ. հունիսի 22–ին, ժամը 16:00–ին, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ 0014, Երևան, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ գրադարանում:

Սեղմագիրը առաքված է 2017թ. մայիսի 22–ին:

037 մասնագիտական խորհրդի գիտական քարտուղար, ֆիզ. մաթ. գիտ. դոկտոր Հ. Գ. Սարուխանյան

Тема диссертациии утверждена в Институте проблем информатики и автоматизации НАН РА

Научный руководитель: кандидат физ. мат. наук М. К. Кюрегян

Официальные оппоненты: доктор физ. мат. наук Л.А. Асланян
кандидат тех. наук А.А. Дживанян

Ведущая организация: Национальный политехнический университет Армении

Защита диссертации состоится 22–го июня 2017 года в 16:00 часов на заседании специализированного совета 037 “Информатики” 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 22–го мая 2017г.

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

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը: Տեղեկատվական տեխնոլոգիաների (ՏՏ) ոլորտի արագ և շարունակական զարգացմանը զուգընթաց ինֆորմացիայի անվտանգությունը ապահովող ծածկագրական համակարգերի մի մասը ժամանակի ընթացքում դառնում է խոցելի: Հարկավոր է անհիւնդհատ կատարելագործել ինֆորմացիոն անվտանգության համակարգերի կայունությունն ու հնարավորությունները, հայտնաբերել ու արագ վերացնել խոցելի կողմերը, և մշակել առավել անվտանգ, արագագործ, փոքր ծավալի հիշողություն պահանջող նոր ծածկագրական համակարգեր:

Ժամանակակից ծածկագրաբանության 4 հիմնական սկզբունքներն են.

1. Գաղտնիությունը (Confidentiality). ինֆորմացիան դարձնել անհասկանալի կողմնակի անձանց համար:
2. Ամբողջականությունը (Integrity). պահպանման և փոխանցման ընթացքում ապահովել ինֆորմացիայի անփոփոխելիությունը:
3. Անժխտողականությունը (Non-repudiation). ինֆորմացիան ստեղծողը/ուղարկողը չպետք է կարողանա ժխտել, որ ինֆորմացիան ստեղծվել և ուղարկվել է իր կողմից:
4. Նույնականացումը (Authentication). ինֆորմացիան ուղարկողը և ստացողը պետք է կարողանան հաստատել միմյանց ինքնությունը:

Բանալիի կիրառմամբ ծածկագրաբանությունը լինում է սիմետրիկ և ասիմետրիկ: Սիմետրիկ ծածկագրաբանության համակարգերը, կամ որ նույնն է գաղտնի բանալիով ծածկագրական համակարգերը տվյալների ծածկագրման (encryption) և վերծանման (decryption) համար օգտագործում են միևնույն բանալին: Իսկ ասիմետրիկ ծածկագրաբանության համակարգերը, որոնք առավել հայտնի են որպես բաց բանալիով (public-key) ծածկագրական համակարգեր անվանումով, օգտագործում են երկու տարբեր բանալիներ. տվյալների ծածկագրման համար օգտագործվող բանալին դրվում է բացեիբաց, իսկ վերծանման համար օգտագործվող բանալին պահվում է գաղտնի: Գաղտնի բանալիով ծածկագրական համակարգերը ի տարբերություն բաց բանալիով ծածկագրական համակարգերի ավելի արագագործ են (մոտ 1000 անգամ[1]) և պահանջում են ավելի փոքր ծավալի հիշողություն: Սակայն առաջին դեպքում առաջանում է գաղտնի բանալիի փոխանցման խնդիր, որը մասնավորապես լուծվում է բաց բանալիով ծածկագրաբանության միջոցով:

Սիմետրիկ ծածկագրաբանության ալգորիթմները օգտագործում են գաղտնիություն ապահովելու համար, տվյալների ամբողջականության պահպանման մեխանիզմներում, նույնականացում ապահովող համակարգերում և թվային ստորագրության (սիմետրիկ բանալիով) սխեմաներում: Բլոկային ծածկագրական համակարգերը սիմետրիկ բանալիով ծածկագրման ալգորիթմներ են, որոնք ինֆորմացիան տրոհում են ավելի փոքր (ֆիքսված) երկարության բայթերի հաջորդականությունների, որոնց անվանում են բլոկեր կամ բաց տեքստեր, և յուրաքանչյուր բլոկ ծածկագրում են առանձին: Մասնավորապես, իտերատիվ բլոկային ծածկագրական համակարգերում միևնույն

[1] https://technet.microsoft.com/en-us/library/cc962028.aspx

բլոկի վրա մի քանի անգամ կիրառվում է միևնույն ձևափոխությունը՝ գաղտնի բանալիից գեներացված ենթաբանալիների մասնակցությամբ: Իտերացիային (ձևափոխությանը) անվանում են ռաունդ:

Իտերատիվ բլոկային ծածկագրական համակարգերի SAFER ("Secure And Fast Encryption Routine"-«Անվտանգ և արագ ծածկագրման ընթացակարգ») ընտանիքը ստեղծվել է պրոֆեսոր Ջեյմս Մեսիի կողմից: Այս ընտանիքի տարբեր բլոկային ծածկագրական համակարգեր ստեղծվել են տարբեր ժամանակահատվածներում: SAFER ընտանիքի 128 բիթ երկարության բլոկի ծածկագրման SAFER+ համակարգը Մեսին ստեղծել է ակադեմիկոս Գուրգեն Խաչատրյանի և ֆ.մ.գ.թ. Մելսիկ Կյուրեղյանի հետ համատեղ՝ AES (Advanced Encryption Standard) մրցույթին ներկայացնելու նպատակով (1998թ.): Համակարգը հետագայում օգտագործվել է BLUTOOTH ստանդարտի "Message authentication codes called E1" և "Key derivation called E21 and E22" սխեմաներում:

Գոյություն ունեցող ծածկագրական հարձակումների (cryptographic attacks) բազմաթիվ տեսակներից իտերատիվ բլոկային ծածկագրական համակարգերի, այդ թվում նաև SAFER ընտանիքի իտերատիվ բլոկային ծածկագրական համակարգերի նկատմամբ արդյունավետ են դիֆերենցիալ և գծային վերլուծությունները (cryptanalysis):

Ատենախոսության նպատակն է.

- Հետազոտել բլոկային ծածկագրական համակարգերի SAFER ընտանիքը և մշակել.
  - 128 բիթ երկարության բլոկի ծածկագրման արագ իրագործման ալգորիթմ՝ բանալիի երեք հնարավոր երկարություններով. 128, 192 և 256 բիթ:
  - 256 բիթային ծածկագրական համակարգ՝ արագ և արդյունավետ ծածկագրման համար:
- Ուսումնասիրել նոր մշակված համակարգերի կրիպտոկայունությունը՝ բայթային բոլոր տեղադրությունների դեպքում:

Հետազոտման օբյեկտը հանդիսանում է բլոկային ծածկագրական համակարգերի SAFER ընտանիքը և նրա նկատմամբ արդյունավետ հարձակում-ծածկավերլուծությունները:

Հետազոտման մեթոդները: Աշխատանքում օգտագործված են SAFER ընտանիքի իտերատիվ բլոկային ծածկագրական համակարգերի մշակման, նրանց նկատմամբ դիֆերենցիալ և գծային ծածկավերլուծությունների մեթոդները:

Արդյունքների գիտական նորույթը.

- SAFER ընտանիքի 128 բիթային ծածկագրական համակարգը, որը 32 բիթ պրոցեսորի վրա ապահովում է մոտավորապես 1,7 անգամ ավելի մեծ արագագործություն, քան SAFER+ համակարգը:
- SAFER ընտանիքի 256 բիթային ծածկագրական համակարգը, որը շնորհիվ կրիպտոկայունության բարձր մակարդակի (ռաունդների փոքր թվի) 256 բիթ երկարության բլոկը ծածկագրում է 1,5 անգամ ավելի արագ, քան 128 բիթային

SAFER+ համակարգը: Նշենք, որ գոյություն ունեցող բլոկային ծածկագական համակարգերի ծածկագրման բլոկի առավելագույն երկարությունը 128 բիթ է:

Արդյունքների կիրառական նշանակությունը: Ստացված արդյունքները կարելի է կիրառել ծածկագրաբանության մեջ: Իսկ դիֆերենցիալ վերլուծություն կատարող C++ լեզվով ստեղծված ծրագրային փաթեթը կարելի է օգտագործել SAFER ընտանիքի նոր համակարգերի մշակման համար:

Պաշտպանության ներկայացվում են հետևյալ դրույթները.

- 128 բիթային SAFER+ բլոկային ծածկագրական համակարգի հիման վրա մշակված, նույն կրիպտոկայունությամբ, սակայն 32 բիթ պրոցեսորի վրա 1,7 անգամ արագագործ 128 բիթ երկարության բլոկի ծածկագրման ալգորիթմ (*ձևափոխած SAFER+*):
- SAFER ընտանիքի բլոկային ծածկագրական համակարգերի հիման վրա մշակված, 256 բիթ երկարության բանալիի կիրառմամբ, 256 բիթ երկարությամբ բլոկի ծածկագրման ալգորիթմ. *SAFER-256*: SAFER+ համակարգի արագագործությունը մոտավորապես 0,7 անգամ մեծ է SAFER-256 համակարգի արագագործությունից, այն դեպքում, երբ առաջին համակարգի բլոկի երկարությունը 2 անգամ փոքր է երկրորդ համակարգի բլոկի երկարությունից (256 բիթ երկարության բանալիի դեպքում):

Աշխատանքի արդյունքների հավաստիությունը հիմնավորվում է մշակված ծրագրային համակարգերի կիրառմամբ ստացված մի շարք փորձնական արդյունքներով:

Աշխատանքի արդյունքների ներդրվել է Երևանի կապի միջոցների գիտահետազոտական ինստիտուտում, այն է ատենախոսության շրջանակներում մշակված 128 բիթային և 256 բիթային բլոկային ծածկագրական համակարգերը օգտագործվել են *Ավտոմատ Հեռախոսային Համակարգի* մեջ:

Աշխատանքի ապրոբացիան: Ատենախոսության արդյունքները զեկուցվել են ՀՀ ԳԱԱ ԻԱՊԻ-ի ընդհանուր սեմինարներում ու կոդավորման և ազդանշանների մշակման լաբորատորիայի մասնագիտական սեմինարներում, հայկական մաթեմատիկական միության 2014թ. տարեկան նստաշրջանում (AMUAS-2014), վեբ-անվտանգության նվիրված կոնֆերանսում (ARMSec-2016):

Հրատարակությունները: Ատենախոսության թեմայով հրատարակվել է 6 գիտական աշխատություն, որոնց ցանկը բերված է սեղմագրի վերջում:

Ատենախոսության կառուցվածքը և ծավալը: Աշխատանքը բաղկացած է բովանդակության ցանկից, ներածությունից, երեք գլխից, եզրակացությունից, օգտագործված գրականության ցանկից, 7 աղյուսակից և 16 նկարից: Աշխատանքի ծավալը կազմում է 113 էջ, օգտագործված գրականության ցանկը պարունակում է 34 անվանում:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածությունում հիմնավորված է թեմայի արդիականությունը, հետազոտության հիմնական նպատակները, ձևակերպված են ուսումնասիրման օբյեկտն ու հիմնադրույթները, հետազոտությունների գիտական նորույթները և ստացված արդյունքների ներդրումը և կիրառական նշանակությունը:

Առաջին գլխում ներկայացված են, ատենախոսության շրջանակներում մշակված SAFER ընտանիքի 128 և 256 բիթային բլոկային ծածկագրական համակարգերը, նրանցում դիֆուզիայի օպտիմալությունը՝ կախված բայթային տեղադրությունից: **1.1** պարագրաֆը ունի ներածական բնույթ, որում հակիրճ ներկայացված է բլոկային ծածկագրական համակարգերի SAFER ընտանիքը: **1.2** պարագրաֆում նկարագրված ու սխեմատիկորեն բերված է արդեն հայտնի SAFER+ համակարգի ընդհանուր կառուցվածքը (տե՛ս Նկար 1), ծածկագրման (տե՛ս Նկար 2) և վերծանման ռաունդները, օգտագործողի կողմից ընտրված 128 և 256 բիթ երկարության բանալիներից ենթաբանալիների գեներացման ալգորիթմները: Ժամանակակից պրոցեսորների առանձնահատկությունները հնարավորություն են տալիս բարելավել համակարգի իրագործման արագությունը, մասնավորապես 32-բիթ ARM (Advanced RISC Machine) պրոցեսորները հնարավորություն են տալիս միաժամանակ **xor** անել 32 հաջորդական բիթեր (4 հաջորդական բայթեր), այսինքն մեծացնել համակարգի արագագործությունը գործողությունների կրճատման հաշվին: Պարագրաֆ **1.3**-ում ներկայացված է 128 բիթային նոր մշակված բլոկային ծածկագրական համակարգը: SAFER+ համակարգի բանալիների ներմուծման շերտերում բիթային գործողությունների (ինչպես երևում է նկար 1-ից և 2-ից բիթային **xor** գործողությունը նախատեսված է 1 կամ 2 հաջորդական բայթերի համար) վերադասավորումից հետո համակարգի տրամաբանական կառուցվածքը պահպանելու համար (տե՛ս Պարագրաֆ 1.4) կատարվել է ձևափոխություններ ցուցչային/լոգարիթմական ֆունկցիաների կիրառման ոչ գծային շերտում, իսկ համակարգի կրիպտոկայունությունը պահպանելու նպատակով դիֆերենցիալ վերլուծությամբ մշակվել է ձևափոխություններ համակարգի հակադարձելի գծային ձևափոխության շերտում: Ստորև բերված են SAFER+ ալգորիթմում կատարված ձևափոխությունները, որոնք նպաստում են համակարգի արագագործության բարելավմանը և պահպանում են նրա կրիպտոկայունությունը.

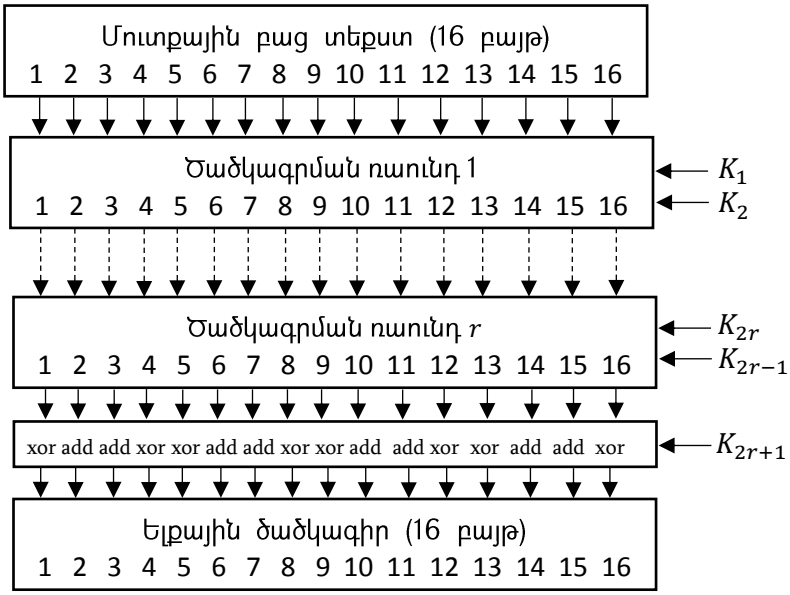
1. Առաջարկվել է **exp** ֆունկցիան 1, 4, 5, 8, 9, 12, 13, 16 բայթերի փոխարեն օգտագործել 1, 2, 3, 4, 9, 10, 11, 12 բայթերի համար, իսկ **log** ֆունկցիան 2, 3, 6, 7, 10, 11, 14, 15 բայթերի փոխարեն՝ 5, 6, 7, 8, 13, 14, 15, 16 բայթերի համար:
2. Առաջարկվել է համակարգում օգտագործվող բայթերի ինդեքսների [9, 12, 13, 16, 3, 2, 7, 6, 11, 10, 15, 14, 1, 8, 5, 4] տեղադրության (Armenian shuffle) փոխարեն օգտագործել [7, 12, 9, 14, 5, 8, 13, 10, 11, 4, 3, 6, 15, 2, 1, 16] տեղադրությունը, որը նույնպես անվանել ենք Armenian shuffle: Վերջինս ձևափոխված ալգորիթմում ապահովում է հնարավոր լավագույն դիֆուզիան:

3. Առաջարկվել է համակարգի գծային ձևափոխությունը սկսել ոչ թե անմիջապես 2-PHT ձևափոխությամբ, այլ [7, 12, 9, 14, 5, 8, 13, 10, 11, 4, 3, 6, 15, 2, 1, 16] բայթերի տեղադրությամբ, որին նորից անվանել ենք Armenian shuffle: 2-PHT (Pseudo-Hadamard Transform) հակադարձելի ձևափոխությունը կատարվում է $H = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ մատրիցի միջոցով. $(A_1, A_2) = (a_1, a_2) \cdot H = (2a_1 + a_2, a_1 + a_2)$, որտեղ թվաբանությունը ըստ մոդուլ 256-ի է, (A_1, A_2)-ը (a_1, a_2) մուտքային երկու հաջորդական բայթերի համապատասխան ելքերն են:

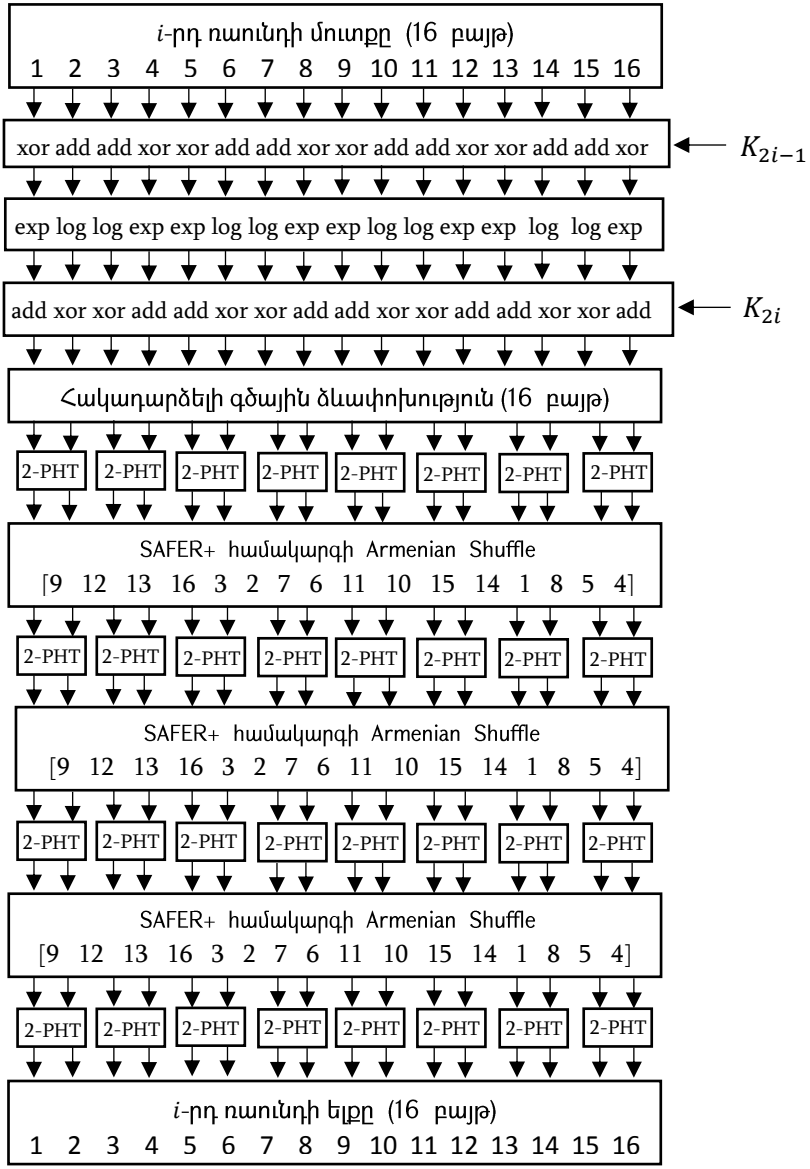
Արագացված SAFER+ համակարգը անվանել ենք ***ձևափոխած SAFER+***:

Ծածկագրից համապատասխան բաց տեքստի վերծանման ալգորիթմը կազմված է ծածկագրման ալգորիթմի ձևափոխությունների հակադարձ ձևափոխություններից: Ծածկագրման ալգորիթմում կիրառվող ենթաբանալիները վերծանման ալգորիթմում կիրառվում են հակառակ հերթականությամբ՝ ծածկագրման վերջին բանալին վերծանման պրոցեսում կիրառվում է առաջինը, նախավերջին բանալին երկրորդը և այսպես շարունակ:

Ձևափոխած SAFER+ համակարգը դիֆերենցիալ և գծային վերլուծությունների նկատմամբ ունի նույն կրիպտոկայունությունը ինչ SAFER+ համակարգը, սակայն 32-բիթ պրոցեսորի վրա 1.7 անգամ ավելի արագագործ է:

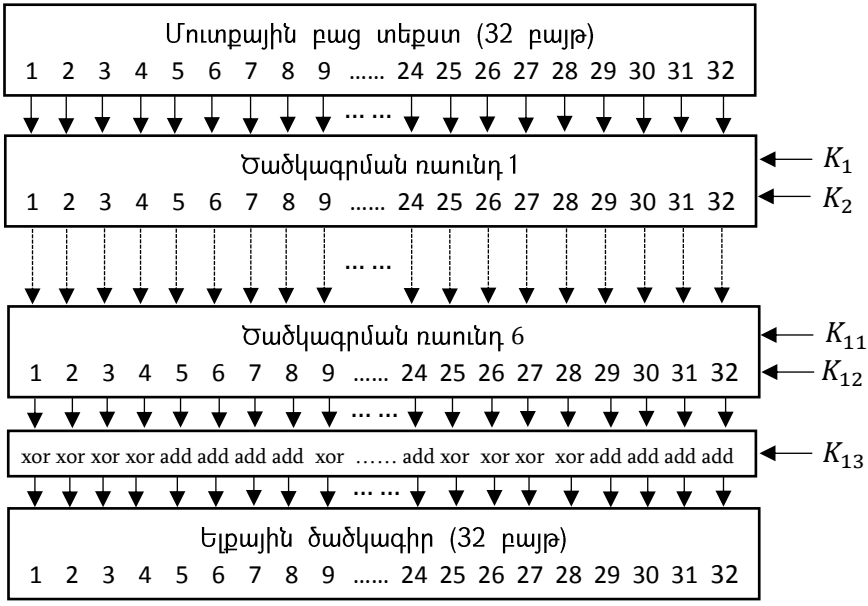


Նկար 1. SAFER+ համակարգի ծածկագրման ընդհանուր կառուցվածքը:

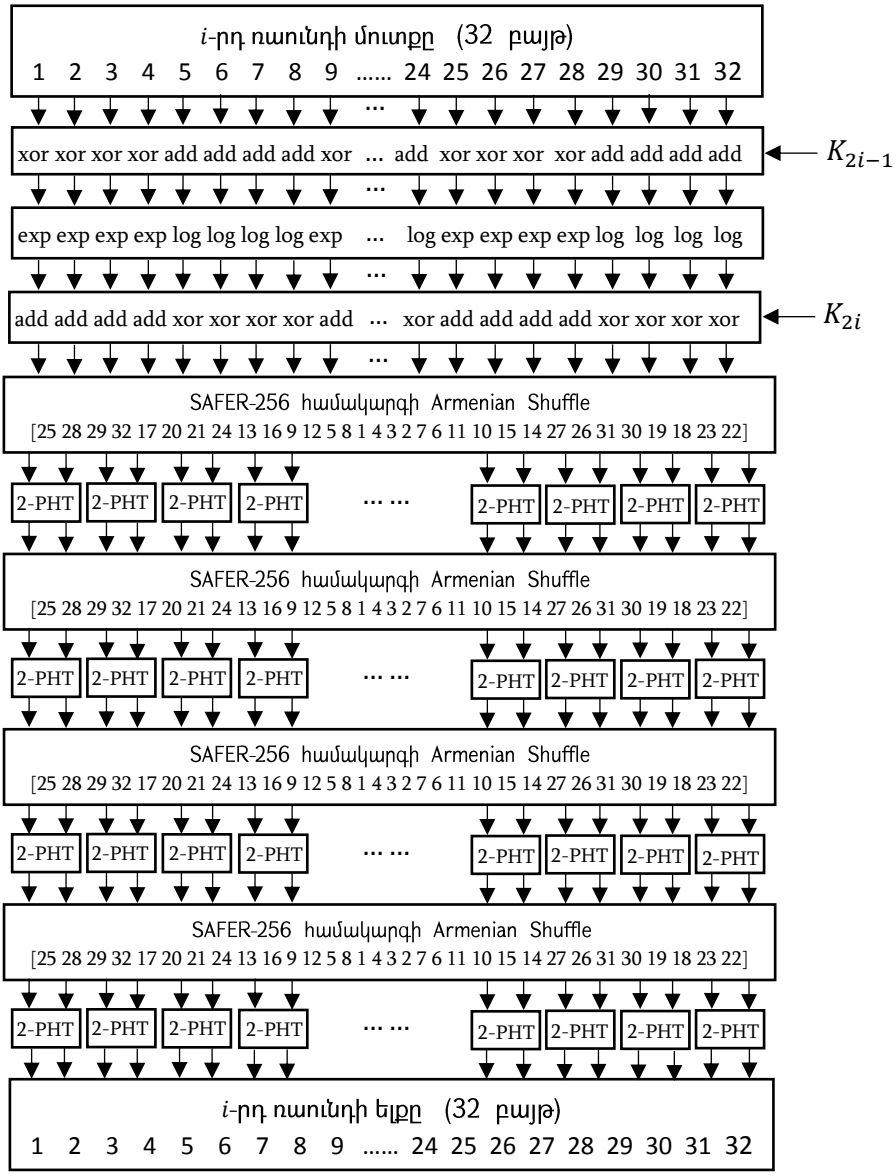


Նկար 2. SAFER+ համակարգի ծածկագրման ռաունդի կառուցվածքը:

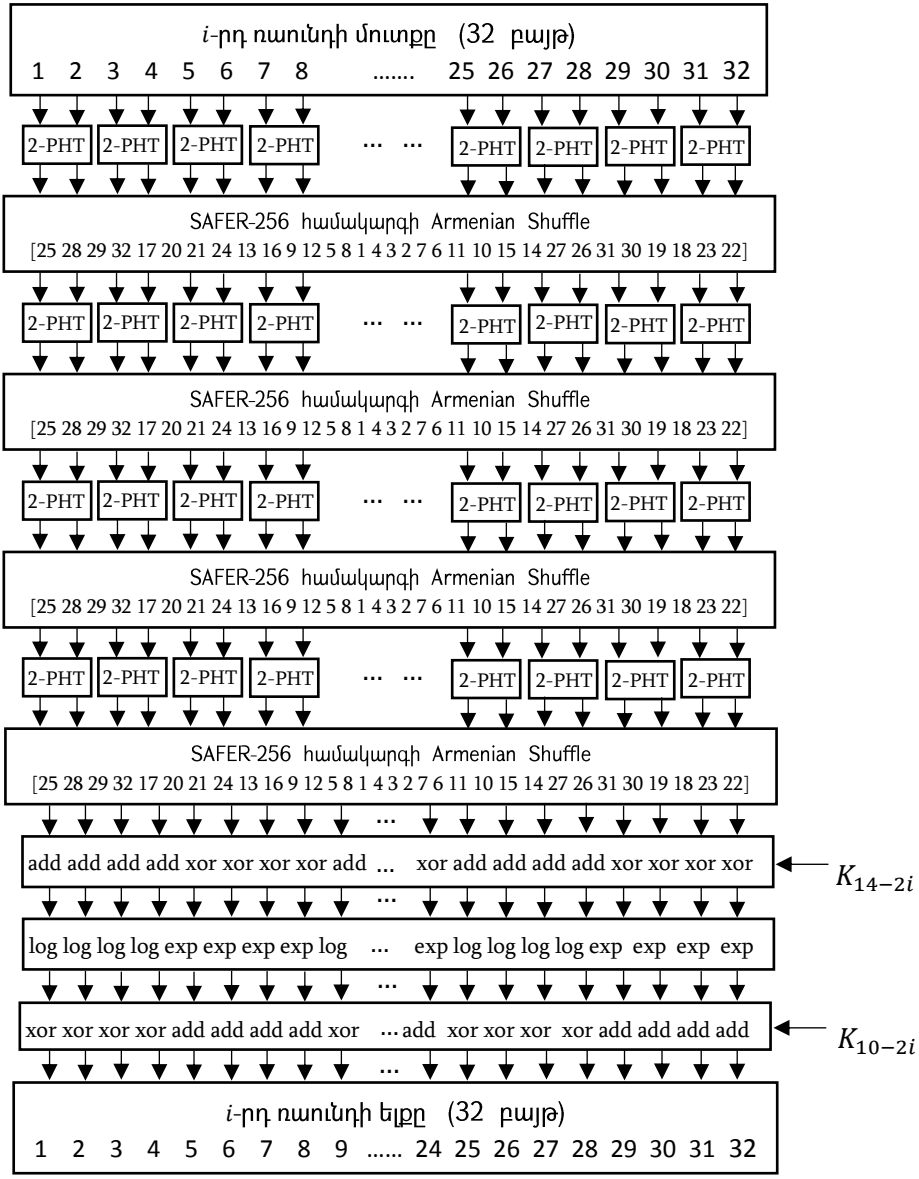
1.4 պարագրաֆում ներկայացված է 256 բիթ բլոկի և բանալու երկարության SAFER ընտանիքի նոր բլոկային ծածկագրական համակարգը (տե՛ս Նկար 3), որն անվանել ենք SAFER-256: 256 բիթային ծածկագրական համակարգ ստեղծելու գաղափարը, որի հիմքը դիֆերենցիալ վերլուծության նկատմամբ ձևափոխած SAFER+ համակարգի բարձր մակարդակի կայունությունն է (դիֆերենցիալ շղթաների անցումային հավանականությունների էական փոքր լինելը (տե՛ս Գլուխ 2)), հետապնդում է երկու նպատակ: Առաջինը այն է, որ գոյություն ունեցող և հայտնի բլոկային ծածկագրական համակարգերը ծածկագրում են առավելագույնը 128 բիթ, այսինքն 128-բիթային բլոկային ծածկագրական համակարգեր են և չնայած այդ համակարգերը ունեն նաև 256 բիթ երկարության օգտագործողի կողմից ընտրված բանալու դեպքը, նրանք իրականում չեն ապահովում 256 բիթ անվտանգություն 128 բիթ երկարության բլոկի համար՝ բախում հարձակման ժամանակ: (Բախում հարձակում (collision attack). գտնել երկու իրարից տարբեր $m_1 \neq m_2$ մուտքեր, այնպիսին, որ $\mathrm{hash}(m_1) = \mathrm{hash}(m_2)$): Իսկ երկրորդը այն է, որ ավելի արագ և արդյունավետ կատարել ինֆորմացիայի ծածկագրումը: SAFER-256 համակարգի ծածկագրման ու վերծանման ռաունդների նկարագրությունները և սխեմաները (տե՛ս Նկար 4, 5) բերված են համապատասխանաբար **1.4.1** և **1.4.2** ենթապարագրաֆներում: Վերծանման ռաունդը կազմված է ծածկագրման ռաունդի ձևափոխությունների հակադարձ ձևափոխություններից (տե՛ս Նկար 5): SAFER-256 համակարգի ենթաբանալիների գեներացման մեթոդը և սխեման ներկայացված են **1.4.3** ենթապարագրաֆում:



Նկար 3. SAFER-256 համակարգի ծածկագրման ընդհանուր կառուցվածքը:



Նկար 4. SAFER-256 համակարգի ծածկագրման ռաունդի կառուցվածքը:



Նկար 4. SAFER-256 համակարգի վերծանման ռաունդի կառուցվածքը:

1.5 պարագրաֆի ենթապարագրաֆներում ներկայացված են SAFER ընտանիքի բլոկային ծածկագրական համակարգերի, հետևաբար ձևափոխված SAFER+ և SAFER-256 համակարգերի տրամաբանական հիմնավորումները.

- Ծածկագրման ընթացակարգը
- Բայթային կողմնորոշվածությունը
- Խմբային գործողությունները ցիկլի սկզբում
- Երկու ադիտիվ խմբերի կիրառումը
- Աստիճանային և լոգարիթմական ֆունկցիաների կիրառումը ալգորիթմի ոչ գծային շերտերում
- Դիֆուզիան մատրիցի միջոցով
- Բանալիների հաջորդականության ընտրությունը
- Ցիկլերի քանակը

1.6 պարագրաֆում ներկայացված է դիֆուզիան SAFER+, ձևափոխած SAFER+ և SAFER-256 համակարգերում: Դիֆուզիան կհամարենք օպտիմալ, եթե բայթային տեղադրությունից կախված համակարգը կայուն է դիֆերենցիալ վերլուծության նկատմամբ մինիմալ թվով ռաունդներից հետո (կատարված հետազոտությունների համաձայն համակարգերը կրիպտոկայուն են նվազագույնը 5 ռաունդից հետո), այսինքն համակարգը առավելագույնս արագագործ է: Իսկ եթե համակարգը կայուն է 6 ռաունդից հետո, կհամարենք, որ տեղադրությունը համակարգում ապահովում է լավ դիֆուզիա:

Ծրագրային փաթեթի ու գծային և դիֆերենցիալ վերլուծությունների միջոցով կատարված ուսումնասիրությունները ցույց են տվել, որ SAFER+, ձևափոխած SAFER+ և SAFER-256 բլոկային ծածկագրական համակարգերից յուրաքանչյուրը ունեն իրենց էկվիվալենտ համակարգերը: Էկվիվալենտ այն իմաստով, որ համակարգերը միմյանցից տարբերվում են միայն բայթային տեղադրությամբ, որոնք ալգորիթմում ապահովում են միևնույն կրիպտոկայունությունը միևնույն թվով ռաունդներից հետո: Օրինակ. SAFER+, ձևափոխած SAFER+ համակարգերի դեպքում լավ կամ օպտիմալ դիֆուզիա ապահովող տեղադրությունների բազմությունը նույնն է և կազմված է 967.680 տեղադրությունից, ընդ որում SAFER+ համակարգում օպտիմալ դիֆուզիա ապահովող տեղադրությունը պարտադիր չի, որ ձևափոխած SAFER+_ում ապահովի օպտիմալ դիֆուզիա:

Նշենք, որ նշված համակարգերի բայթային տեղադրությունները (“Armenian shuffle”) համակարգերում օպտիմալ դիֆուզիա ապահովող տեղադրությունների բազմությունից են:

Երկրորդ և երրորդ գլուխներում ձևափոխված SAFER+ և SAFER-256 բլոկային ծածկագրական համակարգերի կրիպտոկայունության ուսումնասիրությունն է: Իտերատիվ բլոկային ծածկագրական համակարգերի, այդ թվում SAFER ընտանիքի համակարգերի համար ամենաարդյունավետ հայտնի հարձակումները դիֆերենցիալ և գծային վերլուծություններն են: Այս երկու ծածկավերլուծությունների նկատմամբ համակարգերի կրիպտոկայունությունը ուսումնասիրելու նպատակով ստեղծվել են ծրագրային փաթեթներ (C++ լեզվով):

Հակիրճ ներկայացնենք դիֆերենցիալ և գծային վերլուծությունների հիմնական գաղափարները և ընթացակարգը:

SAFER-256 մշակվել է ձևափոխված SAFER+ համակարգի հիման, նրանք ունեն միևնույն տրամաբանական հիմնավորումները և որոշ ընդհանուր կառուցվածքային առանձնահատկություններ: Համակարգերում առկա բլոկի բայթերի տեղադրության կամայական ընտրության դեպքում հնարավոր է համակարգը դիֆերենցիալ ու գծային վերլուծությունների նկատմամբ կրիպտոկայուն լինի մեծ թվով ռաունդներից հետո: Հետևաբար համակարգի համար դիֆերենցիալ ու գծային վերլուծությունների միջոցով ընտրվում է բայթերի այնպիսի տեղադրություն, որի դեպքում համակարգը կլինի կրիպտոկայուն մինիմալ թվով ռաունդներից հետո, հետևաբար մաքսիմալ արագագործ:

Ինչպես երևում է նկար 4-ից, SAFER-256 համակարգի ռաունդի սկզբում ռաունդի 32 բայթ երկարության մուտքային $X = [X_1, X_2, \dots, X_{32}]$ վեկտորին «գումարվում» է ռաունդի առաջին $K_1 = [K_{1,1}, K_{1,2}, \dots, K_{1,32}]$ ենթաբանալին՝ $X \otimes K_1$, որտեղ

$$\otimes = [\oplus, \oplus, \oplus, \oplus, +, +, +, +, \dots, \oplus, \oplus, \oplus, \oplus, +, +, +, +],$$

"$\oplus$" բիթային xor գործողությունն է, իսկ "$+$" ըստ մոդուլ 256-ի բայթային գումար գործողությունն է:

Դիցուք $S = [S_1, S_2, \dots, S_{32}]$ վեկտորը ռաունդի հակադարձելի գծային ձևափոխության մուտքն է: Ինչպես երևում է նկար 2-ից.

$$S_j = 45^{(X_j \oplus K_{1j})} + K_{2j}, \qquad j \in \{1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28\},$$

$$S_j = \log_{45}(X_j + K_{1j}) \oplus K_{2j}, \qquad j \in \{5,6,7,8,13,14,15,16,21,22,23,24,29,30,31,32\},$$

որտեղ $K_{1,j}$-ն և $K_{2,j}$-ն ռաունդի համապատասխանաբար առաջին և երկրորդ ենթաբանալիների բայթերն են: Ռաունդի ելքային $Y = [Y_1, Y_2, \dots, Y_{32}]$ վեկտորը կլինի $Y = S \cdot M$, որտեղ M-ը ձևափոխված SAFER+ համակարգի հակադարձելի գծային ձևափոխությունը արտահայտող մատրիցն է, այսինքն հակադարձելի ձևափոխության կիրառումը համարժեք է M մատրիցով բազմապատկմանը:

32 երկարության $V = [V_1, V_2, \dots, V_{32}]$ և $V' = [V'_1, V'_2, \dots, V'_{32}]$ բայթային վեկտորների ΔV տարբերություն կամ դիֆերենցիալ անվանում են.

$$\Delta V = V \oslash V' = [V_1 \oplus V'_1, V_2 \oplus V'_2, V_3 \oplus V'_3, V_4 \oplus V'_4, V_5 - V'_5, V_6 - V'_6, V_7 - V'_7, V_8 - V'_8, \dots, V_{25} \oplus V'_{25}, V_{26} \oplus V'_{26}, V_{27} \oplus V'_{27}, V_{28} \oplus V'_{28}, V_{29} - V'_{29}, V_{30} - V'_{30}, V_{31} - V'_{31}, V_{32} - V'_{32}],$$

իսկ V և V' վեկտորների $\widetilde{\Delta V}$ քվազի-տարբերություն կամ քվազի-դիֆերենցիալ՝

$$\widetilde{\Delta V} = V - V' = [V_1 - V'_1, V_2 - V'_2, V_3 - V'_3, V_4 - V'_4, V_5 - V'_5, V_6 - V'_6, V_7 - V'_7, V_8 - V'_8, \dots, V_{25} - V'_{25}, V_{26} - V'_{26}, V_{27} - V'_{27}, V_{28} - V'_{28}, V_{29} - V'_{29}, V_{30} - V'_{30}, V_{31} - V'_{31}, V_{32} - V'_{32}]:$$

Դիցուք $X(i)$-ն և $Y(i)$-ն SAFER-256 համակարգի i-րդ ռաունդի համապատասխանաբար ելքն ու մուտքն են: Դիֆերենցիալ վերլուծության ժամանակ, ինչպես միշտ, ենթադրվում է, որ ռաունդի ենթաբանալիները ընտրվում են իրարից անկախ և կամայականորեն

(SAFER-256 համակարգի ենթաբանալիները գեներացվում են գաղտնի բանալիից): Ենթադրենք ոչ զրոյական 32 երկարության բայթային (α, β) վեկտորները ձևափոխված SAFER+ համակարգի $(\Delta X(1), \Delta Y(i))$ i-ռաունդ դիֆերենցիալի արժեքներն են: Ցույց է տրված, որ ձևափոխված SAFER+ համակարգը մարկովյան համակարգ է[2], այսինքն $P(\Delta Y(i) = \beta | \Delta X(1) = \alpha,\ X(1) = \gamma)$ պայմանական հավանականությունը անկախ է γ-ից: Հետևաբար, $\Delta X(1), \Delta Y(1), \Delta Y(2), \dots, \Delta Y(i)$ հանդիսանում է մարկովյան շղթա: Ենթադրենք $(\alpha,\ \beta_1,\ \beta_2, \dots, \beta_{i-1},\ \beta)$ հաջորդականությունը, որին անվանում են i-ռաունդ բնութագրիչ, $\Delta X(1), \Delta Y(1), \Delta Y(2), \dots, \Delta Y(i)$ շղթայի արժեքներն են: i-ռաունդ դիֆերենցիալի $P(\Delta Y(i) = \beta | \Delta X(1) = \alpha)$ հավանականությունը հավասար կլինի i-ռաունդ $(\alpha, \beta_1, \beta_2, \dots, \beta_{i-1}, \beta)$ բնութագրիչի բոլոր $\beta_1, \beta_2, \dots, \beta_{i-1}$ հնարավոր արժեքների

$$P(\Delta Y(1) = \beta_1, \dots, \Delta Y(i-1) = \beta_{i-1}, \Delta Y(i) = \beta | \Delta X(1) = \alpha)$$

հավանականությունների գումարին:

Դիֆերենցիալ վերլուծությամբ հարձակումը r ռաունդից կազմված SAFER ընտանիքի համակարգի վրա հիմնված է հետևյալ հանգամանքի վրա, գտնել $(r-1)$-ռաունդ դիֆերենցիալ, որի հավանականությունը n բայթ բլոկի ($n = 128$ կամ 256) դեպքում էականորեն ավելի մեծ է $\frac{1}{2^n - 1} \approx 2^{-n}$ միջին հավանականությունից: Այսպիսով, որպեսզի r ռաունդից կազմված ծածկագրման համակարգը կայուն լինի դիֆերենցիալ վերլուծության նկատմամբ, պետք է գոյություն չունենա $(r-1)$-ռաունդ դիֆերենցիալ, որի հավանականությունը մեծ է կամ հավասար 2^n-ի:

SAFER ընտանիքի նոր ծածկագրական համակարգերի կրիպտոկայունությունը ուսումնասիրելու նպատակով ատենախոսության շրջանակներում յուրաքանչյուր համակարգի համար ստեղծվել է դիֆերենցիալ վերլուծություն կատարող ծրագրային փաթեթ C++ լեզվով:

Ձևափոխված SAFER+ համակարգի դիֆերենցիալ վերլուծությունը ցույց է տալիս, որ 5-ռաունդ դիֆերենցիալները էականորեն փոքր են 2^{-128}-ից (4-ռաունդ դիֆերենցիալներից ոչ բոլորն են փոքր 2^{-128}-ից): Հետևաբար, ձևափոխած SAFER+ համակարգը լիովին կայուն է դիֆերենցիալ վերլուծության նկատմամբ 6 ռաունդից հետո, այսինքն SAFER+ համակարգի կրիպտոկայունությունը պահպանվել է ձևափոխություններից հետո: Իսկ SAFER-256 համակարգը դիֆերենցիալ վերլուծության նկատմամբ լիովին կրիպտոկայուն է 6 ռաունդից հետո, քանի որ ուսումնասիրությունները ցույց են տվել, որ համակարգի 32 բայթ բլոկի համար նրա 5 և ավելի ռաունդ դիֆերենցիալները էականորեն փոքր են 2^{-256}-ից (այս պայմանը տեղի չունի 4-ռաունդ դիֆերենցիալների համար):

1993 թվականին Մաթսուին ներմուծեց գծային վերլուծության գաղափարը,որը իրենից ներկայացնում է հարձակում իտերատիվ ծածկագրական համակարգերի

[2] Massey J. L., "SAFER K-64: One Year Later", *Fast Software Encryption II* (Ed. B. Preneel) Lecture Notes in Computer Science, New York, Springer, No. 1008, pp. 212-241, 1995.

նկատմամբ և հատկապես առավել արդյունավետ է, երբ համակարգում գումար գործողության մոդուլը ավելի փոքր է:

Բինար ֆունկցիան կոչվում է *հավասարակշռված կամ բալանսավորված*, եթե արգումենտի հնարավոր բոլոր արժեքների կեսի դեպքում ընդունում է 0 արժեք, իսկ մյուս կեսի դեպքում՝ 1 արժեք: Իտերատիվ ծածկագրական համակարգի i-րդ ռաունդի $S^{(i)}$ I/O (Input/Output-մուտք/ելք) գումար անվանում են.

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

որտեղ $X^{(i)} = Y^{(i-1)}$ i-րդ ռաունդի մուտքն է, $Y^{(i)}$-ն i-րդ ռաունդի ելքը, իսկ f_i և g_i ֆունկցիաները բինար-բալանսավորված ֆունկցիաներ են:

f_i և g_i ֆունկցիաները կոչվում են $S^{(i)}$ I/O գումարի համապատասխանաբար մուտքային և ելքային ֆունկցիաներ: Ասում են, որ հաջորդական ռաունդների I/O գումարները *կապակցված են*, եթե այդ I/O գումարներից յուրաքանչյուրի ելքային ֆունցիան հանդիսանում է հաջորդ ռաունդի I/O գումարի մուտքային ֆունկցիան (այսինքն $g_i = f_{i+1}$), բացառությամբ վերջի I/O գումարի: Եթե $S^{(1)}, S^{(2)}, \dots, S^{(\rho)}$ I/O գումարները կապակցված են, ապա նրանց ըստ մոդուլ 2-ի գումարը ևս հանդիսանում է I/O գումար, որին անվանում են ρ-ռաունդ I/O գումար և նշանակում են այսպես

$$S^{(1\dots\rho)} := \bigoplus_{i=1}^{\rho} S^{(i)} = f_1\left(Y^{(1)}\right) \oplus g_\rho\left(Y^{(\rho)}\right),$$

որտեղ $Y^{(1)} = X^{(1)} = X$ առաջին ռաունդի մուտքն է, այսինքն բաց տեքստը, իսկ $Y^{(\rho)}$-ն վերջին ռաունդի ելքն է, այսինքն ծածկագիրը:

B^n-ով նշանակենք n երկարության բինար վեկտորների բազմությունը. $B^n = \{0, 1, 2, \dots, 2^n - 1\}$: $(B^n, \otimes)$ խմբից $(B, \oplus)$ խմբի մեջ հոմոմորֆ արտապատկերումը կամ հոմոմորֆիզմը կոչվում է $\otimes$ գործողության բինար հոմոմորֆիզմ (f արտապատկերումը հոմոմորֆիզմ է, եթե $f(U \otimes V) = f(U) \oplus f(V)$ ցանկացած $U, V \in B^n$ տարրերի համար և f-ը միարժեքորեն 0 չէ:): i-րդ ռաունդից j-րդ ռաունդ $(i \le j)$ անցման I/O գումարը հոմոմորֆ է, եթե մուտքի ֆունկցիան հանդիսանում է բինար հոմոմրֆիզմ $\otimes_i$ գործողության համար, իսկ ելքի ֆունկցիան բինար հոմոմրֆիզմ $\otimes_{j+1}$ գործողության համար: Եռակի գումարը հոմոմրֆ է, եթե հոմոմրֆ է նրա ծնող I/O գումարը:

Գծային վերլուծության մեջ օգտագործվում է պատահական բինար մեծության չբալանսավորվածության գաղափարը: $|2P[V = 0] - 1|$ իրական թվին անվանում են V պատահական բինար մեծության *չբալանսավորվածություն* և նշանակում են $I(V)$-ով: $P[V = 0]$ հավանականություն է այն բանի որ V-ն կընդունի 0 արժեք: Գծային վերլուծության նպատակն է ρ ռաունդից կազմված իտերատիվ համակարգի համար գտնել մեծ չբալանսավորվածությամբ հոմոմորֆ $(\rho - 1)$-ռաունդ I/O գումար:

Ցույց է տրվել, որ արդյունավետ հոմոմորֆ I/O գումար գտնելու միակ արդյունավետ Հերպեսի մեթոդը չի կարող գտնել ոչ-զրոյական չբալանսավորվածությամբ հոմոմորֆ I/O գումար 2-ռաունդ ձևափոխված SAFER+ և SAFER-256 համակարգերի համար:

Ատենախոսության հիմնական արդյունքները

- SAFER ընտանիքի 128-բիթային SAFER+ բլոկային ծածկագրական համակարգի հիման վրա մշակվել է ավելի մեծ արագագործությամբ 128 բիթային բլոկային ծածկագրական համակարգ. ձևափոխած SAFER+: Մշակվել է SAFER+ համակարգի այնպիսի ձևափոխություններ, որոնք մեծացրել են համակարգի արագագործությունը ARM պլատֆորմի 32-բիթ պրոցեսորի վրա մոտավորապես 1,7 անգամ՝ չդարձնելով համակարգի կրիպտոկայունությունը խոցելի դիֆերենցիալ և գծային վերլուծությունների նկատմամբ [1],[2]:

- SAFER ընտանիքի բլոկային ծածկագրական համակարգերի, մասնավորապես ատենախոսության շրջանակներում մշակված ձևափոխած SAFER+ համակարգի հիման վրա մշակվել է 256 բիթ երկարության բլոկի ծածկագրման ալգորիթմ՝ հաշվի առնելով դիֆերենցիալ վերլուծության նկատմամբ ձևափոխած SAFER+ համակարգի կայունության բարձր մակարդակը: Նոր համակարգը անվանել ենք SAFER-256: Այն դիֆերենցիալ վերլուծության նկատմամբ կայուն է նվազագույնը 5 ռաունդի դեպքում (SAFER+ ալգորիթմի հիման վրա մշակված 256-բիթային համակարգերը դիֆերենցիալ վերլուծության նկատմամբ կրիտոկայուն են նվազագույնը 6 ռաունդից հետո), իսկ գծային վերլուծության նկատմամբ 3 ռաունդից հետո: SAFER-256 ապահովում է 256 բիթ անվտանգություն բախում հարձակման նկատմամբ և շնորհիվ դիֆերենցիալ վերլուծութան նկատմամբ բարձր կայունության և ռաունդների փոքր թվի ($r = 6$) 1,5 անգամ ավելի արագ է, քան SAFER+ համակարգը՝ օգտագործողի կողմից ընտրված 256 բիթ երկարության բանալիի դեպքում (երբ ինֆորմացիայի երկարությունը 256 բիթ է) [3],[4]:

- SAFER ընտանիքի SAFER+, ձևափոխած SAFER+ և SAFER-256 բլոկային ծածկագրական համակարգերից յուրաքանչյուրը առանձին առանձին ունեն իրենց համարժեք ծածկագրական համակարգերը՝ կրիպտոկայունության և արագագործության իմաստով: Համարժեք համակարգերը նշված ծածկագրական համակարգից տարբերվում են միայն բայթային տեղադրությամբ, այսինք փոխելով համակարգի Armenian Shuffle բայթային տեղադրությունը կստանանք միևնույն կրիպտոկայունությամբ, միևնույն արագագործությամբ նոր բլոկային ծածկագրական համակարգ [5],[6]:

Հրատարակված աշխատությունների ցանկը

[1] Kyuregyan K.: Some modifications of SAFER+. In Reports of NAS RA, Armenia, Yerevan, 2015, Vol. 115, No. 1, pp. 33-39.

[2] Kyuregyan K. M.: Linear Cryptanalysis of 128-bit Modified SAFER+. Transactions of IIAP NAS RA, Mathematical Problems of Computer Science Vol. 45, pp.127-137, 2016.

[3] Khachatrian G. H., Kyureghyan M. K., Kyuregyan K. M.: Design and Cryptanalysis of a New Encryption Algorithm SAFER-256. Transactions of IIAP NAS RA, Mathematical Problems of Computer Science Vol. 42, pp. 97-106, 2014.

[4] Kyureghyan M. K., Kyuregyan K. M.: Linear Cryptanalysis of SAFER-256. Transactions of IIAP NAS RA, Mathematical Problems of Computer Science. Vol. 45, pp. 111-121, 2016.

[5] Kyuregyan K. M.: On Optimality of Regular SAFER+ and Modified SAFER+ Diffusion. Transactions of IIAP NAS RA, Mathematical Problems of Computer Science Vol. 44, pp. 109-115, 2015.

[6] Kyuregyan K. M.: On Optimality of SAFER-256 Diffusion. Transactions of IIAP NAS RA, Mathematical Problems of Computer Science Vol. 44, pp. 133-137, 2015.

Кнарик Кюрегян

Разработка и реализация 256 битной криптографической системы семьи SAFER

Быстрое и непрерывное развитие области информационных технологий (ИТ) приводят к уязвимости некоторых криптографических систем и, следовательно, информационная безопасность становится под угрозой. Появляется необходимость разработки новых, более безопасных и быстрых систем, требующих малого объема памяти.

Основные принципи современной криптографии являются:

1. Секретность: сделать информацию непонятной для посторонних.
2. Целостность: обеспечить неизменность информации во время хранения и передачи.
3. Неотрицаемость: невозможность отрицания создателем/отправителем, что именно он создал и передал информацию.
4. Идентичность: способность отправителя и получателя информации потвердить личность друг друга.

Алгоритмы шифрования подразделяются на две категории: симметричные шифры и асимметричные шифры (шифры с открытым ключом). Асимметричные шифры используют два различных ключа: ключ для шифрования данных, ставится открыто, а ключ для разшифрования держится в секрете. Симметричные шифры в отличие от шифров с открытым ключом быстрее (примерно в 1000 раз) и требуют меньшего объема памяти. Однако, во втором случае, возникает проблема передачи секретного ключа, которая решается с помощью шифрования с открытым ключом.

Алгоритмы блочных шифров симметричного шифрования используют для обеспечения секретности (например TLS (безопасность транспортного уровня) и IPSec протоколы), применяют в механизмах сохранения целостности данных, в системах распознавания идентичности и в схемах электронной подписи с симметричным ключом.

Блочные шифрые делят информацию на последовательности фиксированной длины байтов (последние называют блоками или открытыми текстами) и отображают на последовательности той же длины байтов. В частности, итерративные блочные шифры несколько раз применяют к блоке одно и тоже преобразование с участием ключей. Преобразование называется раунд-функцией, а повторения - раундами.

Семейство симметричных блочных шифров SAFER было создано профессором Д. Месси. Шифр SAFER+ с длиной блока 128 бит семейства SAFER был разработан совместно Г. Хачатряном и М. Кюрегяном с целью представления на конкурсе AES (1998 г.). В дальнейшем, система использовалась в схеме распознавания идентичности стандарта BLUTOOTH и в схеме генерации ключа.

Из множества разновидностей существующих криптографических атак по отношению к итеративным блочным шифрам, в том числе и к шифрам семейства SAFER, эфективны дифференциальный и линейный криптоанализы.

Цель диссертации

- Исследовать симметричные блочные шифры семейства SAFER и разработать:

- такие преобразования системы SAFER+ с длиной блока 128 бит и ключом длиной 128, 192 или 256 бит, которые не нанесут вреда криптостойкости системы и содействуют её быстродействию.
- 256-битовый криптографический шифр, с учетом уровня криптостойкости систем SAFER+ и преобразованного SAFER+ по отношению к дифференциальному криптоанализу, который определяет эффективность шифра.

- С помощью программных пакетов исследовать какие байтовые перестановки в разработаных системах обеспечивают криптостойкость после минимально возможное количества раундов.

Научная новизна результатов

- Разработан новый 128-битовой блочный шифр, названый модифицированная SAFER+. Модифицированная SAFER+ имея ту же криптоустойчивость, что и система SAFER+, в 1,7 раз быстрее на 32-битовом ARM процессоре.
- Разработан новый блочный шифр семейства SAFER с длиной блока и ключа 256 бит, названый SAFER-256. В случае ключа длиной 256 бит, быстродействие шифра SAFER+ в 0,7 раз выше системы SAFER-256, в том случае, когда длина блока второой системы в 2 раза больше длины блока первой системы. Отметим, что наибольшая длина блока существующих блочных шифров 128 бит.

Основные результаты диссертации

- На основе 128-битового блочного шифра SAFER+ семейства SAFER разработана новая система с длиной блока 128 бит. Разработаны такие изменения системы SAFER+, которые повысили быстродействие системы в 1,7 раз на 32-битовом процессоре платформы ARM, не делая криптостойкость системы уязвимой по отношению к дифференциальному и линейному криптоанализу [1,2].
- На основе блочных шифров семейства SAFER, в частности шифра модифицированной SAFER+, с учетом высокого уровня криптостойкости по отношению к дифференциальному разработан 256-битовый блочный шифр. Новую систему мы назвали SAFER-256. Она имеет стойкость по отношению к дифференциальному криптоанализу в случае как минимум 5-и раундов (разработаные на основе алгоритма SAFER+ 256-битовые системы устойчивы по отношению к дифференциальному криптоанализу, как минимум, после 6 раундов), а по отношению к линейному криптоанализу после 3-х раундов. SAFER-256 по отношению к коллизионной атаки обеспечивает 256 бит безопасности, и в 1,5 раза быстрее, чем SAFER+, когда длина информации 256 бит [3, 4].
- Каждый из блочных шифров SAFER+, модифицированный SAFER+ и SAFER-256 семейства SAFER имеют свои эквивалентные блочные шифры, в смысле криптостойкости и быстродействия. Эквивалентные шифры отличаются только байтовыми перестановками, то есть изменив байтовую перестановку Armenian Shuffle, мы получим новую систему с той же криптостойкостью и с тем же быстродействием [5, 6].

Knarik Kyuregyan

Development and implementation of a 256-bit cryptosystem of SAFER family

The rapid and continous development of information technology (IT) lead to increasing vulnerability of cryptography-based security technologies and information protection appeared under threat. A necessity to develop more secure, fast implemented cryptosystems with a small amount of memory emerges.

Modern cryptography concerns with the following four objectives:

1. Privacy/Confidentiality (the information cannot be understood by anyone for whom it is unintended)
2. Integrity (the information cannot be altered in storage or transited between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Encryption algorithms are primarily classified into two categories: symmetric key and asymmetric key encryption. Symmetric-key algorithms are the classical approach for secure communication. For example, the Transport Layer Security (TLS) and Internet Protocol security (IPSec) protocols use symmetric encryption algorithms to encrypt and decrypt confidential communications between parties. They also are commonly used by technologies that provide bulk encryption of persistent data, such as e-mail messages and document files. For example, Secure/Multipurpose Internet Mail Extensions (S/MIME) uses symmetric keys to encrypt messages for confidential mail, and Encrypting File System (EFS) uses symmetric keys to encrypt files for confidentiality. Symmetric-key ciphers may furthermore serve as a central component in message authentication techniques, data integrity mechanisms, entity authentication protocols, and (symmetric-key) digital signature schemes. But they have a big drawback in that communication partners have to share the same secret key, thus, the problem of key distribution arises. The asymmetric principle solves the key distribution problem in an elegant way by using two different keys, a public and a private one. Encryption and verifying involve a public key that is available to everyone. The private key is used for decryption and signing. However, asymmetric (public key) algorithms are computationally much more expensive than symmetric algorithms (about 1000 times), which is viewed by many as a big knockout criteria for applications such as embedded systems with limited processor power and a small sized memory. Symmetric algorithm's secret key transmission problem is solved by public key cryptography.

Block cipher algorithms work by breaking up the message into smaller blocks and mapping each block to the block with the same length. Iterative block ciphers are block ciphers that work by performing the same transformation over the same blocks. The transformation is called round function and iterations are called rounds.

SAFER is a block cipher family designed by Prof. James Massey. SAFER+ is 128 bit block size encryption algorithm proposed together with Prof. G. Khachatrian and Dr. M. Kyuregian. It was submitted as candidate for Advansed Encryption Standart (AES) and was subsequently adopted

for use in the challenge/response entity authentication scheme in the Bluetooth protocol for wireless communications.

The most effective general attacks against iterative block ciphers, including the previous SAFER family of ciphers are differential and linear cryptanalysis.

The aim of thesis

- Based on symmetric key block ciphers of SAFER family develop:
  - 128-bit block size fast implementing block cipher. Particularly develop such modifications of 128 bit block size cipher SAFER+ that improve system processing speed and doesn't turn system security.
  - 256-bit cryptosystem considering security levels of modified and regular SAFER+ against differential cryptanalysis.
- Consider what kind of byte permutations provide optimal diffusion against block cipher's effective cryptographic attacks after a possible minimum number of rounds in developed block ciphers using software packages created for performing differential cryptanalysis.

Scientific novelty

- A new fast implemented 128 bit block size block cipher named modified SAFER+. This new cipher has the same security level compared with regular SAFER+ and is 1,7 times faster on ARM 32-bit platform.
- 256-bit block and key size block cipher of SAFER family named SAFER-256. 256-bit cipher SAFER-256 processing speed is at least 0,7 times slower compared with 128-bit SAFER+. It should be noted that there do not exist block ciphers with a 256 bit block size yet.

The main results of the thesis

- Based on 128 bit block size cipher SAFER+ of SAFER family new fast implementing 128 bit block size cipher was developed. Particularly some modifications of 128-bit block cipher SAFER+ are developed, which make the algorithm implementation 1.7 times faster on ARM 32-bit platform and do not turn system vulnerable against differential cryptanalysis [1],[2]:
- Based on new developed 128-bit block cipher high security level against differential cryptanalysis a new 256 bit size block cipher of SAFER family was developed. The New cipher we have called SAFER-256, because of its block and key lengths. SAFER-256 is secure against differential cryptanalysis after minimum 5 rounds (SAFER+ construction based 256-bit block cipher is secure against differential cryptanalysis after minimum 6 rounds) and against linear cryptanalysis after minimum 3 rounds. SAFER-256 provides 256-bit security against collision attack and encrypts 256 bit information 1,5 times faster than SAFER+ (key length is 256 bit), because of resistance against differential cryptanalysis after small number of rounds [3],[4]:
- SAFER+, modified SAFER+ and SAFER-256 block ciphers of SAFER family have equivalent block ciphers, in sense of processing speed and same security. Equivalent block ciphers differ from each other only by byte permutations [5],[6]