ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Սողոյան Արմեն Վահանի

ՀԱՇՎՈՂԱԿԱՆ ԽՄԲԵՐԻ ՏԵՍՈՒԹՅԱՆ ՄԵԹՈԴՆԵՐԻ ԿԻՐԱՌՈՒՄԸ ԾԱԾԿԱԳՐՄԱՆ ՄԵՋ

Ա.01.09 «Մաթեմատիկական կիբեռնետիկա եւ մաթեմատիկական տրամաբանություն» մասնագիտությամբ ֆիզիկա-մաթեմատիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երեւան – 2013

ЕРЕВАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Согоян Армен Ваганович

ПРИМЕНЕНИЕ МЕТОДОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕОРИИ ГРУПП В КРИПТОГРАФИИ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата физико-математических наук по специальности
01.01.09 “Математическая кибернетика и математическая логика ”

Ереван-2013

Ատենախոսության թեման հաստատվել է Երեւանի պետական համալսարանում

Գիտական ղեկավար՝ ֆիզ.մաթ.գիտ. դոկտոր Ա.Ա.Ալեքսանյան
Պաշտոնական ընդդիմախոսներ՝ ֆիզ.մաթ.գիտ. դոկտոր Լ.Հ.Ասլանյան
ֆիզ.մաթ.գիտ. թեկնածու Ա.Շ.Մալխասյան
Առաջատար կազմակերպություն՝ ՀՀ ԳԱԱ Ինֆորմատիկայի եւ ավտոմատացման պրոբլեմների ինստիտուտ

Պաշտպանությունը կայանալու է 2013 թ. դեկտեմբերի 6-ին, ժ. 14:30-ին ԵՊՀ-ում գործող ԲՈՀ-ի 044 «Մաթեմատիկական կիբեռնետիկա» մասնագիտական խորհրդի նիստում հետեւյալ հասցեով՝ 0025, Երեւան, Ալ. Մանուկյան 1:

Ատենախոսությանը կարելի է ծանոթանալ ԵՊՀ-ի գրադարանում:

Սեղմագիրն առաքված է 2013 թ. նոյեմբերի 5-ին:

Մասնագիտական խորհրդի
գիտական քարտուղար,
ֆիզ.մաթ.գիտ. դոկտոր Վ.Ժ.Դումանյան

Тема диссертации утверждена в Ереванском государственном университете

Научный руководитель: доктор физ.-мат.наук А.А.Алексанян
Официальные оппоненты: доктор физ.-мат.наук Л.А.Асланян
кандидат физ.-мат.наук А.Ш.Малхасян
Ведущая организация: Институт проблем информатики и автоматизации НАН РА

Защита состоится 6-го декабря 2013 г. в 14:30 часов на заседании действующего в Ереванском государственном университете специализированного совета ВАК 044 “Математическая кибернетика”, по адресу: Ереван 0025, ул. А.Манукяна, 1.

С диссертацией можно ознакомиться в библиотеке Ереванского государственного университета.

Автореферат разослан 5-го ноября 2013 г.

Ученый секретарь специализированного совета,
доктор физ.-мат.наук В.Ж.Думанян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը: Ատենախոսությունում առաջարկված են գաղտնի բանալիով (սիմետրիկ) եւ բաց բանալիով (ասիմետրիկ) ծածկագրման նոր սխեմաներ, որոնք հիմնված են հաշվողական խմբերի տեսության հիմնարար եւ կարեւորագույն Սիմսի (Շրայեր-Սիմսի) ալգորիթմի եւ տեղադրությունների խմբի "ուժեղ" ծնիչների բազմության գաղափարի օգտագործման վրա: Տեղադրությունների խմբի "ուժեղ" ծնիչների բազմությունը թույլ է տալիս միարժեքորեն ներկայացնել խմբի տարրերը ծնիչների բազմության տարրերի արտադրյալների միջոցով եւ հնարավորություն է տալիս էֆեկտիվ եղանակով թվարկել եւ առանց կրկնողությունների գեներացնել խմբի տեղադրությունները: Այն նաեւ թույլ է տալիս էֆեկտիվորեն լուծել մի շարք կարեւոր խնդիրներ այնպիսին ինչպես տրված խմբին տրված տեղադրության պատկանելիության հարցը, տեղադրությունների տրված բազմության տարրերի արտադրյալի միջոցով տրված տեղադրության ներկայացման հնարավորության հարցը, ենթախմբի նորմալ լինելը եւ այլն: Սիմսի ալգորիթմը բազմանդամային ժամանակում կառուցում է տեղադրությունների խմբի "ուժեղ" ծնիչների բազմությունն ելնելով խմբի որեւէ ծնիչների բազմությունից:

XX դարի կեսին հաշվողական տեխնիկայի հայտնագործությունը եւ դրա կիրառումն ինֆորմացիայի կոդավորման եւ ծածկագրման համակարգերի ստեղծման գործում, ինչպես նաեւ դիսկրետ մաթեմատիկայի բուռն զարգացումը եւ կարեւորագույն արդյունքների ստացումը հանգեցրեցին այն բանին, որ մաթեմատիկայի այնպիսի զուտ տեսական համարվող ճյուղերը ինչպես թվերի տեսությունը կամ խմբերի տեսությունը հանկարծակի դարձան կարեւորագույն գործիք ինֆորմացիայի մշակման համակարգերի ստեղծման բնագավառում: Ներկայումս ալգորիթմական թվերի տեսությունը եւ հաշվողական խմբերի տեսությունը մաթեմատիկայի ինքնուրույն եւ բուռն զարգացում ապրող ճյուղեր են: Հաշվողական խմբերի տեսության որպես ինքնուրույն ոլորտի ձեւավորումը հիմնադրվեց 1970 թվականին, երբ Չարլզ Սիմսը առաջարկեց տեղադրությունների խմբի "ուժեղ" ծնիչների բազմության հիման վրա ստեղծված ալգորիթմական մեթոդները: Սիմսի ալգորիթմը (որը նաեւ հայտնի է որպես Շրայեր-Սիմսի ալգորիթմ) հաշվողական խմբերի տեսության հիմնարար մեթոդներից մեկն է: Դրա դերը համեմատելի է գծային հանրահաշվում գծային հավասարումների համակարգերի լուծման Գաուսի մեթոդի դերին:

Ներկայումս ծածկագրաբանությունը գիտության ամենաբուռն զարգացում ապրող ոլորտներից է, հատկապես ուշագրավ են ծածկաբանության մաթեմատիկական

մեթոդները, որոնք հիմնված են թվերի տեսության, հանրահաշվի (մասնավորապես խմբերի տեսության), դիսկրետ օպտիմիզացման տեսության, բարդության տեսության, ինֆորմացիայի տեսության մեթոդների կիրառման վրա: Հատկապես բաց բանալիով ծածկագրման սխեմաների անվտանգությունը հիմնված է այն բանի վրա, որ համակարգի "կոտրելը" համարժեք է դիսկրետ օպտիմիզացման բարդ (NP-լրիվ լամ NP-դժվար) խնդրի լուծմանը: Չնայած այն փաստի, որ գոյություն ունեն բավականին շատ բաց բանալիով ծածկագրման սխեմաներ, բազմաթիվ հետազոտություններ են կատարվում նոր սխեմաների կառուցման ուղղությամբ, քանի որ բաց բանալիով սխեմաները դեռեւս զիջում են գաղտնի բանալիով սխեմաների ապահովության մակարդակին:

Սույն աշխատանքը նվիրված է Սիմսի ալգորիթմի վրա հիմնված գաղտնի եւ բաց բանալիներով նոր ծածկագրման սխեմաների մշակմանը, դրանց անվտանգության մակարդակի հետազոտմանը եւ հաշվողական խմբերի տեսության մեթոդների ներմուծմանը ծածկագրաբանության մեջ:

Ատենախոսության նպատակը եւ խնդիրները.

1) Կառուցել գաղտնի բանալիով ծածկագրման մեթոդներ հիմնված տեղադրությունների խմբերի "ուժեղ" ծնիչների բազմության եւ դրա կառուցման Սիմսի ալգորիթմի վրա:

2) Հետազոտել բաց բանալիով ծածկագրման մեթոդների կառուցման հնարավորությունը հիմնված տեղադրությունների խմբերի "ուժեղ" ծնիչների բազմության գաղափարի եւ Սիմսի ալգորիթմի ընդլայնման վրա:

3) Հետազոտել բաց բանալիով ծածկագրման սխեմայի անվտանգությունը:

Հետազոտման մեթոդները: Ատենախոսության հետազոտություններում օգտագործվել են հաշվողական խմբերի տեսության, դիսկրետ մաթեմատիկայի, դիսկրետ օպտիմիզացման խնդիրների բարդության տեսության մեթոդները:

Գիտական նորությունը: Աշխատանքում կառուցվել են բոլորովին նոր, հաշվողական խմբերի տեսության մեթոդների վրա հիմնված գաղտնի եւ բաց բանալիներով ծածկագրման մեթոդներ: Հետազոտվել է տեղադրությունների հատուկ տեսքի արտադրյալներով ներկայացմանը վերաբերվող որոշ խնդիրների ալգորիթմական բարդությունը: Ապացուցվել է այդ խնդիրների NP-լիվությունը հիմնավորելով առաջարկված բաց բանալիով ծածկագրման մեթոդի հուսալիությունը:

Կիրառական նշանակությունը: Աշխատանքում առաջարկված մեթոդները կարող են օգտագործվել ինֆորմացիայի ծածկագրման գործնական համակարգերի նախագծման եւ կառուցման համար:

Ստացված արդյունքների ապրոբացիան եւ հրապարակումները: Ատենախոսության արդյունքները զեկուցվել են ԵՊՀ Ինֆորմատիկայի եւ կիրառական մաթեմատիկայի ընդհանուր եւ դիսկրետ մաթեմատիկայի եւ տեսական ինֆորմատիկայի ամբիոնի սեմինարներում, ՀՀ ԳԱԱ Ինֆորմատիկայի եւ ավտոմատացման պրոբլեմների ինստիտուտի ընդհանուր սեմինարում: Ատենախոսության հիմնական արդյունքները տպագրված են երեք գիտական հոդվածներում:

Ատենախոսության կառուցվածքը եւ ծավալը: Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, մեկ հավելվածից, ամփոփիչ եզրակացություններից եւ գրականության ցանկից, որը պարունակում է 13 աշխատանք: Ատենախոսության ծավալը 107 էջ է:

Աշխատանքի բովանդակությունը:

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

ԳԼՈՒԽ 1

§1. **Հիմնական սահմանումներ եւ նշանակումներ:** Սույն աշխատանքի կենտրոնական օբյեկտը n տարրարնի վերջավոր բազմության տեղադրությունների խումբն է՝ սիմետրիկ խումբը, որի համար կօգտագործենք ընդունված ստանդարտ S_n նշանակումը: Դիցուք $H \leq G \leq S_n$:

Սահմանում 1.1.1. *G խմբի ըստ H ենթախմբի հարակից դասերի բազմության ներկայացուցիչների բազմությունը կանվանենք H ենթախմբի տրանսվերսալ G խմբում:*

Ակնհայտ է, որ տրանսվերսալի հզորությունը հավասար է $(G : H)$ թվին՝ H ենթախմբի դասիչին (ինդեքսին) G-ում, կամ որ նույնն է, G/H ֆակտոր-խմբի կարգին:

Սահմանում 1.1.2. *G խմբի տարրերի T ենթաբազմությունը կոչվում է ծնիչների բազմություն G խմբի համար, եթե G-ի յուրաքանչյուր տարր կարելի է ներկայացնել T-ի վերջավոր քանակությամբ տարրերի կամ դրանց հակադարձների արտադրյալի*

տեսքով:

§2. **Խմբի "ուժեղ" ծնիչների բազմություն**: Դիցուք $G \le S_n$: Նշանակենք $G_{1,2,\dots,i} = \left\{\alpha \in G \mid \alpha(j) = j,\ j \in \{1,2,\dots,i\}\right\}$: Դյուրին է տեսնել, որ $G \ge G_1 \ge G_{1,2} \ge \dots \ge G_{1,2,\dots,i} \ge G_{1,2,\dots,n-1} = G_{1,2,\dots,n} = \{id_n\}$:

Դիտարկենք $G_{1,2,\dots,i-1} / G_{1,2,\dots,i-1,i}$ ֆակտոր-բազմությունը: $G_{1,2,\dots,i-1}$-ի երկու տեղադրություն միեւնույն հարակից դասից են եթե դրանք i-ն արտապատկերում են նույն տարրի մեջ: Ընտրենք որեւէ $G_{1,2,\dots,i-1,i}$-ի տրանսվերսալ $G_{1,2,\dots,i-1}$-ում որպես ներկայացուցիչ $G_{1,2,\dots,i-1,i}$-ից վերցնելով id_n-ը եւ նշանակենք այն $\Pi_i = \left\{\pi_i^0, \pi_i^1, \pi_i^2, \dots, \pi_i^{k_i}\right\}$, որտեղ $\pi_i^0 = id_n$ եւ $1 + k_i$-ն տրանսվերսալի հզորությունն է, որը չի կարող գերազանցել $n - i$ թվին: Նշանակենք Π-ով բոլոր կառուցված տրանսվերսալների միավորումը՝ $\Pi = \bigcup_{i=1}^{n-1} \Pi_i$: Պարզ է, որ $|\Pi| = (1 + k_1)(1 + k_2)\dots(1 + k_{n-1}) \le n!$ եւ հավասարությունը հնարավոր է միայն երբ $G = S_n$:

Պնդում 1.2.1. *G խմբի յուրաքանչյուր տեղադրություն կարելի է ներկայացնել $\alpha_1\alpha_2\dots\alpha_{n-1}$ արտադրյալի տեսքով, որտեղ $\alpha_i \in \Pi_i$, $i \in \{1,2,\dots,n-1\}$:*

Պնդում 1.2.2. *G խմբի α տեղադրության ներկայացումը $\alpha_1\alpha_2\dots\alpha_{n-1}$ արտադրյալի տեսքով, որտեղ $\alpha_i \in \Pi_i$, $i \in \{1,2,\dots,n-1\}$ որոշված է միարժեքորեն:*

Պնդում 1.2.3. *G խմբի կարգը հավասար է $|\Pi| = (1 + k_1)(1 + k_2)\dots(1 + k_{n-1})$:*

Սահմանում 1.2.4. *$\Pi = \bigcup_{i=1}^{n-1} \Pi_i$ տրանսվերսալների բազմությունը (որը դիտարկվում է աղյուսակ (1)-ի տեսքով) կոչվում է G խմբի "ուժեղ" ծնիչների բազմություն: G խմբի յուրաքանչյուր տեղադրություն միարժեքորեն ներկայացվում է $\alpha_1\alpha_2\dots\alpha_{n-1}$ արտադրյալի տեսքով, որտեղ $\alpha_i \in \Pi_i$, $i \in \{1,2,\dots,n-1\}$:*

§3. **"Ուժեղ" ծնիչների բազմության կառուցման Սիմսի ալգորիթմը:** Դիցուք $G \le S_n$ տեղադրությունների խումբը տրված է ծնիչների T բազմության միջոցով: Քանի որ G խումբը վերջավոր է, ապա յուրաքանչյուր $\alpha \in G$ տեղադրության համար ստույգ է՝ $a^{|G|} = id_n$ եւ $\alpha^{-1} = a^{|G|-1}$: Այդ պատճառով G յուրաքանչյուր տեղադրություն ներկայացվում է T-ի տարրերի արտադրյալի միջոցով: Սիմսի ալգորիթմի մուտքը ծնիչների բազմությունն է, իսկ ելքը՝ "ուժեղ" ծնիչների բազմությունը: Ալգորիթմի աշխատանքի ժամանակ օգտագործվում է $n \times n$-չափանի մի աղյուսակ, որի

վանդակներում տեղադրվում են տեղադրություններ (վանդակները կարող են նաեւ դատարկ լինել)։ Անկյունագծային վանդակներում մշտապես տեղադրված են id_n միավոր տեղադրությունները եւ դրանք փոփոխության ենթակա չեն։ Աղյուսակի անկյունագծից ներքեւ ընկած վանդակները չեն օգտագործվում։ i-րդ տողի վանդակները նախատեսված են Π_i տրանսվերսալի տեղադրությունների համար $i \in \{1,2,\dots,n-1\}$։ i-րդ տողի ($i \in \{1,\dots,n-1\}$) j-րդ վանդակում կարելի է գրել միայն այնպիսի α տեղադրություն, որի համար $\alpha(k) = k$, $k \in \{1,\dots,i-1\}$ եւ $\alpha(i) = j$, $j \in \{i+1,\dots,n\}$։ Ալգորիթմի աշխատանքի սկզբում աղյուսակի վանդակները դատարկ են։ Աշխատանքի ընթացքում աղյուսակի պարունակությունը փոփոխվում է՝ որոշ դատարկ վանդակների մեջ գրվում են նոր տեղադրություններ, որոշ վանդակներ մնում են դատարկ։ Լրացված վանդակի պարունակությունը այլեւս չի փոխվում։ Սիմսի ալգորիթմի աշխատանքի ավարտից հետո աղյուսակի i-րդ տողի վանդակներում ստացված տեղադրությունները կազմում են Π_i տրանսվերսալը եւ աղյուղսակի բոլոր տեղադրությունները՝ “ուժեղ” ծնիչների բազմություն G խմբի համար։

Սիմսի ալգորիթմը հիմնված է որոշակի գործողության պարբերական կրկնության վրա։ Այդ գործողությունը, որի անվանումն է *cascade*, կիրառվում է տրված տեղադրությանը եւ աղյուսակի ընթացիկ վիճակին։ Սիմսի ալգորիթմի աշխատանքի սկզբում աղյուսակը դատարկ է։ T ծնիչների համար հաջորդաբար կատարվում է *cascade* գործողությունը։ Այնուհետեւ *cascade* գործողությունը կատարվում է աղյուսակում գրված, միավորից տարբեր, տեղադրությունների յուրաքանչյուր զույգի արտադրյալի նկատմամբ։ Աղյուսակի տեղադրությունների զույգերի բազմությունը դինամիկ է եւ փոփոխվում է ալգորիթմի աշխատանքի ընթացքում։ Քանի որ աղյուսակի վանդակների քանակը վերջավոր է, այս պրոցեսը կավարտվի վերջավոր քանակությամբ քայլերից հետո։ Արդյունքում ստացված աղյուսակի տողերը կպարունակեն Π_i տրանսվերսալներ եւ աղյուսակն իրենից կներկայացնի G խմբի “ուժեղ” ծնիչների բազմություն։ Եթե ալգորիթմի աշխատանքի որեւէ փուլում աղյուսակում դատարկ վանդակ չի մնում ալգորիթմի աշխատանքը վերջանում է եւ արդյունքում ստացվում է S_n սիմետրիկ խմբի “ուժեղ” ծնիչների բազմություն։

Պնդում 1.3.3. *Սիմսի ալգորիթմը կառուցում է տրված խմբի “ուժեղ” ծնիչների բազմություն։*

Պնդում 1.3.4. *“Ուժեղ” ծնիչների բազմություն կառուցող Սիմսի ալգորիթմն ունի բազմանդամային վատագույն դեպքի բարդություն։*

ԳԼՈՒԽ 2

Սույն գլխում շարադրված են տեղադրությունների "ուժեղ" ծնիչների բազմությունների աղյուսակային ներկայացման հիման վրա կառուցված "գաղտնի (կամ սիմետրիկ) բանալիով" ծածկագրման մեթոդները:

§1. **Խմբի "ուժեղ" ծնիչների բազմության օգտագործման վրա հիմնված "գաղտնի (սիմետրիկ) բանալիով" ծածկագրման մեթոդների ընդհանուր կառուցվածքը:** Նկարագրվում է "ուժեղ" ծնիչների աղյուսակների օգտագործման հիման վրա կառուցված սիմետրիկ ծածկագրման սխեմայի պարզագույն բլոկային տարբերակը, որի միջոցով բացատրվում են դրա հիմնական գաղափարները:

Գաղտնի բանալիների տիրույթը դա S_n սիմետրիկ խմբի "ուժեղ" ծնիչների բազմությունների աղյուսակների եւ որոշակի տեսակի φ արտապատկերումների բազմություններն են: Ընտրենք S_n-ի որեւէ "ուժեղ" ծնիչների բազմություն եւ դրա աղյուսակը նշանակենք T-ով: Սա կլինի մեր գաղտնի բանալու մի մասը:

Նշանակենք $x_1x_2\dots x_k$ -ով ծածկագրման ենթակա բլոկը, որն իրենից ներկայացնում է k բիտ երկարությամբ երկուական բառ: Այսինքն բոլոր հնարավոր բլոկերի բազմությունը դա $X=\{x_1x_2\dots x_k \mid x_i\in\{0,1\}, i=1,2,\dots,k\}$բազմությունն է: Դիտարկենք բնական թվերի վեկտորներից բաղկացած հետեւյալ բազմությունը՝ $Y=\left\{(y_1,y_2,\dots,y_{n-1}) \mid i\le y_i\le n,\ i=1,2,\dots,n-1\right\}$:

Դիցուք $\varphi: X\to Y$ արտապատկերումը սուրյեկտիվ է եւ Φ-ն այդ արտապատկերումն իրացնող որեւէ ալգորիթմ է, իսկ Φ^{-1}-ը հակադարձ արտապատկերումն իրացնող որեւէ ալգորիթմ է (պարզ է, որ Φ^{-1}-ը որոշված է միայն $\varphi(X)$-ի տարրերի համար): Φ-ի աշխատանքի արդյունքը կնշանակենք այսպես. $\Phi(x_1x_2\dots x_k)=(y_1,y_2,\dots,y_{n-1})$: Φ եւ Φ^{-1} արտապատկերումները գաղտնի բանալու մնացած մասն են կազմում:

Պնդում 2.1.1. *Բլոկի առավելագույն երկարությունը փոքր է* $\log_2 n!$*-ից:*

Ծածկագրումը կատարվում է հետեւյալ կերպ: Ստանալով $x_1x_2\dots x_k$ բլոկը հաշվում ենք $\Phi(x_1x_2\dots x_k)=(y_1,y_2,\dots,y_{n-1})$: Ապա "ուժեղ" ծնիչների բազմության T աղյուսակի i-րդ տողից ընտրում ենք y_i-րդ տեղադրությունը, $1\le i\le n-1$: Ընտրված տեղադրությունները բազմապատկում ենք եւ ստանում $\alpha=\alpha_1\alpha_2\dots\alpha_{n-1}$ տեղադրությունը, որը եւ հանդիսանում է $x_1x_2\dots x_k$ բլոկի ծածկագիրը:

Դիցուք α տեղադրությունն որեւէ բլոկի ծածկագիր է: Այն վերծանելու համար կիրառում ենք *cascade* գործողությունը α տեղադրությանը եւ ստանում դրա

ներկայացումը T աղյուսակի տեղադրությունների արտադրյալի միջոցով՝ $\alpha = \alpha_1\alpha_2\ldots\alpha_{n-1}$, ընդ որում, α_i տեղադրությունը T աղյուսակի i-րդ տողին է պատկանում: Կառուցում ենք $(y_1, y_2, \ldots, y_{n-1})$ վեկտորը, որտեղ y_i-ն α_i տեղադրության վանդակի հերթական համարն է եւ հաշվում ենք $\Phi^{-1}((y_1, y_2, \ldots, y_{n-1})) = x_1x_2\ldots x_k$ վերծանելով սկզբնական բլոկը:

Դյուրին է տեսնել, որ նկարագրված ծածկագրման սխեման կոտրելու համար անհրաժեշտ է գուշակել Φ եւ Φ^{-1} արտապատկերումները եւ "ուժեղ" ծնիչների աղյուսակը, ինչը գործնականում անհնար է: Ծածկագրման ելքում ստացվում է տեղադրությունների հաջորդականություն, որն ունի շատ լավ վիճակագրական հատկություններ եւ կայուն է վիճակագրական հետազոտման միջոցով սխեմայի բացահայտման մեթոդների հանդեպ: Առաջարկված մեթոդի հիման վրա կառուցված ալգորիթմներով ծածկագրված ֆայլերը հնարավոր չի եղել սեղմել որեւէ հայտնի ինֆորմացիայի սեղմման ZIP, RAR եւ այլ ալգորիթմներով:

Վերը նկարագրված ընդհանուր մեթոդը կոնկրետացնելով կարելի է ստանալ ծածկագրման տարբեր ալգորիթմներ: Դա կատարելու համար անհրաժեշտ է ճշտել Φ եւ Φ^{-1} արտապատկերումների նկարագրությունները:

§2. **Ալգորիթմ A:** Այս ալգորիթմում մուտքային հաղորդագրությունը տրոհվում է հաստատուն երկարության բլոկերի: S_n տեղադրությունների խմբի "ուժեղ" ծնիչների աղյուսակը կարող է օգտագործվել թե ամբողջությամբ թե մասնակի: Որոշակիության համար այս պահին աղյուսակը կօգտագործվի ամբողջությամբ:

Նախ կառուցենք Φ եւ Φ^{-1} արտապատկերումները: Տրված $X = x_1x_2\ldots$ հաղորդագրությունը կարդացվում է բլոկ առ բլոկ: Նշանակենք $k_i = \lfloor \log_2(n-i) \rfloor + 1$, $1 \le i \le n-1$ (այստեղ $\lfloor a \rfloor$-ն իրական a թվի ամբողջ մասն է): Մեկ բլոկի երկարությունը նշանակենք L-ով եւ այն սահմանենք հավասար $\sum_{i=1}^{n-1} \lfloor \log_2(n-i) \rfloor = \sum_{i=1}^{n-1} (k_i - 1)$: Դիցուք $n-1 = 2^{m-1} + s$, որտեղ $m \ge 3$ եւ $0 \le s \le 2^{m-1} - 1$, ապա $L = (m-3)2^{m-1} + 2 + (m-1)(s+1)$:

Դիցուք $2^{m-1} \le l \le 2^m - 1$: $\varphi_{m,l}(\xi) = \left\lfloor \frac{l}{2^{m-1}-1} \xi \right\rfloor$ արտապատկերումը $[0; 2^{m-1}-1]$ հատվածի բոլոր ամբողջ թվերի բազմությունը սուրյեկտիվ արտապատկերում է $[0; l]$ հատվածի ամբողջ թվերի բազմության մեջ: Դիցուք տրված է η ամբողջ թիվը $[0; l]$ հատվածից եւ հայտնի է, որ գոյություն ունի ամբողջ $\xi \in [0; 2^{m-1}-1]$ այնպիսին, որ $\varphi_{m,l}(\xi) = \left\lfloor \frac{l}{2^{m-1}-1} \xi \right\rfloor = \eta$: Ապա $\varphi^{-1}_{m,l}(\eta) = \xi = \left\lceil \frac{2^{m-1}-1}{l} \eta \right\rceil$, որտեղ $\lceil a \rceil$-ն a իրական թվի ամբողջ մասն է վերեւից, այսինքն ամենափոքր ամբողջ թիվն է, որ մեծ կամ հավասար է

a-ին:

Սահմանենք Φ արտապատկերումը: Նշանակենք X_i-ով X հաղորդագրության հերթական $k_i - 1 = \lfloor \log_2(n-i) \rfloor$ բիտերից կազմված ենթահաջորդականությունը: Հերթական y_i-ն $(i \le n-2)$ ստանալու համար վերցնում ենք X_i ենթահաջորդականությունը եւ ξ-ով նշանակում ենք այն ամբողջ ոչ բացասական թիվը, որի երկուական ներկայացումը համընկնում է վերցված X_i -ի հետ: Ստանում ենք՝ $0 \le \xi \le 2^{k_i-1} - 1$ եւ $2^{k_i-1} \le n - i \le 2^{k_i} - 1$: Հաշվում ենք $\varphi_{k_i,n-i}(\xi) = \left\lfloor \frac{n-i}{2^{k_i-1}-1} \xi \right\rfloor$ եւ սահմանում $y_i = \varphi_{k_i,n-i}(\xi) + i$: Այսպիսով որոշվում է $(y_1, y_2, \dots, y_{n-1})$ վեկտորը եւ սահմանվում Φ արտապատկերումը:

Φ^{-1} արտապատկերումը վերականգնում է $X_1X_2\dots X_{n-2}$ բլոկը $(y_1, y_2, \dots, y_{n-1})$ վեկտորից հետեւյալ կերպ: Դիտարկենք y_i թիվը, $1 \le i \le n-2$: Ունենք, որ $i \le y_i \le n$, հետեւաբար՝ $0 \le y_i - i \le n - i$: Նաեւ ունենք, որ $k_i = \lfloor \log_2(n-i) \rfloor + 1$ եւ $2^{k_i-1} \le n - i \le 2^{k_i} - 1$ ուստի հաշվենք $\xi = \varphi^{-1}_{k_i,n-i}(y_i - i) = \left\lceil \frac{2^{k_i-1}-1}{n-i}(y_i - i) \right\rceil$: Պարզ է, որ $0 \le \xi \le 2^{k_i-1} - 1$: Կազմենք ξ-ի երկուական ներկայացումն օգտագործելով Ճիշտ $k_i - 1$ բիտ: Դրանով կվերականգնվի X_i ենթահաջորդականությունը:

Ապացուցվում է, որ $\lim_{n\to\infty} \frac{L}{n \log_2 n} = 1$ եւ որ Ալգորիթմ A-ում առաջարկված բլոկերի տրոհման եղանակը հանգեցնում է ըստ կարգի բլոկի օպտիմալ երկարությանը:

§3. **Ալգորիթմ B:** Այս ալգորիթմում մուտքային հաղորդագրությունը նույնպես տրոհվում է հաստատուն երկարության բլոկերի: Ընտրենք n-ը կենտ՝ $2^{k-1} \le n - 1 = 2^{k-1} + 2s$ եւ $2s + 1 \le 2^{k-1} - 1$, $k \ge 3$:

Կառուցենք Φ եւ Φ^{-1} արտապատկերումները: Տրված $X = x_1x_2\dots$ հաղորդագրությունը կարդացվում է բլոկ առ բլոկ: Նշանակենք $k_i = \lfloor \log_2((n-2i+2)(n-2i+1)) \rfloor + 1$, $1 \le i \le \frac{n-1}{2}$: Բլոկի երկարությունը նշանակենք $L = \sum_{i=1}^{\frac{n-1}{2}} (k_i - 1) = \sum_{i=1}^{\frac{n-1}{2}} \lfloor \log_2((n-2i+2)(n-2i+1)) \rfloor \ge (k-3)2^{k-1} + 2 + (k-1)(2s+2)$:

Φ արտապատկերումը ստացվում է հետեւյալ քայլերի միջոցով: Ընդհանուր i-րդ քայլում կարդում ենք բլոկի հերթական $k_i - 1 = \lfloor \log_2((n-2i+2)(n-2i+1)) \rfloor$ բիտերը եւ ստացված երկուական բառը դիտարկում ենք որպես ամբողջ ոչ բացասական թիվ՝ x_i, որտեղ $0 \le x_i < (n-2i+2)(n-2i+1)$: Մնացորդով բաժանման միջոցով ստանում ենք z_{2i-1} ե ւ z_{2i} թվերն այնպես, որ $x_i \equiv z_{2i-1} \bmod (n-2i+2)$, $0 \le z_{2i-1} \le n-2i+1$ եւ $x_i \equiv z_{2i} \bmod (n-2i+1)$, $0 \le z_{2i} \le n-2i$: Սահմանում ենք՝ $y_{2i-1} = z_{2i-1} + 2i - 1$ եւ $y_{2i} = z_{2i} + 2i$, որտեղ $2i - 1 \le y_{2i-1} \le n$ եւ $2i \le y_{2i} \le n$:

Վերջին քայլում, երբ $i = \frac{n-1}{2}$ կարդում ենք վերջին $k_{\frac{n-1}{2}} - 1 = \lfloor \log_2(3 \cdot 2) \rfloor = 2$ բիտերը եւ ստացված երկուական բառը դիտարկում ենք որպես ամբողջ ոչ բացասական թիվ՝ $x_{\frac{n-1}{2}}$, որտեղ $0 \le x_{\frac{n-1}{2}} < 3 \cdot 2$: Մնացորդով բաժանման միջոցով ստանում ենք z_{n-2} եւ z_{n-1} թվերն այնպես, որ $x_{\frac{n-1}{2}} \equiv z_{n-2} \bmod 3$, $0 \le z_{n-2} \le 2$ եւ $x_{\frac{n-1}{2}} \equiv z_{n-1} \bmod 2$, $0 \le z_{n-1} \le 1$: Սահմանում ենք՝ $y_{n-2} = z_{n-2} + n - 2$ եւ $y_{n-1} = z_{n-1} + n - 1$, որտեղ $n-2 \le y_{n-2} \le n$ եւ $n-1 \le y_{n-1} \le n$: Այսպիսով կառուցվում է $(y_1, y_2, \ldots, y_{n-1})$ վեկտորը եւ սահմանվում Φ արտապատկերումը:

Նկարագրենք Φ^{-1} արտապատկերումը: Այն վերականգնում է $X_1 X_2 \ldots X_{\frac{n-1}{2}}$ բլոկը $(y_1, y_2, \ldots, y_{n-1})$ վեկտորից հետեւյալ եղանակով: Յուրաքանչյուր $i \in \left\{1, 2, \ldots, \frac{n-1}{2}\right\}$ համար հաշվում ենք՝ $z_{2i-1} = y_{2i-1} - (2i-1)$ եւ $z_{2i} = y_{2i} - 2i$: Դյուրին է համոզվել, որ $0 \le z_{2i-1} \le n - 2i + 1$ եւ $0 \le z_{2i} \le n - 2i$: Φ արտապատկերման նկարագրման x_i թիվը միարժեքորեն վերականգնվում է z_{2i-1} եւ z_{2i} թվերից: Դա անմիջապես բխում է մնացքների մասին "չինական" թեորեմից: Էվքլիդեսի ալգորիթմի միջոցով գտնում ենք u_{2i-1} եւ u_{2i} ամբողջ թվերն որ $u_{2i-1}(n-2i+2) + u_{2i}(n-2i+1) = 1$: Դա հնարավոր է, քանի որ $(n-2i+2)$ եւ $(n-2i+1)$ թվերը փոխադարձաբար պարզ են: Ապա հաշվում ենք $w_i = u_{2i-1}(n-2i+2)z_{2i} + u_{2i}(n-2i+1)z_{2i-1}$ թիվը եւ այն բաժանում ենք մնացորդով $(n-2i+2)(n-2i+1)$-ի վրա (իհարկե եթե $0 \le w_i < (n-2i+2)(n-2i+1)$ բաժանումը չի կատարվում): Մնացորդում ստացված ամբողջ ոչ բացասական թիվը դա հենց x_i-ն է, որը խիստ փոքր է $(n-2i+2)(n-2i+1)$-ից, ուստի դրա երկուական ներկայացման երկարությունը փոքր է $k_i = \lfloor \log_2((n-2i+2)(n-2i+1)) \rfloor + 1$-ից: Բլոկի X_i ենթահաջորդականությունը վերցնում ենք հավասար x_i-ի $k_i - 1$ երկարության երկուական ներկայացմանը:

Ունենալով Φ եւ Φ^{-1} արտապատկերումները նաեւ "ուժեղ" ծնիչների բազմության աղյուսակը ստանում ենք ծածկագրման/վերծանման ալգորիթմները: Ապացուցվում է, որ $\lim_{n\to\infty} \frac{L}{n \log_2 n} = 1$ եւ Ալգորիթմ B-ում նույնպես առաջարկված բլոկերի տրոհման եղանակը հանգեցնում է ըստ կարգի բլոկի օպտիմալ երկարության:

§4. **Ալգորիթմ C:** Այս ալգորիթմում օգտագործվում է "ուժեղ" ծնիչների բազմության աղյուսակի մի մասը:

Ընտրենք $n = 2^k$, $k > 0$, եւ յուրաքանչյուր ամբողջ թիվ $[0; n-1]$ հատվածից ներկայացվում է k բիտանոց երկուական բառով եւ յուրաքանչյուր k բիտանոց երկուական բառ հանդիսանում է $[0; n-1]$ հատվածից ամբողջ թվի երկուական ներկայացում: Դիցուք T-ն S_{2n} սիմետրիկ խմբի "ուժեղ" ծնիչների բազմության

աղյուսակն է: Դիտարկենք T-ի $(n \times n)$ չափանի ենթաաղյուսակը, որը կազմված է առաջին n հատ տողերով եւ վերջին n հատ սյուներով: Ալգորիթմն օգտագործում է T-ի միայն այդ ենթաաղյուսակում պարունակվող տեղադրությունները: Այդ պատճառով ենթաաղյուսակի i,j-րդ $(1 \le i,j \le n)$ տարրին դիմելիս կգրենք $T[i][j+n]$: Թե ծածկագրման, թե վերծանման ժամանակ կատարվող *cascade* գործողությունները կատարվելու են օգտագործելով "ուժեղ" ծնիչների բազմության աղյուսակի նշված ենթաաղյուսակը:

Φ եւ Φ^{-1} արտապատկերումները բավականին պարզ են: Նշենք, որ Ալգորիթմ C-ում Φ-ն արտապատկերում է բլոկերի տիրույթը բնական թվերի վեկտորներից բաղկացած հետեւյալ բազմության մեջ՝ $\{(y_1,y_2,\dots,y_n) \mid 1 \le y_i \le n,\ i = 1,2,\dots,n\}$: Մուտքային բլոկի երկարությունը վերցնում ենք հավասար kn-ի: Կարդալով հաջորդաբար k երկարության բառերը կստանանք n հատ $[0;n-1]$ հատվածին պատկանող ամբողջ թիվ: Այդ թվերից յուրաքանչյուրին գումարելով 1 կստանանք պահանջվող $(y_1,y_2,\dots,y_n)$ վեկտորը: Φ արտապատկերումը բիյեկտիվ է՝ այն փոխմիարժեքորեն արտապատկերում է բլոկերի տիրույթը $\{(y_1,y_2,\dots,y_n) \mid 1 \le y_i \le n,\ i = 1,2,\dots,n\}$ բազմության վրա: Φ^{-1} հակադարձ արտապատկերումը հաշվելու համար բավական է տրված $(y_1,y_2,\dots,y_n)$ վեկտորի տարրերը փոքրացնել 1-ով եւ ստացված թվերի k բիտանոց երկուական ներկայացումները իրար կցագրել վերականգնելով սկզբնական բլոկը:

Ունենալով Φ եւ Φ^{-1} արտապատկերումները բլոկի ծածկագրումը կատարվում է հետեւյալ կերպ: Կարդալով բլոկը ստանում ենք $(y_1,y_2,\dots,y_n)$ վեկտորները եւ կազմում ենք տեղադրությունների հետեւյալ արտադրյալը՝ $T[1][y_1+n] \cdot T[2][y_2+n] \cdot \dots \cdot T[n][y_n+n]$, որն հանդիսանում է բլոկի ծածկագիրը: Վերծանելու համար կատարում ենք *cascade* գործողությունը ծածկագրի նկատմամբ: Ակնհայտ է, որ *cascade*-ի ժամանակ կօգտագործվի "ուժեղ" ծնիչների բազմության աղյուսակի միայն վերը նշված ենթաաղյուսակը: Ստանալով յուրաքանչյուր տողի համար համապատասխան սյան համարը եւ նվազեցնելով այն n-ով կստանանք $(y_1,y_2,\dots,y_n)$ վեկտորը, որից հեշտությամբ կիրառելով Φ^{-1} արտապատկերումը կվերականգնենք սկզբնական բլոկը: Հավելված 1-ում շարադրված է Ալգորիթմ C-ի ծրագրային իրացումը $n = 64$ դեպքի համար եւ կառուցված է սիմետրիկ բանալիով ծածկագրման համակարգ:

§5. **Հոսքային ծածկագրման ալգորիթմներ:** Նախորդ պարագրաֆներում դիտարկված ալգորիթմները բլոկային էին՝ ծածկագրվող հաղորդագրությունը տրոհվում

էր միեւնույն երկարության բլոկների եւ այդ բլոկները ծածկագրվում էին իրարից անկախ: Հոսքային ծածկագրման սխեմաներում յուրաքանչյուր հերթական բլոկ ծածկագրվում է իր ուրույն բանալիով: Այսինքն հաղորդագրության բլոկերի հոսքին զուգընթաց գեներացվում է բանալիների հոսքը եւ այդ բանալիներն օգտագործվում են բլոկերի ծածկագրման համար: Այս պարագրաֆում բացատրվում է թե ինչպես §1-ում նկարագրված ընդհանուր բլոկային սխեման կարելի է փոխակերպել հոսքայինի եւ դիտարկվում է Ալգորիթմ B-ի վրա հիմնված արագագործ ալգորիթմի օրինակ:

§6. **Բանալիների գեներացումը:** Դիտարկվում է գաղտնի բանալիների գեներացումը՝ տվյալ n-ի համար S_n սիմետրիկ խմբի "ուժեղ" ծնիչների բազմության աղյուսակների կառուցման մեթոդը: Այս խնդրի լուծման համար կրկին կօգտագործենք "ուժեղ" ծնիչների բազմության գաղափարը եւս մեկ անգամ շեշտելով դրա "ունիվերսալությունը":

ԳԼՈՒԽ 3

Սույն գլխում քննարկվում են տեղադրությունների խմբի հետ կապված որոշ խնդիրների ալգորիթմական բարդությունները:

Խնդիր 3.1.1. (Տեղադրությունների գեներացում բազմություններով)

Տրված $\pi \in S_n$ տեղադրության եւ S_n-ի ենթաբազմությունների $X_1, X_2, \ldots, X_m$ համակարգի համար որոշել կարելի է արդյո՞ք π տեղադրությունը ներկայացնել $\pi = \sigma_1\sigma_2\ldots\sigma_m$ արտադրյալի տեսքով, որտեղ $\sigma_i \in X_i, \quad 1 \le i \le m,$ եւ դրական պատասխանի դեպքում գտնել σ_i տեղադրությունները:

Խնդիր 3.1.2. (Տեղադրությունների ուսապարկ)

Տրված $\pi \in S_n$ տեղադրության եւ $\sigma_1, \sigma_2, \ldots, \sigma_m \in S_n$ տեղադրությունների հաջորդականության համար որոշել գոյություն ունի արդյո՞ք համարների X ենթահաջորդականություն, ասենք $i_1 < i_2 < \ldots < i_k$, այնպիսին, որ $\pi = \sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$, եւ դրական պատասխանի դեպքում գտնել X-ը (նշենք, որ X-ը կարող է ունենալ ցանկացած հզորություն 1-ից մինչեւ m):

Թեորեմ 3.2.1. *Տեղադրությունների գեներացում բազմություններով խնդիրը NP-լրիվ է:*

Թեորեմ 3.3.2. *Տեղադրությունների ուսապարկ խնդիրը NP-լրիվ է:*

Թեորեմ 3.3.4. *Տեղադրությունների ուսապարկ խնդիրը բազմանդամային ժամանակում հանգեցվում է Տեղադրությունների գեներացում բազմություններով խնդրի մասնավոր դեպքին, երբ $|X_i| = 2$ յուրաքանչյուր $i \in \{1, 2, \ldots, m\}$ համար:*

Հետեւանք 3.3.5. *Տեղադրությունների գեներացում բազմություններով խնդիրը*

մնում է NP-լրիվ նույնիսկ այն դեպքում, երբ բոլոր X_i բազմությունները պարունակում են Ճիշտ 2 տեղադրություն:

ԳԼՈՒԽ 4

Սույն գլխում կշարադրվի տեղադրությունների "ուժեղ" ծնիչների բազմությունների աղյուսակային ներկայացման հիման վրա կառուցված "բաց (կամ ասիմետրիկ) բանալիով" ծածկագրման մեթոդը:

§1. **Տեղադրությունների խմբի ընդհանրացված ծնիչների "ուժեղ" բազմությունը:** Դիցուք $G \le S_n$ եւ $G \equiv G_0 \ge G_1 \ge \ldots \ge G_i \ge \ldots \ge G_m = \{e\}$ ենթախմբերի շղթա է G խմբում: Դիտարկենք G_{i-1}/G_i ֆակտոր-բազմությունը եւ նշանակենք X_i-ով G_i ենթախմբի տրանսվերսալը G_{i-1} խմբում: Այդ տրանսվերսալների միավորումը՝ $X_1 \cup \ldots \cup X_m$ կոչվում է G խմբի **ընդհանրացված "ուժեղ" ծնիչների բազմություն:**

Պնդում 4.1.1. *G խմբի յուրաքանչյուր տարր միարժեքորեն ներկայացվում է $\alpha_1\alpha_2\ldots\alpha_m$ արտադրյալի տեսքով, որտեղ $\alpha_i \in X_i$, $i = 1,2,\ldots,m$:*

Հասարակ "ուժեղ" ծնիչների բազմության դեպքի նման ընդհանրացված "ուժեղ" ծնիչների բազմությունը ներկայացվում է աղյուսակի տեսքով: Ենթադրենք այժմ, որ տրված է G խմբի ընդհանրացված "ուժեղ" ծնիչների բազմության աղյուսակը՝ T_G-ն, որն ունի m տող եւ k_i լրացված վանդակ i-րդ տողում, $i = 1,2,\ldots,m$: Յուրաքանչյուր G_i ենթախմբի համար տրված է դրա հասարակ "ուժեղ" ծնիչների բազմության աղյուսակը՝ T_{G_i}-ն: Սահմանվում է ընդհանրացված *cascade* գործողությունը, որը թույլ է տալիս ստուգել արդյո՞ք տրված տեղադրությունը պատկանում է G խմբին եւ եթե պատկանում է ստանալ դրա ներկայցումը ընդհանրացված "ուժեղ" ծնիչների բազմության տարրերի միջոցով:

§2. **Խմբի ընդհանրացված "ուժեղ" ծնիչների բազմության օգտագործման վրա հիմնված "բաց (ասիմետրիկ) բանալիով" ծածկագրման սխեմա**: Նկարագրվում է բաց բանալիով ծածկագրման մի համակարգ, որը հիմնված է տեղադրությունների խմբի ընդհանրացված "ուժեղ" ծնիչների բազմության օգտագործման վրա:

Դիցուք T_{S_n}-ը S_n խմբի ընդհանրացված "ուժեղ" ծնիչների բազմության աղյուսակ է, որն ունի m տող եւ i-րդ տողում Ճիշտ k_i հատ տեղադրություն: Ընտրենք $S_n \equiv G_0 \ge G_1 \ge \ldots \ge G_i \ge \ldots \ge G_m = \{e\}$ ենթախմբերի շղթա S_n խմբում եւ T_{G_i}-ն G_i խմբի "ուժեղ" ծնիչների բազմության աղյուսակ է, $i = 1,2,\ldots,m$: Ընտրենք S_n-ից տեղադրությունների $\beta_1, \beta_2, \ldots, \beta_m$ պատահական հաջորդականություն եւ ձեւափոխենք T_{S_n} աղյուսակը հետեւյալ կերպ. յուրաքանչյուր α տեղադրություն T_{S_n} աղյուսակի i-րդ

տողից, $i < m$, փոխարինվում է $\beta_i \alpha \beta_{i+1}^{-1}$ տեղադրությամբ, իսկ վերջին, m-րդ, տողի յուրաքանչյուր α տեղադրություն փոխարինվում է $\beta_m \alpha \beta_1$ տեղադրությամբ: Այս ձեւափոխված աղյուսակը նշանակենք $\tilde{T}_{S_n}$-ով եւ այն կլինի համակարգի բաց բանալին: Գաղտնի բանալին բաղկացած է T_{S_n} աղյուսակից, T_{G_i} աղյուսակներից $i = 1,2,\ldots,m$ եւ β_1 տեղադրությունից:

Հաղորդագրման բլոկերի բազմությունն փոխմիարժեքորեն արտապատկերվում է $(s_1, s_2, \ldots, s_m)$, $s_i \in \{1,2,\ldots,k_i\}$ վեկտորների բազմության մեջ: Բլոկի ծածկագիրը ստանալու համար հարկավոր է հաշվել $\gamma = \gamma_{s_1}\gamma_{s_2}\ldots\gamma_{s_m}$ արտադրյալը, որտեղ γ_{s_i}-ն $\tilde{T}_{S_n}$ ձեւափոխված ընդհանրացված "ուժեղ" ծնիչների բազմության աղյուսակի i-րդ տողի s_i-րդ վանդակի տեղադրությունն է:

Վերծանման համար ծածկագրի յուրաքանչյուր տեղադրություն միարժեքորեն ներկայացվում է $\tilde{T}_{S_n}$ աղյուսակի տեղադրությունների $\gamma = \gamma_{s_1}\gamma_{s_2}\ldots\gamma_{s_m}$ արտադրյալի միջոցով, որտեղ $\gamma_{s_i} = \beta_i \alpha_i \beta_{i+1}^{-1}$, եթե $i < m$ եւ $\beta_m \alpha_i \beta_1$, եթե $i = m$, եւ α_i-ն T_{S_n} չձեւափոխված ընդհանրացված "ուժեղ" ծնիչների բազմության աղյուսակի i-րդ տողի s_i-րդ վանդակի տեղադրությունն է: Քանի որ $\gamma_{s_1}\gamma_{s_2}\ldots\gamma_{s_m} = \beta_1\alpha_1\alpha_2\ldots\alpha_m\beta_1$, ապա վերծանելու համար նախ հաշվում ենք $\beta_1^{-1}\gamma\beta_1^{-1} = \alpha_1\alpha_2\ldots\alpha_m$, ապա կիրառում ենք ընդհանրացված *cascade* գործողությունը եւ ստանում $(s_1, s_2, \ldots, s_m)$ վեկտորը, որից եւ վերականգնում ենք հաղորդագրության համապատասխան բլոկը:

Հնարավոր հակառակորդը համակարգը "կոտրելու" համար ստիպված է լուծել հետեւյալ խնդիրը: Տրված է $\alpha \in S_n$ տեղադրությունը եւ տեղադրությունների բազմությունների հաջորդականությունը՝ $X_1, X_2, \ldots, X_m$ (յուրաքանչյուր X_i բազմությունը դա $\tilde{T}_{S_n}$ աղյուսակի i-րդ տողում պարունակվող տեղադրությունների բազմությունն է), այնպիսին, որ $|X_i| \geq 2$ բոլոր $i \in \{1,2,\ldots,m\}$ համար: Անհրաժեշտ է որոշել արդյո՞ք α-ն հնարավոր է ներկայացնել $\beta_1\beta_2\ldots\beta_m$ արտադրյալի տեսքով, որտեղ $\beta_i \in X_i$, $i = 1,2,\ldots,m$, եւ դրական պատասխանի դեպքում գտնել այդ ներկայացումը: Ինչպես ապացուցել ենք Գլուխ 3-ում այս խնդիրը՝ **Տեղադրությունների գեներացում բազմություններով** խնդիրը *NP*-լրիվ է (Թեորեմ 3.2.1. եւ Հետեւանք 3.3.5) ուստի դրա լուծումը կապված է գործնականում անհաղթահարելի հաշվողական բարդության հետ:

ՀԱՎԵԼՎԱԾ 1-ում բերված է Գլուխ 2-ի §4-ում նկարագրված Ալգորիթմ C-ի հիման վրա կառուցված գաղտնի բանալիով ծածկագրման/վերծանման մի համակարգ $n = 64$ պարամետրի համար: Համակարգը ծրագրավորված է ANSI C ծրագրավորման լեզվով:

ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

Ստացված հիմնական արդյունքներն են.

1) Առաջարկված եւ հետազոտված է գաղտնի (սիմետրիկ) բանալիով ծածկագրման սխեմա հիմնված S_n սիմետրիկ խմբի "ուժեղ" ծնիչների բազմության աղյուսակի որպես գաղտնի բանալի օգտագործման վրա:

2) Չեւակերպված են **Տեղադրությունների գեներացում բազմություններով** եւ **Տեղադրությունների ուսապարկ** խնդիրները եւ ապացուցված է, որ դրանք NP-լրիվ են: Ապացուցվել է, որ **Տեղադրությունների գեներացում բազմություններով** խնդիրը մնում NP-լրիվ նույնիսկ եթե բոլոր ենթաբազմությունները պարունակում են յուրաքանչյուրը ճիշտ երկու տեղադրություն:

3) Առաջարկված եւ հետազոտված է բաց (ասիմետրիկ) բանալիով ծածկագրման սխեմա հիմնված տեղադրությունների խմբի "ուժեղ" ծնիչների բազմության գաղափարի ընդլայնման վրա: Ապացուցված է, որ այդ սխեմայի հուսալիությունը բխում է **Տեղադրությունների գեներացում բազմություններով** եւ **Տեղադրությունների ուսապարկ** խնդիրների NP-լրիվությունից:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԹԵՄԱՅԻ ՇՐՋԱՆԱԿՆԵՐՈՒՄ ՀՐԱՏԱՐԱԿԱԾ ԱՇԽԱՏՈՒԹՅՈՒՆՆԵՐԻ ՑԱՆԿԸ

1. **Alexanyan A., Aslanyan H and Soghoyan A.** Lightweight cryptographic schemes for wireless sensor networks, Mathematical Problems of Computer Science, Transactions of IPIA NAS RA, 2010, v. 33, p.127-134.

2. **Soghoyan A**. A Public-Key Encryption Scheme Based on Sim's Algorithm. Proceedings of the Yerevan State University, Physical and Mathematical Sciences, 2012, No 1, p.49-52.

3. **Alexanian A., Soghoyan A**. On NP-completeness of Some Permutation Generation Problems, Reports of NAS RA, Mathematics, 2012, v. 112, No 2, p.170-175.

РЕЗЮМЕ

Согоян Армен Ваганович

ПРИМЕНЕНИЕ МЕТОДОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕОРИИ ГРУПП В КРИПТОГРАФИИ

Диссертационная работа посвящена применению алгоритма Симса (Шрейера-Симса) для построения новых криптографических схем, основанных на использовании систем “сильных” образующих для групп подстановок.

Алгоритм Симса яаляется основным инструментом вычислительной теории групп, из которого по-существу и выросла современная вычислительная теория групп. Алгоритм Симса строит систему “сильных” образующих для группы подстановок, заданной какой-либо системой образующих. Для заданной группы подстановок G рассматривается башня подгрупп $G \geq G_1 \geq G_{12} \geq \ldots \geq G_{12\ldots i} \geq \ldots \geq G_{12\ldots n-1} = G_{12\ldots n} = \{e\}$, где $G_{12\ldots i}$ - подгруппа в G, являющаяся пересечением стабилизаторов чисел $1,2,\ldots,i$. Система “сильных” образующих для G представляется в виде прямоугольной таблицы, в которой ячейки i-ой строки содержат трансверсаль (систему различных представителей) фактор-множества $G_{12\ldots i-1} / G_{12\ldots i}$. Каждая подстановка из G однозначно задается произведением вида $g_1 g_2 \ldots g_{n-1}$, где g_i - подстановка из i-ой строки таблицы системы “сильных” образующих.

Общая схема шифрования с симметричным ключом задается таблицей T системы “сильных” образующих симметрической группы S_n и пары отображений Φ и Φ^{-1}, где Φ отображает множество X входных бинарных строк в множество векторов вида $(y_1, y_2, \ldots, y_{n-1})$, в которых y_i - это порядковый номер подстановки в i-ой строки таблицы. Тройка (T, Φ, Φ^{-1}) служит секретным ключом. В работе приводятся три алгоритма, реализующие данную схему, оптимальные по порядку длины входных блоков.

Общая схема шифрования с асимметричным ключом основывается на обобщенной системе “сильных” образующих, получающейся из произвольной башни подгрупп $G \geq G_1 \geq G_2 \geq \ldots \geq G_i \geq \ldots \geq G_m = \{e\}$. “Открытый” ключ – это особым образом преобразованная таблица обобщенной системы “сильных” образующих, а “секретный” ключ состоит из исходной таблицы и таблиц обычных систем “сильных” образующих подгрупп G_i.

Для раскрытия системы с асимметричным ключом противнику требуется умение решать следующие задачи:

Генерация подстановок множествами – для заданной подстановки π и системы подмножеств из S_n - $X_1, \ldots, X_m$ существует ли представление $\pi = \sigma_1 \sigma_2 \ldots \sigma_m$, где $\sigma_i \in X_i$? В случае положительного ответа найти такое представление.

Рюкзак подстановок - для заданных подстановки π и подстановок $\sigma_1, \sigma_2, \ldots, \sigma_m$ существует ли последовательность индексов $i_1 < i_2 < \ldots < i_k$ такая, что $\pi = \sigma_{i_1} \sigma_{i_2} \ldots \sigma_{i_k}$? В случае положительного ответа найти такую последовательность.

В работе доказано, что вышеуказанные задачи являются NP-полными, что обосновывает криптографическую стойкость системы с асимметричным ключом.

Основные результаты диссертации:

- Предложена и исследована криптографическая схема с симметричным ключом, основанная на использовании систем “сильных” образующих и алгоритма Симса.
- Предложена и исследована криптографическая схема с асимметричным ключом, основанная на использовании обобщенных систем “сильных” образующих и алгоритма Симса.
- Сформулированы задачи **Генерация подстановок множествами** и **Рюкзак подстановок**. Доказана NP-полнота этих задач и обоснована криптографическая стойкость системы с асимметричным ключом.

ABSTRACT

Soghoyan Armen

APPLICATION OF COMPUTATIONAL GROUP THEORY METHODS IN CRYPTOGRAPHY

An application of the Sims (Schreier-Sims) algorithm is considered in construction of new cryptographic schemes based on sets of "strong" generators for permutation groups.

The Sims algorithm is one of basic instruments of the computational group theory, which laid the foundation for the contemporary computational group theory. The algorithm of Sims constructs a set of "strong" generators for a permutation group given by a set of generators. Consider a subgroup tower $G \geq G_1 \geq G_{12} \geq \ldots \geq G_{12\ldots i} \geq \ldots \geq G_{12\ldots n-1} = G_{12\ldots n} = \{e\}$ for a given permutation group G in which $G_{12\ldots i}$ is a subgroup in G coinciding with the intersection of stabilizers for the numbers $1,2,\ldots,i$. A set of "strong" generators for G is presented in form of a table with cells of the i-th row occupied by permutations forming a transversal (a system of distinct representatives) for the factor-set $G_{12\ldots i-1} / G_{12\ldots i}$. Each permutation in G can be expressed as a product $g_1 g_2 \ldots g_{n-1}$, where g_i is a permutation from the i-th row of the table of the "strong" generators set.

The symmetric key encryption general scheme is defined by a table T of a "strong" generators set for the symmetric group S_n and a pair of mappings Φ and Φ^{-1}, where Φ maps the set of binary input strings X into the set of vectors $(y_1, y_2, \ldots, y_{n-1})$ in which y_i is a sequence number of a permutation in the i-th row of the table. The triplet (T, Φ, Φ^{-1}) serves as a secret key. We present three algorithms realizing the general scheme that are optimal by the order of the length of the input blocks.

The asymmetric (public) key encryption general scheme is based on the notion of the generalized "strong" set of generators, which is defined by an arbitrary tower of subgroups $G \geq G_1 \geq G_2 \geq \ldots \geq G_i \geq \ldots \geq G_m = \{e\}$. The public key is the table for the generalized "strong" set of generators that is transformed in a special way. The secret key consists of the original table for the generalized "strong" set of generators and tables for ordinary "strong" sets of generators for subgroups G_i.

In order to break an asymmetric system the adversary is faced with the following problems:

Permutation generation by sets – given a permutation π and a collection of sets of permutations from S_n decide whether π can be expressed as $\pi = \sigma_1 \sigma_2 \ldots \sigma_m$, where $\sigma_i \in X_i$; if the answer is positive find the expression.

Permutation knapsack - given a permutation π and a sequence of permutations $\sigma_1, \sigma_2, \ldots, \sigma_m$ from S_n decide whether there exists a subsequence of indices $i_1 < i_2 < \ldots < i_k$ such that $\pi = \sigma_{i_1} \sigma_{i_2} \ldots \sigma_{i_k}$; if the answer is positive find those indices.

It is proven that the above problems are NP-complete. This justifies cryptographic strength of the system with an asymmetric key.

The main results of the thesis are as follows:

- A general cryptographic scheme with a symmetric key using a set of "strong" generators for a permutation group and the algorithm of Sims is presented and researched.
- A general cryptographic scheme with an asymmetric key using a set of generalized "strong" generators for a permutation group and the algorithm of Sims is presented and researched.
- **Permutation generation by sets** and **Permutation knapsack** are formulated. It was proven that these problems are NP-complete and thus the cryptographic strength of a system with an asymmetric key is justified.