ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Մարգարյան Տիգրան Մելքոնի

ՇԵՆՈՆՅԱՆ ԾԱԾԿԱԳՐՄԱՆ ՀԱՄԱԿԱՐԳՈՒՄ ՏԵՂԵԿՈՒԹՅՈՒՆՆԵՐԻ ՊԱՀՊԱՆՄԱՆ ՀԵՏԱԶՈՏՈՒՄ

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

Ս Ե Ղ Մ Ա Գ Ի Ր

ԵՐԵՎԱՆ - 2014

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Тигран Мелконович Маргарян

ИССЛЕДОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ШЕННОНОВСКОЙ СЕКРЕТНОЙ СИСТЕМЕ

А В Т О Р Е Ф Е Р А Т

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

ЕРЕВАН 2014

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում:

Գիտական ղեկավար՝	ֆ.մ.գ. դոկտոր	Ե. Ա. Հարությունյան
Պաշտոնական ընդդիմախոսներ՝	տ.գ. դոկտոր	Գ. Հ. Խաչատրյան
	ֆ.մ.գ.թ.	Ն. Մ. Գրիգորյան
Առաջատար կազմակերպություն՝	Հայաստանի պետական ճարտարագիտական համալսարան	

Պաշտպանությունը կայանալու է 2014 թ. հունիսի 10-ին, ժամը 15:00-ին, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037-ի մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ.Սևակ 1:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2014թ. մայիսի 10-ին:

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

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

Научный руководитель:	доктор физ.мат.наук	Е. А. Арутюнян
Официальные оппоненты:	доктор тех. наук	Г. Г. Хачатрян
.	кандидат физ.мат.наук	Н. М. Григорян

Ведущая организация: Государственный инженерный университет Армении

Защита состоится 10-ого июня 2014г. в 15:00 на заседании специализированного совета 037 «Информатика и вычислительные системы» 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.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.
Автореферат разослан 10-ого мая 2014г.

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

ԱՇԽԱՏԱՆՔԻ ԸՆՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը

Արդի աշխարհում տեղեկատվության դերի բարձրացման զուգընթաց բազմաթիվ նոր խնդիրներ են առաջանում տեղեկատվության հուսալի հաղորդման հետ կապված: Տեղեկությունների պահպանման հետազոտությունում նոր մեթոդներ է առաջարկում ինֆորմացիայի տեսությունը՝ որը հիմնադրվել է 1948 թվականին Կ. Է. Շենոնը «Հեռահաղորդակցությյան մաթեմատիկական տեսություն» հանրահայտ հոդվածով: Մեկ տարի անց Շենոնը հրապարակեց «Կապի տեսության գաղտնի համակարգեր» հոդվածը, որում նկարագրեց ծածկագրման համակարգի մատեմատիկական մոդելը և սահմանվեց տեսականորեն բացարձակ կայուն (perfectly secure) և կիրառականորեն կայուն (practically secure) ծածկագրման համակարգերի գաղափարը: Հիմք դրվեց գաղտնի կամ համաչափ բանալիով ծածկագրման համակարգերի ուսումնասիրություններին: Տեսականորեն կայուն ծածկագրման համակարգը հուսալի է տեսական և տեխնիկական անսահմանափակ միջոցներ և անվերջ ժամանակ ունեցող հակառակորդի գրոհի նկատմամբ: Նաև ցույց տրվեց այդպիսի ծածկագրման համակարգերի գոյությունը, սակայն այդպիսի համակարգերը գործնականում կիրառելի չեն. օգտագործվում են միայն հույժ գաղտնի դիվանագիտական և ռազմական հաղորդակցություններում: Կիրառականորեն կայուն ծածկագրման համակարգը հուսալի է սահմանափակ տեխնիկական միջոցներ և ժամանակ ունեցող հակառակորդի գրոհի դեպքում: 1976 թվականին Դիֆին և Հելմանը հրապարակեցին «Գաղտնագրության նոր ուղղություններ» հոդվածը, որում առաջարկեցին հաշվարկայնորեն կայուն (computationally secure) ծածկագրման համակարգի մոդել և սկսեց զարգանալ բաց կամ անհամաչափ բանալիով ծածկագրամն համակարգերը:

Հեռահաղորդակցության և համակարգչային տեխնոլոգիաների բուռն զարգացման զուգընթաց արդիական է մնում նոր հաշվարկայնորեն կայուն ծածկագրման համակարգերի ստեղծումը և հետազոտումը: Ինֆորմացիայի տեսությունը լայն հնարավորություններ է ստեղծում այդպիսի համակարգերի մաթեմատիկական մոդելների մշակման և ուսումնասիրման համար:

1994 թ. Մեսսին «Գուշակում և անորոշություն» զեկույցում առաջադրեց գուշակման խնդիրը[1], որը իր կիրառությունները ստացավ կոդավորման տեսությունում[2] [3] և

[1]J. L. Massey, “Guessing and entropy”, *Proceedings of the 1994 IEEE International Symp. Inform. Theory* (Trondheim, Norway, 1994), p. 204.

[2]E. Arikan, “An inequality on guessing and its application to sequential decoding”, *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 99-105, 1996.

[3]H. Yamamoto and K. Okudra, “Channel coding theorem for the number of guesses in decoding”, *IEEE-ISIT2011,pp.419-423*, Saint Petersburg, July 31-August 5, 2011.

ծածկագրությունում [4] [5]:

Վերջին տարիներին ինֆորմացիայի տեսությունում ստեղծվել է նոր ուղղություն, որում ուսումնասիրվում է ծածկագրման համակարգերի գաղտնիության աստիճանը, ըստ գաղտնալսողի գուշակմումնների (wiretapper guessing) Ըստ այս նոր ուղության ծածկագրման համակարգի գաղտնիության չափորոշիչ է համր գաղտնալսողի գուշակման արագությունը, որը ծածկագրման համակարգը ջարդելու համար կատարված գուշակումների սպասվող արժեքնն է:

Ատենախոսությունը նվիրված է գուշակող գաղտնավերլուծողի առկայությամբ Շենոնի ծածկագրման համակարգերի ուսումնասիրությանը: Մշակվել և հետազոտվել են արդեն իսկ հայտնի և նոր ծածկագրման համակարգի մոդելներ, առաջարկված Մերհավի և Արիկանի, Ե. Հարությունյանի և հեղինակի կողմից [4-7], որոնք ունեն մեծ կիրառական նշանակություն: Հետազոտվել և գնահատվել են դիտարկված ծակագրական համակարգերում գաղտնալսողի գուշակման արագությունը (guessing rate), որը լավագույնս արտահայտում է նորագույն համակարգերի կիրառական կայունության աստիճանը:

Աշխատանքի նպատակն ու խնդիրները

Աշխատանքի նպատակն է մշակել գուշակող գաղտնալսողի առկայությամբ Շենոնի ծածկագրման համակարգերի մաթեմատիկական նոր մոդելներ: Դիտարկված համակարգերում սահմանվել է գաղտնալսողի գուշակման արագությունն, որպես համակարգի գաղտնիության հայտանիշ: Ըստ առաջարկված սկզբունքների ինֆորմացիայի տեսության մեթոդներով հետազոտել դիտարկված ծածկագրման համակարգերի գաղտնիության աստիճանը:

Հետազոտման օբյեկտը

Յուրաքանչյուր մշակված ծածկագրման համակարգի մոդելի դեպքում կարևորագույն խնդիրներից է գանահատել համակարգի հուսալիության աստիճանը հակառակորդի գրոհի նկատմամբ: Ծածկագրման համակարգի գաղնիության սկզբունքները բաժանվում են երկու խմբի, երբ համարվում է գաղտնալսողը գաղտնի տեղեկությունը պետք գաղտնազերծի մեկ և մեկից ավելի փորձերով: Առաջին խմբին է պատկանում Շենոնի առաջարկած անորոշության (equivocation) սկզբունքը, որպես գաղտնի տեղեկության կռահման չափ, Մերհավի առաջարկած սկզբունքը՝ մեկ փորձով տեղեկությունը գաղտնազերծելու հավանականությունը: Երկրորդ խմբի գաղտնիության չափի սկզբունքները առավել

[4] N. Merhav and E. Arikan, "The Shannon cipher system with a guessing wiretapper", *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1860-1866, 1999

[5] E. A. Haroutunian, "Realibility approach in wiretapper guessing theory", in "Aspects of Network and Information Security", NATO Science for Peace and Security, series D: Information and Communication Security, IOS Press, vol. 17, pp. 248–260, 2008.

ճշգրիտ են արտահայտում ծածկագրման համակարգի կիրառական կայունությունը: Այս խմբին պատկանող հայտանիշներից են. գաղտնավերլուծողի կողմից կատարված միջին աշխատանքի քանակը ծածկագրման բանալին ստանալու համար, ծածկագրման բալնալին գտնելու սպասվող արժեքը, ծածկագրման բանալին կամ ծածկագրված հաղորգագրությունը գտնելու փորձերի քանակի ρ-րդ մոմենտը՝ գուշակման ցուցիչը (guessing exponent):

Աշխատանքում հետազոտվում է գուշակման ցուցիչի (guessing exponent) առաջին մոմոնտը, որը անվանվում է գուշակման արագություն (guessing rate), Δ- հասանելի գուշակման արագությունը (Δ-achievable guessing rate), երբ ենթադրվում է, որ գաղտնալսողը կարող է գաղտնազերծել հաղորդագրությունը որոշակի Δ-շեղման ճշտությամբ:

Հետազոտման մեթոդները

Ուսումնասիրությունները հիմնվել են ինֆորմացիայի տեսության Չիսարի-Կյորների կազմերի մեթոդի[6] և արագություն-շեղում տեսության[7] վրա: Ուսումնասիրության ընթացքում կառուցված են գաղտնավերլուծության ռազմավարություններ, հաշվի առնելով, Մեսսիի, Մերհավի-Արիկանի առաջարկած գուշակման լավագույն ռազմավարությունները, Ե. Հարությունյանի և Ա. Ղազարյանի առաջարկած գաղտնավերլուծության լավագույն Δ-հասանելի ռազմավարությունները [8]:

Արդյունքների գիտական նորույթը

Աշխատանքի բոլոր հիմնական արդյունքները նոր են: Հետազոտության ընթացքում ուսումնասիրվել են գուշակող գաղտնալսողի առկայությամբ Շենոնի ծածկագրման համակարգի չորս մաթեմատիկական մոդելներ: Մոդելներից մեկը առաջարկվել է Մերհավի և Արիկանի կողմից, մյուս երեքը հեղինակի և Ե. Հարությունյանի կոմից են առաջարկվել, որպես ընդհանրացում Ե. Հարությունյանի, Հայաշիի և Յամամոտոյի ուսումնասիրած մոդելների:

Ստացված արդյունքների կիրառական նշանակությունը

Ուսումնասիրված ծածկագրման համակարգերի կիրառությունների ոլորտը շատ լայն է: Ներդրվում է ռազմական և դիվանագիտական հեռահաղորդակցություններում, ֆինանսական փոխանցումների համակարգերում, օնլայն բանկային ծառայություններում, էլեկտրոնային առևտրում, էլեկտրոնային նամակագրությունում, պետական համակարգի գաղտնի փաստաթղթաշրջանառությունում և այլն: Ստացված արդյունքները նշանակալի են, երբ

[6] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic, 1981.

[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory*,Second Edition, New York: Wiley, 2006.

[8] E. A. Haroutunian and A. R. Ghazaryan, "On the Shannon cipher system with a wiretapper guessing subject to distortion and reliability requirements", *IEEE-ISIT2002,* p.324, Lausanna , June 30-July 5, 2002.

հակառակորդը ստանում է ծածկագրված տեղեկության աղավաղված տարբերակը և այն դեպքում, երբ հնարավորություն ունի վերծանելու տեղեկությունը որոշակի ճշգրտությամբ:

Պաշտպանությանը ներկայացվում են հետևյալ դրույթները

- Շեննոնյան ծածկագրման համակարգը ջարդելու համար աղմուկով գաղտնալսողի գուշակող ռազմավարության կառուցում:
- Աղբյուրի հարաբերակցված երկու ելք ունեցող Շեննոնյան ծածկագրման համակարգի աղմուկով գաղտնալսողի առկայությամբ գաղտնավերլուծում:
- Շեննոնյան ծածկագրման համակարգում գուշակող գաղտնավերլուծողի թույլատրելի շեղման և աղմուկի առկայության դեպքում գաղտնավերլուծության մեթոդի առաջարկում:
- Աղբյուրի հարաբերակցված երկու ելք ունեցող Շեննոնյան ծածկագրման համակարգում գուշակող գաղտնալսողի թույլատրելի շեղման դեպքում գաղտնավերլուծության ալգորիթմի կառուցում:

Ապրոբացիա

Ատենախոսությունում ներկայացված հիմնական արդյունքները զեկուցվել են հետևյալ միջազգային գիտաժողովներում՝

- Կոմպյուտերային գիտություն և ինֆորմացիոն տեխնոլոգիաներ (Երևան, CSIT 2011),
- Հեռահաղորդակցության ֆորում (Բելգրադ, IEEE TELFOR 2012),
- Կոմպյուտերային գիտություն և ինֆորմացիոն տեխնոլոգիաներ (Երևան, IEEE CSIT 2013):

Արդյունքները ներկայացվել են նաև՝

- Հայկական մաթեմատիկական միության տարեկան նստաշրջանին՝ նվիրված Ռաֆայել Ալեքսանդրյանի 90-ամյակին, (Երևան, 2013)
- ՀՀ ԳԱԱ ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի գիտական սեմինարներում:

Հրապարակումներ

Ատենախոսության թեմայով հրապարակված են 3 գիտական հոդվածներ և 4 գիտաժողովների զեկուցումների թեզիսներ, որոնց ցանկը բերված է սեղմագրի վերջում:

Ատենախոսության կառուցվածքը և ծավալը

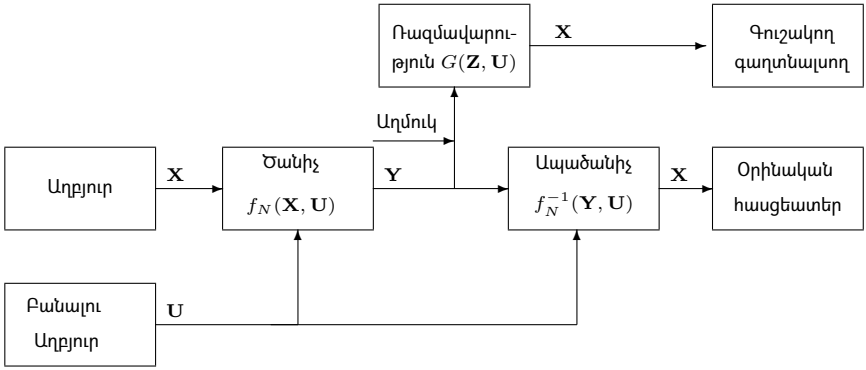
Աշխատությունը բաղկացած է առաջաբանից, չորս գլուխներից, եզրակացությունից և հղված գրականության ցանկից: Ատենախոսությունը շարադրված է 72 էջի վրա:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Առաջաբանում հիմնավորված է թեմայի արդիականությունը, ձևակերպված է հետազոտության նպատակն ու հիմնական խնդիրները, նկարագրված են ուսումնասիրվող օբյեկտները, հետազոտման մեթոդները: Ներկայացված են ստացված արդյունքների գիտական նորույթը և կիրառական նշանակությունը:

Առաջին գլուխը նվիրված է ինֆորմացիայի տեսության հիմնական գաղափարների և նշանակումների նկարագրմանը և խնդրի դրվածքին:

Երկրորդ գլուխում նկարագրվում է առանց հիշողության աղբյուրով Շեննոնյան ծածկագրման համակարգի մաթեմատիկական մոդելը, երբ գաղտնալսողը ստանում է ծածկագրված հաղորդագրությունը առանց հիշողության աղմուկով կապուղիով (նկար 1): Այս խնդիրը առաջարկվել է Մերհավի և Արիկանի կողմից:



Նկար 1. Շեննոնյան ծածկագրման համակարգը աղմուկի առակայությամբ գուշակող գաղտնալսողով

Տեղեկության աղբյուրը ստեղծում է $\{X_i\}_{i=1}^{\infty}$, անկախ միանման բաշխված (ա.մ.բ.) ընդհատ պատահական մեծությունների հաջորդականությունը, որոնք $P^* = \{P^*(x), x \in \mathcal{X}\}$ բաշխումով արժեքներ են ստանում $\mathcal{X}$ վերջավոր այբուբենից: Բանալու աղբյուրը նկարագրվում է $\{U_i\}_{i=1}^{\infty}$ անկախ միանաման բաշխված երկուական այբուբենով պատահական մեծությունների հաջորդականությամբ: Բաց տեքստը ծանվում է $f_N : \mathcal{X}^N \times \mathcal{U}^K \to \mathcal{Y}^M$ ծանման ֆունկցիայով՝ օգտագործելով U^K գաղտնի բանալին: Ստացված $\mathbf{Y}$ ծածկագիրը իրենից ներկայացնում է ա.մ.բ. պատահական վեկտոր $S = \{S(y), y \in \mathcal{Y}\}$ բաշխման ֆունկցիայով: Ծածկագիրը բաց կապուղիով ուղարկվում է օրինական հասցեատիրոջը, որը կարող է ապածանել այն բանալու օգնությամբ: Գաղտնալսողը գողանում է ծածկագիրը աղմուկոտ կապուղիով, որը բնութագրվում է $W^* = \{W^*(z|y), y \in \mathcal{Y}, z \in \mathcal{Z}\}$ հա-

վանականային մատրիցով: Համարվում է, որ գաղտնավերլուծողը տիրապետում է ապածանման f_N^{-1} ֆունկցիային և աղբյի հավանականային բաշխմանը, որոնց օգնությամբ կառուցում է $g^N = \{\mathbf{x}_1(\mathbf{z}), \mathbf{x}_2(\mathbf{z}), \cdots\}$ ռազմավարություն և փորձում է գաղտնազերծել ծածկագիրը: Ընտրված ռազմավարությամբ հաղորդագրությունը վերականգնելու գուշակումների քանակը նշանակված է $G_{f,g}^N(\mathbf{x}|\mathbf{z})$-ով: M/N մեծությունը նշանակված է λ-ով: K/N մեծությունը բանալու արագությունն է նշանակված R_K-ով:

Սահմանում 1: *Շեննոնյան ծածկագրման համակարգում աղմուկով գաղտնալսողի գուշակման արագությունն է*՝

$$R(R_K, W^*, P^*) = \lim_{N\to\infty} \sup_{f_N} \inf_{g_N} \frac{1}{N} \log \mathbf{E}[G_{f,g}^N(\mathbf{X}|\mathbf{Z})],$$

որտեղ $\mathbf{E}[G_{f,g}^N(\mathbf{X}|\mathbf{Z})]$-*ն* $G_{f,g}^N(\mathbf{X}|\mathbf{Z})$-*ի սպասելին է:*

Թեորեմ 1: *Առանց հիշողության* P^* *բաշխում ունեցող աղբյուրով և* R_K *բանալու արագությամբ Շեննոնյան ծածկագրման համակարգում առանց հիշողության* W^* *բաշխում ունեցող կապուղիով գաղտնալսողի գուշակման արագությունը հնարավոր է գնահատել հետևյալ արտահայտություններով՝*

$$R(R_K, W^*, P^*) \le \max_S \max_{P,Q,V} [\min\{H_P(X), \lambda H_{Q,V}(Y|Z) + R_K\} -$$

$$D(P||P^*) - \lambda D(Q \circ V \| S \circ W^*)],$$

$$R(R_K, W^*, P^*) \ge \max_P [\min\{H_P(X), R_K\} - D(P||P^*)] :$$

Հետևանք 1: *Երբ գաղտնալսողի կապուղին անաղմուկ է, վերը նշված արդյունքը հանգում է Մերհավի և Արիկանի արդյունքին*

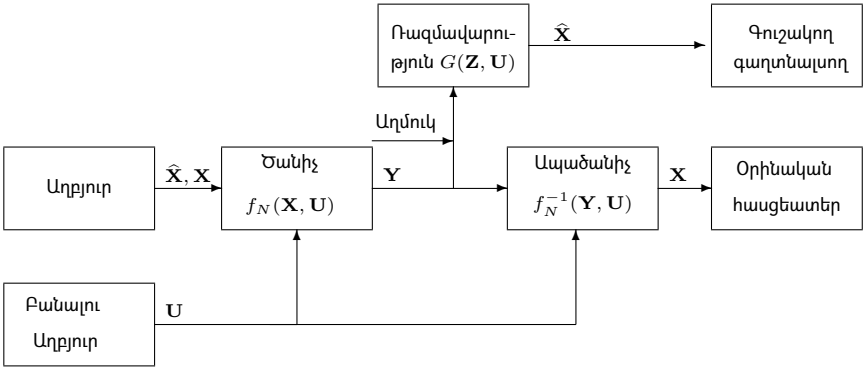
$$R(R_K, P^*) = \max_P [\min\{H_P(X), R_K\} - D(P||P^*)] :$$

Երրորդ գլխում ուսումնասիրվում է հարաբերակցված երկու ելք ունեցող աղբյուրով Շեննոնյան ծածկագրման համակարգի մաթեմատիկական մոդելը, երբ գաղտնալսողը ստանում է ծածկագրված հաղորդագրությունը աղմուկով կապուղիով (նկար 2), որը ընդհանրացումն է Հայաշիի և Յամամոտոյի առաջարկած մոդելի[9]:

Վերջավոր այբուբենով տեղեկության առանց հիշողության աղբյուրը ստեղծում է $P^* = \{P^*(x), x \in \mathcal{X}\}$ բաշխումով $\mathbf{X}$ հաղորդագրությունը և $\widehat{\mathbf{X}}$ գաղտնի տեղեկությունը, որը

[9]Y. Hayashi and H. Yamamoto, "Coding theorems for the Shannon cipher system with a guessing wiretapper and correlated source outputs", *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2808-2817, June 2008.

կապված է հաղորդագրության հետ $V^* = \{V^*(\hat{x}|x), \hat{x} \in \hat{\mathcal{X}}, x \in \mathcal{X}\}$ հավանականային մատրիցով: Բանալու աղբյուրը նկարագրվում է երկուական, անկախ միանաման բաշխված այբուբենով: Քանի որ հաղորդագրությունը տեղեկություն է պարունակում գաղտնի տեքստի վերաբերյալ, այն նախքան հաղորդվելը բաց կապուղիով ծածկագրվում է $f_N : \mathcal{X}^N \times \mathcal{U}^K \to \mathcal{Y}^M$ ծանման ֆունկցիայով: Ծածկագիրը բաց կապուղիով ուղարկվում է օրինական հասցեատիրոջը, որը կարող է ապածանել այն բանալու օգնությամբ: Գաղտնալսողը գողանում է ծածկագիրը առանց հիշողության աղմուկով կապուղիով, որը բնութագրվում է $W^* = \{W^*(z|y), y \in \mathcal{Y}, z \in \mathcal{Z}\}$ հավանականային մատրիցով:



Նկար 2: Գուշակող գաղտնալսողով Շեննոնյան ծածկագրման համակարգը հարաբերակցված երկու ելք ունեցող աղբյուրի և աղմուկի առկայությամբ

Համարվում է, որ գաղտնավերլուծողը տիրապետում է ապածանման f_N^{-1} ֆունկցիաին և աղբյուրի ելքերի հավանականային բաշխումներին, որոնց օգնությամբ կառուցում է $g^N = \{\hat{\mathbf{x}}_1(\mathbf{z}), \hat{\mathbf{x}}_2(\mathbf{z}), \cdots\}$ ռազմավարություն և փորձում է գաղտնազերծել գաղտնի տեղեկությունը: Ընտրված ռազմավարությամբ հաղորդագրությունը վերականգնելու գուշակումների փորձերի քանակը նշանակված է $G_{f,g}^N(\hat{\mathbf{x}}|\mathbf{z})$-ով: M/N մեծությունը նշանակված է λ-ով: K/N մեծությունը բանալու արագությունն է նշանակված R_K-ով:

Սահմանում 2: *Հարաբերակցված երկու ելքերով աղբյուրով Շեննոնյան ծածկագրման համակարգում աղմուկով գաղտնալսողի գուշակման արագությունն է՝*

$$R(R_K, P^*, W^*, V^*) = \lim_{N\to\infty} \sup_{f_N} \inf_{g_N} \frac{1}{N} \log E[G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})],$$

որտեղ $\mathbf{E}[G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})]$-ն $G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})$-ի սպասելին է:

Թեորեմ 2: *Առանց հիշողության աղբյուրի P^* և P^*V^* բաշխում ունեցող ելքերով և R_K բանալու արագությամբ Շեննոնյան ծածկագրման համակարգում առանց հիշողության W^**

կապուղիով գաղտնալսողի գուշակման արագությունը բավարարում է

$$R(R_K, P^*, V^*, W^*) \le \max_S \max_{P,V,Q,W} [\min\{H_{PV}(\hat{X}), \lambda H_{Q,W}(Y|Z) + H_{P,V}(\hat{X}|X) + R_K\} -$$

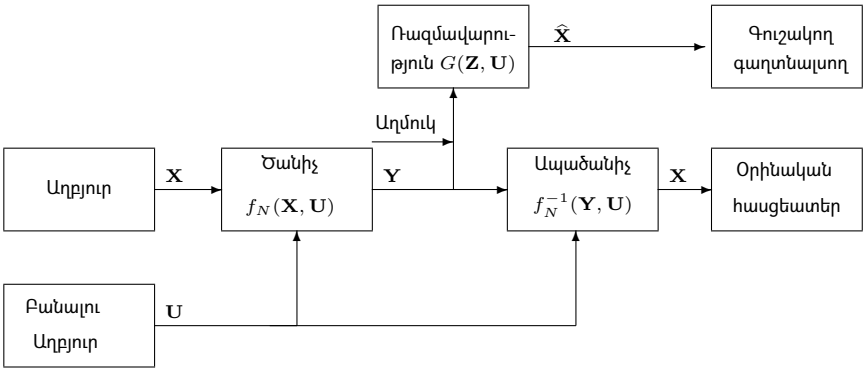
$$D(P \circ V \| P^* \circ V^*) + \lambda D(Q \circ W \| S \circ W^*)],$$

$$R(R_K, P^*, V^*, W^*) \ge \max_{P,V} [\min\{H_{PV}(\hat{X}), R_K + H_{P,V}(\hat{X}|X)\} - D(P \circ V \| P^* \circ V^*)] :$$

Հետևանք 2: *Երբ գաղտնալսողի կապուղին անաղմուկ է, վերը նշված արդյունքը հանգում է Հայաշիի և Յամամոտոյի սփռացած արդյունքին*

$$R(R_K, P^*, V^*) = \max_{P,V} [\min\{H_{PV}(\hat{X}), H_{P,V}(\hat{X}|X) + R_K\} - D(P \circ V \| P^* \circ V^*)] :$$

Չորրորդ գլուխում հետազոտվում է Շենոնյան ծածկագրման համակարգը, երբ գաղտնավերլուծողը ստանում է ծածկագրված հաղորդագրությունը աղմուկով կապուղիով և ցանկանում է վերականգնել բաց տեքստը տրված ճշտությամբ (նկար 3):



Նկար 3: Գուշակող գաղտնալսողով Շեննոնյան ծածկագրման համակարգը աղմուկի առկայության և թույլատրելի շեղման դեպքում

Տեղեկության աղբյուրը ստեղծում է $\{X_i\}_{i=1}^{\infty}$ անկախ միանման բաշխված (ա.մ.բ.) ընհատ պատահական մեծությունների հաջորդականությունը, որոնք $P^* = \{P^*(x), x \in \mathcal{X}\}$ բաշխումով արժեքներ են ստանում $\mathcal{X}$ վերջավոր այբուբենից: Բանալու աղբյուրը նկարագրվում է $\{U_i\}_{i=1}^{\infty}$ անակախ միանաման բաշխված երկուական այբուբենով հաջորդականությամբ: Բաց տեքստը ծանվում է $f_N : \mathcal{X}^N \times \mathcal{U}^K \to \mathcal{Y}^M$ ծանման ֆնկցիայով՝ օգտագործելով գաղտնի բանալին: Ստացված $\mathbf{Y}$ ծածկագիրը ա.մ.բ. պատահական բաղադրիչներով վեկտոր է $S = \{S(y), y \in \mathcal{Y}\}$ բաշխման ֆունկցիայով: Ծածկագիրը բաց

կապուղիով ուղարկվում է օրինական հասցեատիրոջը, որը կարող է ապաճանել այն բանալու օգնությամբ: Գաղտնալսողը գողանում է ծածկագիրը առանց հիշողության աղմուկով կապուղիով, որը բնութագրվում է $W^* = \{W^*(z|y), y \in \mathcal{Y}, z \in \mathcal{Z}\}$ հավանականային մատրիցով: Համարվում է, որ գաղտնավերլուծողը տիրապետում է ապաճանման f_N^{-1} ֆունկցիաին և աղբյուրի հավանականային բաշխմանը, որոնց օգնությամբ կառուցում է $g^N = \{\widehat{\mathbf{x}}_1(\mathbf{z}), \widehat{\mathbf{x}}_2(\mathbf{z}), \cdots\}$ ռազմավարություն և փորձում է գուշակել ծածկագիրը տրված Δ ճշտությամբ: Ընտրված ռազմավարությամբ հաղորդագրությունը վերականգնելու գուշակումների քանակը նշանակված է $G_{f,g}^N(\widehat{\mathbf{x}}|\mathbf{z})$-ով: M/N մեծությունը նշանակված է λ-ով: K/N մեծությունը բանալու արագությունն է նշանակված R_K-ով: Արդյունքում օգտագործվում է աղբյուրի կոդավորումից հայտնի արագություն-շեղում ֆունկցիան[10] $R(P,\Delta) = \min\limits_{V \in \mathcal{V}(P,\Delta)} I_{P,V}(X \wedge \hat{X})$:

Սահմանում 3: *Շեննոնյան ծածկագրման համակարգում աղմուկով գաղտնալսողի Δ-հասանելի գուշակման արագությունն է՝*

$$R(R_K, \Delta, P^*, W^*) = \lim_{N\to\infty} \sup_{f_N} \inf_{g_N} \frac{1}{N} \log \mathbf{E}[G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})],$$

որտեղ $\mathbf{E}[G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})]$-ն $G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})$-ի սպասելին է: Թեորեմ 3: *Առանց հիշողության P^* բաշխում ունեցող աղբյուրով և R_K բանալու արագությամբ Շեննոնյան ծածկագրման համակարգում առանց հիշողության W^* բաշխում ունեցող կապուղիով գաղտնալսողի Δ-հասանելի գուշակման արագությունը գնահատվում է հետևյալ կերպ՝*

$$R(R_K, \Delta, P^*, W^*) \le \max_S \max_{P,Q,W} [\min\{R(P,\Delta), \lambda H_{Q,W}(Y|Z) + R_K\} -$$

$$D(P||P^*) - \lambda D(Q \circ W \| S \circ W^*)]$$

$$R(R_K, \Delta, P^*, W^*) \ge \max_P [\min\{R(P,\Delta), R_K\} - D(P||P^*)] :$$

Հետևանք 3: *Երբ գաղտնալսողի կապուղին անաղմուկ է, վերը նշված արդյունքը հանգում է Հարությունյանի սպացած արդյունքին*

$$R(R_K, \Delta, P^*) = \max_P [\min\{R(P,\Delta), R_K\} - D(P||P^*)] :$$

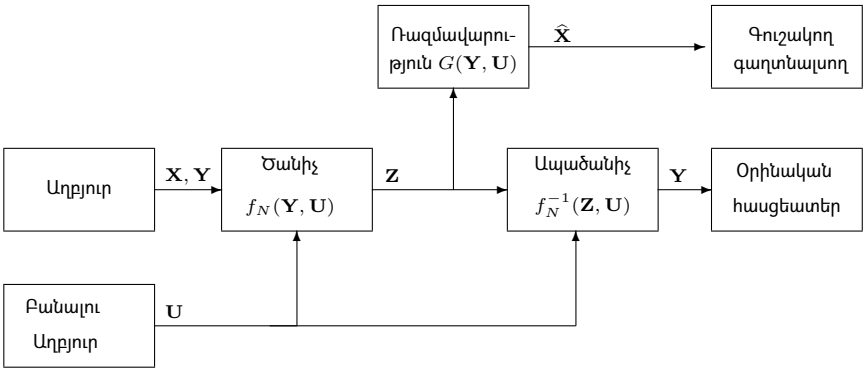
Հետևանք 4: *Երբ գաղտնալսողի թույլատրելի շեղում չունի, սպացվում է թեորեմ 1-ի արդյունքը*

$$R(R_K, P^*, W^*) \le \max_S \max_{P,Q,W} [\min\{H_P(X), \lambda H_{Q,W}(Y|Z) + R_K\} -$$

$$D(P||P^*) - \lambda D(Q \circ W \| S \circ W^*)] :$$

[10] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*, Englewoods Cliffs, NJ: Prentice-Hall, 1971.

Հինգերորդ գլուխում ուսումնասիրված ծածկագրական համակարգի մոդելը ներկայացված է նկար 4-ում:



Նկար 4. Գուշակող գաղտնալսողով Շեննոնյան ծածկագրման համակարգը երկու հարաբերակցված ելքերով աղբյուրի և թույլատրելի շեղման դեպքում

Վերջավոր այբուբենով տեղեկության առանց հիշողության աղբյուրը ստեղծում է $P^* = \{P^*(y), y \in \mathcal{Y}\}$ բաշխումով $\mathbf{Y}$ հաղորդագրությունը և $\mathbf{X}$ գաղտնի տեղեկությունը, որը կապված է հաղորդագրության հետ $V^* = \{V^*(x|y), x \in \mathcal{X}, y \in \mathcal{Y}\}$ հավանականային մատրիցով: Բանալու աղբյուրը նկարագրվում է $\mathbf{U}$ երկուական, անակախ միանաման բաշխված այբուբենով: Քանի որ, հաղորդագրությունը տեղեկություն է պարունակում գաղտնի տեքսի վերաբերյալ, նախքան հաղորդվելը բաց կապուղիով, այն ծածկագրվում է $f_N : \mathcal{Y}^N \times \mathcal{U}^K \to \mathcal{Z}^*$ ծանման ֆունկցիայով: Ծածկագիրը բաց կապուղիով ուղարկվում է օրինական հասցեատիրոջը, որը կարող է ապածանել այն բանալու օգնությամբ: Գաղտնալսողը ստանում է ծածկագիրը անաղմուկով կապուղիով և փորձում է գաղտնազերծել գաղտնի տեղեկությունը տրված Δ հեռավորության և $d : \mathcal{X} \times \hat{\mathcal{X}} \to [0;\infty)$ հեռավորության չափի դեպքում: Համարվում է, որ գաղտնավերլուծողը տիրապետում է ապածանման f_N^{-1} ֆունկցիաին և աղբյուրի ելքերի հավանականային բաշխումներին, որոնց օգնությամբ կառուցում է $g^N = \{\widehat{\mathbf{x}}_1(\mathbf{z}), \widehat{\mathbf{x}}_2(\mathbf{z}), \cdots\}$ գուշակման ռազմավրությունը: Ընտրված ռազմավարությամբ հաղորդագրությունը վերականգնելու գուշակումների փորձերի քանակը նշանակված է $G_{f,g}^N(\widehat{\mathbf{x}}|\mathbf{z})$-ով:

Սահմանում 4:*Աղբյուրի երկու հարաբերակցված ելքով Շեննոնյան ծածկագրման համակարգում գաղտնալսողի Δ-հասանելի գուշակման արագությունն է*՝

$$R(R_K, \Delta, P^*, W^*) = \lim_{N\to\infty} \sup_{f_N} \inf_{g_N} \frac{1}{N} \log \mathbf{E}[G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})],$$

որտեղ $\mathbf{E}[G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})]$-*ն* $G_{f,g}^N(\widehat{\mathbf{X}}|\mathbf{Z})$-*ի սպասելին է:*

Թեորեմ 4:*Առանց հիշողության աղբյուրի* P^* *և* P^*V^* *բաշխում ունեցող ելքերով և* R_K *բանալու արագությամբ Շեննոնյան ծածկագրման համակարգում գաղտնալսողի* Δ-*հասանելի գուշակման արագությունը բավարարում է հետևյալ սահմանափակումներին՝*

$$R(R_K, \Delta, P^*, V^*) \leq \max_{P,V}[\min\{R(P, \Delta), H_{P,V}(X|Y) + R_K\} - D(P \circ V \| P^* \circ V^*)]$$

$$R(R_K, \Delta, P^*, V^*) \geq \max_{P}[\min\{R(P, \Delta), H_P(X) + R_K\} - D(P \circ P^*)] :$$

Անաղմուկ կապուղու դեպքում ստացվում է հետևանք 2-ը, իսկ աղբյուրի մեկ ելքի դեպքում արդյունքը հանգում է հետևանք 3-ին:

Աշխատանքի Հիմնական Արդյունքները

- Գնահատվել է Շեննոնյան ծածկագրման համակարգի աղմուկով գաղտնալսողի գուշակման արագությունը [1,3]:
- Ձևակերպվել է աղբյուրի հարաբերակցված երկու ելք ունեցող Շեննոնյան ծածկագրման համակարգի ինֆորմացիոն-տեսական մոդելը աղմուկի առկայությամբ գուշակող գաղտնավերլուծողի դեպքում: Գնահատվել է համակարգի գաղտնիության աստիճանը [2,4]:
- Նկարագրվել է Շեննոնյան ծածկագրման համակարգի ինֆորմացիոն-տեսական մոդելը գուշակող գաղտնավերլուծողի թույլատրելի շեղման և աղմուկի առկայության դեպքում: Գնահատվել է Δ- հասանելի գուշակման արագությունը [5,6]:
- Առաջարկվել է աղբյուրի հարաբերակցված երկու ելք ունեցող Շեննոնյան ծածկագրման համակարգի ինֆորմացիոն-տեսական մոդելը գուշակող գաղտնալսողի թույլատրելի շեղման դեպքում: Գնահատվել է համակարգի Δ- հասանելի գուշակման արագությունը [7]:

Հրապարակված աշխատությունները

[1] E. A. Haroutunian and T. M. Margaryan, "The Shannon cipher system with a guessing wiretapper eavesdropping through a noisy channel", *Transactions of IIAP of NAS of RA , Mathematical Problems of Computer Science*, vol. 35, pp. 70-76, 2011.

[2] E. A. Haroutunian and T. M. Margaryan, "Wiretapper guessing by noisy channel for the Shannon cipher system with correlated source outputs", *Proceedings of 8th International Conference of Computer Science and Information Technologies (CSIT 2011)*, pp. 125–128, Yerevan , September 26-30, 2011.

[3] E. A. Haroutunian and T. M. Margaryan, "The Shannon cipher system with a guessing wiretapper eavesdropping through a noisy channel", *IEEE 20th Telecommunication Forum (TELFOR)*, pp. 532-536, November 20-22, Belgrade, 2012. *Print ISBN: 978-1-4673-2983-5, INSPEC Accession Number: 13265007*

[4] T. Margaryan, "On the Shannon cipher system with correlated source outputs and guessing wiretapper eavesdropping through a noisy Channel ", *Transactions of IIAP of NAS of RA , Mathematical Problems of Computer Science,* , vol. 37, pp. 17 - 24, 2012.

[5] E. A. Haroutunian and T. M. Margaryan, "On the Shannon cipher system with noisy channel to the wiretapper guessing subject to distortion criterion", *Abstracts of Annual Session Dedicated to 90 Anniversary of Rafael Alexandrian*, pp. 53- 54, Yerevan, 2013.

[6] T. M. Margaryan and E. A. Haroutunian , "On the Shannon cipher system with distortion and guessing wiretapper eavesdropping through a noisy channel", *Proceedings of 9th International Conference of Computer Science and Information Technologies (CSIT 2013)*, pp. 116–120, Yerevan, September 23-27, 2013 *Revised Selected Papers IEEE Explore, Print ISBN: 978-1-4799-2460-8, INSPEC Accession Number: 14042607*

[7] T. M. Margaryan, "The Shannon cipher system with correlated source outputs and wiretapper guessing subject to distortion", *Transactions of IIAP of NAS of RA , Mathematical Problems of Computer Science*, vol. 41, pp. 47-54, 2014.

Tigran Melkon Margaryan

INVESTIGATION OF INFORMATION PROTECTION IN SHANNON CIPHER SYSTEM

SUMMARY

The dissertation is devoted to the investigation of Shannon cipher system with the guessing wiretapper. Through this work modification of the cipher system models is suggested by the author and supervisor. For each system, the most important issue is the system reliability evaluation towards to adversary attack.

The theoretical secrecy of Shannon's model of cipher system is traditionally measured by equivocation. In most of works in this area it is supposed that wiretapper has exactly one chance to estimate the plaintext. Shannon also gave the idea of practical secrecy, which is the average amount of work required to break the key. Hellman took one step forward in study of practical secrecy, proposed to measure the degree of security of the cipher system in terms of the expected number of key-plaintext combinations needed to obtain the given ciphertext. Merhav and Arikan suggested another security criterion, the guessing exponent, for the Shannon cipher system, in which the wiretapper is allowed to have many chances to reconstruct the plaintext. E. Haroutunian examined the system by the first moment of the guessing rate adding reliability requirements.

As a security criterion of the considered ciphers models wiretapper guessing rate or Δ-achievable guessing rate is defined. In the thesis the wiretapper guessing rate (Δ-achievable guessing rate) is defined as an expected number of trials in order to break the cipher system. Four models of cipher system have been studied and the security level has been estimated using the methods of the information theory, especially method of types. Strategies for breaking the cipher system by guessing at the key or the message are constructed.

The importance of extensions of the Shannon cipher system with guessing wiretapper can be explained by the fact that practically it is more probable that the wiretapper can observe a noisy version of the cryptogram. On the other hand the wiretapper is often allowed to reconstruct the plaintext with given distortion.

The following statements are presented for defense.

- Strategy for breaking the Shannon cipher system with a guessing wiretapper eavesdropping through a noisy channel.
- Cryptanalysis for the Shannon cipher system with correlated source outputs and guessing wiretapper eavesdroping through a noisy channel.

- Cryptanalysis for the Shannon cipher system with noisy channel to the wiretapper guessing subject to distortion.
- The method for breaking the Shannon cipher system with correlated source outputs and wiretapper guessing subject to distortion.

The main result of the thesis are.

- The Shannon cipher system with a guessing wiretapper eavesdropping through a noisy channel is investigated. The wiretapper guessing rate of the model is estimated. The system model and the problem were suggested by Merhav and Arikan [1,3].
- The Shannon cipher system with correlated source outputs and guessing wiretapper eavesdroping through a noisy channel is studied. The strategy for wiretapper is constructed and the guessing rate is estimated. Modification of the system model and the definition of the wiretapper guessing rate have been given by E. Haroutunian and the author [2,4].
- The Shannon cipher system with noisy channel to the wiretapper guessing subject to distortion criterion is researched. The lower and upper bounds for Δ-achievable guessing rate are obtained. The considered cipher system model and the problem of estimating the security level of system has been suggested by E. Haroutunian and the author [5,6].
- The Shannon cipher system with correlated source outputs and wiretapper guessing subject to distortion is investigated. The Δ admissible strategy for breaking the system by the guessing at key or plaintext is contracted. The lower and upper bounds the wiretapper Δ-achievable guessing rate are obtained. The system model has been suggested by the author [7].

Тигран Мелконович Маргарян

ИССЛЕДОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ШЕННОНОВСКОЙ СЕКРЕТНОЙ СИСТЕМЕ

РЕЗЮМЕ

Диссертация посвящена исследованию шенноновских секретных систем с угадывающим нарушителем. В данной работе автором и руководителем предложена модификация моделей секретных систем. Для каждой системы наиболее важным вопросом является оценка надежности относительно аттак подслушивателя.

Теоретическая секретность модели секретной системы Шеннона традиционно измеряется неопределенностью (энтропией). В большинстве работ в этой области предполагается, что подслушиватель имеет в точности один шанс оценить текст. Шеннон также дал идею практичекой секретности, которая представляется средним количеством работы, требуемой для взлома ключа. Хеллман продвинулся на шаг вперед в изучении практической секретности, предложив измерять степень безопасности секретной шифра системы в терминах математического ожидания числа ключ-сообщения комбинаций, которые требуются для раскрытия зашифрованого сообщения. Мерхов и Арикан предложили другой критерий безопасности, экспоненту угадывания, для шенноновской секретной системы, при которой нарушителю разрешается иметь много попыток реконструкции текста. Е. Арутюнян исследовал систему применением первого момента скорости угадывания добавив требование надежности.

В диссертации скорость угадывания нарушителем (Δ-достижимая скорость угадывания) определяется как ожидаемое число попыток для взлома секретной системы. Четыре модели секретных систем были изучены и уровень безопасности систем оценен с использованием методов теории информации, в частности методы типов. Стратегии для взлома секретной системы путем угадывания ключа или сообщения построены. Важность рассмотренных обобщений шенноновских секретных систем с угадывающим нарушителем может обьясняться тем, что практически более вероятно, что нарушитель может наблюдать зашумленную версию крипограммы. С другой стороны, часто нарушителю разрешается восстанавливать текст с заданным искажением.

Положения, выносимые на защиту.

- Стратегия для взлома шенноновских секретных систем с угадывающим нарушителем, подслушивающим через канал с шумом.
- Криптоанализ для шенноновских секретных систем с коррелированными сообщениями источника и угадывающим нарушителем, подслушивающим через канал с шумом.

- Криптоанализ для шенноновских секретных систем с зашумленным каналом и нарушителем угадывающей с заданным уровнем искажения.
- Метод для взлома шенноновских секретных систем с коррелированными сообщениями источника и нарушителем угадывания с искажениями.

Основные результаты диссертации.

- Исследована шенноновская секретная система с угадывающим нарушителем, подслушивающим через канал с шумом. Оценена скорость угадывания нарушителем в модели. Модель системы и проблема предложены Мерхавом и Ариканом [1,3].
- Изучена шенноновская секретная система с коррелированными сообщениями источника и угадывающим нарушителем, подслушивающим через канал с шумом. Построена стратегия нарушителя и оценена стратегия угадывания. Модификация модели системы и определение скорости угадывания нарушителя даны Е. Арутюняном и автором [2,4].
- Исследована шенноновская секретная система с зашумленным каналом и нарушителем угадывающей с заданным уровнем искажения. Получена верхняя и нижняя оценки для Δ-достижимой скорости угадывания. Рассматриваемая секретная система и проблема оценки уровня системы были предложены Е. Арутюняном и автором [5,6].
- Шенноновская секретная система с коррелированными сообщениями источника и нарушителем угадывания с искажениями. Построена Δ-приемлемая стратегия для взлома системы угадыванием ключа или текста. Получены верхняя и нижняя границы Δ-достижимой скорости угадывания. Модель системы предложена автором [7].