ՀՏԴ 004.312.26.02

Տ.Ա. ԲԱՂԴԱՍԱՐՅԱՆ

ԳԱՂՏՆԻՔԻ ԲԱՇԽՄԱՆ ՍԽԵՄԱՅԻ ՕՊՏԻՄԱԼ ՇԵՄԻ ԸՆՏՐՈՒԹՅԱՆ ՄԵԹՈԴ: ՇԵՄԻ ՍԱՀՄԱՆԱՅԻՆ ԱՐԺԵՔՆԵՐԻ ՈՐՈՇՈՒՄԸ

Մշակվել է գաղտնիքի բաշխման շեմային սխեմաների օգտագործման պայմաններում օպտիմալ շեմի ընտրության մեթոդ: Մեթոդի հիմքում ընկած են շեմային սխեմաների պաշտպանվածության գնահատման երկու հավանականային չափանիշները՝ գաղտնիքի բաղադրամասի բացահայտման և կորստի և/կամ վնասման հավանականություն: Որպես շեմային սխեմայի օրինակ օգտագործվել է Շամիրի շեմային սխեման:

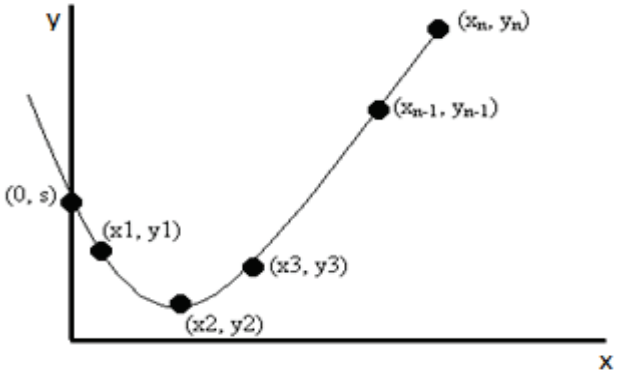
Առանցքային բառեր. գաղտնիքի բաշխում, շեմային սխեմա, օպտիմալ շեմ, Շամիրի սխեմա:

Գաղտնիքի բաշխման արձանագրությունները, որոնք անվանվում են նաև գաղտնիքի բաշխման սխեմաներ, գաղտնագրության շատ կարևոր մի ուղղություն է, որը արագ կերպով զարգանում է վերջին տարիների ընթացքում: Իրենց էությամբ գաղտնիքի բաշխման սխեմաները բազմակողմանի արձանագրություններ են, որոնց ֆունկցիան գաղտնի բանալիների կամ գաղտնաբառերի հաստատումն է: Բանալիների հաստատում ասելով հասկանում ենք գործընթաց կամ կիրառական արձանագրություն, որի կատարման արդյունքում ընդհանուր գաղտնիքը (բանալի, գաղտնաբառ և այլն) դառնում է հասանելի միայն որոշ թվով սուբյեկտների, ինչը թույլ է տալիս ապահովել անհրաժեշտ մակարդակի գաղտնագրային պաշտպանություն: Ի սկզբանե գաղտնիքի բաշխման սխեմաներն օգտագործվում էին միայն բանալիների բաշխման և/կամ նրանց ռեզերվային օրինակների ստեղծման համար [1], սակայն այդ սխեմաները կարող են արդյունավետ օգտագործվել նաև ցանկացած տեսակի այլ գաղտնի տեղեկատվության պաշտպանության համար: Գաղտնիքի բաշխման սխեմաները պարտադիր պիտի բավարարեն հետևյալ պայմանները.

1. Ի սկզբանե տրված քանակով մասնակիցները կարող են միարժեք վերականգնել սկզբնական ընդհանուր գաղտնիքը:
2. Տրված քանակից քիչ քանակությամբ ցանկացած մասնակիցների խումբ չի կարող վերականգնել սկզբնական ընդհանուր գաղտնիքը:
3. Մասնակիցներից ոչ մեկի մի առանձին բաղադրամասը որևէ տեղեկություն չի կարող տալ ընդհանուր գաղտնիքի մասին:

Գաղտնիքի բաշխման այն սխեմաները, որոնց դեպքում գոյություն ունի վերականգնելու համար անհրաժեշտ և բավարար մասնակիցների քանակ, կոչվում են գաղտնիքի բաշխման շեմային սխեմաներ [2]: (M,N) - S գաղտնիքի բաշխման շեմային սխեմա է կոչվում այն սխեման, երբ գաղտնիքը բաժանվում է N բաղադրամասի, որտեղ M≤N, այնպես որ միայն M հատ բաղադրամաս կարող են վերականգ-

նել S գաղտնիքը, իսկ ցանկացած M-1 հատ բաղադրամաս ոչ մի տեղեկություն չեն տալիս S-ի մասին: Շեմային սխեմայի դասական օրինակ է Շամիրի շեմային սխեման [2]: Գաղափարը, որի վրա հիմնված է տվյալ սխեման այն է, որ k-րդ կարգի բազմանդամի միջարկման համար անհրաժեշտ է ունենալ առնվազն k+1 արժեք: Եթե հայտնի են k+1 քանակից ավելի քիչ քանակությամբ արժեքներ, ապա միջարկումը անհնար կլինի: Օրինակ՝ քառակուսային հավասարման դեպքում, երբ k=2, հավասարման գրաֆիկը (նկ. 1) կառուցելու համար անհրաժեշտ է առնվազն 3 կետ:



Նկ. 1. $y = a_3 * x^2 + a_2 * x + a_1$ *հավասարման գրաֆիկը*

Այս դեպքում հավասարման ազատ անդամը (f(0)) հանդես է գալիս որպես գաղտնիք, իսկ (x,y) արժեքների զույգերը՝ որպես գաղտնիքի բաղադրամասեր: Գաղտնիքի արժեքը վերականգնելու համար անհրաժեշտ է կիրառել Լագրանժի միջարկման բազմանդամը [3], որում տեղադրելով հայտնի զույգ արժեքները (բաղադրամասերը) վերականգնվում է սկզբնական հավասարումը:

Ակնհայտ է, որ կոնկրետ նկարագրված դեպքում գաղտնիքի արժեքը ստանալու համար բավարար է օգտագործել 3 զույգ արժեքներ, սակայն ընդհանուր բաղադրամասերի քանակը կարող է լինել անվերջ մեծ, քանի որ հավասարման գրաֆիկի վրա կարելի ստանալ անվերջ քանակությամբ արժեքներ:

Այսինքն, միևնույն գաղտնիքը բաշխելու համար կարելի է ունենալ M-ի և N-ի բավականին տարբեր արժեքներ, օրինակ՝

- M=3, N=5,
- M=10, N=20,
- M=2, N=30,
- M=50, N=100,
- և այլն:

Հարց է առաջանում, թե ինչպիսին պետք է լինեն այդ արժեքները: Այսպիսով, ձևակերպվում է գաղտնիքի բաշխման շեմային սխեմայի օպտիմալ շեմի ընտ-

րության խնդիրը: Այդ խնդիրը լուծելու համար առաջին հերթին հարկավոր է ձևակերպել, թե ինչ է նշանակում օպտիմալ շեմ և ինչպես կարելի է այն գնահատել: Վերը նշված օրինակներից միարժեքորեն պարզ չէ, թե, օրինակ, (M=3,N=5) շեմն է պետք օգտագործել, թե (M=10,N=20) շեմը, ինչպես նաև հայտնի չէ՝ որն է դրանցից ավելի արդյունավետ և որքանով: Բաշխման սխեմայի շեմը գնահատելու համար հարկավոր է ներմուծել արդյունավետության գնահատական: Ընդհանրապես, տեղեկատվության պաշտպանություն ապահովող համակարգերի արդյունավետության ամենակարևոր գնահատականը համակարգի գաղտնակայունությունն է, հետևաբար, շեմային սխեմայի շեմի օպտիմալության գնահատականը ուղիղ կերպով կախված է սխեմայի գաղտնակայությունից: Գաղտնագրային համակարգերի գաղտնակայունությունը իր հերթին որոշվում է հակառակորդի կոնկրետ համակարգի վրա իրականացվող գրոհների արդյունքներով, և թե որքան ժամանակում այդ գրոհների արդյունքում հակառակորդը կարող է «կոտրել» համակարգը և տիրանալ գաղտնի տեղեկատվությանը:

Գաղտնիքի բաշխման սխեմաները, մասնավորապես աշխատանքում օգտագործվող Շամիրի շեմային սխեման, ունեն տեսականորեն անվտանգության հատկություն (information-theoretic security [4]), ինչը նշանակում է, որ երբ գաղտնիքի և դրա բաղադրամասերի չափսերը համընկնում են, հակառակորդը չի կարող կոտրել համակարգը նույնիսկ անսահմանափակ ռեսուրսների միջոցով (այդպիսի գաղտնագրային համակարգի օրինակ է միանգամյա նոթատետրը [4]): (M,N) շեմային սխեմայի պաշտպանվածությունը գնահատելու համար նշենք այնպիսի պայմաններ, որոնց դեպքում համակարգի աշխատանքը կխափանվի, և գաղտնիքի գաղտնիության, հասանելիության կամ ամբողջականության հատկությունները այլևս չեն պահպանվի.

1. Հակառակորդին հաջողվում է բացահայտել գաղտնիքի առնվազն M բաղադրամաս:
2. Որոշակի պատճառներով վնասվում են կամ անհասանելի են դառնում գաղտնիքի N-M+1 բաղադրամաս:

Նկարագրված երկու դեպքում էլ համակարգի պաշտպանվածությունը կխափանվի: Առաջին տարբերակի դեպքում գաղտնիքը կբացահայտվի հակառակորդի կողմից, իսկ երկրորդ տարբերակում գաղտնիքը այլևս հասանելի և ամբողջական չի լինի օրինական օգտագործողի համար: Այսպիսով, կարելի է ձևակերպել բաշխման սխեմայի պաշտպանվածության երկու հավանականային գնահատական՝

1. M հատ բաղադրամասի բացահայտվելու հավանականություն ($P_բ$),
2. N-M+1 հատ բաղադրամասի վնասվելու և/կամ կորստի հավանականություն ($P_կ$):

Շեմային սխեմայի օպտիմալ շեմի ընտրության համար հարկավոր է ունենալ մոդել և կառուցել երկու ֆունկցիա՝

1. $F_բ$ (M,N), որը կնկարագրի $P_բ$ հավանականության կախվածությունը շեմից,
2. $F_կ$ (M,N), որը կնկարագրի $P_կ$ հավանականության կախվածությունը շեմից:

Քննարկենք M և N արժեքների մի քանի սահմանային դեպք.

- M=2, N>>2: Այս դեպքում, քանի որ գաղտնիքը վերականգնելու համար անհրաժեշտ բաղադրամասերի քանակը նվազագույնն է, ապա $P_բ$ -> 1, իսկ $P_կ$->0 քանի որ մեծ քանակությամբ բաղադրամասերից շատ դյուրին է գտնել մեկ անվնաս զույգ: Ընդհանուր առմամբ այսպիսի շեմը կարելի է գնահատել ոչ օպտիմալ, քանի որ հակառակորդի կողմից բացահայտվելու հավանականությունը բարձր է:
- M=N: Այս տարբերակի դեպքում ակնհայտ է, որ հակառակորդի համար շատ ծանր է բացահայտել բոլոր բաղադրամասերը, երբ նույնիսկ մեկ հատի բացակայության դեպքում նա չի կարող բացահայտել բաշխված գաղտնիքը, այսինքն $P_բ$ -> 0: Սակայն, միևնույն ժամանակ, բարդանում է նաև իրավական օգտագործողի խնդիրը, քանի որ նույնիսկ մեկ բաղադրամասի վնասվելու կամ կորստի դեպքում գաղտնիքը այլևս հասանելի չի լինի, հետևաբար՝ $P_կ$->1: Այս դեպքում ևս շեմը կարելի է գնահատել ոչ օպտիմալ, քանի որ հակառակորդի կողմից բացահայտվելու հավանականությունը շատ ցածր է, սակայն բարձր է բաղադրամասերից որևէ մեկի վնասվելու կամ կորստի արդյունքում իրավական օգտագործողին գաղտնիքի հասանելի չլինելու հավանականությունը:

Այսպիսով, աշխատանքի արդյունքում ձևակերպվեցին գաղտնիքի բաշխման շեմային սխեմաների պաշտպանվածության գնահատման հավանականային երկու չափանիշներ, որոնց միջոցով գնահատվեցին օպտիմալ շեմի ընտրության մոդելի սահմանային արժեքները: Ճշգրիտ մոդելի ստացման արդյունքում հնարավոր կդառնա ստանալ շեմի օպտիմալ արժեքներ, միևնույն ժամանակ ներառելով նաև արտաքին չափանիշներ, ինչպիսին է բաշխվող տեղեկատվության գաղտնիության մակարդակը (օրինակ՝ ցածր, միջին, միջին բարձր, բարձր, խիստ բարձր):

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Schneier, Bruce.** Applied Cryptography. - 1994.
2. **Shamir, Adi**. How to share a secret. - 1979.
3. http://mathworld.wolfram.com/LagrangeInterpolatingPolynomial.html
4. http://web.mit.edu/6.857/OldStuff/Fall97/lectures/lecture2.pdf

Т.А. БАГДАСАРЯН

МЕТОД ВЫБОРА ОПТИМАЛЬНОГО ПОРОГА ДЛЯ СХЕМЫ РАСПРЕДЕЛЕНИЯ СЕКРЕТА. ОПРЕДЕЛЕНИЕ ГРАНИЧНОГО ЗНАЧЕНИЯ ПОРОГА

Разработан метод выбора оптимального порога для систем распределения секрета. Метод основан на двух вероятностных критериях оценки защищенности пороговых схем распределения секрета: вероятности раскрытия частей секрета и вероятности потери и/ или искажения частей секрета. В качестве примера использована пороговая схема Шамира.

Ключевые слова: распределение секрета, пороговая схема, оптимальный порог, схема Шамира.

T.A. BAGHDASARYAN

THE OPTIMAL THRESHOLD SELECTION FOR SECRET SHARING SCHEMES. DETERMINING THE BOUNDARY VALUE OF THE THRESHOLD

A method for optimal threshold selection is proposed for systems in which secret sharing schemes are used. The method is based on two probabilistic criteria of the secret sharing threshold scheme security assessment. These criteria are the probability of the share disclosure and the probability of the share loss and/or distortion. Shamir's threshold scheme is used as an example.

Keywords: secret sharing, threshold scheme, optimal threshold, Shamir's scheme.

ՀՏԴ 005.312.26

Վ.Հ. ՀՈՎՍԵՓՅԱՆ

ՇԱՐԺԱԿԱՆ ԲԱՆԱԼՈՒ ԿԻՐԱՌՈՒՄԸ ԱՄՊԱՅԻՆ ՄԻՋԱՎԱՅՐՈՒՄ

Մշակված է գաղտնագրման համակարգ՝ շարժական բանալու ստեղծմամբ, որն ապահովում է տվյալների անվտանգ տեղափոխումը: Շարժական բանալի է անլար ցանցի ցրիչը, որը մշակելով փոխանցվող փաթեթը, գաղտնագրում է այն: Առաջարկված համակարգը հարմար է կիրառել այն ցանցային միացումների դեպքում, որտեղ բացակայում է գաղտնագրումը: Ներկայացված է տվյալների փոխանցման անվտանգությունն ապահովող նոր սկզբունք:

Առանցքային բառեր. գաղտնագրում, անլար ծածկույթ, շարժական բանալի, անվտանգ համացանց:

Ներածություն: Աշխարհում գոյություն ունեն ավելի քան 7.5 միլիարդ սարքեր, որոնք կապված են համացանցին ուղղակի կամ միջանկյալ սարքերով: Արդեն իսկ նոր սերնդի հեռախոսների քանակը գերազանցել է երկրում ապրող մարդկանց քանակը: Ըստ բազմաթիվ հեղինակավոր ընկերությունների, որոնցից են Intel,