უაკ 68Q20

ინფორმაციის შეკუმშვის ერთი სქემის განხილვა კრიპტოგრაფიული უზრუნველყოფის თვალსაზრისით

თეიმურაზ ქოჩლაძე, ნოდარ ნანობაშვილი
თსუ. მათემატიკური კიბერნეტიკის კათედრა, თბილისი, უნივერსტეტის ქ.2

ანოტაცია

სტატიაში განიხილება ინფორმაციის შეკუმშვის ერთი კომბინატორული სქემა და მისი გამოყენება ინფორმაციის დაშიფრვის ამოცანებში. ინფორმაციის შეკუმშვის მოცემული სქემა კომპლექსურად ასახავს ინფორმაციის დაშიფრვის შესაძლებლობას. იმის და მიხედვით, თუ როგორ ხასიათს ატარებს შეტყობინება, შესაძლებელია მისი ორ ფორმაში წარმოდგენა: შეკუმშული ან გაფართოვებული. მიღებული შედეგი ატარებს შემთხვევით ხასიათს. შესაძლებელია შეტყობინების ისეთნაირი დამუშავება და გარდაქმნა, რომ ერთდროულად რეალიზებული იყოს შეკუმშული ინფორმაციის კრიპტოგრაფიული ეფექტი, რაც მკვეთრად ართულებს ინფორმაციის გაშიფრვის შესაძლებლობას.

საკვანძო სიტყვები: *კრიპტოგრაფია, ინფორმაციის დაცვა, ინფორმაციის შეკუმშვა, ინფორმაციის ჩაძირვა, კრიპტოსისტემის მდგრადობა, კომბინატორული მეთოდი.*

განვიხილოთ ინფორმაციის შეკუმშვის ფორმალური სქემა. დავუშვათ მოცემულია m ცალი $n+1$ სიგრძის მოუწესრიგებელი ბინარული ვექტორები:

$$A_1 = (a_n^1;\ a_{n-1}^1;\ \dots\ a_o^1)$$

$$A_2 = (a_n^2;\ a_{n-1}^2;\ \dots\ a_o^2)$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$A_m = (a_n^m;\ a_{n-1}^m;\ \dots\ a_o^m)$$

სადაც $a_i^j \in \{0,1\};\quad i = 0 \dots n;\quad j = 1 \dots m;$

$\{A_1\ A_2\ \dots\ A_m\}$ ვექტორების უშუალო შენახვა და გადაცემა მოითხოვს $m(n+1)$ ბიტს.

განვიხილოთ თეორიული მეთოდი, რომელიც საშუალებას მოგვცემს m მოუწესრიგებელი ბინარული ვექტორის შესანახად და გადასაცემად შემოვიფარგლოთ გარკვეული „სახის" არჩევით, რომლის სიგრძე L ბიტებში გამოისახება შემდეგნაირად:

$$L \langle \begin{cases} m(n+1)-(m+1)+2^{\alpha} & \text{თუ} \quad \alpha < n+1 \\ \alpha\ (\alpha - n + 1) + m & \qquad\quad \alpha > \alpha + 1 \end{cases}$$

სადაც $a = 2^{n+1} - 1$, α არის ხარისხის უდიდესი ძაჩვენებელი m -ის ხარისხებად დაშლის დროს.

ვექტორები $(A_1\ A_2\ \dots\ A_m)$ შეიძლება განვიხილოთ როგორც ორობითი ჩანაწერი შემდეგი რიცხვებისა:

$$A_1 = 2^n \cdot a_n^1 + 2^{n-1} \cdot a_{n-1}^1 + \dots + a_0^1$$

$$A_2 = 2^n \cdot a_n^2 + 2^{n-1} \cdot a_{n-1}^2 + \dots + a_0^2$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$A_m = 2^n \cdot a_n^m + 2^{n-1} \cdot a_{n-1}^m + \dots + a_0^m$$

შემდგომში $A_1\ A_2\ \dots\ A_m$ ჩანაწერის ქვეშ ჩვენ ვიგულისხმებთ ამ ვექტორების რიცხვით (სკალარულ) მნიშვნელობას.

წინასწარ მოვახდინოთ $A_1\ A_2\ .\ .\ .\ A_m$ რიცხვების მოწესრიგება შემდეგი სახით, დავუშვათ:

$A_1 \le A_2 \le . . . \le A_m$

თუ ეს პირობა სრულდება, შეიძლება ითქვას რომ მიმდევრობა $A_1\ A_2\ .\ .\ .\ A_m$ ნაწილობრივ მოწესრიგებულია.

შემოვიტანოთ ფუნქცია

$$f\ (A_1\ A_2\ \ldots\ A_m) = C^{m}_{A_{m+m-1}} + C^{m-1}_{A_{m+m-2}} + \ldots + C^{1}_{A}$$

სადაც

$$C^{j}_{i+j-1} = \frac{(i+j-1)\,(i+j-2)\ldots i}{j!}$$

$f\ (A_1\ A_2\ .\ .\ .\ A_m)$ ფუნქციის ინექტიურობიდან გამომდინარეობს, რომ ნებისმიერი $K=f\ (A_1\ A_2\ .\ .\ .\ A_m)$ ნატურალური რიცხვისათვის არსებობს ერთადერთი რიცხვითი მიმდევრობა რომელიც აკმაყოფილებს პირობას:

$$A_1 \le A_2 \le . . . \le A_m$$

ანუ, თუ ინმფორმაციის შეკუმშვის სქემას განვსაზღვრავთ $f\ (A_1\ A_2\ .\ .\ .\ A_m)$ ფუნქციის საშუალებით, ეს გარდაქმნა იქნება ცალსახა და შესაძლებელი იქნება ინფორმაციის ცალსახად აღდგენა. $f\ (A_1\ A_2\ .\ .\ .\ A_m) = K$ რიცხვს ვუწოდოთ $A_1\ A_2 \ldots A_m$ მიმდევრობის "სახე".

აღწერილ მეთოდს სიმარტივისათვის ვუწოდოთ ინფორმაციის შეკუმშვის კომბინატირული მეთოდი ან უბრალოდ კომბინატირული მეთოდი. კომბინატორული მეთოდით ინფორმაციის შეკუმშვა არის მარტივი და პირდაპირი, იგი არ მოითხოვს წინასწარ სტატისტიკურ შესწავლას და დამატებით ხელოვნურ მეთოდებს, თუმცა ინფორმაციის ნაწილობრივ მოწესრიგებულობის მოთხოვნა მეთოდის პრაქტიკული გამოყენებისათვის საკმაო სირთულეებს წარმოქმნის. განვიხილოთ მაგალითი:

დავუშვათ, ინფორმაციის წყაროდან შემოდის შემდეგი სახის ბინარული მიმდევრობა:

1 0 0 1 1 1 1 0 0 1

ინფორმაციის ჩასაწერად საჭიროა *11* ბიტი. კომბინატორული მეთოდის გამოყენებისათვის საჭიროა ინფორმაციის წინასწარ მოწესრიგება. ბინარული მიმდევრობის მოსაწესრიგებლად გამოვიყენოთ შემდეგი მარტივი მეთოდი: მიმდევრობა დავყოთ ვექტორებად „ერთიანიდან ერთიანამდე", ისე რომ ყოველი შემდეგი ვექტორის შესაბამისი რიცხვითი მნიშვნელობა მეტი ან ტოლი იყოს წინა ვექტორის რიცხვით მნიშვნელობაზე .

1 ; 100; 111; 1001.

შევუსაბამოთ თითოეულ ქვემიმდევრობას რიცხვითი მნიშვნელობა:

$a_1=1;\ a_2=4;\ a_3=7;\ a_4=17;$

მიღებული ვექტორების სისტემის შესაკუმშად გამოვიყენოთ კომბინატორული მეთოდი.

$$f\ (1,4,9,17)=4940$$

$$4940 \rightarrow 10001101001100$$

f(1,4,9,17)=4940 როგორც მიღებული შედეგიდან ვხედავთ „სახის" ჩასაწერად საჭიროა უფრო მეტი ბიტი ვიდრე გამოყენებული იყო საწყის ბინარული მიმდევრობის ჩასაწერად. თუ დავაკვირდებით კომბინატორული მეთოდს, ვნახავთ რომ შეკუმშულ ვექტორთა სისტემას აქვს შემდეგი სახე:

$a_1=1 \rightarrow 0001;\ \ a_2=4 \rightarrow 0100;\ \ a_3=7 \rightarrow 0111;\ \ a_4=17 \rightarrow 1001;$

კომბინატორული მეთოდით მოხდა სწორედ ამ ვექტორთა სისტემის შეკუმშვა, რომლის ჩასაწერადაც საჭიროა 16 ბიტი. როგორც მაგალითიდან ჩანს, ვექტორთა სისტემის მოწესრიგებისას საწყის შესაკუმშ ინფორმაციაში გაჩნდა „დამატებითი ინფორმაცია“ და მხოლოდ შემდეგ მოხდა შეკუმშვა. სწორედ ამან გამოიწვია ის, რომ მიღებული შედეგი მოითხოვს უფრო მეტი ბიტებს რაოდენობას ჩასაწერად, ვიდრე საწყისი. შეკუმშვის თვალსაზრისით ესეთი შედეგი მიუღებელია, მაგრამ ინფორმაციის დაცვის ამოცანებში ასეთი შედეგი საკმაოდ საინტერესოა.

კომბინატორული მეთოდის ეს თვისება კრიპტოგრაფიის ამოცანებისათვის საკმაოდ მოხერხებულია. ცნობილია, რომ მეთოდის მდგრადობის ასამაღლებლად გამოიყენება ინფორმაციის შეკუმშვა და ჩაძირვა, ანუ კრიპტოსისტემა ცვლის დასაცავი ინფორმაციის მიცულობას. როგორც წესი, შეკუმშვა ან ჩაძირვა ხდება განსაზღვრული წესით და წინასწარ ცნობილი შედეგით. კომბინატორული მეთოდის შემთხვევაში შედეგი წინასწარ ცნობილი არ არის და რა მოხდება – ჩაძირვა თუ შეკუმშვა - დამოკიდებულია ინფორმაციის მოწესრიგების მეთოდზე.

$$f\ (A_1\ A_2\ \dots\ A_m) = k_1 C^m_{A_{m+m-1}} + k_2 C^{m-1}_{A_{m+m-2}} + \dots + k_m C^1_A$$

ეს გამოსახულება შეიძლება აღვიქვათ როგორც $A_1\ A_2\ .\ .\ .\ A_m$ მიმდევრობის დაშიფრვა $k_1\ k_2\ .\ .\ .\ .\ k_m$ გასაღების საშუალებით.

როგორც აღვნიშნეთ, მოხდება შეკუმშვა თუ ჩაძირვა, დამოკიდებულია ინფორმაციის მოწესრიგების მეთოდზე. განვიხილოთ კიდევ ერთი მაგალითი:

დავუშვათ შესაკუმშია მიმდევრობა:

00100110101011001111

მოწესრიგების მიზნით მოცემული მიმდევრობა გავყოთ ორ მონოტონურ ქვემიმდევრობად:

0010,0110,1010, (12 ბიტი) და *1, 100, 1111 (8 ბიტი).*

კომბინატორული მეთოდით გადავსახოთ ორივე მიმდევრობა:

f(2,6,10)=137→10001001 (7 ბიტი)

f(1,3,15)=462→111001110 (9 ბიტი)

როგორც მაგალითიდან ჩანს ერთი მიმდევრობა შეიკუმშა, ხოლო მეორე გაფართოვდა და ეს გამოიწვია მოწესრიგების განსხვავებულმა მეთოდმა.

კომბინატორული მეთოდის გამოყენება კრიპტოგრაფიის ამოცანებში შეიძლება ჩავთვალოთ კ. შენონის იდეის რეალიზაციად, რომლის თანახმადაც ინფორმაციის შეკუმშვა ან გაფართოვება ამაღლებს კრიპტოსისტემის მდგრადობის ხარისხს: შეკუმშვა იწვევს საწყისი ინფორმაციის სტატისტიკის წაშლას, ხოლო გაფართოვება იწვევს განუზღვრელობის ხარისხის ზრდას ინფორმაციის გაშიფრვისას.

გამოყენებული ლიტერატურა:

1. Дж. Риордан. «Введение в комбинаторный анализ» Издательство иностранной литературы. Москва 1963.
2. К. А. Рыбников «Введение в комбинаторный анализ» Издательство Московского Университета. 1985.
3. К. Шенон. «Работы по теории информации и кибернетике» Издательство иностранной литературы. Москва 1963.

Article received: 2006-06-14