ურთიერთკომუტატიურ მატრიცათა სიმრავლის შექმნა და მისი გამოყენება ინფორმაციის დასაცავად

გულნარა კოტრიკაძე
თბილისის დავით აღმაშენებლის სახ. უნივერსიტეტი

რეზიუმე

განხილულია სხვადასხვა სახის მატრიცები: ნებისმიერი, შემთხვევითი, სიმეტრიული, ორობითი. ყველა სახის მატრიცებმა მოგვცა კარგი შედეგი. ე.ი. შეიქმნა მატრიცათა $n^2!$ სიმრავლე. ეს კი არის ძალიან დიდი რიცხვი. კრიპტოგრაფიაში 10^{30} არის ქვედა ზღვარი. მაშასადამე, მიღებული მეთოდი ხასიათდება მაღალი საიმედოობით, რაც ემყარება სიმრავლიდან მატრიცათა ამორჩევის სირთულეს.

საკვანძო სიტყვები: კრიპტოგრაფია. სიმეტრიული. ასიმეტრიული. გასაღები. დაშიფვრა. გაშიფვრა. კომუტატიურობა. მატრიცათა სიმრავლე. ძებნის ხანგრძლივობა. მედეგობა.

1. შესავალი

ინფორმაციის დაცვისათვის გამოიყენება კრიპტოგრაფიის ცნობილი სხვადასხვა სისტემები, როგორიცაა, მაგალითად სიმეტრიული და ასიმეტრიული სისტემები.

სიმეტრიული სისტემებით, ინფორმაციის გადაცემა ხდება დახურული არხით, ანუ კურიერის საშუალებით. ასიმეტრიული სისტემებით კი - ღია არხით, ანუ მესამე პირის (კურიერის) ჩარევა არ არის საჭირო. ე.ი. ინფორმაციის გაცვლის პროცესი არის ყველასათვის ხელმისაწვდომი (ღია), მაგრამ იმდენად დაცული, საიმედო და მაღალ-მედეგია, რომ შეუძლებელია მისი „გატეხვა“.

ასიმეტრიული სისტემის დიფი-ჰელმანის მეთოდის ალგორითმი ეყრდნობა GF(P) ველში ლოგარითმების გამოთვლის სირთულეს. გამოყენებულია ახარისხების ფუნქცია [1,2,]. ახარისხება ხდება x საიდუმლო რიცხვით, მოდულით p. ორივე მხარე, რომელთა შორისაც ხდება ინფორმაციის გაცვლა, იღებს ნებისმიერ საიდუმლო x_1 და x_2 რიცხვებს და ორივე მხარე სრულიად ღიად, იღებს ერთიდაიგივე K გასაღებს. შემდგომ კი, ამ გასაღებით ხდება გასაგზავნი ინფორმაციის დაშიფვრა და მიმღების მიერ კი, მიღებული დაშიფრული ინფორმაციის გაშიფვრა [2,3,4].

$$a^{X1\times X2} (\text{mod } p) = a^{X2\times X1} (\text{mod } p) = K$$

სადაც – a მთელი რიცხვია, p არის მარტივი რიცხვი, რომელიც ცნობილია ყველასათვის.

თუმცაღა, X_1 და X_2 რიცხვების ნაცვლად, თუ ავიღებთ A_1 და A_2 მატრიცებს და ახარისხების ნაცვლად გამოვიყენებთ მატრიცაზე გამრავლებას, მიიღება ახალი მეთოდი ინფორმაციის დაცვისათვის [7,8].

A_1 და A_2 მატრიცები უნდა იყოს კომუტატიური ანუ

$$A_1\times A_2 = A_2\times A_1$$

და ორივე X და Y მხარეები მიიღებენ ერთიდაიგივე K გასაღებს:

$$a^{\times A_1\times A_2} (\text{mod} p) = a^{\times A_2\times A_1} (\text{mod} p) = K$$

მაშასადამე, აღნიშნული მეთოდის შესრულებისათვის **აუცილებელი და საკმარისი პირობაა**, A_1 და A_2 საიდუმლო მატრიცების კომუტატიურობა.

2. ძირითადი ნაწილი

2.1. კომუტატიურ მატრიცათა სიმრავლის შექმნა

ამოცანა: ავაგოთ ურთიერთკომუტატიური მატრიცების სიმრავლე, საიდანაც მოხდება A_1 და A_2 მატრიცების ამორჩევა X და Y მხარეების მიერ, რათა მიიღონ ერთიდაიგივე K გასაღები, ინფორმაციის დაშიფვრა-გაშიფვრისათვის [7,8].

ამისათვის განვიხილეთ უამრავი მაგალითი, მათ შორის [6]:

1) თავიდან განვიხილეთ პატარა განზომილების მატრიცები, მაგრამ მალე დაიწყო მატრიცამ გამეორება. ე.ი. ბაზა (მატრიცათა სიმრავლე) არ იქმნებოდა;

2) შემდგომში დავაკვირდით მერამდენე მატიცაზე იწყებოდა გამეორება, თანაც ვითვლიდით, ჯამში მატრიცის ელემენტები, მოდულის გათვალისწინებით, რა რიცხვს გვაძლევდა;

3) შემდგომ კი ვცვალეთ, ხან განზომილება, ხან მოდული და ვაკვირდებოდით გამეორების პრინციპს, ანუ მერამდენე მატრიციდან იწყებოდა გამეორება. მივედით ერთ დასკვნამდე, რომ მოდულის გაზრდა უფრო კარგ და საიმედო შედეგს იძლევა ვიდრე განზომილების გაზრდა. რაც იმას ნიშნავს, რომ როცა განზომილება გავზარდეთ და მოდული იგივე დავტოვე, მატრიცა მაინც მალე გამეორდა; მაგრამ როცა განზომილება დავტოვეთ იგივე და გავზარდეთ მოდული ე.ი. მატრიცაში შემავალი ელემენტების სიდიდე, მაშინ მატრიცამ უფრო გვიან დაიწყო გამეორება. **აქედან დასკვნა**: მოდულის გაზრდა გვაძლევს უფრო კარგ შედეგს, ვიდრე განზომილების გაზრდა.

ამის შემდეგ გადავსინჯეთ სხვადასხვა განზომილებისა და მოდულის მატრიცები და მივიღეთ შემდეგი შედეგები.

2.2. ნებისმიერი სახის მატრიცები

ნებისმიერი მატრიცები, n განზომილებით და m მოდულით:

1) როცა n=4, m=5; 5^{16} – მატრიცათა სიმრავლე, გამეორება დაიწყო 1230-ე მატრიციდან;

2) n=4, m=5; გამეორება დაიწყო 1270-ე მატრიციდან;

3) n=4, m=5; გამეორება დაიწყო 1250-ე მატრიციდან.

ნებისმიერი მატრიცები, მოდულით 11:

1) n=4, m=11; 11^{16} – მატრიცათა სიმრავლე. ოთხ განზომილებიანი მატრიცების შემთხვევაში, მოდულის გაზრდამ ძალიან კარგი შედეგი მოგვცა. განმეორების აღმოჩენა ფაქტიურად შეუძლებელიც კი გახდა, რაც უკვე საკმაოდ კარგი შედეგია.

ამის შემდეგ განხილულ იქნა, ისევ ნებისმიერი სახის მატრიცები, ოღონდ სიმრავლით მიახლოებული 10^{30} რიცხვისა, რადგან ეს რიცხვი კრიპტოგრაფიაში არის ქვედა ზღვარი.

1. განზომილება n=5; მოდული d=5; სიმრავლე $N=5^{25}$; ცვალდების რაოდენობა არის 25, სიდიდით < მოდულზე.

2. განზომილება n=5; მოდული d=7; სიმრავლე $N=7^{25}$; ცვალდების რაოდენობა არის 25, სიდიდით < მოდულზე.

რაც უფრო ვზრდით მოდულის რიცხვით მნიშვნელობას, მით უფრო გვიან იწყებს მატრიცა გამეორებას. ე.ი. მოდულის ზრდასთან ერთად, გამეორების ციფრი მცირდება [5,6].

2.3. სიმეტრიული მატრიცები

განვიხილეთ სიმეტრიული მატრიცები, სიმრავლით მიახლოებული ქვემოდან 10^{30} რიცხვისა.

1. განზომილება n=4; მოდული d=5; სიმრავლე $N=5^{16}$; ცვალდების რაოდენობა არის 16, სიდიდით < მოდულზე.

2. განზომილება n=4; მოდული d=7; სიმრავლე $N=7^{16}$; ცვლადების რაოდენობა არის 16, სიდიდით < მოდულზე.

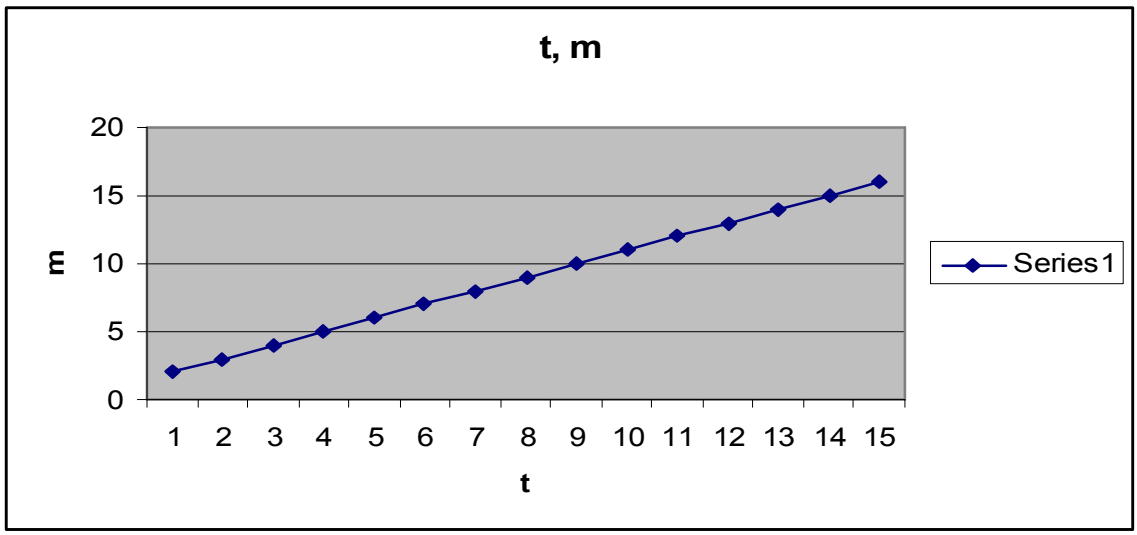
მიღებულია კარგი შედეგი, მატრიცები თანდათან გვიან იწყებს გამეორებას, მოდულის ზრდასთან ერთად [6].

2.4. ორობითი მატრიცები

ახლა განვიხილოთ ნებისმიერად აღებული ორობითი მატრიცები.

მაგალითად, განზომილება n = 10; მოდული p = 2. ე.ი. 2^{10*10} – მატრიცათა სიმრავლე. მატრიცაში შემავალი ცვლადები რაოდენობრივად იქნება 10^2=100, ხოლო სიდიდით – ნაკლები მოდულზე.

მაშასადამე, როდესაც განვიხილეთ ნებისმიერი სახის მატრიცები, მატრიცათა გამეორება დაიწყო თანდათანობით საკმაოდ გვიან, მაშინაც კი როცა მოდული იყო 5 და 7. მოდულის ზრდასთან ერთად მცირდება მატრიცათა გამეორების რიცხვი და თანდათან განმეორებითი მატრიცის ამორჩევაც კი შეუძლებელი ხდება (ნახ.1)



ნახ. 1. t, m დამოკიდებულების გრაფიკი

ნახაზზე მკაფიოდ ჩანს, რომ m - მოდულის ზრდასთან ერთად პროპორციულად იზრდება t დრო, ანუ მატრიცათა სიმრავლიდან ამორჩევის დრო.

როდესაც განვიხილეთ ნებისმიერად აღებული მატრიცები, ოღონდ ორობითი, ამ შემთხვევაშიც მოდულის ზრდასთან ერთად მატრიცათა გამეორების რიცხვი მცირდებოდა [4,5,6].

3. დასკვნა

ნაშრომში შესრულებული კვლევის შედეგები შეიძლება ასე ჩამოვაყალიბოთ:

- ნებისმიერი მატრიცის შემთხვევაში, როცა m=0,1,...,10 – მატრიცაში შემავალი ელემენტებია სიდიდით (mod p), p = 10. n=6 – მატრიცის განზომილებაა, $N = m^{n\times n} = 10^{36}$ – მატრიცათა სიმრავლე.

- ორობითი მატრიცის შემთხვევაში, როცა, m=0,1 – მატრიცაში შემავალი ელემენტებია სიდიდით (mod p), p = 2. n=10 – მატრიცის განზომილებაა, $N = m^{n\times n} = 2^{100}$ – მატრიცათა სიმრავლე.

კრიპტოგრაფიაში კი 2^{100} ანუ დაახლოებით 10^{30} არის ქვედა ზღვარი, რაც იმას ნიშნავს, რომ ამ სიმრავლიდან ორი ურთიერთკომუტატიური მატრიცის ამორჩევა მესამე სუბიექტის მიერ რეალურ დროში შეუძლებელია. $t = m^{n\times n}\times N\times T$ – ძებნის (სიმრავლიდან ამორჩევის) ხანგრძლივობაა,
N – ოპერაციათა ჩატარების რიცხვი და T – კომპიუტერის დრო.

ლიტერატურა:

1. Саломаа А. Криптография с открытым ключом. Мир. М., 1996
2. Мельников В.В. Зашита информации в компьютерных системах. М., 1997
3. Анин Б.. Зашита компьютерной информации. М., 2000
4. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография, скоростные шифры. Ст-Петербург. 2002
5. Виноградов И.М. Основы теории чисел. Наука. М., 1972
6. Тараканов В.Е. Комбинаторные задачи и (0,1) матрицы. М., 1994

7. კოტრიკაძე გ. ინფორმაციის დამუშავებისა და დაცვის, მეთოდური და ალგორითმული საშუალებანი. თდასუ-ს პერ.სამეც.ჟურნ. „აღმაშენებელი", №3. თბ., 2007

8. კოტრიკაძე გ. ინფორმაციის დაცვის ასიმეტრიული სისტემის ახალი მეთოდის შემუშავება. სტუ-ს შრ.კრ. მას №1(6), 2009. გვ.60-65.

THE CREATION OF MULTITUDE OF INTER-COMMUTATIVE MATRIX AND ITS USAGE FOR DEFENSE OF INFORMATION

Kotrikadze Gulnara
Tbilisi David Aghmashenebeli University

Summary

In the article shortly is discussed cryptography, privately, the method of Dipi-Helman in asymmetrical system. But in it making the degrees is changed by multiplication of matrix. It is caused because of that, that making the degrees for finding the key takes more time, than multiplication of matrix, and it gives us reliable result. Besides, it is necessary and enough a matrix to be commutative or inter-modifying for getting the same key for both sides. Matrix must be quadratic, otherwise commutation will be abolished. The Matrix is chosen from available matrix multitude and everybody knows about it beforehand. There had been examined various matrices: arbitrary, accidental, symmetrical, bisectional. If we discuss symmetrical matrix, by it we get two kinds of matrices: the half part of the multitude is symmetrical to X axis, the second part is symmetrical to Y axis. The matrix fields is got by the same way, what is very important. Every kind of matrix gave us good result. The matrixes began the repetition very late, and that means that was created the multitude of matrixes. The multitude is defined by the formula $M^{(n\times n)}$. As big is the space as good result is made. 10^{30} is so big number, that choosing the matrix from such multitude in real time is impossible.

СОЗДАНИЕ МНОЖЕСТВА ВЗАИМОКОММУТАЦИОННЫХ МАТРИЦ И ЕГО ИСПОЛЬЗОВАНИЕ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Котрикадзе Г.
Тбилисский Университет им. Давида Агмашенебели

Резюме

В статье обозревается криптография, а в частности метод Дифи-Гельмана асимметрических систем, только функция возведения в степень заменяется умножением на матрицу. Для возведения в степень требуется больше времени, чем для умножения на матрицу во время получения ключей, что дает надежный результат. Кроме этого, для того чтобы обе стороны получили одинаковый ключ, обязательно чтобы матрицы были коммутативными или же взаимопересадочными. Конечно же, матрицы должны быть квадратными, в противном случае, коммутативность будет расторгнута. Выбор матриц известен всем заранее и доступен всем из множества матриц. Были разобраны разные виды матриц: любая, случайная, симметрическая, двоичная. Если возьмем симметрические матрицы, получим два вида матриц: половина множества симметрична Х оси, а половина – У оси, и что очень важно, также получаем поле матриц. Все виды матриц дали хороший результат. Матрицы стали повторяться позднее, а это означает, что создалось множество матриц. Множество определяется формулой $M^{(n\times n)}$. Чем больше модуль и пространство, тем лучше полученный результат. 10^{30} – это настолько большая цифра, что выбор матриц из такого множества матриц, невозможнен в реальном времени.