Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):1-10
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

THE GENERALIZED METHOD OF GENERATION OF ABELIAN MATRIX MULTIPLICATIVE FINITE FIELD AND A NEW ONE-WAY MATRIX FUNCTION

R.Megrelishvili, M. Jinjikhadze
Tbilisi Iv. Javakhishvili's house State University, Tbilisi, Georgia
Akaki Tsereteli State University, Kutaisi, Georgia

ABSTRACT. This paper presents an original one-way matrix function and a generalized method of generating its appropriate high-order finite matrix field. The general algorithm for building primitive matrix elements through the insertion-extension method is discussed.

ანოტაცია - ნაშრომში განხილულია ორიგინალური მატრიცული ცალმხრივი ფუნქცია და მისი შესაბამისი მაღალი რიგის მატრიცული სასრული ველის გენერაციის განზოგადებული მეთოდი. განხორციელებულია ველის პრიმიტიული ელემენტების აგების ჩასმა–გაფართოების მეთოდის ზოგადი ხერხი.

Аннотация. В данной работе рассмотрена оригинальная однонаправленная функция и соответствующий ей обобщенный метод генераций конечного матричного поля высокого порядка. Представлен обобщенный алгоритм построения примитивных матричних элементов методом вставки-расширения.

KEYWORDS: მატრიცული ცალმხრივი ფუნქცია, აბელის სასრული ველი, ასიმეტრიული კრიპტოგრაფია, მაღალი რიგის მატრიცული სასრული ველი.

შესავალი

ნაშრომის ძირითად მიზანი მდგომარეობს მაღალი რიგის მტარიცების მულტიპლიკაციური კომუტაციური ჯგუფის აგებაში. ჩვენს წინაშე მდგომი ამოცანა მათემატიკურად სავსებით აქტუალურია, მითუმეტეს, ბოლო პერიოდის კვლევები მიუთითებს, რომ გარკველი კრიპტოგრაფიული ამოცანების გადასაწყვეტად ანალოგიური სტურქტურების გამოყენებისადმი ინტერესი გაიზარდა. ჩვენს კონკრეტულ მიზანს კი წარმოადგენს ორიგინალური მატრიცული ცალმხრივი ფუნქციისათვის მაღალი სიძლავრის მქონე მატრიცული სიმრავლით უზრუნველყოფა.

საქმე ეხება ღია არხით კრიპტოგრაფიული გასაღების გაცვლის სწრაფმოქმედ მატრიცულ ფუნქციასა და ალგორითმს [1].

ჩანაფიქრის მიხედვით, ახალი ალგორითმის სწრაფმოქმედება დაახლოებით ისეთივეა, როგორიც შიფრაციისა და დეშიფრაციის სიმეტრიული სისტემების კრიპტოგრაფიულ ალგორითმებს აქვთ. ამ მიზნის წარმოქმნა დაკავშირებულია არსებულ გლობალურ პრობლემასთან, რომლის მიხედვითაც ჯერჯერობით არ არსებობს მოქმედი ასიმეტრიული სისტემა, რომელსაც ექნებოდა ისეთივე სწრაფმოქმედება, როგორიც სიმეტრიულ სისტემებს აქვს. პრობლემის მიზეზი იმალება თვით ცალმხრივ ფუნქციებში, რომლებიც არსებული ასიმეტრიული სისტემების რეალიზების ძირითადი საფუძველია. ზემოთქმულიდან ცხადად ჩანს მაღალი რიგის მატრიცული სიმრავლის აგების მთელი სირთულე და საჭიროება [2].

ცალმხრივი ფუნქცია (ინგლ. one-way function, OWF) წარმოადგენს ფუნქციას, რომლის მნიშვნელობა ადვილი გამოსათვლელია ნებისმიერი არგუმენტისათვის, მაგრამ ფუნქციის მოცემული მნიშვნელობისათვის არგუმენტის პოვნა ძნელია. სიტყვა „ძნელი“ უნდა გავიგოთ გამოთვლის სირთულის თეორიის აზრით. სხვა სიტყვებით რომ ვთქვათ, ფუნქციის მოცემული მნიშვნელობის შესაბამისი არგუმენტის პოვნა რეალურ დროში ძნელია თანამედროვე გამოთვლითი ტექნიკის სიმძლავრის გათვალისწინებით. ე. ი. ფუნქციის შეუქცევადობა ჯერ კიდევ არ ნიშნავს მის ცალმხრივობას.

ცალმხრივი ფუნქციების არსებობას ეყრდნობა ასიმეტრიული კრიპტოგრაფიის იდეა. იგი (ცალმხრივი ფუნქცია) წარმოადგენს ასიმეტრიული კრიპტოგრაფიის, პერსონალური იდენტიფიკაციის, აუტენტიფიკაციის, და ინფორმაციის დაცვის სხვა დარგების ფუნდამენტს. მართალია, ცალმხრივი ფუნქციების არსებობა მკაცრად დამტკიცებული არ არის, მაგრამ არსებობს რამდენიმე პრეტენდენტი (მაგ. გამრავლება და ფაქტორიზაცია, კვადრატში აყვანა და მოდულით ამოფესვა, დისკრეტული ახარისხება და გალოგარითმება), რომელთა ცალმხრივობა (ანუ ფუნქციის მნიშვნელობის შესაბამისი არგუმენტის პოვნის სიძნელე) ჯერჯერობით უძლებს დროს და აქტიურად გამოიყენება ინფორმაციის გაცვლის პროტოკოლებში.

როგორც აღვნიშნეთ, ცალმხრივი ფუნქციები აქტიურად გამოიყენება კრიპტო-გრაფიული გასაღების ღია არხით შემუშავების ალგორითმებში. პირველი იდეა (1976 წ.)

ეკუთვნით უიტფილდ დიფის და მარტინ ჰელმანს (Whitfield Diffie, Martin Hellman). მათი იდეის ბაზაზე ჩამოყალიბდა ცნობილი დიფი-ჰელმან-მერკლის პირველი პრაქტიკული მეთოდი, რომლის საშუალებითაც შესაძლებელი გახდა ღია (დაუცველი) არხის გამოყენებით საერთო კრიპტოგრაფიული გასაღების შემუშავება. ერთი წლის შემდეგ კი ჩამოყალიბდა ასიმეტრიული დაშიფვრის პირველი ალგორითმი RSA, რომელმაც, ფაქტიურად, გადაწყვიტა ღია არხით ინფორმაციის გაცვლის პრობლემა.

ცალმხრივი მატრიცული ფუნქცია

საერთო კრიპტოგრაფიული გასაღების შემუშავების ახალი ცალმხრივი ფუნქცია [1] ეყრდნობა მაღალი რიგის ციკლურ მატრიცულ ჯგუფებს, სიმძლავრით $e = 2^n - 1$, სადაც n – კვადრატული მატრიცის ზომაა. დავუშვათ, A ზემოთნახსენები მატრიცული ჯგუფია, ხოლო A - საწყისი $n \times n$ მატრიცა, მაშინ $A=\{A, A^2, A^3, \dots, A^{2^n-1} = I\}$, სადაც I წარმოადგენს ერთეულოვან მატრიცას.

ცალმხრივი ფუნქცია და საერთო გასაღების შემუშავების ალგორითმი შემდეგი სახისაა:

- გამგზავნი მხარე ირჩევს $A_1 \in A$ საიდუმლო მატრიცას და მიმღებ მხარეს ღია არხით უგზავნის $u_1 = vA_1$ ვექტორს, სადაც $v \in V_n$ ვექტორი საყოველთაოდ ცნობილია (V_n - ვექტორული სივრცეა $GF(2)$ ველზე);
- მიმღები მხარე თავის მხრივ ირჩევს $A_2 \in A$ საიდუმლო მატრიცას და გამგზავნ მხარეს უგზავნის $u_2 = vA_2$ ვექტორს;
- გამგზავნი გამოთვლის $k_1 = u_2A_1$ ვექტორს;
- მიმღები გამოთვლის $k_2 = u_1A_2$, სადაც k_1 და k_2 - საიდუმლო გასაღებებია;

ცხადია, $k_1 = k_2 = k$, რადგანაც $k = vA_1A_2 = vA_2A_1$, A ჯგუფის კომუტაციურობის გამო. $vA_i = u$ ცალმხრივი სწრაფმოქმედი ფუნქციაა.

ვთქვათ, $v = (v_1, v_2, v_3, \cdots, v_n) \in V_n$ და $u = (u_1, u_2, u_3, \cdots, u_n) \in V_n$ არასაიდუმლო ვექტორებია ზემოთმოყვანილი ალგორითმიდან, ხოლო

$$A_1 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in A$$

საიდუმლო მატრიცაა. მაშინ, ალგორითმის თანახმად

$$vA_1 = \begin{pmatrix} v_1a_{11} + v_2a_{21} + \cdots + v_na_{n1} \\ v_1a_{12} + v_2a_{22} + \cdots + v_na_{n2} \\ \vdots \\ v_1a_{n1} + v_2a_{n2} + \cdots + v_3a_{n3} \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \quad (1)$$

მიღებულ წრფივ განტოლებათა სისტემაში უცნობების რაოდენობა განტოლებების რაოდენობის კვადრატია. ცხადია, სისტემის ამოხნა რეალურ დროში შეუძლებელია, თუკი მატრიცის ზომა საკმარისად დიდია. გასათვალისწინებელია ერთი ფაქტი - თუ A_1 მატრიცა შეიცავს შიგა რეკურენტობას, ანუ თუ მისი ყოველი სტრიქონი გარკვეულ რეკურენტულ დამოკიდებულებაშია წინა სტრიქონთან [2,3], მაშინ (1) სისტემის ამოხსნის ამოცანა დაიყვანება გაცილებით მარტივ ამოცანაზე, რომელიც უკვე ადვილი ამოსახსნელი ხდება. ეს იმდენად მნიშვნელოვანი გარემოებაა, რომ თავისთავად აყენებს ეჭვქვეშ ჩვენი ფუნქციის ცალმხრივობას და აუცილებელს ხდის მაღალი რიგისა და სიმძლავრის მქონე, შიგა რეკურენტობისაგან თავისუფალი აბელის მულტიპლიკაციური მატრიცული ჯგუფის არსებობას.

სასრული მატრიცული ჯგუფების აგება

განვიხილოთ $(1+\alpha)^j$, სადაც $j = 0, 1, 2, \cdots$, ხოლო α წარმოადგენს პრიმიტიული პოლინომის ფესვს $GF(2^n)$ ველში მოდულით $p(x)$.

$(1+\alpha)^0 = 1$	1
$(1+\alpha)^1 = 1+\alpha$	11
$(1+\alpha)^2 = 1+\alpha^2$	101
$(1+\alpha)^3 = 1+\alpha+\alpha^2+\alpha^3$	1111
$(1+\alpha)^4 = 1+\alpha^4$	10001
$(1+\alpha)^5 = 1+\alpha+\alpha^4+\alpha^5$	110011

მიღებული პოლინომების კოეფიციენტები ქმნის სტრუქტურას, რომელიც სერპინსკის სამკუთხედის სახელითაა ცნობილი.

მიღებული სტრუქტურა შეიცავს მრავალ ქვესტრუქტურას, რომლებიც მულტიპლიკაციური ჯგუფების გენერატორად (მაწარმოებელ მატრიცად) გამოდგება,

ანუ პრიმიტიულ ელემენტებს წარმოადგენენ. ასეთია, მაგალითად, $P_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$, $P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$, და სხვა მრავალი. მათი ნატურალური ხარისხები ქმნის აბელის მულტიპლიკაციურ ციკლურ ჯგუფს.

მაგ.:

$$P_3^1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, P_3^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \; P_3^3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, P_3^4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$P_3^5 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, P_3^6 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \; P_3^7 = P_3^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ადვილად შეიძლება დავრწმუნდეთ, რომ მიღებული

$$P_3^0, P_3^1, P_3^2, P_3^3, P_3^4, P_3^5, P_3^6 \qquad (2)$$

სიმრავლე აბელის მულტიპლიკაციური ჯგუფია.

შევინარჩუნოთ P_3 მატრიცის სტრუქტურა და გავაფართოვოთ იგი (2) სიმრავლის ელემენტებით ქვემოთმოყვანილი სახით:

$$P_{3^2}(i,j) = \begin{pmatrix} P_3^i & P_3^j & P_3^j \\ P_3^j & 0 & 0 \\ P_3^j & P_3^j & 0 \end{pmatrix}, \text{ სადაც } i,j=0..6.$$

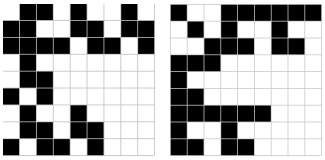
P_3 მატრიცას ვუწოდოთ **საბაზო სტრუქტურა.** P_3^i და P_3^j მატრიცებს ვუწოდოთ შესაბამისად **პირველი და მეორე მაფართოებელი მატრიცები**, ხოლო $P_{3^2}(i,j)$ მატრიცას ვუწოდოთ P_3 **მატრიცის მეორე რიგის** (i,j)**-გაფართოება.**

მაგალითად, როცა $i = 5$ და $j = 6$, მივიღებთ:

$$P_{3^2}(5,6) = \begin{pmatrix} P_3^5 & P_3^6 & P_3^6 \\ P_3^6 & 0 & 0 \\ P_3^6 & P_3^6 & 0 \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & 0 & 0 \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & 0 \end{pmatrix}$$

ასევე, როცა $i = 0$ და $j = 1$, გვექნება (ნახ. 1):

$$P_{3^2}(0,1) = \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & 0 & 0 \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & 0 \end{pmatrix}$$



ნახ.1: $P_{3^2}(5,6)$ და $P_{3^2}(0,1)$

განვიხილოთ $P = [P_{3^2}(5,6)]^2 = \begin{pmatrix} P_3^5 & P_3^6 & P_3^6 \\ P_3^6 & 0 & 0 \\ P_3^6 & P_3^6 & 0 \end{pmatrix} \times \begin{pmatrix} P_3^5 & P_3^6 & P_3^6 \\ P_3^6 & 0 & 0 \\ P_3^6 & P_3^6 & 0 \end{pmatrix}$.

თუ გავითვალისწინებთ, რომ $0, P_3^0, P_3^1, P_3^2, P_3^3, P_3^4, P_3^5, P_3^6$ სიმრავლე ველია, ადვილად დავრწმუნდებით, რომ P მატრიცის თითოეული ქვემატრიცა ამავე სიმრავლის ელემენტია:

$P_{1,1} = P_3^5 \times P_3^5 + P_3^6 \times P_3^6 + P_3^6 \times P_3^6 = P_3^3$, $P_{1,2} = P_3^5 \times P_3^6 + P_3^6 \times 0 + P_3^6 \times P_3^6 = P_3^2$,

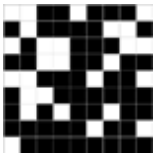
$P_{1,3} = P_3^5 \times P_3^6 + P_3^6 \times 0 + P_3^6 \times 0 = P_3^4$, $P_{2,1} = P_3^6 \times P_3^5 + 0 \times P_3^6 + 0 \times P_3^6 = P_3^4$,

$P_{2,2} = P_3^6 \times P_3^6 + 0 \times 0 + 0 \times P_3^6 = P_3^5$, $P_{2,3} = P_3^6 \times P_3^6 + 0 \times 0 + 0 \times 0 = P_3^5$,

$P_{3,1} = P_3^6 \times P_3^5 + P_3^6 \times P_3^6 + 0 \times P_3^6 = P_3^2$, $P_{3,2} = P_3^6 \times P_3^6 + P_3^6 \times 0 + 0 \times P_3^6 = P_3^5$,

$P_{3,3} = P_3^6 \times P_3^6 + P_3^6 \times 0 + 0 \times 0 = P_3^5$.

ანუ $P = \begin{pmatrix} P_3^3 & P_3^2 & P_3^4 \\ P_3^4 & P_3^5 & P_3^5 \\ P_3^2 & P_3^5 & P_3^5 \end{pmatrix}$ (ნახ. 2).



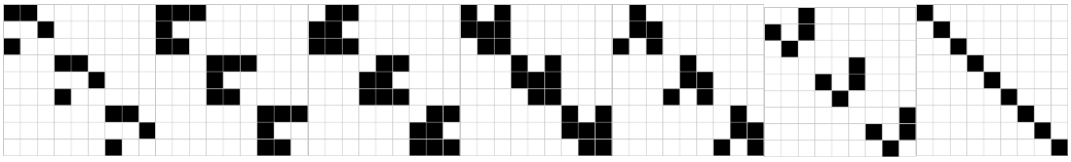
ნახ.2: $P = [P_{3^2}(5,6)]^2$

ჩვენს მიერ შემუშავებული პროგრამული პაკეტის მეშვეობით დამტკიცდა, რომ **$P_{3^2}(5,6)$ მატრიცა პრიმიტიული ელემენტია. მისი ნატურალური ხარისხები წარმოქმნის აბელის მულტიპლიკაციურ ჯგუფს, რომლის სიძლავრეა 2^{3^2-1}**.

$[P_{3^2}(5,6)]^k$ სიმრავლის ელემენტები, როცა k=73, 146, 219, 292, 365, 438, 511, დიაგონალურ მატრიცებს წარმოადგენენ (ნახ.3):

$$\begin{pmatrix} P_3^4 & 0 & 0 \\ 0 & P_3^4 & 0 \\ 0 & 0 & P_3^4 \end{pmatrix}, \begin{pmatrix} P_3^1 & 0 & 0 \\ 0 & P_3^1 & 0 \\ 0 & 0 & P_3^1 \end{pmatrix}, \begin{pmatrix} P_3^5 & 0 & 0 \\ 0 & P_3^5 & 0 \\ 0 & 0 & P_3^5 \end{pmatrix}, \begin{pmatrix} P_3^2 & 0 & 0 \\ 0 & P_3^2 & 0 \\ 0 & 0 & P_3^2 \end{pmatrix}, \begin{pmatrix} P_3^6 & 0 & 0 \\ 0 & P_3^6 & 0 \\ 0 & 0 & P_3^6 \end{pmatrix},$$

$$\begin{pmatrix} P_3^3 & 0 & 0 \\ 0 & P_3^3 & 0 \\ 0 & 0 & P_3^3 \end{pmatrix}, \begin{pmatrix} P_3^0 & 0 & 0 \\ 0 & P_3^0 & 0 \\ 0 & 0 & P_3^0 \end{pmatrix}$$

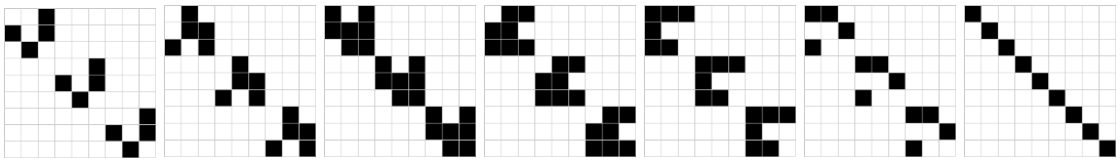


ნახ.3: $[P_{3^2}(5,6)]^k, k = 73, 146, 219, 292, 365, 438, 511$

პრიმიტიული ელემენტია აგრეთვე $P_{3^2}(0,1)$ მატრიცა, ხოლო $[P_{3^2}(0,1)]^k$ სიმრავლის ელემენტები, როცა k=73, 146, 219, 292, 365, 438, 511, შემდეგი სახის დიაგონალური მატრიცებია (ნახ.4):

$$\begin{pmatrix} P_3^3 & 0 & 0 \\ 0 & P_3^3 & 0 \\ 0 & 0 & P_3^3 \end{pmatrix}, \begin{pmatrix} P_3^6 & 0 & 0 \\ 0 & P_3^6 & 0 \\ 0 & 0 & P_3^6 \end{pmatrix}, \begin{pmatrix} P_3^2 & 0 & 0 \\ 0 & P_3^2 & 0 \\ 0 & 0 & P_3^2 \end{pmatrix}, \begin{pmatrix} P_3^5 & 0 & 0 \\ 0 & P_3^5 & 0 \\ 0 & 0 & P_3^5 \end{pmatrix}, \begin{pmatrix} P_3^1 & 0 & 0 \\ 0 & P_3^1 & 0 \\ 0 & 0 & P_3^1 \end{pmatrix},$$

$$\begin{pmatrix} P_3^4 & 0 & 0 \\ 0 & P_3^4 & 0 \\ 0 & 0 & P_3^4 \end{pmatrix}, \begin{pmatrix} P_3^0 & 0 & 0 \\ 0 & P_3^0 & 0 \\ 0 & 0 & P_3^0 \end{pmatrix}$$



ნახ.4: $[P_{3^2}(5,6)]^k,\ k = 73, 146, 219, 292, 365, 438, 511$

დიაგონალური მატრიცების დიაგონალებზე მყოფი ელემენტების სიმრავლე წარმოადგენს $P_3^0, P_3^1, P_3^2, P_3^3, P_3^4, P_3^5, P_3^6$ ჯგუფის (ვუწოდოთ მას **წინარე ჯგუფი**) ერთ–ერთ გადანაცვლებას, რომლის ბოლო ელემენტიც აუცილებლად არის P_3^0.

საბოლოოდ, ექსპერიმენტულად მტკიცდება შემდეგი წინადადების ჭეშმარიტება:

P_3 მატრიცის ნებისმიერი მეორე რიგის $(i, i+1)$ გაფართოება - $P_{3^2}(i, i+1)$, $i = 0..5$, წარმოადგენს პრიმიტიულ ელემენტს და წარმოქმნის აბელის მულტიპლიკაციურ სასრულ ჯგუფს $F(P_{3^2}(i, i+1))$, რომლის სიმძლავრეა $2^{3^2}-1$.

ქვემო მოყვანილია P_3 მატრიცის გაფართოებით მიღებული სხვა პრიმიტიული ელემენტები:

$$P_{3^2}(0,1)=\begin{pmatrix}P_3^0 & P_3^1 & P_3^1\\ P_3^1 & 0 & 0\\ P_3^1 & P_3^1 & 0\end{pmatrix}, P_{3^2}(1,2)=\begin{pmatrix}P_3^1 & P_3^2 & P_3^2\\ P_3^2 & 0 & 0\\ P_3^2 & P_3^2 & 0\end{pmatrix}, P_{3^2}(2,3)=\begin{pmatrix}P_3^2 & P_3^3 & P_3^3\\ P_3^3 & 0 & 0\\ P_3^3 & P_3^3 & 0\end{pmatrix},$$

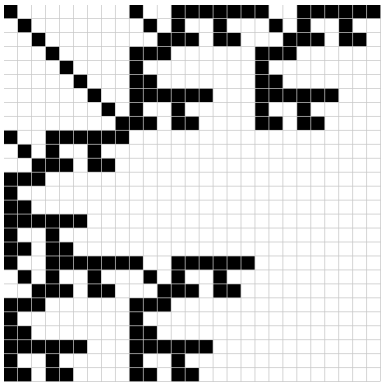
$$P_{3^2}(3,4)=\begin{pmatrix}P_3^3 & P_3^4 & P_3^4\\ P_3^4 & 0 & 0\\ P_3^4 & P_3^4 & 0\end{pmatrix}, P_{3^2}(4,5)=\begin{pmatrix}P_3^4 & P_3^5 & P_3^5\\ P_3^5 & 0 & 0\\ P_3^5 & P_3^5 & 0\end{pmatrix}, P_{3^2}(5,6)=\begin{pmatrix}P_3^5 & P_3^6 & P_3^6\\ P_3^6 & 0 & 0\\ P_3^6 & P_3^6 & 0\end{pmatrix},$$

$$P_{3^2}(6,0)=\begin{pmatrix}P_3^6 & P_3^0 & P_3^0\\ P_3^0 & 0 & 0\\ P_3^0 & P_3^0 & 0\end{pmatrix}$$

უფრო მაღალი რიგის პრიმიტიული ელემენტების მისაღებად ისევ შევინარჩუნოთ P_3 მატრიცის სტრუქტურა და ჩავსვათ მასში $F(P_{3^2}(i,i+1))$ ჯგუფის (წინარე ჯგუფის) ელემენტები, მივიღებთ 3^3 რიგის მატრიცას (ვუწოდოთ მას მესამე რიგის გაფართოება).

მაგალითად, P_3 მატრიცის პირველ და მეორე მაფართოებელ მატრიცებად თუ გამოვიყენებთ $F(P_{3^2}(0,1))$ ჯგუფის ელემენტებს, შესაბამისად $[P_{3^2}(0,1)]^0$ და $[P_{3^2}(0,1)]^1$ მატრიცებს, მივიღებთ შემდეგ მატრიცას (ნახ. 5):

$$P_{3^3}(0,1)=\begin{pmatrix}P_{3^2}^0 & P_{3^2}^1 & P_{3^2}^1\\ P_{3^2}^1 & 0 & 0\\ P_{3^2}^1 & P_{3^2}^1 & 0\end{pmatrix}=\begin{pmatrix}\begin{pmatrix}P_3^0 & 0 & 0\\ 0 & P_3^0 & 0\\ 0 & 0 & P_3^0\end{pmatrix} & \begin{pmatrix}P_3^0 & P_3^1 & P_3^1\\ P_3^1 & 0 & 0\\ P_3^1 & P_3^1 & 0\end{pmatrix} & \begin{pmatrix}P_3^0 & P_3^1 & P_3^1\\ P_3^1 & 0 & 0\\ P_3^1 & P_3^1 & 0\end{pmatrix}\\ \begin{pmatrix}P_3^0 & P_3^1 & P_3^1\\ P_3^1 & 0 & 0\\ P_3^1 & P_3^1 & 0\end{pmatrix} & 0 & 0\\ \begin{pmatrix}P_3^0 & P_3^1 & P_3^1\\ P_3^1 & 0 & 0\\ P_3^1 & P_3^1 & 0\end{pmatrix} & \begin{pmatrix}P_3^0 & P_3^1 & P_3^1\\ P_3^1 & 0 & 0\\ P_3^1 & P_3^1 & 0\end{pmatrix} & 0\end{pmatrix}$$



ნახ.5. $P_{3^3}(0,1)$

განვიხილოთ $[P_{3^3}(0,1)]^k$ სიმრავლე. მას იგივე საბაზო სტრუქტურა P_3 აქვს, რაც წინარე ჯგუფს, აგრეთვე პირველი და მეორე მაფართოებელი მატრიცები წინარე ჯგუფიდანაა აღებული. მოსალოდნელია, რომ ეს სიმრავლე იგივე თვისებებით ხასიათდებოდეს, რაც წინარე ჯგუფს გააჩნია. მართლაც, ექსპერიმენტულად აღმოჩნდა, რომ მასაც გააჩნია დიაგონალური მატრიცები, რომელთა დიაგონალების ელემენტები წინარე ჯგუფის ერთ–ერთ გადანაცვლებას წარმოადგენს.

$[P_{3^3}(0,1)]^k$ სიმრავლის დიაგონალური მატრიცებია $[P_{3^3}(0,1)]^{i\cdot\left(2^{2\cdot3^2}+2^{3^2}+1\right)}$, $i = 1,2,3,\cdots,2^{3^2}-1$.

როცა $i = 2^{3^2}-1$, მივიღებთ $[P_{3^3}(0,1)]^k$ სიმრავლის ბოლო ელემენტს:

$$[P_{3^3}(0,1)]^{(2^{3^2}-1)\cdot\left(2^{2\cdot3^2}+2^{3^2}+1\right)} = [P_{3^3}(0,1)]^{(2^{3^3}-1)} = \begin{pmatrix} [P_{3^0}(0,1)]^0 & 0 & 0 \\ 0 & [P_{3^0}(0,1)]^0 & 0 \\ 0 & 0 & [P_{3^0}(0,1)]^0 \end{pmatrix}$$

. ეს კი ერთეულოვან მატრიცას წარმოადგენს. მაშასადამე, **$P_{3^3}(0,1)$ მატრიცა პრიმიტიული ელემენტია და წარმოქმნის $2^{3^3}-1$ სიმძლავრის მქონე აბელის მულტიპლიკაციურ სასრულ ჯგუფს.**

განმარტება: P_3 მატრიცის k რიგის $(i,i+1)$ გაფართოება ვუწოდოთ შემდეგი სახის მატრიცას:

$$P_{3^k}(i,i+1) = \begin{pmatrix} P_{3^{k-1}}^{i} & P_{3^{k-1}}^{i+1} & P_{3^{k-1}}^{i+1} \\ P_{3^{k-1}}^{i+1} & 0 & 0 \\ P_{3^{k-1}}^{i+1} & P_{3^{k-1}}^{i+1} & 0 \end{pmatrix}, \qquad (3)$$

სადაც $P_{3^{k-1}}^{i} \in F(P_{3^{k-1}}(i,i+1))$.

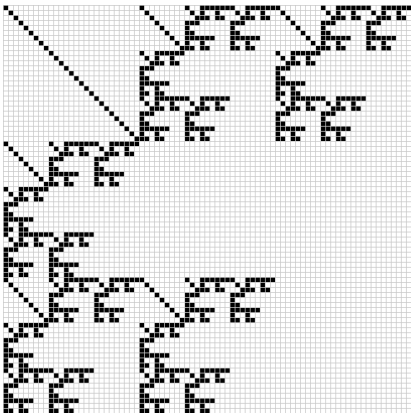
თეორემა: **$P_{3^k}(i,i+1)$ პრიმიტიული ელემენტია და წარმოქმნის აბელის მულტიპლიკაციურ სასრულ $F(P_{3^k}(i,i+1))$ ჯგუფს, რომლის სიმძლავრეა $2^{3^k}-1$.**

საზოგადოდ, მატრიცები $\left[P_{3^k}(i,i+1)\right]^{i(2^{2\cdot3^{k-1}}+2^{3^{k-1}}+1)}$, სადაც $i = 1,2,3,\cdots,2^{3^{k-1}}-1$ დიაგონალურია, დიაგონალზე მდგომი ელემენტების სიმრავლე წინარე ველის ერთ–ერთ გადანაცვლებაა.

როცა $i = 2^{3^{k-1}}-1$, ვღებულობთ

$$\left[P_{3^k}(i,i+1)\right]^{i(2^{2\cdot3^{k-1}}+2^{3^{k-1}}+1)} = \left[P_{3^k}(i,i+1)\right]^{(2^{3^{k-1}}-1)\cdot(2^{2\cdot3^{k-1}}+2^{3^{k-1}}+1)} = \left[P_{3^k}(i,i+1)\right]^{(2^{3^{k-1}}-1)}$$

$$= \begin{pmatrix} \left[P_{3^{k-1}}(i,i+1)\right]^0 & 0 & 0 \\ 0 & \left[P_{3^{k-1}}(i,i+1)\right]^0 & 0 \\ 0 & 0 & \left[P_{3^{k-1}}(i,i+1)\right]^0 \end{pmatrix}$$



ნახ.6. $P_{3^4}(0,1)$

რაც ნიშნავს იმას, რომ (3) სტრუქტურა პრიმიტიული მატრიცაა. მიღებულ პრიმიტიულ მატრიცებს საინტე–რესო ფრაქტალური სტრუქტურა გააჩნიათ (ნახ. 6) ზემოთმოყვანილი მეთოდით მიღებული აბელის მულტიპლიკაციური ჯგუფები ჩვენი ცალმხრივი მატრიცული ფუნქციების რეალიზებისათვის საკმარის სიმრავლეებს წარმოადგენს.

დასკვნა

ბაზური P_3 მატრიცის $P_{3^k}(i, i+1)$გაფართოებები პრიმიტიული მატრიცებია. კვლევის საინტერესო მიმართულებას წარმოქმნის შედეგი მოსაზრება: პირველ და მეორე მაფართოებელ მატრიცებად წინარე ველის ისეთი ელემენტების გამოყენება, რომელთაც ერთი და იგივე მახასიათებელი პოლინომი გააჩნიათ. მნიშვნელოვანია, აგრეთვე, სხვა ბაზური მატრიცების გამოყენების საკითხი, რომელთა გაფართოებაც ახალი ტიპის პრიმიტიულ სტრუქტურებს წარმოშობს.

REFERENCES

1. Megrelishvili R., Chelidze M., Chelidze K., “On the construction of secret and public-key cryptosystems”, in *Applied Mathematics, Informatics and Mechanics*, Tbilisi,Georgia: Tbilisi University Press, vol. 11, No2, 2006, pp.29-36.
2. Megrelishvili R., Chelidze M., Besiashvili G., “One-way matrix function – analogy of Diffie-Hellman protocol”, in *Proceedings of the Seventh International Conference*, IES-2010, 28 September-3 Oktober, Vinnytsia, Ukraine, 2010. pp. 341-344.
3. Мегрелишвили Р. П., Джинджихадзе М. В., “Однонаправленная матричная функция для обмена криптографическими ключами и метод генерации мультипликативных матричних групп”, in *Proceedings of the International Conference SAIT 2011*, May 23-28, Kyiv, Ukraine, 2011. p. 472.