Scientific and Practical Cyber Security Journal (SPCSJ) 3(2): 57- 63 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

მაღალი რიგის პრიმიტიული მატრიცების გენერაცია სხვადასხვა სიმძლავრის აბელის მულტიპლიკაციური ჯგუფების ელემენტებით

Generation of high order primitive matrix elements with elements of abelian multiplicative groups

რ. მეგრელიშვილი[1], მ. ჯინჯიხაძე[2]
[1]თბილისის ივ. ჯავახიშვილის სახ. სახელმწიფო უნივერსიტეტი, თბილისი, საქართველო;
ელ–ფოსტა: richard.megrelishvili@tsu.ge
[2]აკ. წერეთლის სახელმწიფო უნივერსიტეტი, ქუთაისი, საქართველო
ელ–ფოსტა: mjinji@yahoo.com

ანოტაცია - ნაშრომში განხილულია ორიგინალური მატრიცული ცალმხრივი ფუნქცია და მისი შესაბამისი მაღალი რიგის მატრიცული მულტიპლიკაციური სასრული კომუტაციური ჯგუფის გენერაციის განზოგადებული მეთოდი. განხორციელებულია ველის პრიმიტიული ელემენტების აგების ჩასმა–გაფართოების მეთოდის ზოგადი ხერხი სხვადასხვა სიმძლავრის მქონე მატრიცული ჯგუფების ელემენტებით.

ABSTRACT. In this paper is considered the original one-way function matrix and it's corresponding generation method of high level matrix multiplicative finite commutative group. The general method of the insertion-enlarging method of building the primitive elements of the field is derived with elements of the matrix groups with different power.

საკვანძო სიტყვები: მატრიცული ცალმხრივი ფუნქცია, აბელის სასრული ველი, ასიმეტრიული კრიპტოგრაფია, მაღალი რიგის მატრიცული სასრული ველი, პრიმიტიული მატრიცული ელემენტი.

KEYWORDS: matrix one-way function; Abel finite field; asymmetric cryptography; high level matrix multiplicative finite field; primitive matrix element;

ცალმხრივი მატრიცული ფუნქცია

კრიპტოგრაფიული გასაღების გაცვლის დიფი-ჰელმანის ცნობილი მეთოდის ერთ-ერთ მოდიფიკაციას წარმოადგენს გასაღების გაცვლის მატრიცული ალგორითმები, რომელთა

მუშაობის საფუძველს ქმნის მაღალი რიგის ციკლური მულტიპლიკაციური მატრიცული ჯგუფები $GF(2)$ ველზე.

დავუშვათ, P მატრიცა წარმოადგენს ციკლური მატრიცული ჯგუფის პრიმიტიულ ელემენტს. ხოლო $\langle P\rangle$ ამ მატრიცის მიერ წარმოქმნილი მულიტიპლიკაციური ჯგუფია, სიმძლავრით 2^n-1, სადაც n წარმოადგენს P კვადრატული მატრიცის ზომას.

საერთო გასაღების შემუშავების მატრიცული ალგორითმი შემდეგი სახისაა:

- გამგზავნი მხარე მიმღებ მხარეს ღია არხით უგზავნის $u_1 = vP_1$ ვექტორს, სადაც $P_1 \in \langle P\rangle$ გამგზავნის მიერ შერჩეული საიდუმლო მატრიცაა, ხოლო $v \in V_n$ ვექტორი საყოველთაოდ ცნობილია (V_n - ვექტორული სივრცეა $GF(2)$ ველზე);

- მიმღები მხარე თავის მხრივ ირჩევს $P_2 \in \langle P\rangle$ საიდუმლო მატრიცას და გამგზავნ მხარეს უგზავნის $u_2 = vP_2$ ვექტორს;
- გამგზავნი გამოთვლის $k_1 = u_2P_1$ ვექტორს;
- მიმღები გამოთვლის $k_2 = u_1P_2$, სადაც k_1 და k_2 - საიდუმლო გასაღებებია;

ცხადია, $k_1 = k_2 = k$, რადგანაც $k = vP_1P_2 = vP_2P_1$, $\langle P\rangle$ ჯგუფის კომუტაციურობის გამო. 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

$$P_1 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in \langle P\rangle$$

საიდუმლო მატრიცაა. მაშინ, ალგორითმის თანახმად

$$vP_1 = \begin{pmatrix} v_1a_{11} + v_2a_{21} + \cdots + v_na_{n1} \\ v_1a_{12} + v_2a_{22} + \cdots + v_na_{n2} \\ \vdots \\ v_1a_{n1} + v_2a_{n2} + \cdots + v_3a_{n3} \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \quad (1)$$

მიღებულ წრფივ განტოლებათა სისტემაში უცნობების რაოდენობა განტოლებების რაოდენობის კვადრატია. ცხადია, სისტემის ამოხსნა რეალურ დროში შეუძლებელია, თუკი მატრიცის ზომა საკმარისად დიდია. ეს იმდენად მნიშვნელოვანი გარემოებაა, რომ თავისთავად აუცილებელს ხდის მაღალი სიმძლავრის მქონე, აბელის მულტიპლიკაციური მატრიცული ჯგუფის გენერაციას, რომლის პრიმიტიული ელემენტი მაღალი რიგის კავადრატული მატრიცა იქნება.

სასრული მატრიცული ჯგუფები

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

$$
\begin{aligned}
&(1+\alpha)^0 = 1 && 1\\
&(1+\alpha)^1 = 1+\alpha && 11\\
&(1+\alpha)^2 = 1+\alpha^2 && 101\\
&(1+\alpha)^3 = 1+\alpha+\alpha^2+\alpha^3 && 1111\\
&(1+\alpha)^4 = 1+\alpha^4 && 10001\\
&(1+\alpha)^5 = 1+\alpha+\alpha^4+\alpha^5 && 110011
\end{aligned}
\qquad (1)
$$

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

სერპინსკის სტრუქტურა შეიცავს მრავალ ქვესტრუქტურას, რომლებიც მულტიპლიკაციური ჯგუფების გენერატორად (მაწარმოებელ მატრიცად) გამოდგება, ანუ პრიმიტიულ ელემენტებს წარმოადგენენ. ასეთია, მაგალითად,

$$
P_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \; P_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad (2)
$$

და სხვა მრავალი. მათი ნატურალური ხარისხები ქმნის აბელის მულტიპლიკაციურ ციკლურ ჯგუფებს.

ადვილად შეიძლება დავრწმუნდეთ, რომ P_3 , P_5 , P_7 მატრიცების ახარისხებით მიღებული

$$
P_3^k \, , P_5^k \, , P_7^k \, , k = 1,2, \dots , 2^k - 1 \qquad (3)
$$

სიმრავლეები აბელის მულტიპლიკაციურ ციკლურ ჯგუფებს წარმოადგენენ.

მაგ.:

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

$$
P_3^5 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, P_3^6 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \; P_3^7 = P_3^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (4)
$$

ჩვენს მიერ P_3 მატრიცის, როგორც საბაზო სტრუქტურის, ჩასმა-გაფართოების მეთოდით მიღებული იყო მეორე რიგის გაფართოება *****:

$$P_{3^2}(i,j)=\begin{pmatrix} P_3^i & P_3^j & P_3^j \\ P_3^j & 0 & 0 \\ P_3^j & P_3^j & 0 \end{pmatrix}, \text{ სადაც } i,j=0..6. \quad (5)$$

P_3 მატრიცას ეწოდება **საბაზო სტრუქტურა.** P_3^i და P_3^j მატრიცებს - შესაბამისად **პირველი და მეორე მაფართოებელი მატრიცები.**

$P_3^k,\ k=1,2,\dots,2^3-1$ სიმრავლეს ეწოდება $F(P_{3^2}(i,i+1))$ ჯგუფის **წინარე ჯგუფი**.

ჩვენს მიერ დამტკიცებული იყო 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 $2^{3^2}-1$.

მაგალითად, პრიმიტიულია $P_{3^2}(0,1)$ მატრიცა, ხოლო $[P_{3^2}(0,1)]^{2^{2\cdot3^1}+2^{3^1}+1}$ მატრიცა დიაგონალურ მატრიცას წარმოადგენს:

$$[P_{3^2}(0,1)]^{2^{2\cdot3^1}+2^{3^1}+1}=\begin{pmatrix} P_3^3 & 0 & 0 \\ 0 & P_3^3 & 0 \\ 0 & 0 & P_3^3 \end{pmatrix} \quad (6)$$

ცხადია, დიაგონალური მატრიცის ნებისმიერი ხარისხი $\left([P_{3^2}(0,1)]^{2^{2\cdot3^1}+2^{3^1}+1}\right)^i, i=1,2,\dots$ ისევ დიაგონალური მატრიცა იქნება, და რადგან $F(P_{3^2}(0,1))$ სიმრავლე სასრული ჯგუფია, ამიტომ, როცა $i=2^{3^1}-1$, ვღებულობთ

$$\left([P_{3^2}(0,1)]^{2^{2\cdot3^2}+2^{3^2}+1}\right)^i=\begin{pmatrix} (P_3^3)^i & 0 & 0 \\ 0 & (P_3^3)^i & 0 \\ 0 & 0 & (P_3^3)^i \end{pmatrix}=\begin{pmatrix} P_3^{3i\ mod\ i} & 0 & 0 \\ 0 & P_3^{3i\ mod\ i} & 0 \\ 0 & 0 & P_3^{3i\ mod\ i} \end{pmatrix} \quad (7)$$

რადგან მატრიცულ ოპერაციებს ვაწარმოებთ წინარე ჯგუფის მოდულით, შესაბამისად, (7) ერთეულოვანი მატრიცაა. რაც ნიშნავს, რომ $F(P_{3^2}(0,1))$ სიმრავლე სასრული ჯგუფია.

შევნიშნოთ, რომ საბაზო სტრუქტურად შეიძლება ავიღოთ (4) სიმრავლის სხვა ნებისმიერ არაერთეულოვანი ელემენტი. არსებობს ამ ელემენტის ისეთი გაფართოება P_3^0 და P_3^1 მაფართოებელი მატრიცებით, რომელიც პრიმიტიული ელემენტია.

მაგალითად, პრიმიტიული იქნება შემდეგი გაფართოებები :

$$\begin{pmatrix} P_3^1 & P_3^1 & 0 \\ 0 & 0 & P_3^1 \\ P_3^0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} P_3^1 & 0 & P_3^0 \\ P_3^1 & P_3^1 & P_3^1 \\ 0 & P_3^1 & P_3^1 \end{pmatrix}, \begin{pmatrix} 0 & P_3^1 & 0 \\ 0 & P_3^1 & P_3^1 \\ P_3^0 & 0 & P_3^1 \end{pmatrix} \qquad (8)$$

განვიხილოთ სერპინსკის სამკუთხედის უფრო მაღალი რიგის ქვესტრუქტურა :

$$P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

ადვილად მოწმდება, რომ P_5 პრიმიტიული ელემენტია, რაც ნიშნავს, რომ P_5^k , $k = 1,2, \dots, 2^5 - 1$ სასრულ მულტიპლიკაციურ კომუტაციურ ჯგუფს წარმოადგენს.

საბაზო სტრუქტურად ავიღოთ P_3 მატრიცა და გავაფართოვოთ იგი P_5^0 და P_5^1 მატრიცებით.

არსებობს P_3 მატრიცის ისეთი გაფართოებები P_5^0 და P_5^1 მატრიცებით, რომლებიც წარმოადგენს პრიმიტიულ ელემენტებს. მაგალითად,

$$\begin{pmatrix} P_5^1 & P_5^1 & P_5^1 \\ P_5^1 & 0 & 0 \\ P_5^0 & P_5^1 & 0 \end{pmatrix}, \begin{pmatrix} P_5^1 & P_5^1 & P_5^1 \\ P_5^1 & 0 & 0 \\ P_5^1 & P_5^0 & 0 \end{pmatrix} \qquad (9)$$

მატრიცები პრიმიტიული ელემენტებია. შესაბამისად, $F\left(P_{3\times 5^1}\left(P_5^0, P_5^1\right)\right)$ სიმრავლე სასრული მულტიპლიკაციური კომუტაციური ჯგუფია.

მართლაც, ადვილი შესამოწმებელია, რომ

$$\left[P_{3\times 5^1}\left(P_5^0, P_5^1\right)\right]^{2^{2\cdot 5^1}+2^{5^1}+1} = \begin{pmatrix} P_5^2 & 0 & 0 \\ 0 & P_5^2 & 0 \\ 0 & 0 & P_5^2 \end{pmatrix} \quad (10)$$

მატრიცა დიაგონალურია. (7) გარდაქმნის ანალოგიური მსჯელობით მივიღებთ, რომ

$\left(\left[P_{3\times 5^1}\left(P_5^0, P_5^1\right)\right]^{2^{2\cdot 5^1}+2^{5^1}+1}\right)^i, i = 1,2, \dots$ მატრიცები დიაგონალურია, ხოლო როცა $i = 2^{5^1} - 1$, მივიღებთ

$$\begin{pmatrix} P_5^{2i \bmod i} & 0 & 0 \\ 0 & P_5^{2i \bmod i} & 0 \\ 0 & 0 & P_5^{2i \bmod i} \end{pmatrix} \quad (11)$$

ერთეულოვან მატრიცას. რაც ნიშნავს იმას, რომ, $F\left(P_{3\times 5^1}\left(P_5^0, P_5^1\right)\right)$ სიმრავლე სასრული მულტიპლიკაციური კომუტაციური ჯგუფია, სიმძლავრით $2^{3\times 5^1} - 1$.

ახლა განვიხილოთ P_5 პრიმიტიული მატრიცის $k = 2$ რიგის გაფართოებები P_5^i, $i = 1,2, \dots, 2^5 - 1$ კომუტაციური ჯგუფის ელემენტებით - $P_{5^k}\left(P_5^0, P_5^1\right), k = 2$. არსებობს P_5 მატრიცის ისეთი გაფართოება, რომელიც პრიმიტიულ მატრიცას ქმნის. მაგალითად,

$$P_{5^k}\left(P_5^0, P_5^1\right) = \begin{pmatrix} P_5^1 & P_5^1 & P_5^1 & P_5^1 & P_5^0 \\ P_5^1 & 0 & 0 & 0 & 0 \\ P_5^1 & P_5^1 & 0 & 0 & 0 \\ P_5^1 & 0 & P_5^1 & 0 & 0 \\ P_5^1 & P_5^1 & P_5^1 & P_5^1 & 0 \end{pmatrix}, k = 2 \quad (12)$$

ჩვენს მიერ შემუშავებული პროგრამული პროდუქტის საშუალებით მოწმდება, რომ $\left(P_{5^k}\left(P_5^0, P_5^1\right)\right)^i$ მატრიცა, სადაც $i = 2^{4\cdot 5^{k-1}} + 2^{3\cdot 5^{k-1}} + 2^{2\cdot 5^{k-1}} + 2^{5^{k-1}} + 1$, $k = 2$ დიაგონალურ მატრიცას წარმოადგენს:

$$\left(P_{5^k}\left(P_5^0, P_5^1\right)\right)^{2^{4\cdot 5^{k-1}} + 2^{3\cdot 5^{k-1}} + 2^{2\cdot 5^{k-1}} + 2^{5^{k-1}} + 1} = \begin{pmatrix} P_5^4 & 0 & 0 & 0 & 0 \\ 0 & P_5^4 & 0 & 0 & 0 \\ 0 & 0 & P_5^4 & 0 & 0 \\ 0 & 0 & 0 & P_5^4 & 0 \\ 0 & 0 & 0 & 0 & P_5^4 \end{pmatrix}$$

რომლის ნებისმიერი ნატურალური ხარისხი $\left(P_{5^k}\left(P_5^0, P_5^1\right)\right)^{i\times j}$, ცხადია, დიაგონალური მატრიცაა, რომლის დიაგონალზეც განლაგებულია P_5^i, $i = 1,2, \dots, 2^5 - 1$ წინარე ჯგუფის ელემენტები. ხოლო, როცა $j = 2^{3^{k-1}} - 1$, მივიღებთ

$$\begin{pmatrix} P_5^{4j \bmod j} & 0 & 0 & 0 & 0 \\ 0 & P_5^{4j \bmod j} & 0 & 0 & 0 \\ 0 & 0 & P_5^{4j \bmod j} & 0 & 0 \\ 0 & 0 & 0 & P_5^{4j \bmod j} & 0 \\ 0 & 0 & 0 & 0 & P_5^{4j \bmod j} \end{pmatrix} = \begin{pmatrix} P_5^0 & 0 & 0 & 0 & 0 \\ 0 & P_5^0 & 0 & 0 & 0 \\ 0 & 0 & P_5^0 & 0 & 0 \\ 0 & 0 & 0 & P_5^0 & 0 \\ 0 & 0 & 0 & 0 & P_5^0 \end{pmatrix}$$

ერთეულოვან მატრიცას.

მიღებული შედეგი იძლევა მაღალი რიგის მატრიცების მულტილიკაციური კომუტაციური სასრული ჯგუფების გენერირების პერსპექტივას.

გამოყენებული ლიტერატურა:

[1] Mohammad Mehdi Nasrabadi, Ali Gholamian - On A-nilpotent abelian groups - Proceedings - Mathematical Sciences, Springer, November 2014, Volume 124, Issue 4, pp 517–525

[2] Chiş C, Chiş M and Silberberg G, Abelian groups as autocommutator groups, Arch. Math. (Basel) 90(6) (2008) 490–492