მაღალი რიგის მატრიცული მულტიპლიკაციური სასრული კომუტაციური ჯგუფის აგების მეთოდი

მელქისადეგ ჯინჯიხაძე

ელ-ფოსტა: malkhazjinji@gmail.com.
კომპიუტერულ მეცნიერებათა დეპარტამენტი,
ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი
ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, თბილისი, საქართველო.

ნაშრომში განხილულია მაღალი რიგის მატრიცული სასრული ველის გენერაციის განზოგადებული მეთოდი მატრიცული ცალმხრივი ფუნქციებისათვის. განხორციელებულია ველის პრიმიტიული ელემენტების აგების ჩასმა-გაფართოების მეთოდი.

არსებობს მრავალი სტრუქტურა, რომელთა ნატურალური ხარისხები ქმნის აბელის მულტიპლიკაციურ სასრულ ჯგუფს. მაგალითად,

$$P_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

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

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

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

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

ლიტერატურა

[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.