The method of generation of Abelian Matrix multiplicative finite field

Melkisadeg Jinjikhadze

e-mail: malkhazjinji@gmail.com.
Department of computer sciences,
Faculty of natural and exact sciences,
Inane Javakhishvili Tbilisi State University, Tbilisi, Georgia.

This work presents a generalized method of generating high-order finite matrix field for the one-way matrix functions. The general algorithm for building primitive matrix elements through the insertion-extension method is discussed.

There is many matrices can be used as a generator of multiplicative groups.

For example,

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

Definition: The matrix of the following type is called $(i, i+1)$ extension of order k of the matrix P_3:

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

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

Theorem: $P_{3^k}(i, i+1)$ is the primitive element and generates the abelian multiplicative finite group $F(P_{3^k}(i, i+1))$ of order $2^{3^k} - 1$.

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.