Abstracts of MMA2015, May 26–29, 2015, Sigulda, Latvia

RECURSIVE INVOLUTORY MATRIX GENERATION ALGORITHM, WHICH IS BASED ONLY WITH ELEMENTS ±1 AND ±2

S. KAMENCHENKO

Transport and Telecommunication Institute

Lomonosova 1, LV-1019, Riga, Latvia

E-mail: freeon@inbox.lv

The existence of involutory matrix class is mentioned in matrix theory [1; 2] for which the initial and its inverse form are the same $A = A^{-1}$, then $A \cdot A^{-1} = A \cdot A = A^2 = I$.

One of the published involutory matrix generation algorithm [3] is based on using matrix elements range from 0 to m, where $m \in N$. This method allows to generate involutory matrices with size 4×4, for which $A^2 \pmod{m} = I$. However, there are presented heuristic methods of involutory matrix generation algorithms in scientific literature [3], which are based only with elements $\pm 2^n$, where $n \in N$.

Based on involutory matrices investigation process, which contain only elements $\pm 2^n$, where n is minimal possible integer, we found that such kind of matrices can be constructed only with the following dimensions $2^k \times 2^k$ $(1 < k \in N)$. It is quite easy to find involutory matrices with small dimension by using brute force tactic, but if the involutory matrix dimension k is increasing then to find involutory matrices is more complex task for acceptable period of time.

Existing recursive matrix generation algorithms [4] allow to generate involutory matrices with higher dimension based on previously founded involutory matrices with lower dimension. But, unfortunately, the resulting involutory matrices elements size is increased to $\pm 2^{n+1}$ at every generation stage. For generating involutory matrices with $2^k \times 2^k$ $(1 < k \in N)$ dimensions one initial involutory matrix is not enough, so we need to find two involutory matrices with different dimensions by using brute force tactics. For creating involutory matrices with higher dimensions which are based only with minimum possible elements ±1 and ±2, we need to use brute force tactics due to lack of involutory matrix generation algorithms with specific matrix elements requirements.

One way of recursive involutory matrix generation algorithm which is based only with elements ±1 and ±2, is proposed in the article. There is proved that any involutory matrix with specific requirements can form unified basis for recursive involutory matrix generation algorithm with $2^k \times 2^k$ $(2 < k \in N)$ dimensions and all resulting involutory matrices are based only with elements ±1 and ±2.

REFERENCES

[1] N. Franklyn. *Matrix theory.* Dover Publications, Canada, 1993.

[2] F. Zhang. *Matrix theory.* Springer, USA, 1999.

[3] B. Acharya, G.S. Rath, S.K. Patra, S.K. Panigrahy. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm. *International Journal of Security*, **1** (1):14–21, 2007.

[4] S. Pollock. On Kronecker Products, Tensor Products and Matrix Differential Calculus. ,
$http : //www.le.ac.uk/economics/research/RePEc/lec/leecon/dp11 - 34.pdf$.