

## **ANALYSIS OF THE MATRIX ONE-WAY FUNCTION AND TWO VARIANTS OF ITS IMPLEMENTATION**

**R. P. MEGRELISHVILI**

Javakhishvili Tbilisi State University,

### **Abstract**

In this article we first announced about two versions of the new matrix one-way function (With respect to the issue of relevance, we repeat, that the main advantage of the matrix one-way function is high speed operation). The first variant is the result of the natural development of cryptography and is associated with the use in the cryptography of new tropical arithmetic operations. The results their applications may be named as "Tropical Cryptography." But at the same time, regardless of the general algebraic values "Tropical Cryptography", it is fact, that the construction of multiplicative groups, based on the our tropical operations, may be accepted as an integral part of the realization of the matrix one-way function. Therefore, its adoption and an implementation can be associated with its recognition. The second option, at this stage, is the result of repeated analysis of matrix one-way function and is associated with the use of exponential one-way function within a certain time frame (Assuming the exponential one-way function, which Diffie and Hellman took from Number Theory). However it is obvious that the use of the degree (exponential) one-way function, in a certain time interval is not associated with loss of speed for the matrix one-way function, therefore, and also - for the corresponding key exchange algorithm via an open channel communication or to perform other actions.

-----  
**Keywords:** Cryptography, matrix one-way function, key exchange algorithm, Tropical Cryptography.