Construction of New Matrix One-Way Function and Tropical Cryptography

Richard Megrelishvili
Email: richard.megrelishvili@tsu.ge
Department of Computer Science of Tbilisi State University
University St. 13

The goal of this paper is to substantiate the original high-speed matrix one-way function and key exchange algorithm for an open channel which is considering on based the mentioned matrix one-way function. It is connected, obviously, with the existing global problem. This problem lies in the fact that in the present no other one-way functions (known and recognized) which would have a higher speed than the same functions in the asymmetric algorithms of Diffie-Hellman and RSA. The author concludes that such a function may be a matrix one-way function, which is described in this paper. The paper also examines the new tropical operations to build the systems of the tropical cryptography.

Matrix one-way function has the following form (It should also be noted that the one-way functions used in the algorithms of Diffie-Hellman and RSA, there are well-known functions in number theory, while matrix one-way function by us has been studied and accepted):

$$v A = u,$$

where each matrix $A \in \hat{A}$ is a secret parameter, it is selected at random from the set $\hat{A}$ high cardinality; the initial matrix of the set $\hat{A}$ (i.e. a generator-matrix) is open, so we can say that $\hat{A}$ is open; also $v, u \in V_n$ are open (For simplicity, is considered GF(2) field).This function is fundamentally different from the function which is used in the algorithms of Diffie-Hellman and RSA, because it uses the multiplication operations, instead of exponential operations. Therefore, this function will be implemented with a much faster rate and it will be competitive with respect to symmetric systems, however, as an asymmetric system, it has its own special advantages.

In this paper we introduce new tropical operations, which for simplicity also are considered for systems over the field GF (2). In the binary case the additive operations remain the same as in the classical case, but the multiplication operations are fundamentally changing. We use the properties of the newly introduced operations and also of other areas of cryptography, such as encryption and decryption of information, etc (Detailed consideration of issues of tropical cryptography is beyond the scope of abstracts).

,