Tropical Cryptography and Two Variants of Implementation of the Original Matrix One-Way Function

Richard P. Megrelishvili
I. Javakhishvili Tbilisi State University,
University St. 13, 0186 Tbilisi, Georgia

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-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 - 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.

1. INTRODUCTION

The analysis showed that the matrix-way function is broken, if it is used without a joint application with Tropical cryptography or without the use of one-way function (ie, the function is not a carrier of properties one-way function if it is applied without any special versions of, see below).

Matrix one-way function is as follows:

$$v\ A = u. \qquad (1)$$

Where A Є Ă, a Ă is a set of high power from an n-dimensional quadratic commutative matrices [1]. Along with this, v, u Є V_n. Where V_n vector space of dimension n (for simplicity Ă and V_n is considered over the Galois field GF(2)). In expression (1) v and u are open and A' is secret, although A - initial matrix is open with which may be formed a plurality Ă (e.g., a plurality Ă can be produced with degrees of matrix A). Therefore, if the expression (1) is considered as a one-way function, then it can break down in the following ways: 1. If the matrix set Ă contains recursion (that was identified by us), then the expression (1) can easily be broken with the help Companion matrices, that is, the set of n^2 unknown can be lead to a matrix with n unknowns, for any square matrix A' Є Ă can be bring to n unknown, i.e., using the equation (1) can obtain a system of n equations in n unknowns, etc. These issues have been discussed in [2-5, 6]. 2. If the matrix of set of Ă does not contain recursion (or hard to find), then the matrix one-way function can be broken with the use of the basic matrixes of A^0, A^1, A^2,..., A^{n-1} which is not hard to get, if we know the initial matrix A.

2. ON THE POSSIBILITY OF BREAKING THE MATRIX ONE-WAY FUNCTION

We want to show that though (1) the matrix one-way function is broken without additional versions, but this is exceptional function. It is special function because of its speed and therefore deserves special attention. We are convinced that the additional versions will not reduce the speed and efficiency of the entire system. It is interesting, how it is can be possible with additional means maintained the speed, the efficiency and the strength of the system? In addition, for this article we consider the ability to break of matrix one-way function, and then we will discuss the possibilities of using tropical cryptography and exponential one-way function. We'll look at how break the matrix one-way function with the use of said of basis matrixes (other questions, how to hack the function (1), were considered in [2-5,6]). We will consider breaking this function in the particular example.

Suppose, it is given the multiplicative group Ă of the commutative matrices of dimension 3x3 (the group has a maximal order, e = 23 - 1 = 7):

$$A=\begin{pmatrix}1&0&1\\1&0&0\\0&1&1\end{pmatrix},\quad A^2=\begin{pmatrix}1&1&0\\1&0&1\\1&1&1\end{pmatrix},\quad A^3=\begin{pmatrix}0&0&1\\1&1&0\\0&1&0\end{pmatrix},\ldots,A^7=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}. \qquad (2)$$

Suppose, the two subjects X (Alice) and Y (Bob) can form the secure key k with matrix one-way algorithm via public channel (This algorithm is based on a matrix one-way function (1)). Then Alice selects matrix $A_1 = A^2$ as the secret matrix in (2). Bob, for his part, chooses the matrix $A_2 = A^3$, we also assume that v = (110). Then our algorithm will be functioning as follows:

- Alice computes and sends to Bob the following vector:

$$u_1 = v\, A_1 = (011). \qquad (3)$$

- Bob computes and sends to Alice the following vector:

$$u_2 = vA_2 = (111). \qquad (4)$$

- Elice computes the exchanged key:

$$k_1 = u_2A_1 = (100). \qquad (5)$$

- Bob computes the exchanged key:

$$k_2 = u_1A_2 = (100). \qquad (6)$$

As we see $k = k_1 = k_2$ and the results are correct (The matrixes are commutative: $vA_1A_2 = vA_2A_1$).

As noted above, we plan to break the algorithm by means of the basis matrix comprising a multiplicative set $\breve{A} = \{ c_0\, A^{2^0} . c_1\, A^{2^1} \ldots\ c_{n-1}\, A^{2^{n-1}} \}$ (where $\{c_0,\ c_1, \ldots, c_{n-1}\} \in$ GF(2)). For a set of (2) we form an appropriate basis:

$$A^0 = I,\ A^1, A^2, \qquad (7)$$

Where $A^0 = I$ is the identity matrix. In the beginning we define the matrix $A_1 = A^2$ selected by Alice. The required matrix is denoted by $A_1(x)$, then we will have:

$$A_1(x) = c_0 A^0 + c_1A^1 + c_2 A^2. \qquad (8)$$

Since Ellis opened calculates the value of $u_1 = v\, A_1(x)$, then we have:

$$u_1 = v\, A_1(x) = c_0 vA^0 + c_1vA^1 + c_2vA^2 = c_0w_0 + c1w_1 + c_2w_2. \quad (9)$$

Considering (2), (3) and (9) we can determine the values of u_1 and w_0, w_1, w_2:

$$vA^0 = (110)\, A^0 = (110) = w_{0,}$$

$$vA^1 = (110)\, A^1 = (001) = w_{1,} \qquad (10)$$

$$vA^2 = (110)\, A^2 = (011) = w_{2,}$$

$$u_1 = (011).$$

Using (9) and (10) we may form a system of equations for the coefficients c_0, c_1, c_2:

$$1c_0 + 0c_1 + 0c_2 = 0,$$

$$1c_0+0c_1+1c_2 = 1, \qquad (11)$$

$$0c_0 + 1c_1 + 1c_2 = 1.$$

Solving the system of equations (11), we define the values of the coefficients: $c_0 = 0$, $c_1 = 0$, $c_2 = 1$. Then, from (8) we obtain the value of the ratio of the desired matrix: $A_1(x) = A^2$, i.e. get the matrix A^2 of (2). The answer is correct. (Similar we can find the matrix A_2, chosen by Bob).

3. TWO EMBODIMENT OF THE ONE-WAY FUNCTION MATRIX

As stated above, this paper first announced two special versions of the matrix one-way function. First option, as a result of the natural development of cryptography, involves the use of new tropical arithmetic operations in cryptography. When applying was found that the new tropical operations apart from a general purpose can be thought integral part of our matrix one-way function. Therefore, if earlier, for the construction of matrices Ă had to use classical arithmetic operations, it is now necessary to apply our new tropical arithmetic. With new tropical operations, we must build a set of matrices Ă with the properties with the same as before: high dimension and order, i.e. we should construct a multiplicative group Ă that is formed by degrees of an initial matrix A of new form (of a new structure). Construction of a new matrix of Ă, as noted above, is already a meaningful (traditional) problem and we would not have shown any effect if there was not having contact with her. Consider the issues of the first option, that we have introduced, or questions about Tropical Cryptography.

The obtained tropical operations, for simplicity, considered over the Galois field GF (2). Additive operations, in this case, are the same as the classical operations:

$$0 + 0 = 0;\ 0 + 1 = 1;\ 1 + 0 = 1;\ 1 + 1 = 0. \qquad (12)$$

But the multiplicative operations are fundamentally different from the classical operations [7]:

$$0 * 0 = 0;\ 0 * 1 = 1;\ 1 * 0 = 1;\ 1 * 1 = 1. \qquad (13)$$

Interestingly, what feature and utility of our proposed tropical operations? Must be stated that the new operations cause so impressive effect in their application that raises another question? It is about ensuring the stability of the matrix one-way function (1), i.e. on the solubility or insolubility of the system of equations (11), depending on what kind of arithmetic operations will be applied - the classic or offered by us? For example, in our opinion, the system of equations (11) does not have a unique solution, matrix-way function (1), with tropical operations will not be broken, and satisfies the conditions of stability (under appropriate conditions, implying the proper dimension and higher order for a set of matrices Ă). Indeed, when using the new operations (12) and (13), a system (14) has not a unique solution in real time (to the counterweight (11)), since by multiplication coefficients of w_0, w_1, w_2 on the coefficients c_0, c_1, c_2 will not cause the formation of null values but on the contrary, causes the formation of new unknowns (While, in the classical operations and using the Gauss method, the system (11) is rapidly soluble):

$$1 * c_0 + 0 * c_1 + 0 * c_2 = 0,$$

$$1 * c_0 + 0 * c_1 + 1 * c_2 = 1, \qquad (14)$$

$$0 * c_0 + 1 * c_1 + 1 * c_2 = 1.$$

For example, the first line of system (14) has the six unknowns, therefore, when dimension has high order (and there are used our tropical operations), the system (14) does not has a solution in real time. Therefore, our matrix one-way function according to the first embodiment ensures durability, since it is not can to break in real time (Take into account the fact that tropical group (15) is a multiplicative group and not a field). As an example we present the multiplicative group (in

(14) are used: A^0, A^1, A^2, which are a base of (15) matrixes and the corresponding $u = vA^3$, where $v = (110)$):

$$A=\begin{pmatrix}1&0&1\\1&0&0\\0&1&0\end{pmatrix},\ A^2=\begin{pmatrix}1&0&0\\0&0&1\\0&0&0\end{pmatrix},\ A^3=\begin{pmatrix}0&0&1\\1&1&0\\0&1&1\end{pmatrix},\dots,\ A^7=A^0=\begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix} \qquad (15)$$

The implementation of the algorithm according to (15) does not differ from the implementation of the algorithm (3) - (6), since the main issue here - the generation of the multiplicative group of maximal order, which meets the requirements of Tropical Cryptography (12) - (13).

Interestingly than can one explain that - the second embodiment has, too, a high efficiency and durability as the first, whereas radically different from the first? In a second embodiment, with respect to the matrix of our one-way function is used a different one-way function (i.e. there is a new problem), but as a method of processing, it shows identity with the decision of other cryptography tasks, which, in our opinion, deserves attention (see. below).

For example, ElGamal uses a one-way function to solve their problems, but the thing is - how? He uses a one-way function periodically, for a certain length of time [8]. The similarity with our second option is a period of time for which use the function [9]. In the algorithm of ElGamal degree one-way function is used within a certain time period, to meet the challenges of authentication and verification, we use it also within a certain time period, to resolve the problem of the steady of our matrix one-way function. To do this periodically, by using a degree one-way function is occurs a key exchange via the open channel and the exchanged key is use as secret parameter (k = v) in the same time period, when we realized exchange the keys with our algorithm. In this case, in (1) parameters v, A' are secret and only parameter u is open. This change defines the steady of (1) one-way function and - of (3) - (6) the algorithm and it does not cause decrease in the rate of operations.

4. REFERENCES

[1] R.Megrelishvili, M.Chelidsze, K.Chelidze, "On the construction of secret and public key cryptosystems," Iv.Javakhishvili Tbilisi State University, I.Vekua Institute of Applied Mathematics, Informatics and Mechanics (AMIM), v. 11, No 2, 2006, pp. 29-36.

[2] R.Megrelishvili, A.Sikharulidze, "New matrix sets generation and the cryptosystems," Proceedings of the European Computing Conference and 3rd International Conference on Computational Intelligence, Tbilisi, Georgia, June, 26-28, 2009, pp. 253-255.

[3] R.Megrelishvili, M.Chelidze, G.Besiashvili, "Investigation of new matrix-key function for the public cryptosystems". Proceedings of The Third International Conference, Problems of Cybernetics and Information, v.1, September, 6-8, Baku, Azerbaijan, 2010, pp. 75-78.

[4] R.Megrelisvili, M.Chelidze, G.Besiashvili, "One-way matrix function - analogy of Diffie-Hellman protocol", Proceedings of the Seventh International Conference, IES-2010, 28 September-3 October, Vinnytsia, Ukraine, 2010, pp. 341-344.

[5] R.Megrelishili, M.Jinjikhadze, Matrix one-way function for the exchange of cryptographic keys and method for the generation of multiplicative matrix groups ", in Proceedings of The International Conference SAIT 2011, May 23-28, Kyiv, Ukraine, in 2011. p. 472.

[6] W.P.Wardlaw, Matrix Reprezentacion of Finite Fields, U.S. Navy, March 12, 1992, pp. 1-10, NRL/MR/5350.1-92-6953.

[7] R.P.Megrelishvili, New Direction in Construction of Matrix One-Way Function and Tropical Ctyptography, Archil Eliashvili Institute of Control Systems of The Georgian Technical University, Proceedings, N 16, 2012, pp.244-248.

[8] T.ElGamal. "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transaction on Information Theory, v. IT-31, n. 4, 1985, pp. 469-472.

[9] W.Diffie and M.E.Hellman. New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22, n.6, Nov. 1976, pp. 644-654.