Two New Versions of Numbers Fast Multiplication and Tropical Cryptography

Richard P. Megrelishvili
Department of Computer Sciences
Iv.Javakhishvili Tbilisi State University,
University Str.13, 0186 Tbilisi, Georgia

ABSTRACT

This article discusses the rapid multiplication of two numbers. But first considered [1] the work that created the foundation of [1].

In this article [1] is took into consideration and used the fact that the leading countries in cryptography used the ElGamal algorithmic method (Digital Signature). This method is used, just like in an algorithm, for performing certain actions in a certain period of time. Our new one-way matrix function [1] is a protected algorithm that meets the known qualities of asymmetric cryptography, i.e. it is not directly related of Number Theory to the exponential functions of $a^x = y$ (mod p) and Euler's Theorem. That is why it [1] (2013) is distinguished with high speed, i.e. connected to of vector and of matrix multiplication operations with simplicity (This article also discusses protection issues of algorithm).

Naturally, the question is: do use more Diffie-Hellman algorithm (as well as the RSA algorithm) for the same period of time?

This important fast realizing is considered in the present article. Get a new results multiplication of numbers in high speed with module considering.

It is when the two vectors (as two numbers) are multiplied to each other.

Keywords

Digital signature, matrix one-way function, key exchange algorithm, Tropical cryptography.

1. INTRODUCTION

The idea of the product of a vector on a matrix arose earlier, back in 2006 [2]. It was necessary to generate sets of matrices in two directions: 1.When the order of the matrices is maximal, 2.When the order of the matrices coincides with the Mersenne numbers. After successful studies of matrix sets, tropical cryptography has been obtained [3] (here are other publications), which is based on the change of classical operations (see this article). Following proper analysis, [1] the one-way functionality of the algorithm was protected with ElGamal method, which led the way today's article.

For this you do not need to use one parameter of confidentiality what for example has the ElGamal address. Some two parameters need to be secret. Which gives us the opportunity to use Diffie-Hellman and RSA of algorithms the secrecy of the appropriate parameters.

2. TWO VERSIONS OF THE RESULTS

<u>Like the Diffie-Hellman algorithm</u>**.**

After some adjustment the Diffie-Hellman algorithm is the first version. First of all, let's define the options. The N and n parameters is defined and is secure by the algorithm of Diffie-Hellman (N^{-1} value is determined by the Y side, it is obvious that $NN^{-1} = 1$ (mod n). The secrecy of the number here is guaranteed by the ordinary algorithm of Diffie-Hellman, for a certain section of time.

New let's quickly multiply the M and N numbers.

Consider now the M is a message (information) and by X side was encrypted and transmitted to an open channel to Y side and the Y side it is decrypted. This will be done: C = M N (mod n) (M = CN^{-1}(mod n)). The algorithm is implemented, or the number M is fast multiplied by N number.

<u>Like the RSA algorithm.</u>

After some correction, RSA is the second fast version. First of all, it is necessary to define the Euler's f(N) function and with the ordinary algorithm of Diffie-Hellman to create its secrecy, i.t. from X side to the Y side f(n) is transfer (f(n) is Euler's function).

It is also important to define the e and d values for mod f(n) (e and d is classified as a secret).

New let's quickly multiply the M and e numbers (M is message, or information).

After that, the X side on open channel to the Y side C information has transmission, i.e. C = M e (mod f (N)) (Then it is restore the information provided by the Y side: M = C d (mod f (N))).

The algorithm is implemented, or the number M is multiplied by e number.

(It may be that the algorithm of numbers fast multiplied includes another variant of the RSA algorithm associated with the mod n, n = p q).

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

The analysis showed that the matrix 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 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 [2]. Where v, u

Є V_n. V_n is 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 (without any special versions) 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).

We want to show that though (1) the matrix 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 [4-7]). 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 = 2^3 - 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:

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

_ Bob computes and sends to Alice the following vector:
2

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

_ Alice computes the exchanged key:

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

_ Bob computes the exchanged key:

$k_2 = u_1A_2 = (100)$. (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 Ă = { $c_0\, A^{2^0}. c_1\, A^{2^1} \ldots\ c_{n-1}\, A^{2^{n-1}}$ } (where { $c_0, c_1, \ldots, c_{n-1}$ } Є GF(2)). For a set of (2) we form an appropriate basis:

$A^0 = I,\ A^1, A^2, \ldots$ (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:

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

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

$u_1 = v\ A_1(x) = c_0\, vA^0 + c_1vA^1 + c_2vA^2 = c_0w_0 + c_1w_1 + c_2w_2$. (9)

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

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

$vA^1=(110)A^1=(001)=w_{1,}$ (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:

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

$1c_0+0c_1+1c_2=1,$ (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).

4. TWO EMBODIMENT OF THE ONE-WAY MATRIX FUNCTION

This article is the result of an investigation of matrix one-way functions. As stated above, this paper 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:

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

But the multiplicative operations are fundamentally different from the classical operations [3.8-11]:

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

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 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 function (1), with tropical operations, is one-way function, it will not be broken in real time, 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 (to the counterweight (11)), since by multiplication coefficients of c_0, c_1, c_2 on the w_0, w_1, w_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):

$$\begin{aligned} &1 * c_0 + 0 * c_1 + 0 * c_2 = 0, \\ &1 * c_0 + 0 * c_1 + 1 * c_2 = 1, \qquad (14) \\ &0 * c_0 + 1 * c_1 + 1 * c_2 = 1. \end{aligned}$$

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 (15). For the key exchange algorithm are used: A is an Initial Matrix of (15) 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.

For example, ElGamal uses an exponential 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 [9]. The similarity with our

second option is a period of time for which use the function. In the algorithm of ElGamal degree (exponential) 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 stability of our matrix one-way function. For this, by using exponential one-way function occurs a key exchange via the open channel. The result of this key exchange is the secret parameter k = v. In this same time period occurs the key exchange, or other operations carried out, with our algorithm. In this case, in (1) parameters v, A' are secret and only u parameter is open. This change defines the stability of one-way function (1) and also of algorithm (3) - (6), and it does not cause decrease the rate of operations.

5. REFERENCES

[1] R.P.Megrelishvili, Analysis of the Matrix one-Way Function and Two Variants of Its Implementation, International Journal of Multidisciplinary Research and Advances in Engineering (IJMRAE), Vol. 5, No. IV (Octomber2013), pp. 99-105.

[2] R. Megrelishvili, M.Chelidsze, K.Chelidze, Construction of Secret and Public Key Cryptosystems, Iv.Javakhishvili Tbilisi State University, of I.Vekua Institute of Applied Mathematics, Informatics and Mechanics (AMIM), v. 11, No 2, 2006, pp. 29-36.

[3] 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.

[4] Richard P. Megrelishvili, Tropical Cryptography and Analysis of Implementation of New Matrix One-Way Function, Proceedings of the 2014 International Conference on Mathematical Models and Methods in Appled Sciences (MMAS '14). Saint Peterburg, Russia, September 23-25, 2014, pp. 273-275.

[5] R.Megrelishvili, A.Sikharulidze, New matrix sets generation and the cryptosystems, Proceedings of the European Computing Conference and 3th International

Conference on Computational Intelligence, Tbilisi, Georgia, June, 26-28, 2009, pp. 253-255.

[6] R. Megrelishvili, M.Chelidze, G.Besiashvili, Investigation of New Matrix-Key Function for the Public Cryptosystems, Proceedings of Third International Conference, Problems of Cybernetics and Information, v.1, September, 6-8, Baku, Azerbaijan, 2010, pp. 75-78.

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

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

[9] 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.

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

[11] R.L.Rivest, A. Shamir and I.M. Adleman, A Method for Obtaining Digital Signature and Public-Key Cryptosystems, Communications of the ASM, v. 21, n. 2, Feb. 1978, pp. 120-126.