ON THE ORIGINAL ONE-WAY MATRIX FUNCTION AND THE IMPLEMENTATION OF THE KEY EXCHANGE PROTOCOL ON OPEN CHANNEL

R. Megrelishvili[1], S. Shengelia[2]

[1]Ivane Javakhishvili Tbilisi State University
0186 University Street 2, Tbilisi, Georgia
[2]Sokhumi State University
0186 Anna Politkovskaia Street 9, Tbilisi, Georgia

(Received: 20.11.2012; accepted: 30.12.2012)

Abstract

The aim of this work is the foundation of a new original high speed performing matrix algorithm, about key-exchange on open channel. According to the plan, the high speed performance of a new algorithm should be approximately like the ones, that are used by the cryptographic encryption and decryption algorithms of the symmetric systems. The achievement of this goal, seems to be related with the existing global problems, as for now, there are no existing asymmetric systems which have high speed performance like the one, that symmetric system has.

Key words and phrases: Open channel, key exchange, one-way function.

AMS subject classification: 1594.

1 Introduction

First one-way matrix function was recorded in the work [1], in which it was presented as the operation of multiplication of a vector on a matrix. On the basis of this one-way matrix function, given in the same work [1] for the first time, the key exchange on open channel was also described (An algorithm, alternative to the Diffie-Hellman protocol [2]). Future results were published in the following works, for example[3-7]. The answer on the question about high speed performance of one-way matrix function, already shown in the annotation paragraph of this work, directly follows from the answer on the question about - From what kind of operations consists one-way matrix function itself? According to the authors, after getting familiar with the subsequent paragraph, there should be no doubts about the high speed performance of the matrix function, as well as about high speed performance of the key-exchange algorithm on open channel.

2 One-Way Matrix Function and Key-Exchange Algorithm on Open Channel Connection

For the implementation of the one-way matrix function $n \times n$ matrix A is given. For the simplicity of the statement, the matrices are considered over the GF (2) field. Matrix A presents a secret parameter, selected randomly from a group of high powered $\hat{A}$; so, $A \in \hat{A}$, $v \in V_n$ where V_n is a vector space over GF (2) (v is an open parameter). Then, one-way matrix function looks like this:

$$v\ A = u, \tag{1}$$

where, both $u \in V_n$ and u are open parameters.

It should be mentioned, that if for Diffie-Hellman's algorithm the one-way function

$$a^x = y\ mod\ p \tag{2}$$

Is based on a problem of a discrete logarithm, then for function (1) the problem appears to be the recursion inside the matrix. This problem was examined in details in the works [3-7].

Whatever concerns the high speed performance of the functions (1) and (2), they could be judged, as it was already mentioned above, according to their operation character.

Function (1) fundamentally differs from function (2), as for function (1) the operation of multiplication is used, while for function (2) - exponential function.

Matrix algorithm about key-exchange on open channel is implemented the following way:

• Alice (randomly) chooses $n \times n$ matrix $A_1 \in \hat{A}$ and sends the following vector to Bob:

$$u_1 = v\ A_1. \tag{3}$$

• Bob (randomly) chooses $n \times n$ matrix $A_2 \in \hat{A}$ and sends Alice the vector

$$u_2 = v\ A_2, \tag{4}$$

where n is a size of vectors v, u (open), A_1 and A_2 are (secret) matrix keys.

• Alice computes

$$k_1 = u_2\ A_1. \tag{5}$$

• Bob Computes

$$k_2 = u_1\ A_2, \tag{6}$$

Where, k_1 and k_2 are secret keys. $k_1 = k_2 = k$ because, $k = vA_1A_2 = vA_2A_1$.

3 Construction of cyclic multiplicative groups of initial n x n matrices

As it is shown above, for the implementation of the key-exchange algorithm the presence of multiple $n \times n$ matrices of high power, which at the same time are commutative, is required. Number commutation in Diffie-Hellman's algorithm is implemented naturally, in accordance to (2), while, for our algorithm (1), construction of the commutative multiplicity of $\hat{A}$ for each value dimension n presents a difficult task.

In the Given work, an effective and constructive solution is presented. The characteristics of effective and constructive methods, for construction of the matrices is included in the following:

• For each $n > 1$ dimension, the initial $n \times n$ matrix should generate either the maximum number of matrices $(2^n - 1)$, or this number should be the number of Mersen, meaning. $2^j - 1$, where $j < n$;

• The method of synthesis of any $n \times n$ matrix for any dimension, should be the same (where n is probably implementable maximal dimension of the initial matrices). Hence the technology of the construction for initial matrices should be implementable and similar for any given dimension of n.

Besides the above mentioned, it should be considered, that the structure of the matrices should not contain recursion inside the matrix [3-7].

At the beginning of the presentation of matrix generation method, we would state, that the authors came up to the formation of the presented method during the study process of absolutely different issue. Let's suppose, that the task of determining primitivism of the elements $(1 + \alpha)$ is being considered in the field GF(2^n) according to the module of the cyclic polynomial $p(x) = 1 + x^2 + \cdots + x^n$, where $p(\alpha) = 0$.

Now, let's suppose, that the meanings of j - type element degrees $(1+\alpha)$, provided, that $j < n$. Then, we would have the following order of the element degrees $(1 + \alpha)$, with corresponding field elements and vectors from V_n over the field GF (2):

$$\begin{array}{ll}
(1+\alpha)^0 = 1 & (1000000000...0) \\
(1+\alpha)^1 = 1+\alpha & (1100000000...0) \\
(1+\alpha)^2 = 1+\alpha^2 & (1010000000...0) \\
(1+\alpha)^3 = 1+\alpha+\alpha^2+\alpha^3 & (1111000000...0) \\
(1+\alpha)^4 = 1+\cdots+\alpha^4 & (1000100000...0) \\
(1+\alpha)^5 = 1+\alpha+\cdots+\alpha^4+\alpha^5 & (1100110000...0) \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots ..
\end{array} \tag{7}$$

The structure indicated by the formula (7), is nothing, but the Sierpinski triangle, with all the characteristics of a fractal structure.

Definition 1. Suppose, that the given structure (1) ads a single row as the first row, then we get totally fractal structure (Fig. 1).

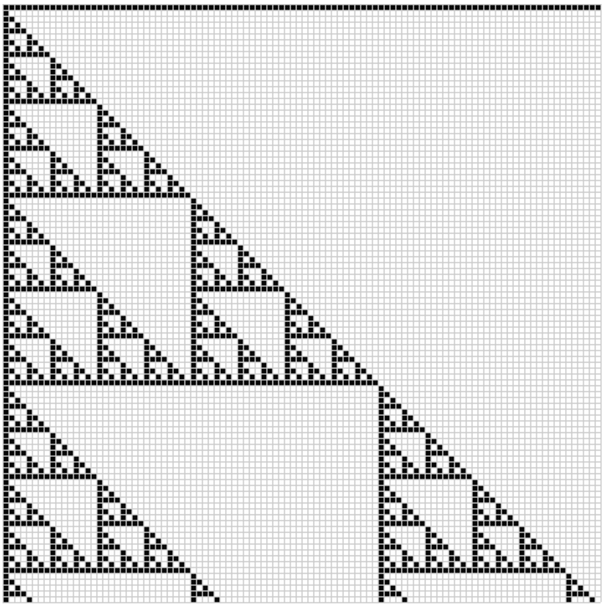


Fig. 1 - Totally fractal structure

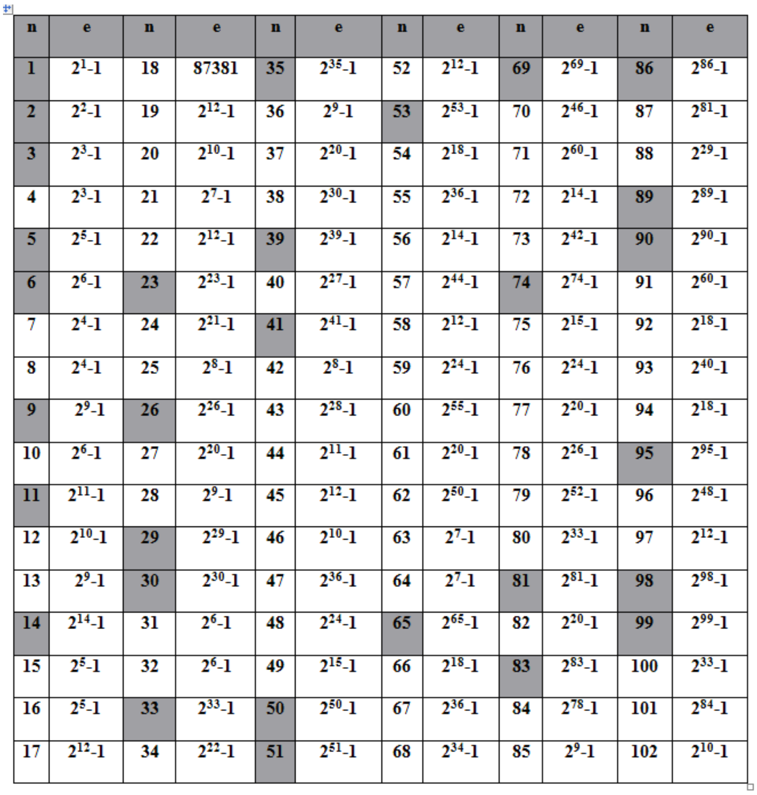
Definition 2. Normal $n \times n$ matrix structure is a matrix formed from the primary $n \times n$ elements, or from first lines and first columns of a total fractal structure.

Example. Below (8) appear normal matrix structures with dimension $n = 2,\ 3,\ 4$ received from total fractural structure:

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}. \tag{8}$$

By using software, orders of e were calculated for the initial normal $n \times n$ matrix structures and the results are shown in the table below



n	e	n	e	n	e	n	e	n	e	n	e
1	2^{1}-1	18	87381	35	2^{35}-1	52	2^{12}-1	69	2^{69}-1	86	2^{86}-1
2	2^{2}-1	19	2^{12}-1	36	2^{9}-1	53	2^{53}-1	70	2^{46}-1	87	2^{81}-1
3	2^{3}-1	20	2^{10}-1	37	2^{20}-1	54	2^{18}-1	71	2^{60}-1	88	2^{29}-1
4	2^{3}-1	21	2^{7}-1	38	2^{30}-1	55	2^{36}-1	72	2^{14}-1	89	2^{89}-1
5	2^{5}-1	22	2^{12}-1	39	2^{39}-1	56	2^{14}-1	73	2^{42}-1	90	2^{90}-1
6	2^{6}-1	23	2^{23}-1	40	2^{27}-1	57	2^{44}-1	74	2^{74}-1	91	2^{60}-1
7	2^{4}-1	24	2^{21}-1	41	2^{41}-1	58	2^{12}-1	75	2^{15}-1	92	2^{18}-1
8	2^{4}-1	25	2^{8}-1	42	2^{8}-1	59	2^{24}-1	76	2^{24}-1	93	2^{40}-1
9	2^{9}-1	26	2^{26}-1	43	2^{28}-1	60	2^{55}-1	77	2^{20}-1	94	2^{18}-1
10	2^{6}-1	27	2^{20}-1	44	2^{11}-1	61	2^{20}-1	78	2^{26}-1	95	2^{95}-1
11	2^{11}-1	28	2^{9}-1	45	2^{12}-1	62	2^{50}-1	79	2^{52}-1	96	2^{48}-1
12	2^{10}-1	29	2^{29}-1	46	2^{10}-1	63	2^{7}-1	80	2^{33}-1	97	2^{12}-1
13	2^{9}-1	30	2^{30}-1	47	2^{36}-1	64	2^{7}-1	81	2^{81}-1	98	2^{98}-1
14	2^{14}-1	31	2^{6}-1	48	2^{24}-1	65	2^{65}-1	82	2^{20}-1	99	2^{99}-1
15	2^{5}-1	32	2^{6}-1	49	2^{15}-1	66	2^{18}-1	83	2^{83}-1	100	2^{33}-1
16	2^{5}-1	33	2^{33}-1	50	2^{50}-1	67	2^{36}-1	84	2^{78}-1	101	2^{84}-1
17	2^{12}-1	34	2^{22}-1	51	2^{51}-1	68	2^{34}-1	85	2^{9}-1	102	2^{10}-1

Table. The results for calculated orders of e for the initial normal $n \times n$ matrices.

It should be mentioned, that the obtained results completely match (for matrix of any dimension) with the results obtained in the work process [8], hence it is well known, that in the work process [8] the initial matrices are absolutely other structures. To be more specific, these are structures, which are attained from generalized codes of Gray. It is also worst to mention, that the order of the matrices in the table is established by the help of sequential computation of all degrees till the dimension of $n = 63$ initial matrix. However, order computation for $n > 63$ dimension, was accomplish by using a special program.

The designated project has been fulfilled by financial support of the Shota Rustaveli National Science Foundation (Grant No 12/60).

References

1. R. Megrelishvili, M. Chelidze, K. Chelidze, On the construction of secret and public-key cryptosystems, *Appl. Math. Inform. Mech.* **11** (2006), no. 2, 29-36.

2. W. Diffie, M. E.Hellman, New Directions in Cryptography. IEEE Transactions on Information Theory. V. IT-22, n.6, Nov, 1976, pp. 644-654

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

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

5. 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.

6. R. Megrelishvili, G. Besiashivli, S. Shengelia, New one-way matrix function and public key-exchange, Proceedings of International Conference SAIT 2011, System Analysis and Information Technologies, Kyiv, Ukraine, May 23-28, 2011, p. 407.

7. R. Megrelishvili, G. Besiashivli, S. Shengelia, Original one-way cryptography function using n x n matrices, Proceedings of the 11th International Conference, Pattern Recognition and Information Processing, PRIP 2011, (18-20 May 2011), Minsk, Belarus, 2011, pp. 355-357.

8. A. Belitski, D. Stetsenko, Order of Abelian Cycle Groups, generated by the generalized transformation of Gray, Electronics and signal management systems, N1(23), 2010, pg 5-11.