Bulletin of TICMI
Vol. 23, No. 1, 2019, 3–8

Research and Synthesis of Fractal Structures for Cryptographic Algorithms

Sofia Shengelia*

Sokhumi State University
61 Politkovkaia St., 0186, Tbilisi, Georgia
(*Received October 09, 2018; Revised February 25, 2019; Accepted March 1, 2019*)

The present paper is devoted to constructing a set of high order strong matrices for an open channel key exchange matrix algorithm and creating a quick one-way matrix function. A high order fractal matrix set consisting of primitive matrices was constructed. The fractal family consisting of matrices and used in the cryptographic algorithm was studied. This issue concerns a global problem.

Keywords: Fractal structures, Matrix, Cryptographic algorithm.

AMS Subject Classification: 15B99.

1. Introduction

Each cryptographic system uses its own procedure, types of keys, methods of their distribution and coding algorithms. The basis of the asymmetric cryptography is the specificity of the one-way function. The one-way function is a $y = f(x)$ function, the meaning of which is possible to obtain by computer calculations in case x is known, whereas the meaning of x argument is impossible to receive by means of $f(x)$ function meaning by computer calculations in a real time. This is obviously illustrated by the Diffie-Hellman one-way function example $a^x = y(\mathrm{mod}p)$.

First one-way matrix function was recorded in the work 2006, 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 for the first time, the key exchange on open channel was also described [1]-[3] (An algorithm, alternative to the Diffie-Hellman protocol). Future results were published in the following works. The answer to 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 to 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 the open channel.

* Email: sofia_shengelia@mail.ru

ISSN: 1512-0082 print

2. Matrix function

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:

$$vA = u, \tag{2.1}$$

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

$$a^x = y \mathrm{mod} p \tag{2.2}$$

is based on a problem of a discrete logarithm, then for the function the problem appears to be the recursion inside the matrix. Whatever concerns the high-speed performance of the functions and, they could be judged, as it was already mentioned above, according to their operation character. One-way function fundamentally differs from one-way function, as for one-way function the operation of multiplication is used, while for function-exponential function.

3. Matrix algorithm about key-exchange on open channel is implemented in the following way

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

$$u_1 = vA_1, \tag{3.1}$$

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

$$u_2 = vA_2, \tag{3.2}$$

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

• Mariam computes

$$k_1 = u_2 A_1, \tag{3.3}$$

• George computes

$$k_2 = u_1 A_2, \tag{3.4}$$

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

The one-way matrix function and a new matrix algorithm for the corresponding open channel key exchange considered in this paper was obtained and studied for the first time by Doctor of Technical Sciences, Professor R. Megrelishvili.

For simplicity, the square matrices of the n order and other structures are considered in Galois GF(2) field. It is obvious that to generate high power matrix set for the functioning of the new key exchange function is especially important. The synthesis of such matrix sets and their structural study attracts attention [1]-[4], [6].

The new algorithm is an original cryptographic approach, especially when its quickness is taken into account. However, at the same time this algorithm needs analyzing in regard to its cracking and generating a required set of high order matrices. Study, analysis and software implementation of such issues is also the main goal.

4. Software Implementation

The study object is a matrix, discovery of such a structure, the existence of which makes the matrix to generate a multiplication cyclic group of matrices with a maximum value or a value equal to the Meresenne prime degree.

In order to find out such structures it was necessary to verify matrices of different orders regarding whether this scheme gave such a multiplication group of matrices that was generated by any matrix constructed by this structure and the value of the degree of which was maximal, i.e. whether this matrix was primitive (a matrix is primitive in case it generates a group with maximum value of the degree). For this purpose a method for natural increase of matrix order has been introduced, among them a method for natural increase of the n order.

Several types of nondegenerate initial matrixes were experimentally tested. As a result, a general structure was obtained, the matrixes obtained from which generate multiplication groups, sometimes with maximum degree value and sometimes - with a degree value equal to Mersenne prime. Only in a single case (except when $n = 18$) [5],[7], [8] the matrix degree value is not a Mersenne prime and it is a subject to an individual structural study. The paper also touches new original fractal matrix structures, banded matrices, etc.

The original matrix algorithm described in the paper is in some degree a similar model to the Diffie-Hellman open channel key exchange algorithm. When the Diffie-Hellman algorithm stability depends on the highest values of p simple number (i.e. stability depended on a real scale of time), the one-way matrix function stability also depends on the high value of the A set.

The research was carried out for the matrices that were free from the internal recursion. A high order matrix set consisting of primitive matrixes was constructed (see Figure 1, Figure 2, Figure 3).

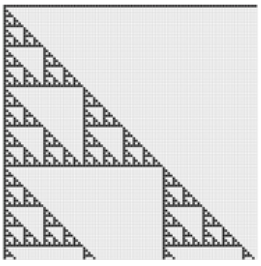

Figure 1. Totally Fractal Structure

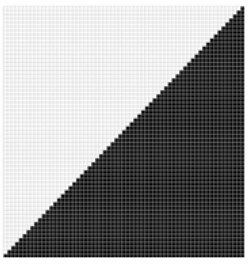

Figure 2. Triangular Fractal Matrix

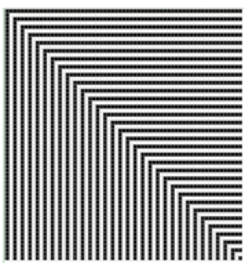

Figure 3. Fractal Matrix

Matrix of the first Fractal structure:

$$n=3,\ A=\begin{pmatrix}1&1&1\\1&0&0\\1&1&0\end{pmatrix};\ n=4,\ A=\begin{pmatrix}1&1&1&1\\1&0&0&0\\1&1&0&0\\1&0&1&0\end{pmatrix};n=5,\ A=\begin{pmatrix}1&1&1&1&1\\1&0&0&0&0\\1&1&0&0&0\\1&0&1&0&0\\1&1&1&1&0\end{pmatrix}. \quad (4.1)$$

Matrix of the second Fractal structure:

$$n=3,\ A=\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix};\ n=4,\ A=\begin{pmatrix}0&0&0&1\\0&0&1&1\\0&1&1&1\\1&1&1&1\end{pmatrix};n=5,\ A=\begin{pmatrix}0&0&0&0&1\\0&0&0&1&1\\0&0&1&1&1\\0&1&1&1&1\\1&1&1&1&1\end{pmatrix}. \quad (4.2)$$

Matrix of the third Fractal structure:

$$n=3,\ A=\begin{pmatrix}1&1&1\\1&0&0\\1&0&1\end{pmatrix};\ n=4,\ A=\begin{pmatrix}1&1&1&1\\1&0&0&0\\1&0&1&1\\1&0&1&0\end{pmatrix};n=5,\ A=\begin{pmatrix}1&1&1&1&1\\1&0&0&0&0\\1&0&1&1&1\\1&0&1&0&0\\1&0&1&0&1\end{pmatrix}. \quad (4.3)$$

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 (Table 1).

1. Each initial n order square matrix is primitive (the degree value is equal to 2^n-1) or its degree value is a Mersenne prime 2^j-1, when $j<n$ (except $n=18$);

2. The corresponding matrices of the pairs (3, 4), (7, 8), (15,16), (31, 32), (63, 64), (127, 128), (255, 256) and (511, 512) of values $(n,\ n+1)$ are described by the following formulae:

$$A_{2^r-1}^{2^{r+1}-1}=E_{2^r-1};\quad A_{2^r}^{2^{r+1}-1}=E_{2^r},\quad \text{where } r\geq 2. \quad (4.4)$$

3. It is also noteworthy that nowadays in cryptographic algorithms the 2^{89} probable selection variants are very difficult task even for the latest computers. We have calculated all matrices including the 600×600 size matrices. Each initial n order square matrix is primitive, the degree value is equal to 2^n-1 (Table 2).

4. It is noteworthy that these results completely coincide with the results of Ukrainian scientist, Professor Anatoly Beletsky. Although it is well known that in [9] the initial matrices are completely different structures, i.e. structures that are derived from generalized Gray Codes.

n	e	n	e	n	e	n	e	n	e	n	e	n	e	n	e
1	2^1-1	17	2^{12}-1	33	2^{33}-1	49	2^{15}-1	65	2^{65}-1	81	2^{81}-1	97	2^{12}-1	113	2^{113}-1
2	2^2-1	18	87381	34	2^{22}-1	50	2^{50}-1	66	2^{18}-1	82	2^{20}-1	98	2^{98}-1	114	2^{38}-1
3	2^3-1	19	2^{12}-1	35	2^{35}-1	51	2^{51}-1	67	2^{36}-1	83	2^{83}-1	99	2^{99}-1	115	2^{30}-1
4	2^3-1	20	2^{10}-1	36	2^9-1	52	2^{12}-1	68	2^{34}-1	84	2^{78}-1	100	2^{33}-1	116	2^{29}-1
5	2^5-1	21	2^7-1	37	2^{20}-1	53	2^{53}-1	69	2^{69}-1	85	2^9-1	101	2^{84}-1	117	2^{92}-1
6	2^6-1	22	2^{12}-1	38	2^{30}-1	54	2^{18}-1	70	2^{46}-1	86	2^{86}-1	102	2^{10}-1	118	2^{78}-1
7	2^4-1	23	2^{23}-1	39	2^{39}-1	55	2^{36}-1	71	2^{60}-1	87	2^{81}-1	103	2^{66}-1	119	2^{119}-1
8	2^4-1	24	2^{21}-1	40	2^{27}-1	56	2^{14}-1	72	2^{14}-1	88	2^{29}-1	104	2^{45}-1	120	2^{12}-1
9	2^9-1	25	2^8-1	41	2^{41}-1	57	2^{44}-1	73	2^{42}-1	89	2^{89}-1	105	2^{105}-1	121	2^{81}-1
10	2^6-1	26	2^{26}-1	42	2^8-1	58	2^{12}-1	74	2^{74}-1	90	2^{90}-1	106	2^{70}-1	122	2^{84}-1
11	2^{11}-1	27	2^{20}-1	43	2^{28}-1	59	2^{24}-1	75	2^{15}-1	91	2^{60}-1	107	2^{28}-1	123	2^{36}-1
12	2^{10}-1	28	2^9-1	44	2^{11}-1	60	2^{55}-1	76	2^{24}-1	92	2^{18}-1	108	2^{15}-1	124	2^{41}-1
13	2^9-1	29	2^{29}-1	45	2^{12}-1	61	2^{20}-1	77	2^{20}-1	93	2^{40}-1	109	2^{18}-1	125	2^{25}-1
14	2^{14}-1	30	2^{30}-1	46	2^{10}-1	62	2^{50}-1	78	2^{26}-1	94	2^{18}-1	110	2^{24}-1	126	2^{110}-1
15	2^5-1	31	2^6-1	47	2^{36}-1	63	2^7-1	79	2^{52}-1	95	2^{95}-1	111	2^{37}-1	127	2^8-1
16	2^5-1	32	2^6-1	48	2^{24}-1	64	2^7-1	80	2^{33}-1	96	2^{48}-1	112	2^{60}-1	128	2^8-1

Table 1. The results for calculated orders of e for the initial normal $n \times n$ matrices

119	183	233	281	338	410	443	530
131	186	239	293	350	411	453	531
134	189	243	299	354	413	470	543
135	191	245	303	359	414	473	545
146	194	251	306	371	419	483	554
155	209	254	309	377	426	491	558
158	210	261	323	378	429	495	561
173	221	270	326	386	431	509	575
174	230	273	329	393	438	515	585
179	231	278	330	398	441	519	593

Table 2. Higher order matrices

The paper considers the original quick matrix function used for construction of algorithms; the pre-requisite of the one-way of the matrix function is considered. The considered one-way matrix function is quick as it requires only multiplication and addition operations. The research is conducted for matrices that are free from internal recursion. A high order matrix set consisting of primitive matrices is constructed. A fractal family consisting of matrices used for key exchange matrix algorithm is studied. One of the most essential tasks of Asymmetric Cryptography is to improve its quickness.

Acknowledgements

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) [#YS17_40].

References

[1] R. Megrelishvili, M. Chelidze, K. Chelidze, *On the construction of secret and public-key cryptosystems*, Appl. Math. Inform. Mech. **11**, 2 (2006), 2936

[2] 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, September 6-8, 2010, Baku, Azerbaijan, 75-78

[3] R. Megrelishvili, *New direction in construction of matrix one-way function and tropical cryptography*, Archil Eliashvili Institute of Control Systems of the Georgian Technical University Proceedings, **16** (2012), 244-248

[4] R. Megrelishvili, *Analysis of the matrix one-way function and two variants of its implementation*, International J. of Multidisciplinary Research And Advances In Engineering (IJMRAE), **5**, 4 (2013), 99-105
[5] R. Megrelishvili, S. Shengelia, *On the original one-way matrix function and the implementation of the key exchange protocol on open channel*, Appl. Math. Inform. Mech., **17**, 2 (2012), 20-25
[6] R. Megrelishvili, *Analysis of the matrix one-way function and two variants of its implementation*, Computer Sciences and Telecommunication Reviewed Electronic Scientific Journal, **43**, 3 (2014), 37-41
[7] R. Megrelishvili, S. Shengelia, *Matrix function and its realization problems*, IV International Conference of the Georgian Mathematical Union, Batumi, September 9-15, 2013, 138-139
[8] R. Megrelishvili, S. Shengelia, *Open Channel Key Exchange Algorithm and Fractal Structures Research*, 2015 Tbilisi International Conference on Computer Science and Applied Mathematics, March 21-23, 2015, 93-97
[9] A.Y. Belesky, D.A. Stetsenko, *The order of the abelian cyclic group generated by the generalized transformations of Gray*, Electronics and control systems, **23**, 1 (2010), 5-11