Transactions of A. Razmadze
Mathematical Institute
Vol. **175** (2021), issue 2, 253–258

FRACTAL STRUCTURES FROM THE BAND MATRICES FOR MATRIX ALGORITHMS

RICHARD MEGRELISHVILI[1] AND SOFIA SHENGELIA[2]

Abstract. The aim of the present paper is to construct a set of high order strong matrices for a key-exchange matrix algorithm on an open channel and to create a high-speed one-way matrix function. Fractal structures are synthesized from band matrices. Square matrices are considered over a Galois field of GF (2). Each initial n-th order square matrix is primitive (the degree value is equal to $2^n - 1$) or its degree value is a Mersenne number $2^j - 1$, when $j < n$ (except $n = 18$).

1. Introduction

In cryptographic algorithms, the main task is the question of reliability of the algorithm. In matrix algorithms, the process of encryption and decryption is implemented by matrices, and for the algorithm to be reliable it is necessary to create powerful high-order matrix sets.

Each cryptographic system uses its own procedure, types of keys, methods of their distribution and coding algorithms. The essence of the asymmetric cryptography consists in a specific character of a one-way function. The one-way function is a $y = f(x)$ function; its value can be obtain by computer calculations in case x is known, but it is impossible to get the value of x argument by means of the function $f(x)$ and computer calculations at a real time. This fact is clearly illustrated by an example of the Diffie–Hellman [2] one-way function $a^x = y(\bmod p)$.

2. The Matrix Function

To implement a one-way matrix function, we have the $n \times n$ matrix A. For 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 $\hat{A}$; thus, $A \in \hat{A}$, $v \in V_n$, where V_n is a vector space over GF (2) (v is an open parameter). Then the one-way matrix function looks as

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

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

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

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

is based on the problem of a discrete logarithm, then the problem for that function appears to be the recursion inside the matrix [4, 7]. In a cryptographic algorithm, the use is made of a one-way function for solving the authentication and verification tasks for a certain period of time. We also use this function for solving the problem of stability of our matrix one-way function for a certain period of time. Towards this end, using the exponential one-way function, the key exchange takes place through the open channel. The result of this key exchange is the secret parameter $k = v$. At the same time period, the key exchange or other operations are performed with our algorithm. In this case, parameters v and A in (2.1) are secret and only parameter u is open [3].

In authors' opinion, after reading the next section there should be no doubt both about the high-speed of the matrix one-way function and about that of the key exchange algorithm on an open channel.

2020 *Mathematics Subject Classification.* 15B99.
Key words and phrases. Fractal Structures; Band Matrices; Matrix Algorithms.

The function (2.1) fundamentally differs from the function (2.2) by the fact that for the function (2.1) is used the operation of multiplication, whereas the function (2.2) is exponential.

3. The Matrix Algorithm

The Matrix Algorithm about Key-Exchange on an Open Channel is Implemented in the Following Way:

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

$$u_1 = vA_1;$$

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

$$u_2 = vA_2,$$

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

- Mariami computes

$$k_1 = u_2 A_1;$$

- George computes

$$k_2 = u_1 A_2,$$

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 have been first obtained and studied by the first author.

As is shown above, for the implementation of the key-exchange algorithm we need high power multiple $n \times n$ matrices which are, at the same time, commutative. A number commutation in Diffie–Hellman's algorithm is implemented naturally, in accordance with the construction of the commutative multiplicity of $\hat{A}$ for each value of dimension n, while for our algorithm this task is difficult.

In the given work, we present an effective and constructive solution. The characteristics of effective and constructive methods for construction of matrices are included in the following statements:

- For each $n > 1$ dimension, the initial $n \times n$ matrix should generate either a maximum number of matrices $(2^n - 1)$, or this number should be the number of Mersenne, meaning $2^j - 1$, where $j < n$.
- The method of synthesis of any $n \times n$ matrix of 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 to any given dimension of n.

For simplicity, the n-th order square matrices and other structures are considered in the Galois GF(2) field. Obviously, of great importance is generation of a high power matrix set for the functioning of a new key exchange function. The synthesis of such matrix sets and their structural study attract particular attention [5,6].

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. The study, analysis and software implementation of such issues is also the main goal.

4. Software Implementation

The object of our study is a matrix, finding such a structure, whose existence makes the matrix able to generate a multiplication cyclic group of matrices with a maximum value or a value equal to the Mersenne prime degree.

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

Several types of nondegenerate initial matrixes are experimentally tested. As a result, a general structure is obtained, the matrices generating multiplication groups, sometimes with maximum degree value and sometimes with a degree value equal to Mersenne prime are alo abtained. Only in a single case, (except for $n = 18$) [8–10], the matrix degree value is not a Mersenne prime and it is a subject to an individual structural study. The paper also deals with 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 depending on a real scale of time), the one-way matrix function stability also depends on the high value of the A set.

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

Matrix of the first Fractal structure:

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

Matrix of the second Fractal structure:

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

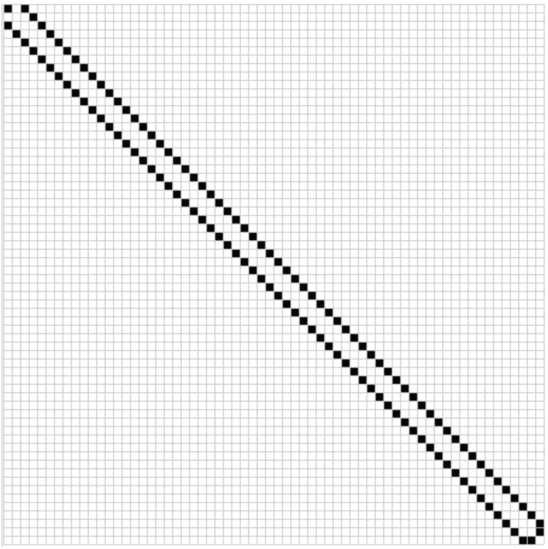


Figure 1. The fractal structure from the band matrix.

Matrix of the third Fractal structure:

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

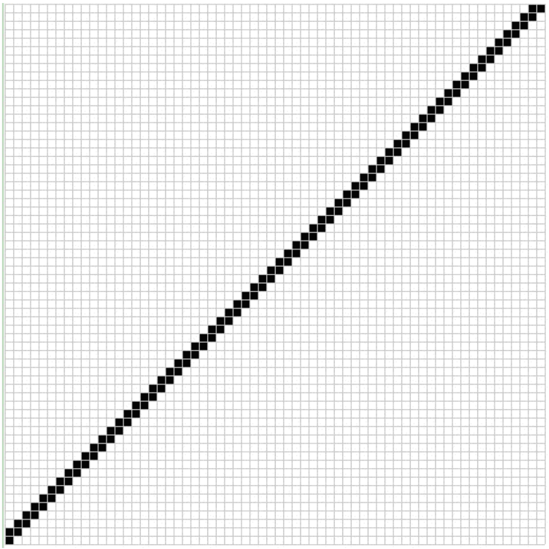


Figure 2. The fractal structure from the band matrix.

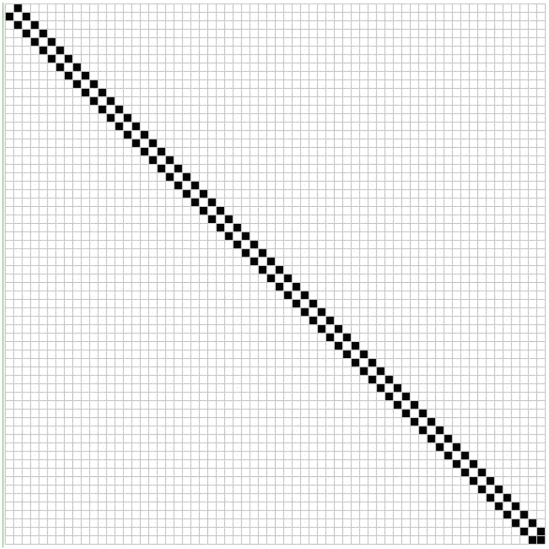


Figure 3. The fractal structure from the band matrix.

By using software, the 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).

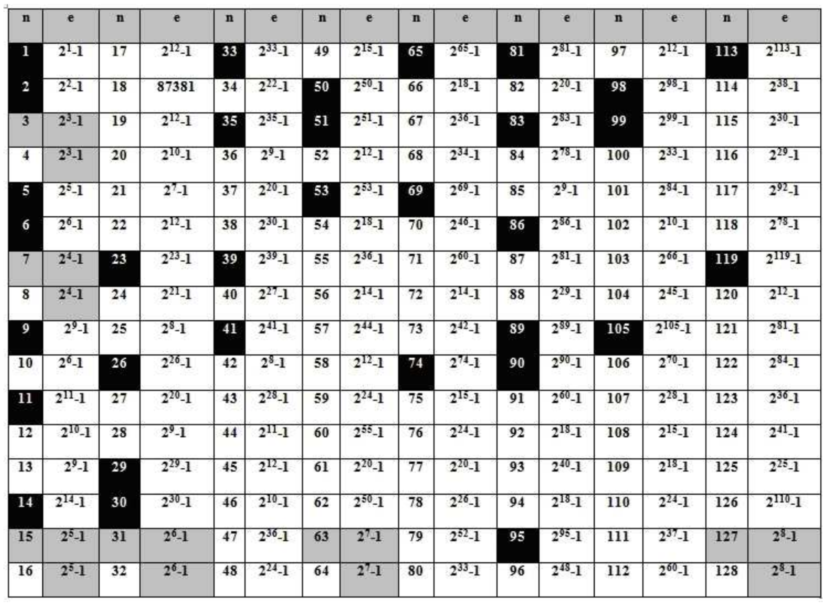
1. Each initial n order square matrix is primitive (the degree value is equal to $2^n - 1$) or its degree value is a Mersenne prime $2^j - 1$, when $j < n$ (except for $n = 18$).

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:

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

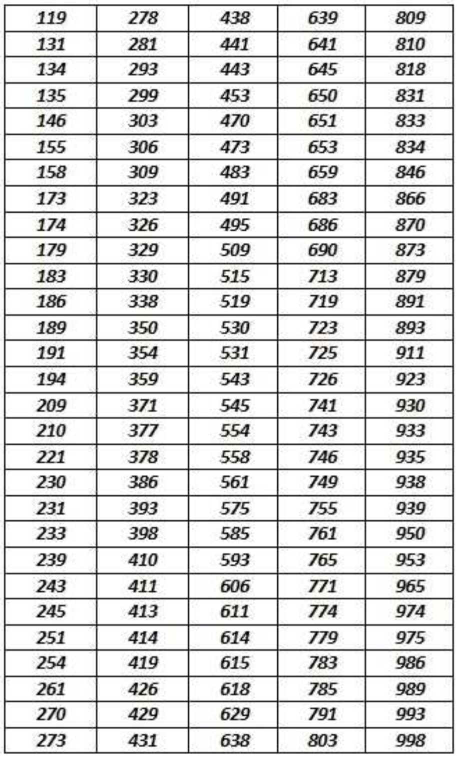
3. It is also noteworthy that nowadays in cryptographic algorithms the 2^{89} probable selection variants are very difficult even for the latest computers. We have calculated all matrices including the 1000×1000 size matrices. Each initial n order square matrix is primitive and its degree value is equal to $2^n - 1$ (Table 2).

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



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 2. Higher order matrices.



119	278	438	639	809
131	281	441	641	810
134	293	443	645	818
135	299	453	650	831
146	303	470	651	833
155	306	473	653	834
158	309	483	659	846
173	323	491	683	866
174	326	495	686	870
179	329	509	690	873
183	330	515	713	879
186	338	519	719	891
189	350	530	723	893
191	354	531	725	911
194	359	543	726	923
209	371	545	741	930
210	377	554	743	933
221	378	558	746	935
230	386	561	749	938
231	393	575	755	939
233	398	585	761	950
239	410	593	765	953
243	411	606	771	965
245	413	611	774	974
251	414	614	779	975
254	419	615	783	986
261	426	618	785	989
270	429	629	791	993
273	431	638	803	998

4. It is noteworthy that these results completely coincide with the results of Ukrainian scientist, Professor Anatoly Beletsky. Although, as is well known, the initial matrices have completely different structures, [1] i.e., the structures that are derived from the generalized Gray Codes.

During the last decades overwhelming necessity has arisen for modern scientific-theoretical and technological studies in security (reliability) and high-speed performance and their practical use in asymmetric cryptography systems. The paper considers a new trend in asymmetric cryptography, namely, a single-sided matrix function and the issues of generation of matrix sets, necessary for its fulfilment, and also the problems of new fractal matrix structure synthesis. The above circumstances provide actuality of the issue and its immense theoretical and practical value.

Acknowledgement

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

References

1. A. Belesky, D. Stetsenko, The order of the abelian cyclic group generated by the generalized transformations of Gray. *Electronics and control systems* **23** (2010), no. 1, 5–11.
2. W. Diffie, M. E. Hellman, New directions in cryptography. *IEEE Trans. Inform. Theory* **IT-22** (1976), no. 6, 644–654.
3. R. Megrelishvili, Analysis of the Matrix one-Way Function and Two Variants of Its Implementation. *International Journal of Multidisciplinary Research and Advances in Engineering (IJMRAE)* **5** (2013), no. 4, 99–105.
4. R. Megrelishvili, Tropical Cryptography and Analysis of Implementation of New Matrix One-Way Function. (Russia) Im: *Proceedings of the 2014 International Conference on Mathematical Models and Methods in Appled Sciences (MMAS '14). Saint Peterburg*, pp. 273–275, 2014.
5. R. Megrelishvili, Analysis of the Matrix One-Way Function and Two Variants of Its Implementation. *Computer Sciences and Telecommunication Reviewed Electronic Scientific Journal* **43** (2014), no. 3, 37–41.
6. R. Megrelishvili, Two New Versions of Numbers Fast Multiplication and Tropical Cryptography. *The Communications on Applied Electronics (CAE)* Foundation of Computer Science FCS, New York, USA, **7** (2017), no. 8, 12–15.
7. 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, 91.
8. 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** (2012), no. 2, 20–25, 56–57.
9. R. Megrelishvili, S. Shengelia, Matrix function and its realization problems. In: *IV International Conference of the Georgian Mathematical Union, Batumi*, pp. 138–139, 2013.
10. R. Megrelishvili, S. Shengelia, Open Channel Key Exchange Algorithm and Fractal Structures Research. In: *Tbilisi International Conference on Computer Science and Applied Mathematics*, pp. 93–97, 2015.

(Received 27.05.2019)

[1]I. Javakhishvili Tbilisi State University, 13 University Str., Tbilisi 0186, Georgia

[2]Sokhumi State University, 61 Politkovkaia Str., Tbilisi 0186, Georgia
E-mail address: richard.megrelishvili@tsu.ge
E-mail address: sofia_shengelia@mail.ru