Proceedings of I. Vekua Institute
of Applied Mathematics
Vol. 63, 2013

THE FRACTAL STRUCTURES AND THEIR PROPERTIES

Megrelishvili R., Shengelia S.

Abstract. A fractal is a mathematical object, a geometric pattern that is repeated at ever smaller scales to produce (self similar) irregular shapes and surfaces that cannot be represented by classical (Euclidian) geometry. Fractals are used especially in computer modeling of irregular patterns and structures found in nature. The Sierpinski triangle is the classic example of an orbital fractal. Mandelbrot and Sierpinski are two mathematicians who made important contributions in the field of fractals. The Sierpinski triangle has all the properties of a fractal: A fractal is a geometric shape which is selfsimilar and which has a fractal dimension.

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

AMS subject classification (2000): 15A15

1. Introduction

A fractal is a mathematical object, a geometric pattern that is repeated (iterated) at ever smaller (or larger) scales to produce (self similar) irregular shapes and surfaces that cannot be represented by classical (Euclidian) geometry. Fractals are used especially in computer modeling of irregular patterns and structures found in nature. The first fractals were described at the end of the XIXth Century and Cantor Set and Cantor Dust are probably the first fractals described by teh German mathematician Georg Cantor (1845-1918) in 1883. Waclaw Sierpinski (1882-1969) was a Polish mathematician. His work predated Mandelbrot's discovery of fractals. He is best known for the 'Sierpinski triangle', but there are many other Sierpinski-style fractals. The Sierpinski Triangle is the classic example of an Orbital fractal.

2. Construction of cyclic multiplicative groups of initial $n \times n$ 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 Mersenne, 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 [3-4].

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):

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

From (1) we conclude: The structure indicated by the formula (1), is nothing, but the Sierpinski triangle, with all the characteristics of a fractal structure.

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

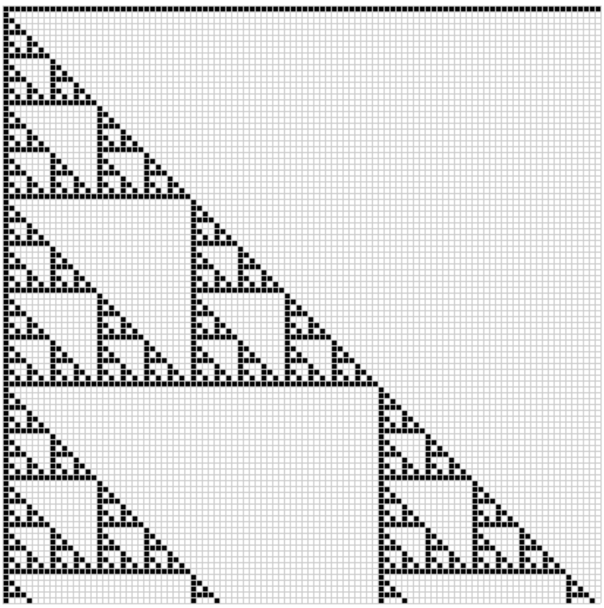

Fig. 1. fractal structure

Definition 2. Mersenne $n \times n$ 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. (Where n = 3, 7, 15, 31, 63, 127, 255, 511). Mersenne $n \times n$ matrix structures have the property of self-similarity (Fig. 2, 3, 4).

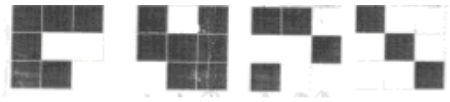

Fig. 2. 3×3 Matrix

Fig. 3. 7×7 Matrix

Fig. 4. 15×15 Matrix

Mersenne $n \times n$ matrix structures were calculated for the initial order e with software and the results obtained are shown in Table 1.

n	e	n	e	n	e	n	e
3	2^3-1	15	2^4-1	63	2^7-1	255	2^{10}-1
7	2^4-1	31	2^4-1	127	2^8-1	511	2^{11}-1

Tab. 1

$$(e_{2^r-1} = 2^{r+1} - 1, \ \ where \ \ r \geq 2).$$

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

REFERENCES

1. Megrelishvili R., Chelidze M., Chelidze K. On the construction of secret and public-key cryptosystems, Iv. Javakhishvili Tbilisi State University I.Vekua Institute of Applied Mathematics. *Applied Mathematics, Informatics and Mechanics, AMIM*, **11**, 2 (2006), 29-36.

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

3. Megrelishvili R., Sikharulidze A. New matrix-set generation and the cryptosystems. *Proceedings of the European Computing conference and 3rd International Conference on Computational Intelligence, Tbilisi, Georgia*, June **26-28** (2009), 253-256.

4. Megrelishvili R., Besiashivli G., Shengelia S. 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), 407.

5. Belitski A, Stetsenko D. Order of Abelian Cycle Groups, generated by the generalized transformation of Gray, Electronics and signal management systems, **1**, 23 (2010), 5-11.

Received 31.07.2013; revised 07.10.2013; accepted 02.12.2013.

Authors' addresses:

R. Megrelishvili
Iv. Javakhishvili Tbilisi State University
2, University St., Tbilisi 0186
Georgia

Sokhumi State University
9, Anna Politkovskaia St., Tbilisi 0186
Georgia
E-mail: sofia_shengelia@mail.ru