# Tropical Cryptography and Analyses of New Matrix One-Way Function with two Versions of Protection

R. P. Megrelishvili

***Abstract* —** This article is an expanded version of Article that was published in one of the EUROPMENT Conference (in particular to St Petersburg in 2014). In this article the new results there are: Tropical Cryptography and matrix one-way function, which is the basis building a high-speed algorithm of key exchange, a prototype of which, in a sense, is the Diffie-Hellman algorithm and also are two versions of protection of this matrix one-way function. We can estimate the importance of Tropical cryptography as a new trend in cryptography, a fortiori if it will be stable with respect to the same researched algebraic methods of attack. With respect to the issue of importance of matrix one-way function, we repeat, that the main advantage of the matrix one-way function is high speed operation. Tropical cryptography opens a new direction in cryptography. It should be noted also that the stability of the matrix one-way function justified by long-standing tradition of proven algorithms of Diffie-Hellman and ElGamal. In the extended version of the paper are added the fourth and fifth sections: Matrices with an inside recursion dependence and Generation of special classes of $n \times n$ matrices.

***Keywords* —** *Cryptography, matrix one-way function, key exchange algorithm, Tropical Operations, Tropical Cryptography.*

## I. Introduction

The analysis showed that the matrix one-way 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 one-way function is as follows:

$$v A' = u. \quad (1)$$

Where A' Є Ă, a Ă is a set of high power from an n-dimensional quadratic commutative matrices [1]. Along with this, v, u Є $V_n$. Where $V_n$ 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). Therefore, if the expression (1) is considered as a one-way function, then it can break down in the following ways:

1. If the matrix set Ă contains recursion (that was identified by us), then the expression (1) can easily be broken with the help Companion matrices, that is, the set of $n^2$ unknown can be lead to a matrix with n unknowns, for any square matrix A' Є Ă can be bring to n unknown, i.e., using the equation (1) can obtain a system of n equations in n unknowns, etc. These issues have been discussed in [2-5, 6].
2. If the matrix of set of Ă does not contain recursion (or hard to find), then the matrix one-way function can be broken with the use of the basic matrixes of $A^0$, $A^1$, $A^2$,..., $A^{n-1}$ which is not hard to get, if we know the initial matrix A.

If the methods will are justified, what tropical cryptography and method of matrix one-way function, whose prototype is the ElGamal algorithm, the authors preoccupied with security and the protection of web-based systems [10-12] considerably greatly will are interested of methods discussed in the article..

## II. On the possibility of breaking the matrix one-way function

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 [2-5,6]). 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):

$$A=\begin{pmatrix}1&0&1\\1&0&0\\0&1&1\end{pmatrix},\quad A^2=\begin{pmatrix}1&1&0\\1&0&1\\1&1&1\end{pmatrix},\quad A^3=\begin{pmatrix}0&0&1\\1&1&0\\0&1&0\end{pmatrix},\ldots,A^7=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}. \quad (2)$$

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:

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

Bob computes and sends to Alice the following vector:

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

Elice computes the exchanged key:

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

Bob computes the exchanged key:

$$k_2 = u_1A_2 = (100). \quad (6)$$

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 = { $c_0 A^{2^0}, c_1 A^{2^1} \dots c_{n-1} A^{2^{n-1}}$} (where $\{c_0, c_1, \dots, c_{n-1}\} \in$ GF(2)). For a set of (2) we form an appropriate basis:

$$A^0 = I,\ A^1, A^2, \quad (7)$$

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:

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

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

$$u_1 = v\,A_1(x) = c_0\,vA^0 + c_1vA^1 + c_2vA^2 = c_0w_0 + c1w_1 + c_2w_2. \quad (9)$$

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

$$\begin{gathered} vA^0 = (110)\,A^0 = (110) = w_0, \\ vA^1 = (110)A^1 = (001) = w_1 \\ vA^2 = (110)\,A^2 = (011) = w_2, \\ u_1 = (011). \end{gathered} \quad (10)$$

Using (9) and (10) we may form a system of equations for the coefficients $c_0$, $c_1$, $c_2$:

$$\begin{gathered} 1c_0 + 0c_1 + 0c_2 = 0, \\ 1c_0+0c_1+1c_2=1, \\ 0c_0 + 1c_1 + 1c_2 = 1. \end{gathered} \quad (11)$$

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).

## III. Two Embodiment of the One-Way Function Matrix

As stated above, this paper first 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 [7]:

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

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):

$$\begin{gathered} 1^* c_0 + 0 * c_1 + 0 * c_2 = 0, \\ 1*c_0+0*c_1+1*c_2=1, \\ 0^* c_0+ 1^* c_1 + 1^* c_2 = 1. \end{gathered} \quad (14)$$

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):

$$A=\begin{pmatrix}1&0&1\\1&0&0\\0&1&0\end{pmatrix},\ A^2=\begin{pmatrix}1&0&0\\0&0&1\\0&0&0\end{pmatrix},\ A^3=\begin{pmatrix}0&0&1\\1&1&0\\0&1&1\end{pmatrix},$$

$$\ldots,\ A^7=A^0=\begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix} \quad (15)$$

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 (see. below). 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 [8]. The similarity with our second option is a period of time for which use the function [9]. 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 a 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 parameter u 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.

## IV. Matrices with an Inside Recursion Dependence

We want to draw attention to the fact that some non-degenerate matrices (matrices with nonzero determinants) contain inside-matrix recursion dependence. This dependence exists among matrix rows or columns. However it is not a usual linear dependence. That is why such matrices remain non-degenerate.

Matrices of this kind can be easily broken when they are used for cryptographic purposes. It is possible to construct special classes with inside-matrix recursion dependence, but in a number of cases (especially for matrices of large size) the revealing of inside-matrix recursion dependence is not a simple task.

matrices with inside-matrix recursion dependence can be constructed with the aid of the galois field $GF(p^n)$. for the sake of simplicity, this construction will be considered here as a field of polynomials $GF(2^n)$ modulo an irreducible polynomial $p(x)$ over $GF(2)$. for example, a multiplicative group of the field $GF(2^3)$ generated by means of $\alpha$, which is the root of a primitive polynomial $p(x)=1+x+x^3$, has the form [2,3]:

$$\begin{aligned}
&\alpha^0=1 && -(100)\\
&\alpha^1=\alpha && -(010)\\
&\alpha^2=\alpha^2 && -(001)\\
&\alpha^3=1+\alpha && -(110)\\
&\alpha^4=\alpha+\alpha^2 && -(011)\\
&\alpha^5=1+\alpha+\alpha^2 && -(111)\\
&\alpha^6=1+\alpha^2 && _\ (101)\\
&\text{----------} &&\\
&\alpha^7=1 &&
\end{aligned} \quad (16)$$

The multiplicative group (16) is written in terms of powers of $\alpha$, the corresponding entries are written in terms of polynomials of $\alpha$ with their corresponding vectors which together with a zero vector form the vector space $V_{n=3}$ over the field $GF(2)$. By virtue of (16), we can write, for example, a multiplicative group of matrices $A$, $A^2$, $A^7=I$ $A^3,\ldots,$ ($I$ is the unit matrix) as follows:

$$A=\begin{pmatrix}0&1&0\\0&0&1\\1&1&0\end{pmatrix},\ A^2=\begin{pmatrix}0&0&1\\1&1&0\\0&1&1\end{pmatrix},\ A^3=\begin{pmatrix}1&1&0\\0&1&1\\1&1&1\end{pmatrix},\ldots,A^7=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \quad (17)$$

This group is generated by the primitive matrix $A$ which corresponds to an element $\alpha$ (it is assumed that (1) and (2) are isomorphic). It is obvious that the order of each matrix $A^i$ coincides with the order of an element $\alpha^i$.

All matrices $A^i(2)$ have an inside-matrix recursion dependence predetermined by the polynomial $p(x)$. We will illustrate this dependence using $p(x)=1+x+x^3$ as an example. Any matrix from (2) consists of $n^2=9$ unknowns:

$$A^i=\begin{pmatrix}x_{11}&x_{12}&x_{13}\\x_{21}&x_{22}&x_{23}\\x_{31}&x_{32}&x_{33}\end{pmatrix} \quad (18)$$

However, if we take into account inside-matrix recursion dependence, then we can easily obtain from (18) a matrix $A_1^i$ with the number of unknowns equal to $n=3$:

$$A_1^i = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{13} & x_{11}+x_{13} & x_{12} \\ x_{12} & x_{13}+x_{12} & x_{11}+x_{13} \end{pmatrix} \qquad (19)$$

This matrix can be easily broken even in the case of a single cryptographic application, for example, when it is used to fulfil the operation of multiplication of a vector by a matrix (we mean, say, the realization of the Diffie-Hellman protocol on matrices).

It is obvious that the number of matrices with an inside-matrix recursion dependence corresponds to the number of irreducible polynomials used for the construction of $GF(2^n)$, but may be greater. In our opinion, this question is essential and therefore we consider it in the next example.

As an example we give a construction, different from (2), of a multiplicative group of matrices with a period $e=3$:

$$A=\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix},\quad A^2=\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},\quad A^3=I=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (20)$$

In the matrices $A$, $A^2$ and $A^3$ (20) the observed recursion dependence has a different form. It is connected with a certain sequence of elements from (16). For example, the rows in the matrix $A$ (20) are the vectors corresponding to the elements $\alpha^3$, $\alpha^5$, $\alpha^7=\alpha^0$ (16), while in the matrix $A^2$ (20) they are the vectors corresponding to the elements $\alpha^2$, $\alpha^6$, $\alpha^{10}=\alpha^3$ (16), and the rows in the matrix $A^3$ (20) are the vectors corresponding to the elements $\alpha^0$, $\alpha^1$, $\alpha^2$ (16).

It should be said that it is not evidently a simple matter to reveal and count such modified dependences having a regular character. However, if the considered dependence $l=f(k)$ is linear, as in the example (20) (where $l$ is the exponent of the power of a field element $\alpha^l$ (16), and $k$ is the matrix row number, $k=1,2,...,n$, then the revealing of such a dependence may turn out to be a relatively simple task. The dependence $l=f(k)$ shown in Fig. 1 for matrices of the group (20) is linear. It is obvious that the dependence $l=f(k)$ for all the above-considered matrices with an inside-matrix recursion dependence is also linear. However, as different from the matrices (20) (see Fig. 1), the linearity of all matrices of the form (17) is one and the same (i.e. $\beta$ is a constant value) and can be easily determined. Therefore inside-matrix recursion dependence in them is trivial.

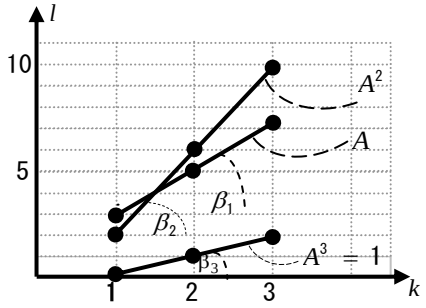


**Fig. 1 The linear dependence $l = f(k)$ for the multiplicative group (20)**

In reality, not all matrix sets (groups) will have the linear dependence $l=f(k)$. For example, matrices of the multiplicative group (21), with period $e=7$, do not contain the recursion dependences considered above:

$$A=\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix},\quad A^2=\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},\quad A^3=\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix},...,A^7=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad (21)$$

Summarizing and generalizing the above results, we distinguish three cases (three kinds of matrix sets):

- For a set of $n\times n$ matrices of the form (17)-(19) we have a trivial inside-matrix recursion dependence;
- For a set of $n\times n$ matrices of the form (20), we have linear inside-matrix recursion dependence $l=f(k)$.
- For a set of $n\times n$ matrices, of the form (21), the inside-matrix recursion dependence is not observed.

## V. The Generation of Special Classes of $n\times n$ Matrices

Our aim is to construct a multiplicative group of matrices that will be free of an inside-matrix recursion dependence. Besides, each initial $n\times n$ matrix must be primitive, i.e. have a maximal order equal to $e=2^n-1$ and generate a multiplicative group with a maximal period. The considered matrix groups are commutative. Formulas (7) show the initial matrices, which, in the authors' opinion, satisfy the conditions discussed above. The construction of initial matrix structures is based (for example) on the symmetry of elements and at the same time the asymmetry with respect to the diagonals is also taken into account.

The initial $5\times 5$ matrix $A_{n=5}$ is constructed on the basis of the matrix $A_{n=3}$. Next initial matrix $A_{n=7}$ is constructed on the basis of the matrix $A_{n=5}$, i.e. to obtain the matrix $A_{n=7}$, the matrix $A_{n=5}$ is also encircled by a sequence of 1's and 0's according to a certain rule. This rule also remains in force when constructing the initial matrix $A_{n=9}$ on the basis of the matrix $A_{n=7}$ and so on until we obtain an $n\times n$ matrix

maximum extent where $n=2k-1,\ k>1$ is an integer number.

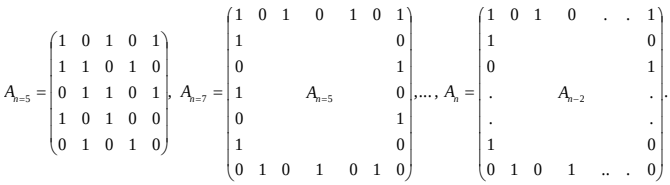

**Fig. 2 The method of construction of special classes of $n\times n$ matrixes.**

Each initial $n\times n$ matrix $A\in \mathsf{A}$ generates a multiplicative group which may have a maximum order e, then $A,A^2,A^3,...,A^{2^n-1}=I$, and which in the case of a sufficiently large value of $n$ ($n\approx 150$) generates a set of commutative matrices $\mathsf{A}$ (of high power) to be used for cryptographic purposes.

## REFERENCES


[1] R.Megrelishvili, M.Chelidsze, K.Chelidze, "On the construction of secret and public key cryptosystems," Iv.Javakhishvili Tbilisi State University, I.Vekua Institute of Applied Mathematics, Informatics and Mechanics (AMIM), v. 11, No 2, 2006, pp. 29-36.

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

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

[4] 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.

[5] R.Megrelishili, M.Jinjikhadze, Matrix one-way function for the exchange of cryptographic keys and method for the generation of multiplicative matrix groups ", in Proceedings of The International Conference SAIT 2011, May 23-28, Kyiv, Ukraine, in 2011. p. 472.

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

[7] 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.

[8] 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.

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

[10] Rodrigo Cesar Ferrarezi, Reinaldo Squillante Junior, Jeferson A.L. Souza, … Formal Verification of Safety Control System based on GHENESYS NET 51, Proceedings of The 18th International Conference on Circuits, Systems, Communications and Computers (CSCC 2014), Sentorini Island, Greece, July 17-21, 2014, The CIRCUITS Volume, ADVANSES in ROBOTICS, MECHATRONICS and CIRCUITS, pp. 133-139. Also in the Independent Books: Mathematics and Computers in Sciences and Industry; Copyright, 2014, by the editors, pp. 51-57.

[11] Ján Ivanka, Petr Navrátil, Optosensors Systems in Spherical Safety Protection Security Systems, Proceedings of The 2014 International Conference on Applied Mathematics, Computational Science and Engineering (AMCSE 2014), Varna, Bulgaria, September 13-15, 2014, The Volume, APPLIED MATHEMATICS, COMPUTATIONAL SCIENCE and ENGINEERING, 2014, pp. 56-61.

[12] L.Pálka, F.Schauer, R.Jašek, Safety of Database Storage for Remote Laboratories and Laboratory Management System, Proceedings of The 2014 International Conference on Applied Mathematics, Computational Science and Engineering (AMCSE 2014), Varna, Bulgaria, September 13-15, 2014, The Volume, APPLIED MATHEMATICS, COMPUTATIONAL SCIENCE and ENGINEERING, 2014, pp. 119-133.



**Richard P. Megrelishvili**

Doctor of Technical Sciences (DScTech),
Professor,
Ph.: (+995-595) 55-91-59,
I.Javakhishvili Tbilisi State University,
University St. 2, Tbilisi 0143, Georgia
E-mail: r_megreliishvili@yahoo.com ; richard.megrelishvili@tsu.ge

B. Day: 1 January 1934; Tbilisi, Georgia
Scientific field: Coding Theory, Cryptography, Artificial Intelligence;

Education: Faculty of Energetics, Georgian Technical University, 1957; Aspirant, Institute of Automation and Telemechanics, Academy of Sciences, USSR, 1960-63;
Candidate of Technical Sciences, 1966; Doctor of Technical Sciences, 1997.
Appointments:
Scientific Collaborator, Institute of Electronics, Automation and Telemechanics, Academy of Sciences, Georgian SSR, 1957-66;
Chief, Department of Physical Cybernetics Problems, Laboratory of Javakhishvili, Tbilisi State University, 1967-2006;
Professor, Ivane Javakhishvili Tbilisi State University, 2000.