Post-quantum Key Exchange Protocol Using High Dimensional Matrix

Richard Megrelishvili
I. J. Tbilisi State University
Tbilisi, Georgia
richard.megrelishvili@tsu.ge

Melkisadeg Jinjikhadze
Akaki Tsereteli State University
Kutaisi, Georgia
mjinji@yahoo.com

Maksim Iavich
Caucasus University
Tbilisi, Georgia
m.iavich@scsa.ge

Avtandil Gagnidze
Georia University
Tbilisi, Georgia
gagnidzeavto@yahoo.com

Giorgi Iashvili
Georia University
Tbilisi, Georgia
g.iashvili@scsa.ge

***Abstract*— Active work is being done to create and develop quantum computers. Google Corporation, NASA and the Universities Space Research Association (USRA) have teamed up with DWAFE, the manufacturer of quantum processors. D-Wave 2X is a quantum processor that contains 2,048 physical qubits. 1152 qubits from the whole number of qubits are used to perform the calculations. As we see, quantum computers can easily solve the problem of calculating the discrete logarithm used in Diffie-Hellman algorithm. So it can break Diffie-Hellman algorithm.**

When quantum computers are released all existing crypto systems will be useless, because there will be no way to transfer the key securely.

In the article is proposed the new key exchange method using high dimensional matrix, this method is safe against attacks implemented using quantum computers. The case concerns the matrix function and algorithm for cryptographic keys exchange with open channel. For the algorithm is offered the method of building a high dimensional matrix multiplicative group.

The arising of this goal is that traditional key exchange methods are vulnerable to quantum computer attacks.

Keywords*— *post-quantum cryptography, attacks, a matrix one-way function, Abelian multiplicative group, asymmetric cryptography, high dimensional matrix finite field

I. Introduction

One of the fundamental problems of cryptography is the safe communication over the listening channel. Messages need to be encrypted and decrypted, but for this, both parties need to have a common key. If this key is transmitted via the same channel, then the listening side will also receive it, and the meaning of the encryption will disappear.

Diffie-Hellman algorithm allows the two parties to obtain a common secret key using an unprotected, but spoofed, communication channel. The received key can be used to exchange messages using symmetric encryption.

The security of forming a common key in the Diffie-Hellman algorithm follows from the fact that, although it is relatively easy to calculate exponents modulo a prime number, it is very difficult to calculate discrete logarithms. For large prime numbers of hundreds and thousands of bits, the task is considered unsolvable, since it requires a tremendous amount of computational resources. But this problem can easily be solved by quantum computers using Shor algorithm [1,2].

The security of RSA algorithm relies on factorization problem, but this problem can be easily solved using quantum computers [3].

Active work is being done to create and develop quantum computers. Google Corporation, NASA and the Universities Space Research Association (USRA) have teamed up with DWAFE, the manufacturer of quantum processors. D-Wave 2X is a quantum processor that contains 2,048 physical qubits. 1152 qubits from the whole number of qubits are used to perform the calculations. As we see, quantum computers can easily solve the problem of calculating the discrete logarithm used in Diffie-Hellman algorithm. So it can break Diffie-Hellman algorithm.

When quantum computers are released all existing crypto systems will be useless, because there will be no way to transfer the key securely [4,5].

In the article is proposed the new key exchange algorithm using high dimensional matrix. This algorithm is safe against quantum computer attacks.

The case concerns the matrix function and algorithm for cryptographic keys exchange with open channel.

For this is offered the method building a high dimensional matrix multiplicative group.

The arising of this goal is that traditional key exchange methods are vulnerable to quantum computer attacks.

One-way function (OWF) is a function whose value is easy to calculate for any argument, but it is “difficult” to find an argument for the given value of the function. The word "difficult" is to understand the complexity of the computation. In other words, finding the relevant argument of the given function in real time is difficult even with the modern computing techniques. The irreversibility of function does not mean that the function is one-way [6,7].

The existence of one-way functions is the basis for the idea of asymmetric cryptography. It (one-way function) is the foundation of asymmetric cryptography, personal identification, authentication, and other fields of information protection. Although there is no theoretical proof of the existence of one-way functions in general, there are several “possible pretendents” (eg, multiplication and factorization, squaring and module rooting, discreet exponent and logarithmization), whose one-wayity (ie the difficulty of finding the argument for the value of function) at this time real and is actively used in information exchange protocols.

As we have mentioned, one-way functions are actively used in the algorithms for developing a cryptographic open key. The initial idea (1976) belongs to Whitfield Duffie and Martin Helman. Based of their idea was established the first practical wel-known Diffie-Helman-Merkel method, which enabled the development of a common cryptographic key using the open (unprotected) channel. A year later, the first RSA algorithm of asymmetric encryption was formed. The RSA in fact, resolved the problem of exchange information with open channel. Both algorithms are not safe against quantum computers attacks. Are proposed quantum key exchange protocols, but quantum computers are needed to implement them [8,9].

II. ONE-WAY MATRIX FUNCTION

The new one-way function for the development of common cryptographic keys is based on high order cyclic matrix groups, with the power $e = 2^n - 1$, where the n is row dimension of the square matrix. Let's assume that "***A***" is the above matrix group, while A is the initial $n \times n$ matrix, then "***A***" = A={A, A^2, $A^3, \dots, A^{2^n-1} = I$} (1)
where I represents an identity matrix.

One-way function and algorithm for common key development are as follows:

- The sender chooses $A_1 \in A$ secret matrix to send to the receiving party via open channel the
$$\text{u}u_1 = vA_1 \tag{2}$$
vector where $v \in V_n$ vector is known (V_n – is a vector space on GF field);
- The receiving party shall, on the other hand, choose $A_2 \in A$ secret matrix and send to the sender
$$u_2 = vA_2 \tag{3}$$
vector;
- Sender calculates $k_1 = u_2A_1$ (4)
vector;
- Receivier calculates $k_2 = u_1A_2$ (5)
where $k_1$and k_2 – are secret keys;
- Obviously, $k_1 = k_2 = k$, because
$$k = vA_1A_2 = vA_2A_1 \tag{6}$$
because of the commutativeness of the "A" group. The
$vA_i = u$ (7)
is one-way fast function.

Let $v = (v_1, v_2, v_3, \cdots, v_n) \in V_n$ (8)
and
$u = (u_1, u_2, u_3, \cdots, u_n) \in V_n$ are non-secret vectors from the above algorithm and
$$A_1 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in A \tag{9}$$
is a secret matrix. Then, according to algorithm the following system is formed:
$$vA_1 = \begin{pmatrix} v_1a_{11} + v_2a_{21} + \cdots + v_na_{n1} \\ v_1a_{12} + v_2a_{22} + \cdots + v_na_{n2} \\ \vdots \\ v_1a_{n1} + v_2a_{n2} + \cdots + v_3a_{n3} \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \tag{10}$$
The number of unknowns in the system of linear equations is the square of number of equations. Obviously, the system can not be solved in limited time, if the size of the matrix is large enough. Size of the matrix must be chosen considering Grover’s algorithm. Classically, searching requires a linear search, which is O(N) in time. Grover's algorithm needs O($\text{N}^{1/2}$) time, it is considered as fastest quantum algorithm for searching an unsorted information. This algorithm provides a quadratic speedup [10,11].

One fact must be taken into consideration if the A_1 matrix contains the internal recurrence, or if each of its rows are in a certain recurrence with the previous row, then the task of solving the system will be replaced by a simpler task that is easy to solve. It is so important that it puts itself in doubt the one-way character of our function and requires the existence of Abelian multiplicative matrix group with a high order, that is free from the recurrence of the inside.

III. FINITE MATRIX GROUPS CONSTRUCTION

Let's consider $(1 + \alpha)^j$, where j = 0,1,2, ⋯, and α represents the root of primitive polynomial in the $GF(2^n)$ field odule with the module p (x).

$(1 + \alpha)^0 = 1$	1
$(1 + \alpha)^1 = 1 + \alpha$	11
$(1 + \alpha)^2 = 1 + \alpha^2$	101
$(1 + \alpha)^3 = 1 + \alpha + \alpha^2 + \alpha^3$	1111
$(1 + \alpha)^4 = 1 + \alpha^4$	10001
$(1 + \alpha)^5 = 1 + \alpha + \alpha^4 + \alpha^5$	110011

The polynomial coefficients generated the structure known as Serpinsky Triangle. The derived structure contains a number of sub-structures that can be used as a generator (generating matrix) for multiplicative groups, ie primitive elements. Such is, for example,
$$P_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \text{ (9)}, \quad P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \text{ (11)}$$
And many more. Their natural powers create Abelian multiplicative cyclic group.

For example:
$$P_3^1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, P_3^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$
$$P_3^3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, P_3^4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$
$$P_3^5 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, P_3^6 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$
$$P_3^7 = P_3^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{12}$$
It’s easy to confirm that
$P_3^0, P_3^1, P_3^2, P_3^3, P_3^4, P_3^5, P_3^6$

is an Abelian multiplicative group.

Lets keep the structure of P_3 matrix and extend it by elements of set (2) as follows:

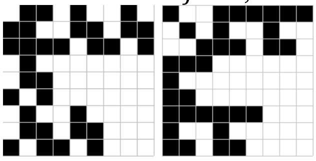
$$P_{3^2}(i,j) = \begin{pmatrix} P_3^i & P_3^j & P_3^j \\ P_3^j & 0 & 0 \\ P_3^j & P_3^j & 0 \end{pmatrix}, \text{ where } i,j=0..6. \quad (13)$$

Fore example, when $i = 5$ and $j = 6$, we have

$$P_{3^2}(5,6) = \begin{pmatrix} P_3^5 & P_3^6 & P_3^6 \\ P_3^6 & 0 & 0 \\ P_3^6 & P_3^6 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & 0 & 0 \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} & 0 \end{pmatrix} \quad ((14)$$

When $i = 0$ and $j = 1$, we have (pic. 1):



Pic.1: $P_{3^2}(5,6)$ *and* $P_{3^2}(0,1)$

$$P_{3^2}(0,1) = \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & 0 & 0 \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} & 0 \end{pmatrix} \quad (15)$$

Consider $P = [P_{3^2}(5,6)]^2 =$

$$= \begin{pmatrix} P_3^5 & P_3^6 & P_3^6 \\ P_3^6 & 0 & 0 \\ P_3^6 & P_3^6 & 0 \end{pmatrix} \times \begin{pmatrix} P_3^5 & P_3^6 & P_3^6 \\ P_3^6 & 0 & 0 \\ P_3^6 & P_3^6 & 0 \end{pmatrix} \quad (16)$$

If we take into consideration that the set $0, P_3^0, P_3^1, P_3^2, P_3^3, P_3^4, P_3^5, P_3^6$ is a field, it is easy to assure that each sub-matrix of the P matrix is in the the same set:

$P_{1,1} = P_3^5 \times P_3^5 + P_3^6 \times P_3^6 + P_3^6 \times P_3^6 = P_3^3,$

$P_{1,2} = P_3^5 \times P_3^6 + P_3^6 \times 0 + P_3^6 \times P_3^6 = P_3^2,$

$P_{1,3} = P_3^5 \times P_3^6 + P_3^6 \times 0 + P_3^6 \times 0 = P_3^4,$

$P_{2,1} = P_3^6 \times P_3^5 + 0 \times P_3^6 + 0 \times P_3^6 = P_3^4,$

$P_{2,2} = P_3^6 \times P_3^6 + 0 \times 0 + 0 \times P_3^6 = P_3^5,$

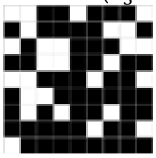
$P_{2,3} = P_3^6 \times P_3^6 + 0 \times 0 + 0 \times 0 = P_3^5,$

$P_{3,1} = P_3^6 \times P_3^5 + P_3^6 \times P_3^6 + 0 \times P_3^6 = P_3^2,$

$P_{3,2} = P_3^6 \times P_3^6 + P_3^6 \times 0 + 0 \times P_3^6 = P_3^5,$

$P_{3,3} = P_3^6 \times P_3^6 + P_3^6 \times 0 + 0 \times 0 = P_3^5.$

$$\text{or } P = \begin{pmatrix} P_3^3 & P_3^2 & P_3^4 \\ P_3^4 & P_3^5 & P_3^5 \\ P_3^2 & P_3^5 & P_3^5 \end{pmatrix} (15) \text{ (see pic. 2).}$$

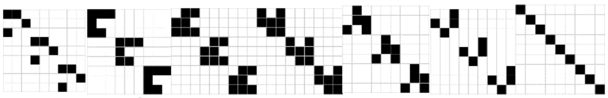


pic.2: $P = [P_{3^2}(5,6)]^2$

Using the software package we have developed it has been confirmed that the $\boldsymbol{P_{3^2}(5,6)}$ matrix is a primitive element. Its natural powers generate Abelian multiliplicative group, whose power is $\mathbf{2^{3^2-1}}$.

The elements of $[P_{3^2}(5,6)]^k$ when k = 73, 146, 219, 292, 365, 438, 511 are diagonal matrices (see pic. 3):

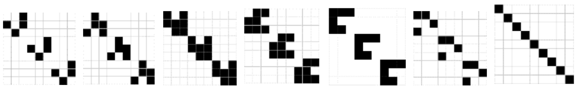
$$\begin{pmatrix} P_3^4 & 0 & 0 \\ 0 & P_3^4 & 0 \\ 0 & 0 & P_3^4 \end{pmatrix}, \begin{pmatrix} P_3^1 & 0 & 0 \\ 0 & P_3^1 & 0 \\ 0 & 0 & P_3^1 \end{pmatrix}, \begin{pmatrix} P_3^5 & 0 & 0 \\ 0 & P_3^5 & 0 \\ 0 & 0 & P_3^5 \end{pmatrix},$$
$$\begin{pmatrix} P_3^2 & 0 & 0 \\ 0 & P_3^2 & 0 \\ 0 & 0 & P_3^2 \end{pmatrix}, \begin{pmatrix} P_3^6 & 0 & 0 \\ 0 & P_3^6 & 0 \\ 0 & 0 & P_3^6 \end{pmatrix},$$
$$\begin{pmatrix} P_3^3 & 0 & 0 \\ 0 & P_3^3 & 0 \\ 0 & 0 & P_3^3 \end{pmatrix}, \begin{pmatrix} P_3^0 & 0 & 0 \\ 0 & P_3^0 & 0 \\ 0 & 0 & P_3^0 \end{pmatrix}$$



Pic.3 : $[P_{3^2}(5,6)]^k, k = 73, 146, 219, 292, 365, 438, 511$

Also $P_{3^2}(0,1)$ matrix is a primitive element, and elements of the set $[P_{3^2}(0,1)]^k$, when k=73, 146, 219, 292, 365, 438, 511, are diagonal matrices(pic 4):

$$\begin{pmatrix} P_3^3 & 0 & 0 \\ 0 & P_3^3 & 0 \\ 0 & 0 & P_3^3 \end{pmatrix}, \begin{pmatrix} P_3^6 & 0 & 0 \\ 0 & P_3^6 & 0 \\ 0 & 0 & P_3^6 \end{pmatrix}, \begin{pmatrix} P_3^2 & 0 & 0 \\ 0 & P_3^2 & 0 \\ 0 & 0 & P_3^2 \end{pmatrix},$$
$$\begin{pmatrix} P_3^5 & 0 & 0 \\ 0 & P_3^5 & 0 \\ 0 & 0 & P_3^5 \end{pmatrix}, \begin{pmatrix} P_3^1 & 0 & 0 \\ 0 & P_3^1 & 0 \\ 0 & 0 & P_3^1 \end{pmatrix},$$
$$\begin{pmatrix} P_3^4 & 0 & 0 \\ 0 & P_3^4 & 0 \\ 0 & 0 & P_3^4 \end{pmatrix}, \begin{pmatrix} P_3^0 & 0 & 0 \\ 0 & P_3^0 & 0 \\ 0 & 0 & P_3^0 \end{pmatrix}$$



pic.4: $[P_{3^2}(5,6)]^k,\ k = 73, 146, 219, 292, 365, 438, 511$

Set of non-zero elements of the diagonal matrices represents the perturbation of the group $P_3^0, P_3^1, P_3^2, P_3^3, P_3^4, P_3^5, P_3^6$ (called as primary group) and one of the elements is P_3^0.

Finally, we can conclude that empirically we proved the following fact:

The second order $(i, i+1)$ expansion $P_{3^2}(i, i+1)$, $i = 0..5$, of the matrix P_3 is a primitive element and creates the Abelian multiplicative finite group $F(P_{3^2}(i, i+1))$, with the power $2^{3^2} - 1$.

Below we can see other primitive elements that are results of expansion of P_3 matrix:

$$P_{3^2}(0,1) = \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix},$$

$$P_{3^2}(1,2) = \begin{pmatrix} P_3^1 & P_3^2 & P_3^2 \\ P_3^2 & 0 & 0 \\ P_3^2 & P_3^2 & 0 \end{pmatrix},$$

$$P_{3^2}(2,3) = \begin{pmatrix} P_3^2 & P_3^3 & P_3^3 \\ P_3^3 & 0 & 0 \\ P_3^3 & P_3^3 & 0 \end{pmatrix}$$

$$P_{3^2}(3,4) = \begin{pmatrix} P_3^3 & P_3^4 & P_3^4 \\ P_3^4 & 0 & 0 \\ P_3^4 & P_3^4 & 0 \end{pmatrix}$$

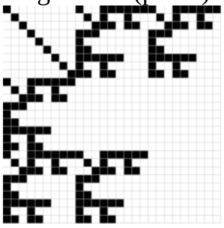
$$P_{3^2}(4,5) = \begin{pmatrix} P_3^4 & P_3^5 & P_3^5 \\ P_3^5 & 0 & 0 \\ P_3^5 & P_3^5 & 0 \end{pmatrix}$$

$$P_{3^2}(5,6) = \begin{pmatrix} P_3^5 & P_3^6 & P_3^6 \\ P_3^6 & 0 & 0 \\ P_3^6 & P_3^6 & 0 \end{pmatrix}$$

$$P_{3^2}(6,0) = \begin{pmatrix} P_3^6 & P_3^0 & P_3^0 \\ P_3^0 & 0 & 0 \\ P_3^0 & P_3^0 & 0 \end{pmatrix} \quad (17)$$

In order to get higher order primitive elements, we still retain the structure of P_3 matrix and put into the elements of the group $F(P_{3^2}(i, i+1))$. We get 3^3 order matrix (call it a third order expansion).

For example, if we use the elements of group $F(P_{3^2}(0,1))$ for the first and second expansions of the matrix of P_3 , respectively $[P_{3^2}(0,1)]^0$ $[P_{3^2}(0,1)]^1$ matrices, we get the following matrix (pic. 5):



pic.5. $P_{3^3}(0,1)$

$$P_{3^3}(0,1) = \begin{pmatrix} P_{3^2}^0 & P_{3^2}^1 & P_{3^2}^1 \\ P_{3^2}^1 & 0 & 0 \\ P_{3^2}^1 & P_{3^2}^1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} \begin{pmatrix} P_3^0 & 0 & 0 \\ 0 & P_3^0 & 0 \\ 0 & 0 & P_3^0 \end{pmatrix} & \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix} & \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix} \\ \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix} & 0 & 0 \\ \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix} & \begin{pmatrix} P_3^0 & P_3^1 & P_3^1 \\ P_3^1 & 0 & 0 \\ P_3^1 & P_3^1 & 0 \end{pmatrix} & 0 \end{pmatrix} \quad (18)$$

Let's consider $[P_{3^3}(0,1)]^k$ set. It has the same basic structure P_3 as the primary group, as well as the first and second expansion matrices taken from the primary group. It is expected that this set is characterized by the same properties as the primary group has. Indeed, experimentally, it also has diagonal matrices, whose diagonal elements represent one of the perturbations of the primary group.

For the set $[P_{3^3}(0,1)]^k$ diagonal matrices are $[P_{3^3}(0,1)]^{j\cdot\left(2^{2\cdot 3^2}+2^{3^2}+1\right)}$, $j = 1,2,3,\cdots,2^{3^2}-1$.

When $j = 2^{3^2} - 1$, we get the final element of the set $[P_{3^3}(0,1)]^k$:

$$[P_{3^3}(0,1)]^{(2^{3^2}-1)\cdot\left(2^{2\cdot 3^2}+2^{3^2}+1\right)} = [P_{3^3}(0,1)]^{(2^{3^3}-1)} =$$

$$= \begin{pmatrix} [P_{3^0}(0,1)]^0 & 0 & 0 \\ 0 & [P_{3^0}(0,1)]^0 & 0 \\ 0 & 0 & [P_{3^0}(0,1)]^0 \end{pmatrix} (19)$$

We see that this is an Identity matrix. Therefore $P_{3^3}(0,1)$ is a primitive element and creates the Abelian multiplicative finite group with power $2^{3^3} - 1$.

Definition: We call the following matrix

$$P_{3^k}(i, i+1) = \begin{pmatrix} P_{3^{k-1}}^{i} & P_{3^{k-1}}^{i+1} & P_{3^{k-1}}^{i+1} \\ P_{3^{k-1}}^{i+1} & 0 & 0 \\ P_{3^{k-1}}^{i+1} & P_{3^{k-1}}^{i+1} & 0 \end{pmatrix} \quad (20)$$

where $P_{3^{k-1}}^{i} \in F(P_{3^{k-1}}(i, i+1))$, as the k^th^ order $(i, i+1)$ expansion of the P_3 matrix.

Theorem: $P_{3^k}(i, i+1)$ is a primitive element and creates the abelian multiplicative finite group $F(P_{3^k}(i, i+1))$ with power $2^{3^k} - 1$.

In general matrices $\left[P_{3^k}(i, i+1)\right]^{j(2^{2\cdot 3^{k-1}}+2^{3^{k-1}}+1)}$, where $j = 1,2,3,\cdots,2^{3^{k-1}}-1$ are diagonal matrices and diagonal elements are one of the permutations of the elements of the primary group.

When $j = 2^{3^{k-1}} - 1$, we get

$$\left[P_{3^k}(i, i+1)\right]^{j\left(2^{2\cdot 3^{k-1}}+2^{3^{k-1}}+1\right)}=$$

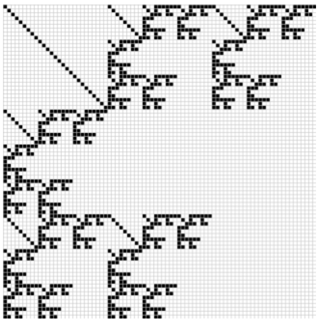
$$= \left[P_{3^k}(i, i+1)\right]^{(2^{3^{k-1}}-1)\cdot(2^{2\cdot 3^{k-1}}+2^{3^{k-1}}+1)}=$$

$$= \left[P_{3^k}(i, i+1)\right]^{(2^{3^{k-1}}-1)}$$

$$= \begin{pmatrix} \left[P_{3^{k-1}}(i, i+1)\right]^0 & 0 & 0 \\ 0 & \left[P_{3^{k-1}}(i, i+1)\right]^0 & 0 \\ 0 & 0 & \left[P_{3^{k-1}}(i, i+1)\right]^0 \end{pmatrix}$$

(21)

This means that (3) the structure is a primitive matrix. The primitive matrices obtained have an interesting fractal structure (see pic. 6). Abelian multiplicative groups adopted by the above mentioned method represent sufficient sets for realizing our one-way matrix functions



pic.6. $P_{3^4}(0,1)$

IV. Conclusion

Basic P_3 matrix $P_{3^k}(i, i+1)$ expansions are primitive matrices they generate abelian multiplicative matrix groups.

An interesting trend of research results in the idea: use the elements of the primary field as the first and second expanding matrices with the same characteristic polynom. It is also important the use of other baseline matrices, which enlarges a new type of primitive structures. Elements of abelian multiplicative matrix groups can be used in implementation of one way function, that we offer. So the key exchange method is got and it is secure against quantum computers attacks.

ACKNOWLEDGEMENT

The Work Was Conducted as a Part of Research Grant of Joint Project of Shota Rustaveli National Science Foundation and Science & Technology Center in Ukraine [№ STCU-2016-08]

References

[1]. Shor, *P*. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)

[2]. Jones, J. A. NMR quantum computation. Prog. NMR Spectrosc. 38, 325–360 (2001)

[3]. Ekert, A. & Jozsa, R. Quantum computation and Shor's factoring algorithm. Rev. Mod. Phys. 68(3**)**, 733–753 (1996).

[4]. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 4, 2017, p. 28-3

[5]. Avtandil Gagnidze & Maksim Iavich & Giorgi Iashvili, 2017. "Some Aspects Of Post-Quantum Cryptosystems," Eurasian Journal of Business and Management, Eurasian Publications, vol. 5(1), pages 16-20

[6]. Werner Alexi , Benny Chor , Oded Goldreich , Claus P. Schnorr, RSA and Rabin functions: certain parts are as hard as the whole, SIAM Journal on Computing, v.17 n.2, p.194-209, April 1988 [doi>10.1137/0217013]

[7]. R. P. Megrelishvili, Analysis of the matrix one-way function and two variants of its implementation, International J. of Multidisciplinary Research And Advances In Engineering (IJMRAE), v.5, n. IV (October 2013), pp. 99-105.

[8]. G. L. Long, X. S. Liu , Theoretically efficient high-capacity quantum-key-distribution scheme, Phys. Rev. A 65, 2002

[9]. W. Shor, John Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol Peter Phys. Rev. Lett. 85, 441, 2000

[10]. Shu-Shen Li, Gui-Lu Long, Feng-Shan Bai, Song-Lin Feng and Hou-Zhi Zheng, Quantum computing, PNAS 2001 October, 98 (21) 11847-11848. https://doi.org/10.1073/pnas.191373698

[11]. Marlan O. Scully and M. S. Zubairy, Quantum optical implementation of Grover's algorithm, PNAS 2001 August, 98 (17) 9490-9493. https://doi.org/10.1073/pnas.171317798