Generation of high order primitive matrix elements for post-quantum key exchange protocol

Richard Megrelishvili
Math *dept. Tbilisi State University*
Tbilisi, Georgia
richard.megrelishvili@tsu.ge

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

Avtandil Gagnidze
Faculty of management.
Bank of Georgia University
Tbilisi, Georgia
gagnidzeavto@yahoo.com

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

Giorgi Iashvili
School of technology. Caucasus University
Tbilisi, Georgia
g.iashvili@scsa.ge

Abstract— Active work is performed to create quantum computers. Quantum computers can break existing public key cryptography. So they can break Diffie-Hellman key exchange protocol. Matrix algorithms of key exchange can be considered as the alternative to Diffie-Hellman key exchange protocol.

The improved method of key-exchange protocol is offered in the article. The method deals with the original matrix one-way function and the generalized method of processing the corresponding high order matrix multiplicative finite commutative group.

The general method of the insertion-enlarging method of building the primitive elements of the field is derived from elements of the matrix groups with different power.

The article describes the results that give us the prospect of generating the high order multiplicative Abelian matrix groups and of creating key-exchange protocol, resistant to quantum computers attacks by means of this groups.

Keywords— Matrix One-way Function, Abelian Finite Field, Asymmetric Cryptography, High order finite matrix Field, Primitive Matrix Element, quantum computers, post-quantum cryptography.

I. Introduction

Scientists and experts are actively working on the creation of quantum computers. GOOGLE Corporation, NASA the association USRA (Universities Space Research Association and D-Wave teamed-up to develop quantum processors.
Quantum computers can break existing public-key crypto systems. Quantum computer solves the discrete logarithm problem both for finite fields and elliptic curves. Being able to calculate efficiently discrete logarithms, it can break Diffie-Hellman key exchange protocol.
Quantum computer also solves the factorization problem, so it can easily break RSA cryptosystem.

Public-key cryptography is used in different products, on different platforms and in various fields. Many commercial products use public-key cryptography, the number of which is actively growing. Public-key cryptography is also widely used in operating systems from Microsoft, Apple, Sun, and Novell. It is used in secure phones, Ethernet, network cards, smart cards, and it is widely used in cryptographic hardware. Public-key technology is used in protected Internet communications, such as S / MIME, SSL and S / WAN. It is used in government, banks, most corporations, different laboratories and educational organizations. Breaking existing public-key crypto-systems will cause complete chaos [1,2].
Public-key crypto systems, resistant to quantum attacks, are developed. But nowadays successful attacks are recorded on these systems [3,4].

II. One-way matrix function

One of the modifications of Diffie-Hellman's well-known method of cryptographic key exchange is the matrix algorithms of the exchange, the basis for which is the high order cyclic multiplicative matrix groups in the GF (2) field.
Suppose that the P matrix is a primitive element of a cyclic matrix group. While (P) is a multiplicative group formed by this matrix, with the power $2^n - 1$, where n is the size of the square matrix.
The matrix algorithm for general key development is the following:

- The sender sends to the receiving party via the open channel $u_1 = vP_1$ vector, where $P_1 \in \langle P \rangle$ is the secret matrix, selected by the sender, and $v \in V_n$ is commonly known (V_n – is vector space on $GF(2)$ field);
- The receiving party chooses $P_2 \in \langle P \rangle$ to send a secret matrix and sends to the sender $u_2 = vP_2$ vector;

- Sender calculates $k_1 = u_2 P_1$ vector;
- Receiver calculates $k_2 = u_1 P_2\, v$, where k_1 and k_2 – are secret keys.

It is evident, thar $k_1 = k_2 = k$, because $k = vP_1P_2 = vP_2P_1$, while $\langle P \rangle$ is a commutative group. Let $v = (v_1, v_2, v_3, \cdots, v_n) \in V_n$ and $u = (u_1, u_2, u_3, \cdots, u_n) \in V_n$ are non-secret vectors from the above mentioned algorithm and

$$P_1 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in \langle P \rangle$$

is the secret matrix. Then, according to the algorithm:

$$vP_1 = \begin{pmatrix} v_1a_{11} + v_2a_{21} + \cdots + v_na_{n1} \\ v_1a_{12} + v_2a_{22} + \cdots + v_na_{n2} \\ \vdots \\ v_1a_{n1} + v_2a_{n2} + \cdots + v_3a_{n3} \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \quad (1)$$

The number of variables in the system of linear equations is the square of the number of equations. Generally, solutions in such cases are not uniquely defined, and the system has infinitely many solutions. However, because we deal with a special types of matrices, the solution is defined uniquely. In addition, it is obvious that the solution of the system is very time consuming and is practically impossible in real time if the size of the matrix is large enough.

All this makes it necessary to generate high order Abelian multiplication matrix group, whose primitive element will be a high order quadratic matrix.

III. FINITE MATRIX GROUPS

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

$$\begin{aligned} (1+\alpha)^0 &= 1 && 1 \\ (1+\alpha)^1 &= 1+\alpha && 11 \\ (1+\alpha)^2 &= 1+\alpha^2 && 101 \\ (1+\alpha)^3 &= 1+\alpha+\alpha^2+\alpha^3 && 1111 \\ (1+\alpha)^4 &= 1+\alpha^4 && 10001 \\ (1+\alpha)^5 &= 1+\alpha+\alpha^4+\alpha^5 && 110011 \end{aligned}$$

The polynomial coefficients generated by the above structure, are known as the Serpinsky triangle. Serpinsky's structure contains a number of sub-structures, that can be used as a generator (generating matrix) for multiplication groups, i.e. primitive elements. For example,

$$P_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

$$P_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \quad (2)$$

Many others examples can be provided. Their natural powers form the Abelian multiplicative cyclic group.

It's easy to see that natural powers of matrices P_3 , P_5 , P_7

$$P_3^k\ ,\ P_5^k\ ,P_7^k\ , k = 1,2, \dots, 2^k - 1 \quad (3)$$

Form the Abelian multiplicative cyclic group:

$$P_3^1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, P_3^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \ P_3^3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, P_3^4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$
$$P_3^5 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, P_3^6 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \ P_3^7 = P_3^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (4)$$

Therefore we derived the insertion-enlargement method of second order enlargement of the basic structure of P_3 [5].

Let's keep the structure of the matrix P_3 and enlarge it by elements of the set (4) as following [5]:

$$P_{3^2}(i,j) = \begin{pmatrix} P_3^i & P_3^j & P_3^j \\ P_3^j & 0 & 0 \\ P_3^j & P_3^j & 0 \end{pmatrix}, \text{ where } i,j=0..6. \quad (5)$$

P_3 matrix is called a basic structure and let's call P_3^i and P_3^j matrices the first and the second enlarged matrice and $P_{3^2}(i,j)$ matrix let's call the second order $(\boldsymbol{i},\boldsymbol{j})$ enlargement of P_3.

The set P_3^k , $k = 1,2,\dots,2^3 - 1$ is called the primary group for $F(P_{3^2}(i,i+1))$ group.

We have proved the following statement:

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

For example, the matrix $P_{3^2}(0,1)$ is primitive, and the matrix $[P_{3^2}(0,1)]^{2^{2\cdot 3^1}+2^{3^1}+1}$ is diagonal matrix:

$$[P_{3^2}(0,1)]^{2^{2\cdot 3^1}+2^{3^1}+1}=\begin{pmatrix} P_3^3 & 0 & 0 \\ 0 & P_3^3 & 0 \\ 0 & 0 & P_3^3 \end{pmatrix} \quad (6)$$

All powers $\left([P_{3^2}(0,1)]^{2^{2\cdot 3^1}+2^{3^1}+1}\right)^i$, $i = 1,2,\dots$ of the diagonal matrix are also diagonal and because of the set $F(P_{3^2}(0,1))$ are a finite group, when $i = 2^{3^1} - 1$, so we see:

$$\left([P_{3^2}(0,1)]^{2^{2\cdot 3^2}+2^{3^2}+1}\right)^i = \begin{pmatrix} (P_3^3)^i & 0 & 0 \\ 0 & (P_3^3)^i & 0 \\ 0 & 0 & (P_3^3)^i \end{pmatrix}$$

$$\begin{pmatrix} (P_3^3)^i & 0 & 0 \\ 0 & (P_3^3)^i & 0 \\ 0 & 0 & (P_3^3)^i \end{pmatrix} = \begin{pmatrix} P_3^{3i \bmod i} & 0 & 0 \\ 0 & P_3^{3i \bmod i} & 0 \\ 0 & 0 & P_3^{3i \bmod i} \end{pmatrix} \quad (7)$$

As we perform the matrix operations correspondig to the module of the primary group, the matrix (7) is the identity matrix. That means, that the set $F(P_{3^2}(0,1))$ is a finite group.

Note that we can consider any element of (4) as the basic structure. There exist the enlargement of this element using P_3^0 and P_3^1 matrices, that is primitive.

For example, following enlargements are primitive:

$$\begin{pmatrix} P_3^1 & P_3^1 & 0 \\ 0 & 0 & P_3^1 \\ P_3^0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} P_3^1 & 0 & P_3^0 \\ P_3^1 & P_3^1 & P_3^1 \\ 0 & P_3^1 & P_3^1 \end{pmatrix}, \begin{pmatrix} 0 & P_3^1 & 0 \\ 0 & P_3^1 & P_3^1 \\ P_3^0 & 0 & P_3^1 \end{pmatrix} \quad (8)$$

Consider higher order sub-structures of the Serpinsky triangle:

$$P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

It is easy to check that P_5 is a primitive element. It means that P_5^k , $k = 1,2,\dots,2^5 - 1$ is a finite Abelian multiplicative group.

Consider basic structure P_3 and enlarge it by P_5^0 and P_5^1 matrices.

There exist such enlargements of P_3 matrix by P_5^0 and P_5^1 matrices, that are primitive elements. For example:

$$\begin{pmatrix} P_5^1 & P_5^1 & P_5^1 \\ P_5^1 & 0 & 0 \\ P_5^0 & P_5^1 & 0 \end{pmatrix}, \begin{pmatrix} P_5^1 & P_5^1 & P_5^1 \\ P_5^1 & 0 & 0 \\ P_5^1 & P_5^0 & 0 \end{pmatrix} \quad (9)$$

matrices are primitive elemenents. Therefore the set $F\left(P_{3\times 5^1}(P_5^0,P_5^1)\right)$ is a finite Abelian multiplicative group.

It is easy to check that

$$[P_{3\times 5^1}(P_5^0,P_5^1)]^{2^{2\cdot 5^1}+2^{5^1}+1} = \begin{pmatrix} P_5^2 & 0 & 0 \\ 0 & P_5^2 & 0 \\ 0 & 0 & P_5^2 \end{pmatrix} \quad (10)$$

is a diagonal matrix. With the analogy to (7) we see that $\left([P_{3\times 5^1}(P_5^0,P_5^1)]^{2^{2\cdot 5^1}+2^{5^1}+1}\right)^i$, $i = 1,2,\dots$ matrices are diagonal, and when $i = 2^{5^1} - 1$, we see

$$\begin{pmatrix} P_5^{2i \bmod i} & 0 & 0 \\ 0 & P_5^{2i \bmod i} & 0 \\ 0 & 0 & P_5^{2i \bmod i} \end{pmatrix} \quad (11)$$

the identity matrix. That means, that the set $F\left(P_{3\times 5^1}(P_5^0,P_5^1)\right)$ is a finite Abelian multiplicative group with power of $2^{3\times 5^1} - 1$.

Consider now enlargements of order k=2 P_5^i , $i = 1,2,\dots,2^5 - 1$ of the primitive element P_5 using elements $P_{5^k}(P_5^0,P_5^1), k = 2$. There exist such enlargements, that form a primitive matrix. For example:

$$P_{5^k}(P_5^0,P_5^1) = \begin{pmatrix} P_5^1 & P_5^1 & P_5^1 & P_5^1 & P_5^0 \\ P_5^1 & 0 & 0 & 0 & 0 \\ P_5^1 & P_5^1 & 0 & 0 & 0 \\ P_5^1 & 0 & P_5^1 & 0 & 0 \\ P_5^1 & P_5^1 & P_5^1 & P_5^1 & 0 \end{pmatrix}, k = 2$$

(12)

Using the software developed by us, it could be seen that the matrix $\left(P_{5^k}(P_5^0, P_5^1)\right)^i$, where $i = 2^{4\cdot 5^{k-1}} + 2^{3\cdot 5^{k-1}} + 2^{2\cdot 5^{k-1}} + 2^{5^{k-1}} + 1$, $k = 2$ is a diagonal matrix:

$$\left(P_{5^k}(P_5^0, P_5^1)\right)^{2^{4\cdot 5^{k-1}}+2^{3\cdot 5^{k-1}}+2^{2\cdot 5^{k-1}}+2^{5^{k-1}}+1} = \begin{pmatrix} P_5^4 & 0 & 0 & 0 & 0 \\ 0 & P_5^4 & 0 & 0 & 0 \\ 0 & 0 & P_5^4 & 0 & 0 \\ 0 & 0 & 0 & P_5^4 & 0 \\ 0 & 0 & 0 & 0 & P_5^4 \end{pmatrix}$$

All powers $\left(P_{5^k}(P_5^0, P_5^1)\right)^{i\times j}$, are diagonal matrices with elements P_5^i, $i = 1,2,\dots,2^5 - 1$ from primary group on diagonal. When $j = 2^{3^{k-1}} - 1$, we have the identity matrix:

$$\begin{pmatrix} P_5^{4j \bmod j} & 0 & 0 & 0 & 0 \\ 0 & P_5^{4j \bmod j} & 0 & 0 & 0 \\ 0 & 0 & P_5^{4j \bmod j} & 0 & 0 \\ 0 & 0 & 0 & P_5^{4j \bmod j} & 0 \\ 0 & 0 & 0 & 0 & P_5^{4j \bmod j} \end{pmatrix} = \begin{pmatrix} P_5^0 & 0 & 0 & 0 & 0 \\ 0 & P_5^0 & 0 & 0 & 0 \\ 0 & 0 & P_5^0 & 0 & 0 \\ 0 & 0 & 0 & P_5^0 & 0 \\ 0 & 0 & 0 & 0 & P_5^0 \end{pmatrix}$$

CONCLUSIONS

The results, described above, give us the prospect of generating the high order multiplicative Abelian matrix groups and of the creating key-exchange protocol, resistant to quantum computers attacks.

ACKNOWLEDGMENT

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]. Gagnidze A.G., Iavich M.P., Iashvili G.U., Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, 2017, p.29-36

[2]. Song F. (2014) A Note on Quantum Security for Post-Quantum Cryptography. In: Mosca M. (eds) Post-Quantum Cryptography. PQCrypto 2014. Lecture Notes in Computer Science, vol 8772. Springer, Cham

[3]. Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani Phys. Rev. Lett. 98, 230501 – Published 4 June 2007

[4]. 1. Dinh H., Moore C., Russell A. (2011) McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks. In: Rogaway P. (eds) Advances in Cryptology – CRYPTO 2011. CRYPTO 2011. Lecture Notes in Computer Science, vol 6841. Springer, Berlin, Heidelberg

[5]. 5. R. Megrelishvili, M. Jinjikhadze, M. Iavich, A. Gagnidze, G. Iashvili, Post-quantum Key Exchange Protocol Using High Dimensional Matrix; CEUR Workshop Proceedings (http://ceur-ws.org/Vol-2145/), Vol-2145 2019

[6]. Damaševičius, R., Napoli, C., Sidekerskienė, T., & Woźniak, M. (2017). IMF mode demixing in EMD for jitter analysis. Journal of Computational Science, 22, 240-252.