The Third International Conference "Problems of Cybernetics and Informatics"
September 6-8, 2010, Baku, Azerbaijan. Section #1 "Information and Communication Technologies"
www.pci2010.science.az/1/18.pdf

INVESTIGATION OF NEW MATRIX-KEY FUNCTION FOR THE PUBLIC CRYPTOSYSTEMS

Richard Megrelishvili[1], Malkhaz Chelidze[2], Gela Besiashvili[3]

[1,3]Iv.Javakhishvili Tbilisi State University, Tbilisi, Georgia
[2]Sukhumi State University, Tbilisi, Georgia
[1]*richard.megrelishvili@tsu.ge*, [2]*makho111@hotmail.com*, [3]*gela.besiashvili@tsu.ge*

The main aim of this work consists in the investigation of new matrix structures that can be used in constructing cryptographic methods and algorithms. The idea is that these constructions must perform the same functions as in the well-known algorithms operating via an open channel. Here, in the first place we mean the Diffie-Hellman protocol, i.e., our intention is to develop functional schemes with the aid of matrices which are analogous to a one-way function. An idea of matrix-key construction is not new [1], though has recently again evoked interest in scientific circles [2]. The justification of efforts undertaken by scientists evidently lies in fast-operating schemes and software solutions for matrix structures [2,3].

We want to draw attention to the fact that some non-degenerate matrices (matrices with nonzero determinants) contain an intro-matrix recurrent dependence [4,5]. This dependence exists among matrix rows and 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 an intro-matrix recurrent dependence, but, in a number of cases (especially for matrices of large size) the revealing of an intro-matrix recurrent dependence is not a simple task.

Matrices with an intro-matrix recurrent 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 α, which is the root of a primitive polynomial $p(x)=1+x+x^3$, has the form [6]:

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

The multiplicative group (1) is written in terms of powers of α, the corresponding entries are written in terms of polynomials of α 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 (1), we can write, for example, a multiplicative group of matrices A, A^2, A^3, . . . , $A^7 = I$ (I is the unit matrix) as follows:

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

This group is generated by the primitive matrix A which corresponds to an element α (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 α^i. All matrices A^i *(2)* have an intro-matrix recurrent 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:

$$A^i=\begin{pmatrix}x_{11}&x_{12}&x_{13}\\x_{21}&x_{22}&x_{23}\\x_{31}&x_{32}&x_{33}\end{pmatrix}. \tag{3}$$

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

$$A_1^i=\begin{pmatrix}x_{11}&x_{12}&x_{13}\\x_{13}&x_{11}+x_{13}&x_{12}\\x_{12}&x_{13}+x_{12}&x_{11}+x_{13}\end{pmatrix}. \tag{4}$$

This matrix can be easily broken even in the case of a single cryptographic application, for example, when it is used to realization 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 intro-recurrent 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.

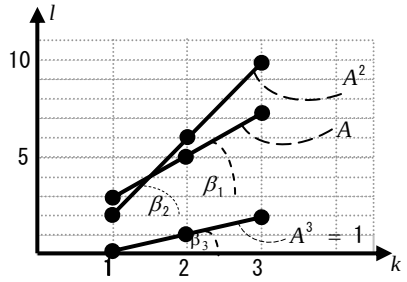
As an example we give a construction, different from (2), of a multiplicative group of matrices with period $e=3$:

$$A=\begin{pmatrix}1&1&0\\1&1&1\\1&0&0\end{pmatrix},\quad A^2=\begin{pmatrix}0&0&1\\1&0&1\\1&1&0\end{pmatrix},\quad A^3=I=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}. \tag{5}$$

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

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 (5) (where l is the exponent of the power of a field element α^l (1), 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 (5) is linear. It is obvious that the dependence $l=f(k)$ for all the above-considered matrices with an intro-matrix recurrent dependence is also linear. However, as

different from the matrices (5) (see Fig. 1), the linearity of all matrices of the form (2) is one and



the same (i.e. β is a constant value) and can be easily determined. Therefore the intro-matrix recurrent dependence in them is trivial.

Fig. 1 The linear dependence $l = f(k)$ for the multiplicative group (5).

In reality, not all matrix sets (groups) will have the linear dependence $l = f(k)$. For example, matrices of the multiplicative group (6), with period $e = 7$, do not contain the recurrent dependences considered above:

$$A=\begin{pmatrix}1&0&1\\1&0&0\\0&1&1\end{pmatrix},\ A^2=\begin{pmatrix}1&1&0\\1&0&1\\1&1&1\end{pmatrix},\ A^3=\begin{pmatrix}0&0&1\\1&1&0\\0&1&0\end{pmatrix},\ldots,A^7=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}. \quad (6)$$

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 (2)-(4) we have a trivial intro-matrix recurrent dependence;
- For a set of $n \times n$ matrices of the form (5), we have the linear intro-matrix recurrent dependence $l = f(k)$.
- For a set of $n \times n$ matrices, of the form (6), the intro-matrix recurrent dependence is not observed.

Our aim is to construct a multiplicative group of matrices that will be free of an intro-matrix recurrent 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 on the symmetry of elements and at the same time the asymmetry with respect to the diagonals is also taken into account.

The initial 5×5 matrix $A_{n=5}$ is constructed on the basis of the matrix $A_{n=3}$. The 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 where $n = 2k - 1$, $k > 1$, is an integer number.

$$A_{n=5}=\begin{pmatrix}1&0&1&0&1\\1&1&0&1&0\\0&1&1&0&1\\1&0&1&0&0\\0&1&0&1&0\end{pmatrix},\ A_{n=7}=\begin{pmatrix}1&0&1&0&1&0&1\\1&&&&&&0\\0&&&&&&1\\1&&&A_{n=5}&&&0\\0&&&&&&1\\1&&&&&&0\\0&1&0&1&0&1&0\end{pmatrix},\dots,\ A_n=\begin{pmatrix}1&0&1&0&.&.&1\\1&&&&&&0\\0&&&&&&1\\.&&&A_{n-2}&&&.\\.&&&&&&.\\1&&&&&&0\\0&1&0&1&..&.&0\end{pmatrix}. \tag{7}$$

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

To realize an alternative algorithm, we should prescribe the initial $n\times n$ matrix A (the matrix A is open), which generates a multiplicative group of high power A (see Section 3).

The algorithm of matrix key exchange via an open channel is realized as follows:

• Alice chooses (at random) an $n\times n$ matrix $A_1\in\mathsf{A}$ and send Bob the vector $b=aA_1$.

• Bob chooses (at random) an $n\times n$ matrix $A_2\in\mathsf{A}$ and sends Alice the vector $c=aA_2$, where a is an n-dimensional vector (open), A_1 and A_2 are the (secret) matrix keys.

• Alice computes $k_1=cA_1$.

• Bob computes $k_2=bA_2$, where k_1 and k_2 are the secret keys. $k_1=k_2=k$ because $k=aA_1A_2=aA_2A_1$.

The main results obtained in the paper are as follows:

– A new method of constructing a special class of matrix sets of high power is worked out. In constructing $n\times n$ matrices, the initial matrices are always primitive with a maximal period equal to $e=2^n-1$. The multiplicative group of generated matrices is commutative.

– To obtain matrices with the prescribed properties, we investigated the problem of intro-matrix recurrent dependences. The results of our investigation led to the conclusion that the group of generated matrices contains no intro-recurrent dependences.

– The matrices of the constructed multiplicative groups can be applied as a one-way function.

– Based on the set of obtained matrices, we developed a matrix key exchange algorithm analogous to the Diffie-Hellman protocol, which also can be used in encryption-decryption.

References

1. Hill. L.S. Cryptography in an Algebraic Alphabet. American Mathematical Monthly, v. 36, Jun-Jull 1929, pp. 306-312.
2. Erosh I. L., Sergeev N.B. (in Russian) Speedy encryption-decryption of variety information. Voprosi Peredachi. Zaŝ. Inf., Sankt-Petersburg, 133-155 (2006).
3. Schneir B.: Applied cryptography. John Wiley and Sons. New York (1996).
4. Megrelishvili,R , Sikharulidze A. New Matrix-Sets Generation and the Cryptosystems. Proceedings of the International Conference on Computing and Computational Intelligence, Tbilisi, Georgia, (2009), pp. 253-256.
5. Megrelishvili R., Sikharulidze A., Chelidze M., Tkhilaishvili R.. (in Russian) Generation of matrix-keys and the cryptosystems. Intercultural Communications; Intercultural Relation Society; Tbilisi, №9, (2009), pp. 230-235.
6. Peterson W.: Error-correcting codes. John Wiley and Sons. New York- London (1961).