New Matrix-Sets Generation and the Cryptosystems

RICHARD MEGRELISHVILI
Department of Exact and Natural Sciences
Iv.Javakhishvili Tbilisi State University
2, University st. Tbilisi 0143
GEORGIA
r_megreliishvili@yahoo.com

ANNA SIKHARULIDZE
Department of Exact and Natural Sciences
Iv.Javakhishvili Tbilisi State University
2, University st. Tbilisi 0143
GEORGIA
anikge@yahoo.com

Abstract: - The aim of this paper is to give the new generation of the sets of $n \times n$ matrices, which are isomorphic to Galois Field $GF(2^n)$. The order of primitive matrices of a multiplicative group is $e = 2^n - 1$. On that ground the matrix- key exchange algorithm via public channel, as analogous of Diffie-Hellman protocol and the algorithm of message encryption – decryption with key-exchange by public-channel are constructed. It is shown that these cryptosystems are not breaking with chosen-plaintext attack and they are generally faster than well-known public-key algorithms.

Key-Words: - **C**ryptography, Message, Plaintext, Encryption, Public channel, Matrix-key, Chosen plaintext attack, Cipertext.

1 Introduction

The paper discusses the matrix construction method, which generates high capacity sets of matrices. For simplicity the construction of matrices is discussed on Galois Field $GF(2)$. These sets are characterized by following properties:

– The dimension of matrices is $n \times n$, where $n > 4$ is any odd number;

– Matrices create multiplicative group which is isomorphic to multiplicative group of Galois Field $GF(2^n)$. The order of primitive elements of this group is Mersen's number $e = 2^n - 1$;

– These matrices are commutative.

Bellow we discuss the following questions:

– The method of matrix construction;

– The algorithm on matrices analogical to Diffie-Hellman protocol;

– Performing encryption – decryption on matrix-keys by public-channel.

The basis of matrices construction is symmetry of their elements and, in same course, diagonal asymmetry. Using primitive A matrix of $n \times n$ dimension we construct $A^2, A^{2^2}, ..., A^{2^{n-1}}$ matrices, which represent the basis of set of Matrices **A**. The order of this set is $e = 2^n - 1$. If we add zero matrix we obtain matrix filed with 2^n elements. This process is analogical to the construction of Galois Field $GF(2^n)$. This analogy is reflected, as an example in the following theorem:

Let $p(x)$ be a polynomial of degree n with coefficients in $GF(p)$, which is irreducible in this field and let α be a root of $p(x)$ in extension field. Then $\alpha, \alpha^p, ..., \alpha^{p^n}$ are all the roots of $p(x)$ ([1], Theorem 6.26.). If α is primitive element then $\alpha, \alpha^2, \alpha^3, ..., \alpha^e = 1$ are elements of multiplicative group of $GF(2^n)$ Field. The matrices discussed bellow generate the group of matrices $A, A^2, A^3, ...A^e = I$ which are isomorphic to multiplicative group of $GF(2^n)$ field. I is $n \times n$ identity matrix, the order of group is $e = 2^n - 1$. The choice of $A^i \in$ **A** matrix can be performed according to above theorem.

2 Construction of Multiplicative Group of Matrices

Each initial 5×5 matrix $A(5)$ is constructed as indicated above (for example as in Fig. 1). The following 7×7 matrix $A(7)$ is constructed based on $A(5)$ and so on, each $n \times n$ matrix $A(n)$ is constructed based on $A(n-2)$ matrix, where $n = 2k + 1$, $k > 1$ is an integer.

$$A(5)=\begin{pmatrix}1&0&1&0&1\\1&1&0&1&0\\0&1&1&0&1\\1&0&1&0&0\\0&1&0&1&0\end{pmatrix},$$

$$A(7)=\begin{pmatrix}1&0&1&0&1&0&1\\1&&&&&&0\\0&&&&&&1\\1&&&A(5)&&&0\\0&&&&&&1\\1&&&&&&0\\0&1&0&1&0&1&0\end{pmatrix},$$

$$\ldots..$$

$$A(n)=\begin{pmatrix}1&0&1&0&.&\ldots&1\\1&&&&&&0\\0&&&&&&1\\.&&&A(n-2)&&&.\\\vdots&&&&&&\vdots\\1&&&&&&0\\0&1&0&1&.&\ldots&0\end{pmatrix}.$$

Fig. 1. Construction of $A(n)$ matrix.

Fig.2 shows the example of multiplicative group where 5×5 matrix A is the primitive matrix of group.

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

$$A^{30}=\begin{pmatrix}0&1&0&0&1\\1&1&1&0&1\\0&1&0&1&1\\1&1&1&0&0\\1&0&0&1&0\end{pmatrix},\ A^{31}=\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}.$$

Fig.2. The multiplicative group generated by $A(5)$ matrix.

As seen the order of matrix A is $e=25-1=31$. Any matrix from this group excluding A^{31} is primitive. e is Mersen's number. Matrices are commutative.

3 Matrix- key algorithm as analogous of Diffie-Hellman protocol

The matrix-key exchange algorithm via public channel goes as follows: X chooses a random $n\times n$ matrix $A_1\in\mathbf{A}$ and sends to Y

$$b=aA_1,$$

where a is an public n-dimensional vector; A_1 matrix is private key.

Y chooses a random $n\times n$ matrix $A_2\in\mathbf{A}$ and sends to X

$$c=aA_2,$$

where A_2 matrix is private key.

X computes

$$K_1=cA_1,$$

where K_1 is the secret key.

Y computes

$$K_2=bA_2,$$

where K_2 is the secret key. $K_1=K_2=K$ because $K=aA_1A_2=aA_2A_1$.

4 Encryption and decryption with matrix-key

The process of encryption-decryption is as follows:

X chooses a random $n\times n$ matrix $A^i\in\mathbf{A}$ and sends to Y

$$c=aA^i,$$

where a is a message (plaintext), c is ciphertext .

Y chooses $A^i\in\mathbf{A}$, where $A^iA^j=A^e$ and decrypts plaintext:

$$a=c\,A^j,$$

where X computes j and sends secretly to Y via public channel (section 2) or sends via secret channel as in symmetric cryptosystems.

5 Improving security

The algorithm of encryption and decryption which is discussed in section 3, is breaking with chosen-plaintext attack [2]. Bellow we discussed how this algorithm can be improved.

Suppose encryption and decryption is performed using A^i and A^j matrix keys (see Fig.3). Change of keys by open channel can be performed by encrypted massage (ciphertext) or by using pseudo-random sequence.

Let us consider the change of keys by messages on a specific example. Suppose that for A^i and A^j matrix keys we have chosen A and A^{30} matrixes depicted on Fig.2 ($AA^{30}=A^{31}=I$). Suppose also that 15-tuple message is the following sequence:

$$a_1=010101011110110 \qquad (1)$$

Let us divide this sequence into five blocks of three

bits and transform in such a way that all five of these blocks are different. It is needed that blocks correspond to five binary numbers: 000, 001, 010, 011, 100. X will secretly receive

$$a_{11} = 010'000'011'001'100 \qquad (2)$$

plaintext, or $a_{11} = 2,0,3,1,4$ message, and Y will receive it encrypted (ciphertext). The rule for obtaining a_{11} message from a_1 massage is public [3]. This message corresponds to matrix permutation key:

$$t_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 0 & 3 & 1 & 4 \end{pmatrix}. \qquad (3)$$

(3) secret key will change rows in matrix A and columns in matrix A^{30}.

Thus we will obtain modified keys:

$$A_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

$$A_1^{30} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \qquad (4)$$

that satisfy condition $AA^{30} = A^{31} = I$.

Keys (4) will perform next step of encryption and decryption. For example, if $a_2 = 101101101110101$ is next message, then:

$$(10110)A_1 = (00011),\ (00011)A_1^{30} = (10110),$$
$$(11011)A_1 = (01000),\ (01000)A_1^{30} = (11011), \qquad (5)$$
$$(10101)A_1 = (10011),\ (10011)A_1^{30} = (10101).$$

During the second step the message $a_2 = 101101101110101$ will modify A_1 and A_1^{30} matrix keys and so on.

Obviously the increase of dimension of matrices will cause the growth of algorithm's security.

Finally, it must be mentioned the isomorphism of matrices with elements of $GF(2^n)$ field is obvious, but dependency (canonicity) between matrix components, which is important, is not yet researched fully.

It is obvious also, that against chosen-plaintext attack we will obtain better results, if for changing matrix keys we use shift-register generators as means of generating pseudo-random sequences [1,3]. Such version can not be broken by chosen-plaintext attack.

6 Conclusion

Main results discussed in this paper are:

– New method of matrix generation is developed. In generated set of $n \times n$ always exists primitive matrix, order of which is connected with the dimension of matrices, n, is maximal and equals to Mersen's number: $e = 2^n - 1$. The set of matrices is commutative.

– Based on the set of matrices matrix–key public exchange algorithm is developed, which is analogical to Diffie-Hellman protocol.

– With the purpose of growth of security the exchange of keys in open channel and encryption-decryption algorithm are developed.

Discussed Cryptosystems are generally faster then well-known public-key algorithms and are not breaking with chosen plaintext attack.

References:

[1] W.W. Peterson, *Error-correcting codes*, John Wiley and Sons, Inc. New York – London, 1961.

[2] B.Schneier, *Applied cryptography*, John Wiley and Sons, Inc. New York, 1996.

[3] R.P.Megrelishvili, G.K.Khutsishvili and M.A.Chelidze, *One method of construction of mutually inverse matrices over the Galois Field and new cryptosystem*, Georgian Engineering News, N.2, 2006, pp. 40-44.