ON THE CONSTRUCTION OF SECRET AND PUBLIC-KEY CRYPTOSYSTEMS

R. Megrelishvili, M. Chelidze, K.Chelidze

Faculty of Exact and Natural Sciences,
Iv. Javakhishvili Tbilisi State University
0143 University Street 2, Tbilisi, Georgia

(Received: 08.07.05; accepted: 11.05.06)

Abstract

In this is work is proposed the method the of constructional generation of mutually inverse matrices. It is shown that there a possibility of constructing $n \times n$ matrices over the Galois Field $GF(q)$ for any integer $n > 0$. These matrices are applied for the construction secret-key cryptosystem and combined cryptosystem. Alternative one-way function and public-key cryptosystem are also subject of study in the proposed work.

Key words and phrases: Key words and phrases: Non-singular matrices, Mutually inverse matrices, Cryptosystem, Private-key, Algebra of polynomials over the finale fields, Chosen-text attack, Public-key, Combined cryptosystem, One-way function.

1 Generatin of mutually inverse matrices

The construction of proposed square n-dimensional mutually inverse matrices is based on the algebra of polynomials over the Galois Field $GF(q)$. Below there are represented some necessary properties of matrices in algebra of polynomials.

Let A_n be the algebra of polynomials modulo $x^n - 1$ over the Galois Field $GF(q)$. It is known that in the algebra A_n there are monic polynomials $g(x)$ and $h(x)$ of minimum degrees which generate corresponding ideals I and I'. If $g(x)h(x) = x^n - 1$, then

$$a(x)b(x) \equiv 0\,(mod x^n - 1) \tag{1.1}$$

for every $a(x) \in I$ and $b(x) \in I'$. There are cyclic subspaces V and $V' \in V_n$ to each ideals I and I' (where V_n is vector space over $GF(q)$). Subspace V is a cyclic subspace if for each vector $v = (v_1, ..., v_n) \in V$ the vector $v^{(1)} = (v_n, v_1, ..., v_{n-1})$ obtained by shifting the components of v cyclically one unit to the right is also in V.

For the subspaces V and V' there is the condition (similar to (1.1)):

$$vH^T = 0, \tag{1.2}$$

where $v \in V$.

Therefore if $v^{(k)} = (v_{n-k+1}, ..., v_n, v_1, ..., v_{n-k})$ and $u^{(l)} = (v_{n-l+1}, ..., v_n, v_1, ..., v_{n-l})$[1] are the vectors obtained by shifting $v \in V$ and $u \in V'$, then from (1.2)

$$\sum_{i=1}^{n} v_i^{(k)} \cdot v_i^{(l)} = 0. \tag{1.3}$$

Consider non-singular square $n \times n$ matrices:

$$A_1 = \begin{bmatrix} g_r & g_{r-1} & ... & g_0 & 0 & ... & 0 \\ 0 & g_r & ... & g_1 & g_0 & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 0 & 0 & ... & g_r \end{bmatrix}, \tag{1.4}$$

$$A_2 = \begin{bmatrix} h_k & h_{k-1} & ... & h_0 & 0 & ... & 0 \\ & h_k & ... & h_1 & h_0 & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 0 & 0 & ... & h_k \end{bmatrix}, \tag{1.5}$$

where $n = r+k$; $g_r = h_k = 1$ because $g(x)$ and $h(x)$ are monic polynomials; $g(x)h(x) = x^n - 1$. Denote by $g(i)$ and $h(j)$ corresponding i^{th} row of the matrix A_1 and j^{th} column of matrix A_2 $(i, j \in \{1, ..., n\})$. Then,

$$g(i)A_2 = s(i), \tag{1.6}$$

where $s(i) = (s_1(i), s_2(i), ..., s_n(i)) \in V_n$.

This requires that each j^{th} component of the vector $s(i)$ satisfies the condition:

$$s_j(i) = \begin{cases} 1, \, if \; i = j; \\ 0, \, if \; i \neq j. \end{cases} \tag{1.7}$$

From (1.7) follows that

$$A_1 A_2 = I, \tag{1.8}$$

where I is the $n \times n$ identity matrix; vector $s(i)$ is the i row of matrix I; $n > 0$. It is true also of

$$A_2 A_1 = I.$$

[1]Vector $u^{(l)}$ is a vector consisting of the coefficients of $b(x)$ in reverse order.

Theorem 1.1 *Let A_n be the algebra of polynomials modulo $x^n - 1$ over $GF(q)$ and let $g(x)h(x) = x^n - 1$, where $g(x)$ and $h(x)$ are monic polynomials of degree corresponding r and k $(r + k = n)$. then $g(x)$ and $h(x)$ generate mutually inverse matrices of from (1.4) and (1.5):*

$$A_1 A_2 = I, \;\; A_2 A_1 = I \tag{1.9}$$

where I is the $n \times n$ identity matrix.

There are constructive methods for generating the corresponding polynomials which fulfil the conditions $g(x)h(x) = x^n - 1$. It is also easy to construct any less dimensional matrices from n-dimensional matrices A_1 and A_2. Generally there is a possibility of constructing the classes of mutually inverse matrices (with polynomials $g(x)$ and $h(x)$for any large integer $n > 0$.

2 Simple matrix secret-key cryptosystem (SMCS)

Below it is considered the possibility of constructing secret-key symmetric cryptosystem using matrix keys. The initial matrices A_1 (1.4) and A_2 (1.5) are public. These matrices become secret-key after the permutation of the rows of matrix A_1 and the corresponding columns of matrix A_2 (or the permutation of the columns of A_1 and the rows of A_2).

The operation of permutation is secret as well.

Generally the secret-key is:

$$K = (s_1, s_2, ..., s_N). \tag{2.10}$$

K consists of the sequences of symbols s^i and the sequences are divided into the blocks of length $l = N/n$; l is minimum integer satisfying the condition $n \leq 2^l$.

Each block can be written in a way of binary number $k_i \, (i = 1, ..., n)$. Then the secret-key will be the following:

$$K' = (k_1, ..., k_n). \tag{2.11}$$

This means that i^{th} row of A_1 will move to the $(k_i+1)^{th}$ place. The key K' determines the permutation in A_1 and generation of secret-key matrix A_1'. For receiver the key K' determines the permutation of corresponding columns in A_2 and generation of secret-key matrix A_2'. Analogously, we can permute the columns in A_1 that corresponds to the permutation of rows in A_2. Generally, the number of permutations is $(n!)^2$.

Instead of K' key we can use the permutation matrix P generated by the permutation of rows in identity matrix I with K' key. P is $n \times n$ matrix

with only one "1" in $(k_i+1)^{th}$ position in i^{th} row $(i = 1, ..., n)$. The matrix P can be used for generation of matrices A'_1 and A'_2.

Encryption in SMCS

In SMCS the encryption is done by

$$C = MA'_{1,} \tag{2.12}$$

where C : ciphertext of length n,
M : plaintex message of length n,
$A'_1 = PA_1 : n \times n$ matrix secret-key, (is secret)
$A_1 : n \times n$ matrix (1.4) (is public),
$P : n \times n$ permutation matrix (is secret).

Decryption in SMCS

Decryption is obtained in the following way:

$$M = CA'^T_2, \tag{2.13}$$

where $A'_2 = PA^T_2 : n \times n$ matrix secrete-key,
$A_2 : n \times n$ matrix (1.5) (is public).

This kind of cryptosystem (SMCS) may be broken by chosen-text attack. That is why below is considered modified cryptosystem (MMCS).

3 Modified matrix secret-key cryptosystem (MMCS)

Our intent here is to apply maximum-length pseudo-random sequence for improving crypto-strength of SMCS. In this approach m symbols of the key K (2.1) specify the maximum-length sequences.

This secret string is applicated before the encryption. The same string is used is used for decryption. The algorithm and generator polynomial $p(x) = 1 + p_1x + p_2x^2 + ... + x^m$ are public (see 3.1). The key K and the matrices A'_1 and A'_2 ((1.4), (1.4)) are secret.

31. Generation of maximum-length sequences

Consider the recurrence relation or difference equation:

$$z_{i+m} = -\sum_{j=0}^{m-1} p_j z_{i+j,} \tag{3.14}$$

where $p \neq 0, p_m = 1$, and each p_j is a coefficient of primitive polynomial $p(x)$ over $GF(2)$.

It is known that the solution of this equation is the maximum-length sequence $z_1, z_2, z_3, ...$ It is also known that linear sequential switching circuit simply calculates the sum indicates in equation (3.1) and generates periodic maximum-length sequences [1]. The initial values $z_1, z_2, ..., z_m$ in the storage devices (shifting registers) are any m symbols of the secret-key K. XOR-ing plaintext with a secret string $z_j, z_{j+1}, ..., z_{j+n-1}$ is applicated before the encryption of message.

32. Encryption and decryption in MMCS

Encryption in modified secret-key cryptosystem is done by

$$C = (M + Z)A_1', \tag{3.15}$$

where C' : ciphertext of length n,

Z : symbols of maximum-length sequences of length n (are secret, but the polynomial $p(x)$ from (3.1) is public),

$A_1' = PA_1 : n \times n$ matrix secret-key,

$A_1 : n \times n$ matrix (1.4) (is public),

$P :$ $n \times n$ permutation matrix (is secret).

Decryption is obtained in the following way:

$$M = C' A_2'^T - Z, \tag{3.16}$$

where $A_2' = PA_2^T : n \times n$ matrix secret-key,

$A_2 : n \times n$ matrix (1.5) (is public).

4 The combined symmetric system

From modified matrix secret-key cryptosystem (MMCS) can easily be obtained the combined cryptosystem with public-key cryptography method. For this we can use the Diffie-Hellman method [2]. In this approach the secret-key K can form another secret K' (applied [2]) (2.4) key. Only one small problem here is that in the key $K = k_1, ..., k_n$ the values of some blocks may coincide ($k_i = k_j$). Due to this a simple procedure can be used: the first block of the key K' is $k_1' = k_1 mod\ n$; if $k_2 \neq k_1$, then $k_2' = k_2\ \ mod\ n$; if $k_2 = k_1$ then $k_2' = (k_2 + 1)\ mod\ n$, etc. Some minimal value can be added to any k_i block to fulfill the following condition:

$$k_i' \in \{k_1', ..., k_{i-1}'\},$$

where $i = 2, 3, ..., n$.

After forming the secret-key K' this system works as the Modified Matrix Cryptosystem (MMCS) with the secret-key K' (2.2).

5 The alternative one-way function and the public-key cryptosystem

The obtained variants of one-way function are considered in [3]. Below is suggested the alternative approach of the design of one-way function and public-key cryptosistem.

Unlike Diffie-Hellman in spite of integers there are applied square matrices of order n over the field $GF(q)$. In [2] there is used the fact that for y in the one-way function $a^x = y \ mod \ p$ it is impossible to calculate x (by higher values of parameters: p, x, a). At the same time it is simple to calculate y applying x.

The idea of alternative approach is the following..

Let A be the set of commutative matrices of high order (the strength of the set A is approximately 10^{30}, i.e. $|A| \approx 2^{100}$, and this is equal of contemporary cryptosystem). Also let the matrices[2]

$$A^{2^0}, A^{2^1}, A^{2^2}, ..., A^{2^{t-1}} \tag{5.17}$$

create the basis of the set A, where $A^{2^i} \neq A^{2^j}$, if $i \neq j$ and $t \geq 100$.

So, any matrix A of the set A is obtained as the linear combination of matrices (5.1):

$$A = c_0 A^{2^0} + c_1 A^{2^1} + ... + c_{t-1} A^{2^{t-1}}, \tag{5.18}$$

where $c_i \in GF(2)$.

Let's define the order of matrices A from the following:

$$q^{n^2} \geq 2^{100}.^3 \tag{5.19}$$

For example, if $q = 11$, $n = 6$, then the absolute amount of 6×6 dimensional matrices over the field $GF(11)$ will be 11^{36}, and this satisfies the crypto strength. If $q = 2$. i.e. there is done the binary field $GF(2)$, then the minimum order of matrices will be $n = 10$.

According to (5.1)-(5.3), it is possible to obtain the method of key formation via public channel. Let the basis (5.1) or its matrix A' is known. The vector $a = (a_1, ..., a_n)\,(a_i \in GF(q))$ is also known. Then the two subjects X and Y will form the crypto-key K by the following order.

[2]The linear independent system.

[3]It is impossible to choose matrices like A in real time.

The subject X from the set A will choose matrix A_1 (private-key) and calculate vector

$$b_1 = aA_1$$

which will be transmitted to the subject Y via public channel.

Then subject Y will choose matrix A_2 (private-key) from the set A and calculate the vector

$$K_1 = b_1 A_2.$$

Subject Y will calculate the vector

$$b_2 = aA_2$$

and will transmit to subject X via public channel.

Consequently subject X will calculate the vector

$$K_2 = b_2 A_1.$$

According to the commutability of the set A, i.e. the equations $aA_1A_2 = aA_2A_1$ and $b_1A_2 = b_2A_1$,

$$K_1 = K_2.$$

That's why both subjects X and Y form same keys $K = K_1 = K_2$.

Above discussed approach can also be used for the encryption-decryption of information and for other tasks.

One can obtain the basis (5.1) by representing the elements of the field $GF(p^m)$ in the form of matrices and by its modification.[4]The matrix will be choused also by random way. Private researches don't exclude the chances of obtaining such fields of matrices, the formation of which will not be associated with the primitive polynomials over the field $GF(p)$.

For example, over the field $GF(2)$ applying basis matrices

$$A^1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, A^4 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad (5.20)$$

it is obtained the field $GF(2^3)$ (multiplicative group):

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

[4]See the article in this journal. R.Megrelishvili, M.Chelidze.: A CLASSES OF OPTIMAL AND BURST-ERROR-CORRECTING (n, k)-CODES.

$$A^4 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, A^5 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \tag{5.21}$$

$$A^6 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, A^7 = I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The multiplicative group (5.4) (and field A) is isomorphic to modulo $p(x)1 + x + x^3$ Galois field $GF(2^3)$. For example, in the A (5.4):

$$A^1 + A^2 + A^4 = 0;$$

also in the field $GF(2^3)$ is fulfilled:

$$\alpha + \alpha^2 + \alpha^4 = 0.$$

However, each matrix of (5.4) is not represented applying the primitive polynomial $p(x)$. The structure of these matrices can be defined probably using the practical realization of multiplicative group of the field A.

References

1. Peterson W.W., Weldon E.J.. Error-correcting codes. The MIT Press, Cambridge, Massachusetts, and London, England, 1972.

2. Diffie W. and Hellman M.E.. New Direction in Cryptography. IEEE Trans. Inform. Theory, v. IT-22, pp. 644-654, 1976.

3. Schneier B. Applid Cryptography. John Wiley and Sons, Ins. New York, 1996.