The Optimal Error-Correcting-Codes and Cryptosystem with Coding Matrices over the Finite Fields

Richard Megrelishvili
Department of Structural Research of Intellectual Systems of the Iv. Javakhishvili Tbilisi State University

The structures of the generalized Vandermonde Determinants over Galois Fields *GF(q)* are researched. the obtained results enable tosynthesize the optimal *(by condition (1,2))* classes linear error-correcting *(n,k,d)*-codes over *GF(2^m)(n=m+d, k=m+1, d=3;5)* and their effective linear *(n,k)*-codes over *GF(2)* with the single and double burst-error-correction.
The synthesis of *n*-dimensional non-singular matrices and their inverse matrices for any *n*>0 is realized and new matrix hybrid (public-private) cryptosystem is developed.

1. Generalized Vandermonde Determinants and the Optimal Error-Correcting-Codes

From the Theory of the correcting linear (*n,k,d*) - codes it is well known that

$$n-k \geq d-1, \tag{1.1}$$

where *n* is the length of the code words, *k* is informational symbols number and *d* is a minimal distance between the code words.

If

$$n-k = d-1, \tag{1.2}$$

then the codes are called the optimal codes [1].

It is known how important are the properties of Vandermonde Determinants for the research and formation of the code structures. However the generalized Vandermonde Determinants, which are so well researched over the fields of real numbers, yet represent problems over finite Galois Fields.

In the given work the structures of the quadratic matrices over *GF*(p^m) are researched. It is demonstrated that generalized Vandermonde Determinants for these matrices differ from 0, that allows to obtain codes over *GF*(p^m) satisfying the condition (1.2) and also to realize the synthesis of effective classes linear codes over *GF*(2).

Let *A* be the system with $\alpha_{i,j} = \alpha^{ij} \in GF\left(2^m\right),\ \left(i, j = 0,1,\ldots,m\right)$ elements of the Galois finite field modulo

$$p(x) = \sum_{\nu=0}^{m} x^{\nu}\ ,\ \ p(\alpha) = 0:$$

$$A = \begin{bmatrix} \alpha_{0,0} & \alpha_{0,1} & \cdots & \alpha_{0,m} \\ \alpha_{1,0} & \alpha_{1,1} & \cdots & \alpha_{1,m} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{m,0} & \alpha_{m,1} & \cdots & \alpha_{m,m} \end{bmatrix}, \tag{1.3}$$

where *m* is any integer for which *p*(*x*) is irreducible polynomial over *GF*(2), $\alpha \in GF\left(2^m\right)$ is the element of cyclic multiplicative subgroup of the *GF*(2^m).

Let’s consider the quadratic matrices with the elements in the arbitrary *i*-th row and *j*-th column of the system *A*:

$$A_2 = \begin{bmatrix} \alpha_{i_1,j_1} & \alpha_{i_1,j_2} \\ \alpha_{i_2,j_1} & \alpha_{i_2,j_2} \end{bmatrix}, \ A_3 = \begin{bmatrix} \alpha_{i_1,j_1} & \alpha_{i_1,j_2} & \alpha_{i_1,j_3} \\ \alpha_{i_2,j_1} & \alpha_{i_2,j_2} & \alpha_{i_2,j_3} \\ \alpha_{i_3,j_1} & \alpha_{i_3,j_2} & \alpha_{i_3,j_3} \end{bmatrix}, \qquad (1.4)$$

where $i_1 \neq i_2 \neq i_3$, $j_1 \neq j_2 \neq j_3 \in \{0,1,\ldots,m\}$.

Suppose D_2 and D_3 determinants correspond to the matrices A_2 and A_3 (1.4). Then the following theorem is correct:

Theorem 1.1. Let $GF(2^m)$ be the Galois Field of polynomials over $GF(2)$ modulo

$$p(x) = \sum_{\nu=0}^{m} x^{\nu} ,$$

and let $\alpha \in GF\left(2^m\right)$, $p(\alpha) = 0$. Then

$$D_2 \neq 0 , \ \ D_3 \neq 0 , \qquad (1.5)$$

where $\alpha \in GF\left(2^m\right)$ is element of cyclic multiplicative subgroup of $GF(2^m)$.

The determinant D_3 (1.5) is generalized Vandermonde Determinant of order three over the field $GF(2^m)$ and D_3 always differs from 0 if $p(x)$ is irreducible over $GF(2)$.

It is not difficult to show, as well, that the determinant of matrix

$$A_4 = \begin{bmatrix} \alpha_{i,j_1} & \alpha_{i,j_2} & \alpha_{i,j_3} & \alpha_{i,j_4} \\ \alpha_{i+1,j_1} & \alpha_{i+1,j_2} & \alpha_{i+1,j_3} & \alpha_{i+1,j_4} \\ \alpha_{i+2,j_1} & \alpha_{i+2,j_2} & \alpha_{i+2,j_3} & \alpha_{i+2,j_4} \\ \alpha_{i+3,j_1} & \alpha_{i+3,j_2} & \alpha_{i+3,j_3} & \alpha_{i+3,j_4} \end{bmatrix} \qquad (1.6)$$

$(i;\, j_1 \neq j_2 \neq j_3 \in \{0,1,\ldots,m\})$ differs form 0:

$$D_4 \neq 0 . \qquad (1.7)$$

The obtained results enable to synthesize the optimal (by condition (1.2.)) classes linear (n,k,d) - codes over $GF(2^m)$ modulo

$$p(x) = \sum_{\nu=0}^{m} x^{\nu}$$

($n=m+d$, $k=m+1$, d=3;5) and their linear (n,k) - codes over $GF(2)$ with the single and double burst-error-correction (where correspondingly $n = lm(m+1) + 2lm$, $k = lm(m+1)$; $n = lm(m+1) + 4lm$, $k = lm(m+1)$, $b = (l-1)m + 1$ is the bursts' length, $l \geq 1$ is integer).

Particularly from (1.5) and (1.6) follows that the basis matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ 0 & 0 & 1 & 0 & 0 & \alpha_2 & \alpha_4 & \alpha_1 & \alpha_3 \\ 0 & 0 & 0 & 1 & 0 & \alpha_3 & \alpha_1 & \alpha_4 & \alpha_2 \\ 0 & 0 & 0 & 0 & 1 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 \end{bmatrix} \qquad (1.8)$$

generates the optimal (n=9, k=5, d=5) - code over $GF(2^4)$ with the double-error-correction, where, $p(x) = 1 + x + x^2 + x^3 + x^4$, and one of the corresponding (n,k) - code over $GF(2)$ has the following parameters: n=72, k=40, $l = 2$, which corrects double bursts with length b=5.

2. A New Hybrid Cryptosystem with Coding Matrices Defined Over the Finite Field

The cryptographic methods based on the matrix structures create systems different from those obtained by Vigenere algorithm and its modifications. These systems are insufficiently researched [2].

Usually the information word for encryption of message represents the vector $a \in V_n$ of linear vector space defined over Galois Finite Field $GF(q)$ or element $a(x)$ of linear algebra A_n of polynomials modulo a polynomial $f(x)$ of degree *n* over $GF(q)$.

The ciphertext is formed from multiplying vector *a* on special *n*-dimensional matrices *A*. The decryption is realized by multiplying vector *b* on A^{-1} inverse matrices so that:

$$aA = b; \quad bA^{-1} = a. \tag{2.1}$$

In this case the main cryptographic problem represents the question of forming of the key sets or problem of forming the matrices which are algorithmically constructive in real time as well as the encryption-decryption speed, etc.

The main purpose of the following research is the synthesis of the constructions of non-singular n-dimensional matrices on a finite field and their inverse matrices and to prove that the method being researched makes the constructive presentation of an algorithm easier.

The Common Methods of Construction of the Cryptographic Matrix Keys

There are known the methods of forming of matrix A and its inverse A^{-1} matrx[3]. For example it is possible to construct the inverse of $A = (a_{ij})_1^n$ as follows:

$$A^{-1} = \begin{bmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \dots & \frac{A_{n1}}{|A|} \\ \frac{A_{12}}{|A|} & \frac{A_{22}}{|A|} & \dots & \frac{A_{n2}}{|A|} \\ \dots & \dots & \dots & \dots \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \dots & \frac{A_{nn}}{|A|} \end{bmatrix}, \tag{2.2}$$

where A_{ij} is the algebraic adjunct of a_{ij} element of A matrix.

Despite that the operations in *GF(2)* field are comparatively simple, the method which realizes (2.2) can't be accepted for some users because that matrices A and A^{-1} are not represented obviously due to the complicated calculations.

The expected result is not obtained even after the multiplication of the matrices (2.3):

$$\begin{gathered} E_k E_{k-1} \dots E_1 A = I, \\ E_k E_{k-1} \dots E_1 = A^{-1}, \end{gathered} \tag{2.3}$$

where $E_1, \dots, E_k$ are the elementary matrices, which are used to bring matrix A to $k \times k$ unit matrix *I*.

In order to calculate the elements $x_1, \dots, x_n$ of the i-th column of A^{-1} matrix according to the equation $AA^{-1} = I$ the solution of the following equation system can be also used:

$$a_{k1}x_1 + a_{k2}x_2 + \dots + a_{kn}x_n = \begin{cases} 0, & k \neq i; \\ 1 & k = i \end{cases} \tag{2.4}$$

where $k = 1, \dots, n$ and similarly to the above $|\mathrm{A}| \neq 0$.

It is known that in algebra A_n of polynomials over *GF(q)* field modulo *f(x)* certain set of basic $(k \times n)$-dimensional H and $((n-k) \times n)$-dimensional G matrices can be defined satisfying following condition:

$$GH^T = 0, \tag{2.5}$$

where H^T is the transposed H matrix.

The space of rows of G and H matrices generate ideals. For such matrices corresponding generator polynomials *g(x)* and *h(x)* ($g(x)h(x) = f(x)$) are defined, which form G and H matrices.

Similarly of the above-mentioned n-dimensional quadrate matrices (and their inverse matrices) can be written in the following way:

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \\ 0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ 0 & 0 & a_1 & \dots & a_{n-3} & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_1 & a_2 \\ 0 & 0 & 0 & \dots & 0 & a_1 \end{bmatrix}, \tag{2.6}$$

where the rows of matrix (2.6) contain the components of any $a \in V_n$ vector.

Obtaining an ideal cryptographic system is impossible (generally speaking). In reality the gain in cryptographic strength will result in loosing of speed or spoiling other characterizing values, or other. But simultaneously the difference in cryptographic characteristics is approved because of the dissimilarity of conditions of practical use.

The advantage of matrix methods over the Vigenere method is that the only one breaking of the cipher text does not cause the breaking of the key. This is achieved on the base of speed reduction, which is compensated by higher quality of cryptography strength of system. The constructed method of the synthesis of the direct and inverse matrices is discussed in the following part (it should be mentioned that the set of keys for fixed *n* is of about $(n!)^2$ -th degree).

The Synthesis of Cryptographic Matrixes Based upon theAlgebraic Structures of Coding

The process of constructing discussed matrixes (2.6) can become more purposeful [4,5]. The equivalence of matrix elements was denoted as $a = (a_1, a_2, ..., a_n) \in V_n$ and

$$a(x) = \sum_{i=0}^{n} a_i x^i \in A_n \; .$$

It’s known that in algebra $\mathrm{A}_n \mod f(x)$ for any ideal I there exists unique monic polynomial $g(x)$ of minimum degree such that, the residue class $\{g(x)\}$ belongs to ideal I and, vice versa, each monic polynomial $g(x)$, which divides $f(x)$ generates the ideal I, in which is the monic polynomial with minimum degree in I. Then by shifting the components of $v = (v_0, v_1, \dots, v_{n-1})$ cyclically by i unit is obtained the vector $v^{(i)} \in I$ i.e. the polynomial $g(x^{(i)}) = g(x)x^i \mod(x^n - 1)$ is obtained also by multiplication in the $\mathrm{A}_n \mod(x^n - 1)$.

Suppose that $g(x)h(x) = x^n - 1$ and, $g(x)$ and $h(x)$ generate I and I' ideals and

$$G=\begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & g_0 & \dots & g_r \end{bmatrix},$$

(2.7)

$$H=\begin{bmatrix} h_0^* & h_1^* & \dots & h_k^* & 0 & \dots & 0 & \dots & 0 \\ 0 & h_0^* & \dots & h_{k-1}^* & h_k^* & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & h_0^* & \dots & h_k^* \end{bmatrix}.$$

Than for any polynomials $g(x^{(i)})$ and $h(x^{(i)})$ the following equation is correct:

$$g(x^{(i)})h(x^{(i)})\equiv 0 \bmod (x^n-1), \qquad (2.8)$$

where $i,j\in\{1,...,n\}$. Considering that for any element $g\in I$ the multiplications of vectors and polynomials on the field *GF*(2) don't coincide,

$$gH^{*T}=0, \qquad (2.9)$$

where the matrix H^* is produced by vector h^*, which consists from the components of vector h, written in reverse order.

Lets discuss quadratic matrices of n-th order corresponding to (2.6) matrix, which are produced by $g(x)$ and $h(x)$ polynomials:

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

(2.10)

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

where j -th column of matrix A_2 represents the vector $h'(j)$ in algebra of polynomials modulo x^n-1, *i*-th components of which are the components of vector $h^*(x)x^{r+j-1}$, if $i\le j$ and $h_i^{'}=0$ if *i*>*j*.

The following theorem is correct:

<u>Theorem 1.</u> Suppose $g(x)$ and $h(x)$ polynomials in algebra A_n modulo x^n -1 over the field *GF*(2). Degrees of $g(x)$ and $h(x)$ are, correspondingly, *r* and *k*; $g(x)h(x)=x^n-1$. Let matrices A_1 and A_2 be generated by $g(x)$ and $h(x)$ polynomials , then A_1 and A_2 are mutually inverse:

$$A_1A_2=I\,,\ A_2A_1=I\,,$$

where I is the identity matrix.

Note, that methods of constructing $g(x)$ and $h(x)$ polynomials in an algebra A_n are known, and they enable constructive fulfillment of result derived from the theorem 1 [4].

Particularly if $g(x)=1+x+x^3$, $h(x)=1+x+x^2+x^4$ are polynomials in the algebra A_7 modulo x^7-1 over $GF(2)$, $g(x)h(x)=x^7-1$, then $g(x)$ and $h(x)$ generate the initial matrices A_1 and A_2 correspondingly (2.10):

$$A_1=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\\0&0&0&0&0&0&1\end{bmatrix},\ A_2=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&0&0&1&1&1&0\\0&0&0&0&1&1&1\\0&0&0&0&0&1&1\\0&0&0&0&0&0&1\end{bmatrix}.$$

The Realization of the Process of Encryption and Decryption

The transmitter X and receiver Y using open or secret channels choose matrix keys A_1 and A_2 . The equation (2.10) settles the initial states of matrixes (for known polynomials $g(x)$ and $h(x)$). The processes of key choosing represents the permutation of columns and rows of matrixes A_1 and A_2 known only to X and Y. permutation using open key K is performed by Diffie-Hellman Algorithm [6] or other algorithms. Binary number of n_0 dimension (n_0 sequence) key K is divided into blocks of minimal m length m_1,..., m_n, where $2^m-1\geq n$, n is the dimension of matrices A_1 and A_2. For any i-th row in the matrix A_1 it is possible to choose $k_{(i)}\ (i=1,...,n)$ position using the decimal number of any m_i block (here and afterwards permutation of columns is implied for the matrix A_2 and vice versa).

Using the binary number of the first $m_1(i=1)$ block, position of the first row $k_1=m_1(\mathrm{mod}\,n)+1$ is determined. If $m_2(\mathrm{mod}\,n)\neq k_1-1$, then $k_2=m_2(\mathrm{mod}\,n)+1$ determines the position of second row, and if $m_2(mod\,n)=k_2-1$, then the position of the second row is determined by value $k_2=(m_2+1)\,\mathrm{mod}\,n+1$, etc. For any $i>1$ row $k_i=(m_i+j)mod\,n+1\ (j\in\{0,1,\ldots,n-1\})$ is determined so that the following condition is fulfilled:

$$k_i\notin\{k_1,\cdots,k_{i-1}\}, \tag{2.11}$$

$i=1,\ldots,n$; $k_1\neq\cdots\neq k_n$.

For defense from plaintext attacks addition (XOR) of the given initial $M^{(i)}$–th informational block with n dimensional $K^{(i)}$ block of K key is performed step by step before the encryption:

$$\mathbf{M}^{(\mathbf{i})'}=\mathbf{M}^{(\mathbf{i})}+\mathbf{K}^{(\mathbf{i})}. \tag{2.12}$$

The process of encryption-decryption is realized by the following view:

$$M^{(i)}\Rightarrow M^{(i)'}\Rightarrow M^{(i)'}A_1=C^{(i)}\Rightarrow C^{(i)}A_2=M^{(i)'}\Rightarrow M^{(i)'}+K^{(i)}=M^{(i)}, \tag{2.13}$$

where $K^{(i)}$ is the secret and is known only to X and Y.

One-way Hash Function and Digital Signature

Digital signature is based on existence of sequence of natural numbers k_i (i=1,...,n), known to transmitter X and receiver Y. The synthesis is stipulated by the secret key K. The common block length of the binary sequence corresponding to the k_i numbers is $n' = C_{n+1}^{2}$.

The hash function h=$H(M)$ is the execution of the following process. The n`-dimensional information $M = (M_1, \ldots M_{n'})$ is divided into n binary blocks $M^{(k_i)} = (M_1, \ldots M_{k_i})$. Each $M^{(k_i)}$block represent to the vectors over the field GF(2) with dimensions corresponding to above mentioned (2.11) integer numbers. If the *Heming* weight $w(M^{(k_i)})$of $M^{(k_i)}$ vector is odd, then $h_i = H(M^{(k_i)})$=1, if even – $h_i = 0$. Totally n-dimensional vector $h = (h_1, \ldots, h_n)$ is obtained for the n`-dimensional information.

Thus hash function h=$H(M)$ is defined in the following way. $M = (M_1, \ldots M_{n'}) \in V_{n'}$ is the informational vector and $h = (h_1, \ldots, h_n) \in V_n$ is vector obtained through hashing:

$$\begin{gathered} M_1 + \cdots + M_{k_1} = h_1 \\ M_{k_1} + \cdots + M_{k_1+k_2} = h_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ M_{n'-k_{n-1}} + \cdots + M_{n'} = h_n \end{gathered} , \qquad (2.14)$$

where the operation of addition is defined over the field GF(2).

X transfers to Y the following concatenation:

$$|M||h|,$$

where h is the signature.

The receiver Y verifies the correctness of the signature using the secret key K and the discussed open algorythm.

The discussed methodology is different from the known one [7]. This is the case when Y uses secret parameters along with the open algorythm for verification of the signature.

It should be also mentoined that secret values are the constituent parameters of the cryptographic system.

References

1. Mac Williams F.J.Sloane N.J.A. The theory of error-correcting codes. North-Holland publishing company, Amsterdam, New York, Oxford, 1977.
2. Schneier B. Applied cryptography, John Wiley and Sons, Inc. New York, 1996.
3. Gantmakher F.R. Theory of Matrices (Russian). Moscow: Nauka, 1967.
4. Peterson W.W. and Weldon E.J. Error-correcting codes. The Mit Press Cambridge, Massachusetts and London, 1972.
5. Megrelishvili R., Bulavrishvili D.,Gnolidze T. etc. Synthesis of a symmetrical cryptographic method with matrices difined over the finite field (Russian). Procsedings of Javakhishvili Tbilisi State University: Applied Mathematics, Computer Sciences, v.342(20), p.83-90, 2000.
6. Diffie W. and Hellman M.E. New Direction in Cryptography. IEEE Trans. on Inf. Theory, v. IT-22, n.6., Nov., pp. 644-654, 1976.
7. ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, v. IT-31, n. 4., pp. 469-472, 1985.