Encryption with First Order Splines

Alla LEVINA, Yuri DEMJANOVICH

***Abstract*—The aim of this paper is to construct new cryptography algorithm. Proposed algorithm bases on wavelet decompositions for the spaces of first order splines. The algorithm is simple in practice and analysis; processes of enciphering and deciphering have explicit mathematical structures.**

***Keywords*—First order splines, mesh, formulas of decomposition and reconstruction from wavelet theory.**

I. Introduction

Well-known piecewise linear continuous functions (first order splines) had been used in mathematics since Euler. Spline theory had been developed in the middle of the XXth century. The term *spline* were introduced in mathematics by Isaac Schoenberg (1946). Splines were the tool of theoretical investigations till 1960. Since 1960 splines had become also the tool for computer simulations of different situations in science, engineering and techniques.

Proposed paper discusses an application of splines to construction of cryptography algorithms. Using of splines and their wavelet decompositions lead to rather wide variety of the keys defined by mesh, order of ejection of nodes and number of rounds. The offered algorithms can be also applied to the key transfer. At present research on using wavelet decomposition of splines of second, third and upper order continues, algorithm based on wavelet decomposition of splines of second degree is presented in work [1, 2].

The paper is organized as follows, in section II basic concepts of algorithm are presented, sections III and IV presents processes of enciphering and deciphering, and section V demonstrates the work of the discussed algorithm in the case of the block size equal to 256 bits.

II. Basic concepts

Presented algorithm is relative to class of block ciphers, process of enciphering and deciphering consists of K identical rounds.

We discuss mesh X as the ordered set of real numbers x_j, such that $x_j < x_{j+1}$: $X = \{x_j\}_{j\in \mathtt{Z}}$.

Let $\mathtt{K} = (X, \gamma, K)$ be *a key*; here X is a mesh, γ is an order of ejection of nodes from the mesh and K is number of round.

Let us suppose that the mesh is periodic with the period N so $x_j = x_{j+N}\ \forall j \in \mathtt{Z}$.

The order of nodes that will be removed from the mesh X is $\gamma = \{\gamma_n\}_{n\in[1,\dots,K]}$, where K is the number of round of enciphering; on each round only one node is removed from the mesh and γ_n is the number of casually chosen node x_j.

St. Petersburg State University, Math and Mechanics department, Russia.
Email: alla_levina239@yahoo.com

Let us suppose that a sequence $C = \{c_i\}_{i\in\ Z}$, $|c_i| = M$ is a plaintext; here $|c_i|-$quantity of elements which are ciphered, C is the ordered set.

On each round one node with the number γ_j is taken out from the mesh, where j is number of the round. Process of enciphering based on formulas of decomposition from wavelet theory; as a result we get sequence $\{c_i^{-j}\}_{i\in J}$, and after K rounds we obtain the ciphertext. On deciphering the plaintext restores with the help of formulas of reconstruction from wavelet theory.

III. Process of enciphering

Let us describe in more details process of enciphering. In the process of encryption K rounds are made. On first round we get plaintext $\{c_i\}_{i=0,\dots,M}$, and also we know key $\mathtt{K}$.

For the convenience of record of formulas we shall consider nonnegative integers i, j.

The first round:

1) Let eject node x_{γ_1} from primary mesh X.
2) Received mesh defines as X^{-1}, its nodes will be equal:

$$x_j^{-1} = x_j \quad \text{if} \quad j < \gamma_1 \tag{1}$$

$$x_j^{-1} = x_{j+1} \quad \text{if} \quad j > \gamma_1 \Rightarrow \tag{2}$$

$X^{-1} = \{x_j^{-1}\}$. The node x_{γ_1} will be defined as ξ.

3) Let us write down and count formulas of decomposition for splines of first degree:

$$c_i^{-1} = c_i \quad \text{if} \quad 0 \le i < \gamma_1 \tag{3}$$

$$c_i^{-1} = c_{i+1} \quad \text{if} \quad \gamma_1 \le i \le M-1 \tag{4}$$

$$b^{-1} = c_{\gamma_1} - (x_{\gamma_1+1}^{-1} - x_{\gamma_1}^{-1})(x_{\gamma_1+1}^{-1} - \xi)^{-1} c_{\gamma_1-1} - \\ -(x_{\gamma_1}^{-1} - \xi)(x_{\gamma_1+1}^{-1} - \xi)^{-1} c_{\gamma_1+1} \tag{5}$$

4) At the end we make a shift of sequence c_i^{-1} as follows:

$$c_0^{-1} \to c_1^{-1} \to c_2^{-1} \dots \to c_{M-1}^{-1} \to c_0^{-1}$$

Formulas (3)-(6) are written down using the notation of a new mesh X^{-1}. On first round sequences $\{c_i^{-1}\}_{i=0,\dots M-1}$ and b^{-1} have been got.

All rounds except K-th round go by analogy with the first, we take out from the mesh X^{-i} node x with number γ_i and count formulas of decomposition for splines of the first degree.

K-th round:

1) By analogy with previous rounds we have:

$$c_i^{-K} = c_i^{-K+1} \quad \text{if} \quad 0 \le i < \gamma_K \tag{6}$$

$$c_i^{-K} = c_{i+1}^{-K+1} \quad \text{if} \quad \gamma_K \le i \le M-K \tag{7}$$

$$b^{-K} = c_{\gamma_K}^{-K+1} - (x_{\gamma_K+1}^{-K} - x_{\gamma_K}^{-K})(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K-1}^{-K} - \\ -(x_{\gamma_K}^{-K} - \xi)(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K+1}^{-K} \quad (8)$$

On $K-$th round shift is not made. Sequence $\{c_i^{-K}\}_{i=0,\dots M-K}$ and b^{-K} have been received.

As a result after K rounds we have got two sequences

$$\{b^{-n}\}_{n=1,2,\dots,K}, \quad \{c_i^{-K}\}_{i=0,1,2,\dots,M-K}.$$

Sequence $\{c_i^{-K}, b^{-n}\}_{n=1,2,\dots,K;i=0,1,2,\dots,M-K}$ *is the ciphertext.*

IV. Process of deciphering

Process of decryption goes by analogy with process of encryption, the same key K and formulas of reconstruction are used.

We know number of rounds K so the sequence $\{c_i^{-K}, b^{-n}\}_{n=1,2,\dots,K;i=0,1,2,\dots,M-K}$ can be divided in two sequences:

$$\{b^{-n}\}_{n=1,2,\dots,K}, \quad \{c_i^{-K}\}_{i=0,1,2,\dots,M-K}.$$

We know the primary mesh X and the order of nodes removal γ so we can receive meshes $X^{-1}, \dots, X^{-K+1}, X^{-K}$, as it has been described in process of enciphering.

On each round we are taking out from the mesh X^{-i+1} only one node x with the number γ_i, where i is the number of round, and we are receiving mesh X^{-i}. For deciphering we need the reverse order, i.e. on first round we need the mesh X^{-K}, on second X^{-K+1} and on $K-$th $-X^{-1}$.

The first round:

1) We take the mesh X^{-K}, $\xi = x_{\gamma_k}^{-K}$
2) We write down and count formulas of reconstruction for the splines of first degree:

$$c_i^{-K+1} = c_i^{-K} \quad \text{if} \quad 0 \le i < \gamma_K \quad (9)$$

$$c_i^{-K+1} = c_{i-1}^{-K} \quad \text{if} \quad \gamma_K + 1 \le i \le M - K + 1 \quad (10)$$

$$c_{\gamma_k}^{-K+1} = (x_{\gamma_K+1}^{-K} - x_{\gamma_K}^{-K})(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K-1}^{-K} + \\ +(x_{\gamma_K}^{-K} - \xi)(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K}^{-K} + b^{-K} \quad (11)$$

3) We make a shift c_i^{-K+1} as follows:

$$c_0^{-K+1} \leftarrow c_1^{-K+1} \leftarrow c_2^{-K+1} \dots \leftarrow c_{M-K+1}^{-K+1} \leftarrow c_0^{-K+1}$$

We have got the sequence $\{c_i^{-K+1}\}_{i=0,\dots,M-K+1}$.

K-th round:

1) We take the mesh X^{-1}, $\xi = x_{\gamma_1}$
2)

$$c_i = c_i^{-1} \qquad 0 \le i < \gamma_1 \quad (12)$$

$$c_i = c_{i-1}^{-1} \qquad \gamma_1 + 1 \le i \le M \quad (13)$$

$$c_{\gamma_1} = (x_{\gamma_1+1}^{-1} - x_{\gamma_1}^{-1})(x_{\gamma_1+1}^{-1} - \xi)^{-1} c_{\gamma_1-1}^{-1} + \\ +(x_{\gamma_1}^{-1} - \xi)(x_{\gamma_1+1}^{-1} - \xi)^{-1} c_{\gamma_1}^{-1} + b^{-1} \quad (14)$$

Shift is not made on $K-$th round.

Thus, after K *rounds the initial text* $\{c_i\}_{i=0,\dots,M}$ *has been restored.*

V. Demonstration of the work of algorithm

Presented algorithm is a parametrized algorithm in that it can operate on block sizes of 128, 192, 256 or 512 bits. Now will be presented the work of the algorithm with the block size of 256 bits.

If block size equal to 32 bytes then 30 rounds are specified and we will have 33 nodes in the mesh.

A plaintext is a sequence $\{c_0, c_1, \dots, c_{31}\}$, and key is $\mathrm{K} = \{X, \gamma, K\}$, where $K = 30$, $X = \{x_0, x_1, \dots, x_{32}\}$, $\gamma = \{\gamma_n\}_{n=0,\dots 32}$.

Elements of plaintext held in the matrix C.

Number of columns — N, $N = M/4$, and 4 rows. For block equal 32 bytes C will be 4x8 matrix.

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ c_{16} & c_{17} & c_{18} & c_{19} & c_{20} & c_{21} & c_{22} & c_{23} \\ c_{24} & c_{25} & c_{26} & c_{27} & c_{28} & c_{29} & c_{30} & c_{31} \end{pmatrix}.$$

Nodes of primary mesh held in matrix X: $X = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \dots \\ x_{32} \end{pmatrix}$.

$c_0, c_1, \dots, c_{31}, x_0, \dots, x_{32}$ - bytes.

- *Process of the encrypting.*
  Process of encrypting consists of four operation:
  - Getting of mesh, which will be using on this round.
  - Getting of new elements.
  - Shift of the elements.
  - Creating of matrix B.

  On each round number of elements in matrix C will be decrease on one element, for staying matrix C four-by-eight matrix, we will add 0 on each round, as it will be presented below.
  Also on each round we will get element b^{-i}, and we will put it in the matrix B, matrix B is also four-by-eight matrix.
  In the beginning

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

  Elements $\{b^{-n}\}_{n=1\dots K}$ we will put in the matrix B from the position $\{M-K \text{ div N}, M-K \text{ mod N}\}$, numeration of rows and columns in B starts from {0,0}.
  On first round we get matrix C, mesh X, and number of node γ_1.

Process of enciphering on $i-$*th round:*

1) We get mesh X^{-i}:

$$X^{-i} = \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ ... & ... & ... & ... & ... \\ ... & ... & 0 & ... & ... \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 0 & 0 \\ 0 & 0 & ... & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0^{-i+1} \\ x_1^{-i+1} \\ ... \\ x_{\gamma_i}^{-i+1} \\ ... \\ ... \\ x_{L-i}^{-i+1} \end{pmatrix} =$$

$$= \begin{pmatrix} x_0^{-i} \\ x_1^{-i} \\ ... \\ x_{L-i-1}^{-i} \end{pmatrix}.$$

2) We get matrix C^{-i} : $C^{-i} =$

$$= \begin{pmatrix} c_0^{-i+1} & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & c_{\gamma_i-1}^{-i+1} & c_{\gamma_i+1}^{-i+1} & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & c_{M-i+1}^{-i+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

3) Shift of the elements:

$$\begin{pmatrix} c_0^{-i+1} & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & c_{\gamma_i-1}^{-i+1} & c_{\gamma_i+1}^{-i+1} & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & c_{M-i+1}^{-i+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rightarrow$$

$$\begin{pmatrix} c_{M-i+1}^{-i+1} & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & c_{\gamma_i-1}^{-i+1} & c_{\gamma_i+1}^{-i+1} & ... & ... & ... \\ ... & ... & ... & ... & ... & c_0^{-i+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Let us write matrix C^{-i} in new designations:

$$C^{-i} = \begin{pmatrix} c_0^{-i} & c_1^{-i} & c_2^{-i} & c_3^{-i} & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & c_{M-i}^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

4) We count and put down in the matrix B element b^{-i} :

$$b^{-i} = \left(1, -\frac{(x_{\gamma_i+1}^{-i} - x_{\gamma_i}^{-i})}{(x_{\gamma_i+1}^{-i} - \xi)}, -\frac{(x_{\gamma_i}^{-i} - \xi)}{(x_{\gamma_i+1}^{-i} - \xi)} \right) \cdot \begin{pmatrix} c_{\gamma_i}^{-i+1} \\ c_{\gamma_i-1}^{-i+1} \\ c_{\gamma_i+1}^{-i+1} \end{pmatrix},$$

$$\xi = x_{\gamma_i}^{-i+1}$$

$$B = \begin{pmatrix} 0 & 0 & b^{-1} & b^{-2} & b^{-3} & ... & ... & ... \\ b^{-7} & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & b^{-i} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

$K-th$ round:

1) We get mesh X^{-K}:

$$X^{-K} = \begin{pmatrix} 1 & 0 & ... & 0 \\ ... & ... & ... & ... \\ ... & ... & ... & ... \\ 0 & ... & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0^{-K+1} \\ x_1^{-K+1} \\ x_2^{-K+1} \\ x_3^{-K+1} \end{pmatrix} =$$

$$= \begin{pmatrix} x_0^{-K} \\ x_1^{-K} \\ x_2^{-k} \end{pmatrix}.$$

2) We calculate C^{-K} :

$$C^{-K} = \begin{pmatrix} c_0^{-K} & c_2^{-K+1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

In new designations:

$$C^{-K} = \begin{pmatrix} c_0^{-K} & c_1^{-K} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

3) Shift is not made.

4) We calculate and put in the matrix B element b^{-K}

$$b^{-K} = \left(1, -\frac{(x_{\gamma_K+1}^{-K} - x_{\gamma_K}^{-K})}{(x_{\gamma_K+1}^{-K} - \xi)}, -\frac{(x_{\gamma_K}^{-K} - \xi)}{(x_{\gamma_K+1}^{-K} - \xi)} \right) \cdot \begin{pmatrix} c_{\gamma_K}^{-K+1} \\ c_{\gamma_K-1}^{-K+1} \\ c_{\gamma_K+1}^{-K+1} \end{pmatrix}$$

$$\xi = x_{\gamma_K}^{-K+1}$$

$$B = \begin{pmatrix} 0 & 0 & b^{-1} & b^{-2} & b^{-3} & ... & ... & ... \\ b^{-7} & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & b^{-K} \end{pmatrix}.$$

Ciphertext is $\mathtt{C} = C^{-K} + B$:

$$\mathtt{C} = \begin{pmatrix} c_0^{-K} & c_1^{-K} & b^{-1} & b^{-2} & b^{-3} & b^{-4} & b^{-5} & b^{-6} \\ b^{-7} & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & b^{-K} \end{pmatrix}.$$

- *Process of the decripting.*

We have the matrix C and the key $\mathtt{K} \Rightarrow$ so we know the number of rounds $K \Rightarrow$ we know block length $M = K + 2$.

If we know the block length we can get from the matrix C matrix C^{-K} and B :

$$B = \begin{pmatrix} 0 & 0 & b^{-1} & b^{-2} & b^{-3} & b^{-4} & b^{-5} & b^{-6} \\ b^{-7} & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & b^{-K} \end{pmatrix},$$

$$C^{-K} = \begin{pmatrix} c_0^{-K} & c_1^{-K} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We know the primary mesh X, so we can count $X^{-1}, ...X^{-i}, ...X^{-K}$, and put it in the matrix X^{all},

matrix X^{all} is $L-1$-by-K, in this case 32-by-30

$$X^{all} = \begin{pmatrix} x_0^{-1} & \dots & x_0^{-i} & \dots & x_0^{-K} \\ x_1^{-1} & \dots & x_1^{-i} & \dots & x_1^{-K} \\ x_2^{-1} & \dots & x_2^{-i} & \dots & x_2^{-K} \\ \dots & \dots & \dots & x_3^{-i} & 0 \\ \dots & \dots & \dots & \dots & 0 \\ x_{31}^{-1} & \dots & \dots & \dots & 0 \end{pmatrix}.$$

Process of dechiphering consists of two operations:

- Counting of elements.
- Shift of the elements.

Process of deciphering on i-th round:

1) We take $L-i$ elements of $i-$th column of the matrix $X^{all} \Rightarrow$

$$X^{-i} = \begin{pmatrix} x_0^{-i} \\ x_1^{-i} \\ x_2^{-i} \\ \dots \\ x_{L-i}^{-i} \end{pmatrix}.$$

Count:

$$c_{\gamma_i}^{-i+1} = \begin{pmatrix} \frac{(x_{\gamma_i+1}^{-i} - x_{\gamma_i}^{-i})}{(x_{\gamma_i+1}^{-i} - \xi)}, \frac{(x_{\gamma_i}^{-i} - \xi)}{(x_{\gamma_i+1}^{-i} - \xi)}, b^{-i} \end{pmatrix} \cdot \begin{pmatrix} c_{\gamma_i-1}^{-i} \\ c_{\gamma_i}^{-i} \\ 1 \end{pmatrix}$$

$\xi = x_{\gamma_i}^{-i+1}$

Let us write C^{-i+1} : $C^{-i+1} =$

$$\begin{pmatrix} c_0^{-i} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & c_{\gamma_i-1}^{-i} & c_{\gamma_i}^{-i+1} & c_{\gamma_i}^{-i} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & c_{M-i}^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2) Let make a shift of C^{-i+1}:

$$\begin{pmatrix} c_0^{-i} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & c_{\gamma_i-1}^{-i} & c_{\gamma_i}^{-i+1} & c_{\gamma_i}^{-i} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & c_{M-i}^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rightarrow$$

$$\begin{pmatrix} c_1^{-i} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{\gamma_i-1}^{-i} & c_{\gamma_i}^{-i+1} & c_{\gamma_i}^{-i} & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & c_{M-i}^{-i} & c_0^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let us write it in new designations:

$$C^{-i+1} = \begin{pmatrix} c_0^{-i+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_8^{-i+1} \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & c_{M-i+1}^{-i+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

$k-$th round:

1) From the matrix X^{all} we are taking 1-th row $\Rightarrow$

$$X^{-1} = \begin{pmatrix} x_0^{-1} \\ x_1^{-1} \\ x_2^{-1} \\ \dots \\ x_{31}^{-1} \end{pmatrix}.$$

Count:

$$c_{\gamma_1} = \begin{pmatrix} \frac{(x_{\gamma_1+1}^{-1} - x_{\gamma_1}^{-1})}{(x_{\gamma_1+1}^{-1} - \xi)}, \frac{(x_{\gamma_1}^{-1} - \xi)}{(x_{\gamma_1+1}^{-1} - \xi)}, b^{-1} \end{pmatrix} \cdot \begin{pmatrix} c_{\gamma_1-1}^{-1} \\ c_{\gamma_1}^{-1} \\ 1 \end{pmatrix}$$

where $\xi = x_{\gamma_1}$

Let us write matrix C :

$$C = \begin{pmatrix} c_0^{-1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & c_{\gamma_1-1}^{-1} & c_{\gamma_1} & c_{\gamma_1}^{-1} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & c_{30}^{-1} \end{pmatrix},$$

Let us write elements of matrix C in new designations:

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ c_{16} & c_{17} & c_{18} & c_{19} & c_{20} & c_{21} & c_{22} & c_{23} \\ c_{24} & c_{25} & c_{26} & c_{27} & c_{28} & c_{29} & c_{30} & c_{31} \end{pmatrix}.$$

2) Shift is not made on last round.

The plaintext has been restored.

VI. Conclusion

The offered algorithm is well protected against attacks, process of enciphering and deciphering flows quickly. Also one of the advantages of the given algorithm is that it can be used both as block and as a stream algorithm. In the future it is planned to analyze the application of this cryptoalgorithm in different areas.

Acknowledgment

This work was supported (partly) with RFFI grants 07-01-00269 and 07-01-00451.

References

[1] Demjanovish Y. K., Levina A. B. *On wavelet decomposition of linear spaces over arbitary field and some applications* Mathematical modeling 2008 T. 20 (on russian)

[2] Demjanovish Y. K., Levina A. B. *Wavelet decomposition and decoding* St. Petersburg, Methods of calculations 22. Spb: St. Petersburg University, 2008. p. 56-64 (on russian)

[3] Demjanovish Y. K., *Minmal splines and splaches* Vestnic of StPetersburg University . Number 1. 2008, 2 p. 8-22 (on russian)

[4] Demjanovish Y. K., Makarov A. A. *Kalibrovochnye parities for nonpolinomial splines* St.Petersburg, problems of mathematical analyze 34, 2006 p. 29-54 (on russian)

[5] Demjanovish Y. K., *Splaches and minimal splines* St. Petersburg, 2003. p. 200. (on russian)