Cryptoalgorithm Based on Formulas of Reconstruction and Decomposition on the Non-uniform Grid

Alla Levina *

Abstract—**The cryptography is nowadays applied to almost all information systems - from Internet up to databases. Swindle attempts are made and legality of financial transactions is provided by means of cryptographic algorithms. This paper is devoted to an algorithm based on the wavelet decomposition of B-splines of the second degree on a non-uniform grid.**

Keywords: B-splines, non-uniform grid, formulas of decomposition and reconstruction

1 Introduction

In this paper the new cryptoalgorithm based on wavelets decomposition of B-splines of the second degree on a non-uniform grid is presented. The algorithm is simple in practical application and analysis, processes of enciphering and decoding have easy mathematical structures that help in analysis of stability of the algorithm and its application.

Section 2 describes the main concepts of presented algorithm. Sections 3 and 4 describe processes of coding and decoding. Section 5 gives an example which illustrates the work of algorithm. An overview of functions of this algorithm is presented in section 6.

2 The basic concepts

Suppose X is a non-uniform grid, γ is the order of ejection of units from this grid, and K is quantity of rounds.

Let $\mathtt{K} = (X, \gamma, K)$ be a key.

We discuss the grid X as the ordered set of units x_j,

$$X = \{x_j\}_{j \in Z};$$

suppose the grid is periodic with the period N so the $x_j = x_{j+N}$ for $\forall i \in Z$.

Order of ejection of units is $\gamma = \{\gamma_n\}_{n \in [1,\dots K]}$ where K is the number of rounds of enciphering, γ_n is the number of casually chosen unit x_j.

Suppose a sequence $C = \{c_i\}_{i \in Z}$, $|c_i| = M$ is an open text; here $|c_i|-$quantity of elements which are ciphered, C is the ordered set.

3 Process of enciphering

Process of enciphering consists of K rounds, on the first round we deal with sequence $\{c_i\}$. The first round of enciphering is made by means of a key K and formulas of decomposition.

For the convenience of record of formulas we shall consider i and $j \in N_0$.

Let's describe in more detail the process of enciphering.

The first round:

1. Let's throw unit x_{γ_1} from primary grid X
2. The received grid is defined as X^{-1} its units 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 thrown out unit x_{γ_1} will be defined as ξ.
3. Let's write down and count formulas of decomposition for $B-$splines of the second degree:
$$c_0^{-1} = c_0 \tag{3}$$
$$c_1^{-1} = -(x_3^{-1} - \xi)(\xi - x_1^{-1})^{-1} c_0 + \\ +(x_3^{-1} - x_1^{-1})(\xi - x_1^{-1})^{-1} c_1 \tag{4}$$
$$c_i^{-1} = c_{i+1} \quad \text{if} \quad 2 \le i \le M-1 \tag{5}$$
$$b^{-1} = \Big[(x_4^{-1} - \xi)(x_3^{-1} - \xi)c_0 - (x_4^{-1} - \xi)(x_3^{-1} - x_1^{-1})c_1 + \\ +(x_4^{-1} - x_2^{-1})(\xi - x_1^{-1})c_2 - (\xi - x_2^{-1})(\xi - x_1^{-1})c_3\Big] \cdot \\ \cdot (x_4^{-1} - x_2^{-1})^{-1}(\xi - x_1^{-1})^{-1} \tag{6}$$

*The work is supported (partly) with RFFI grants 07-01-00269 and 07-01-00451. St. Petersburg State University, Math and Mechanics department, Tell 812-750-1123 Email: alla_levina239@yahoo.com

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

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

Formulas (3)-(6) are written down in designations of a new grid X^{-1}. On the first round the sequences $\{c_i^{-1}\}$ and b^{-1} have been received.

The second round:

On the second round we deal with sequence $\{c_j^{-1}\}$, grid X^{-1} and number of unit γ_2.

1. We take out unit $x_{\gamma_2}^{-1}$ from a grid X^{-1}
2. We receive grid X^{-2} with units:

$$x_j^{-2} = x_j^{-1} \quad \text{if} \quad j < \gamma_2$$

$$x_j^{-2} = x_{j-1}^{-1} \quad \text{if} \quad j > \gamma_2 \Rightarrow$$

$$X^{-2} = \{x_j^{-2}\}$$

Taken out unit is $\xi = x_{\gamma_2}^{-1}$.

3. Formulas (3) - (6) in new designations are:

$$c_0^{-2} = c_0^{-1} \tag{7}$$

$$c_1^{-2} = -(x_3^{-2} - \xi)(\xi - x_1^{-2})^{-1} c_0^{-1} + \\ +(x_3^{-2} - x_1^{-2})(\xi - x_1^{-2})^{-1} c_1^{-1} \tag{8}$$

$$c_i^{-2} = c_{i+1}^{-1} \quad \text{if} \quad 2 \le i \le M-2 \tag{9}$$

$$b^{-2} = \Big[(x_4^{-2}-\xi)(x_3^{-2}-\xi)c_0^{-1} - (x_4^{-2}-\xi)(x_3^{-2}-x_1^{-2})c_1^{-1} \\ +(x_4^{-2} - x_2^{-2})(\xi - x_1^{-2})c_2^{-1} - (\xi - x_2^{-2})(\xi - x_1^{-2})c_3^{-1}\Big] \cdot \\ \cdot (x_4^{-2} - x_2^{-2})^{-1}(\xi - x_1^{-2})^{-1} \tag{10}$$

4. Shift of c_i^{-2} following:

$$c_0^{-2} \to c_1^{-2} \to c_2^{-2} ... \to c_{M-1}^{-2} \to c_0^{-2}$$

The sequences $\{c_i^{-2}\}$ and b^{-2} have been received.

K-th round:

1. By analogy with the previous rounds we have:

$$c_0^{-K} = c_0^{-K+1} \tag{11}$$

$$c_1^{-K} = -(x_3^{-K+1} - \xi)(\xi - x_1^{-K+1})^{-1} c_0^{-K+1} + \\ +(x_3^{-K+1} - x_1^{-K+1})(\xi - x_1^{-K+1})^{-1} c_1^{-K+1} \tag{12}$$

$$c_i^{-K} = c_{i+1}^{-K+1} \quad \text{if} \quad 2 \le i \le M-K \tag{13}$$

$$b^{-K} = \Big[(x_4^{-K+1}-\xi)(x_3^{-K+1}-\xi)c_0^{-K+1} - (x_4^{-K+1}-\xi) \cdot \\ \cdot (x_3^{-K+1} - x_1^{-K+1})c_1^{-K+1} + \\ +(x_4^{-K+1} - x_2^{-K+1})(\xi - x_1^{-K+1})c_2^{-K+1} - \\ -(\xi - x_2^{-K+1})(\xi - x_1^{-K+1})c_3^{-K+1}\Big] \cdot \\ \cdot (x_4^{-K+1} - x_2^{-K+1})^{-1}(\xi - x_1^{-K+1})^{-1} \tag{14}$$

On $K-$th round shift is not made.

Sequences $\{c_i^{-K}\}$ and b^{-K} have been received.

As a result after K rounds we received two sequences

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

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

Remarks:

(A) For calculation of formulas of decomposition the quantity of units in a grid should be ≥ 3

(B) Denominators in formulas calculating values $\{c_i^{-1}\}, ...\{c_i^{-K}\}$ *and* b^{-1},... b^{-K} *should not be equaled to zero.*

4 Process of decoding

Process of decoding goes by analogy to process of enciphering the same key K and formulas of reconstruction are used.

We know number of rounds K the sequence $\{c_i^{-K}, b^{-n}\}_{n=1,2,...K;i=0,1,2,...,N-K}$ is divided in two sequences.

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

We know the primary grid X and the order of ejection of units γ so we can receive grids $X^{-1}, ..., X^{-K+1}, X^{-K}$. For decoding we need the return order, i.e. on the first round we need the grid X^{-K} on the second X^{-K+1} and on $K-$th —X^{-1} to the avoid repeating this calculation K times it's calculated once and entered in the table:

Round	Grid
1	X^{-K}
2	X^{-K+1}
...	...
K-1	X^{-2}
K	X^{-1}

The first round:

1. We take out of the table a grid X^{-K}, $\xi = x_{\gamma_k}^{-K}$

2. We write out formulas of reconstruction:

$$c_0^{-K+1} = c_0^{-K} \tag{15}$$

$$c_i^{-K+1} = c_{i-1}^{-K} \quad \text{if} \quad 3 \le i \le N-K+1 \tag{16}$$

$$c_1^{-K+1} = c_0^{-K}(x_3^{-K} - \xi)(x_3^{-K} - x_1^{-K})^{-1} + \\ + c_1^{-K}(\xi - x_1^{-K})(x_3^{-K} - x_1^{-K})^{-1} \tag{17}$$

$$c_2^{-K+1} = c_1^{-K}(x_4^{-K} - \xi)(x_4^{-K} - x_2^{-K})^{-1} + \\ + c_2^{-K}(\xi - x_2^{-K})(x_4^{-K} - x^{-K}{}_2)^{-1} + b^{-K} \tag{18}$$

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

$$c_0^{-K+1} \leftarrow c_1^{-K+1} \leftarrow c_2^{-K+1} ... \leftarrow c_{N-K+1}^{-K+1} \leftarrow c_0^{-K+1}$$

We have received the sequence $\{c_i^{-K+1}\}$.

K-th round:

1. We take a grid X^{-1}, $\xi = x_{\gamma_1}$
2.

$$c_0 = c_0^{-1} \tag{19}$$

$$c_i = c_{i-1}^{-1} \quad \text{if} \quad 3 \le i \le N \tag{20}$$

$$c_{-1} = c_0^{-1}(x_3^{-1} - \xi)(x_3^{-1} - x_1^{-1})^{-1} + \\ + c_1^{-1}(\xi - x_1^{-1})(x_3^{-1} - x_1^{-1})^{-1} \tag{21}$$

$$c_2 = c_1^{-1}(x_4^{-1} - \xi)(x_4^{-1} - x_2^{-1})^{-1} + \\ + c_2^{-1}(\xi - x_2^{-1})(x_4^{-1} - x_2^{-1})^{-1} + b^{-1} \tag{22}$$

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

Thus, after K rounds the initial text $\{c_i\}$ has been restored.

5 Example

We will set an example which will demonstrate work of the presented algorithm.

Let us transfer the message $\{4, 6, 7, 9, 1, 8\}$.

The key $\mathtt{K} = (\{1, 3, 5, 9, 10\}, \{2, 5\})$.

In the given example numbers of rounds are $K = 2$.

1 round:

1. We write out a grid X^{-1} : $X^{-1} = \{1, 3, 9, 10\}$ and $\xi = x_{\gamma_1} = 5$
2. According to the formulas (3) - (6) we receive:

$$c_0^{-1} = c_0 = 4$$

$$c_1^{-1} = -(10-5)(5-3)^{-1}4 + (10-3)(5-3)^{-1}6 = 11$$

$$c_2^{-1} = c_3 = 9$$

$$c_3^{-1} = c_4 = 1$$

$$c_4^{-1} = c_5 = 8$$

$$b^{-1} = [(1-5)(10-5)4 - (1-5)(10-3)6 + (1-9)(5-3)7 - \\ -(5-9)(5-3)9](1-9)^{-1}(5-3)^{-1} = -3$$

3. We make a shift:

$$c_0^{-1} = 8$$

$$c_1^{-1} = 4$$

$$c_2^{-1} = 11$$

$$c_3^{-1} = 9$$

$$c_4^{-1} = 1$$

Sequences $c^{-1} = \{8, 4, 11, 9, 1\}$ and $b^{-1} = -3$ have been received

2 round:

1. We write out a grid X^{-2} : $X^{-2} = \{1, 9, 10\}$ and $\xi = x_{\gamma_2}^{-1} = 3$.
2. According to the formulas (9)-(12) we receive:

$$c_0^{-2} = c_0 = 8$$

$$c_1^{-2} = -(1-3)(3-9)^{-1}8 + (1-9)(3-9)^{-1}4 = \frac{8}{3}$$

$$c_2^{-2} = c_3^{-1} = 9$$

$$c_3^{-2} = c_4^{-1} = 1$$

$$b^{-2} = [(9-3)(1-3)11 - (9-3)(1-9)9 + (9-10)(3-9)1 - \\ -(3-10)(3-9)8](9-10)^{-1}(3-9)^{-1} = -36$$

After two rounds sequences $\{8, \frac{8}{3}, 9, 1\}$ and $\{-3, -36\}$ have been received.

The code is the sequence $\{8, \frac{8}{3}, 9, 1, -3, -36\}$

Let us try to restore the initial information:

1 round:

1. The primary grid is $\{1, 3, 5, 9, 10\}$ the order of ejection of units is $\{2, 5\}$ hence on last step the grid $\{1, 9, 10\}$ has been received and $\xi = 3$. Two rounds were carried out $\Rightarrow \{c_i^{-K}\}_{i=0,...3} = \{8, \frac{8}{3}, 9, 1\}$ and $\{b^{-n}\}_{n=1,2} = \{-3, -36\}$.

2. According to the formulas (17)-(20) we will receive:

$$c_0^{-1} = c_0^{-2} = 8$$
$$c_3^{-1} = c_2^{-2} = 9$$
$$c_4^{-1} = c_3^{-2} = 1$$
$$c_1^{-1} = 8(1-3)(1-9)^{-1} + \frac{8}{3}(3-9)(1-9)^{-1} = 4$$
$$c_2^{-1} = \frac{8}{3}(9-3)(9-10)^{-1} + 9(3-10)(9-10)^{-1} - 36 = 11.$$

3. We make a shift:

$$c_0^{-1} = 4$$
$$c_1^{-1} = 11$$
$$c_2^{-1} = 9$$
$$c_3^{-1} = 1$$
$$c_4^{1} = 8$$

Sequence $c^{-1} = \{4, 11, 9, 1, 8\}$ has been received.

2 round:

1. On this round the grid is: $\{1, 3, 9, 10\}$, $\xi = 5$.
2. $\Rightarrow$

$$c_0 = c_0^{-1} = 4$$
$$c_3 = c_2^{-1} = 9$$
$$c_4 = c_3^{-1} = 1$$
$$c_5 = c_4^{-1} = 8$$
$$c_1 = 4(10-5)(10-3)^{-1} + 11(5-3)(10-3)^{-1} = 6$$
$$c_2 = 11(1-5)(1-9)^{-1} + 9(5-9)(1-9)^{-1} - 3 = 7.$$

Sequence $c = \{4, 6, 7, 9, 1, 8\}$ has been received.

From the example we can see that the transferred message has been completely restored.

6 Use of the algorithm for block and line enciphering

One of the advantages of the given algorithm is that it can be used both as block, and as a line algorithm.

- *Use of algorithm as the block code*

  The given algorithm can be used as block algorithm. The initial text C is divided into ξ blocks of identical length, $\alpha = \{c_l\}_{l \in Z}$. Then primary sequence $C = \bigcup_{k=1}^{\xi} \alpha_k$. Processes of enciphering and deciphering go as described in item 1 and 2.

  Theorem 1: In order to avoid initial message elements not transferred thought formulas type (12) it's necessary to have $M_\xi - 1 \le K \le L - 3$ where L is quantity of units x_j, $L = |x_j|$, K is a number of rounds, M_ξ is a quantity of elements in the block.

  The proof:

  1. Let us prove an inequality $M_\xi - 1 \le K$.

  Consider $k-$th round:

  Let on $k-$th round the sequence $\{c_0^{-k}, c_1^{-k}\}$ has been received, hence before rearrangement $c_0^{-k} = c_1^{-k}$ and was calculated under the formula of type (12), and $c_1^{-k} = c_0^{-k}$.

  Let us lead one more round: $c_0^{-k+1} = c_0^{-k}$, and c_1^{k-1} are calculated under the formula similar (12). Thus it has been received that on $k+1$ round all the received elements have passed transformation of type (12).

  But in order for $k-$th round to remain only two elements it would be necessary that a condition in formulas (13) was not fulfilled, i.e. $2 \ge i \ge M_\xi - K \Rightarrow M_\xi - 2 \le K \Rightarrow$ on $k+1$ round $M_\xi - 2 \le K + 1 \Rightarrow$

$$M_\xi - 1 \le K$$

  2. Let's prove an inequality $K \le L - 3$

  From the remark (A) $\Rightarrow L_{\text{rem}}^K \ge 3$, where L_{rem}^K is the remained quantity of units on $K-$th step. As during one round one unit is thrown out it is possible to write down $L_{\text{rem}}^{K-1} \ge 3 + 1 \Rightarrow$

$$L \ge 3 + K.$$

  end.

- *Use of algorithm as the line code*

  The algorithm cipher strongly increases if at line enciphering conditions of the Theorem 1 and $M \le L-2$ are fulfilled, where M is a quantity of ciphered elements and L is a quantity of units.

7 Conclusion and Future Work

The offered algorithm is well protected against attacks, process of enciphering and decoding flows quickly. In future it's planned to analyze the application of this cryptoalgorithm in different areas.

References

[1] Smart Nigel, *Cryptography: An Introduction*, 2nd Edition, The McGraw-Hill Publication, 2003.

[2] Demjanovich, Y.K., *Splashes and the minimal splines*, St. Petersburg University Publication 2003.