New Approach in Creating of Block Ciphers Based on Wavelet Decomposition of Splines

Alla Levina *

Abstract—**Cryptography is used in all information systems ranging from Internet to databases. This paper devoted to the algorithm based on wavelet decomposition of splines of third order**

Keywords: Block ciphers, splines, algebraic theory of spline-wavelet decompositions

1 Introduction

This paper presents new idea which can be used in different areas of cryptography, the idea is based on wavelet decomposition of splines. The aim of this paper is to present the cryptoalgorithm structure based on the algebraic theory of spline-wavelet decompositions.

The presented algorithm has new structure. The idea of the algorithm based just on the algebraic calculation, with the help of algebraic formulas we can code and decode information. This algorithm do not have XOR operation with the round key and its do not use S-boxes.

Let us give the main idea of usage of spline-wavelet decompositions in cryptography.

In this paper will be used splines of third degree, the same researches were made for the splines of first and second degree.

A sequence of real numbers $\{x_i\}_{i=0,1,\dots,L-1}$ which called grid X is used for constructing of spline space. Another spline space (embedded in last one) is constructed from the new grid which is obtained by deleting one element (number) from grid X.

Wavelet decomposition of mentioned spaces gives decomposition/reconstruction formulas; the last ones are used in analysis/restoring of initial number stream in split between main stream and wavelet stream. These formulas are defined by elements of the grid, and they can be discussed not only in the field of real numbers but (under certain conditions) also in finite fields.

These researches can be implement in different areas of cryptography; in hash functions, key transformation and many others. In this paper will be present one way of implementation of this idea in creating of block ciphers.

In this realization a plain text is regarded as an initial stream, ciphertext consists of main stream and wavelet stream, and a key consists from the grid X.

Section 2 describes the main concepts of mathematical theory, used in the presented algorithm. Sections 3 describes the main concept of presented algorithm. Section 4 describes processes of enciphering and deciphering.

2 Idea of wavelet decomposition of splines

Now will be briefly given a concept of wavelet decomposition of splines. On the set X we build splines. Set X consists from the elements $\{x_i\}_{i=0,\dots,L-1}$, where $\{x_i\}_{i=0,\dots,L-1}$ natural numbers. L is a number of elements in the set X. This set is called grid.

Third order splines are presented in the formulas below:

$$\sum_{j=k-3}^{k} \omega_j(t) = 1, \quad t \in [x_k, x_{k+1})$$

$$\sum_{j=k-3}^{k} \frac{1}{3}\left(x_{j+1}+x_{j+2}+x_{j+3}\right)\omega_j(t) = t, \quad t \in [x_{k+1}, x_{k+2})$$

$$\sum_{j=k-3}^{k} \frac{1}{3}\left(x_{j+1}x_{j+2} + x_{j+1}x_{j+3} + x_{j+2}x_{j+3}\right)\omega_j(t) = t^2,$$

$$t \in [x_{k+2}, x_{k+3})$$

$$\sum_{j=k-3}^{k} x_{j+1}x_{j+2}x_{j+3}\,\omega_j(t) = t^3, \quad t \in [x_{k+3}, x_{k+4}).$$

Splines are defined as $\omega_j(t)$ and x_j elements of our grid X.

For wavelet decomposition of splines we take out one element x_k and we get new grid $\overline{X}$, elements of this grid are equals:

$$\overline{x}_j = x_j \text{ if } j \le k-1, \text{ and } \overline{x}_j = x_{j+1} \text{ if } j \ge k, \quad \xi = x_k.$$

*The Saint Petersburg State University of Information Technologies, Mechanics and Optics, Tell 812-750-1123 Email: alla_levina239@yahoo.com

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

With the use of new grid $\overline{X}$ we can get new splines $\overline{\omega}_j$ but these new splines can be represent as a combination of splines which were build on the grid X :

$$\overline{\omega}_j(t) = \omega_j(t) \quad \forall j \le k-4; \qquad \overline{\omega}_j(t) = \omega_{j+1}(t) \quad \forall j \ge k.$$

$$\overline{\omega}_{k-4}(t) = \omega_{k-4}(t) + \frac{x_{k+1} - \xi}{x_{k+1} - x_{k-3}}\omega_{k-3}(t),$$

$$\overline{\omega}_{k-3}(t) = \frac{\xi - x_{k-3}}{x_{k+1} - x_{k-3}}\omega_{k-3}(t) + \frac{x_{k+2} - \xi}{x_{k+2} - x_{k-2}}\omega_{k-2}(t),$$

$$\overline{\omega}_{k-2}(t) = \frac{\xi - x_{k-2}}{x_{k+2} - x_{k-2}}\omega_{k-2}(t) + \frac{x_{k+3} - \xi}{x_{k+3} - x_{k-1}}\omega_{k-1}(t),$$

$$\overline{\omega}_{k-1}(t) = \frac{\xi - x_{k-1}}{x_{k+3} - x_{k-1}}\omega_{k-1}(t) + \omega_k(t).$$

Also splines $\omega_j(t)$ can be gotten with the help of the splines $\overline{\omega}_j(t)$. It gives us two types of formulas: formulas of decomposition and formulas of reconstruction. Step by step we can take out elements from the primary grid X and to build new splines which uses new grids, up to $L-3$ times (each time we take one element and get new grid and new splines), this formulas called formulas of decomposition, for reconstruction of original splines we use formulas of reconstruction.

3 Basic concepts of the algorithm

The presented algorithm relative to class of block cipher algorithms. A process of enciphering and deciphering consists of K identical rounds.

This algorithm can work with the block length up to 2048 bits, and it is not a limit. The number of rounds is denoted by K, $X\gamma$ is a key length and M is a block length (in the table below M and $X\gamma$ are bytes). Number of rounds and key length as a function of the block length given in Table 1.

	$(K, X\gamma)$
$M = 8$ bytes	$(6, 15)$
$M = 16$ bytes	$(14, 31)$
$M = 24$ bytes	$(22, 47)$
$M = 32$ bytes	$(30, 63)$
$M = 64$ bytes	$(62, 127)$
$M = 128$ bytes	$(126, 255)$
$M = 256$ bytes	$(254, 511)$

Table 1.

Let $\mathtt{K} = (X, \gamma)$ be *a key*; here X is an ordered set, $X = \{x_j\}_{j=0,\dots,L-1}$, where L is a number of elements in the set X.

In this algorithm on each round one element from the set X is removed. Let γ be the order of elements removed from the set X.

A sequence $C = \{c_i\}_{i=0,\dots,M-1}$ *is a plaintext;* $|C| = M$ is a quantity of elements which are ciphered, C is the ordered set.

Elements $\{c_i\}_{i=0,\dots,M-1}$ and $\{x_j\}_{j=0,\dots,L-1}$ are bytes (we are working with one-bytes words, but we also can work with 4-bytes words).

Let us suppose that the set X and C can be periodic with the period M so $x_j = x_{j+M}$ and $c_j = c_{j+M} \quad \forall j \in z$, where M is a block length.

Process of enciphering is based on the formulas of decomposition from wavelet theory, after K rounds we obtain the ciphertext. For deciphering we use formulas of reconstruction.

All calculation are carried out by mod N, N is a prime number, in this application $N = 283$.

4 Mathematical basis of process of enciphering and deciphering

Let us describe in more details process of enciphering. In the process of encryption K rounds are made. On first round we will get plaintext $\{c_i\}_{i=0,\dots,M-1}$ and also we know the key K.

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

First round:

1. We eject element x_{γ_1} from the primary set X. The received set is defined as X_{-1}[1] and $X_{-1} = \{x_{-1,i}\}$ and elements of a new set are equal:

$$x_{-1,i} = x_i \quad \text{if} \quad i < \gamma_1 \tag{1}$$

$$x_{-1,i} = x_{i+1} \quad \text{if} \quad i > \gamma_1 \Rightarrow \tag{2}$$
$$X_{-1} = \{x_{-1,i}\}.$$

   The element x_{γ_1} which has been taken out from the set X is defined as ξ.

2. Now we write formulas of decomposition for the splines of third degree.

$$c_{-1,i} = c_i \quad \text{if} \quad 0 \le i \le \gamma_1 - 5, \tag{3}$$

$$c_{-1,i} = c_{i+1} \quad \text{if} \quad \gamma_1 - 1 \le i \le M - 2, \tag{4}$$

$$c_{-1,\gamma_1-3} = \left(\frac{\xi - x_{-1,\gamma_1}}{\xi - x_{-1,\gamma_1-3}} \cdot c_{\gamma_1-4} + \right.$$

[1] To avoid misunderstanding with numeration in this work if it's written $\{...\}_{-j,i}$ $-j$ is a number of round and i is a number of element, if it's just $\{...\}_{-j}$ $-j$ is a number of round

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$+\frac{x_{-1,\gamma_1}-x_{-1,\gamma_1-3}}{\xi-x_{-1,\gamma_1-3}}\cdot c_{\gamma_1-3})(\mathrm{mod}N), \quad (5)$$

$$c_{-1,\gamma_1-2}=((\xi-x_{-1,\gamma_1})(\xi-x_{-1,\gamma_1+1})\cdot c_{\gamma_1-4}+$$
$$+(\xi-x_{-1,\gamma_1+1})(x_{-1,\gamma_1}-x_{-1,\gamma_1-3})\cdot c_{\gamma_1-3}+$$
$$+(x_{-1,\gamma_1+1}-x_{-1,\gamma_1-2})(\xi-x_{-1,\gamma_1-3})\cdot c_{\gamma_1-2})\cdot$$
$$\cdot[\xi-x_{-1,\gamma_1-2}]^{-1}[\xi-x_{-1,\gamma_1-3}]^{-1}(\mathrm{mod}N), \quad (6)$$

$$b_{-1}=(c_{\gamma_1-1}-\frac{x_{-1,\gamma_1+2}-\xi}{x_{-1,\gamma_1+2}-x_{-1,\gamma_1-1}}\cdot c_{-1,\gamma_1-2}-$$
$$-\frac{\xi-x_{-1,\gamma_1-1}}{x_{-1,\gamma_1+2}-x_{-1,\gamma_1-1}}\cdot c_{-1,\gamma_1-1})(\mathrm{mod}N). \quad (7)$$

3. At the end we make a shift of sequence $c_{-1,i}$ as follows:

$$c_{-1,0}\to c_{-1,1}\to c_{-1,2}...\to c_{-1,M-2}\to c_{-1,0}$$

Here $\{c_i\}_{i=0,...,M-1}$ plain text, $\{c_{-1,i}\}_{i=0,...,M-2}$ main stream, elements which we get after the first round and use on next round, also we get element b_{-1} an element of wavelet stream.

These formulas are throwing out one element with number γ_1-1 from our set $\{c_i\}_{i=0,...,M-1}$, moving elements $\{c_i\}_{i=0,...,\gamma_1-2,\gamma_1,...,M-1}$ and counting two elements with the help of formulas (5)-(6).

In formulas (3)-(7) we are using elements of a new set X_{-1}. On first round the sequence $\{c_{-1,i}\}_{i=0,...,M-2}$ and b_{-1} have been gotten.

On next round we are working with the set X_{-1} and $\{c_{-1,i}\}_{i=0,...,M-2}$.

In formulas (5)-(7) calculation are carried out by modN, it helps us to avoid division in these formulas, and to change division on calculation like $\frac{A}{B}$modN. We are using such module N so on each round equations presented below will take place:

1. $(\xi-x_{-j,\gamma_{j-2}})(\mathrm{modN})\neq 0$
2. $(x_{-j,\gamma_{j+1}}-x_{-j,\gamma_{j-1}})(\mathrm{modN})\neq 0$

All rounds except the final round goes by analogy with the first round, we take out from the set X_{-j} element x with number γ_j and count formulas of decomposition for splines.

Process of decryption goes by analogy with process of encryption, the same key K is used.

All rounds except the first round goes by analogy, on first round shift is not made.

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

$$\{b_{-n}\}_{n=1,2,...,K},\quad \{c_{-K,i}\}_{i=0,1,2,...,M-K-1}.$$

We know the primary set X and the order of elements removal γ so we can receive sets $X_{-1},\dots,X_{-K+1},X_{-K}$, as it is described in process of enciphering.

On each round we take out from the set X_{-j+1} only one element x with the number γ_j, where j is the number of round, and we receive set X_{-j}. For deciphering we need the reverse order, i.e. on first round we need the set X_{-K}, on the second X_{-K+1} and on last round X_{-1}.

First round:

1. We work with the set X_{-K}, $\xi=x_{-K,\gamma_k}$
2. We write formulas of reconstruction for the splines of third degree:

$$c_{-K+1,i}=c_{-K,i}\quad \text{if}\quad 0\le i\le\gamma_K-4, \quad (8)$$

$$c_{-K+1,i}=c_{-K,i-1}\quad \text{if}\quad \gamma_K\le i\le M-K, \quad (9)$$

$$c_{-K+1,\gamma_K-3}=(\frac{x_{-K,\gamma_K}-\xi}{x_{-K,\gamma_K}-x_{-K,\gamma_K-3}}\cdot c_{-K,\gamma_K-4}+$$
$$+\frac{\xi-x_{-K,\gamma_K-3}}{x_{-K,\gamma_K}-x_{-K,\gamma_K-3}}\cdot c_{-K,\gamma_K-3})(\mathrm{mod}N), \quad (10)$$

$$c_{-K+1,\gamma_K-2}=(\frac{x_{-K,\gamma_K+1}-\xi}{x_{-K,\gamma_K+1}-x_{-K,\gamma_K-2}}\cdot c_{-K,\gamma_K-3}+$$
$$+\frac{\xi-x_{-K,\gamma_K-2}}{x_{-K,\gamma_K+1}-x_{-K,\gamma_K-2}}\cdot c_{-K,\gamma_K-2})(\mathrm{mod}N), \quad (11)$$

$$c_{-K+1,\gamma_K-1}=(\frac{x_{-K,\gamma_K+2}-\xi}{x_{-K,\gamma_K+2}-x_{-K,\gamma_K-1}}\cdot c_{-K,\gamma_K-2}+$$
$$+\frac{\xi-x_{-K,\gamma_K-1}}{x_{-K,\gamma_K+2}-x_{-K,\gamma_K-1}}\cdot c_{-K,\gamma_K-1}+b_{-K})(\mathrm{mod}N). \quad (12)$$

On next round we work with the set X_{-K+1}, we also use $\{c_{-K+1,i}\}_{i=0,....,M-K}$ and b_{-K+1}, on the second round of process of deciphering we get the sequence $\{c_{-K+2,i}\}_{i=0,....,M-K+1}$ etc.

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

It is possible to create different types of algorithms based on the idea of spline-wavelet decomposition. In this realization the key become smaller on each round, we cipher two bytes and other bytes just move, but there is a realization when the key do not became smaller and each

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

byte is ciphered on each round. This idea is under construction now.

The presented algorithm stays strong to differential and linear cryptanalyses.

5 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] Demjanovich, Y.K., *Splaches decomposition in spaces of splines on a non-uniform grid*, Publication of RAS 2002. . 382, P. 313-316 (in Russian).

[2] Burova, I.G., Demjanovich, Y.K., *Theory of minimal splines*, St. Petersburg University Publication 2003 (in Russian).

[3] Demjanovich, Y.K., *Splashes and the minimal splines*, St. Petersburg University Publication 2003 (in Russian).

[4] Smart Nigel: *Cryptography*: An Introduction, 2nd Edition.

ISBN: 978-988-18210-9-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)