САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

На правах рукописи

Левина Алла Борисовна

СПЛАЙН-ВЭЙВЛЕТЫ И ИХ НЕКОТОРЫЕ ПРИМЕНЕНИЯ

05.13.18 — математическое моделирование, численные методы
и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Санкт-Петербург
2009

Работа выполнена на кафедре параллельных алгоритмов
математико-механического факультета
Санкт-Петербургского государственного университета

Научный руководитель: доктор физико-математических наук,
профессор Демьянович Юрий Казимирович

Официальные оппоненты: доктор физико-математических наук,
профессор Жук Владимир Васильевич
(Санкт-Петербургский государственный
университет)

доктор физико-математических наук,
профессор Ходаковский Валентин Аветикович
(Санкт-Петербургский государственный
университет путей сообщения)

Ведущая организация: Научно-исследовательский вычислительный центр Московского государственного университета им. М.В. Ломоносова (НИВЦ МГУ)

Защита диссертации состоится " " 2009 г. в часов на заседании совета Д 212.232.51 по защите докторских и кандидатских диссертаций при Санкт-Петербургском государственном университете по адресу: 198504, Санкт-Петербург, Старый Петергоф, Университетский пр., 28, ауд. 405.

С диссертацией можно ознакомиться в Научной библиотеке им. М. Горького Санкт-Петербургского государственного университета по адресу: 199034, Санкт-Петербург, Университетская наб., 7/9.

Автореферат разослан " " 2009 г.

Ученый секретарь
диссертационного совета,
доктор физ.-мат. наук,
профессор Даугавет И.К.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Сплайны и вэйвлеты широко используются для обработки числовых информационных потоков (см. [1]); эта область исследований относится к численным методам. Использование цепочек вложенных пространств сплайнов позволяет строить вэйвлетные разложения (декомпозицию и реконструкцию) в весьма общих условиях, в том числе, с использованием неравномерной сетки (см. [2]), последняя может рассматриваться как ключ в шифровании исходного числового потока, при котором результаты шифрования представлен вэйвлетным разложением. Поскольку постоянно рассматриваются новые способ шифрования, то построение сплайн - вэйвлетных разложений и разработка на их основе сплайн-вэйвлетных криптосистем представляются актуальными.

Одной из областей математического моделирования традиционно является криптография. Началом современной криптографии можно считать работы Клода Шеннона опубликованные в 1948 году "A Mathematical Theory of Communication"в которой сформулированы основы теории информации, большую ценность представляет другая его работа - "Communication Theory of Secrecy Systems". В основу блочных шифров легли работы Хорста Фейстеля начатые им в 1971 году и опубликованные в журнале Scientific American в 1973. Было введено понятие "сеть Фейстеля", которое легло в основу большинства современных блочных шифров. Развитием криптографии, созданием и исследованием новых алгоритмов занимались многие ученые: У. Фридман, Д. Копперсмит, Й. Дамен и В. Раймен, Р. Ривестом, М. Робшау и Р. Сиднеем, Б. Шнайер, Э. Бихам и А. Шамир, Мацуи и многие другие.

На протяжении многих лет криптография была засекречена и использовалась только в государственных и военных целях. Однако в настоящее время эта наука широко используется в электронной почте, в системах банковских платежей, при торговле через Internet. В современном мире компьютерных технологий очень много информации финансового, коммерческого и персонального характера хранится в компьютерных банках данных. В связи с этим возникает потребность в качественном сокрытии информации и в создании соответствующих пакетов программ.

Цель диссертационной работы

Целью диссертационной работы является построение сплайн-вэйвлетных разложений и получение новых криптоалгоритмов, основанных на вэйвлетных разложениях сплайнов первого, второго и третьего порядка, апробация работы этих алгоритмов на модельных примерах и исследования их устойчивости по отношению к криптоатакам, а также анализ условий, при которых представленные алгоритмы могут обеспечить абсолютную стойкость, и апробация представленных алгоритмов на числовых примерах.

Методы исследования

В диссертации используются методы математического анализа, теория алгоритмов, для построения криптоалгоритмов используются современная теория криптографии и математические основы криптографии.

Достоверность и обоснованность

Достоверность результатов подтверждена строгими доказательствами; результаты согласуются с проведенными численными экспериментами.

Результаты, выносимые на защиту

1. Построены новые сплайн-вэйвлетные разложения и изучены их свойства.
2. Предложены новые алгоритмы шифрования, построенные на вэйвлетных разложениях пространств сплайнов первого, второго и третьего порядков в конечных полях. Процесс шифрования основывается на формулах декомпозиции сплайн-вэйвлетных разложений, а процесс дешифрования на формулах реконструкции.
3. Проведен анализ устойчивости предложенных алгоритмов по отношению к криптоатакам.
4. Проведен анализ стойкости алгоритмов, установлены условия, в которых упомянутые алгоритмы являются абсолютно стойкими.
5. Теоретические результаты апробированы на модельных числовых примерах с использованием комплекса программ, основанных на предложенных алгоритмах.

Научная новизна

В данной работе впервые разработаны новые сплайн-вэйвлетные разложения и получены криптоалгоритмы основанные на вэйвлетном разложении сплайнов в конечных полях, проведен анализ стойкости представленных алгоритмов. Все основные результаты являются новыми.

Теоретическая и практическая полезность

Работа носит теоретический характер, представленные результаты можно использовать на практике. Предложенные алгоритмы шифрования могут быть применены не только для шифрования текстовой информации, но и для шифрования сигналов, поступающих от различных устройств. Предложенные алгоритмы можно модернизировать и изменять в зависимости от поставленных задач.

Апробация работы

Основные результаты были представлены на следующих конференциях и семинарах:

1. Процессы управления и устойчивость. XXXVII международная научная конференция аспирантов и студентов, С.-Петербург, Россия, 10-13 апреля 2006 г.

2. Процессы управления и устойчивость. XXXVIII международная научная конференция аспирантов и студентов, С.-Петербург, Россия, 9-12 апреля 2007 г.

3. Космос, астрономия и программирование (Лавровские чтения), С.-Петербург, 20-22 мая 2008 г.

4. World Congress on Engineering 2008, London, U.K., 2-4 July, 2008.

5. International School on Mathematical Cryptology, Mathematical Foundations of Cryptology, Barcelona, Spain, 21-27 September 2008.

6. 3^{rd} Information Security and Cryptology Conference, Ankara, Turkey, 25-27 December.

7. Fast Software Encryption 2009, Leuven, Belgium, February 22-25, 2009.

8. Семинар кафедры параллельных алгоритмов математико-механического факультета Санкт-Петербургского государственного университета.

Публикации

Основные результаты опубликованы в восьми работах [1-8]. Работа [6] опубликована в издании входящем в список рекомендованных Высшей аттестационной комиссией на момент публикации. В работах [3, 6] диссертанту принадлежит реализация идеи использования сплайн-вэйвлетных разложений в криптографии, описание процессов шифрования и дешифрования. В работе [6] диссертантом описан алгоритм, основанный на сплайн-вэйвлетных разложениях первого порядка, данный алгоритм представлен для блочного шифрования.

Структура и объем работы

Диссертация объемом 214 страниц состоит из введения, четырех глав, заключения, списка литературы и приложения. Приложение содержит описание пакета программ, основанного на предложенных алгоритмах и предназначенного для выбора их параметров (ключа, входного потока), шифрования и дешифрования испытуемых потоков.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность диссертационной работы и излагаются основные полученные результаты.

В **первой главе** приведен краткий обзор классических симметричных шифров (см. [3]), введено понятие блочных и поточных шифров. Рассмотрены пассивные и активные атаки, введено понятие стойкости шифров.

Приведена Теорема Шеннона о стойкости криптоалгоритмов.

Далее излагаются наиболее известные симметричные алгоритмы блочного шифрования, шифр Фейстеля, *DES* и алгоритм *Rijndael*, который является стандартом шифрования США с 2002 года. Во **второй главе** рассматриваются сплайн-вэйвлетные разложения. Для координатных сплайнов строятся системы функционалов $\{g^{(i)}\}_{i\in\mathbb{Z}}$ биортогональные системам координатных сплайнов $\{\omega_j\}_{j\in\mathbb{Z}}$.

Пусть $X: \quad \ldots < x_{-1} < x_0 < x_1 < \ldots$— сетка,

$$\alpha = \lim_{j\to-\infty} x_j,\ \beta = \lim_{j\to+\infty} x_j,$$

положим здесь α и β могут быть конечными или бесконечными.

Для фиксированного $k \in \mathbb{Z}$ положим

$$\overline{x}_j \stackrel{\text{def}}{=} x_j \text{ при } j \le k-1, \text{ и } \overline{x}_j \stackrel{\text{def}}{=} x_{j+1} \text{ при } j \ge k, \quad \xi \stackrel{\text{def}}{=} x_k,$$

и рассмотрим новую сетку $\overline{X}: \quad \ldots < \overline{x}_{-1} < \overline{x}_0 < \overline{x}_1 < \ldots$. Таким образом сетка $\overline{X}$получается из сетки X выбрасыванием узла ξ.

Для сетки $\overline{X}$, полученной из сетки X удалением одного узла, строятся сплайны $\overline{\omega}_j$, устанавливаются калибровочные соотношения, выражающие сплайны $\overline{\omega}_j$ в виде линейной комбинации сплайнов ω_j: $\overline{\omega}_i = \sum_j d_{i,j}\omega_j$,

Теорема 1. *Для сплайнов первого порядка коэффициенты $d_{i,j}$, $i,j \in \mathbb{Z}$ отыскиваются по формулам:*

$$d_{i,j} = \delta_{i,j} \qquad при \quad i \le k-3, \qquad \forall j \in \mathbb{Z},$$

$$d_{k-2,k-2} = 1, \ \ d_{k-2,k-1} = (x_{k+1} - x_k)(x_{k+1} - x_{k-1})^{-1},$$
$$d_{k-2,j} = 0 \ при\ j \notin \{k-2, k-1\}, \qquad d_{k-1,j} = 0 \ при\ j \notin \{k-1, k\},$$
$$d_{k-1,k-1} = (x_k - x_{k-1})(x_{k+1} - x_{k-1})^{-1}, d_{k-1,k} = 1,$$
$$d_{i,j} = \delta_{i,j-1} \qquad при \quad i \ge k, \qquad \forall j \in \mathbb{Z}.$$

Для сплайнов второго и третьего порядков устанавливаются аналогичные калибровочные соотношения.

Калибровочные отношения для сплайнов второго порядка представлены в теореме 2.

Теорема 2. *Справедливы соотношения*

$$\overline{\omega}_i = \sum_j d_{i,j}\omega_j,$$

где для $i,j \in \mathbb{Z}$ числа $d_{i,j}$ отыскиваются по формулам:

$$d_{i,j} = \delta_{i,j} \qquad при \quad i \le k-4,$$

$$d_{k-3,k-3} = 1, \ \ d_{k-3,k-2} = (\overline{x}_k - \xi)(\overline{x}_k - \overline{x}_{k-2})^{-1}, d_{k-3,j} = 0 \ при\ j \notin \{k-3, k-2\},$$
$$d_{k-2,k-2} = (\xi - \overline{x}_{k-2})(\overline{x}_k - \overline{x}_{k-2})^{-1}, d_{k-2,k-1} = (\overline{x}_{k+1} - \xi)(\overline{x}_{k+1} - \overline{x}_{k-1})^{-1},$$
$$d_{k-2,j} = 0 \quad при \quad j \notin \{k-2, k-1\},$$

$$d_{k-1,k-1} = (\xi - \overline{x}_{k-1})(\overline{x}_{k+1} - \overline{x}_{k-1})^{-1}, \;\; d_{k-1,k} = 1, \; d_{k-1,j} = 0 \;\; при \;\; j \notin \{k-1, k\},$$
$$d_{i,j} = \delta_{i+1,j} \qquad при \quad i \geq k.$$

Далее во второй главе строятся сплайн-вэйвлетные разложения и выводятся формулы реконструкции и декомпозиции.

$\Omega(X)$ пространство, являющееся линейной оболочкой функций ω_j,

$$\Omega(X) \stackrel{\text{def}}{=} \{ \; u \mid u \stackrel{\text{def}}{=} \sum_j c_j \omega_j \;\; \forall c_j \in \mathbb{R}^1 \; \};$$

пространство $\Omega(X)$ называется *пространством сплайнов на сетке* X, а ω_j — *образующими* этого пространства.

В соответствии с этим определением $\Omega(\overline{X})$ является пространством сплайнов на сетке $\overline{X}$,

$$\Omega(\overline{X}) = \{ \; \overline{u} \mid \overline{u} \stackrel{\text{def}}{=} \sum_j \overline{a}_j \overline{\omega}_j \;\; \forall \overline{a}_j \in \mathbb{R}^1 \; \}.$$

Согласно теореме 1 справедливо включение $\Omega(\overline{X}) \subset \Omega(X)$.

Рассматривается оператор P проектирования пространства $\Omega(X)$ на подпространство $\Omega(\overline{X})$, задаваемый формулой

$$Pu \stackrel{\text{def}}{=} \sum_j \langle \overline{g}^{(j)}, u \rangle \; \overline{\omega}_j \qquad \forall u \in \Omega(X).$$

Это проектирование определяет прямое разложение

$$\Omega(X) = \Omega(\overline{X}) \dot{+} W_k, \tag{1}$$

где W_k — пространство вэйвлетов.

Пусть $u \in \Omega(X)$; используя соотношение (1), получаем два представления элемента u

$$u = \sum_j c_j \omega_j,$$

$$u = \sum_j a_i \overline{\omega}_i + \sum_j b_j \omega_j.$$

Связь между коэффициентами этих представлений устанавливается в следующем утверждение:

Теорема 3(*Формулы декомпозиции*). *Для сплайн-вэйвлетного разложения (1) пространства $\Omega(X)$ сплайнов первого порядка верны формулы:*

$$a_i = c_i \quad при \quad i \leq k-2, \qquad a_i = c_{i+1} \quad при \quad i \geq k-1,$$
$$b_j = 0 \quad при \quad j \neq k-1$$
$$b_{k-1} = c_{k-1} - (x_{k+1} - x_k)(x_{k+1} - x_{k-1})^{-1} c_{k-2} -$$
$$-(x_k - x_{k-1})(x_{k+1} - x_{k-1})^{-1} c_k.$$

Теорема 4(*Формулы реконструкции*). *Для рассматриваемого сплайн-вэйвлетного разложения (1) пространства* $\Omega(X)$ *сплайнов первого порядка верны формулы:*

$$c_j = a_j \quad \textit{при } j \le k-2, \qquad c_j = a_{j-1} \quad \textit{при } j \ge k,$$

$$c_{k-1} = (x_{k+1} - x_k)(x_{k+1} - x_{k-1})^{-1} a_{k-2} + (x_k - x_{k-1})(x_{k+1} - x_{k-1})^{-1} a_{k-1} + b_{k-1}.$$

Также выведены формулы реконструкции и декомпозиции для сплайнов второго и третьего порядка.

Теорема 5. *Для рассматриваемого сплайн-вэйвлетного разложения (1) пространства* $\Omega(X)$ *сплайнов второго порядка формулы реконструкции имеют вид*

$$c_j = a_j + b_j \quad \textit{при } j \le k-3,$$

$$c_{k-2} = a_{k-3}(\overline{x}_k - \xi)(\overline{x}_k - \overline{x}_{k-2})^{-1} + a_{k-2}(\xi - \overline{x}_{k-2})(\overline{x}_k - \overline{x}_{k-2})^{-1} + b_{k-2},$$

$$c_{k-1} = a_{k-2}(\overline{x}_{k+1} - \xi)(\overline{x}_{k+1} - \overline{x}_{k-1})^{-1} + a_{k-1}(\xi - \overline{x}_{k-1})(\overline{x}_{k+1} - \overline{x}_{k-1})^{-1} + b_{k-1},$$

$$c_j = a_{j-1} + b_j \quad \textit{при } j \ge k.$$

Теорема 6. *Для сплайн-вэйвлетного разложения (1) пространства* $\Omega(X)$ *сплайнов второго порядка формулы декомпозиции имеют вид*

$$a_i = c_i \qquad \textit{при} \quad i \le k-3,$$

$$a_{k-2} = -(\overline{x}_k - \xi)(\xi - \overline{x}_{k-2})^{-1} c_{k-3} + (\overline{x}_k - \overline{x}_{k-2})(\xi - \overline{x}_{k-2})^{-1} c_{k-2},$$

$$a_i = c_{i+1} \qquad \textit{при} \quad i \ge k-1,$$

$$b_j = 0 \quad \textit{при} \quad j \ne k-1,$$

$$b_{k-1} = \Big[(\overline{x}_{k+1} - \xi)(\overline{x}_k - \xi)c_{k-3} - (\overline{x}_{k+1} - \xi)(\overline{x}_k - \overline{x}_{k-2})c_{k-2} + (\overline{x}_{k+1} - \overline{x}_{k-1})(\xi - \overline{x}_{k-2})c_{k-1} -$$

$$- (\xi - \overline{x}_{k-1})(\xi - \overline{x}_{k-2})c_k\Big](\overline{x}_{k+1} - \overline{x}_{k-1})^{-1}(\xi - \overline{x}_{k-2})^{-1},$$

Для полиномиальных сплайнов первого порядка рассматривается вопрос о восстановление сетки по исходному потоку и по вэйвлетной составляющей и о построение сетки по поступающему потоку. Эти результаты сформулированы в следующих теоремах:

Теорема 7. *Если*

$$c_{k-2} \ne c_k,$$

то узел ξ *определяется однозначно по формуле*

$$\xi = x_{k-1} + q_k(x_{k+1} - x_{k-1}),$$

где

$$q_k = \frac{c_{k-1} - c_{k-2} - b_{k-1}}{c_k - c_{k-2}}.$$

Если же

$$c_{k-2} = c_k,$$

то в качестве ξ можно взять любую точку интервала (x_{k-1}, x_{k+1}).

Теорема 5. *В условиях теоремы 4 при $c_{k-2} \neq c_k$, вэйвлетная составляющая b_{k-1} равна нулю тогда и только тогда, когда выполнено соотношение*

$$\frac{c_k - c_{k-1}}{c_{k-1} - c_{k-2}} = \frac{h_k}{h_{k-1}},$$

где $h_k \stackrel{\text{def}}{=} x_{k+1} - x_k$.

Третья глава посвящена построению алгоритмов шифрования, основанных на сплайн-вэйвлетных разложениях, рассматриваемых в конечных полях. Эти алгоритмы используют сплайн-вэйвлетные разложения полиномиальных сплайнов первого, второго и третьего порядка. Предлагаемые криптосистемы относится к симметричным алгоритмам блочного шифрования, в которых при шифровании и дешифровании используется один ключ.

Ключ $\mathbb{K}$ имеет две составляющие: сетку X и порядок выбрасывания узлов γ: $\mathbb{K} = (X, \gamma)$; здесь $X = \{x_j\}_{j=0,...L-1}$, где L количество узлов в сетке, x_j— (различные) узлы сетки. $\gamma = \{\gamma_n\}_{n=1,...K}$, K число раундов шифрования, γ_n—номер выбрасываемого узла. Сетку X можно считать периодической (имея ввиду, например, сетку на окружности): $x_{j+L} = x_j$ для $\forall j \in \mathbb{Z}$, L— натуральное число $L \geq 5$.

Открытым текстом является последовательность $C = \{c_i\}_{i \in J}$, $J \subset \mathbb{Z}$. Открытый текст разбивается на l блоков $|C_i|$ одинаковой длины, $|C_i| = M$, $|C_i|$ — число элементов в блоке, $i = 1, 2, ...l$. На $k-$м раунде число элементов преобразованного блока C_i^{-k} равно $M - k$; при необходимости последовательность $C_i^{-k} = \{c_i^{-k}\}_{i=1,...,M-k}$ продлевается периодически с периодом $M - k$.

Все вычисления проводятся в конечных полях, по модулю N, где $N-$простое число. N передается вместе с открытым текстом. При шифровании сплайнами первого порядка считаем, что $\xi \neq x_{\gamma_{i+1}}^{-i} (\mathrm{mod} N)$, где $i-$номер раунда, а $x_{\gamma_{i+1}}^{-i}$ узел на $i-$ом раунде с номером γ_{i+1}. Здесь и в дальнейшем все неравенства относятся к конечным полям классов сравнений по модулю N.

Для сплайнов второго порядка предполагается, что:
$\xi \neq x_{\gamma_{i-2}}^{-i}$,
$x_{\gamma_{i+q}}^{-i} \neq x_{\gamma_{i+q-2}}^{-i}, q = 0, 1.$
Для сплайнов третьего порядка:
$\xi \neq x_{\gamma_{i-q}}^{-i}, q = 2, 3,$
$x_{\gamma_{i+p}}^{-i} \neq x_{\gamma_{i+p-3}}^{-i}, p = 0, 1, 2.$

В представленных алгоритмах преобразование каждого раунда имеет структуру сети Фейстеля, часть битов в каждом промежуточном состоянии просто перемещается без изменений.

На каждом раунде из сетки выбрасывается один узел с номером γ_k, где $k-$номер раунда, получается "подключ", используемый на этом раунде. Далее при шифровании по формулам декомпозиции вычисляем последовательность $\{c_i^{-k}\}_{i \in J}$, после проведения K раундов получается шифротекст. Все раундовые функции обратимы. При дешифровании текст восстанавливается с помощью формул реконструкции.

Представленные алгоритмы могут работать с блоками произвольной длины, в частности, с блоками равными 512 и 1024 бит, что раньше не представлялось возможным для алгоритмов *3DES* и *Rijndael*.

В этой главе представлены численные примеры, демонстрирующие работу предложенных алгоритмов. Также продемонстрирована работа алгоритмов с блоками длиной 128, 256 и 512 бит.

В **четвертой главе** проведен анализ устойчивости предложенных криптоалгоритмов. Проверены условия теоремы Шеннона, выведены условия, при которых предложенные алгоритмы являются абсолютно стойкими.

Теорема 8. *Если для* $k \in 1, ..., K$ *выполнены соотношения*

- $c_{\gamma_k-1}^{-k+1} \neq c_{\gamma_k+1}^{-k+1}$;
- $(x_{\gamma_k+1}^{-k} - x_{\gamma_k}^{-k}) \cdot (x_{\gamma_k+1}^{-k} - \xi)^{-1} \neq (\overline{x_{\gamma_k+1}^{-k}} - \overline{x_{\gamma_k}^{-k}}) \cdot (\overline{x_{\gamma_k+1}^{-k}} - \overline{\xi})^{-1}$;
  $(x_{\gamma_k+1}^{-k} - \xi)^{-1} \neq (x_{\gamma_k+1}^{-k} - \overline{\xi})^{-1}$;
  где $\overline{\xi}$, $\overline{x_{\gamma_k+1}^{-k}}$ *и* $\overline{x_{\gamma_k}^{-k}}$ *элементы сетки* $\overline{X} \neq X$;
- $x_{\gamma_k+1}^{-k} \neq x_{\gamma_k}^{-k}$,

то криптосистема, основанная на вэйвлетном разложении сплайнов первого порядка, является абсолютно стойкой.

Теорема 9. *При выполнении соотношений, где* $k \in 1, ..., K$,

- $c_{\gamma_k-3}^{-k+1} \neq c_{\gamma_k-2}^{-k+1}$;
- $\left(\overline{\xi}(x_{\gamma_k}^{-k} - x_{\gamma_k-2}^{-k}) - \xi(\overline{x_{\gamma_k}^{-k}} - \overline{x_{\gamma_k-2}^{-k}}) + \overline{x_{\gamma_k}^{-k}} x_{\gamma_k-2}^{-k} - x_{\gamma_k}^{-k}\overline{x_{\gamma_k-2}^{-k}}\right) \neq 0$,
  $\left(\overline{\xi}(x_{\gamma_k-1}^{-k} - x_{\gamma_k+1}^{-k}) - \xi(\overline{x_{\gamma_k-1}^{-k}} - \overline{x_{\gamma_k+1}^{-k}}) + \overline{x_{\gamma_k-1}^{-k}} x_{\gamma_k+1}^{-k} - x_{\gamma_k-1}^{-k}\overline{x_{\gamma_k+1}^{-k}}\right) \neq 0$,
  $\left((\overline{x_{\gamma_k}^{-k}} - \overline{\xi})c_{\gamma_k-3}^{-k+1} - (\overline{x_{\gamma_k}^{-k}} - \overline{x_{\gamma_k-2}^{-k}})c_{\gamma_k-2}^{-k+1} + (\overline{\xi} - \overline{x_{\gamma_k-2}^{-k}})c_{\gamma_k}^{-k+1}\right) \neq 0$,
  где $\overline{\xi}, \overline{x_{\gamma_k-2}^{-k}}, \overline{x_{\gamma_k-1}^{-k}}, \overline{x_{\gamma_k}^{-k}}, \overline{x_{\gamma_k+1}^{-k}}$;
- $\left((x_{\gamma_k}^{-k} - \overline{\xi})c_{\gamma_k-3}^{-k+1} - (x_{\gamma_k}^{-k} - x_{\gamma_k-2}^{-k})c_{\gamma_k-2}^{-k+1} + (\overline{\xi} - x_{\gamma_k-2}^{-k})c_{\gamma_k}^{-k+1}\right) \neq 0$,
  $\xi \neq \overline{\xi}$,
  где $\overline{\xi}$ *узел, выбрасываемый на* $k-$*ом раунде из сетки* X, *при этом* $\overline{\gamma} \neq \gamma$,

криптосистема, основывающаяся на вэйвлетных разложениях сплайнов второго порядка, является абсолютно стойкой.

Теорема 10. *Если при* $k \in 1, ..., K$ *справедливы формулы*

- $c_{\gamma_k-4}^{-k+1} \neq c_{\gamma_k-3}^{-k+1}$;
- $c_{\gamma_k-2}^{-k} \neq c_{\gamma_k-1}^{-k}$;
- $\left(\overline{\xi}(x_{\gamma_k}^{-k} - x_{\gamma_k-3}^{-k}) - \xi(\overline{x_{\gamma_k}^{-k}} - \overline{x_{\gamma_k-3}^{-k}}) + \overline{x_{\gamma_k}^{-k}} x_{\gamma_k-3}^{-k} - x_{\gamma_k}^{-k}\overline{x_{\gamma_k-3}^{-k}}\right) \neq 0$,
  $\left(\overline{\xi}(x_{\gamma_k-1}^{-k} - x_{\gamma_k+2}^{-k}) - \xi(\overline{x_{\gamma_k-1}^{-k}} - \overline{x_{\gamma_k+2}^{-k}}) + \overline{x_{\gamma_k-1}^{-k}} x_{\gamma_k+2}^{-k} - x_{\gamma_k-1}^{-k}\overline{x_{\gamma_k+2}^{-k}}\right) \neq 0$,
  $\left(c_{\gamma_k-4}^{-k+1} \cdot (\overline{\xi} - \overline{x_{\gamma_k}^{-k}}) + c_{\gamma_k-3}^{-k+1} \cdot (\overline{x_{\gamma_k}^{-k}} - \overline{x_{\gamma_k-3}^{-k}}) - (\overline{\xi} - \overline{x_{\gamma_k-3}^{-k}})c_{\gamma_k-2}^{-k+1}\right) \neq 0$,
  где $\overline{\xi}$, $\overline{x_{\gamma_k-3}^{-k}}$, $\overline{x_{\gamma_k-1}^{-k}}$, $\overline{x_{\gamma_k}^{-k}}$ *и* $\overline{x_{\gamma_k+2}^{-k}}$ *элементы сетки* $\overline{X} \neq X$;

- $\left(c_{\gamma_k-4}^{-k+1}\cdot(\overline{\xi}-x_{\gamma_k}^{-k})+c_{\gamma_k-3}^{-k+1}\cdot(x_{\gamma_k}^{-k}-x_{\gamma_k-3}^{-k})-(\overline{\xi}-x_{\gamma_k-3}^{-k})c_{\gamma_k-2}^{-k+1}\right)\neq 0,$
  $\xi\neq\overline{\xi},$
  где $\overline{\xi}$ *узел, выбрасываемый на* k*—ом раунде из сетки* X*, при этом* $\overline{\gamma}\neq\gamma$,

то криптосистема, основывающаяся на вэйвлетных разложениях сплайнов третьего порядка, является абсолютно стойкой.

Проведен анализ устойчивости алгоритмов к атаке методом перебора и к атаке с выбором открытого текста.

В **заключении** перечислены основные результаты исследований.

Приложение содержит пакет программ для реализации шифрования и дешифрования с помощью сплайн-вэйвлетных разложений в конечных полях. В качестве исходных данных задается модуль конечного поля, исходный числовой поток, ключ, на выходе получается результат шифрования. Дешифрование позволяет по результату шифрования с помощью ключа получить исходный поток. Программирование велось на C^{++} и Pascal. Пакет распадается на две независимые части - шифрование и дешифрование.

При шифровании на каждом раунде создается сетка, выводится основной поток и вэйвлетная составляющая, при дешифровании на каждом раунде выводится восстановленный поток. Программа выводит разность между исходным и реконструированным потоком — массив уклонений; равенство нулю всех элементов данного массива демонстрирует, что исходный числовой поток был корректно восстановлен.

Список цитируемой литературы

[1] **Демьянович Ю. К.** Минимальные сплайны и всплески // Вестн. С.–Петерб. ун-та. Сер. 1. 2008. Вып. 2. С. 8–22.

[2] **Малла С.** Вэйвлеты в обработке сигналов // Пер. с англ. Я. М. Жилейкина. М.: Мир, 2005. 671 с.

[3] **Смарт Н.** Криптография // Москва: ТЕХНОСФЕРА, 2005. 528с.

Список опубликованных работ по теме диссертации

[1] **Левина А. Б.** Устойчивость алгоритмов шифрования при использовании параллельных систем // Процессы управления и устойчивость: Тр. 37-й междунар. науч. конф. аспирантов и студентов. СПб., 10–13 апреля 2006г. / Под ред. А. В. Платонова, Н. В. Смирнова. – СПб.: Изд-во С.-Петерб. ун-та, 2006. С. 365–367.

[2] **Левина А. Б.** Распараллеливание алгоритма Rijndael // Процессы управления и устойчивость: Тр. 38-й междунар. науч. конф. аспирантов и студентов. СПб., 9–12 апреля 2007г. / Под ред. А. В. Платонова, Н. В. Смирнова. – СПб.: Изд-во С.-Петерб. ун-та, 2007. С. 381–386.

[3] **Демьянович Ю. К., Левина А. Б.** Вэйвлетные разложения и шифрование// Методы вычислений–2008: Выпуск 22: Изд-во С.-Петерб. ун-та, 2008. С. 41-63.

[4] **Demjanovich Yu. K., Levina A. B.** Encryption with first order splines // Third Information Security Cryptology Conference, Ankara, Turkey, 25-27 December 2008. p. 169-172.

[5] **Levina A. B.** Cryptoalgorithm Based on Formulas of Reconstruction and Decomposition on the Non-uniform Grid // Lecture Notes in Engineering and Computer Science, World Congress on Engineering 2008, London, U.K. 2-4 July, 2008. p. 1724-1727.

[6] **Демьянович Ю. К., Левина А. Б.** О вэйвлетных разложениях линейных пространств над произвольным полем и о некоторых приложениях// Журнал Математическое моделирование– 2008: Том 20, номер 11, С. 104-108.

[7] **Левина А. Б.** Работа криптосистемы, основанной на формулах реконструкции и декомпозиции на неравномерной сетке// Математические модели теория и приложения, сборник научных статей – 2008: Выпуск 9, С. 3-29.

[8] **Levina A. B.** Block ciphers based on wavelet decomposition of splines// http://fse2009rump.cr.yp.to/5e510e48d1e166b3e7ade715bcab744e.pdf