УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2021 Том 21 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2021 Vol. 21 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2021-21-6-936-941
УДК 004.052.42

Сплайн-вейвлетные надежные бент-коды

Алла Борисовна Левина[1]✉, Глеб Александрович Ряскин[2]

[1,2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197376, Российская Федерация

[1] alla_levina@mail.ru✉, https://orcid.org/0000-0003-4421-2411
[2] Ryaskinkgleb20@gmail.ru, https://orcid.org/0000-0003-3046-0473

Аннотация

Предмет исследования. В работе рассмотрено применение бент-функций различных степеней для построения *R*-надежных кодов, для обеспечения защиты от атак по сторонним каналам. Использование в алгоритмах кодирования бент-функции различных степеней дает возможность менять параметры надежности кода и время кодирования информации. Более высокие степени бент-функций увеличивают вероятность обнаружения ошибок при передаче или хранении данных, тогда как меньшие степени сокращают время кодирования информации, но в ущерб свойствам надежности. В предложенном алгоритме кодирования можно задавать степень бент-функции через использование сплайн-вейвлетного разложения с помощью изменения процесса генерирования сплайн-вейвлетной сетки. **Метод.** В рамках работы построены бент-функции на основе нелинейных функций и элементов сплайн-вейвлетного разложения. Разработан метод построения новой кодовой конструкции сплайн-вейвлет надежного бент-кода. **Основные результаты.** Использование сплайн-вейвлетов позволяет изменять конструкции и параметры кодов в процессе выполнения, что увеличивает защищенность системы от действий злоумышленника. Отличия различных кодовых конструкций заключается в использовании сеток для сплайн-вейвлетного преобразования и в выборе бент-функций разных степеней. Разработанная конструкция надежного кода обладает меньшей вероятностью маскировки ошибок в случае использования бент-функции высокой степени. При меньшей степени бент-функция имеет быстрое время кодирования по сравнению с существующими надежными кодами. **Практическая значимость.** Полученные результаты могут быть использованы для защиты от атак по сторонним каналам при хранении и передаче информации в системах связи.

Ключевые слова

надежные коды, бент-функции, сплайн-вейвлетное разложение информации, атаки по сторонним каналам, атака по ошибкам вычислений

Благодарности

Работа была поддержана Министерством науки и высшего образования Российской Федерации «Госзадание» № 075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0015).

Ссылка для цитирования: Левина А.Б., Ряскин Г.А. Сплайн-вейвлетные надежные бент-коды // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 6. С. 936–941. doi: 10.17586/2226-1494-2021-21-6-936-941

Spline-wavelet bent robust codes

Alla B. Levina[1]✉, Gleb A. Ryaskin[2]

[1,2] Saint Petersburg State Electrotechnical University (LETI), Saint Petersburg, 197376, Russian Federation

[1] alla_levina@mail.ru✉, https://orcid.org/0000-0003-4421-2411
[2] Ryaskinkgleb20@gmail.ru, https://orcid.org/0000-0003-3046-0473

Abstract

The paper examines the application and properties of bent functions of various degrees to construct *R*-robust codes with a spline wavelet grid for the protection against side-channel attacks. The use of the bent function of various degrees in coding algorithms allows changes the robust parameters and the information coding time. Higher degrees of bent

functions in robust coding algorithms increase the likelihood of detecting errors in the transmission or storage of data. In comparison, smaller degrees reduce the time for coding information but at the expense of robust properties. As part of the coding algorithm, it is possible to change the degree of the bent function through the use of the spline-wavelet decomposition; for this, it is necessary to change the process of generating the spline-wavelet grid. In this work, bent functions were compiled from nonlinear functions and elements of the spline-wavelet composition. Based on the results obtained, a new construction of a spline-wavelet robust bent code was proposed. The use of spline wavelets allows one to change the designs and parameters of codes during execution, which increases the security of the system against attacker's actions. The distinction between the given code constructions lies in the use of different grids for the spline-wavelet transform and in the choice of bent functions of various degrees. The developed design of a robust code has a lower probability of error concealment in the case of using a high-degree bent function, while a lesser degree entails a faster coding time compared to existing robust codes. These code constructions can be used to protect against side-channel attacks when storing and transmitting information in communication systems.

Keywords
robust codes, bent functions, spline-wavelet decomposition of information, side channel attacks, attack on computational errors

Acknowledgements
This work was supported by the Ministry of Science and Higher Education of the Russian Federation, the state Assignment No. 075-01024-21-02 dated 29.09.2021 (the project No. FSEE-2021-0015).

For citation: Levina A.B., Ryaskin G.A. Spline-wavelet bent robust codes. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 6, pp. 936–941 (in Russian). doi: 10.17586/2226-1494-2021-21-6-936-941

Введение

Вейвлетное преобразование стало широко известным и используемым во многих областях науки начиная с 1982 года [1, 2]. Основные понятия вейвлетного преобразования можно найти в работе Добеши [3]. Теория вейвлетов нашла применение в таких технических областях, как сжатие данных, анализ сигналов и системах связи [1–4].

Одно из новых направлений приложения теории вейвлетов — помехоустойчивые коды [4–13]. Коды, обнаруживающие ошибки, используются для защиты в телекоммуникационных каналах, они обеспечивают надежность и безопасность устройств, осуществляют защиту от программных ошибок, а также защиту от атак по сторонним каналам [4–9, 11–13]. Основной задачей помехоустойчивых кодов является обеспечение связи в каналах таким образом, чтобы принимающая сторона могла обнаруживать и исправлять ошибки при передаче информации. Эта цель достигается с помощью алгоритмов помехоустойчивого кодирования, которые преобразуют информацию методом добавления дополнительных символов перед ее отправкой [4–13].

Осуществляя различные воздействия на аппаратные компоненты криптографического устройства с целью искажения информации, проводя при этом управление и анализ ошибок, злоумышленник может изменить информацию, передаваемую по каналу. Этот тип атаки называется атакой по ошибкам вычислений [4, 5]. Для обеспечения защиты от атак данного типа используются надежные коды, построенные на нелинейных функциях, так как линейные функции не обнаруживают все ошибки в канале из-за линейных свойств пространства [4, 5]. Применение бент-функций и сплайн-вейвлетов для построения надежного кода рассмотрено в работах [12, 13], но предложенные конструкции не обладают максимальным значением надежности и не структурированы. В работах [13–15] изучены свойства использования бент-функций различных степеней для улучшения параметров надежности, и предложена универсальная конструкция сплайн-вейвлет надежного бент-кода.

В настоящей работе исследованы свойства кодов, построенные на бент-функциях различных степеней и на сплайн-вейвлетном разложении. Данные конструкции кодов — надежны, так как не обладают необнаруживаемыми ошибками. Представлен универсальный метод построения данного класса кодов, выполнен анализ преимуществ и недостатков, а также проведено их сравнение с существующими надежными кодами.

Теоретический обзор

Линейные коды, которые используются в большинстве протоколов и стандартов передачи данных, не подходят для защиты от злонамеренных атак, поскольку всегда можно выбрать ошибку, которая не будет обнаружена получателем. Для решения этой проблемы Марк Карповский в своей работе [5] предложил использовать надежные коды, в настоящее время данный класс кодов активно исследуется с целью повышения уровня защиты информации от атак по ошибкам вычислений.

Определение. Надежные коды — это нелинейные коды, обнаруживающие ошибки в канале передачи данных.

Надежные коды обеспечивают равномерную защиту от всех ошибок без каких-либо предположений о распределении ошибок, возможностях и методах злоумышленника [4–9, 11–13].

Определение. Код $C \subseteq CF(2^n)$ называется R-надежным кодом, если область пересечения кода C и любого его дополнения $\tilde{C} = \{\tilde{x} | \tilde{x} = x + e, x \in C, e \in GF(2^n), e \neq 0\}$ ограничена сверху значением R: $R = \max\limits_{e \in GF(2^n)} |\{x | x \in C, x + e \in C\}|$, где «+» — покомпонентное сложение по модулю два; x — кодовое слово; e — ошибка [7, 8].

Пусть $M = |C|$ — количество кодовых слов в коде C. По определению R-надежного кода существует не более

R кодовых слов, которые не могут быть обнаружены для любой фиксированной ошибки e.

$$R = \max|\{x|x \in C, x + e \in C\}|.$$

Вероятность маскировки ошибки можно определить как:

$$Q(e) = \frac{|\{x|x \in C, x + e \in C\}|}{M}.$$

Один из основных критериев оценки эффективности надежного кода — максимальная вероятность маскирования ошибок:

$$\max Q(e) = \max \frac{|\{x|x \in C, x + e \in C\}|}{M} = \frac{R}{M}.$$

Использование линейных кодов не позволяет обнаружить все ошибки в канале передачи данных, как правило, они дают возможность только выявить ошибки с определенным весом Хэмминга. Надежные коды определяют все ошибки в канале с вероятностью не меньше, чем максимальная вероятность маскирования ошибок, но не позволяют исправлять ошибки из-за недостаточного для этого значения минимального кодового расстояния. Соответственно, чем меньше значение параметра максимальной вероятности маскировки ошибки, тем более защищенной является система от атак по ошибкам вычислений. Величина данного параметра косвенно связана с нелинейностью функции, которая используется при построении надежного кода.

Определение. Нелинейность функции f — расстояние от функции f до класса афинных функций. Обозначим нелинейность функции f в терминах N_f: $N_f = d(f, A(n)) = \min_{g \in A(n)} d(f, g)$, где $A(n)$ — класс линейных функций.

Для построения надежных кодов возможно использование различных классов нелинейных функций, в настоящей работе рассмотрим построение надежных кодов на максимально нелинейных функциях — бент-функциях различных степеней.

Впервые бент-функции были исследованы О. Ротхаусом в середине XX века. В настоящее время исследование бент-функций широко распространено, однако многие вопросы в этой теме остаются неизученными и требуют внимательного рассмотрения [14, 15].

Определение. Бент-функция — булева функция с четным числом переменных, для которой расстояние Хэмминга от множества аффинных булевых функций с одинаковым числом переменных является максимальным.

Функция $f \in P_2(n)$ называется максимально нелинейной, если $N_f = 2^{n-1} - 2^{(n/2)-1}$.

Рассмотрим надежные коды, построенные на бент-функциях, которые обладают минимальным параметром максимальной вероятности маскировки ошибок в сравнении с наиболее используемыми надежными кодами.

С точки зрения теории кодирования важными критериями, которым должна удовлетворять булева функция f из n переменных, являются следующие [14]:

1) Равновесие — функция f принимает значения 0 и 1 одинаково часто;

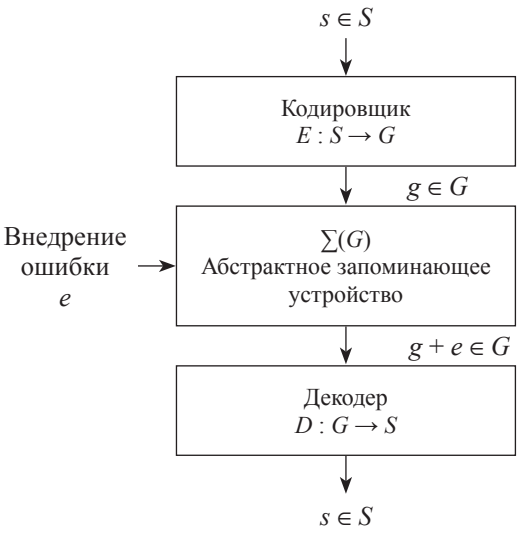

Рисунок. Вероятность обнаружения ошибок для разных конструкций кодов

Figure. Probability of error detection for different code constructions

2) Критерий распространения $PC(k)$ — для порядка k- для любого ненулевого вектора $y \in z_2^n$ весом не более k, результат функции $f(x + y) + f(x)$ сбалансировано;
3) Максимальная нелинейность — функция f такова, что значение ее нелинейности N_f максимально.

При атаке по сторонним каналам, злоумышленник имеет прямой доступ к физическому устройству. В процессе атаки он может вносить разные типы ошибок, которые не будут обнаруживаться приемным устройством, в силу различной частоты поступления кодовых слов, и может постоянно менять внедряемую ошибку. Общая модель атаки по сторонним вычислениям над абстрактным устройством хранения показана на рисунке.

Если используются надежные коды, ошибка будет обнаружена после определенного количества кодовых слов, но все может пойти по наихудшему сценарию — если злоумышленник адаптируется к последовательности наиболее повторяющихся кодовых слов. Следовательно, если есть алгоритм, который по определенным дополнительным параметрам сможет изменять алгоритм, не ухудшая параметры надежного кода, защищенность устройства от действий «умного» злоумышленника повысится. Выберем в качестве такого алгоритма — сплайн-вейвлет разложение информации.

Сплайн-вейвлет код на бент-функции

Идея вейвлет-преобразования основана на разбиении сигнала $s(t)$ на две составляющие — аппроксимирующую $A_m(t)$ и детализирующую $D_m(t)$:

$$s(t) = A_m(t) + \sum_{i=1}^{m} D_i(t),$$

где m — уровень декомпозиции (реконструкции).

Применим сплайн-вейвлетное разложение. Для сплайн-вейвлетного преобразования, кроме самого информационного потока, необходима сетка равной длины, состоящая из элементов того же поля, что и исходный поток.

С помощью сплайн-вейвлетных разложений создадим большое количество различных кодовых конструкций. Ключевая особенность данного метода — возможность изменения значений сетки при выполнении алгоритма. Следовательно, в качестве алгоритма изменения параметров надежного кода можно использовать сплайн-вейвлетную сетку. Более подробную информацию о сплайн-вейвлетах можно найти в [1, 2].

Приведем пример построения надежного кода на основе бент-функций и сплайн-вейвлетного преобразования со статической сеткой [13].

Пусть $c = \{c_1, c_2, \ldots, c_{n-1}, c_n\}$ — кодовое слово некоторого общего (n, k) кода, при этом $\{c_1, c_2, \ldots, c_{k-1}, c_k\}$ — информационная часть кода и $\{c_{k+1}, \ldots, c_n\}$ — дополнительная.

Сплайн-вейвлет бент надежный код со статической сеткой. В данной конструкции, для всех кодов, сетка выбирается как $x = \{x_1, x_2, \ldots, x_{n-1}, x_k\}$, любые элементы отбрасываются по усмотрению специалиста. Количество выброшенных предметов равно $(n - k)/2$. Количество символов строго четное и кратное 4, отношение $\frac{k}{n} = \frac{2}{3}$. Извлеченные элементы обозначены множеством $z = \{z_1, \ldots, z_{(n-k)/2}\}$, элементы вейвлета — $b = \{b_1, \ldots, b_{(n-k)/2}\}$. Пусть $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ — вектор поля $GF(2^n)$, $1 \le i \le n$. Вектор $\mathbf{c}$ принадлежит кодовому слову, если

$$c_{k+j} = b_j = c_{z_i} + c_{z_i+1} + \\ + (x_{z_i+2} + x_{z_i-1})(x_{z_i+2} + x_{z_i})^{-1}(c_{z_i-1} + c_{z_i+1}).$$

При этом для четного z_i:

$$c_{k+j+(n-k)/2} = c_1c_2 + \ldots + b_jc_{z_i-1} + \ldots + c_{k-1}c_k;$$

для нечетного z_i:

$$c_{k+j+(n-k)/2} = c_1c_2 + \ldots + b_jc_{z_i+1} + \ldots + c_{k-1}c_k,$$

где $1 \le j \le (n - k)/2$; k — количество символов четности в коде; $z_i \in z$; «+» — сложение по модулю 2; $c_{k+j+(n-k)/2}$ — элемент бент-функции.

Функцией для дополнительных элементов в конструкции служит бент-функция (код Кердока), элементами которой являются информационные элементы и сплайн-вейвлет элементы. В результате строится новая бент-функция, степень которой зависит от сплайн-вейвлетной сетки. Более подробную информацию о данных конструкциях надежного кода можно найти в [13].

Для приведенного примера степень бент-функции равна 2, но если использовать сплайн-вейвлет сетку на основе информационного слова, то степень бент-функции увеличивается до 3, и уменьшается параметр максимальной вероятности маскировки ошибки. В результате возникает предположение, что увеличение степени бент-функции может дать наилучшие значения для параметра R и уменьшить параметр максимальной вероятности маскировки ошибки, что проверено в рамках настоящей работы.

Сплайн-вейвлетный код на бент-функции с различными степенями

При использовании надежных кодов для защиты от атак по ошибкам вычислений параметр R является более важным. Используя сплайн-вейвлеты, можно создавать большое количество надежных кодов, строить бент-функции и увеличивать их степень, тем самым улучшая качество надежных кодов.

Рассмотрим функции с разными степенями на основе сплайн-вейвлетов и информационных символов для $n = 8$ и сравним по параметру R. Степень бент-функции не может превышать значение $n/2$ [14], и поэтому максимальная степень бент-функции от 8 элементов будет равняться 4. Чем больше число переменных, тем более высокой степенью может обладать бент-функция.

Построим бент-функции разных степеней для данной длины информационного слова на основе сплайн-вейвлетного разложения информации.

Для всех функций сплайн-вейвлетный элемент вычислим из одной и той же функции:

$$Wave_k = c_k - c_{k+1} - (x_{k+2} - x_{k-1})\,(x_{k+2} - x_k)^{-1}(c_{k-1} - c_{k+1}).$$

Функции для $n = 8$ представлены в табл. 1 и приведены с учетом условий сетки и степени функции. Все функции являются бент-функциями независимо от значений сетки.

Таблица 1. Сплайн-вейвлет бент-функции для $n = 8$

Table 1. Spline wavelet bent function for $n = 8$

Номер функции	Сетка	Функция	Deg(f) — степень функции
1	$x_i = c_i$	$f_i = c_{i+1}c_{i+3}c_{i+4} + c_{i+2}c_{i+3}c_{i+5} + Wave_{i+2}c_{i+6} + c_ic_{i+3} + c_ic_{i+5} + c_{i+2}c_{i+3} + c_{i+2}c_{i+4} + c_{i+2}c_{i+5} + c_{i+3}c_{i+4} + c_{i+3}c_{i+5} + c_{i+6}c_{i+7}$	4
2	Статичная	$f_i = c_{i+1}c_{i+3}c_{i+4} + c_{i+2}c_{i+3}c_{i+5} + Wave_{i+2}c_{i+6} + c_ic_{i+3} + c_ic_{i+5} + c_{i+2}c_{i+3} + c_{i+2}c_{i+4} + c_{i+2}c_{i+5} + c_{i+3}c_{i+4} + c_{i+3}c_{i+5} + c_{i+6}c_{i+7}$	2
3	Статичная	$f_i = c_ic_{i+1}Wave_{i+2} + c_{i+1}c_{i+3}Wave_{i+4} + c_ic_{i+1} + c_ic_{i+3} + c_{i+1}c_{i+5} + c_{i+2}c_{i+4} + c_{i+3}c_{i+4} + c_{i+6}c_{i+7}$	3
4	$x_i = c_{7-i}$	$f_i = c_ic_{i+1} + Wave_{i+2}c_{i+3} + c_{i+4}c_{i+5} + c_{i+6}c_{i+7}$	4
5	Статичная	$f_i = c_ic_{i+1} + Wave_{i+2}c_{i+3} + c_{i+4}c_{i+5} + c_{i+6}c_{i+7}$	2

Таблица 2. Параметр R и $Q(e)$ для $n = 8$
Table 2. Parameter R and $Q(e)$ for $n = 8$

Номер функции	Степень бент-функции	R	Максимальная вероятность сокрытия ошибок, $Q(e)$	Среднее значение времени, с
1	4	96	0,37500	0,071
2	2	128	0,50000	0,051
3	3	120	0,46875	0,062
4	4	96	0,37500	0,069
5	2	128	0,50000	0,049

Таблица 3. Сравнение сплайн-вейвлет надежных бент-кодов с надежными кодами
Table 3. Comparison of spline-wavelet robust bent codes with robust codes

Надежный код	R	Максимальная вероятность сокрытия ошибок, $Q(e)$	Среднее значение времени, с
Сплайн-вейвлет надежный код с функцией 1	96	0,375	0,071
Код Кердока	128	0,500	0,059
Надежный повторяющийся код	128	0,500	0,063

Из табл. 1 видно, что пары бент-функций 1 и 2, 4 и 5 — одинаковы и отличаются только в использовании типа сплайн-вейвлетной сетки. Построим новую конструкцию кода для всех вышеперечисленных функций с двумя избыточными символами $r_0 = f_0$, $r_1 = f_1$. Рассчитаем параметр R надежного кода, максимальную вероятность маскировки ошибок и время кодирования 6000 Б информационных векторов, результаты приведем в табл. 2.

Алгоритмы кодирования, построенные на вышеперечисленных функциях, являются надежными, так как максимальная вероятность сокрытия ошибок менее 1 — нет необнаруживаемых ошибок. Степень бент-функции равная 4, обладает более низким значением параметра R, тем самым понижая значение максимальной вероятности сокрытия ошибок и повышая вероятность обнаружения ошибки в канале в случае равновероятного появления кодовых слов. Если необходим баланс времени кодирования и параметра максимальной вероятности сокрытия ошибки, можно использовать бент-функцию степени 3. Используя сплайн-вейвлетное разложение в алгоритме кодировки, можно менять значения сетки, тем самым создавая различные между собой алгоритмы кодирования и увеличивать степень бент-функции, тем самым улучшая параметр R надежных кодов. Таким образом, специалист выбирает бент-функцию необходимой степени исходя из требований безопасности и времени кодирования. Можно определить более структурированную новую конструкцию сплайн-вейвлет бент-кода, которую специалист может внедрять с определенной бент-функцией и сеткой исходя из своей задачи.

Сплайн-вейвлет надежный код с меньшим значением *R*. Пусть $c = \{c_1, c_2, \ldots, c_{n-1}, c_n\}$ — кодовое слово некоторого общего (n, k) кода, при этом $\{c_1, c_2, \ldots, c_{k-1}, c_k\}$ — информационная часть кода, $\{c_{k+1}, \ldots, c_n\}$ — дополнительная, $n = k + 2$. Сетка выбирается в зависимости от вейвлет-функции сплайна, $f_i\{c_1, c_2, \ldots, c_{k-1}, c_m\}$ — функция из табл. 2. Вектор **c** принадлежит коду, если

$$c_{k+1} = f_0(c_1, \ldots, c_m) + c_{m+1}c_{m+2} + \ldots + c_{k-1}c_k;$$
$$c_{k+2} = f_1(c_1, \ldots, c_m) + c_{m+1}c_{m+2} + \ldots + c_{k-1}c_k.$$

Выполним сравнение построенных кодов по параметру R, $Q(e)$ и времени кодирования 6000 Б информации с существующими конструкциями надежных кодов той же длины. Результаты сравнения приведены в табл. 3.

Конструкция обеспечивает более высокий параметр защиты от атак по ошибкам вычислений в случае более высокой степени бент-функции, поскольку параметр R и максимальная вероятность маскирования ошибок $Q(e)$ ниже, чем у существующих решений.

Заключение

В работе предложена обобщенная конструкция надежного кода на основе сплайн-вейвлетных разложений и бент-функций различных степеней. Исследованы свойства бент-функций различных степеней при использовании в алгоритмах надежного кодирования информации. Более высокая степень бент-функции обладает более низким значением параметра R, тем самым понижая значение максимальной вероятности сокрытия ошибок и повышая вероятность обнаружения ошибки при хранении или передаче информации. Использование бент-функций степени 2 дает выигрыш по времени кодирования информации, но в ущерб параметрам надежности. Изменение используемой сплайн-вейвлетной сетки серьезно меняет параметры надежного кода. Предложенная обобщенная конструкция обеспечивает более высокий параметр защиты от атак по ошибкам вычислений при использовании бент-функций более высоких степеней.

Литература

1. Демьянович Ю.К., Ходаковский В.А. Введение в теорию вэйвлетов: учебное пособие. СПб.: Изд-во ПГУПС, 2008. 50 с.
2. Левина А.Б. Сплайн-вэйвлеты и их некоторые применения: диссертация на соискание ученой степени кандидата физико-математических наук / Санкт-Петербургский государственный университет. Москва, 2009. 215 с.
3. Добеши И. Десять лекций по вейвлетам. М., Ижевск: НИЦ «Регулярная и хаотическая динамика», 2004. 464 с.
4. Cramer R., Fehr S., Padró C. Algebraic manipulation detection codes // Science China Mathematics. 2013. V. 56. N 7. P. 1349–1358. https://doi.org/10.1007/s11425-013-4654-5
5. Karpovsky M.G., Kulikowski K., Wang Z. Robust error detection in communication and computation channels // Proc. of the International Workshop on Spectral Techniques. 2007.
6. Levina A., Taranov S. Spline-wavelet robust code under non-uniform codeword distribution // Proc. of the 3rd International Conference on Computer, Communication, Control and Information Technology (C3IT). 2015. P. 7060125. https://doi.org/10.1109/C3IT.2015.7060125
7. Levina A., Taranov S. Algorithms of constructing linear and robust codes based on wavelet decomposition and its application // Lecture Notes in Computer Science. 2015. V. 9084. P. 247–258. https://doi.org/10.1007/978-3-319-18681-8_20
8. Levina A., Taranov S. Second-order spline-wavelet robust code under non-uniform codeword distribution // Procedia Computer Science. 2015. V. 62. P. 297–302. https://doi.org/10.1016/j.procs.2015.08.453
9. Levina A., Taranov S. Creation of codes based on wavelet transformation and its application in ADV612 chips // International Journal of Wavelets, Multiresolution and Information Processing. 2017. V. 15. N 2. P. 1750014. https://doi.org/10.1142/S021969131750014X
10. Carlet C. Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010. P. 257–397. https://doi.org/10.1017/CBO9780511780448.011
11. Levina A.B., Carlet C., Taranov S.V. Algebraic manipulation detection codes with perfect nonlinear functions under non-uniform distribution // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 6. С. 1052–1062. https://doi.org/10.17586/2226-1494-2017-17-6-1052-1062
12. Levina A., Ryaskin G., Zikratov I. Spline-wavelet bent robust codes // Proc. of the Federated Conference on Computer Science and Information Systems (FedCSIS). 2019. P. 227–230. https://doi.org/10.15439/2019F134
13. Левина А.Б., Ряскин Г.А. Создание надежных кодов на основе бент-функций и вейвлет-преобразований // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6(118). С. 1008–1015. https://doi.org/10.17586/2226-1494-2018-18-6-1008-1015
14. Токарева Н.Н. Нелинейные булевы функции: бент-функции и их обобщения: Теоретические результаты. Saarbrucken, Germany: LAP LAMBERT Academic Publishing, 2011.180 с.
15. Carlet C., Mesnager S. Four decades of research on bent functions // Designs, Codes, and Cryptography. 2016. V. 78. N 1. P. 5–50. https://doi.org/10.1007/s10623-015-0145-8

References

1. Dem'yanovich Yu.K., Khodakovskii V.A. *Introduction to Wavelet Theory*. Tutorial. St. Petersburg, PSURT Publ., 2008, 50 p. (in Russian)
2. Levina A.B. *Spline Wavelets and Some Applications*. Dissertation for the degree of candidate of physical and mathematical sciences. Moscow, 2009, 215 p. (in Russian)
3. Daubechies I. *Ten Lectures on Wavelets*. Philadelphia, SIAM, 1992, 376 p.
4. Cramer R., Fehr S., Padró C. Algebraic manipulation detection codes. *Science China Mathematics*, 2013, vol. 56, no. 7, pp. 1349–1358. https://doi.org/10.1007/s11425-013-4654-5
5. Karpovsky M.G., Kulikowski K., Wang Z. Robust error detection in communication and computation channels. *Proc. of the International Workshop on Spectral Techniques*, 2007.
6. Levina A., Taranov S. Spline-wavelet robust code under non-uniform codeword distribution. *Proc. of the 3rd International Conference on Computer, Communication, Control and Information Technology (C3IT)*, 2015, pp. 7060125. https://doi.org/10.1109/C3IT.2015.7060125
7. Levina A., Taranov S. Algorithms of constructing linear and robust codes based on wavelet decomposition and its application. *Lecture Notes in Computer Science*, 2015, vol. 9084, pp. 247–258. https://doi.org/10.1007/978-3-319-18681-8_20
8. Levina A., Taranov S. Second-order spline-wavelet robust code under non-uniform codeword distribution. *Procedia Computer Science*, 2015, vol. 62, pp. 297–302. https://doi.org/10.1016/j.procs.2015.08.453
9. Levina A., Taranov S. Creation of codes based on wavelet transformation and its application in ADV612 chips. *International Journal of Wavelets, Multiresolution and Information Processing*, 2017, vol. 15, no. 2, pp. 1750014. https://doi.org/10.1142/S021969131750014X
10. Carlet C. Boolean functions for cryptography and error-correcting codes. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Cambridge University Press, 2010, pp. 257–397. https://doi.org/10.1017/CBO9780511780448.011
11. Levina A.B., Carlet C., Taranov S.V. Algebraic manipulation detection codes with perfect nonlinear functions under non-uniform distribution. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 6, pp. 1052–1062. https://doi.org/10.17586/2226-1494-2017-17-6-1052-1062
12. Levina A., Ryaskin G., Zikratov I. Spline-wavelet bent robust codes. *Proc. of the Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2019, pp. 227–230. https://doi.org/10.15439/2019F134
13. Levina A.B., Ryaskin G.A. Robust codes creation based on bent-functions and wavelet transformation. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 6(118), pp. 1008–1015. (in Russian). https://doi.org/10.17586/2226-1494-2018-18-6-1008-1015
14. Tokareva N.N. *Nonlinear Boolean Functions: Bent Functions and Their Generalizations*. Saarbrucken, Germany, LAP LAMBERT, 2011, 180 p. (in Russian)
15. Carlet C., Mesnager S. Four decades of research on bent functions. *Designs, Codes, and Cryptography*, 2016, vol. 78, no. 1, pp. 5–50. https://doi.org/10.1007/s10623-015-0145-8

Авторы

Левина Алла Борисовна — кандидат физико-математических наук, доцент, доцент, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197376, Российская Федерация, SC 56427692900, https://orcid.org/0000-0003-4421-2411, alla_levina@mail.ru

Ряскин Глеб Александрович — инженер, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, 197376, Российская Федерация, SC 57211483428, https://orcid.org/0000-0003-3046-0473, Ryaskinkgleb20@gmail.ru

Authors

Alla B. Levina — PhD, Associate Professor, Associate Professor, Saint Petersburg State Electrotechnical University (LETI), Saint Petersburg, 197376, Russian Federation, SC 56427692900, https://orcid.org/0000-0003-4421-2411, alla_levina@mail.ru

Gleb A. Ryaskin — Engineer, Saint Petersburg State Electrotechnical University (LETI), Saint Petersburg, 197376, Russian Federation, SC 57211483428, https://orcid.org/0000-0003-3046-0473, Ryaskinkgleb20@gmail.ru

Статья поступила в редакцию 01.11.2021
Одобрена после рецензирования 08.11.2021
Принята к печати 30.11.2021

Received 01.11.2021
Approved after reviewing 08.11.2021
Accepted 30.11.2021