Научная статья
УДК 519.872
https://doi.org/10.31854/1813-324X-2026-12-3-7-15
EDN:BOSQJI

Повышение нелинейности булевых функций адаптивной модификацией вейвлет-спектра

Алла Борисовна Левина✉, alla_levina@mail.ru
Никита Андреевич Панченко, n9218972301@gmail.com

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова, Санкт-Петербург, 197022, Российская Федерация.

Аннотация

Актуальность. *Булевы функции являются основой современных криптографических систем и алгоритмов шифрования, хеширования и генерации псевдослучайных последовательностей. Их ключевые свойства – высокая нелинейность и сбалансированность. Однако традиционные методы построения булевых функций с высокой нелинейностью основаны на применении бент-функций, которые обладают идеальными спектральными свойствами, но ограничены областью существования (только для четного числа переменных) и требуют сложных алгебраических конструкций. Это создает противоречие между теоретической оптимальностью бент-структур и их низкой практической реализуемостью. Таким образом, актуальной научной задачей является разработка методов формирования булевых функций, приближенных по спектральным характеристикам к бент-функциям, но пригодных для практического применения.*

Цель исследования *заключается в повышении нелинейности булевых функций за счет разработки метода адаптивной модификации детализирующих коэффициентов вейвлет-разложения, позволяющего перераспределять спектральную энергию и усиливать высокочастотные компоненты без усложнения алгебраической структуры функций.*

Для достижения цели использованы ***методы*** *спектрального анализа, дискретного вейвлет-преобразования Хаара, алгоритмизация и экспериментальное моделирование. Вейвлет-анализ применяется не только для декомпозиции функции, но и как инструмент управляемого спектрального преобразования.*

Решение. *Предложен метод адаптивной коррекции детализирующих коэффициентов вейвлет-разложения, обеспечивающий перераспределение спектральной плотности в сторону высокочастотных компонент. Проведены эксперименты для булевых функций размерностей n = 8, 10 и 12, подтверждающие увеличение спектральной нелинейности на 12–18 % по сравнению с исходными функциями.*

Новизна. *Впервые предложено применение дискретного вейвлет-преобразования для целенаправленного повышения спектральной нелинейности булевых функций. Ранее оно использовалось преимущественно для анализа сигналов. Введена формула адаптивной модификации детализирующих коэффициентов, позволяющая управлять спектральной структурой функций без привлечения сложных алгебраических преобразований.*

Теоретическая значимость *работы состоит в обосновании нового подхода к формированию булевых функций на основе спектрального моделирования вейвлет-коэффициентов.*

Практическая значимость *результатов заключается в том, что предложенный подход открывает возможность для дальнейшей автоматизации процессов синтеза булевых функций и S-блоков с заданными спектральными характеристиками. Это может быть использовано при разработке новых стандартов шифрования и оценке стойкости алгоритмов к перспективным видам криптоанализа.*

Ключевые слова: *булевы функции, вейвлет-преобразование, нелинейность, спектр Уолша, криптография*

Ссылка для цитирования: Левина А.Б., Панченко Н.А. Повышение нелинейности булевых функций адаптивной модификацией вейвлет-спектра // Труды учебных заведений связи. 2026. Т. 12. № 3. С. 7–15. DOI:10.31854/1813-324X-2026-12-3-7-15. EDN:BOSQJI

Original research
https://doi.org/10.31854/1813-324X-2026-12-3-7-15
EDN:BOSQJI

Increasing the Nonlinearity of Boolean Functions by Adaptive Wavelet Spectrum Modification

Alla B. Levina✉, alla_levina@mail.ru
Nikita A. Panchenko, n9218972301@gmail.com

Saint-Petersburg Electrotechnical University "LETI",
St. Petersburg, 197022, Russian Federation

Annotation

Relevance. *Boolean functions are the foundation of modern cryptographic systems and algorithms for encryption, hashing, and pseudorandom sequence generation. Their key properties are high nonlinearity and balancedness. However, traditional methods for constructing Boolean functions with high nonlinearity are based on the use of bent functions, which have ideal spectral properties but are limited in their domain of existence (only for an even number of variables) and require complex algebraic constructions. This creates a contradiction between the theoretical optimality of bent structures and their low practical feasibility. Therefore, a pressing scientific challenge is the development of methods for generating Boolean functions with spectral characteristics close to bent functions, but suitable for practical application.* ***The aim of this study*** *is to improve the nonlinearity of Boolean functions by developing a method for adaptively modifying the detailing coefficients of wavelet decomposition, allowing for the redistribution of spectral energy and enhancement of high-frequency components without complicating the algebraic structure of the functions.*

Methods. *Spectral analysis, the discrete Haar wavelet transform, algorithmization, and experimental modeling were used to achieve this goal. Wavelet analysis is used not only for function decomposition but also as a tool for controlled spectral transformation.*

Solution. *An algorithm for adaptively correcting the detailing coefficients of wavelet decomposition is proposed, ensuring the redistribution of spectral density toward high-frequency components. Experiments were conducted for Boolean functions of dimensions n = 8, 10, and 12, confirming an increase in spectral nonlinearity by 12–18 % compared to the original functions. Novelty. This paper proposes for the first time the use of a discrete wavelet transform to purposefully enhance the spectral nonlinearity of Boolean functions. Previously, it was used primarily for signal analysis. A formula for adaptive modification of detailing coefficients is introduced, allowing for control of the spectral structure of functions without resorting to complex algebraic transformations.*

The theoretical significance *of this work lies in the substantiation of a new approach to generating Boolean functions based on spectral modeling of wavelet coefficients.*

The practical significance *of the results lies in the fact that the proposed approach opens the possibility of further automating the synthesis of Boolean functions and S-boxes with specified spectral characteristics. This can be used in the development of new encryption standards and in assessing the resistance of algorithms to advanced types of cryptanalysis.*

Keywords: *boolean functions, wavelet transform, nonlinearity, Walsh spectrum, cryptography*

For citation: Levina A.B., Panchenko N.A. Increasing the Nonlinearity of Boolean Functions by Adaptive Wavelet Spectrum Modification. *Proceedings of Telecommunication Universities.* 2026;12(3):7–15. (in Russ.) DOI:10.31854/1813-324X-2026-12-3-7-15. EDN:BOSQJI

ВВЕДЕНИЕ

Булевы функции являются ключевыми компонентами современных криптографических систем, они применяются при построении шифров, хеш-функций и генераторов псевдослучайных последовательностей. Для обеспечения стойкости к криптоанализу важнейшими свойствами функций выступают высокая нелинейность, сбалансированность и устойчивость к линейным и дифференциальным атакам [1, 2]. Эталоном в этой области слу-

жат бент-функции, обладающие максимальной нелинейностью и равномерным спектром Уолша. Однако их практическое применение ограничено, они существуют только для четного числа переменных, не являются сбалансированными и требуют сложных алгебраических конструкций [2, 3]. Классические методы их построения масштабируются плохо, что делает невозможным использование бент-функций в реальных криптосистемах.

В настоящее время актуальной задачей является разработка методов формирования булевых функций, приближенных по спектральным характеристикам к бент-структуре, но более удобных для практического использования [4–6]. Традиционные подходы основаны на преобразовании Уолша – Адамара [5], которое эффективно для спектрального анализа, но не позволяет локально управлять спектром функции.

Перспективным инструментом для решения этой задачи является дискретное вейвлет-преобразование, позволяющее разложить функцию на многомасштабные компоненты и модифицировать ее высокочастотные характеристики. В отличие от ряда предыдущих исследований [5], где вейвлет-преобразование применялось исключительно для анализа, в данной работе предлагается его использование для спектральной модификации булевых функций. Цель работы – разработать метод адаптивной коррекции детализирующих коэффициентов вейвлет-разложения, увеличивающего нелинейность булевых функций без усложнения их алгебраической структуры.

ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

Булевые функции и спектр Уолша

Булевы функции играют ключевую роль в современных информационных технологиях, особенно в областях криптографии и теории кодирования.

Определение 1. Булева функция – это отображение вида:

$$f: F_2^n \to F_2,$$

где $F_2^n = \{0,1\}$ – поле, состоящее из двух элементов; n – количество переменных функции.

Одним из важнейших направлений использования булевых функций является криптография. Булевы функции применяются при построении S-блоков, генераторов псевдослучайных последовательностей и хеш-функций, которые определяют стойкость шифров. Для обеспечения криптографической стойкости булевы функции должны обладать рядом специфических свойств, в первую очередь, высокой нелинейностью, сбалансированностью и устойчивостью к линейному и дифференциальному анализу [1, 2].

Нелинейность функции – это минимальное расстояние по Хэммингу между функцией и множеством всех аффинных функций:

$$NL(f) = \min_{g \in A_n} d_H(f, g), \quad (1)$$

где A_n – множество всех аффинных функций; $d_H(f, g)$ – расстояние по Хэммингу между функциями f и g [2, 7].

Чем выше нелинейность, тем более затруднено применение различных аналитических атак, особенно тех, которые используют линейные, или близкие к линейной зависимости. Эта характеристика функций является одной из ключевых при проектировании компонентов шифров, таких как S-блоки и поточные генераторы. Еще одним важным криптографическим свойством булевых функций является сбалансированность.

Определение 2. Булева функция называется сбалансированной, если она принимает значения 0 и 1 одинаковое количество раз на всем множестве входов.

В криптографии сбалансированность важна для того, чтобы выход функции был непредсказуемым, если функция склоняется к одному значению, это может дать возможность атаки через статистический анализ.

Анализ булевых функций с точки зрения их криптографических характеристик требует не только изучения их структурных свойств, таких как сбалансированность и нелинейность, но и применения спектральных методов. Одним из наиболее эффективных методов спектрального анализа является преобразование Уолша – Адамара, позволяющее описать булеву функцию в частотной области и получить точные численные характеристики [2, 7, 8].

Преобразование Уолша – Адамара функции f представляет собой целочисленную функцию, которая задана на множестве Z_2^n равенством:

$$W(v) = \sum_{u \in Z_2^n} (-1)^{\langle u,v \rangle \oplus f(u)}, \quad (2)$$

где $\langle u, v \rangle$ – скалярное произведение векторов по модулю 2.

Спектр Уолша отражает корреляцию функции с линейными функциями. Чем выше значение спектра, тем выше корреляция с соответствующей функцией, что нежелательно для криптографии [1, 8].

Рассмотрим основные свойства спектра Уолша.

1) Равенство Парсеваля показывает сохранение энергии при переходе из временно́й области в спектральную:

$$\sum\nolimits_{u \in Z_2^n} (W(v))^2 = 2^{2n}. \quad (3)$$

2) Связь с нелинейностью функции. Значение нелинейности булевой функции выражается через значение спектра. Чем меньше максимальное значение спектра Уолша, тем выше нелинейность функции.

Нелинейность можно рассчитать по формуле:

$$NL(f) = 2^{n-1} - \frac{1}{2} * \max_{u} |W_f(u)|. \quad (4)$$

3) Сбалансированность функции. Функция, которая принимает значения 0 и 1 одинаковое количество наборов; если она сбалансирована, то выполняется равенство:

$$W_f(0) = 0.$$

Спектр Уолша не только предоставляет количественное описание корреляционных свойств булевой функции, но и служит основным инструментом для анализа ее нелинейности – ключевого критерия криптографической стойкости. Это позволяет выделить особый подкласс – бент-функции, обладающие экстремальными спектральными свойствами.

Определение 3. Бент-функция – это булева функция, у которой значения всех коэффициентов спектра Уолша равна $\pm 2^{\frac{n}{2}}$:

$$|W(v)| = 2^{\frac{n}{2}}.$$

Модуль всех коэффициентов спектра Уолша является постоянным и достигает теоретического максимума [2, 7]. Это свойство делает бент-функции идеальными с точки зрения спектральных характеристик.

Особенности бент-функций:

– существуют только для четного n [2, 7];

– несбалансированные (число единиц и нулей различается);

– спектр строго равномерный по модулю.

В криптографии бент-функции используются как базовые блоки при построении более сложных структур, таких как векторные функции (S-блок), защищенные генераторы ключевого потока и хеш-функции.

Дискретное вейвлет-преобразование

Одним из ключевых подходов к анализу и формированию булевых функций с высокой нелинейностью является спектральный метод. Традиционно для этих целей используется преобразование Уолша – Адамара, позволяющее оценить отклонение булевой функции от линейных отображений. Однако данный подход не обеспечивает локальной оценки структуры функции, поскольку глобален по своей природе.

Вейвлет-преобразование предлагает альтернативный и дополнительно информативный способ представления булевой функции в виде совокупности частотно-локализованных компонент. Оно позволяет рассматривать структуру функции на множестве масштабов, идентифицируя как общую тенденцию ее изменения (аппроксимацию), так и локальные вариации (детализацию). Переход к вейвлет-представлению открывает возможность направленного управления локальной спектральной структурой функции, что может быть использовано для формирования или модификации функций с целевой нелинейностью.

Дискретное вейвлет-преобразование – математическое преобразование цифрового сигнала, при котором определяются локальные особенности сигнала в различных частотных диапазонах без потери информации о временно́й структуре. Теоретический фундамент дискретного вейвлет-преобразования базируется на предложенной С. Малла концепции многомасштабного анализа [9] и теории построения компактных ортогональных базисов, детально изложенной в трудах И. Добеши [10]. В отличие от глобального преобразования Уолша – Адамара, вейвлет-анализ позволяет выявлять локальные особенности функции. Применение дискретного вейвлет-преобразования к анализу дискретных структур и функций на конечных интервалах обосновано в работах Ю.К. Демьяновича [11], где вейвлет-разложения рассматриваются как эффективный инструмент адаптивной аппроксимации.

На практике дискретного вейвлет-преобразования прямое использование вейвлет-функций и функций масштабирования очень затруднено и ресурсоемко: необходимо генерировать все их сдвиги и масштабы, а также вычислять большое количество численных интегралов или скалярных произведений. Поэтому для удобства вычисления основным методом реализации данного типа преобразования является использование цифровых фильтров. При данном методе выполняется линейная фильтрация и субдискретизация сигнала [8, 12].

В рамках дискретного вейвлет-преобразования используются два основных фильтра:

– низкочастотный $h[n]$ (с помощью данного фильтра из сигнала извлекается его аппроксимирующая составляющая, а именно сглаженное, крупномасштабное приближение);

– высокочастотный $g[n]$ (данный фильтр выделяет детализирующую информацию сигнала, а именно его высокочастотные особенности: скачки, шум, границы).

Эти фильтры реализуются как конечные последовательности коэффициентов, соответствующие выбранному семейству вейвлетов. На практике фильтрация выполняется как свертка сигнала $x[n]$ с соответствующим фильтром, за которой следует процедура субдискретизации:

$$A[n] = \sum_{k=0} h[k] \cdot x[2n-k],$$
$$D[n] = \sum_{k=0} g[k] \cdot x[2n-k], \quad (5)$$

где $A[n]$ – аппроксимирующие коэффициенты; $D[n]$ – детализирующие коэффициенты; $h[k]$ и $g[k]$ – коэффициенты фильтров низких и высоких частот соответственно.

Аппроксимирующие и детализирующие коэффициенты представляют собой разложение сигнала на его структурные уровни, глобальные формы и локальные особенности. Они позволяют эффективно анализировать сигналы, выявлять важные события и изменения, а также применять преобразование к задачам в различных областях.

Аппроксимирующие коэффициенты несут информацию о глобальной структуре сигнала, включая его форму, тренды и медленно изменяющиеся характеристики. Они отвечают за крупномасштабное приближение сигнала и позволяют анализировать его на более общем уровне, без учета мелких деталей. Значения этих коэффициентов отражают степень выраженности медленно изменяющихся компонентов сигнала в различных временны́х интервалах.

Детализирующие коэффициенты, напротив, отражают локальные особенности сигнала, такие как границы, переходы, всплески, шумовые выбросы и другие высокочастотные компоненты, они критически важны для анализа резких переходов в сигнале, позволяя точно определить места, где происходят значимые изменения. Интерпретируя значения детализирующих коэффициентов, можно судить о характере и интенсивности изменений в сигнале, высокие значения по модулю свидетельствуют о резких изменениях, таких как обрыв, край или шумовой пик, тогда как значения, близкие к нулю, указывают на гладкий и однородный участок.

Одним из наиболее простых примеров дискретного вейвлет-преобразования является преобразование Хаара. Данное преобразование представляет исходный сигнал в виде набора аппроксимирующих и детализирующих коэффициентов, которые рассчитываются по формулам:

$$a_k = \frac{f_{2k} + f_{2k+1}}{\sqrt{2}}, d_k = \frac{f_{2k} - f_{2k+1}}{\sqrt{2}}. \quad (6)$$

Вейвлет Хаара широко используется при реализации дискретного вейвлет-преобразования благодаря простоте его структуры и вычислительной реализации, что позволяет получить поуровневое разложение функции без усложнения алгоритмической реализации.

МЕТОД АДАПТИВНОЙ МОДИФИКАЦИИ ВЕЙВЛЕТ-КОЭФФИЦИЕНТОВ

Булевы функции занимают ключевое место в криптографии, теории кодирования и построении логических схем. Особый интерес в этих приложениях вызывают функции с высокой нелинейностью, поскольку именно они обеспечивают устойчивость к линейному и дифференциальному криптоанализу. Соответственно, одной из важных задач является генерация функций с такими свойствами. Одним из подходов к решению этой задачи является использование спектральных методов анализа, в частности вейвлет-преобразований, позволяющих локализовать высокочастотные особенности функции. Ключевую роль в таких анализах играют детализирующие коэффициенты, изменение которых может существенно повлиять на спектральную структуру функции и, как следствие, на ее нелинейность [8, 13]. Именно детализирующие коэффициенты вейвлет-преобразования определяют наличие скрытых линейных зависимостей, предсказуемость поведения и криптографическую стойкость функции. Их анализ и контролируемая модификация являются основой предлагаемого метода.

На рисунке 1 представлены детализирующие коэффициенты дискретного вейвлет-преобразования (вейвлет Хаара) для булевых функций при $n = 6$.

Можно сделать следующие выводы:

– в линейной функции (рисунок 1a), представленной формулой $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1 \oplus x_2$, доминируют нулевые значения, что отражает минимальную частотную сложность;

– средне нелинейная функция (рисунок 1b), представленная формулой $f(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1 \wedge x_2) \oplus x_3$, демонстрирует более разнообразную и сложную структуру, но при этом распределение коэффициентов остается неравномерным;

– бент-функция (рисунок 1c), имеющая вид $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_4x_6$, показывает наибольшую плотность и равномерность в распределении детализирующих коэффициентов.

Значения коэффициентов бент-функции разбросаны по всему набору уровней преобразования и обладают высокой амплитудой, что указывает на отсутствие локальной гладкости. Поскольку структура детализирующих коэффициентов определяет нелинейность функции, ее спектральную плоскость и устойчивость, модификация этих коэффициентов позволяет управляемо приближать произвольную булеву функцию к бент-структуре. Целью такой модификации является перераспределение спектральной энергии в сторону более равномерного покрытия высокочастотных компонент, а также подавление доминирующих низкочастотных элементов [7, 8].

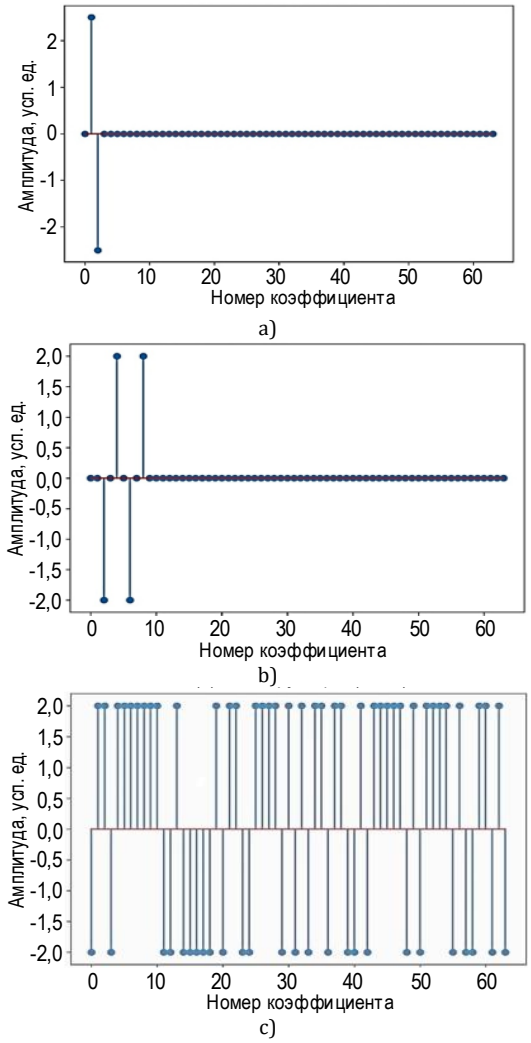

Рис. 1. Детализирующие коэффициенты разных видов функций

Fig. 1. Detailing Coefficients for Different Types Functions

Для достижения этой цели рассмотрим метод модификации, применяемый к произвольной булевой функции.

Входные данные:

– булева функция F;

– параметры модификации (масштабирующий коэффициент, порог модификации, случайное отклонение, шумовой сдвиг).

Выходные данные:

– новая булева функция $\hat{F}$;

– нелинейность новой функции $NL(\widehat{F})$.

Этап 1. Преобразование в вещественную форму.

Для применения дискретного вейвлет-преобразования к булевой функции необходимо представить ее в вещественной форме.

Бинарные значения функции $f(x) \in \{0,1\}$ преобразуются в вещественные по следующему правилу:

$$f'(x) = (-1)^{f(x)}. \quad (7)$$

Этап 2. Вычислить дискретное вейвлет-преобразование над $f'(x)$ с базисом Хаара и получить аппроксимирующие и детализирующие коэффициенты для всех уровней.

Этап 3. Модификация коэффициентов.

Произвести модификацию каждого детализирующего коэффициента, применяя формулу (8), где $d_{j,k}$ – исходный детализирующий коэффициент на уровне j, позиции k; T – порог модификации; A_j – масштабный коэффициент на уровне j; $\text{sign}(d_{j,k})$ – знак исходного коэффициента, сохраняющий направление воздействия; $\mu_{j,k}$ – случайная величина для внесения нерегулярности в амплитуду; $d_{\max}^{(j)}$ – максимальное значение детализирующего коэффициента на уровне j; $\varepsilon_{j,k}$ – шумовой сдвиг.

Этап 4. Произвести обратное дискетное вейвлет-преобразование по аппроксимирующим и модифицированным детализирующим коэффициентам. В результате будет получен сигнал $g(x)$.

$$d'_{j,k} = \begin{cases} d_{j,k}, & \text{если } |d_{j,k}| \geq T \\ A_j * \text{sign}(d_{j,k}) * (1 + \mu_{j,k}) * d_{\max}^{(j)} + \varepsilon_{j,k}, & \text{если } |d_{j,k}| < T \end{cases}. \quad (8)$$

Этап 5. Бинаризация.

Преобразовать полученный сигнал обратно в булеву функцию:

$$\widehat{f(x)} = \begin{cases} 1, & g(x) < \tau \\ 0, & g(x) \geq \tau \end{cases}.$$

В рамках предлагаемого метода на практике достаточно использовать фиксированное значение порога $\tau = 0$, что соответствует бинаризации по знаку сигнала. Однако при более сильной модификации вейвлет-коэффициентов может быть полезен адаптивный выбор порога (например, по среднему или медиане сигнала), либо подбор порога, оптимизирующего нелинейность на выходе.

Этап 6. Оценка нелинейности полученной функции и сравнить ее с исходной.

Основой данного метода является модификация детализирующих коэффициентов вейвлет-преобразования с помощью формулы (8). Эта формула была составлена на основе следующих операций, которые влияют на нелинейность функции:

1) локальное усиление слабых компонент (если модуль коэффициента меньше заданного порога, то он заменяется на псевдослучайное значение с фиксированной амплитудой; это позволяет воздействовать только на слабые детали, сохраняя основную структуру функции);

2) неравномерность в спектре позволяет устранить симметрии или регулярности, увеличивая спектральную неопределенность функции;

3) добавление нормированного шума, внедрение псевдослучайных небольших колебаний в равные или нулевые коэффициенты для разрушения регулярной структуры спектра.

Рассмотрим основные компоненты формулы (8) подробнее. Ее структура напрямую вытекает из описанных принципов и реализует их в виде кусочно-заданной функции. Метод разделяет обработку сигнала на два случая в зависимости от их абсолютного значения относительно порога T.

В таблице 1 рассмотрены назначение и способ вычисления основных параметров формулы (8).

ТАБЛИЦА 1. Описание параметров формулы

TABLE 1. Description of Formula Parameters

Параметр	Назначение	Значение
Порог модификации (T)	Определение коэффициентов, которые имеют очень маленькие значения. Коэффициенты, которые меньше данного порога, будут модифицироваться.	$T = \tau * d_{\max}^{(j)}$, $\tau \in [0{,}05; 0{,}2]$
Знак исходного коэффициента, $\text{sign}(d_{j,k})$	Функция знака сохраняет направление исходного колебания, предотвращая разрушение фазовой структуры. Это важно для стабильности спектра при обратном преобразовании.	$\text{sign}(d_{j,k}) = \begin{cases} -1, & d_{j,k} < 0 \\ 1, & d_{j,k} \geq 0 \end{cases}$
Максимальное значение детализирующего коэффициента на уровне j, $d_{\max}^{(j)}$	Данное значение делает величину модификации пропорциональной масштабу уровня и гарантирует относительное соответствие измененных значений спектру данного уровня.	$d_{\max}^{(j)} = \max(d_0^{(j)}, d_1^{(j)}, \dots, d_n^{(j)})$
Масштабный коэффициент на уровне j, A_j	Масштабный коэффициент уровня определяет интенсивность модификации слабых детализирующих коэффициентов на каждом уровне вейвлет-декомпозиции.	Формула для масштабного коэффициента: $A_j = A_0 * e^{-aj}$, где $A_0 \in [1{,}2; 1{,}5]$ – начальный уровень масштаба; $a \in [0{,}2; 0{,}4]$ – скорость затухания с глубиной уровня j.
Случайная величина для внесения нерегулярности в амплитуду, $\mu_{j,k}$	Данная величина вносит случайные колебания в амплитуду модифицированных коэффициентов. Это используется для того, чтобы избежать равномерности в спектре и разрушению линейной корреляции.	Значение данной величины является случайным числом из диапазона $[-\beta; \beta]$. Границы данного диапазона можно рассчитать по формуле: $\beta = 0{,}05 * d_{\max}^{(j)}$.
Шумовой сдвиг, $\varepsilon_{j,k}$	Данный шум добавляется к каждому модифицируемому коэффициенту. Это позволяет добавить дополнительную спектральную нестабильность и устранить симметричность спектра.	Шумовой сдвиг обычно вычисляется с помощью нормального распределения с нулевым средним: $\varepsilon_{j,k} \sim N(0, \sigma^2)$. При этом параметр этого распределения можно рассчитать по формуле: $\sigma = 0{,}05 * d_{\max}^{(j)}$.

ЭКСПЕРИМЕНТАЛЬНЫЕ РЕЗУЛЬТАТЫ

В данном разделе проводится проверка эффективности предложенного метода модификации детализирующих коэффициентов вейвлет-преобразования для повышения спектральной нелинейности булевых функций. Анализ включает как пример, позволяющий пошагово проследить изменение структуры функции, так и серию массовых экспериментов на булевых функциях от 8, 10 и 12 переменных [3]. Все функции преобразовывались из булевой формы $f(x)$ в вещественную по формуле (7). Затем применялось дискретное вейвлет-преобразование Хаара, модификация коэффициентов проводилась по предложенной в методе формуле, обратное преобразование и восстановление бинарного представления функции проводилось с использованием порога $\tau = 0$. Спектральная нелинейность оценивалась как для исходной, так и для модифицированной функции. Рассмотрим случайную булеву функцию от десяти переменных (9). Представим данную булеву функцию в вещественной форме (10).

$$f(x) = [0,1,0,1,1,0,0,1,0,0,1,1,0,1,1,0,1,0,1,0,0,1,1,0,0,1,0,1,1,0,0,1,\dots,0,1,1,0,1,0,0,1]. \quad (9)$$

$$f(x) = [1,-1,1,-1,-1,1,1,-1,1,1,-1,-1,1,-1,-1,1,-1,1,-1,1,1,-1,-1,1,1,-1,1,-1,-1,1,1,-1,\dots,1,-1,-1,1,-1,1,1,-1]. \quad (10)$$

Применим к ней преобразование Хаара. В результате данного преобразования вычисляются аппроксимирующие и детализирующие коэффициенты по формулам (6).

Для примера проведем детализирующие коэффициенты на пятом уровне:

$$d_5 = [0{,}12;\ -0{,}31;\ 0{,}05;\ 1{,}42; \dots; -0{,}08; 0{,}21].$$

После расчета всех уровней коэффициентов модифицируем детализирующие коэффициенты по формуле (8).

Рассчитаем параметры модификации для детализирующих коэффициентов пятого уровня:

$$\max(|d_5|) = 1{,}42,$$
$$T_5 = 0{,}1 * \max(|d_5|) = 0{,}142.$$

Согласно полученному порогу необходимо модифицировать 20 коэффициентов. Определим параметры формулы для данного уровня:

$$A_5 = 1{,}3 * e^{-0{,}3*5} \approx 0{,}29,$$
$$\mu \in [-0{,}071; 0{,}071],$$
$$\varepsilon \sim N(0; 0{,}005041).$$

По полученным параметрам произведем расчет новых детализирующих коэффициентов, приведем расчеты некоторых из них.

Для нулевого коэффициента:

$$d_5[0] = 0{,}29 * 1 * (1 + 0{,}03) * 1{,}42 - 0{,}01 \approx 0{,}42,$$

где $\mu = 0{,}03$ и $\varepsilon = -0{,}01$.

Для второго коэффициента:

$$d_5[2] = 0{,}29 * 1 * (1 + 0{,}07) * 1{,}42 + 0{,}07 \approx 0{,}51,$$

где $\mu = 0{,}07$ и $\varepsilon = 0{,}07$.

Для тридцатого коэффициента:

$$d_5[30] = 0{,}29 * (-1) * (1 + 0{,}071) * 1{,}42 - 0{,}09 \approx$$
$$\approx -0{,}53,$$

где $\mu = 0{,}071$ и $\varepsilon = -0{,}09$.

После всех модификаций детализирующие коэффициенты 5 уровня имеют следующий вид:

$$d_5 = [0{,}42;\ -0{,}31;\ 0{,}51;\ 1{,}42; \dots; -0{,}53; 0{,}21].$$

Аналогичные модификации производятся со всеми детализирующими коэффициентами на всех уровнях разложения. После модификации всех коэффициентов применяем обратное вейвлет-преобразование и получаем следующий вектор значений:

$$g(x) = [0{,}91; -1{,}24; 1{,}37; -0{,}85; -0{,}72; 0{,}63;$$
$$-1{,}08; 0{,}95, \dots].$$

Бинаризируем полученный вектор значений по формуле из этапа 5 метода модификации:

$$\widehat{f(x)} = [0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, \dots].$$

Произведем оценку нелинейности:

$$NL(f) = 368,$$
$$NL(\widehat{f}) = 436,$$
$$\Delta NL = 436 - 368 = 68.$$

Пример показал, что нелинейность функции в результате модификаций повысилась на 68 единиц.

Произведен эксперимент с помощью программных средств на 100 функциях при n = 8, 10, 12. Результаты эксперименты сведены в таблице 2.

ТАБЛИЦА 2. Результаты эксперимента

TABLE 2. Experimental Results

Размерность, *N*	Средняя исходная нелинейность	Средняя новая нелинейность	Среднее изменение нелинейности	Прирост нелинейности, %
8	100,3	112,1	11,8	11,8
10	372,6	438,9	66,3	17,8
12	1512,4	1756,2	243,8	16,1

При различных размерностях эксперимент демонстрирует прирост нелинейности на 12–18 %. Максимальный прирост нелинейности был при n = 10 и составил 17,8 %.

На рисунке 2 изображены графики нелинейности функций в зависимости от нелинейности. Графики демонстрируют, как предложенный метод приближает нелинейность к значениям бент-функции.

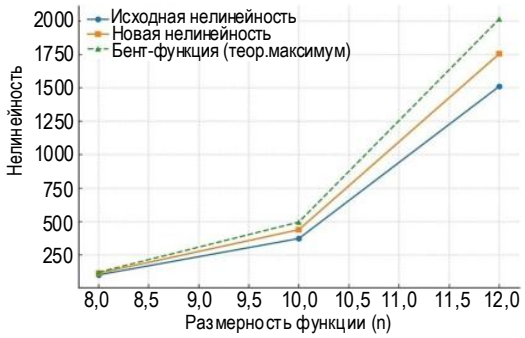

Рис. 2. Графическое представление приближения нелинейности к уровню бент-функций

Fig. 2. Comparison of Nonlinearity with Bent-Functions Level

ВЫВОД

Предложен метод повышения нелинейности булевых функций на основе адаптивной модификации детализирующих коэффициентов вейвлет-разложения Хаара. Экспериментально подтверждено, что селективное усиление слабых высокочастотных компонент спектра (60–65 % коэффициентов) обеспечивает прирост нелинейности на 12–18 % для функций размерности n = 8, 10, 12. Метод позволяет приближать свойства функций к бент-характеристикам без сложных алгебраических конструкций и применим для автоматизиро-

ванной генерации криптографически стойких S-блоков и хеш-функций. Дальнейшие исследования будут направлены на оптимизацию параметров модификации для больших n и анализ устойчивости к атакам.

Список источников

1. Carlet C. Boolean Functions for Cryptography and Error Correcting Codes. Cambridge University Press, 2007.
2. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. №1(3). С. 15–37. EDN:KGCEZH
3. Langevin P., Gillot V., Polujan A. Normality of 8-Bit Function // arXiv: 2504.21779. 2025. DOI:10.48550/arXiv.2504.21779
4. Carlet C., Đurasevic M., Jakobovic D., Picek S., Mariot L. A Systematic Study on the Design of Odd-Sized Highly Nonlinear Boolean Functions via Evolutionary Algorithms // arXiv: 2504.17666. 2025. DOI:10.48550/arXiv.2504.17666
5. Шибакин И.В., Левина А.Б. Алгоритм генерации бент-функций с помощью вейвлет-преобразования // Безопасность информационных технологий. 2025. Т. 32. № 4. С. 106–121. DOI:10.26583/bit.2025.4.08. EDN:EGISZJ
6. Carlet C., Đurasevic M., Jakobovic D., Mariot L., Picek S., Polujan A. On Counts and Densities of Homogeneous Bent Functions: An Evolutionary Approach // arXiv: 2511.12652. 2025. DOI:10.48550/arXiv.2511.12652
7. Pandey S.K., Dass B.K. On Walsh Spectrum of Cryptographic Boolean Function // Defence Science Journal. 2017. Vol. 67. Iss. 5. PP. 536–541. DOI:10.14429/dsj.67.10638
8. Штарк Г.Г. Применение вейвлетов для ЦОС. Пер. с англ. М.: Техносфера, 2007. 183 с.
9. Mallat S. A Wavelet Tour of Signal Processing: The Sparse Way. Academic Press, 2008. 832 p.
10. Добеши И. Десять лекций по вейвлетам. Пер. с англ. Ижевск: Регулярная и хаотическая динамика, 2001. 464 с.
11. Демьянович Ю.К., Ходаковский В.А. Введение в теорию вейвлетов: курс лекций. СПб., 2007. 49 с.
12. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в MATLAB. М.: ДМК Пресс, 2008. 448 с. EDN:RAZCLT
13. Jiang N., Zhuo Z., Chen G., Wang L. The Walsh transform of a class of Boolean functions // Wuhan University Journal of Natural Sciences. 2021. Vol. 26. Iss. 6. PP. 453–458. DOI:10.1051/wujns/2021266453. EDN:EJIKQK

References

1. Carlet C. *Boolean Functions for Cryptography and Error Correcting Codes*. Cambridge University Press, 2007.
2. Tokareva N.N. Bent Functions: Results and Applications. A Survey. *Prikladnaya Diskretnaya Matematika*. 2009:1(3):15-37. (in Russ.) EDN:KGCEZH
3. Langevin P., Gillot V., Polujan A. Normality of 8-Bit Function. *arXiv: 2504.21779*. 2025. DOI:10.48550/arXiv.2504.21779
4. Carlet C., Đurasevic M., Jakobovic D., Picek S., Mariot L. A Systematic Study on the Design of Odd-Sized Highly Nonlinear Boolean Functions via Evolutionary Algorithms. *arXiv: 2504.17666*. 2025. DOI:10.48550/arXiv.2504.17666
5. Shibakin I.V., Levina A.B. Algorithm for generation of bent functions using wavelet transform. *IT Security (Russia)*. 2025;32(4):106–121. (in Russ.) DOI:10.26583/bit.2025.4.08. EDN:EGISZJ
6. Carlet C., Đurasevic M., Jakobovic D., Mariot L., Picek S., Polujan A. On Counts and Densities of Homogeneous Bent Functions: An Evolutionary Approach. *arXiv: 2511.12652*. 2025. DOI:10.48550/arXiv.2511.12652
7. Pandey S.K., Dass B.K. On Walsh Spectrum of Cryptographic Boolean Function. *Defence Science Journal*. 2017;67(5):536–541. DOI:10.14429/dsj.67.10638
8. Stark H.-G. *Wavelets and Signal Processing: An Application-Based Introduction*. Springer, 2005. 160 p.
9. Mallat S. *A Wavelet Tour of Signal Processing: The Sparse Way*. Academic Press, 2008. 832 p.
10. Daubechies I. *Ten Lectures on Wavelets*. SIAM, 1992. 376 p.
11. Dem'yanovich Yu.K., Khodakovsky V.A. *Introduction to Wavelet Theory: Lecture Course*. St. Petersburg, 2007. 49 p. (in Russ.)
12. Smolentsev N.K. *Fundamentals of Wavelet Theory. Wavelets in MATLAB*. Moscow: DMK Press Publ.; 2008. 448 p. (in Russ.) EDN:RAZCLT
13. Jiang N., Zhuo Z., Chen G., Wang L. The Walsh transform of a class of Boolean functions. *Wuhan University Journal of Natural Sciences*. 2021;26(6):453–458. DOI:10.1051/wujns/2021266453. EDN:EJIKQK

Статья поступила в редакцию 07.10.2025; одобрена после рецензирования 11.04.2026; принята к публикации 13.04.2026.
The article was submitted 07.10.2025; approved after reviewing 11.04.2026; accepted for publication 13.04.2026.

Информация об авторах:

ЛЕВИНА Алла Борисовна — кандидат физико-математических наук, доцент, доцент кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова
https://orcid.org/0000-0003-4421-2411

ПАНЧЕНКО Никита Андреевич — аспирант кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова
https://orcid.org/0009-0003-5850-7154

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.