На правах рукописи

Шапоренко Александр Сергеевич

Построение бент-функций на основе их производных и связанные открытые вопросы

Специальность 1.2.3 —
«Теоретическая информатика, кибернетика»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск — 2024

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Новосибирский национальный исследовательский государственный университет».

Научный руководитель: **Токарева Наталья Николаевна**
кандидат физико-математических наук, с.н.с.

Официальные оппоненты: **Фомичев Владимир Михайлович,**
доктор физико-математических наук, профессор,
Общество с ограниченной ответственностью «Код Безопасности», научный консультант

Панкратова Ирина Анатольевна,
кандидат физико-математических наук, доцент,
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет»,
заведующая лабораторией компьютерной криптографии

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М. В. Ломоносова».

Защита состоится 19 июня 2024 г. в 16 часов 00 минут на заседании диссертационного совета 24.1.074.04 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга 4.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук и на сайте http://math.nsc.ru.

Автореферат разослан «__» _____ 2024 года.

Ученый секретарь
диссертационного совета
24.1.074.04,
к.ф.-м.н. Батуева Цындыма Чимит-Доржиевна

Общая характеристика работы

Актуальность темы. Работа посвящена исследованию класса булевых функций от четного числа переменных, отличительным свойством которых является достижение верхней границы значения нелинейности. Такие булевы функции называются бент-функциями. Максимальное значение нелинейности представляет большой интерес для симметричной криптографии, однако бент-функции также связаны с некоторыми объектами теории кодирования, алгебры и комбинаторики. В работе исследуется построение бент-функций с помощью их производных, а также связь между известными открытыми проблемами, посвященными бент-функциям, и производными бент-функций.

Приведем необходимые определения.

Пусть $\mathbb{Z}_q = \{0,\ldots,q-1\}$, где q – целое положительное число. Пространство векторов длины n над $\mathbb{Z}_q$ обозначается $\mathbb{Z}_q^n$. Пусть $\oplus$ обозначает сложение по модулю 2. Для $x, y \in \mathbb{Z}_2^n$, мы будем использовать следующее произведение:

$$\langle x,y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n,$$

где x_i – i-ая координата x, $i = 1,\ldots,n$.

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Обозначим через $\mathcal{F}_n$ множество всех булевых функций от n переменных. *Весом Хэмминга* $wt(y)$ вектора $y \in \mathbb{Z}_2^n$ называется количество ненулевых координат y: $wt(y) = |\{i : y_i = 1\}|$. *Весом Хэмминга* $wt(f)$ функции $f \in \mathcal{F}_n$ называется количество ненулевых значений f: $|\{x \in \mathbb{Z}_2^n : f(x) = 1\}|$. Функция $f \in \mathcal{F}_n$ называется *уравновешенной*, если $wt(f) = 2^{n-1}$. *Расстояние Хэмминга* $\mathrm{dist}(f,g)$ между двумя булевыми функциями $f, g \in \mathcal{F}_n$ вычисляется следующим образом: $\mathrm{dist}(f,g) = |\{x \in \mathbb{Z}_2^n : f(x) \neq g(x)\}|$.

Каждую булеву функцию f от n переменных можно единственным образом представить в виде *полинома Жегалкина* (*алгебраической нормальной формы или АНФ*):

$$f(x_1,\ldots,x_n) = a_0 \oplus \bigoplus_{k=1}^{n} \bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} x_{i_1} \cdot \ldots \cdot x_{i_k},$$

где при каждом k индексы i_1,...,i_k различны и в совокупности пробегают все k-элементные подмножества $\{1,...,n\}$, а коэффициенты a_{i_1},...,a_{i_k},a_0 принимают значение 0 или 1.

Алгебраической степенью (степенью) $\deg(f)$ функции f называется количество переменных в самом длинном слагаемом ее полинома Жегалкина, при котором коэффициент не равен нулю. Функции степени два называются *квадратичными*. Булева функция называется *однородной*, если все мономы ее полинома Жегалкина имеют одинаковые степени.

Функция f от n переменных *линейно зависит от переменной* x_i, если $f(x_1,\ldots,x_n) = g(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n) \oplus x_i$, где $g \in \mathcal{F}_{n-1}$ и $1 \leqslant i \leqslant n$.

Если переменная не входит в АНФ булевой функции, то эта переменная называется *фиктивной*.

Производной булевой функции $f \in \mathcal{F}_n$ по *направлению* $y \in \mathbb{Z}_2^n$ называется функция $D_y f(x) = f(x) \oplus f(x \oplus y)$. Булева функция f *имеет линейную структуру*, если существует ненулевое направление $y \in \mathbb{Z}_2^n$ такое, что $D_y f(x) \equiv \text{const}$.

Булева функция $\ell_{a,b} = \langle x, a \rangle \oplus b$, где $a \in \mathbb{Z}_2^n$ и $b \in \mathbb{Z}_2$, называется *аффинной функцией* от n переменных. Множество всех аффинных функций от n переменных обозначим $\mathcal{A}_n$.

Булева функция $g \in \mathcal{F}_n$ получена из функции $f \in \mathcal{F}_n$ *аффинным преобразованием переменных*, если существует невырожденная квадратная двоичная матрица A порядка $n \times n$ и вектор $b \in \mathbb{Z}_2^n$ такие, что $g(x) = f(Ax \oplus b)$.

Нелинейностью N_f булевой функции $f \in \mathcal{F}_n$ называется расстояние Хэмминга от данной функции до множества всех аффинных функций, а именно

$$N_f = \text{dist}(f, \mathcal{A}_n) = \min_{a \in \mathbb{Z}_2^n, b \in \mathbb{Z}_2} \text{dist}(f, \ell_{a,b}),$$

где $\ell_{a,b}(x) = \langle a, x \rangle \oplus b$, $a \in \mathbb{Z}_2^n$ и $b \in \mathbb{Z}_2$.

Для каждого $y \in \mathbb{Z}_2^n$ *коэффициентом Уолша–Адамара* $W_f(y)$ булевой функции $f \in \mathcal{F}_n$ называется величина, определяемая равенством

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}.$$

С помощью коэффициентов Уолша–Адамара можно определять расстояние от функции $f \in \mathcal{F}_n$ до аффинных функций:

$$\text{dist}(f, \ell_{a,0}) = 2^{n-1} - \frac{1}{2} W_f(a).$$

Поскольку $\text{dist}(f, \ell_{a,1}) = 2^n - \text{dist}(f, \ell_{a,0})$, то справедливо следующее:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{Z}_2^n} |W_f(a)|.$$

Для коэффициентов Уолша–Адамара справедливо равенство Парсеваля:

$$\sum_{y \in \mathbb{Z}_2^n} W_f^2(y) = 2^{2n}.$$

Из него следует, что $\max\limits_{a \in \mathbb{Z}_2^n} |W_f(a)| \geqslant 2^{n/2}$. Таким образом, $N_f \leqslant 2^{n-1} - 2^{\frac{n}{2}-1}$.

Булева функция от четного числа n переменных, значение нелинейности которой достигает наибольшего значения $2^{n-1} - 2^{\frac{n}{2}-1}$, называется **бент-функцией**. Известен также следующий критерий: функция $f \in \mathcal{F}_n$ является бент-функцией, если и только если ее производные по всем ненулевым направлениям уравновешены. Обозначим через $\mathcal{B}_n$ множество всех бент-функций от n переменных.

Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ – *обобщенная булева функция* от n переменных, где $q \geqslant 2$ – целое положительное число. *Преобразование Уолша–Адамара* обобщенной функции от n переменных определяется следующим образом:

$$W_f(x) = \sum_{y \in \mathbb{Z}_2^n} \omega^{f(y)} (-1)^{\langle x,y \rangle},$$

где $x \in \mathbb{Z}_2^n$ и $\omega = e^{2\pi i/q}$. В случае $q = 4$ получаем $\omega = i$.

Обобщенная булева функция f от n переменных является *обобщенной бент-функцией*, если $|W_f(x)| = 2^{n/2}$ для любого $x \in \mathbb{Z}_2^n$. Отметим, что обобщенные бент-функции существуют и при нечетных n. В работе мы будем рассматривать только случай $q = 4$. Для $q = 4$ множество всех обобщенных булевых функций и множество всех обобщенных бент-функций от n переменных обозначим $\mathcal{GF}_n$ и $\mathcal{GB}_n$ соответственно.

Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *q-значной функцией* от n переменных, где $q \geqslant 2$ – целое положительное число. Для $x, y \in \mathbb{Z}_q^n$, мы будем использовать следующее произведение:

$$x.y = x_1 y_1 + \cdots + x_n y_n \bmod q.$$

Преобразование Уолша–Адамара q-значной функции f от n переменных определяется следующим образом:

$$W_f(x) = \sum_{y \in \mathbb{Z}_q^n} \omega^{f(y)+x.y},$$

где $x \in \mathbb{Z}_q^n$ и $\omega = e^{2\pi i/q}$. В случае $q = 4$ такие функции называются *кватернарными функциями*.

Пусть f – q-значная булева функция от n переменных. Тогда f является *q-значной бент-функцией*, если $|W_f(x)| = q^{n/2}$ для любого $x \in \mathbb{Z}_q^n$. Отметим, что q-значные бент-функции также существуют и при нечетных n. В данной работе мы будем рассматривать только кватернарные функции. Множество всех кватернарных функций и множество всех кватернарных бент-функций от n переменных обозначим $\mathcal{QF}_n$ и $\mathcal{QB}_n$ соответственно.

За годы использования булевых функций в системах шифрования были сформулированы математические требования, которые на них накладываются, для противодействия различным криптографическим атакам. Такие свойства булевых функций называют криптографическими. Одной из наиболее важных криптографических характеристик булевой функции является ее нелинейность. Шифры, которые используют функции с высокой нелинейностью в качестве своих компонент, являются более стойкими к линейному криптоанализу[1]. Большой

[1] *Matsui M.* Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology — EUROCRYPT '93. 1994. P. 386–397. Part of the Lecture Notes in Computer Science book series (LNCS, volume 765).

интерес, конечно, представляют булевы функции с максимальным значением нелинейности.

Бент-функции определил в 1960-х годах O. S. Rothaus в работе, опубликованной в 1976 году[2]. Однако известно, что бент-функции также исследовались в Советском Союзе математиками В. А. Елисеевым и О. П. Степченковым, которые использовали термин “минимальная функция”.

Бент-функции использовались в построении блочного шифра CAST-128[3], поточного шифра Grain[4] и хэш-функции HAVAL[5].

К основным криптографическим свойствам относятся также уравновешенность, корреляционная иммунность, строгий лавинный критерий, критерий распространения, алгебраическая иммунность, отсутствие линейных структур. Очевидно, что для криптографических приложений интересны функции, которые обладают сразу несколькими криптографическими свойствами. Для более детального знакомства с важными криптографическими свойствами можно порекомендовать книги О. А. Логачева, А. А. Сальникова, С. В. Смышляева, В. В. Ященко[6] и T. W. Cusick и P. Stănĭca[7].

Однако не все свойства хорошо сочетаются друг с другом. Так, например, основным криптографическим недостатком бент-функций является тот факт, что бент-функции не являются уравновешенными. Одним из способов решения этой проблемы является преобразование бент-функций с целью получения уравновешенных булевых функций, которые сохраняют высокие значения нелинейности.

Бент-функции также связаны с другими математическими объектами. Так, например, R. L. McFarland[8] и J. F. Dillon[9] исследовали бент-функции в терминах разностных множеств. Бент-функции могут быть использованы для построения последовательностей, которые будут иметь предельно низкую автокорреляцию

---

[2] *Rothaus O. S.* On “bent” functions // Journal of Combinatorial Theory, Series A. 1976. Vol. 20, no. 3. P. 300—305.

[3] *Adams C. M.* Constructing Symmetric Ciphers Using the CAST Design Procedure // Designs, Codes and Cryptography. 1997. Vol. 12, no. 3. P. 283—316.

[4] A Stream Cipher Proposal: Grain-128 / M. Hell [et al.] // 2006 IEEE International Symposium on Information Theory. 2006. P. 1614—1618.

[5] *Zheng Y.*, *Pieprzyk J.*, *Seberry J.* HAVAL — A one-way hashing algorithm with variable length of output (extended abstract) // Advances in Cryptology — AUSCRYPT ’92. Berlin, Heidelberg : Springer Berlin Heidelberg, 1993. P. 81—104. Part of the Lecture Notes in Computer Science book series (LNCS, volume 718).

[6] Булевы функции в теории кодирования и криптологии / О. А. Логачев [и др.]. ЛЕНАНД, 2015. 576 с.

[7] *Cusick T. W.*, *Stănică P.* Cryptographic Boolean Functions and Applications. 2nd ed. Acad. Press, 2017. 288 p.

[8] *McFarland R. L.* A family of difference sets in non-cyclic groups // Journal of Combinatorial Theory, Series A. 1973. Vol. 15, no. 1. P. 1—10.

[9] *Dillon J. F.* Elementary Hadamard difference sets : PhD thesis / Dillon J. F. Univ. of Maryland, 1974.

и взаимную корреляцию[10,11]. Хорошо известной задачей теории кодирования является определение радиуса покрытия кода Рида–Маллера $RM(\ell, n)$. Если код имеет порядок 1, то эта задача связана с задачей поиска булевых функций с максимально возможной нелинейностью[12,13].

В 2006 году K.-U. Schmidt[14] в контексте построения четверичных кодов постоянной амплитуды (quaternary constant-amplitude codes) для мультикодовых систем CDMA предложил новое обобщение бент-функций – отображения из $\mathbb{Z}_2^n$ в $\mathbb{Z}_4$ с некоторыми специальными спектральными свойствами. В 1985 году P. V. Kumar, R. A. Scholtz и L. R. Welch в работе[15] с целью построения q-значных бент-последовательностей, применимых в системах CDMA, предложили обобщение бент-функций для отображений из $\mathbb{Z}_q^n$ в $\mathbb{Z}_q$, которые называются q-значными бент-функциями.

В работе исследуется следующая известная[16] гипотеза: любая булева функция от четного числа переменных n степени не больше $n/2$ может быть представлена как сумма двух бент-функций от n переменных.

Описанию известных результатов и открытых вопросов, связанных с бент-функциями, посвящены монографии Н. Н. Токаревой[17] и S. Mesnager[18].

Целью работы является исследование возможности построения бент-функций на основе их производных. В работе предложена конструкция бент-функций, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных. Также доказано необходимое и достаточное условие того, что функция, которая линейно зависит от некоторой своей переменной, является производной бент-функции. Доказано, что произвольная булева функция от n переменных степени не больше $n/2$ раскладывается в сумму двух бент-функций от n переменных тогда и только тогда, когда любая уравновешенная функция от $n+2$ переменных степени не больше $n/2$, которая линейно зависит от некоторой своей переменной и является производной некоторой булевой функции от $n+2$ переменных, является производной бент-функции от $n+2$ переменных. Тем самым доказана связь

[10] *Olsen J.*, *Scholtz R.*, *Welch L.* Bent-function sequences // IEEE Transactions on Information Theory. 1982. Vol. 28, no. 6. P. 858–864.

[11] *Zhang B.*, *Lü S.* I/O correlation properties of bent functions // Science in China Series E: Technological Sciences. 2000. Vol. 43, no. 3. P. 282–286.

[12] *Kavut S.*, *Maitra S.*, *Yucel M. D.* Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class // IEEE Transactions on Information Theory. 2007. Vol. 53, no. 5. P. 1743–1751.

[13] *Maitra S.*, *Sarkar P.* Maximum nonlinearity of symmetric Boolean functions on odd number of variables // IEEE Transactions on Information Theory. 2002. Vol. 48, no. 9. P. 2626–2630.

[14] *Schmidt K.-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // IEEE Transactions on Information Theory. 2006. Vol. 55, no. 4. P. 1824–1832.

[15] *Kumar P. V.*, *Scholtz R. A.*, *Welch L. R.* Generalized bent functions and their properties // Journal of Combinatorial Theory, Series A. 1985. Vol. 40, no. 1. P. 90–107.

[16] *Carlet C.*, *Mesnager S.* Four decades of research on bent functions // Designs, Codes and Cryptography. 2016. Vol. 78. P. 5–50.

[17] *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Academic Press, 2015. 220 p.

[18] *Mesnager S.* Bent functions: Fundamentals and results. Springer, 2016. 544 p.

проблемы о разложении булевых функций в сумму двух бент-функций и следующей гипотезы о производных бент-функций: любая уравновешенная булева функция от четного числа переменных n степени не больше $n/2-1$, которая является производной некоторой булевой функции от n переменных, является производной бент-функции от n переменных. Гипотеза о производных бент-функций доказана для квадратичных булевых функций. Получено точное число бент-функций, которые имеют некоторую отличную от константы аффинную функцию своей производной. Этот результат был использован для получения итеративной нижней оценки числа бент-функций. Предложен метод построения уравновешенных функций от четного числа переменных без линейных структур с высокой нелинейностью. Показано, что свойство быть бент-функцией кватернарной функции $f(x+2y) = a(x,y) + 2b(x,y)$ от n переменных, где $a,b \in \mathcal{F}_{2n}$ и $x,y \in \mathbb{Z}_2^n$, не зависит от того, являются ли $b, a \oplus b$ бент-функциями от $2n$ переменных. В работе также исследуется возможность характеризации однородных бент-функций, с помощью клик максимального размера графов $\Gamma(n,k)$, вершинами которых являются неупорядоченные подмножества размера k множества $\{1,\ldots,n\}$, которые соединены ребром, если рассматриваемые подмножества имеют в точности один общий элемент. Было доказано, что если $n = \frac{(k+1)k}{2}$, то максимальный размер клики равен $k+1$, а количество клик максимального размера равно $\frac{n!}{(k+1)!}$.

Основные положения, выносимые на защиту:

1. Предложен метод построения уравновешенных функций от четного числа $n \geqslant 20$ переменных без линейных структур с нелинейностью $2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$. Полученные значения нелинейности уравновешенных функций являются наибольшими достигнутыми для указанного числа переменных.
2. Представлена конструкция бент-функций, производная которых по некоторому ненулевому направлению линейно зависит хотя бы от одной из своих переменных. Получено необходимое и достаточное условие того, что уравновешенная функция, которая линейно зависит хотя бы от одной из своих переменных, является производной бент-функции.
3. Доказано, что гипотеза о разложении булевых функций в сумму двух бент-функций верна в том и только том случае, если гипотеза о производных бент-функций верна для уравновешенных функций, которые линейно зависят хотя бы от одной из своих переменных.
4. Доказано, что любая квадратичная уравновешенная функция, которая может быть производной булевой функции, является производной бент-функции. Получено точное число бент-функций, имеющих некоторую отличную от константы аффинную функцию своей производной. Как следствие получена итеративная нижняя оценка числа бент-функций.
5. Известно, что каждая однородная бент-функция от 6 переменных степени 3 соответствует дополнению клики максимального размера в графе

Нэги $\Gamma(6,3)$. Доказано, что для графа Нэги $\Gamma(n,k)$, где $n = \frac{(k+1)k}{2}$, максимальный размер клики равен $k+1$ и точное число клик максимального размера в таких графах равно $\frac{n!}{(k+1)!}$. Установлено, что функции, соответствующие дополнениям клик максимального размера в графах $\Gamma(10,4)$ и $\Gamma(28,7)$, не являются бент-функциями.

Научная новизна и значимость работы: Работа носит теоретический характер. Все результаты диссертации являются новыми и снабжены полными доказательствами. Полученные результаты могут быть использованы для дальнейшего изучения производных бент-функций и их связи с открытыми проблемами из области исследования бент-функций. Например, в работе доказано, что изучение производных бент-функций связано с проблемой разложения булевых функций в сумму двух бент-функций.

Методология и методы исследования. В диссертации используются комбинаторные методы и методы дискретного анализа.

Апробация работы. Основные результаты работы докладывались на следующих конференциях и семинарах: Международная конференция «Boolean Functions and their Applications (BFA 2022)» (Норвегия, г. Балестранд, 2022 г.), Симпозиум «Современные тенденции в криптографии» (CTCrypt 2021) (Московская область, 2021 г.), Пятая конференция по программной инженерии и организации информации (SEIM-2020) (Санкт-Петербург, 2020 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография (SIBECRYPT)» имени Геннадия Петровича Агибалова (г. Абакан, 2018 г.; г. Томск, 2019; г. Новосибирск, 2021 г.), семинары «Дискретный анализ», «Комбинаторика и символьные последовательности», «Теория кодирования», «Криптография и криптоанализ» Института математики им. С. Л. Соболева СО РАН и кафедры теоретической кибернетики ММФ НГУ.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель работы.

В первой главе представлены основные определения и вспомогательные утверждения, а также ключевые для работы открытые проблемы: о разложении булевых функций в сумму двух бент-функций и о производных бент-функций, а также обзор известных результатов, посвященным им.

Следующая гипотеза была представлена и проверена для $n \leqslant 6$ в работе Н. Н. Токаревой 2011 года[19].

[19] *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances in Mathematics of Communications. 2011. Vol. 5, no. 4. P. 609–621.

Гипотеза 1. *Пусть n – целое четное число. Тогда любая булева функция от n переменных степени не больше $n/2$ может быть разложена в сумму двух бент-функций от n переменных.*

В 2016 году была представлена и проверена для $n \leqslant 6$ следующая гипотеза: любая уравновешенная булева функция f от четного числа n переменных степени не больше $n/2-1$ такая, что $f(x) = f(x \oplus y)$ для любого $x \in \mathbb{Z}_2^n$ и некоторого ненулевого $y \in \mathbb{Z}_2^n$, является производной бент-функции от n переменных[20]. Мы предлагаем следующее уточнение этой гипотезы.

Гипотеза 2. *Любая уравновешенная булева функция f от четного числа n переменных степени не больше $n/2-1$, которая линейно зависит хотя бы от одной из своих переменных, такая, что $f(x) = f(x \oplus y)$ для любого $x \in \mathbb{Z}_2^n$ и некоторого ненулевого $y \in \mathbb{Z}_2^n$, является производной бент-функции от n переменных.*

В работе доказано, что между Гипотезой 2 и проблемой о разложении булевых функций в сумму двух бент-функций существует прямая связь.

Вторая глава посвящена построению уравновешенных функций с высокой нелинейностью и другими криптографическими свойствами. Предложена следующая конструкция.

Конструкция 1. *Пусть $g_1, g_2 \in \mathcal{F}_n$, $h \in \mathcal{F}_{n+2}$ и вектор $y \in \mathbb{Z}_2^n$. Будем строить функцию $f \in \mathcal{F}_{n+2}$ следующим образом:*

$$f(x,x_{n+1},x_{n+2}) = \big((D_y g_1(x) \oplus 1)h(x,x_{n+1},x_{n+2}) \oplus D_y g_2(x)\big)x_{n+1} \\ \oplus g_1(x)h(x,x_{n+1},x_{n+2}) \oplus g_2(x),$$

где $x \in \mathbb{Z}_2^n, x_{n+1}, x_{n+2} \in \mathbb{Z}_2$.

Функции g_1, g_2, h и вектор y будем считать параметрами конструкции.

Доказана следующая теорема, в которой описаны параметры Конструкции 1, при которых функции будут обладать рядом криптографических свойств.

Теорема 1. *Пусть g_1, $g_2 \in \mathcal{F}_n$, $y \in \mathbb{Z}_2^n$ и $h(x,x_{n+1},x_{n+2}) = \langle b,x\rangle \oplus c \oplus x_{n+2}$ для любого $x \in \mathbb{Z}_2^n$, где $b \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$. Тогда для функции $f \in \mathcal{F}_{n+2}$ из Конструкции 1 справедливо, что*

1. *функция f имеет h своей производной по направлению $(y,1,\langle b,y\rangle)$;*
2. *функция f — уравновешенная функция тогда и только тогда, когда g_2 – уравновешенная функция;*
3. $N_f = 2^{n+1} - \max\limits_{a \in \mathbb{Z}_2^n, g \in \{g_2, g_1 \oplus g_2\}} |W_g(a)|$;
4. *если g_2 и $g_1 \oplus g_2$ — корреляционно-иммунные порядка r, то функция f является корреляционно-иммунной порядка r.*

[20] *Токарева Н. Н.* О множестве производных булевой бент-функции // Прикладная дискретная математика. Приложение. 2016. № 9. С. 35.

5. *если g_2 и $g_1 \oplus g_2$ — уравновешенная функция и бент-функция соответственно, то функция f — уравновешенная без линейных структур.*

В данной главе предложен итеративный метод построения уравновешенных функций от четного числа $n \geqslant 18$ переменных с высокой нелинейностью без линейных структур. Пусть функцию f_{16} является уравновешенной функцией от 16 переменных с нелинейностью 32 598[21].

Метод 1. *Будем строить булевы функции от n переменных, используя Конструкцию 1 со следующими параметрами:*
- *при $n = 18$ функция $g_2 = f_{16}$;*
- *при $n \geqslant 20$ функция g_2 — функция f из Конструкции 1, полученная с помощью Метода 1 на предыдущем шаге;*
- *функция $h(x,x_{n+1},x_{n+2}) = \langle b,x\rangle \oplus c \oplus x_{n+2}$ для любого $x \in \mathbb{Z}_2^n$, где $b \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$;*
- *функция g_1 такая, что $g_1 \oplus g_2$ — бент-функция;*
- *вектор $y \in \mathbb{Z}_2^n$ — произвольный.*

Теорема 2. *Функции от $n \geqslant 18$ переменных полученные с помощью Метода 1 являются уравновешенными функциями без линейных структур с нелинейностью $2^{n-1} - (2^{\frac{n}{2}-1} + 2^{\frac{n}{2}-3} + 2^{\frac{n}{2}-5} + 2^{\frac{n}{2}-7})$.*

Результаты главы опубликованы в работе [1].

Третья глава посвящена гипотезе о производных бент-функций и ее связи с проблемой о разложении булевых функций в сумму двух бент-функций. Доказана следующая теорема, в которой представлено необходимое и достаточное условие того, что функция, линейно зависящая от некоторой своей переменной, является производной бент-функции. Кроме того, теорема представляет достаточное условие для того, чтобы функции, получаемые с помощью Конструкции 1, были бент-функциями.

Теорема 3. *Пусть $n \geqslant 2$ – четное целое число, функции g_1, g_2, $h_1 \in \mathcal{F}_n$, вектор $(y,1,y_{n+2}) \in \mathbb{Z}_2^{n+2}$ и $h(x,x_{n+1},x_{n+2}) = (D_y h_1(x) \oplus y_{n+2})x_{n+1} \oplus h_1(x) \oplus x_{n+2}$. Тогда $f \in \mathcal{F}_{n+2}$ из Конструкции 1 является бент-функцией тогда и только тогда, когда g_2, $g_1 \oplus g_2$, $g_2 \oplus h_1$ и $g_1 \oplus g_2 \oplus h_1$ — бент-функции. При этом любая функция f от $n+2$ переменных, которая имеет h своей производной по направлению $(y,1,y_{n+2})$, имеет представление из Конструкции 1. Кроме того, для различных параметров (g_1, g_2) получаются различные бент-функции f.*

В данной главе также доказано, что проблемы о разложении булевой функции в сумму двух бент-функций и о производных бент-функций являются эквивалентными.

[21] *Gini A., Méaux P.* Weightwise Perfectly Balanced Functions and Nonlinearity // Codes, Cryptology and Information Security. Cham : Springer Nature Switzerland, 2023. P. 338—359. Part of the Lecture Notes in Computer Science book series (LNCS, volume 13874).

Теорема 4. *Гипотеза 1 и Гипотеза 2 являются эквивалентными.*

Также в данной главе исследуются аффинные производные бент-функций. Доказана следующая теорема.

Теорема 5. *Пусть $n \geqslant 2$, $\ell \in \mathcal{A}_{n+2}$ и не является константой. Тогда ℓ является производной $(2^{n+1}-1)$ | $\mathcal{B}_n$ |^2 бент-функций от $n+2$ переменных.*

Таким образом, получено точное число бент-функций, которые имеют некоторую отличную от константы аффинную функцию своей производной. Теорема 5 в дальнейшем используется, чтобы получить следующую итеративную нижнюю оценку числа бент-функций.

Теорема 6. *Для любого $n \geqslant 2$ справедливо* | $\mathcal{B}_{n+2}$ |$\geqslant (2^{n+2}-2)$ | $\mathcal{B}_n$ |^2.

Также гипотеза о производных бент функций была доказана для квадратичных функций.

Теорема 7. *Пусть f – квадратичная уравновешенная булева функция от $n \geqslant 6$ переменных такая, что $f(x) \oplus f(x \oplus y) = 0$ для некоторого ненулевого $y \in \mathbb{Z}_2^n$ и произвольного $x \in \mathbb{Z}_2^n$. Тогда f является производной некоторой бент-функции от n переменных.*

Результаты главы опубликованы в работах [2; 5; 6].

Четвертая глава посвящена исследованию связи кватернарных и булевых бент-функций. В этой главе доказано, что между свойствами функций $f \in \mathcal{QF}_n$ и $a, b \in \mathcal{F}_{2n}$ таких, что $f(x+2y) = a(x,y) + 2b(x,y)$, где $x, y \in \mathbb{Z}_2^n$, быть бент-функциями нет зависимости. А именно, доказаны следующие утверждения.

Утверждение 18. *Для любых целых $n \geqslant 2$ существует кватернарная бент-функция $f(x+2y) = a(x,y)+2b(x,y)$ от n переменных, где b и $a \oplus b$ не являются бент-функциями от $2n$ переменных.*

Утверждение 19. *Для любых целых $n \geqslant 1$ существуют булевы бент-функции b и $a \oplus b$ от $2n$ переменных такие, что функция $f(x+2y) = a(x,y) + 2b(x,y)$ от n переменных не является кватернарной бент-функцией.*

Результаты главы опубликованы в работах [3; 7–9].

В **пятой главе** мы изучаем связь однородных бент-функций и графов $\Gamma(n,k)$, вершинами которого являются неупорядоченные подмножества размера k множества $\{1,\ldots,n\}$, которые соединены ребром, если рассматриваемые подмножества имеют в точности один общий элемент. Известно, что все однородные бент-функции от 6 переменных находятся во взаимно однозначном соответствии с дополнениями к кликам максимального размера графа $\Gamma(6,3)$[22]. Следовательно,

[22] *Charnes C., Rötteler M., Beth T.* Homogeneous Bent Functions, Invariants, and Designs // Designs, Codes and Cryptography. 2002. Vol. 26, no. 1. P. 139–154.

возникает вопрос о возможности классификации однородных бент-функций от большего числа переменных с помощью выделения в графе $\Gamma(n,k)$ дополнений к кликам максимального размера. Доказана следующая теорема.

Теорема 8. *Пусть* $n = \frac{(k+1)k}{2}$, *где* $k > 1$. *Тогда максимальный размер клики в графе* $\Gamma(n,k)$ *равен* $k+1$. *При этом количество клик максимального размера равно* $\frac{n!}{(k+1)!}$.

В данной главе установлено, что булевы функции, которые соответствуют дополнениям клик максимального размера в графах $\Gamma(10,4)$ и $\Gamma(28,7)$, не являются бент-функциями.

Результаты главы были представлены в работах [4; 10].

В **заключении** приведены основные результаты работы.

Благодарности. Автор выражает признательность своему научному руководителю Наталье Николаевне Токаревой за постановку интересных задач, постоянное внимание к работе и поддержку. Также автор хотел бы выразить благодарность Николаю Александровичу Коломейцу и Александру Владимировичу Куценко за ценные советы и интересные обсуждения по теме работы.

Публикации. Основные результаты по теме диссертации изложены в 10 печатных изданиях, 4 из которых изданы в журналах, рекомендованных ВАК, 6 — в тезисах докладов. Статья [3] опубликована в соавторстве с Н. Н. Токаревой и P. Solé, при этом результаты параграфов 4, 5 и 8.2 статьи [3] получены автором лично.

Объем и структура работы. Диссертация состоит из введения, 5 глав и заключения. Полный объём диссертации составляет 82 страницы, включая 6 таблиц. Список литературы содержит 103 наименования.

Публикации автора по теме диссертации

1. *Шапоренко А. С.* Конструкция уравновешенных функций с высокой нелинейностью и другими криптографическими свойствами // Прикладная дискретная математика. — 2024. — № 63. — С. 8—24.
2. *Shaporenko A.* Derivatives of bent functions in connection with the bent sum decomposition problem // Designs, Codes and Cryptography. — 2023. — Vol. 91, no. 5. — P. 1607—1625.
3. *Tokareva N. N.*, *Shaporenko A. S.*, *Solé P.* Connections between quaternary and Boolean bent functions // Siberian Electronic Mathematical Reports. — 2021. — Vol. 18, no. 1. — P. 561—578.
4. *Шапоренко А. С.* Связь однородных бент-функций и графов Нэги // Дискретный анализ и исследование операций. — 2019. — Т. 26, № 4. — С. 121—131.

5. *Shaporenko A.* New approaches to the study of the “bent sum decomposition problem” // Proceedings of the 7th workshop Boolean Functions and their Applications (BFA 2022), Balestrand, Norway, September 11-16, 2022. — 2022.

6. *Шапоренко А. С.* О производных булевых бент-функций // Прикладная дискретная математика. Приложение. — 2021. — № 14. — С. 57—58.

7. *Shaporenko A.* On relationship between quaternary and Boolean bent functions // Proceedings of Fifth Conference on Software Engineering and Information Management (SEIM-2020), Saint Petersburg, Russia, May 16, 2020. — 2020. — P. 19—23.

8. *Шапоренко А. С.* Связь между кватернарными и компонентными булевыми бент-функциями // Прикладная дискретная математика. Приложение. — 2020. — № 13. — С. 35—37.

9. *Шапоренко А. С.* О взаимосвязи между кватернарными и булевыми бент-функциями // Прикладная дискретная математика. Приложение. — 2019. — № 12. — С. 73—75.

10. *Шапоренко А. С.* Связь однородных бент-функций и графов пересечений // Прикладная дискретная математика. Приложение. — 2018. — № 11. — С. 52—53.

Шапоренко Александр Сергеевич

Построение бент-функций на основе их производных и связанные открытые вопросы

Автореф. дис. на соискание ученой степени канд. физ.-мат. наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж 120 экз.
Типография _____