РОССИЙСКАЯ АКАДЕМИЯ НАУК
СИБИРСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТ МАТЕМАТИКИ им. С. Л. СОБОЛЕВА

На правах рукописи

УДК 519.1, 519.7

ТОКАРЕВА Наталья Николаевна

СИЛЬНО НЕЛИНЕЙНЫЕ БУЛЕВЫ ФУНКЦИИ: БЕНТ-ФУНКЦИИ И ИХ ОБОБЩЕНИЯ

специальность 01.01.09 – дискретная математика и математическая кибернетика

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Новосибирск – 2008

Работа выполнена в Институте математики
имени С. Л. Соболева СО РАН

Научный руководитель:	кандидат физ.-мат. наук, Ю. Л. Васильев.
Официальные оппоненты:	доктор физ.-мат. наук, Е. А. Окольнишникова, кандидат физ.-мат. наук, Ю. В. Таранников.
Ведущая организация:	Томский государственный университет

Защита состоится 12 ноября 2008 г. в 15 часов на заседании диссертационного совета Д.003.015.01 в Институте математики им. С. Л. Соболева СО РАН по адресу: пр. Академика Коптюга, 4, 630090, г. Новосибирск.

С диссертацией можно ознакомиться в библиотеке Института математики имени С. Л. Соболева СО РАН.

Автореферат разослан 12 октября 2008 г.

Ученый секретарь
диссертационного совета
Д.003.015.01 при Институте математики
имени С. Л. Соболева СО РАН
доктор физ.-мат. наук Шамардин Ю. В.

Bent functions deserve
our bent to study them...[1]

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Работа относится к такой области дискретной математики, как булевы функции и их приложения в комбинаторике, теории кодирования и криптографии. Исследуется важный класс булевых функций, обладающих сильными свойствами нелинейности: бент-функции и их обобщения.

Мера нелинейности является важной характеристикой булевой функции. Линейность и близкие к ней свойства часто свидетельствуют о простой (в определенном смысле) структуре этой функции и, как правило, представляют собой богатый источник информации о многих других ее свойствах. Задача построения булевых функций, обладающих нелинейными свойствами, естественным образом возникает во многих областях дискретной математики. И часто (что является типичной ситуацией в математике) наибольший интерес вызывают те функции, для которых эти свойства экстремальны. Такие булевы функции называются *максимально-нелинейными* (или *бент-*) *функциями*[2].

Приведем ряд определений.
Пусть $\mathbf{u} = (u_1, \ldots, u_m)$, $\mathbf{v} = (v_1, \ldots, v_m)$ — двоичные векторы длины m. Обозначим через $\langle \mathbf{u}, \mathbf{v} \rangle$ их скалярное произведение по модулю 2,

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 \oplus \ldots \oplus u_m v_m,$$

где $\oplus$ означает сложение над $\mathbb{Z}_2$. *Булевой функцией* от m переменных называется произвольная функция из $\mathbb{Z}_2^m$ в $\mathbb{Z}_2$. Булева функция f от переменных $v_1, \ldots, v_m$ называется *аффинной*, если она имеет вид

$$f(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle \oplus a$$

для некоторого вектора $\mathbf{u} \in \mathbb{Z}_2^m$ и константы $a \in \mathbb{Z}_2$. *Расстоянием Хэмминга* между векторами $\mathbf{u}$, $\mathbf{v}$ называется число координат, в

[1] Игра слов: «Бент-функции заслуживают нашего стремления изучить их...» (англ.)
[2] В литературе встречается также термин *совершенно нелинейные функции*.

которых они различаются. Под расстоянием между двумя булевыми функциями от m переменных понимается расстояние Хэмминга между их векторами значений длины 2^m.

Максимально нелинейной называется булева функция от m переменных (m — любое натуральное число) такая, что расстояние Хэмминга от данной функции до множества всех аффинных функций является максимально возможным. В случае четного m это максимально возможное расстояние равно $2^{m-1} - 2^{(m/2)-1}$. В случае нечетного m точное значение максимального расстояния неизвестно (поиск этого значения или его оценок представляет весьма любопытную и сложную комбинаторную задачу [15]). Термин «максимально нелинейная функция» принят в русскоязычной литературе, тогда как в англоязычной широкое распространение получил термин «бент-функция» (от англ. слова bent[3] — изогнутый, наклоненный). Аналогия между терминами не полная. При четном числе переменных m бент-функции и максимально нелинейные функции совпадают, а при нечетном m бент-функции (в отличие от максимально нелинейных) не существуют.

Преобразованием Уолша—Адамара булевой функции f от m переменных называется целочисленная функция W_f, заданная на множестве $\mathbb{Z}_2^m$ двоичных векторов длины m равенством

$$W_f(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle \oplus f(\mathbf{u})}.$$

В литературе функцию W_f также называют *дискретным преобразованием Фурье* или *преобразованием Адамара* функции f. Значения $W_f(\mathbf{v})$, $\mathbf{v} \in \mathbb{Z}_2^m$, называются *коэффициентами Уолша—Адамара* функции f. Для них справедливо равенство Парсеваля:

$$\sum_{\mathbf{v} \in \mathbb{Z}_2^m} (W_f(\mathbf{v}))^2 = 2^{2m}.$$

Поскольку число всех коэффициентов равно 2^m, из равенства следует, что максимум модуля коэффициента Уолша—Адамара не может быть меньше величины $2^{m/2}$. Заметим, что расстояние Хэммин-

[3]Английское слово bent очень многозначно; среди его значений: «изогнутый», «кривой», «натяжение», «напряженное состояние», «призвание», а еще и «соцветие подорожника».

га от произвольной булевой функции f до множества всех аффинных функций тесно связано с коэффициентами Уолша—Адамара этой функции. А именно, это расстояние равно величине $2^{m-1} - \frac{1}{2}\max_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f(\mathbf{v})|$. Очевидно, что чем меньше максимум модуля коэффициента Уолша—Адамара функции f, тем больше это расстояние.

Бент-функцией называется булева функция от m переменных (m четно) такая, что модуль каждого коэффициента Уолша—Адамара этой функции равен $2^{m/2}$. Другими словами, функция f — бент-функция, если максимум модуля $W_f(\mathbf{v})$ достигает своего минимального возможного значения. В силу равенства Парсеваля это имеет место, только если модули всех коэффициентов Уолша—Адамара этой функции совпадают и равны $2^{m/2}$. Таким образом, эквивалентность определению максимально нелинейной функции (при четном m) становится очевидной.

В геометрической (кодовой) интерпретации векторы значений всех аффинных булевых функций от m переменных образуют двоичный линейный код Адамара (или иначе его называют код Рида—Маллера первого порядка) длины 2^m, а векторы значений бент-функций удалены от этого кода на максимально возможное расстояние Хэмминга $2^{m-1} - 2^{(m/2)-1}$ (при четном m).

Бент-функции были введены О. Ротхаусом еще в 60-х годах XX века, хотя его работа [23] на эту тему была опубликована лишь в 1976 году. Дж. Диллон [10] и Р. Л. МакФарланд [20] рассматривали бент-функции в связи с разностными множествами. В настоящее время известно большое число конструкций бент-функций, см. обзоры [3, 12, 7]. Тем не менее класс всех бент-функций от m переменных до сих пор не описан, для мощности этого класса не найдена асимптотика и не установлено даже приемлемых нижних и верхних оценок (некоторые продвижения в этом направлении можно найти в [9]).

Масштабы исследования бент-функций и их приложений поистине впечатляют. В настоящее время несколько сотен математиков и инженеров по всему миру регулярно публикуют свои статьи по этой тематике. Результаты обсуждаются на таких международных конференциях как EUROCRYPT, CRYPTO, ASIACRYPT, INDOCRYPT,

SETA, FSE, AAECC, ISIT, ITW, BFCA, ACCT, SIBECRYPT, МаБИТ и многих других. А счет общего числа публикаций о бент-функциях (и близких вопросах) уже идет на тысячи. К сожалению, публикаций на русском языке (по крайней мере, в открытой печати) известно не так уж много — всего несколько десятков. Своей работой мне хотелось бы привлечь внимание, прежде всего, российских исследователей к этой активно развивающейся области.

Актуальность исследования бент-функций подтверждается их многочисленными теоретическими и практическими приложениями в комбинаторике, алгебре, теории кодирования, теории информации, теории символьных последовательностей, криптографии и криптоанализе. Приведем (далеко не полную) серию таких примеров.

Классическая комбинаторная задача построения *матриц Адамара* порядка n, известная с 1893 года, в случае $n = 2^m$ (m четно) при некоторых ограничениях сводится к задаче построения бент-функций от m переменных [23]. В теории конечных групп построение *элементарных адамаровых разностных множеств* специального вида эквивалентно построению максимально нелинейных булевых функций, см. [3]. В теории кодирования широко известна задача определения радиуса покрытия произвольного *кода Рида—Маллера*, которая эквивалентна (в случае кодов первого порядка) поиску наиболее нелинейных булевых функций. В теории оптимальных кодов специальные семейства квадратичных бент-функций определяют класс *кодов Кердока* [16], обладающих исключительным свойством: вместе с растущим кодовым расстоянием (при увеличении длины кода) каждый код Кердока имеет максимально возможную мощность. Этим свойством коды Кердока «обязаны» экстремальной нелинейности бент-функций. Отметим, что задача построения таких семейств бент-функций, задающих код Кердока, несложно переводится в задачу поиска *ортогональных разветвлений* (orthogonal spreads) в конечном векторном пространстве [14], что представляется элегантным примером связи бент-функций с экстремальными геометрическими объектами. Другим примером из теории кодирования служат так называемые *бент-коды* — линейные двоичные коды, каждый из которых определенным образом строится из некоторой бент-функции [7]. В принципе тем же способом можно строить ли-

нейные коды из любых булевых функций, но только бент-коды будут иметь всего два ненулевых значения для весов кодовых слов и при этом максимально возможные кодовые размерности.

Семейства *бент-последовательностей* из элементов -1 и $+1$, построенные на основе бент-функций, имеют предельно низкие значения как взаимной корреляции, так и автокорреляции (достигают нижней границы Велча) [21]. Поэтому такие семейства успешно применяются в коммуникационных системах коллективного доступа. Генераторы бент-последовательностей легко инициализируются случайным образом и могут быстро перестраиваться с одной последовательности на другую. Этот факт используется в работе со стандартом CDMA – Code Division Multiple Access (множественный доступ с кодовым разделением каналов) – одним из двух стандартов для цифровых сетей сотовой связи в США. Отметим здесь же, что в системах CDMA для предельного снижения отношения пиковой и средней мощностей сигнала (peak-to-average power ratio) используются, так называемые, коды постоянной амплитуды (constant-amplitude codes). И например, четверичные такие коды можно построить с помощью обобщенных булевых бент-функций [24]. Не обходится без бент-функций или их аналогов и в квантовой теории информации, см. например, [22].

Бент-функцию можно определить как функцию, которая крайне плохо аппроксимируется аффинными функциями. Это базовое свойство бент-функций используется в криптографии. В блочных и поточных шифрах бент-функции и их векторные аналоги способствуют предельному повышению стойкости этих шифров к основным методам криптоанализа — линейному [19] и дифференциальному [6]. Стойкость достигается за счет использования сильно нелинейных булевых функций в S-блоках (важнейших компонентах современных шифров). Бент-функции и их обобщения находят свое применение также в схемах аутентификации, хэш-функциях и псевдослучайных генераторах.

Широко исследуются различные обобщения, подклассы и надклассы бент-функций, такие как *платовидные функции*, *частично бент-функции*, *частично определенные бент-функции*, *q-значные бент-функции*, *обобщенные булевы бент-функции*, *полу-бент-функции*,

ненормальные бент-функции, *бент-функции на конечной абелевой группе*, *однородные бент-функции*, *гипер-бент-функции*, *$\mathbb{Z}-$бент-функции*, *нега-бент-функции* и др. С одной стороны эти исследования мотивированы высокой сложностью задачи описания бент-функций и являются попытками перехода к более общим (или более частным) ее постановкам — в надежде на частичное решение основной проблемы. С другой стороны интерес к обобщениям постоянно стимулируется новыми запросами со стороны приложений.

Обзоры некоторых результатов о бент-функциях можно найти в замечательной российской монографии [3] О. А. Логачева, А. А. Сальникова и В. В. Ященко (2004 год), статье [12] немецких криптографов Х. Доббертина и Г. Леандера (2004 год), главах [7] и [8] французского математика и криптографа К. Карле, написанных для готовящейся к печати книги «Boolean Methods and Models» (2008 год). Однако, любой обзор в этой области очень быстро устаревает и a priori неполон.

Цель работы — предложить новое обобщение бент-функций — *k-бент-функции*, — отражающее возможность поэтапного усиления (с ростом целого параметра k) нелинейных свойств булевой функции. Основная идея обобщения заключается в том, что принадлежность функции f классу бент-функций не исключает того, что f может оказаться достаточно хорошо аппроксимируемой функциями, являющимися нелинейными, но обладающими свойством «линейности в другом смысле». Опираясь на недавние результаты теории кодирования, связанные с исследованием альтернативной «линейности» кодов, мы выделим $m/2$ различных типов «линейности» булевой функции от m переменных, схожих с обычной линейностью. Для этого построим специальную серию из $m/2$ кодов типа Адамара, на каждом из которых возможно определение групповой операции, согласованной с метрикой Хэмминга. Кодовые слова этих кодов есть векторы значений булевых функций вида $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$, где операция $\langle \cdot, \cdot \rangle_k$ для каждого k, $1 \leqslant k \leqslant m/2$, является аналогом скалярного произведения векторов. Булеву функцию назовем *k-бент-функцией*, $1 \leqslant k \leqslant m/2$, если она максимально нелинейна при k различных типах «линейности» одновременно. В таком определении 1-бент-функции совпадают с обычными бент-функциями,

— т. е. «линейность» номер 1 есть линейность в обычном смысле, — а $(m/2)$-бент-функции могут считаться «наиболее нелинейными» в данной иерархии. Цель работы — исследовать свойства k-бент-функций, привести способы их построения, классифицировать такие функции от малого числа переменных и рассмотреть возможные приложения k-бент-функций в криптографии. А именно, исследовать возможность квадратичного криптоанализа блочных шифров на основе квадратичных аппроксимаций специального вида и показать, что использование k-бент-функций в качестве функций шифрования максимально повышает стойкость шифра к данным квадратичным аппроксимациям.

Методика исследований. В диссертации используются комбинаторные и алгебраические методы дискретного анализа, методы теории кодирования, теории графов и криптографии. Для построения примеров и проверки гипотез проводились компьютерные исследования (используемый язык программирования C++).

Научная новизна. Все результаты диссертации являются новыми и снабжены строгими доказательствами.

Апробация работы. Результаты докладывались на российских и международных конференциях: Шестой молодежной научной школе по дискретной математике и ее приложениям в 2007 году в Москве, ISIT'2007 — IEEE Международном Симпозиуме по Теории Информации в Ницце (Франция), Шестой школе-семинаре SIBECRYPT'07 — «Компьютерная безопасность и криптография» в Горно-Алтайске, международной конференции «Математика в современном мире» в Новосибирске в 2007 году, Четвертой международной конференции BFCA'2008 — «Булевы функции: криптография и приложения» в Копенгагене (Дания), 15-ой международной конференции «Проблемы теоретической кибернетики» в Казани в 2008 году, SIBIRCON-2008 — IEEE Международной Конференции «Вычислительные Технологии в Электрической и Электронной Инженерии» в Новосибирске, Седьмой школе-семинаре SIBECRYPT'08 — «Компьютерная безопасность и криптография» в Красноярске.
Результаты докладывались на семинарах «Дискретный анализ», «Теория кодирования», «Геометрия, топология и их приложения»

и общеинститутском семинаре Института Математики СО РАН; научных семинарах Института проблем передачи информации имени А. А. Харкевича в Москве; лаборатории информатики, сигналов и систем национального центра научных исследований (I3S CNRS) в Софии Антиполисе (Франция); кафедры защиты информации и криптографии Томского государственного университета. Результаты кандидатской диссертации отмечены премией школы «Компьютерная безопасность и криптография» — SIBECRYPT'07 — в 2007 году. Работа выполнена при поддержке интеграционного проекта СО РАН N 35 «Древовидный каталог математических Интернет-ресурсов mathtree.ru», Российского фонда фундаментальных исследований (проекты 07-01-00248, 08-01-00671), гранта «Лучшие аспиранты РАН» за 2008 год Фонда содействия отечественной науке, гранта «NUGET» (Agence Nationale de la Recherche, France), совета научной молодежи ИМ СО РАН и Новосибирского государственного университета.

Основные результаты диссертации.

1. На множестве двоичных векторов длины m введены новые бинарные операции $\langle \mathbf{u}, \mathbf{v} \rangle_k$, являющиеся аналогами скалярного произведения. Исследованы их свойства. Определены новые понятия ***k-нелинейности*** и ***k-преобразования Уолша—Адамара*** булевой функции.

2. Введено новое обобщение понятия бент-функции — ***k-бент-функция***, — отражающее возможность поэтапного усиления нелинейности булевой функции с ростом целого параметра k. Бент-функции и 1-бент-функции совпадают. Доказано, что класс k-бент-функций строго вложен в класс ℓ-бент-функций при $k > \ell$.

3. Предложены способы построения k-бент-функций и исследованы их свойства. Доказано существование k-бент-функций от m переменных любой степени нелинейности d, где $2 \leqslant d \leqslant \max\{2, (m/2) - k + 1\}$.

4. Классифицированы k-бент-функции от малого числа переменных.

5. Исследованы квадратичные аппроксимации вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, где $\mathbf{v}$ — вектор переменных; перестановка π, целое k и вектор $\mathbf{u}$ — параметры. Показано, что использование k-бент-функций в качестве

функций шифрования максимально повышает стойкость блочного шифра к таким аппроксимациям.

6. Рассмотрены четырехразрядные подстановки, рекомендованные для S-блоков алгоритмов ГОСТ 28147-89, DES, s^3DES; с помощью компьютера показано, что для всех этих подстановок (кроме одной) существуют более вероятные (по сравнению с линейными) квадратичные приближения функциями вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$.

7. Отмечена аналогия между проблемами нижних—верхних оценок числа бент-функций и двоичных кодов, таких как совершенные и равномерно упакованные. Для числа равномерно упакованных двоичных кодов установлена новая (лучшая на данный момент) верхняя оценка.

Практическая и теоретическая ценность. Результаты, представленные в диссертации, носят теоретический характер, но могут иметь непосредственные приложения в теории кодирования и криптографии.

На защиту выносится совокупность результатов о k-бент-функциях: их свойства, конструкции, связи с кодами, результаты по использованию k-бент-функций для построения стойких блочных шифров.

Публикации. По теме диссертации опубликовано 13 работ, [26–38]. Из них 4 статьи в журналах, 9 работ в трудах и тезисах международных конференций. На web-странице `www.math.nsc.ru/~tokareva` работы и текст диссертации доступны в электронном виде.

Структура и объем работы. Диссертация состоит из введения, пяти глав, заключения, предметного указателя и списка литературы из 153-х наименований. Общий объем работы — 120 страниц.

СОДЕРЖАНИЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Во **введении** обсуждается актуальность исследования бент-функций и их обобщений; дается обзор полученных результатов.

В **первой главе** диссертации приводятся основные понятия и обзор известных результатов о бент-функциях. Особое внимание уделяется существующим обобщениям бент-функций, пока еще очень слабо

освещенным в обзорной литературе. Отдельный раздел главы посвящен векторным бент-функциям. Отмечается аналогия между проблемами нижних—верхних оценок для числа бент-функций и числа двоичных кодов, таких как совершенные и равномерно упакованные. Для числа равномерно упакованных двоичных кодов в **Теореме 1** устанавливается новая (лучшая на данный момент) верхняя оценка (доказательство теоремы приведено в главе 5).

Во **второй главе** вводится специальная серия двоичных кодов типа Адамара, с помощью которой определяются бинарные операции $\langle\cdot,\cdot\rangle_k$ на множестве двоичных векторов и изучаются их свойства; определяются *k-преобразование Уолша—Адамара*, *k-нелинейность* булевой функции, и вводится понятие *k-бент-функции*.

С 90-х годов в теории кодирования активно стали исследоваться нелинейные коды, образы которых под действием подходящих (как правило, взаимно-однозначных и изометричных) отображений в другие метрические пространства линейны. Так, ярким примером служат *$\mathbb{Z}_4$-линейные коды* — двоичные коды, прообразы которых относительно *отображения Грея*

$$\varphi : 0 \to 00, 1 \to 01, 2 \to 11, 3 \to 10,$$

являются линейными кодами над кольцом $\mathbb{Z}_4$. Интересно, что многие нелинейные в обычном смысле двоичные коды (среди них коды Кердока, Препараты, Геталса и др.) оказались $\mathbb{Z}_4$-линейными, см. работы 1989 года А. А. Нечаева [4] и П. Солé [25], работу 1994 года А. Р. Хэммонса и др. [13]. Можно сказать, что это явление *альтернативной линейности*, которое удалось обнаружить, послужило ключом к структуре таких кодов и впервые позволило перенести богатый аппарат линейных методов теории кодирования в нелинейную область. В данной диссертации альтернативный подход к линейности используется для изучения булевых функций.

Рассмотрим $\mathbb{Z}_2$- и $\mathbb{Z}_4$-линейные коды с параметрами кодов Адамара (далее кратко — *коды типа Адамара*). Известно, что $\mathbb{Z}_2$-линейный (т. е. линейный в обычном смысле) двоичный код Адамара длины 2^m единствен с точностью до эквивалентности. Д. С. Кротовым [18] было показано, что существуют в точности $\lfloor m/2 \rfloor$ попарно неэквивалентных $\mathbb{Z}_4$-линейных кодов типа Адамара длины 2^{m+1} при $m > 2$.

Опираясь на классификацию [18] всех таких кодов, рассмотрим специальную серию двоичных кодов типа Адамара A_m^k, $1 \leqslant k \leqslant m/2$, длины 2^m (m четно). В этой серии каждый код A_m^k получается из линейного над $\mathbb{Z}_4$ кода $\mathcal{A}_m^k$ заменой элементов $0, 1$ на 0 и элементов $2, 3$ на 1 в каждой координате, где $\mathcal{A}_m^k$ — подкод соответствующего линейного четверичного кода Адамара типа $4^k 2^{m-2k}$ (см. [18]), состоящий из всех кодовых векторов, имеющих в первой координате только 0 или 2. Каждый код A_m^k образует абелеву группу относительно операции $\bullet$, индуцированной операцией $+$ покоординатного сложения над $\mathbb{Z}_4$, определенной на векторах кода $\mathcal{A}_m^k$.

Теорема 2. *При четном m, целом k, $1 \leqslant k \leqslant m/2$, выполняются*
(i) *код A_m^k является кодом с параметрами кода Адамара;*
(ii) *код A_m^1 линеен, коды $A_m^1, \ldots, A_m^{m/2}$ попарно неэквивалентны;*
(iii) *операция $\bullet$, заданная на A_m^k, согласована с метрикой Хэмминга.*

Множество $\mathfrak{A}_m^k$ булевых функций, векторами значений которых являются кодовые векторы кода A_m^k, представляет собой аналог множества аффинных функций — это функции вида $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$, где $a \in \mathbb{Z}_2$ и операция $\langle \cdot, \cdot \rangle_k$ играет роль скалярного произведения. Такие функции далее названы *k-аффинными*[4] . Коды A_m^k выбраны таким образом, чтобы операции $\langle \cdot, \cdot \rangle_k$ обладали многими свойствами обычного скалярного произведения и на их основе оказались возможными конструктивные построения. Отметим, что каждая операция $\langle \cdot, \cdot \rangle_k$ при $k \geqslant 2$ не является билинейной формой. Явный вид операции $\langle \mathbf{u}, \mathbf{v} \rangle_k$ следующий.

Теорема 3. *Пусть m, k — целые, $1 \leqslant k \leqslant m/2$. Для любого целого i, $1 \leqslant i \leqslant m/2$, любых $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ пусть $Y_i = (u_{2i-1} \oplus u_{2i})(v_{2i-1} \oplus v_{2i})$. Тогда*

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \Big(\bigoplus_{i=1}^{k} \bigoplus_{j=i}^{k} Y_i Y_j \Big) \oplus \langle \mathbf{u}, \mathbf{v} \rangle.$$

[4]Необходимо отметить, что термин «k-аффинная функция» в другом значении уже использовался ранее М. Л. Буряковым и О. А. Логачевым [1]. Параметр k в их работе играет роль *уровня аффинности* булевой функции и не имеет ничего общего с параметром, определяемым здесь. К сожалению, такое совпадение терминов было замечено уже достаточно поздно.

Каждый класс функций $\mathfrak{A}_m^k$ состоит из $2^{m-k+1}(k+1)$ аффинных функций и $2^{m-k+1}(2^k-k-1)$ квадратичных функций.
С помощью операции $\langle\cdot,\cdot\rangle_k$ определяются *k-преобразование Уолша—Адамара* $W_f^{(k)}$ и *k-нелинейность* $N_f^{(k)}$ булевой функции f. Верна

Теорема 4 (равенство Парсеваля для $W_f^{(k)}$). *Для любой булевой функции f от m переменных выполняется*

$$\sum_{\mathbf{v}\in\mathbb{Z}_2^m}\left(W_f^{(k)}(\mathbf{v})\right)^2 = 2^{2m}.$$

Булеву функцию от четного числа переменных m назовем *максимально k-нелинейной (k-бент-) функцией*, $1 \leqslant k \leqslant m/2$, если вектор значений этой функции удален на максимально возможное расстояние $2^{m-1} - 2^{(m/2)-1}$ от каждого кода типа Адамара A_m^j, $j = 1,\ldots,k$ (или, что эквивалентно, $W_f^{(j)}(\mathbf{v}) = \pm 2^{m/2}$ для любого $\mathbf{v}\in\mathbb{Z}_2^m$ и каждого $j = 1,\ldots,k$). Другими словами, каждая k-бент-функция одинаково плохо аппроксимируется булевыми функциями из каждого класса $\mathfrak{A}_m^j$, $j = 1,\ldots,k$. Обычные бент-функции представляют собой класс 1-бент-функций. Через $\mathfrak{B}_m^k$ обозначим класс всех k-бент-функций от m переменных.
Результаты второй главы опубликованы в работах [26, 30, 31, 32].

В **третьей главе** изучаются способы построения k-бент-функций и их свойства. Известно, что задача описания бент-функций для произвольного числа переменных m, или хотя бы нахождения хороших нижних и верхних оценок числа таких функций является очень сложной. Об этом свидетельствует, например, тот факт, что число 6 является максимальным значением для m, при котором еще известно точное значение числа бент-функций (равное $5\,425\,430\,528 \simeq 2^{32,3}$, см. описание в [5]), несмотря на длительный срок их исследования и большой интерес к этим объектам. В первой части третьей главы дается простое описание класса 2-бент-функций от четырех переменных.

Теорема 5. *Пусть параметры i_1, i_2, i_3 и i_4 принимают различные целые значения от 1 до 4. Тогда множество функций $\mathfrak{B}_4^2$ состоит из всех функций степени 2 с квадратичными частями вида:*

$v_{i_1}v_{i_2} \oplus v_{i_3}v_{i_4}$ (3 *типа*);
$v_{i_1}v_{i_2} \oplus v_{i_1}v_{i_3} \oplus v_{i_2}v_{i_4}$ *при* $\{i_1, i_2\} = \{1, 2\}$ *или* $\{3, 4\}$ (4 *типа*);
$v_{i_1}v_{i_2} \oplus v_{i_2}v_{i_3} \oplus v_{i_3}v_{i_4} \oplus v_{i_1}v_{i_3}$ *при* $\{i_1, i_2\} = \{1, 2\}$ *или* $\{3, 4\}$ (4 *типа*);
$v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$ (1 *тип*).

Тем самым, параметр $m = 6$ становится наименьшим, при котором k-бент-функции пока не описаны.

Во второй части главы приводится итеративная конструкция k-бент-функций. Пусть $\mathfrak{F}_m$ — множество булевых функций от m переменных, $\mathfrak{F}_2^1$ — множество симметрических функций от двух переменных.

Теорема 6. *Пусть числа* $m, r \geqslant 0$ *четны,* $j \geqslant 0$ *— любое,* k *такое, что* $1 \leqslant k \leqslant m/2$*, и пусть функция* $f \in \mathfrak{F}_{2j+m+r}$ *представима в виде*

$$f(a_1, a'_1, \ldots, a_j, a'_j, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^{j} s_i(a_i, a'_i) \right) \oplus p(\mathbf{u}') \oplus q(\mathbf{u}''),$$

где $s_1, \ldots, s_j \in \mathfrak{F}_2^1, p \in \mathfrak{F}_m$ *и* $q \in \mathfrak{F}_r$ *— функции с непересекающимися множествами переменных. Тогда* f *принадлежит классу* $\mathfrak{B}_{2j+m+r}^{j+k}$*, если и только если* $s_1, \ldots, s_j \in \mathfrak{B}_2^1$*,* $p \in \mathfrak{B}_m^k$ *и* $q \in \mathfrak{B}_r^1$*.*

В качестве следствия устанавливается, что для $k > \ell \geqslant 1$ класс k-бент-функций $\mathfrak{B}_m^k$ является собственным подклассом класса ℓ-бент-функций $\mathfrak{B}_m^\ell$. Показывается, что существуют k-бент-функции с любой степенью нелинейности d, где $2 \leqslant d \leqslant \max\{2, (m/2)-k+1\}$. Напомним, что *степенью нелинейности* булевой функции называется число переменных в самом длинном слагаемом ее алгебраической нормальной формы (или многочлена Жегалкина).

Пусть $S_{m,k}$ — подгруппа группы S_m подстановок на m элементах, порожденная k транспозициями: $(1, 2), (3, 4), \ldots, (2k-1, 2k)$. Пусть $\mathfrak{F}_m^k$ обозначает множество всех функций $f \in \mathfrak{F}_m$, постоянных на каждой орбите множества $\mathbb{Z}_2^m$ под действием группы $S_{m,k}$; справедливо $|\mathfrak{F}_m^k| = 2^{2^{m-k\log_2\frac{4}{3}}}$. Доказана следующая теорема о связи k-бент-функций и бент-функций.

Теорема 7. *При любом четном* $m \geqslant 2$*, целом* k*,* $1 \leqslant k \leqslant m/2$*, справедливо равенство* $\mathfrak{F}_m^k \cap \mathfrak{B}_m^k = \mathfrak{F}_m^k \cap \mathfrak{B}_m^1$*.*

Результаты третьей главы опубликованы в работах [32, 33, 37].

В **четвертой главе** исследуется возможность квадратичного криптоанализа блочных шифров, в основу которого положены квадратичные аппроксимации специального вида, и роль k-бент-функций при конструировании таких шифров. Квадратичный криптоанализ является нелинейной модификацией известного метода линейного криптоанализа блочных шифров, предложенного М. Мацуи [19] в 1993 году для шифров FEAL и DES и являющегося в настоящее время одним из наиболее эффективных.
Идея метода линейного криптоанализа заключается в следующем. Сначала для известного алгоритма шифрования определяется линейное соотношение L на биты открытого текста, шифротекста и ключа, выполняющееся с вероятностью $p = 1/2+\varepsilon$, достаточно сильно отличающейся от $1/2$. Число ε называется *преобладанием* соотношения L. Затем при фиксированном неизвестном ключе K криптоаналитиком собирается статистика из N пар {открытый текст — соответствующий шифротекст}, и на ее основе с учетом знака ε производится различение двух простых статистических гипотез: выполняется ли соотношение L для данного неизвестного ключа K или нет. В результате для битов ключа K устанавливается новое вероятностное соотношение. Для надежной работы этого метода мощность статистики N должна быть пропорциональна величине $|\varepsilon|^{-2}$.
Общий подход к использованию в линейном криптоанализе нелинейных аппроксимаций предложили в 1996 году Л. Кнудсен и М. Робшау [17]. Основная его идея: обогатить класс аппроксимирующих функций нелинейными функциями и за счет этого повысить качество аппроксимации. Но при этом криптоаналитику придется столкнуться со следующими трудностями. *Как эффективно выбрать хорошую нелинейную аппроксимацию?* В линейном случае возможно решение такой задачи перебором всех 2^m линейных функций (от m переменных). В общем случае полный перебор 2^{2^m} булевых функций неосуществим даже при малых значениях m. *Как объединить нелинейные аппроксимации отдельных раундов?* В целом метод нелинейного криптоанализа не получил пока должного развития.

В данной работе предлагается аппроксимировать булевы функции от m переменных $v_1, \ldots, v_m$ функциями вида $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, где π —

любая перестановка на m переменных, параметры $\mathbf{u} \in \mathbb{Z}_2^m$, k ($1 \leqslant k \leqslant m/2$) произвольны. Класс Δ_m всех таких аппроксимирующих функций может быть описан следующим образом. Пусть АНФ(f) — алгебраическая нормальная форма функции f; пусть $\mathrm{Act}(f)$ — подмножество максимальной мощности множества $\{1, 2, \ldots, m/2\}$ такое, что для любых различных элементов i, j из $\mathrm{Act}(f)$ одночлены $v_{2i-1}v_{2j-1}$, $v_{2i-1}v_{2j}$, $v_{2i}v_{2j-1}$, $v_{2i}v_{2j}$ принадлежат множеству АНФ(f). Через $\rho = \rho(f)$ обозначим любую перестановку m переменных такую, что $|\mathrm{Act}(f^\rho)| = \max\limits_{\pi \in S_m} |\mathrm{Act}(f^\pi)|$, где по определению $f^\pi(\cdot) = f(\pi(\cdot))$. Справедлива

Теорема 8. *Булева функция $f \in \mathfrak{F}_m$, степени не больше двух, такая что $f(\mathbf{0}) = 0$, принадлежит классу Δ_m тогда и только тогда, когда f удовлетворяет условиям*

1) *для любых различных чисел i, j ($1 \leqslant i, j \leqslant m/2$) одночлены*

$$v_{2i-1}v_{2j-1},\ v_{2i-1}v_{2j},\ v_{2i}v_{2j-1},\ v_{2i}v_{2j}$$

одновременно принадлежат / не принадлежат АНФ(f^ρ);

2) *множество* АНФ(f^ρ) *не содержит одночлены вида $v_{2i-1}v_{2i}$*;

3) *в точности одна из переменных v_{2i-1}, v_{2i} принадлежит* АНФ(f^ρ) *для каждого элемента $i \in \mathrm{Act}(f^\rho)$.*

Из теоремы 8 следует, что множество аппроксимирующих функций состоит из 2^m (т. е. всех) линейных функций и не более чем $2^{m(1+\log_2 m)}$ квадратичных функций, что не ограничивает криптоаналитика в возможности их полного перебора.

Выбор таких функций для аппроксимации обусловлен наличием простых формул для вычисления расстояния Хэмминга от произвольной булевой функции f до класса $\mathfrak{A}_{m,0}^k(\pi)$ функций $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$ при фиксированных параметрах π и k:

$$\mathrm{dist}(f, \mathfrak{A}_{m,0}^k(\pi)) = 2^{m-1} - \frac{1}{2} \max_{\mathbf{v} \in \mathbb{Z}_2^m} W_f^{(k)}(\pi(\mathbf{v})),$$

а также свойствами таких функций, близкими к линейным.
Исследования носят теоретический характер. Предложены модификации алгоритмов 1 и 2 линейного криптоанализа Мацуи [19] для

расширенного класса аппроксимирующих функций. Приведены формулы для вычисления абсолютных значений преобладаний и надежности алгоритмов. Показано, что использование k-бент-функций в качестве функций шифрования позволяет снижать максимальное абсолютное значение преобладания до его минимального значения, а следовательно максимально повышать стойкость шифра к данным квадратичным аппроксимациям.
Пусть $F : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m_{\text{key}}} \to \mathbb{Z}_2^m$ — функция шифрования блочного шифра; P, C и K — открытый текст, шифротекст и ключ соответственно. Пусть вещественное число $\varepsilon(K)$ — преобладание равенства

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = \langle \mathbf{d}, \tau(K) \rangle_k,$$

при фиксированном ключе K, где $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^m$, $\mathbf{d} \in \mathbb{Z}_2^{m_{\text{key}}}$, перестановки $\pi, \sigma \in S_m$, $\tau \in S_{m_{\text{key}}}$, целые числа i, j, k — некоторым образом выбранные параметры. Упомянутую выше роль k-бент-функций в блочном шифре отражает следующее утверждение.

Теорема 9. *Пусть фиксирован ключ K. Если вектор $\mathbf{b}$, перестановки π, σ и параметр j, таковы что функция*

$$\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$$

является $(m/2)$-бент-функцией, то справедливо равенство

$$\max_{i,k,\mathbf{a},\mathbf{d},\tau} |\varepsilon(K)| = \min_{i,k,\mathbf{a},\mathbf{d},\tau} |\varepsilon(K)| = 2^{-(m/2)-1}.$$

Приведены свойства аппроксимирующих функций $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, которые могут быть использованы при согласовании нелинейных раундовых аппроксимаций в квадратичном криптоанализе. В заключение рассмотрены примеры четырехразрядных подстановок, рекомендованных для применения в узлах замены (S-*блоках*) алгоритмов ГОСТ 28147-89, DES, s^3DES; с помощью компьютера показано, что для всех этих подстановок (кроме одной) существуют более вероятные (по сравнению с линейными) квадратичные соотношения специального вида на входные и выходные биты этих подстановок.
Результаты четвертой главы опубликованы в работах [35, 36, 38].

В **пятой главе** диссертации приводится доказательство Теоремы 1, формулировка которой дана в первой главе. Результаты главы опубликованы в работах [27, 28, 29].

Благодарности. Я искренне признательна своему научному руководителю Ю. Л. Васильеву (Институт математики им. С. Л. Соболева) за неизменную поддержку и постоянное внимание к данной работе. Моя самая глубокая благодарность А. А. Нечаеву (Московский государственный университет) и Л. А. Бассалыго (Институт проблем передачи информации им. А. А. Харкевича, Москва), проявившим неподдельный интерес к моей работе и высказавшим немало ценных замечаний и критики. Я очень благодарна сотрудникам института математики им. С. Л. Соболева: Д. С. Кротову — за ценные замечания, позволившие существенно расширить множество кодов, для которых справедлива Теорема 1, и В. Н. Потапову, взявшему на себя труд прочитать рукопись и указавшему на целый ряд неточностей. Мне очень приятно выразить признательность профессору Патрику Солé (Национальный Центр Научных Исследований — CNRS, — София Антиполис, Франция) за гостеприимство и увлекательную совместную работу в области бент-функций, благодаря которой удалось узнать много нового. С большим удовольствием я благодарю Лилию Будагян (Университет Бергена, Норвегия) за консультации по векторным бент-функциям, внимательное прочтение текста и замечания, которые трудно переоценить. Отдельную благодарность я приношу всем рецензентам печатных работ, обратившим мое внимание на многие существенные вопросы.

Список литературы

[1] *Буряков М. Л., Логачев О. А.* Об уровне аффинности булевых функций // Дискретная математика. 2005. Т. 17, N 4. С. 98–107.

[2] *Кротов Д. С.* $\mathbb{Z}_4$-линейные совершенные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, N 4. С. 78–90 (translated at `http://arxiv.org/abs/0710.0198`).

[3] *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004.

[4] *Нечаев А. А.* Код Кердока в циклической форме // Дискретная математика. 1989. Т. 1, N 4. С. 123–139.

[5] *Agievich S. V.* On the representation of bent-functions by bent-rectangles // Fifth Int. Petrozavodsk conf. on probabilistic methods in discrete mathematics (Petrozavodsk, Russia. June 1–6, 2000). Proc. Boston: VSP, 2000. P. 121–135.

[6] *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4, N 1. P. 3–72.

[7] *Carlet C.* Boolean functions for cryptography and error correcting codes // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at `www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`.

[8] *Carlet C.* Vectorial Boolean functions for cryptography // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at `www-rocq.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf`.

[9] *Carlet C., Klapper A.* Upper bounds on the numbers of resilient functions and of bent functions // 23rd Symposium on Information Theory (Benelux, Belgium. May, 2002) Proc. 2002. P. 307-314. The full version will appear in Lecture Notes dedicated to Philippe Delsarte.

[10] *Dillon J. F.* A survey of bent functions // The NSA Technical J. 1972. Special Issue. P. 191–215.

[11] *Dillon J. F.* Elementary Hadamard difference sets // Ph. D. Thesis, Univ. of Maryland, 1974.

[12] *Dobbertin H., Leander G.* A survey of some recent results on bent functions // Sequences and their applications. – SETA 2004. Third Int. conference (Seul, Korea. October 24–28, 2004). Revised selected papers. Berlin: Springer, 2005. P. 1–29 (Lecture Notes in Comput. Sci. V. 3486).

[13] *Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P.* The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. V. 40, N 2. P. 301–319.

[14] *Kantor W. M.* Codes, quadratic forms and finite geometries // Proceedings of Symposia in Applied Math. 1995. V. 50. P. 153–177.

[15] *Kavut S., Maitra S., Yucel M. D.* Search for Boolean functions with excellent profiles in the rotation symmetric class // IEEE Trans. Inform. Theory. 2007. V. 53, N 5. P. 1743–1751.

[16] *Kerdock A. M.* A class of low-rate non-linear binary codes // Inform. Control. 1972. V. 20, N 2. P. 182–187.

[17] *Knudsen L. R., Robshaw M. J. B.* Non-linear approximation in linear cryptanalysis // Advances in Cryptology – EUROCRYPT'96. Workshop on the theory and application of cryptographic techniques (Saragossa, Spain. May 12–16, 1996). Proc. Springer-Verlag. 1996. P. 224–236 (Lecture Notes in Comput. Sci. V. 1070).

[18] *Krotov D. S.* $\mathbb{Z}_4$-linear Hadamard and extended perfect codes // Proc. of the Int. Workshop on Coding and Cryptography (Paris, France. January 8–12, 2001). P. 329–334.

[19] *Matsui M.* Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT'93. Workshop on the theory and application of cryptographic techniques (Lofthus, Norway. May 23–27, 1993). Proc. Berlin: Springer, 1994. P. 386–397 (Lecture Notes in Comput. Sci. V. 765).

[20] *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15, N 1. P. 1–10.

[21] *Olsen J. D., Scholtz R. A., Welch L. R.* Bent-function sequences // IEEE Trans. Inform. Theory. 1982. V. 28, N 6. P. 858–864.

[22] *Riera C., Parker M.G.* Generalised bent criteria for Boolean functions (I) // IEEE Trans. Inform. Theory 2006. V. 52, N 9. P. 4142–4159.

[23] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20, N 3. P. 300–305.

[24] *Schmidt K-U.* Quaternary constant-amplitude codes for multicode CDMA // Available at `http://arxiv.org/abs/cs.IT/0611162`.

[25] *Solé P.* A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties // Third International Colloquium «Coding Theory and Applications» (Toulon, France. November 2–4, 1988). Proc. Springer. 1989. P. 193–201 (Lecture Notes in Comput. Sci. V. 388).

Публикации автора по теме диссертации (доступны по адресу `www.math.nsc.ru/∼tokareva`)

[26] *Токарева Н. Н.* Иерархия классов бент-функций кратной нелинейности // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, Россия. 16–21 апреля, 2007) Часть III, 2007. С. 5–11.

[27] *Токарева Н. Н.* О верхней оценке числа равномерно упакованных двоичных кодов // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, Россия. 16–21 апреля, 2007) Часть III, 2007. С. 11–16.

[28] *Tokareva N. N.* An upper bound for the number of uniformly packed codes // IEEE International Symposium on Information Theory — ISIT'2007. (Nice, France. June 24–29, 2007). Proc. 2007. P. 346–350.

[29] *Токарева Н. Н.* О верхней оценке числа равномерно упакованных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14, N 3. С. 90–97.

[30] *Tokareva N. N.* On k-bent functions // Вестник Томского госуниверситета. Приложение. 2007. N 23. С. 74–76.

[31] *Токарева Н. Н.* Бент-функции кратной нелинейности: k-бент-функции // Материалы российской конференции «Математика в современном мире» (Новосибирск, Россия. 17–21 сентября, 2007). С. 288–289.

[32] *Токарева Н. Н.* Бент-функции с более сильными свойствами нелинейности: k-бент-функции // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14, N 4. С. 76–102.

[33] *Tokareva N. N.* k-Bent functions and quadratic approximations in block ciphers // Proc. Fourth International Conference BFCA — Boolean Functions: Cryptography and Applications (Copenhagen, Denmark, May 19–21, 2008). P. 132–148.

[34] *Токарева Н. Н.* k-Преобразование Уолша-Адамара в теории кодирования и криптографии // Материалы XV Международной конференции «Проблемы теоретической кибернетики» (Казань, Россия, 2–7 июня, 2008). С. 113–114.

[35] *Tokareva N. N.* k-Bent functions: from coding theory to cryptology // Proc. First IEEE International Conference SIBIRCON — Computational Technologies in Electrical and Electronics Engineering (Novosibirsk, Russia, July 21–25, 2008). P. 36–40.

[36] *Токарева Н. Н.* О квадратичных аппроксимациях в блочных шифрах // Пробл. передачи информ. 2008. Т. 44, Вып. 3. С. 105–127.

[37] *Токарева Н. Н.* Описание k-бент-функций от четырех переменных // Дискр. анализ и исслед. операций. 2008. Т. 15, N 4. С. 74–83.

[38] *Токарева Н. Н.* Квадратичные аппроксимации специального вида для четырехразрядных подстановок в S-блоках // Прикладная дискретная математика. 2008. Т. 1, N 1. С. 50–54.

Токарева Наталья Николаевна

Сильно нелинейные булевы функции: бент-функции и их обобщения

Автореферат диссертации на соискание ученой степени кандидата физико-математических наук

Подписано в печать 2 октября 2008 г. Формат 60x84 1/16.
Усл. печ. л. 1,4. Уч.-изд. л. 1,4.
Тираж 140 экз. Заказ N 173.

Отпечатано в ООО "Омега Принт"
630090 Новосибирск, пр. Лаврентьева, 6.