Московский государственный университет имени М.В.Ломоносова

На правах рукописи

Смышляев Станислав Витальевич

КОМБИНАТОРНЫЕ СВОЙСТВА СОВЕРШЕННО УРАВНОВЕШЕННЫХ БУЛЕВЫХ ФУНКЦИЙ

Специальность **05.13.19.** —
Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2012

Работа выполнена на кафедре математической кибернетики факультета Вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова.

Научный руководитель: *кандидат физико-математических наук, старший научный сотрудник, Логачев Олег Алексеевич;*

Официальные оппоненты:

Михайлов Владимир Гаврилович доктор физико-математических наук, старший научный сотрудник (ФГБУН "Математический институт имени В.А. Стеклова Российской академии наук")

Таранников Юрий Валерьевич кандидат физико-математических наук, доцент (ФГБОУ ВПО "Московский государственный университет имени М.В.Ломоносова")

Ведущая организация: *ОАО «Концерн "Автоматика"»*

Защита диссертации состоится 19 декабря 2012 года в 16 ч. 45 м. на заседании диссертационного совета *Д.501.002.16* при Московском государственном университете имени М.В. Ломоносова по адресу: РФ, 119991, Москва, ГСП-1, Ленинские горы, д. 1, МГУ, Главное здание, механико-математический факультет, аудитория 14-08.
С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ имени М.В. Ломоносова (Главное здание, 14 этаж).

Автореферат разослан «19» ноября 2012 г.

Ученый секретарь диссертационного
совета Д 501.002.16 при МГУ,
доктор физико-математических
наук, профессор Корнев Андрей Алексеевич

Общая характеристика работы

Актуальность темы.

Вопросы разработки методов и средств защиты информации, а также обоснование их эффективности является одним из важнейших направлений исследований в области обеспечения информационной безопасности в процессе сбора, хранения, обработки и передачи информации. При этом разработка и исследования свойств аппаратно-программных средств обеспечения информационной безопасности проводятся, как правило, с использованием математических моделей и методов.

Одним из важнейших классов математических моделей являются модели, построенные на основе использования булевых функций(систем булевых функций). Конкретные аппаратно-программные средства, обеспечивающие информационную безопасность, должны обладать определенными особенностями (качествами), вытекающими из реализуемых ими защитных функций в общей системе информационной безопасности. Особенности средств защиты находят свое отражение в булевых математических моделях в виде ряда специфических свойств используемых булевых функций(систем булевых функций).

Значительная часть этих свойств связана с теорией кодирования или с криптологией и необходима для обеспечения конфиденциальности, целостности, идентификации, аутентификации и решения других задач информационной безопасности.

Одним из таких важных свойств булевых функций является свойство совершенной уравновешенности. С помощью совершенно уравновешенных функций можно синтезировать средства обеспечения информационной безопасности, обладающие необходимыми статистическими, теоретико-кодовыми и криптографическими свойствами. Совершенно уравновешенные функции(в соответствующей интерпретации) исследовались рядом авторов в рамках таких разделов математики, как теория дискретных функций, теория кодирования, символическая динамика и криптология. В теории динамических систем в разделе, называемом символической динамикой, они исследуются как «блоковые отображения», порождающие сюръективные эндоморфизмы символических динамических систем[1]. В теории кодирования они рассматриваются как ос-

[1] *Hedlund G. A.* **Endomorphisms and automorphisms of the shift dynamical system**. Theory of Computing Systems. 1969. Vol. 3(4). Pp. 320–375.

новные элементы «кодирующих устройств»[2], реализующих скользящие блоковые коды без потери информации[3] В математической криптографии и криптоанализе совершенно уравновешенные булевы функции изучаются как «функции усложнения» таких криптографических примитивов, как комбинирующие и фильтрующие генераторы. Соответствующее дискретное устройство, состоящее из проходного двоичного регистра сдвига и булевой функции, определяющей элементы выходных наборов, в различных источниках называют регистром сдвига с функцией усложнения, кодером, кодирующим устройством и т.п. Далее мы остановимся на термине "кодирующее устройство".

Одними из важнейших свойств используемых в криптологии и теории кодирования функций являются следующие:

1. принципиальная возможность получить на выходе кодирующего устройства произвольный двоичный набор;

2. в предположении о том, что входная последовательность кодирующего устройства представляет собой реализацию последовательности независимых в совокупности и равномерно распределенных (с вероятностями $\frac{1}{2}$ для нуля и единицы) случайных величин, выходная последовательность кодирующего устройства должна представлять собой реализацию последовательности таких же случайных величин;

3. возможность однозначного восстановления по любому выходному набору кодирующего устройства всех символов входного набора, если известны начало и конец (некоторой фиксированной длины) входного набора.

Булева функция, удовлетворяющая первому из перечисленных свойств, называется «функцией без запрета», второму — «сильно равновероятной функцией» (далее в работе будет использоваться термин «совершенно уравновешенная функция»), третьему — «функцией без потери информации».

Длительное время свойство совершенной уравновешенности булевой функции связывали с линейностью ее по первой (или по-

[2] *Huffman D. A.* **Canonical forms for information-lossless finite-state logical machines** IRE Transactions on Circuit Theory. 1959. Vol. 5. Pp. 41–59.

[3] *Adler R., Coppersmith D., Hassner M.* **Algorithms for sliding block codes — an application of symbolic dynamics to information theory** IEEE Transactions on Information Theory. 1983. Vol. 29(1). Pp. 5–22.

следней) переменной. Серьезные продвижения в исследовании совершенно уравновешенных булевых функций были сделаны Хэдлундом[1] и Сумароковым[4]. В частности, в них были сформулированы и доказаны необходимые и достаточные условия, связывающие свойство совершенной уравновешенности булевой функции со свойствами быть функцией без запрета и без потери информации. Было также показано, что свойства совершенной уравновешенности, отсутствия запрета и отсутствия потери информации эквивалентны. Кроме того, впервые был приведен пример совершенно уравновешенной булевой функции, не являющейся линейной по первой или последней переменной.

В диссертации исследуются вопросы, связанные со свойствами совершенно уравновешенных булевых функций и методами построения функций из данного класса.

Р. Андерсоном[5] были выявлены определенные криптографические слабости у ряда функций усложнения, используемых или предлагаемых для использования в системах потокового шифрования. Им же было сформулировано требование к функции усложнения, гарантирующее отсутствие слабостей данного вида и эквивалентное совершенной уравновешенности булевой функции, в связи с чем была поставлена задача построения классов таких функций и изучения их свойств.

Й. Голичем[6] был рассмотрен класс совершенно уравновешенных функций линейных по первой и/или последней переменной, было продемонстрировано негативное криптографическое свойство кодирующих устройств с такими функциями усложнения в случае использования их в системах потокового шифрования; более того, позднее Голичем был предложен метод криптоанализа («инверсионная атака»), существенно использующий это свойство. Была также показана достаточность линейной зависимости булевой функции от крайней переменной для того, чтобы функция оставалась совершенно уравновешенной при добавлении/изъятии произвольного числа несущественных переменных.

[4] *Сумароков С. Н.* **Запреты двоичных функций и обратимость для одного класса кодирующих устройств**. Обозрение прикладной и промышленной математики. 1994. 1(1). 33–55.

[5] *Anderson R. J.* **Searching for the optimum correlation attack**. **Lecture Notes in Computer Science**. 1995. Vol. 1008. Pp. 137–143.

[6] *Golić J. D.* **On the security of nonlinear filter generators**. Lecture Notes in Computer Science. 1996. Vol. 1039. Pp. 173–188.

Дихтлом[7] было продолжено исследование вопросов, поднятых в работе Голича — в частности, было сформулировано и доказано утверждение о необходимом условии совершенной уравновешенности, использование которого могло бы быть полезно для получения верхних оценок числа совершенно уравновешенных булевых функций. К сожалению, доказательство этого необходимого условия содержало ошибку и оно является верным только лишь для некоторого подмножества совершенно уравновешенных функций.

О. А. Логачевым[8] была введена (аналогично введенной Хэдлундом в операции композиции эндоморфизмов символических динамических систем) специальная операция композиции функций усложнения и было доказано, что данная операция сохраняет класс совершенно уравновешенных функций; был приведен пример, демонстрирующий возможность с помощью данной операции получать совершенно уравновешенные функции, нелинейно зависящие от первой и последней существенной переменной.

А. Гуже и Х. Сибер[9] провели исследование связи свойств функций в модели с равномерным распределением на множестве входных последовательностей кодирующего устройства[10] и в модели с рекуррентной последовательностью небольшого периода. При анализе оптимального в определенном смысле класса функций в первой из моделей (класса совершенно уравновешенных функций) Гуже и Сибер столкнулись с существенными трудностями. По этой причине Гуже и Сибер уделили большее внимание рассмотрению класса функций, обладающих положительными свойствами во второй из рассматриваемых ими моделей, — класса квази-иммунных функций, который был описан в терминах свойств полиномов Жегалкина и оказался значительно более удобным для анализа.

В литературе также обсуждался вопрос получения верхних оценок длины запрета (минимальной длины набора, который нельзя получить на выходе кодирующего устройства) функций, не являю-

[7] *Dichtl M.* **On nonlinear filter generators**. Lecture Notes in Computer Science. 1997. Vol. 1267. Pp. 103–106.

[8] *Логачев О. А.* **Об одном классе совершенно уравновешенных булевых функций**. **Материалы Третьей Международной Научной Конференции по Проблемам Безопасности и Противодействия Терроризму (МаБИТ-2007)**. 2008. 137–141.

[9] *Gouget A., Sibert H.* **Revisiting correlation immunity in filter generators** Lecture Notes in Computer Science. 2007. Vol. 4876. Pp. 378–395.

[10] *Golić J. D.* **Conditional correlation attack on combiners with memory**.Electronics Letters. 1996. Vol. 32(24). Pp. 2193–2195.

щихся совершенно уравновешенными[11].

Несмотря на немалое количество работ, в которых уделялось большое внимание совершенной уравновешенности булевых функций, большинство исследований и рассмотрений, за небольшим исключением, касались функций, линейных по первой и/или последней существенной переменной — узкого и наименее интересного подмножества совершенно уравновешенных функций. Исследование совершенно уравновешенных функций, нелинейных по крайним (первой и последней) существенным переменным, ограничивалось исключительно примерами таких функций. Одним из неприятных следствий такого подхода стал ряд неверных результатов, полученных при попытках обобщения свойств функций линейных по крайним переменным на все совершенно уравновешенные функции.

С другой стороны, как было отмечено Й. Голичем, линейность функции по одной из крайних переменных является серьезным недостатком функции усложнения в случае использования кодирующего устройства с данной функцией в качестве примитива в системах потокового шифрования. Кроме того, достаточно широкий подкласс линейных по последней переменной функций, как показано О. А. Логачевым, обладает негативным для ряда криптографических приложений свойством локальной обратимости.

Таким образом, является важной задача разработки математического аппарата для исследования алгебраических, комбинаторных и криптографических свойств совершенно уравновешенных булевых функций, нелинейно зависящих от крайних переменных, а также разработка методов построения классов совершенно уравновешенных функций с определенными положительными криптографическими качествами.

Цель диссертационной работы заключается

1) в разработке математического аппарата исследования комбинаторных и криптографических свойств совершенно уравновешенных булевых функций;

2) в исследовании связей между совершенной уравновешенностью булевых функций и возможностью обращения соответствующих кодирующих устройств в различных моделях;

[11] *Бабаш А. В.* **Запреты автоматов и двоичных функций**. Труды по дискретной математике. 2006. 9. 7–20.

3) в разработке методов построения классов совершенно уравновешенных булевых функций.

Методологической основой и научно-теоретической базой диссертации являются работы С.Н. Сумарокова, О.А. Логачева, Й. Голича, М. Дихтла, Кс. Лэя и Дж. Месси о свойствах совершенно уравновешенных булевых функций.

В диссертации применялись методы теории булевых функций, теории графов, комбинаторного анализа.

Научная новизна. Все результаты диссертации являются новыми. Основные результаты диссертационной работы состоят в следующем.

1) Разработан эффективный алгоритм распознавания свойства совершенной уравновешенности булевой функции по вектору значений. С помощью программной реализации данного алгоритма получено полное описание совершенно уравновешенных булевых функций от 4 и 5 переменных.

2) Для класса булевых функций с барьером длины 3 доказан критерий принадлежности произвольной функции данному классу. Получены новые верхняя и нижняя асимптотические оценки логарифма мощности данного класса. Получены новые нижние асимптотические оценки логарифма числа совершенно уравновешенных булевых функций, не являющихся линейными по крайним существенным переменным.

3) Описаны параметры, определяющие структуру прообразов выходных наборов кодирующих устройств с совершенно уравновешенными функциями, имеющими барьер. Доказаны утверждения, связывающие данные параметры с другими комбинаторными свойствами таких функций, позволившие доказать критерий наличия у булевой функции свойства, констатирующего невозможность получить ненулевую информацию о выходных символах кодирующего устройства по предшествующим выходным символам и начальным входным символам.

4) Доказаны свойства локально обратимых булевых функций, позволившие установить критерий локальной обратимости булевой функции; установлены связи между различными модификациями свойства локальной обратимости, а также определенные достаточные условия отсутствия у функции свойства локальной обратимости.

5) Установлена асимптотика логарифма числа булевых функций с левым барьером длины 1 без правого барьера. Получены новые нижние асимптотические оценки логарифма числа совершенно уравновешенных булевых функций без барьера.

Теоретическая и практическая значимость. Полученные в диссертации результаты могут быть использованы для развития и совершенствования математических моделей аппаратно-программных средств защиты информации, что будет способствовать повышению обоснованности методов оценки защищенности информации. Эти результаты могут найти применение также при разработке новых принципов создания аппаратно-программных средств защиты информации. В частности:

1) при синтезе и анализе систем обеспечения информационной безопасности на основе потоковых шифров, использующих фильтрующие генераторы;

2) при изучении свойств и обосновании параметров преобразований, обеспечивающих аутентификацию, идентификацию, целостность и защиту информации, реализуемых на основе регистров сдвига и булевых функций;

3) в учебном процессе студентов-математиков, проходящих обучение в рамках специализации «Математические и программные методы обеспечения информационной безопасности»;

4) в научных центрах, проводящих исследования в области защиты информации.

Апробация работы. Основные результаты диссертации докладывались на следующих научных конференциях и семинарах:

- семинаре «Дискретная математика и математическая кибернетика» кафедры математической кибернетики факультета Вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова;

- семинаре «Булевы функции в криптологии» кафедры дискретной математики Механико-математического факультета Московского государственного университета имени М.В. Ломоносова;

- семинаре отдела дискретной математики Математического института имени В.А. Стеклова РАН;
- IV международной научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008), 2008 год;
- V международной научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009), 2009 год;
- VI международной научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2010), 2010 год;
- VII международной научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2011), 2011 год;
- VIII международной конференции «Дискретные модели в теории управляющих систем», 2009 год;
- XVI международной конференции «Проблемы теоретической кибернетики», 2011 год;
- международной конференции «Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes», Велико-Тырново, Болгария, 2008 год;

Публикации. Основное содержание диссертации опубликовано в 18 работах [1–18], список которых приведён в конце диссертации.

Личный вклад автора. Все представленные в диссертации результаты получены лично автором.

Структура работы. Диссертация состоит из введения, 4 глав, заключения, библиографии и приложения. Объем диссертации 164 страницы, включая 8 рисунков. Библиография включает 45 наименований.

Содержание работы

Во **введении** обосновывается актуальность темы, формулируются цель и задачи исследования, указывается научная новизна,

структура и практическая значимость работы, указаны публикации и апробация работы.

Глава 1 посвящена общим свойствам совершенно уравновешенных булевых функций. В разделе 1.1 вводятся используемые в работе понятия и обозначения, а также основные используемые в работе ранее известные результаты: приводится понятие совершенно уравновешенной булевой функции, приводятся основные утверждения о данном классе функций, в частности, утверждение об эквивалентности понятий функции без запрета и совершенно уравновешенной функции. Определяется отображение $f_r : V_r \to V_{r+n-1}$, описывающее функционирование кодирующего устройства, построенного с помощью регистра сдвига и функции n переменных f в течение r тактов.

Раздел 1.2 посвящен методам исследования свойств совершенно уравновешенных функций с помощью множеств начальных фрагментов прообразов последовательностей относительно отображений f_r. В терминах свойств таких множеств доказывается критерий совершенной уравновешенности (Лемма 1.2.1), следствие из которого (Следствие 1.2.1) оказывается полезным при исследовании булевых функций с барьером и используется в разделе 4.3. Кроме того, доказывается утверждение (Теорема 1.2.1) о существовании для всякого $n \geqslant 2$ булевых функций от n переменных, не являющихся совершенно уравновешенными, но при этом не имеющих запретов длины менее 2^{n-1}. Для всякого $n \geqslant 2$ строится широкий класс таких функций.

В разделе 1.3 рассматриваются вопросы построения алгоритмов распознавания совершенной уравновешенности по вектору значений булевой функции n переменных. Наилучший из ранее известных алгоритмов был предложен М. И. Рожковым[12] и позволяет распознать совершенную уравновешенность булевой функции за $O(N \cdot 2^{N/2})$ операций, где $N = 2^n$ — длина вектора значений. Данный алгоритм основан на результате о совершенной уравновешенности всякой булевой функции f, для которой верно, что отображение $f_{\mu(n)}$ является уравновешенным при $\mu(n) = 2^{n-1}$.

Далее в этом разделе рассматривается утверждение, полученное ранее Й. Голичем с определенным пробелом в доказательстве, аналогичное утверждению Рожкова, но снижающее $\mu(n)$ до величины

[12] *Рожков М. И.* **Некоторые алгоритмические вопросы идентификации конечных автоматов по распределению выходных m-грамм III**. Обозрение прикладной и промышленной математики. 2009. 16(1). 35–60.

n. Следовательно, данное утверждение Голича предположительно позволяет построить более быстрый алгоритм распознавания совершенной уравновешенности. Далее в разделе 1.3 работы приводятся ряд утверждений, следствием из которых становится Теорема 1.3.2, опровергающая утверждение Голича, а также целый класс возможных ослаблений данного утверждения — доказывается, что для всякого сколь угодно большого c найдется такое n и такая функция f, что отображение f_{n+c} является уравновешенным, но при этом функция f совершенно уравновешенной не является.

Для построения существенно более быстрого, чем алгоритм М. И. Рожкова, алгоритма распознавания свойства совершенной уравновешенности далее в разделе 1.3 работы вводится понятие графа сдвигов булевой функции. В терминах графа сдвигов доказывается критерий совершенной уравновешенности булевой функции (Теорема 1.3.4), на основе которого строится алгоритм распознавания свойства совершенной уравновешенности по вектору значений булевой функции за $O(N^2)$ операций. Таким образом, впервые получен полиномиальный алгоритм распознавания свойства совершенной уравновешенности по вектору значений.

Как следует из результатов С. Н. Сумарокова, символы выходной последовательности кодирующего устройства являются независимыми равномерно распределенными (в предположении, что таковы символы входной последовательности) в том и только в том случае, когда функция усложнения данного кодирующего устройства совершенно уравновешена. В разделе 1.4 исследуются свойства преобразований, осуществляемых кодирующими устройствами в случае, когда ни в какой из возможных входных последовательностей не встречаются определенные поднаборы. Доказывается Теорема 1.4.1, представляющая критерий совершенной уравновешенности, описывающий особенности поведения кодирующих устройств на таких множествах входных последовательностией в зависимости от совершенной уравновешенности функций усложнения.

Ранее, за исключением единичных примеров, не было известно каких-либо множеств совершенно уравновешенных функций, нелинейно существенно зависящих от крайних переменных. Данное обстоятельство существенно осложняло как исследование свойств совершенно уравновешенных булевых функций (что продемонстрировано в разделах 2.2 и 4.1 опровержениями полученных ранее утверждений о совершенно уравновешенных функциях), так и синтез совершенно уравновешенных функций для использования в прак-

тических приложениях (зачастую свойство линейности по одной из крайних переменных является нежелательным). С целью развития данного направления исследований в **главе 2** вводится класс функций с барьером.

В разделе 2.1 вводится понятие барьера булевой функции, устанавливаются простейшие свойства функций с барьером: обосновывается достаточность наличия у функции барьера для совершенной уравновешенности, описываются классы сохраняющих свойство барьера преобразований, вводятся простейшие классы совершенно уравновешенных булевых функций с барьером. Доказывается (Теорема 2.1.1) существование булевых функций, которые не имеют барьера, но при этом являются совершенно уравновешенными. Строится метод, позволяющий получать (с ростом числа переменных) булевы функции со сколь угодно большой длиной барьера. Доказывается утверждение (Теорема 2.1.3) о существовании для сколь угодно большого натурального c таких совершенно уравновешенных булевых функций, длина барьера которых превосходит число переменных не менее, чем на c. В заключение раздела приводится описание строения множества функций с барьером длины 1 (линейные по крайней переменной функции) и 2 (не зависящие существенно от одной из крайних переменных и линейные по соседней с ней).

Как следует из результатов раздела 2.1, совершенно уравновешенные функции с барьером, зависящие нелинейно от крайних существенных переменных, следует искать во множестве функций с барьером длины не менее 3. В разделе 2.2 проводится изучение множества существенно зависящих от крайних переменных функций с барьером длины 3. С помощью разработанного аппарата помеченных графов де Брейна формулируется и доказывается критерий наличия у функции правого барьера длины 3 (Теорема 2.2.1). Этот критерий позволяет для определения наличия данного свойства у функции переходить от проверки выполнимости системы булевых уравнений к проверке некоторого конечного набора свойств подфункций. Он оказывается удобным для проверки наличия у булевой функции барьера длины 3 — с помощью него далее в разделе 2.2 обосновывается некорректность результата Кс. Лэя и Дж. Месси о достаточном условии кодирующего устройства быть 2-обратимым[13].

[13] *Lai X., Massey J.* **Some connections between scramblers and invertible automata** Proceedings of 1988 Beijing International Workshop on Information Theory. 1988. Pp. DI 5.1 – DI 5.5.

Далее также с помощью полученного критерия наличия у булевой функции барьера длины 3 строится опровержение доказанного (с пробелом в доказательстве) Маркусом Дихтлом неверного результата о необходимом условии совершенной уравновешенности. Строится булева функция с барьером длины 3, не удовлетворяющая необходимому условию Дихтла.

В разделе 2.3 рассматриваются свойства частично определенной булевой функции, определяющей процедуру частичного восстановления входной последовательности кодирующего устройства с функцией, обладающей правым барьером. С помощью развития аппарата помеченных графов де Брейна формулируется и доказывается утверждение (Теорема 2.3.1) об уравновешенности упомянутой частично определенной булевой функции на своей области определения. В заключение раздела рассматриваются примеры, демонстрирующие существенность свойств кодирующего устройства с функцией с барьером для уравновешенности частично определенной функции описанного вида в случае ее существования.

Глава 3 посвящена исследованию свойств булевых функций без предсказывания. Такие функции гарантируют кодирующему устройству отсутствие принципиальной возможности по начальному отрезку входной последовательности и сколь угодно большому отрезку выходной последовательности получать информацию о последующих выходных символах. Вторая половина данной главы посвящена свойству функций, при наличии которого существует принципиальная возможность при возникновении некоторых наборов в выходной последовательности однозначно восстанавливать входную последовательность. Булевы функции с таким свойством называются локально обратимыми булевыми функциями.

В разделе 3.1 разрабатывается аппарат исследования булевых функций с барьером с помощью множеств начальных состояний. Устанавливается (Теорема 3.1.1) свойство булевых функций с барьером, определяющее структуру множества прообразов произвольного набора достаточно большой длины относительно отображения f_r. Доказывается критерий наличия у булевой функции барьера фиксированной длины (Теорема 3.1.2), позволяющий ввести для произвольной функции с правым (левым) барьером целочисленный параметр e_f^R (соответственно, e_f^L), через который выражаются мощности таких множеств, как образ отображения f_r при фиксированном начале (конце) входной последовательности, множества начал фиксированной длины и окончаний (окончаний фиксирован-

ной длины и начал) входных последовательностей в прообразе любой выходной последовательности. Устанавливаются неравенства на параметры e_f^R и e_f^L, а также критерии равенств в данных неравенствах.

С помощью разработанного аппарата в разделе 3.2 устанавливается критерий принадлежности функции классу функций без предсказывания (Теорема 3.2.2): свойство булевой функции быть функцией без предсказывания оказывается эквивалентно свойству наличия у функции правого барьера, причем величина отрезка выходной последовательности, после которой каждый последующий символ (в естественной вероятностной модели, предполагающей независимость и равномерное на множестве $0, 1$ распределение всех символов входной последовательности, за исключением известных) не может быть предсказан с вероятностью, отличной от $\frac{1}{2}$, даже при наличии полной информации о начале входной последовательности, оказывается находящейся в прямой зависимости от длины правого барьера данной функции, а при сокращении отрезка существуют ситуации, при которых предсказывание символов с отличной от $\frac{1}{2}$ вероятностью всегда возможно.

Полученные результаты оказываются чрезвычайно полезными для исследования поставленной в качестве открытого вопроса[14] задачи о мощности множества так называемых инверсионных функций для произвольной функции с барьером. В завершение раздела 3.2 приводится утверждение (Теорема 3.2.3), представляющее решение данной задачи.

При исследовании кодирующих устройств естественным вопросом является возможность однозначного восстановления части входной последовательности кодирующего устройства по части выходной последовательности. В частности, при использовании таких кодирующих устройств в составе фильтрующих генераторов наличие возможности получения по конечному отрезку выходной последовательности достаточно большой части символов входной последовательности делает возможным нахождение секретного ключа простым решением линейной системы уравнений. Одним из возможных вариантов формализации данного свойства функций усложнения является следующий: существование таких наборов, что в случае их присутствия в выходной последовательности кодирую-

[14] *Lai X., Massey J.* **Some connections between scramblers and invertible automata** Proceedings of 1988 Beijing International Workshop on Information Theory. 1988. Pp. DI 5.1 – DI 5.5.

щего устройства оставшиеся символы входной последовательности можно восстанавливать однозначно по последующим символам выходной последовательности.

Данное понятие было формализовано О. А. Логачевым как понятие локальной обратимости булевой функции[15], посвященной изучению соответствующих свойств функций, линейных по последней переменной. В той же работе был получен критерий локальной обратимости порождаемых такими функциями отображений, связывающий данное понятие с так называемым возвратным свойством булевой функции.

В разделе 3.3 проводится исследование свойства локальной обратимости произвольных булевых функций. Устанавливается ряд необходимых свойств локальной обратимости, в частности, совершенная уравновешенность и наличие барьера. Доказывается критерий (Теорема 3.3.6), связывающий локальную обратимость произвольной булевой функции с характеристиками булевых функций с барьером, описанными в разделе 3.2. Следствиями из полученных результатов являются методы построения булевых функций с положительными криптографическими свойствами, не допускающих локального обращения: в частности, для недопущения наличия у булевой функции свойства локальной обратимости достаточно выбирать ее из класса булевых функций без барьера.

В **главе 4** исследуются методы построения определенных классов совершенно уравновешенных булевых функций. Описывается операция композиции функций, соответствующая композиции соответствующих кодирующих устройств и приводится полученное О. А. Логачевым утверждение о совершенной уравновешенности функций, полученных такой композицией. В разделе 4.1 доказывается ряд утверждений о свойствах операции композиции кодирующих устройств, позволяющих доказать утверждение (Теорема 4.1.1), которое содержит конструктивное описание широкого класса совершенно уравновешенных булевых функций, нелинейным существенным образом зависящих от обеих крайних переменных. Мощность данного класса представляет собой новую, существенно превосходящую все ранее полученные, нижнюю оценку числа таких функций: $2^{2^{n-3}+1} - 5 \cdot 2^{2^{n-4}}$. С использованием данного класса строится

[15] *Логачев О. А.* **О локальной обратимости одного класса булевых отображений**. Материалы IX Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова. 2007. 440–442.

(Теорема 4.1.2) последовательность классов совершенно уравновешенных булевых функций (при всяком $n \geqslant 7$ имеющих мощность не менее $2^{2^{n-6}} - 2^{2^{n-7}}$), не удовлетворяющих необходимому условию совершенной уравновешенности, предложенному Дихтлом.

Раздел 4.2 посвящен получению верхних и нижних оценок числа функций с правым барьером длины 3. Известной нижней оценкой логарифма числа таких функций n переменных, полученной Лэем и Месси, является $0.75 \cdot 2^{n-2}$. С использованием критерия барьера длины 3 и представления функций с барьером длины 3 с помощью троек помеченных графов де Брейна, а также результатов Н. Лихиардопола[16], оценки размеров максимальных по мощности независимых множеств в определенных модификациях графов де Брейна в разделе 4.2 получена (Теорема 4.2.3) новая нижняя асимптотическая оценка логарифма класса функций с правым барьером длины 3:

$$\left(1 + (\log_2 5)/4 - \mathrm{O}(1/\sqrt{n})\right) \cdot 2^{n-2} \gtrsim 1{,}58048 \cdot 2^{n-2}.$$

Кроме того, используя определенную модификацию метода доказательства данной оценки, удается (Теорема 4.2.4) получить также новую нижнюю асимптотическую оценку логарифма числа нелинейно зависящих от крайних переменных совершенно уравновешенных булевых функций.

Далее в разделе 4.2 с помощью развития аппарата представления булевых функций с правым барьером длины 3 тройками помеченных графов де Брейна и дальнейшего анализа критерия барьера длины 3 устанавливается (Теорема 4.2.5) верхняя оценка логарифма числа таких функций: $2{,}100641 \cdot 2^{n-2}$.

Как следует из полученных результатов о локально обратимых булевых функциях, для обеспечения отсутствия у функции усложнения негативного свойства локальной обратимости при наличии свойства совершенной уравновешенности, достаточно выбирать данную функцию из класса совершенно уравновешенных булевых функций без барьера. Методам построения широких классов таких функций, а также получению оценок мощностей этих классов посвящен раздел 4.3. Разработан метод построения классов совершенно уравновешенных булевых функций без барьера по классам функций с односторонним барьером, что позволяет далее для достижения поставленных целей рассматривать булевы функции с наличием пра-

[16] *Lichiardopol N.* **Independence number of de Bruijn graphs**. Discrete Mathematics. 2006. Vol. 306(12). Pp. 1145 – 1160.

вого барьера и отсутствием левого.

В терминах полиномиального представления приводится (Теорема 4.3.2) конструктивное описание широкого класса совершенно уравновешенных булевых функций без правого барьера, устанавливается асимптотика логарифма его мощности: $\frac{1}{3}\cdot 2^{n-1}$. Разрабатывается аппарат представления булевых функций с помощью пометок ациклических подграфов графа сдвигов булевой функции, в терминах данного представления описываются необходимые и достаточные условия отсутствия у функции правого барьера. Полученные утверждения используются для исследования класса функций с односторонним барьером — функций с правым барьером длины 1 без левого барьера. С использованием данных результатов оказывается возможным (Теорема 4.3.3 и Следствие 4.3.2) установить асимптотику логарифма данного класса. В заключительной части раздела 4.3 устанавливается (Теорема 4.3.4 и Следствие 4.3.4) новая нижняя оценка числа совершенно уравновешенных булевых функций без барьера, представляющая также и нижнюю оценку числа совершенно уравновешенных булевых функций, не являющихся локально обратимыми.

В **заключении** перечислены основные результаты диссертации.

В **приложении** содержится полное описание совершенно уравновешенных булевых функций от 4 и 5 переменных, полученное с помощью описанного в разделе 1.3 алгоритма распознавания свойства совершенной уравновешенности.

Благодарности. Автор диссертации выражает благодарность своему научному руководителю кандидату физико-математических наук, старшему научному сотруднику Логачеву Олегу Алексеевичу за постановку задач, постоянное внимание к работе и поддержку. Также автор выражает благодарность доктору физико-математических наук, профессору Алексееву Валерию Борисовичу, доктору физико-математических наук, профессору Вороненко Андрею Анатольевичу, кандидату физико-математических наук, доценту Селезневой Светлане Николаевне, кандидату физико-математических наук, доценту Применко Эдуарду Андреевичу, кандидату физико-математических наук, доценту Карпунину Григорию Анатольевичу, кандидату физико-математических наук Ященко Валерию Владимировичу, Варновскому Николаю Павловичу, а также всем сотрудникам кафедры математической кибернетики факультета ВМК МГУ имени М.В. Ломоносова за доброжелательное отношение и творческую атмосферу.

Публикации автора по теме диссертации

Публикации в изданиях из Перечня ВАК

1. О.А. Логачев, С.В. Смышляев, В.В. Ященко. Новые методы изучения совершенно уравновешенных булевых функций. Дискретная математика. Том 21, выпуск 2, 2009, с. 51–74. (С.В. Смышляеву принадлежат следующие результаты: алгоритм распознавания свойства совершенной уравновешенности, описание свойств функций с барьером, доказательство существования функций без барьера, критерий наличия у булевой функции барьера длины 3, описание совершенно уравновешенных булевых функций от $n \leqslant 5$ переменных.)

2. С.В. Смышляев. Барьеры совершенно уравновешенных булевых функций. Дискретная математика. Том 22, выпуск 2, 2010, с. 66–79.

3. С.В. Смышляев. Булевы функции без предсказывания. Дискретная математика. Том 23, выпуск 1, 2011, с.102–118.

4. О.А. Логачев, С.В. Смышляев, В.В. Ященко. Ро-уравновешенные булевы функции. Дискретная математика. Том 24, выпуск 2, 2012, с. 154–159. (С.В. Смышляеву принадлежат следующие результаты: нижние оценки параметра $\mu(n)$, определяющего нижнюю границу M, при которой свойство ρ_M-уравновешенности функции n переменных эквивалентно ее совершенной уравновешенности.)

5. С.В. Смышляев. О числе совершенно уравновешенных булевых функций с барьером длины 3. Прикладная дискретная математика. Выпуск 1(11), 2011, с.26–33.

6. С.В. Смышляев. Локально обратимые булевы функции. Прикладная дискретная математика. Выпуск 4, 2011, с. 11–22.

7. S.V. Smyshlyaev. Perfectly Balanced Boolean Functions and Golic Conjecture. Journal of Cryptology, 25(3): 464–483, 2012.

Публикации в изданиях не из Перечня ВАК

8. С.В. Смышляев. О криптографических слабостях некоторых классов преобразований двоичных последовательностей. Прикладная дискретная математика. Выпуск 1(7), 2010, с. 5–15.

9. С.В. Смышляев. Построение классов совершенно уравновешенных булевых функций без барьера. Прикладная дискретная математика. Выпуск 3(9), 2010, с. 41–50.

10. С.В. Смышляев. О некоторых свойствах совершенно уравновешенных булевых функций. Материалы Четвертой Международной Научной Конференции по Проблемам Безопасности и Противодействия Терроризму. МГУ имени М.В.Ломоносова, Москва, 30-31 октября 2008 года. МЦНМО, М., 2009, с. 57–64.

11. С.В. Смышляев. О преобразовании двоичных последовательностей с помощью совершенно уравновешенных булевых функций. Материалы Пятой Международной Научной Конференции по Проблемам Безопасности и Противодействия Терроризму. МГУ имени М.В.Ломоносова, Москва, 29-30 октября 2009 года. МЦНМО, М., 2010, с. 31–41.

12. С.В. Смышляев. О свойствах булевых функций без предсказывания. Материалы Шестой Международной Научной Конференции по Проблемам Безопасности и Противодействия Терроризму. МГУ имени М.В.Ломоносова, Москва, 11-12 ноября 2010 года. МЦНМО, М., 2011, с. 47–56.

13. С.В. Смышляев. О совершенно уравновешенных булевых функциях без барьера. Материалы Восьмой Международной конференции «Дискретные модели в теории управляющих систем», МГУ имени М.В.Ломоносова, Москва, 6-9 апреля 2009 года. МАКС Пресс, М., с. 278–284.

14. О.А. Логачев, С.В. Смышляев, В.В. Ященко. Ро-уравновешенные булевы функции и их свойства. Материалы Шестнадцатой Международной Конференции «Проблемы Теоретической Кибернетики», с. 272–276. (С.В. Смышляеву принадлежат следующие результаты: опровержение утверждения Голича о достаточном условии совершенной уравновешенности.)

15. С.В. Смышляев. Совершенная уравновешенность дискретных функций и условие Голича. Прикладная дискретная математика. Приложение 5, 2012, с. 28–30.

16. С.В. Смышляев. О некоторых классах булевых функций дефекта нуль. Сборник тезисов XV Международной научной

конференции студентов, аспирантов и молодых ученых «Ломоносов —- 2008». Секция «Вычислительная математика и кибернетика». 8—11 апреля, Москва, МГУ имени М.В.Ломоносова. М.: МАКС Пресс, 2008. С. 44–45.

17. С.В. Смышляев. Построение классов совершенно уравновешенных булевых функций без барьера. Сборник тезисов лучших дипломных работ факультета ВМиК МГУ за 2011 год, с. 89–90.

18. O.A. Logachev, A.A. Salnikov, S.V. Smyshlyaev, V.V. Yashchenko. Symbolic Dynamics, Codes and Perfectly Balanced Functions. Proceedings of the NATO Advanced Research Workshop on Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, Veliko Tarnovo, Bulgaria, 6-9 October 2008. IOS Press, 2009, 222–233. (С.В. Смышляеву принадлежат следующие результаты: описание класса совершенно уравновешенных булевых функций без правого барьера, теорема о сохранении барьеров при операции суперпозиции специального вида, доказательство несуществования не являющихся линейными ни по одной переменной булевых функций, сохраняющих совершенную уравновешенность при введении произвольного набора фиктивных переменных.)