Московский государственный университет
имени М. В. Ломоносова

На правах рукописи

Буряков Михаил Леонидович

Алгебраические, комбинаторные и криптографические свойства параметров аффинных ограничений булевых функций

Специальность 05.13.19 — методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2009

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: доктор физико-математических наук, ведущий научный сотрудник Фомичев Владимир Михайлович (Институт проблем информатики РАН)

кандидат физико-математических наук, старший научный сотрудник Кузнецов Юрий Владимирович (НИИ системных исследований РАН).

Ведущая организация: ФГУП «НИИ Автоматики».

Защита диссертации состоится 25 февраля 2009 г. в 16:45 на заседании диссертационного совета Д 501.002.16 при Московском государственном университете имени М. В. Ломоносова по адресу: Российская Федерация, 119991, Москва, ГСП-1, Ленинские горы, д. 1, Московский государственный университет имени М. В. Ломоносова, механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан «23» января 2009 г.

Ученый секретарь
диссертационного совета
доктор физико-математических наук Корнев А. А.

Общая характеристика работы

Актуальность темы. Обеспечение информационной безопасности является одной из важнейших государственных задач наряду с обеспечением обороноспособности страны, развитием экономики, образования и здравоохранения. Основополагающим документом, который регламентирует политику России в области информационной безопасности, является Доктрина информационной безопасности Российской Федерации[1], утвержденная в сентябре 2000 года Президентом РФ. Секция Научного совета при Совете Безопасности РФ на основе Доктрины разработала Перечень приоритетных проблем научных исследований, связанных с информационной безопасностью[2]. Он включает в себя направления в областях развития общей теории обеспечения информационной безопасности и, в частности, защиты информации различными методами, в том числе с использованием криптографических механизмов, разработку методов и средств защиты в системах электронного документооборота, включая использование электронной цифровой подписи. Одним из наиболее важных направлений в Перечне является «разработка фундаментальных проблем теоретической криптографии и смежных с ней областей математики» (п. 54 Перечня).

Качество криптографических методов защиты определяется криптографической стойкостью системы защиты. Основной количественной мерой стойкости является вычислительная сложность решения задачи преодоления криптографической защиты. Количественная оценка уровня защиты информации с использованием криптосистемы определяется как вычислительная сложность наиболее эффективного из известных алгоритмов ее вскрытия.

Разработка алгоритмов преодоления криптографической защиты основана на использовании математических моделей, адекватно описывающих процесс функционирования системы защиты. Математическая формализация работы криптосистем в процессе криптоанализа во многих случаях приводит к необходимости решения уравнений в различных алгебраических системах. Системы нелинейных булевых уравнений являются одной из распространенных моделей описания процессов функци-

[1] *Доктрина информационной безопасности Российской Федерации.* В сб. «Научные и методологические проблемы информационной безопасности». Под ред. В. П. Шерстюка, сс. 149–197 — М.: МЦНМО, 2004.

[2] *Приоритетные проблемы научных исследований в области информационной безопасности Российской Федерации.* Математика и безопасность информационных технологий. Материалы конференции в МГУ 23–24 октября 2003 г., сс. 21–28 — М.: МЦНМО, 2004.

онирования различных дискретных устройств. Необходимость изучения и решения систем булевых уравнений возникает в ряде задач теории конечных автоматов, теории кодирования и криптологии. В частности, в криптологии это направление относится к синтезу и анализу традиционных криптографических систем с секретным ключом. В ходе такого исследования системы нелинейных булевых уравнений связывают элементы неизвестного ключа криптосистемы с известными данными. Основные криптографические примитивы, являющиеся источниками систем булевых уравнений в криптоанализе, — это комбинирующие генераторы (рис. 1) и фильтрующие генераторы (рис. 2) потоковых шифров (РСЛОС-i, $i = 1, \ldots, n$, РСЛОС — регистры сдвига с линейными обратными связями; f — комбинирующая (фильтрующая) булева функция от n переменных; $g_i(\mathbf{v})$, $i = 1, 2, \ldots, n$, $g(\mathbf{v})$ — полиномы обратных связей регистров сдвига), а также s-боксы блоковых шифров и раундовые преобразования, используемые в хэш-функциях[3].

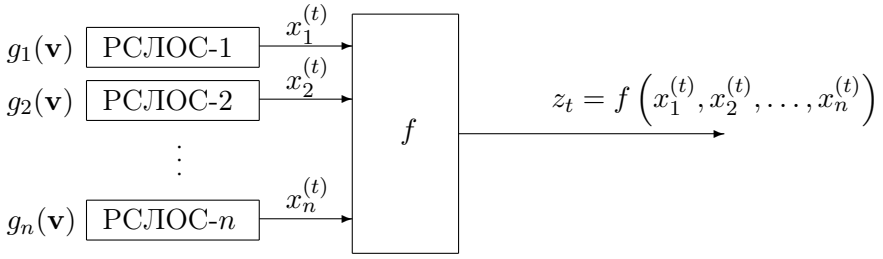

Рис. 1: комбинирующий генератор

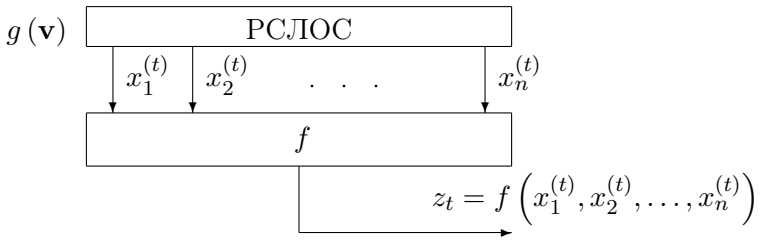

Рис. 2: фильтрующий генератор

Задача решения произвольной системы нелинейных булевых уравнений является NP-трудной. На настоящее время для решения подобных систем в общем случае не существует алгоритма со сложностью, по порядку меньше, чем $2^{O(n)}$, где n — число неизвестных в системе. Вместе

[3]Menezes A., P. van Oorschot, Vanstone S. *Handbook of applied cryptography.* CRC Press Inc., 1997

с тем, анализ конкретных систем уравнений для криптосистем с секретным ключом (при $n \approx 100$–200 и более) является актуальной научной проблемой.

В криптоанализе разработаны различные подходы к решению нелинейных систем булевых уравнений. В ряде случаев для нахождения решения системы используются теоретико-вероятностные, статистические, и теоретико-кодовые методы[4,5,6,7]. При другом подходе предлагается погружать систему уравнений в действительную область и находить ее решение с помощью соответствующей системы псевдобулевых неравенств[8,9]. Кроме того, в случае использования итераций в процессе шифрования возможна линеаризация исходной криптографической задачи (например, нахождения ключа) с использованием определенных степеней итерируемого отображения, которые представляют собой аффинные отображения[10]. Рассматриваются алгебраические методы решения систем нелинейных булевых уравнений над конечными полями на основе базисов Гребнера[11].

Наиболее эффективными, как показывает практика криптоанализа, являются методы, использующие линеаризацию исходной системы. Эти методы можно условно разбить на два класса.

Первый класс составляют методы линеаризации нелинейной системы булевых уравнений с введением новых переменных, последующим эффективным решением полученной линейной системы и затем нахождением решения исходной системы. В практике криптоанализа этот метод называют алгебраической атакой.

---

[4]Siegenthaler T. *Correlation-immunity of nonlinear combining functions for cryptographic applications.* IEEE Trans. on Information Theory V. IT-30.5, pp. 776–780, 1984.

[5]Meier W., Staffelbach O. *Fast correlation attacks on certain stream ciphers.* Journal of Cryptology V. 1, № 3, pp. 159–1762, 1989.

[6]Chepyzhov V., Smeets B. *On a fast correlation attacks on certain stream ciphers.* Advances in Cryptology: EUROCRYPT'91, LNCS V. 547, pp. 176–185, Springer-Verlag, 1991.

[7]Chepyzhov V., Johansson T., Smeets B. *A simple algorithm for fast correlation attacks on stream ciphers.* Advances in Cryptology: FSE'2000, LNCS V. 1978, pp. 181–195, Springer-Verlag, 2000.

[8]Г. В. Балакин, В. Г. Никонов. *Методы сведения булевых уравнений к системам пороговых соотношений.* Обозрение прикладной и промышленной математики., т. 1, вып. 3, сс. 389–401, 1994.

[9]К. К. Рыбников, А. С. Хохлушин. *О взаимосвязях различных алгоритмических методов погружения множества решений системы булевых уравнений в действительную область.* Вестник МГУЛ. Лесной вестник, № 5 (25), сс. 189–194, 2002.

[10]В. М. Фомичев. *Дифференциация элементов в конечных группах и в автоматах по заданным признакам, определяющим криптографические свойства систем защиты информации.* Диссертация на соискание ученой степени доктора физико-математических наук, специальность 05.13.19, Москва, 2006.

[11]Ars G., Faugère J.-C., Imai H., Kawazoe M., Sugita M. *Comparsion between XL and Gröbner basis Algorithms.* Advances in Cryptology: ASIACRYPT'04, LNCS V. 3329., pp. 338–353, Springer-Verlag, 2004.

Второй класс объединяет методы линеаризации нелинейных систем булевых уравнений без введения новых переменных. В этом случае речь идет об ограничениях булевых функций (иногда этот прием называют сужением), обладающих свойствами аффинных функций.

В 2003 году была рассмотрена[12] атака по открытому и шифрованному тексту на комбинирующий генератор (см. рис. 1) потокового шифра с угрозой вскрытия ключа и предложен метод реализации этой атаки. Этот метод основан на частичном опробировании ключей и использующий ранговый критерий отбраковки ложной части опробуемого ключа. При этом последовательно перебираются возможные начальные заполнения (ключи) определенной, специальным образом подобранной части регистров сдвига с линейными обратными связями РСЛОС-i_r, $r = 1, \ldots, s$. (см. рис. 1). Среди выходных последовательностей этих регистров находятся такты, задающие подходящие значения переменных $x_{i_1}, \ldots, x_{i_s}$ булевой функции f и определяющие ее аффинные ограничения. Подходящие фиксации (значения переменных) совместно с известными элементами выходной последовательности в этих тактах определяют линейные системы уравнений, которые используются для нахождения начальных состояний опробуемых регистров.

Подфункцией данной булевой функции называют ограничение этой функции на некоторое подмножество ее области определения. Тесно связано с понятием подфункции булевой функции понятие частично определенной булевой функции. Использование подфункций в криптоанализе определило интерес исследователей к изучению совместных криптографических свойств булевых функций и их подфункций, а также к наследованию свойств булевой функции ее подфункциями.

Уровень аффинности ($\mathrm{la}(f)$) булевой функции f определяется как минимальное число фиксаций переменных этой функции, переводящих исходную функцию в аффинную функцию от меньшего числа переменных. Понятие частичного уровня аффинности ($\mathrm{la}^0(f)$) определяет минимальное число нулевых фиксаций переменных булевой функции f, превращающих исходную функцию в аффинную. Обобщенный уровень аффинности ($\mathfrak{La}(f)$) булевой функции f определяется как минимальная разность между числом переменных функции f и размерностью плоскости (смежного класса по подпространству), ограничение на которую

[12] О. А. Логачев, А. А. Сальников, В. В Ященко. *Корреляционная иммунность и реальная секретность,* Математика и безопасность информационных технологий. Материалы конференции в МГУ 23–24 октября 2003 г., сс. 165–170 — М.: МЦНМО, 2004.

совпадает с аффинной функцией. Различные виды уровня аффинности связаны между собой соотношением

$$\mathfrak{La}(f) \leqslant \mathrm{la}(f) \leqslant \mathrm{la}^0(f).$$

Естественным образом указанные выше параметры линеаризации могут быть распространены и на булевы отображения.

Уровень аффинности $\mathrm{la}(f)$ комбинирующей функции f (рис. 1) определяет (наряду с другими параметрами) трудоемкость описанного выше метода нахождения ключей.

Другим важным направлением исследований является изучение криптографических свойств булевых функций и связей между этими свойствами. Достаточное число математически содержательных соотношений между параметрами, описывающими различные (в том числе и конфликтующие) криптографические свойства, облегчает решение сложной оптимизационной задачи выбора булевых функций (отображений) при синтезе стойких криптосистем. Примерами могут служит изучение пар криптографических свойств «корреляционная иммунность–нелинейность»[13,14], «корреляционная иммунность–алгебраическая иммунность»[15], «нелинейность–алгебраическая иммунность»[16,17], а также использование локальных аффинностей для изучения криптографических свойст булевых функций[18,19,20,21].

Цель диссертации. Целью данной диссертации является разработка новых математических подходов к анализу и синтезу криптосистем с

[13]Ю. В. Таранников. *О корреляционно-иммунных и устойчивых булевых функциях.* Математические вопросы кибернетики. Вып. 11, сс. 91–148 — М.: Физматлит, 2002.

[14]Sarkar P., Maitra S. *Nonlinearity bounds and constructions of resilient Boolean functions,* CRYPTO'2000, LNCS V. 1880, pp. 515–532, Springer-Verlag, 2000.

[15]А. А. Ботев. *О свойствах корреляционно-иммунных функций с высокой нелинейностью.* Диссертация на соискание ученой степени кандидата физико-математических наук, Москва, 2005.

[16]Dalai D. K., Gupta K. C., Maitra S. *Results on algebraic immunity for cryptographically significant Boolean functions.* Progress in Cryptology: INDOCRYPT'04, LNCS V. 1880, pp. 92–106, Springer-Verlag, 2004.

[17]Lobanov M. *Tight bounds between nonlinearity and algebraic immunity,* Cryptology ePrint Archive, Report 2005/441, 2005.

[18]Clark W. E., Hou X. D., Mihailovs A. *The affinity of permutations of a finite vector space.* Finite Fields and Their Applications V. 13, Issue 1, pp. 80–112, 2007.

[19]Hou X. D. *Affinity of permutations of* P_2^n. Discrete Applied Mathematics archive, v. 154, Issue 2, pp. 313–325, 2006.

[20]Canteaut A., Daum M., Dobbertin H., Leander G. *Finding nonnormal bent functions.* Discrete Applied Mathematics archive, v. 154 , Issue 2, pp 202–218, 2006.

[21]Logachev O., Yashenko V., Denisenko M. *Local affinity of Boolean mappings.* Proceedings of NATO ASI "Boolean functions in cryptology and information sequrity", Moscow, 8–18 september, 2007.

секретным ключом, а также изучение различных, в том числе криптографических, свойств аффинных ограничений булевых функций.

Научная новизна. Все результаты диссертации являются новыми. Основные результаты диссертации следующие:

- найдены параметры линеаризации и их оценки для различных, в том числе криптографических, классов булевых функций;
- доказаны свойства параметров, характеризующие методы линеаризации булевых функций в целом;
- получены соотношения, связывающие параметры линеаризации с основными криптографическими свойствами булевых функций;
- доказаны верхние и нижние асимптотические оценки уровня аффинности для почти всех булевых функций, а также асимптотическое неравенство для уровня аффинности квадратичных булевых функций;
- доказана *NP*-трудность задачи определения уровня аффинности булевых функций с ограничением на количество мономов.

Научная и практическая ценность. Работа носит теоретический характер. Установлены различные свойства аффинных ограничений (уровня аффинности) булевых функций. Доказаны соотношения между криптографическими параметрами булевых функций и параметрами их аффинных ограничений. Доказаны асимптотические оценки уровня аффинности.

Полученные результаты могут найти применение: для решения некоторых классов систем булевых уравнений; для синтеза и анализа криптографических примитивов (булевых функций и отображений), обладающих свойствами, необходимыми для обеспечения криптографической стойкости; при изучении общих свойств булевых функции и отображений; в учебном процессе.

Методы исследования. В диссертации используются методы теории булевых функций, линейной алгебры, комбинаторного анализа, элементы теории сложности и теории вероятности.

Апробирование. Результаты диссертации неоднократно докладывались на семинаре по криптографии Института проблем информационной безопасности МГУ, на семинаре «Булевы функции в криптологии» механико-математического факультета МГУ, на семинаре «Дискретная математика и математическая кибернетика» кафедры математической кибернетики факультета ВМК МГУ, на международном семинаре «Дискретная математика и ее приложения», на международных конференциях МАБИТ'05 (2005 г.) и «Boolean Functions in Cryptology and Information Security» (2007 г.).

Публикации по теме диссертации. По теме диссертации опубликовано 8 работ [1–8], 3 из которых — в печатных изданиях из перечня ВАК [1–3].

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, трех приложений и списка литературы, включающего 70 наименований. Объем работы 114 страниц.

Краткое содержание диссертации

Глава 1 посвящена исследованию уровня аффинности некоторых классов булевых функций.

В разделе 1.1 вводятся необходимые понятия и параметры булевых функций, даются определения исследуемых в диссертации параметров линеаризации, а также формулируются основные криптографические свойства булевых функций такие как нелинейность, корреляционная иммунность и устойчивость, алгебраическая иммунность, лавинные характеристики, линейные структуры.

В разделе 1.2 рассматриваются основные классы булевых функций и конструкции для построения булевых функций с заданными криптографическими характеристиками. Для конструкций суперпозиции булевых функций вида прямой суммы, конкатенации, конструкции вида $g(\mathbf{x}, \mathbf{y}) = f(\mathbf{x} \oplus \mathbf{y})$ и ряда других доказываются соотношения, определяющие их уровень аффиннности. Для бент-функций, построенных с помощью конструкции Майорана–Мак-Фарланда, доказывается следующее утверждение:

Теорема 1.5. *Пусть* $n = 2m$, $\Phi = (f_1, \ldots, f_m)$ — *взаимнооднозначное*

отображение V_m на себя, $h \in \mathcal{F}_m$. Тогда для бент-функции

$$f(\mathbf{z}) = f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \Phi(\mathbf{y}) \rangle \oplus h(\mathbf{y}) = \bigoplus_{i=1}^{m} x_i f_i(\mathbf{y}) \oplus h(\mathbf{y}),$$

$\mathbf{z} \in V_n$, $\mathbf{x} \in V_m$, $\mathbf{y} \in V_m$ справедливо соотношение $\mathrm{la}(f) = m$.

Кроме того, для устойчивых булевых функций, построенных с помощью конструкции Майорана–Мак-Фарланда, устанавливается соотношение (Теорема 1.6), связывающее уровень аффинности и размерность образа соответствующего пространства для отображения $\Phi\colon V_{n-t} \to V_t$:

$$\mathrm{la}(f) \leqslant n - t.$$

Далее рассматривается рекуррентный способ построения булевых функций, предложенный Таранниковым Ю. В., который позволяет получать устойчивые булевы функции с максимально возможным значением нелинейности. Для этого класса функций доказано неравенство (Теорема 1.8)

$$\mathrm{la}(f) \leqslant \left[\frac{m+3}{2}\right],$$

где m — порядок устойчивости функции f.

Для более общего метода построения корреляционно-иммунных функций, также предложенного Таранниковым, доказывается утверждение, говорящее о том, что уровень аффинности функций, построенных с помощью этого метода, не превосходит величины $2(k-2)$, где k — номер итерации метода, которому соответствует данная функция (Теорема 1.9).

В разделе 1.3 доказывается следующее утверждение:

Теорема 1.11. *Для булевой функции f из $\mathcal{F}_n$ соотношение* $\mathrm{la}(f) = n-1$ *выполнено тогда и только тогда, когда*

$$f(x_1, \ldots, x_n) = \bigoplus_{i<j} x_i x_j \oplus \ell_{\mathbf{a},\varepsilon},$$

где $\ell_{\mathbf{a},\varepsilon}$ — произвольная аффинная функция.

Эта теорема дает полное описание класса функций с максимально возможным уровнем аффинности.

В разделе 1.4 изучается уровень аффинности булевой функции при известных коэффициентах алгебраической нормальной формы этой функции, то есть при известном преобразовании Мебиуса этой функции, которое также является булевой функцией. Рассматриваются весовые характеристики преобразования Мебиуса, существование несущественной переменной у этой функции, линейность и квазилинейность по переменным

(Предложения 1.7–1.10). Для подобных функций доказываются оценки уровня аффинности.

В разделе 1.5 рассматривается связь между спектральными характеристиками булевой функции (коэффициентами Уолша–Адамара) и уровнем аффинности. Доказывается утверждение

Теорема 1.12. *Пусть $f \in \mathcal{F}_n$. Тогда для коэффициентов Уолша–Адамара функции f выполняется неравенство*

$$\max_{\mathbf{u} \in V_n} |\mathrm{W}_f(\mathbf{u})| \geqslant 2^{n-\mathrm{la}(f)}.$$

Глава 2 посвящена получению соотношений, связывающих уровень аффинности с основными криптографическими свойствами (параметрами) булевых функций.

В разделе 2.1 получены следующие оценки, связывающие уровень аффинности и нелинейность булевых функций:

- $\mathrm{N}_f \leqslant 2^{n-1} - 2^{n-\mathrm{la}(f)-1}$ (Предложение 2.1);
- $\mathrm{la}(f) \geqslant k$ для бент-функции $f \in \mathcal{B}_{2k}$ (Предложение 2.2);
- $\mathrm{la}(f) \geqslant r$ для платовидной порядка $2r$ функции $f \in \mathcal{F}_n$ (Предложение 2.3).

В разделе 2.2 получены результаты, показывающие связь между порядком корреляционной иммунности булевой функции и ее уровнем аффинности.

Для неуравновешенных корреляционно-иммунных булевых функций, не являющихся константами, доказано (Теорема 2.1) неравенство

$$\mathrm{la}(f) > \mathrm{cor}(f).$$

Показано также, что для m-устойчивых булевых функций, которые по определению являются уравновешенными, явной связи между уровнем аффинности и порядком корреляционной иммунности нет. Приведены примеры устойчивых булевых функций, для которых порядок корреляционной иммунности находится в различном отношении к уровню аффинности.

Кроме того, в этом разделе рассмотрен класс булевых функций, которые одновременно имеют высокий уровень корреляционной иммунности и высокую нелинейность, и доказано следующее утверждение:

Теорема 2.3. *Пусть* $f \in \mathcal{F}_n$, $\mathrm{sut}(f) = m \leqslant n-2$, $\mathrm{N}_f = 2^{n-1} - 2^{m+1}$. *Тогда*

$$\mathrm{la}(f) \geqslant n - m - 2.$$

В разделе 2.3 получено соотношение, связывающее уровень аффинности и алгебраическую иммунность булевых функций.

Доказано утверждение (Теорема 2.4), выводящее неравенство между алгебраической иммунностью булевой функции и ее алгебраической иммунностью на какой-либо плоскости пространства V_n :

Теорема 2.4. *Пусть* $f \in \mathcal{F}_n$, $L \subseteq V_n$ — *линейное подпространство* V_n, $\mathbf{a} \in V_n$. *Тогда*

$$\mathrm{AI}(f) \leqslant \mathrm{AI}|_{L \oplus \mathbf{a}}(f) + n - \dim L.$$

Как следствие из этой теоремы, доказано неравенство (Следствие 2.2):

$$\mathrm{AI}(f) \leqslant \min_{\substack{0 \leqslant k \leqslant \lceil n/2 \rceil, \\ 0 \leqslant i_1 < \cdots < i_k \leqslant n, \\ \mathbf{c} \in V_k}} \left\{ \deg\left(f_{i_1,\ldots,i_k}^{c_1,\ldots,c_k}\right) + k \right\},$$

откуда получено (Следствие 2.3), что для любой булевой функции $f \in \mathcal{F}_n$

$$\mathrm{la}(f) \geqslant \mathrm{AI}(f) - 1.$$

Соотношения, связывающие с уровнем аффинности такие параметры булевых функций как алгебраическая степень, глобальные аффинные характеристики, пространства линейных структур, линеаризационные множества, рассмотрены в разделе 2.4.

В Предложении 2.4 показывается, что для любого $n \geqslant 3$, $2 \leqslant d \leqslant n$, $1 \leqslant k \leqslant n-2$ существует функция $f_{n,d,k} \in \mathcal{F}_n$ такая, что $\deg(f) = d$, $\mathrm{la}(f) = k$.

Для симметрических булевых функций доказывается утверждение:

Теорема 2.5. *Пусть* $f \in \mathcal{F}_n$ — *симметрическая булева функция,* $\deg(f) = d$, $d > 1$. *Тогда*

$$\mathrm{la}(f) > n - d.$$

При рассмотрении лавинных характеристик булевых функций, доказано, что для любой функции $f \in \mathcal{F}_n$, удовлетворяющей $\mathrm{SAC}(t)$, $\mathrm{la}(f) \geqslant t$ (Предложение 2.5).

Доказано соотношение, связывающее уровень аффинности булевой функции и размерностью пространства линейных структур этой функции (Предложение 2.6):

$$\mathrm{la}(f) \leqslant n - \dim L_f - 1.$$

Также в этом разделе рассмотрен вопрос о связи уровня аффинности с понятием линеаризационных множеств и с понятием индекса линейности отображения. Доказано, что если функция f является сильно k-аффинной, то она представима в виде линейного разветвления, то есть $k > \operatorname{ill}(f)$.

Глава 3 посвящена асимптотическим оценкам уровня аффинности для почти всех булевых функций.

В разделе 3.1 получена нижняя асимптотическая оценка обобщенного уровня аффинности для почти всех булевых функций:

Теорема 3.1. *Пусть $\alpha \in \mathbb{R}$, $\alpha > 1$ — произвольная фиксированная константа. Тогда асимптотически при $n \to \infty$ для почти всех функции из $\mathcal{F}_n$*

$$\mathfrak{La}(f) \geqslant n - \alpha \log_2 n.$$

В разделе 3.2 получена верхняя асимптотическая оценка частичного уровня аффинности для почти всех булевых функций из одного широкого класса:

Теорема 3.3. *Пусть $\varphi(n)$ — произвольная монотонная неограниченная функция, $\varphi(n) > 0$ для любого n; $\beta \in \mathbb{R}$, $\beta > 1$ — некоторая фиксированная константа. Тогда асимптотически при $n \to \infty$ для почти всех функций из $\mathcal{F}_n^{\varphi^\beta(n)}$*

$$\mathrm{la}^0(f) \leqslant n - \log_2 \varphi(n),$$

здесь $\mathcal{F}_n^{\varphi^\beta(n)} = \left\{ f \in \mathcal{F}_n \setminus \mathcal{A}_n \colon \operatorname{len}^*(f) < \dfrac{2^n}{\varphi^\beta(n)} \right\}$, $\operatorname{len}^*(f)$ — количество нелинейных мономов в АНФ функции f.

Как следствие из этой теоремы выведена асимптотическая оценка частичного уровня аффинности для функций с ограничением на степень: асимптотически при $n \to \infty$ для почти всех функций $f \in \mathcal{F}_n$ таких, что $\deg(f) \leqslant d$ (d фиксировано),

$$\mathrm{la}^0(f) \leqslant \frac{\beta - 1}{\beta} n + \frac{1}{\beta} \log_2 D_d^n,$$

где $\beta \in \mathbb{R}$, $\beta > 1$ — произвольная фиксированная константа, $D_d^n = \sum_{i=0}^{d} \binom{n}{i}$.

В разделе 3.3 рассмотрен вопрос об асимптотическом поведении уровня аффинности квадратичных булевых функций, доказано утверждение:

Теорема 3.4. *Вероятность того, что для произвольной булевой функции* $f \in \mathcal{F}_n$, $\deg(f) \leqslant 2$

$$\lfloor M(n) \rfloor \leqslant \mathrm{la}(f) \leqslant \lceil M(n) \rceil,$$

где $M(n) = 2\left(\log_2 n - \log_2 \log_2 n + \log_2 \frac{e}{2}\right)$, *стремится к* 1 *при* $n \to \infty$.

Глава 4 посвящена алгоритмическим вопросам нахождения уровня аффинности.

В разделе 4.1 приводится алгоритм определения уровня аффинности булевых функций общего вида со сложностью $O(N^3)$ $(N = 2^n)$.

В разделе 4.2 рассматриваются симметрические булевы функции. В терминах константных и чередующихся слоев булевой функции доказывается Теорема 4.1, позволяющая находить уровень аффинности симметрической булевой функции исходя из ее упрощенного вектора значений. На основании этой теоремы приводится алгоритм, определяющий уровень аффинности симметрической булевой функции по ее упрощенному вектору значений со сложностью $O(n)$ операций сравнения, где n — длина входа.

В разделе 4.3 показана NP-трудность задачи определения уровня аффинности булевых функций с ограничением на количество мономов в АНФ:

Теорема 4.4. *Задача нахождения уровня аффинности булевой функции из* $\mathcal{F}_{\mathrm{c}}(n)$ *является NP-трудной. Здесь*

$$\mathcal{F}_{\mathrm{c}}(n) = \{f \in \mathcal{F}_n \colon \mathrm{len}(f) \leqslant cn, c = \mathrm{const}\},$$

где $\mathrm{len}(f)$ *— количество мономов в АНФ функции* f.

Благодарности

Автор выражает глубокую благодарность своему научному руководителю кандидату физико-математических наук Логачеву Олегу Алексеевичу за постановку задачи, всестороннюю помощь и внимание к работе над диссертацией, а также всем сотрудникам кафедры математической кибернетики факультета ВМК МГУ имени Ломоносова за доброжелательное отношение и творческую атмосферу.

Публикации автора по теме диссертации

1. М. Л. Буряков, О. А. Логачев. *Об уровне аффинности булевых функций.* Дискретная математика, том 17, вып. 4, 2005, сс. 98–107.

2. М. Л. Буряков. *О связи уровня аффинности с криптографическими параметрами булевых функций.* Дискретная математика, том 20, вып. 2, 2008, сс. 3–15.

3. М. Л. Буряков. *Асимптотические оценки уровня аффинности для почти всех булевых функций.* Дискретная математика, том 20, вып. 3, 2008, сс. 73–79.

4. М. Л. Буряков. *Об уровне аффинности некоторых классов булевых функций.* VI Международная конференция «Дискретные модели в теории управляющих систем. Москва, 7–11 декабря 2004 г. Труды. Сс.231–235, М.: Издательский отдел Факультета ВМиК МГУ им. М. В. Ломоносова, 2004.

5. М. Л. Буряков. *О некоторых свойствах уровня аффинности комбинирующих булевых функций.* Математика и безопасность информационных технологий. Материалы конференции в МГУ 28–29 октября 2004 г., сс. 136–141 — М.: МЦНМО, 2005.

6. М. Л. Буряков, О. А. Логачев. *О распределении уровня аффинности на множестве булевых функций.* Математика и безопасность информационных технологий. Материалы конференции в МГУ 28–29 октября 2004 г., сс. 141–146 — М.: МЦНМО, 2005.

7. М. Л. Буряков. *Об уровне аффинности комбинирующих булевых функций.* Сборник тезисов лучших дипломных работ 2005 года, сс. 62–64 — М.: Издательский отдел Факультета ВМиК МГУ им. М. В. Ломоносова, 2005.

8. М. Л. Буряков. *Об уровне аффинности симметрических булевых функций.* Материалы IX Международного семинара «Дискретная математика и ее приложения», сс. 421–423 — М.: Издательство механико-математического факультета МГУ, 2007.