МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

На правах рукописи

Тарannиков Юрий Валерьевич

КОНСТРУКЦИИ И СВОЙСТВА КОРРЕЛЯЦИОННО-ИММУННЫХ И ПЛАТОВИДНЫХ БУЛЕВЫХ ФУНКЦИЙ

2.3.6 — методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

доктора физико–математических наук

Москва 2023

Работа выполнена в ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» на Механико-математическом факультете на кафедре дискретной математики.

Официальные оппоненты:

Алексеев Валерий Борисович,
доктор физико-математических наук,
профессор, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра математической кибернетики.

Кротов Денис Станиславович,
доктор физико-математических наук,
профессор РАН, главный научный сотрудник, ФГБУН Институт математики имени С. Л. Соболева СО РАН.

Черемушкин Александр Васильевич,
доктор физико-математических наук,
профессор, академик Академии криптографии РФ.

Защита состоится 27 сентября 2023 года в 16 час. 45 мин. на заседании диссертационного совета МГУ.012.3 ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» по адресу: Российская Федерация, 119234, Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М. В. Ломоносова, Механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВО МГУ имени М. В. Ломоносова, по адресу: Москва, Ломоносовский проспект, д. 27 и на портале: https://dissovet.msu.ru/dissertation/012.3/2603.

Автореферат разослан «28» июня 2023 года.

Ученый секретарь
диссертационного совета МГУ.012.3
кандидат физико-математических наук Галатенко Алексей Владимирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертация посвящена решению проблемы обеспечения стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности.

С помощью математических подходов автором изучены параметры криптографически важных функций, в первую очередь корреляционно-иммунных и платовидных, установлены оценки на эти параметры и на их взаимосвязь между собой. Построены функции, обладающие криптографически хорошими параметрами, в том числе экстремальными, в широких диапазонах значений. Предложены эффективные схемные и программные реализации таких конструкций. Получены эффективные оценки, асимптотические и точные формулы для числа функций из криптографически важных классов и вспомогательных комбинаторных объектов, включая разбиения пространства на аффинные подпространства.

Актуальность темы. Методы разработки и анализа систем (средств) обеспечения информационной безопасности имеют математическую природу и используются в рамках математических моделей, описывающих функционирование таких систем, действия противника и возможные угрозы информационной безопасности. Фундаментальной проблемой в области разработки и анализа систем обеспечения информационной безопасности является обеспечение стойкости систем защиты информации против криптографических атак, среди которых выделяются различные виды корреляционных атак. Признанным и распространенным средством противостояния указанным криптографическим атакам является использование в качестве криптографического примитива булевых функций, обладающих хорошими специфическими характеристиками, включающими степень корреляционной иммунности, нелинейность,

глобальную автокорреляционную характеристику и другими. Большое число криптографически важных булевых функций строится на основе платовидных функций — функций с трехуровневым носителем спектра. Про некоторые функции с оптимальными криптографическими свойствами доказано, что они обязаны быть платовидными. В связи с этим являются актуальными задачи изучения возможности построения, разработки конструкций и исследования свойств булевых функций, в том числе корреляционно-иммунных и платовидных, противостоящих в качестве криптографического примитива различным видам корреляционных атак на системы защиты информации. Методы решения этих задач имеют математическую природу и используют математический аппарат и подходы различных разделов математики, в том числе методы арифметики, элементарной, линейной и высшей алгебры, теории функций, перечислительной и словарной комбинаторики, теории комбинаторных дизайнов, теории сложности вычислений.

Таким образом, тема диссертации, посвященной обеспечению стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности актуальна как в теоретическом, так и в прикладном смысле.

Области исследования. Диссертация представляет результаты исследований в области информационной безопасности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 2.3.6 (физико-математические науки) по следующим областям исследования.

1. Теория и методология обеспечения информационной безопасности и защиты информации.

9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

10. Модели и методы оценки защищенности информации и информационной безопасности объекта.

15. Принципы и решения (технические, математические, организаци-

онные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Исследования базируются на известных теоретических положениях арифметики, элементарной, линейной и высшей алгебры, теории функций, перечислительной и словарной комбинаторики, теории комбинаторных дизайнов, теории сложности вычислений.

Цель работы — анализ возможности построения, разработка эффективных конструкций и исследование свойств булевых функций, в первую очередь корреляционно-иммунных и платовидных, для противодействия в качестве криптографического примитива различным видам корреляционных атак на системы защиты информации. Получение эффективных оценок, асимптотических и точных формул для числа функций из криптографически важных классов и вспомогательных объектов.

Для достижения поставленной цели в диссертации представлены новые теоретические результаты, существенно расширяющие возможности использования и анализа булевых функций в качестве криптографического примитива в системах защиты информации. Приводятся новые результаты о булевых функциях и их криптографически важных свойствах: корреляционной иммунности, устойчивости, нелинейности, автокорреляционных характеристиках, аффинном ранге, совокупностях коэффициентов Уолша булевой функции (ее спектре), их структуре и характеристиках. Предлагаются новые конструкции функций, их схемные и программные реализации, оценки параметров, оценки числа исследуемых функций и вспомогательных объектов.

Научная новизна работы состоит в строго доказанных новых утверждениях и характеризуется следующими результатами:

— установлен факт, что верхняя оценка нелинейности $2^{n-1} - 2^{m+1}$ для

m-устойчивых функций от n переменных может достигаться только на функциях, достигающих равенства в неравенстве Зигенталера;

— разработаны методы построения m-устойчивых функций от n переменных с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$, в частности, с использованием введенных подходящих и обобщенных подходящих матриц;

— с помощью разработанных методов построены m-устойчивые функции от n переменных с нелинейностью $2^{n-1} - 2^{m+1}$ при всех парах (m, n), удовлетворяющих неравенству $0{,}6n - 1 \leq m \leq n - 2$, а асимптотически при $0,5789\ldots(1 + o(1)) \leq m/n$;

— получена нижняя оценка автокорреляционной характеристики m-устойчивой функции от n переменных;

— получен вид формул для числа корреляционно-иммунных и устойчивых порядка $m = n - k$ булевых функций от n переменных; доказано, что эта формула является полиномом степени $p(k)$; получены оценки на величину $p(k)$;

— построены платовидные функции с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$ для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1} - 2$;

— установлен факт, что при q, равном степени простого числа, для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$; получены нижние и верхние оценки на величину $N_q(m)$, найдено точное значение $N_q(2) = q + 1$; результаты того же типа получены для разбиений на грани;

— установлен факт, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1;

— получен критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций, сводящий рассматриваемую задачу для функций к соответствующей задаче для мно-

жеств слов.

Теоретическая значимость. Результаты могут найти применение в теории защиты информации, теории синтеза схем, теории кодирования, математической кибернетике, дискретной математике.

Практическая значимость. Разработанные автором в диссертационной работе методы, построенные функции и смежные объекты, установленные свойства, в частности разработанные эффективные схемные и программные методы реализации m-устойчивых функций от n переменных, могут применяться в криптографических примитивах и системах защиты информации, в частности, в поточных шифрах. Не исключено приложение метода, включающего обобщенные подходящие матрицы, для построения систем функций, а также в блочных шифрах. Результаты по корреляционно-иммунным функциям могут быть задействованы при разработке криптографических масок.

На защиту выносятся: обоснование актуальности, научная новизна, теоретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в заключении диссертации.

1. Эффективные схемные и программные методы реализации m-устойчивых функций от n переменных для криптографических примитивов и систем защиты информации.

2. Верхняя оценка на число нелинейных переменных в устойчивых булевых функциях высокого порядка.

3. Теорема для регулярных булевых функций типа теоремы Симона–Вегенера.

4. Описание всех возможных значений аффинного ранга платовидной функции с носителем спектра мощности 16.

5. Установление вида асимптотических формул для числа разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств и граней при $m = \text{const}$, $n \to \infty$.

6. Описание всех булевых функций, равномерно распределенных по шарам со степенью 1, и точный подсчет их количества.

7. Описание всех минимальных бесконечных инвариантных классов; доказательство, что число таких классов — континуум.

СОДЕРЖАНИЕ РАБОТЫ

Глава 1 диссертации начинается с параграфа 1.1, в котором даются основные определения и понятия, принятые в литературе по булевым функциям и используемые в диссертации. В параграфе 1.2 приводятся простейшие результаты. Эти результаты широко известны и содержатся в монографиях[1] [2] [3], обзорной статье автора [4]. Приведенные простейшие результаты для полноты изложения снабжены доказательствами, как правило, в изложении диссертанта. В параграфе 1.3 описывается связь корреляционно-иммунных функций с ортогональными массивами, описываются известные результаты для ортогональных массивов, уже без доказательств. В параграфе 1.4 устанавливается верхняя оценка нелинейности корреляционно-иммунной порядка m и m-устойчивой функций от n переменных.

Теорема 1.2. *Пусть $f(x_1, \ldots, x_n)$ является m-устойчивой булевой функцией, $m \leq n-2$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^{m+1}. \tag{1.8}$$

Теорема 1.2 была доказана автором[5] [6] и независимо Саркаром и

[1] Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В. Булевы функции в теории кодирования и криптологии. М: Ленанд, 2021. 576 с.

[2] Cusick T. W., Stanica P. Cryptographic Boolean Functions and Applications (Second Edition), Academic Press, 2017.

[3] Carlet C. Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press, 2020.

[4] Тарапников Ю. В. О критериях бесконечности инвариантных классов дискретных функций, Математические вопросы кибернетики, Вып. 9, М., Физматлит, 2000, с. 59–78.

[5] Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/005, March 2000, 18 pp.

[6] Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity, Proceedings of Indocrypt 2000, Lecture Notes in Computer Science, V. 1977, pp. 19–30, Springer-Verlag, 2000.

Майтрой[7] и Зенгом и Зангом[8]. Заметим, что в каждой из указанных работ есть дополнительные результаты, не содержащиеся в других работах. В частности, автором была установлена следующая далее теорема 1.3, которая в параллельных работах Саркара–Майтры и Зенга–Занга получена не была.

Теорема 1.3. *Пусть $f(x_1, \ldots, x_n)$ является m-устойчивой неоптимальной булевой функцией, $m \leq n-3$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^{m+2}.$$

Неоптимальной здесь называется функция, для которой не достигается равенство в неравенстве Зигенталера.

В конце параграфа 1.4 приводится верхняя оценка нелинейности неуравновешенных корреляционно-иммунных функций. Следующая теорема 1.6 была доказана автором. Этот же результат получен и в параллельных работах Саркара и Майтры и Зенга и Занга.

Теорема 1.6. *Пусть $f(x_1, \ldots, x_n)$ — неуравновешенная корреляционно-иммунная порядка m булева функция, $m < n$. Тогда*

$$nl(f) \leq 2^{n-1} - 2^m. \tag{1.12}$$

Заметим, что из следствия 1.7 вытекает, что m-устойчивая функция, на которой достигается равенство в оценке (1.8), обязана быть платовидной; конструкциям таких функций будет посвящена следующая глава 2. Глава же 1 заканчивается параграфом 1.5, в котором рассматриваются линейные и квазилинейные переменные и свойства обладающих такими переменными функций. Эти факты будут использованы при разработке и анализе конструкций в следующей главе 2.

[7]Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions, In Advanced in Cryptology: Crypto 2000, Proceedings, Lecture Notes in Computer Science, V. 1880, 2000, pp. 515–532.

[8]Zheng Y., Zhang X. M. Improved upper bound on the nonlinearity of high order correlation immune functions, Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Science, V. 2012, pp. 264–274, Springer-Verlag, 2001.

Глава 2 диссертации посвящена конструкциям m-устойчивых булевых функций от n переменных, нелинейность которых достигает верхней границы $2^{n-1} - 2^{m+1}$. До того, как была установлена оценка (1.8), такие функции специально не изучались, однако изучение существовавших конструкций показывает, что они позволяли построить функции, нелинейность которых достигает оценки (1.8), лишь для m не меньше, чем примерно $n - \log_2 n$. На протяжении главы излагаются последовательно улучшающиеся автором методы, позволяющие построить m-устойчивые функции для все большего диапазона параметров. Несмотря на последовательное улучшение методов, результаты более ранних параграфов не вкладываются полностью в последующие результаты, поскольку последующие результаты приобретают все более асимптотический характер.

В параграфе 2.1 представлена предложенная автором рекурсивная конструкция, в которой из двух функций, связанных определенными условиями, строятся две новых. Эта конструкция позволила построить m-устойчивые булевы функции от n переменных, нелинейность которых достигает верхней границы $2^{n-1} - 2^{m+1}$, при $\frac{2n-7}{3} \leq m \leq n-2$. В параграфе 2.2 конструкция предыдущего параграфа была доработана и установлена следующая теорема.

Теорема 2.2. *Для целых m и n, удовлетворяющих неравенствам $\frac{2n-7}{3} \leq m \leq n - \log_2 \frac{n+2}{3} - 2$, существует m-устойчивая булева функция на $\mathbf{F}_2^n$ с нелинейностью $2^{n-1} - 2^{m+1}$, достигающая неравенства Зигенталера для каждой отдельной переменной.*

Заметим, что на самом деле не просто установлен факт существования, а предложен конструктивный и эффективный метод построения таких криптографически важных функций, полезных в системах защиты информации.

В параграфе 2.3 из множества построенных в предыдущих двух параграфах функций выделены две специальные последовательности регулярных функций, обладающих экстремальными свойствами.

В параграфе 2.4 рассматриваются аспекты схемной реализации функций, построенных в предыдущих параграфах. Показано, что такая реа-

лизация может быть осуществлена с линейными по числу переменных сложностью и временем, что делает применение построенных функций перспективным для использования в криптографических примитивах и системах защиты информации.

В параграфе 2.5 описывается предложенный автором усовершенствованный по сравнению с параграфом 2.1 метод построения устойчивых функций, достигающих верхней границы нелинейности. Вводится и подробно описывается центральное для этого метода понятие **подходящей (k_0, k, p, t)-матрицы.** В параграфе 2.6 строятся эффективные примеры подходящих матриц, удовлетворяющих определениям, данным в параграфе 2.5. С их помощью строятся m-устойчивые функции от n переменных с максимальной нелинейностью $2^{n-1} - 2^{m+1}$ для более широкого, чем в предыдущих параграфах, диапазона значений. В частности, доказана следующая теорема.

Теорема 2.8. $\mathrm{nlmax}(n, m) = 2^{n-1} - 2^{m+1}$ *для* $0.6n - 1 \leq m \leq n - 2$.

В параграфе 2.7 излагается следующее усовершенствование. Понятие подходящей матрицы обобщается до **обобщенной (k_0, k, p, t)-подходящей матрицы.** Изучаются свойства обобщенных подходящих матриц и возможность их использования для построения m-устойчивых функций с максимальной возможной нелинейностью. В частности, доказана следующая теорема.

Теорема 2.9. *Если существует обобщенная (k, k, p, t)-походящая матрица, то можно построить последовательность m-устойчивых функций на $\mathbf{F}_2^n$, достигающих границы (1.8), при $n \to \infty$, $\frac{m}{n} \to \frac{t}{t+k}$.*

В параграфе 2.8 предлагаются и исследуются рекурсивные конструкции на основе обобщенных подходящих матриц. В результате доказывается следующее утверждение.

Следствие 2.3. *Пусть α — действительная константа,* $0.5789... \leq \alpha \leq 1$. *Тогда существует последовательность m-устойчивых функций на $\mathbf{F}_2^n$, достигающих границы (1.8), для которой $\frac{m}{n} \to \alpha$.*

В параграфе 2.9 обсуждается сложность реализации функций из предложенных в параграфе 2.8 конструкций. Показывается, как эффек-

тивно вычислить значение реализуемой функции ветвящейся программой, имеющей небольшую вычислительную сложность. Отмечено, что если зафиксировать обобщенную (k, k, p, t)-подходящую матрицу, и последовательно применять ее в конструкции растущее число раз, а перестановки переменных на каждом шаге ограничить последними не более чем $2p$ разрядами, то сложность вычисления значения построенной функции ветвящейся программой будет линейной.

В параграфе 2.10 решается комбинаторная задача, тесно связанная с существованием и построением *подходящих матриц,* рассматривавшихся в параграфах 2.5 и 2.6 для построения устойчивых функций, достигающих верхней границы нелинейности. Помимо вышесказанного результаты этого параграфа имеют и общекомбинаторное значение. В параграфе 2.10 устанавливается максимальное число непересекающихся граней с нижним уровнем $l_1 = 1$ и верхним уровнем l_2 в булевом кубе B^n и строится пример, показывающий, что попытка казалось бы естественного обобщения теоремы о максимальном паросочетании в двух соседних слоях булева куба является, вообще говоря, несостоятельной.

В параграфе 2.11 элементы техники, использовавшейся для построения обобщенных подходящих матриц в параграфе 2.8, выделены в самостоятельный комбинаторный объект: *упаковки* (n, k)*-продуктов.* Введено понятие *совершенной упаковки* (n, k)*-продуктов,* которую можно рассматривать как разновидность комбинаторных дизайнов, близкую виктурнирам. Отметим, что существование совершенной упаковки $(10, 3)$-продуктов позволило ранее установить основные результаты параграфа 2.8. Приведены некоторые оценки величин $A_{n,k}$ — максимальной мощности упаковки (n, k)-продуктов.

В параграфе 2.12 показано, что, ограничиваясь средствами, предложенными в предыдущих параграфах этой главы, нельзя построить m-устойчивые функции от n переменных с оптимальной нелинейностью при $m/n \leq \frac{1}{1+\log_2(1.971044...)}(1 + o(1)) = 0.505316...(1 + o(1))$. Впрочем, сказанное не исключает дальнейшего совершенствования методов. Заметим, что отношение m/n, близкое к $0.505316...$, для многих практических це-

лей является хорошим, поэтому построения в рамках техники работы[9] тоже представляют интерес.

В то время, как в главе 2 исследовалась связь корреляционной иммунности булевых функций с их нелинейностью, **глава 3** посвящена анализу взаимосвязей корреляционной иммунности с другими криптографически важными свойствами булевых функций, в частности, с их автокорреляционными характеристиками. Главным методом изучения в этой главе является спектральный анализ, т. е. использование коэффициентов Уолша и их свойств, а также автокорреляционных коэффициентов.

В параграфе 3.1 представлена нижняя оценка для абсолютной автокорреляционной характеристики Δ_f устойчивых функций, сформулированная в следующей теореме.

Теорема 3.2. *Пусть f является m-устойчивой булевой функцией на $\mathbf{F}_2^n$. Тогда $\Delta_f \geq \left(\frac{2m-n+3}{n+1}\right) 2^n$.*

Эта оценка является нетривиальной при $2m-n+3 > 0$ и в указанном диапазоне лучшей из известных.

В параграфе 3.2 доказывается верхняя оценка на число нелинейных переменных в устойчивых булевых функциях высокого порядка. Функции, которые зависят от некоторых переменных линейно, являются во многих приложениях криптографически слабыми, поэтому их использование на практике нежелательно. Кроме того, такие функции не представляют интереса и с теоретической точки зрения, поскольку линейные переменные можно просто отбросить (удалив их в полиноме функции или, что то же самое, подставив вместо них константу 0). Тогда и число переменных функции, и степень ее устойчивости уменьшатся на число отброшенных линейных переменных и задача сведется к исследованию функции без линейных переменных. Поэтому важным вопросом является здесь существование устойчивых функций, которые зависят от

[9]Таранников Ю. В. Несократимые разложения однородных произведений двучленов для построения m-устойчивых функций с максимально возможной нелинейностью. Проблемы теоретической кибернетики. Материалы XVII Международной конференции (Казань, 16–20 июня 2014 г.). — Проблемы теоретической кибернетики. — Казань: Отечество, 2014. — с. 271–272.

всех своих переменных нелинейно. Первоначально автором было доказано[10] [11] [12], что для любого натурального k существует минимальное неотрицательное целое $p(k)$, любая $(n-k)$-устойчивая функция от n переменных зависит нелинейно от не более чем $p(k)$ переменных. Позднее[13] [14] автором совместно с его студентом Денисом Кириенко было доказано, что $p(k) \leq (k-1)4^{k-2}$. В этом параграфе доказывается оценка $p(k) \leq (k-1)2^{k-2}$, полученная автором в 2001 году в работе[15] (результаты этой работы содержится в также в работе[16]). При $k = 3$ эта оценка достигается на функции $f_3(x_1, \ldots, x_4)$, приведенной в параграфе 2.3. При $k = 4$ оценка уже не точна, поскольку в работах[17] [18] показано, что

[10]Tarannikov Yu. Ramsey-like theorems on the structure and numbers of higher order correlation-immune functions, Moscow State University, French-Russian Institute of Applied Mathematics and Informatics, Preprint No 5, Moscow, October 1999, 20 pp.

[11]Тарасников Ю. В. О структуре и числе корреляционно-иммунных функций наивысших порядков, Материалы IX Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 16–19 декабря 1998 г.), Москва, Изд-во механико-математического факультета МГУ, 1999, с. 81–92.

[12]Tarannikov Yu. On the structure and numbers of higher order correlation-immune functions, Proceedings of 2000 IEEE International Symposium on Information Theory ISIT2000, Sorrento, Italy, June 25–30, 2000, p. 185.

[13]Тарасников Ю. В., Кириенко Д. П. Спектральный анализ корреляционно-иммунных функций высокого порядка, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 177–189.

[14]Тарасников Ю. В., Кириенко Д. П. Спектральный анализ корреляционно-иммунных функций высокого порядка, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 177–189.

[15]Тарасников Ю. В. Об автокорреляционных свойствах корреляционно-иммунных функций, Материалы VII международного семинара «Дискретная математика и ее приложения» (29 января — 2 февраля 2001 г.), М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 3, с. 331–333.

[16]Tarannikov Yu., Korolev P., Botev A. Autocorrelation coefficients and correlation immunity of Boolean functions, Proceedings of Asiacrypt 2001, Gold Coast, Australia, December 9–13, 2001, Lecture Notes in Computer Science, V. 2248, pp. 460–479, Springer-Verlag, 2001.

[17]Тарасников Ю. В., Кириенко Д. П. Спектральный анализ корреляционно-иммунных функций высокого порядка, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 177–189.

[18]Tarannikov Yu., Kirienko D. Spectral analysis of high order correlation immune functions, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/050, October 2000, 8 pp.

$p(4) = 10$; однако отличается от нижней оценки $p(k) \geq 3 \cdot 2^{k-2} - 2$, достигаемой на специальной последовательности функций, впервые построенной автором в работе[19] и приведенной в параграфе 2.3, в линейное по k число раз. Результаты параграфа опубликованы в работе автора[20] и входят в состав работы[21].

Помимо представления булевой функции полиномом Жегалкина, существует также единственное представление булевой функции f мультилинейным полиномом над $\mathbf{R}$. Степень этого полинома (т. е. длина самого длинного монома) называется *действительной степенью* функции f. В 1994 году Нисан и Сегеди доказали[22], что у булевой функции с действительной степенью не выше d число существенных переменных не превосходит $d \cdot 2^{d-1}$. Оказалось, что этот результат эквивалентен оценке автора $p(k) \leq (k-1)2^{k-2}$. Насколько известно автору, факт эквивалентности этих задач в явном виде до сих пор не опубликован. В неявном виде указание на эквивалентность задач было опубликовано в 2014 году О'Доннеллом в качестве непронумерованного замечания между утверждениями 6.23 и 6.24 в монографии[23].

В 2020 году результат Нисана–Сегеди был усилен до $n \leq C \cdot 2^d$, где $C = 6.614\ldots$ [24] и $C = 4.416\ldots$ [25]. Заметим, что это автоматически означает усиление оценки теоремы 3.4 до $p(k) \leq C \cdot 2^{k-1}$ с тем же самым зна-

[19] Tarannikov Yu. On a method for the constructing of cryptographically strong Boolean functions, Moscow State University, French-Russian Institute of Applied Mathematics and Informatics. Preprint No 6, Moscow, October 1999, 24 pp.

[20] Тарапников Ю. В. Об автокорреляционных свойствах корреляционно-иммунных функций, Материалы VII международного семинара «Дискретная математика и ее приложения» (29 января — 2 февраля 2001 г.), М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 3, с. 331–333.

[21] Tarannikov Yu., Korolev P., Botev A. Autocorrelation coefficients and correlation immunity of Boolean functions, Proceedings of Asiacrypt 2001, Gold Coast, Australia, December 9–13, 2001, Lecture Notes in Computer Science, V. 2248, pp. 460–479, Springer-Verlag, 2001.

[22] Nisan N., Szegedy M. On the degree of Boolean functions as real polynomials, Comput Complexity, Vol. 4, 1994, pp. 301–313.

[23] O'Donnell, R. Analysis of Boolean Functions, Cambridge: Cambridge University Press, 2014.

[24] Chiarelli J., Hatami P., Saks M. An asymptotically tight bound on the number of relevant variables in a bounded degree Boolean function, Combinatorica, Vol. 40, 2020, pp. 237–244.

[25] Wellens J. Relationships between the number of inputs and other complexity measures of Boolean functions. Ithaca, NY: Cornell Univ., 2020. (Cornell Univ. Libr. e-Print Archive; arXiv:2005.00566).

чением $C = 4.416\ldots$. Отметим, что авторы статьи[26] наряду с верхней оценкой $n \leq 6.614 \cdot \cdots \cdot 2^d$, доказывают также и нижнюю, эквивалентную оценке автора $p(k) \geq 3 \cdot 2^{k-2} - 2$ и достигающуюся на той же самой последовательности функций (только заданной в другой форме), что свидетельствует о том, что эквивалентность двух указанных выше задач и статьи по параллельной тематике были еще в 2020 году неизвестны даже некоторым активно работающим в этой области исследователям.

В параграфе 3.3 коэффициенты Уолша применяются для исследования корреляционно-иммунных и устойчивых булевых функций. В параграфе устанавливаются необходимые условия, связывающие число переменных, устойчивость и вес неуравновешенных неконстантных корреляционно-иммунных функций и доказывается, что такие функции не существуют при $m > 0.75n - 1.25$. Похожие утверждения известны[27] [28] для функций с несколькими выходами (операторов), но для обычных булевых функций до работ автора утверждения такого типа не были сформулированы даже как гипотезы. Для высоких порядков m этот неожиданный факт превзошел хорошо известное неравенство Бирбрауэра–Фридмана[29] [30]. Одновременно главный результат параграфа явился новым необходимым условием на число строк простого двоичного ортогонального массива. Заметим, что это необходимое условие впервые (если не считать очевидного факта, что число строк должно делиться на двойку в степени, равной силе массива) имеет немонотонное по числу строк поведение. До настоящего времени все усилия исследователей в этой области были направлены исключительно на получение

[26]Chiarelli J., Hatami P., Saks M. An asymptotically tight bound on the number of relevant variables in a bounded degree Boolean function, Combinatorica, Vol. 40, 2020, pp. 237–244.

[27]Bierbrauer J., Gopalakrishnan K., Stinson D. R. Orthogonal arrays, resilient functions, error correcting codes and linear programming bounds, SIAM J. Discr. Math., V. 9, 1996, p. 424–452.

[28]Levenshtein V. Split orthogonal arrays and maximum independent resilient systems of functions, Designs, Codes and Cryptography, V. 12, 1997, pp. 131–160.

[29]Friedman J. On the bit extraction problem, Proc. 33rd IEEE Symposium on Foundations of Computer Science, 1992, pp. 314–319.

[30]Bierbrauer J. Bounds on orthogonal arrays and resilient functions, Journal of Combinatorial Designs, V. 3, 1995, pp. 179–183.

нижних оценок для числа строк в массиве (или как иногда любят говорить, для «мощности дизайна»).

В 2007 году Дмитрий Германович Фон-Дер-Флаасс усилил главный результат этого параграфа и доказал[31], что неуравновешенные неконстантные корреляционно-иммунные функции порядка m от n переменных не существуют при $m > \frac{2}{3}n - 1$, назвав свой результат доказательством «гипотезы Таранникова». Этот результат Фон-Дер-Флаасса является во многих отношениях окончательным, поскольку известны бесконечные семейства функций с $m = \frac{2}{3}n - 1$. В 2010 году ученик автора А. В. Халявин обобщил[32] результат Фон-Дер-Флаасса на ортогональные массивы, доказав, что если при $m > \frac{2}{3}n - 1$ существует $OA(N, n, 2, m)$, то $N \geq 2^{n-1}$; причем если $N = 2^{n-1}$, то ортогональный массив является простым.

В теореме 3.5 параграфа 3.3 дано необходимое условие существования неуравновешенных неконстантных корреляционно-иммунных булевых функций высокого порядка. В теореме 3.4 параграфа 3.2 дана верхняя оценка для числа нелинейных переменных в устойчивых функциях высокого порядка. Однако в некоторых случаях эти оценки можно улучшить более тонким исследованием. Элементы такого подхода разрабатываются в параграфе 3.4. Приведенные в нем результаты содержатся в работах[33] [34].

В параграфе 3.4 результаты о спектральной структуре корреляционно-иммунных и устойчивых булевых функций используются для исследования корреляционно-иммунных функций высокого

[31]Fon-Der-Flaass D. G. A bound on correlation immunity. Siberian electronic mathematical reports. — 2007. — Vol. 4. — pp. 133–135.

[32]Халявин А. В. Оценка мощности ортогональных массивов большой силы. Вестник Московского университета. Серия 1: Математика. Механика. — 2010. — №3. — с. 49–51.

[33]Таранников Ю. В., Кириенко Д. П. Спектральный анализ корреляционно-иммунных функций высокого порядка, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 177–189.

[34]Tarannikov Yu., Kirienko D. Spectral analysis of high order correlation immune functions, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/050, October 2000, 8 pp.

порядка. Вводится матрица ненулевых коэффициентов Уолша и устанавливаются важные свойства этой матрицы. Эти свойства применяются для доказательства несуществования неуравновешенной неконстантной корреляционно-иммунной порядка $n-4$ функции от $n \geq 10$ переменных.

Асимптотики числа корреляционно-иммунных функций и устойчивых от n переменных малого порядка k (т. е. когда k или константа, или растет достаточно медленно по отношению к n) были получены в работах[35] [36]. В параграфе 3.5 изучаются количества таких функций высокого порядка, а именно устанавливается вид точных и асимптотических формул для числа корреляционно-иммунных и устойчивых порядка $n-k$ функций от n переменных при $k = \text{const}$, $n \to \infty$.

Обозначим через $A(k,i)$ число $(i-k)$-устойчивых булевых функций на $\mathbf{F}_2^i$.

Теорема 3.12. *Число $R(n, n-k)$ устойчивых порядка $n-k$ функций на $\mathbf{F}_2^n$ выражается формулой*

$$R(n, n-k) = \sum_{i=0}^{p(k)} A(k,i) \binom{n}{i};$$

при $n > 3k-3$ число $K(n, n-k)$ корреляционно-иммунных порядка $n-k$ функций на $\mathbf{F}_2^n$ выражается формулой

$$K(n, n-k) = 2 + R(n, n-k) = 2 + \sum_{i=0}^{p(k)} A(k,i) \binom{n}{i}.$$

Следствие 3.4. *Асимптотика числа $R(n, n-k)$ устойчивых порядка $n-k$ функций на $\mathbf{F}_2^n$, так же как и асимптотика числа $K(n, n-k)$ корреляционно-иммунных порядка $n-k$ функций на $\mathbf{F}_2^n$ при $k = const$, $n \to \infty$, выражается следующей формулой*

$$R(n, n-k) \sim K(n, n-k) \sim \frac{A(k, p(k))}{p(k)!} n^{p(k)}.$$

[35] Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций, Дискретная математика, 1991, Т. 3, вып. 2, с. 25–46.

[36] Canfield E. R., Gao Z., Greenhill C., McKay B. D., Robinson R. W. Asymptotic enumeration of correlation-immune Boolean functions, Cryptogr. Commun., Vol. 2, No 1, 2010, pp. 111–126.

Основное содержание параграфа 3.6 составляет теорема для регулярных функций типа теоремы Симона–Вегенера.

Следствие 3.6. *Для заданного натурального n минимальное возможное c, такое что существует c-регулярная булева функция на $\mathbf{F}_2^n$, существенно зависящая от всех своих переменных, удовлетворяет соотношению*

$$\min c = \log_2 n + O(\log_2 \log_2 n).$$

Теорему Симона–Вегенера можно наглядно сформулировать следующим образом.

Теорема Симона–Вегенера 3.14.[37] [38] *Для заданного натурального n минимальное $c(n)$, такое что существует булева функция, существенно зависящая от всех своих n переменных, у которой любой набор имеет* **не более** *$c(n)$ соседних с ним, на которых функция принимает другое значение, удовлетворяет асимптотическому соотношению*

$$c(n) = (1/2) \log_2 n + O(\log_2 \log_2 n).$$

Основной результат параграфа 3.6 переформулируется в стиле теоремы Симона–Вегенера следующим образом.

Теорема 3.15. *Для заданного натурального n минимальное $c(n)$, такое что существует булева функция, существенно зависящая от всех своих n переменных, у которой любой набор имеет* **ровно** *$c(n)$ соседних с ним, на которых функция принимает другое значение, удовлетворяет асимптотическому соотношению*

$$c(n) = \log_2 n + O(\log_2 \log_2 n).$$

[37] Simon H.-U. A tight $\Omega(\log \log n)$-bound on the time for parallel RAM's to compute nondegenerated boolean functions, FCT'83, Lecture Notes in Computer Science, V. 158, 1984, p. 439–444.

[38] Wegener I. The complexity of Boolean functions, Stutgart: B. G. Teubner, Chichester, John Wiley & Sons, 1987.

Глава 4 посвящена исследованию свойств платовидных функций, основное внимание уделяется значению их аффинного ранга в зависимости от мощности носителя спектра.

Платовидные функции представляют большой интерес сами по себе и для построения различных классов криптографически важных функций. Так, бент-функции можно рассматривать как частный случай платовидных. Специально подчеркнем, что изучавшиеся в предыдущих главах корреляционно-иммунные и устойчивые булевы функции при накладывании разнообразных дополнительных требований во многих случаях могут быть лишь платовидными. Так, например, из следствия 1.7 вытекает, что m-устойчивая функция, на которой достигается равенство в оценке (1.8), и, тем самым, обладающая максимально возможной нелинейностью при заданном порядке устойчивости, обязана быть платовидной; конструкциям таких функций почти целиком посвящена самая большая глава 2.

Толчком к исследованиям аффинного ранга платовидных функций для автора послужила статья[39], в которой рассматривался аффинный ранг только кубических функций с максимальной устойчивостью, но эти функции, как было несложно показано, обязаны были быть платовидными. Поэтому при исследовании аффинного ранга переходим к рассмотрению всех платовидных функций.

В параграфе 4.1 напоминаются основные понятия и используемые в главе 4 определения, дается описание направления исследований и полученных в главе результатов.

В параграфе 4.2 исследуется аффинные преобразования в $\mathbf{F}_2^n$; причем как аффинные преобразования самой функции, так и аффинные преобразования ее носителя спектра. В частности, доказана следующая лемма.

Лемма 4.2. *Пусть* $W_f(x) \to W'(x) = W_f(\mathbf{A}x)$ *— аффинное пре-*

[39]Carlet C., Charpin P. Cubic Boolean functions with highest resiliency, IEEE Transactions on Information Theory, Vol. 51, No 2, 2005, pp. 562–571.

образование спектра функции f, заданной на $\mathbf{F}_2^n$. Тогда коэффициенты $W'(x)$ являются коэффициентами Уолша некоторой функции f', причем

$$f'(x) = f(xA^{-1}) + < a, xA^{-1} > .$$

Лемма 4.2 показывает, что можно работать с булевой функцией, осуществляя аффинные преобразования ее носителя спектра. Многие свойства функции при этом, выраженные через ее коэффициенты Уолша, либо не меняются, либо меняются контролируемым образом. Особенно удобны аффинные преобразования носителя спектра при преобразованиях платовидных функций. Лемма 4.2 используется как на протяжении данной главы, так и в последующих работах.

В параграфе 4.3 доказываются различные утверждения, касающиеся платовидных функций, ранга и аффинного ранга и их взаимосвязей. Эти утверждения являются вспомогательными в рамках главы 4, но представляют также и самостоятельный интерес.

В параграфе 4.4 представлены все возможные значения аффинного ранга $\mathbf{k}$ платовидных булевых функций с носителем спектра мощности 16. Ранее в работе[40] для подкласса платовидных функций с носителем спектра мощности 16 (более точно, для кубических устойчивых порядка $n-4$ функций) была получена оценка $\mathbf{k} \leq k \leq 9$. В параграфе 4.4 доказано, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6.

В параграфе 4.5 рассматриваются полученные автором оценки аффинного ранга платовидной булевой функции с произвольной мощностью $|S_f|$ носителя спектра. В частности, установлена следующая теорема.

Теорема 4.2. *Для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1} - 2$ существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$.*

[40] Carlet C., Charpin P. Cubic Boolean functions with highest resiliency, IEEE Transactions on Information Theory, Vol. 51, No 2, 2005, pp. 562–571.

Из более поздних результатов Саньяла[41] [42] следует асимптотическая оценка $\mathbf{k} = O(h \cdot 2^h)$.

В **главе 5** рассматриваются разбиения пространства $\mathbf{F}_q^n$ на аффинные подпространства, приведены результаты о числе таких разбиений. Эти вопросы связаны с основной темой диссертации следующим образом. Среди конструкций платовидных вообще и бент-функций в частности, есть конструкции, в которых функция строится путем сборки из подфункций с непересекающимися носителями спектра. Если все исходные функции являются платовидными с одинаковым значением модуля ненулевых коэффициентов Уолша, то полученная функция снова будет платовидной. Если при этом объединение носителей спектра подфункций есть все пространство $\mathbf{F}_2^n$, то получается бент-функция. Однако задачей является нахождение подходящего множества платовидных функций с непересекающимися носителями спектра. Оказывается, что если взять в качестве носителя спектра аффинное подпространство, то каждая платовидная функция с таким носителем спектра эквивалентна бент-функции от числа переменных, равных размерности аффинного подпространства; более того, между множествами таких функций существует взаимнооднозначное соответствие, которое задается аффинным преобразованием носителя спектра, описанным в лемме 4.2 главы 4.

Во вступлении к главе 5 описана конструкция K, предложенная Баксовой и Таранниковым в работе[43], где показано, что конструкция задает бент-функцию. Более того, из описания конструкции K следует, что число бент-функций от n переменных, порождаемых конструкцией K, при заданном параметре n_1 и $n_2 = n - n_1$ равно

$$L = b_{n_2-n_1}^{2^{n_1}} \cdot N_{n_2}^{n_2-n_1}, \tag{5.1}$$

[41] Sanyal S. Near-optimal upper bound on Fourier dimension of Boolean functions in terms of Fourier sparsity, Automata, Languages, and Programming. 42nd Int. Colloquium, ICALP 2015, Kyoto, Japan, July 6–10, 2015. Proceedings. Part I. Springer, Berlin, 2015, pp. 1035–1045.

[42] Sanyal S. Fourier Sparsity and Dimension. Theory of Computing, Vol. 15, No 11, 2019, pp. 1–13.

[43] Баксова И. П., Таранников Ю. В. Об одной конструкции бент-функций. Обозрение прикладной и промышленной математики. — 2020. — Т. 27, №1. — с. 64–66.

где $b_{n_2-n_1}$ — число бент-функций от $n_2 - n_1$ переменных, $N_{n_2}^{n_2-n_1}$ — число упорядоченных разбиений $\mathbf{F}_2^{n_2}$ на 2^{n_1} классов смежности линейных подпространств размерности $n_2 - n_1$.

Ту же конструкцию, но в другой терминологии предложил ранее С. В. Агиевич[44], который также получил формулу (5.1).

В параграфе 5.1 обсуждаются задачи разбиения пространства $\mathbf{F}_q^n$ на линейные и аффинные подпространства в разных их формулировках, вводится понятие разбиений, примитивных по Агиевичу (или А-примитивных разбиений).

Пусть $\bigsqcup_i E_i = \mathbf{F}_q^n$, где E_i — аффинные подпространства пространства $\mathbf{F}_q^n$, $E_i = L_i + b_i$, L_i — соответствующие линейные подпространства пространства $\mathbf{F}_q^n$, $b_i \in \mathbf{F}_q^n$. Обозначим $\bigcap_i L_i = W$. Агиевич назвал разбиение $\{E_i\}$ *примитивным,* если $W = \{\vec{0}\}$. Мы будем называть такое разбиение *примитивным по Агиевичу* или *А-примитивным.*

В параграфе 5.2 описываются свойства скалярных произведений векторов, когда один из векторов фиксирован, а второй пробегает аффинное подпространство.

В параграфе 5.3 представлены результаты о существовании А-примитивных разбиений.

Теорема 5.2. *Пусть q — степень простого числа. Для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует А-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$.*

Верхняя оценка на величину $N_q(m)$ дается следующей теоремой.

Теорема 5.3. *Пусть q — степень простого числа. Тогда $N_q(m) \leq m \cdot q^{m-1}$.*

Рекуррентная оценка на величину $N_q(m)$ дается следующей теоремой.

[44] Agievich S. Bent rectangles, Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, Amsterdam: IOS Press, 2008. P. 3–22. (NATO science for peace and security Series D: Information and communication security, Vol. 18).

Теорема 5.4. *Пусть q — степень простого числа. Тогда*

$$N_q(m+1) \geq q \cdot N_q(m) + 1.$$

Нижняя оценка на величину $N_q(m)$ дается следующей теоремой.

Теорема 5.5. *Пусть q — степень простого числа. Тогда*

$$N_q(m) \geq \frac{q^m - 1}{q - 1}.$$

Установленное точное значение величины $N_q(2)$ дается следующей теоремой. Ранее Агиевич[45] фактически доказал, что $N_2(2) = 3$.

Теорема 5.7. *Пусть q — степень простого числа. Тогда*

$$N_q(2) = q + 1.$$

В параграфе 5.4 результаты того же типа, что и в параграфе 5.3, установлены для разбиений на грани (они же координатные подпространства, или подкубы). Разбиения на грани можно рассматривать для произвольного q, поэтому результаты параграфа установлены для q, не обязательно являющихся степенью простого, для чего пришлось преодолеть дополнительные технические сложности.

В параграфе 5.5 изучается число разбиений (не обязательно A-примитивных) пространства F_q^n на q^m аффинных подпространств размерности $n - m$, а также на такое же число граней той же размерности в случае $m = \text{const}$, $n \to \infty$. Установлены асимптотики для числа таких разбиений, которые даны в следующих теоремах.

Теорема 5.14. *Пусть q (степень простого числа) и m фиксированы, $n \to \infty$. Тогда*

$$c_q(n, m) \sim C q^{N_q(m) \cdot n},$$

[45] Agievich S. Bent rectangles, Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, Amsterdam: IOS Press, 2008. P. 3–22. (NATO science for peace and security Series D: Information and communication security, Vol. 18).

где $C = \frac{c_q^*(N_q(m),m)}{q^{(N_q(m))^2}\cdot\left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)}}$*; величина* $\left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)} = \prod_{i=1}^{N_q(m)}\left(1-\frac{1}{q^i}\right)$ *известна как* q*-символ Почхаммера.*

Теорема 5.15. *Пусть* q *и* m *фиксированы,* $n \to \infty$*. Тогда*

$$c_q^{\mathrm{coord}}(n,m) \sim C' n^{N_q^{\mathrm{coord}}(m)},$$

где $C' = \frac{c_q^{\mathrm{coord}*}(N_q^{\mathrm{coord}}(m),m)}{N_q^{\mathrm{coord}}(m)!}$.

В главах 2 и 4 главное внимание уделено корреляционно-иммунным и устойчивым булевым функциям, т. е. функциям, единичные значения которых абсолютно равномерно распределены по подкубам заданной размерности $(n-m)$. Не всегда такое абсолютно равномерное распределение достижимо, особенно когда оно должно удовлетворять каким-то дополнительным требованиям. В то же время с практической точки зрения часто достаточно иметь не абсолютно равномерное, а почти равномерное распределение. В **главе 6** рассматриваются булевы функции, количество единичных значений которых в однотипных подмножествах (подкубах и шарах) одинакового размера (но зато любого) различается не более чем на заданную величину l.

В параграфе 6.1 приводятся доказательства теорем рамсеевского типа о симметрических подфункциях. Результаты данного параграфа используются в этой и последующей главах, однако они представляют и самостоятельный интерес.

В параграфе 6.2 представлены результаты изучения l-уравновешенных булевых функций. Пусть l — целое неотрицательное число. Булева функция $f(x_1, x_2, \ldots, x_n)$ называется *l-уравновешенной,* если для любых ее подфункций f_1 и f_2 от одинакового числа переменных выполнено неравенство $|wt(f_1) - wt(f_2)| \le l$. Величина $\rho(f) = wt(f)/2^n$ называется плотностью n-местной булевой функции f.

В работе[46] описаны все 1-уравновешенные булевы функции. Некоторые оценки веса l-уравновешенных булевых функций приведены в ра-

[46]Тарапников Ю. В. Класс 1-уравновешенных функций и сложность его реализации, М., — Издательство Московского университета, Вестник Московского университета. Серия 1, Математика, Механика. 1991, N 2, с. 83–85.

боте[47]. Главной целью параграфа 6.2 является доказательство того, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1. Главный результат параграфа 6.2 сформулирован в следующей теореме.

Теорема 6.5. *Для любого натурального l и любого положительного ε существует такое натуральное N, что для любого натурального n, не меньшего N, и для любой l-уравновешенной булевой функции f от n переменных имеет место одно из следующих пяти неравенств:*

$$wt(f) \le 2l;$$
$$|\rho(f) - 1/3| < \varepsilon;$$
$$|\rho(f) - 1/2| < \varepsilon;$$
$$|\rho(f) - 2/3| < \varepsilon;$$
$$wt(f) \ge 2^n - 2l.$$

Здесь и далее *шаром* радиуса r с центром α будем называть множество наборов, отстоящих от α на расстояние, не большее r. Весом функции f на шаре (или для краткости просто весом шара) будем называть число 1-наборов функции f, принадлежащих этому шару. Шар радиуса r веса m будем для краткости называть (r, m)-шаром. Шар радиуса r веса не меньше m будем называть $(r, m)^*$-шаром.

Пусть l — целое неотрицательное число. Булеву функцию $f(x_1, x_2, \ldots, x_n)$ будем называть *равномерно распределенной по шарам со степенью l (l-РРШ функцией),* если модуль разности весов любых двух шаров одинакового радиуса не превосходит l.

В параграфе 6.3 представлены результаты изучения функций, равномерно распределенных по шарам со степенью 1, и дано полное описание таких функций. Равномерное распределение единичных значений булевых функций по шарам ранее не изучалось интенсивно, хотя представляется, что булевы функции, единичные значения которых равномерно распределены по шарам, могут иметь разнообразные полезные приложе-

[47]Тарапников Ю. В. О числе единичных значений l-уравновешенных булевых функций, Дискретный анализ и исследование операций. 1995. Т. 2, N 1. с. 80–81.

ния, например, когда булева функция играет роль хеширующей функции, или когда желательно, чтобы при использовании характеристического кода этой функции все возможные слова на выходе канала связи имели бы приблизительно одинаковое количество способов подходящего декодирования. Такие булевы функции имеют в качестве комбинирующих функций в потоковых шифрах хорошую устойчивость против статистических атак, когда противник имеет возможность изменять некоторое (ограниченное) число входов функции, поэтому доказательство несуществования таких функций в некоторых случаях (для некоторых значений параметров) доказывает и то, что упомянутые статистические атаки в таких случаях могут иметь гарантированный успех.

В качестве возможного объяснения того, почему подобными вопросами не занимались ранее, можно отметить, что полученный результат является достаточно неожиданным, а используемая техника — неочевидной. Действительно, равномерно распределить наборы по шарам какого-го одного радиуса возможно. Несложно заметить, что характеристическая функция совершенного кода с кодовым расстоянием 3 (например, кода Хэмминга) и функция $f(x_1, \ldots, x_{2n+1}) = \bigoplus_{i=1}^{n+1} x_i$ абсолютно равномерно распределены по шарам радиуса 1; функция от нечетного числа переменных n, которая принимает одинаковые значения на противоположных наборах, абсолютно равномерно распределена по шарам радиуса $\frac{n-1}{2}$. Однако оказывается, что равномерно распределить единичные значения по шарам разных радиусов (даже не абсолютно, а приблизительно) во многих случаях оказывается уже невозможно.

Основной результат параграфа 6.3 сформулирован в следующей теореме.

Теорема 6.6. *Если n-местная булева функция f с весом $wt(f) \leq 2^{n-1}$ является 1-РРШ функцией, то имеет место хотя бы один из*

следующих трех случаев:

$$1)\ wt(f) \leq 2;$$
$$2)\ n \leq 4;$$
$$3)\ n = 6, wt(f) = 4.$$

Как следствие, подсчитано число 1-РРШ функций.

Следствие 6.7. *Число* 1*-РРШ функций от* n *переменных равно*

$$\begin{cases} 2^{2^n} & \textit{при}\ \ n \leq 2, \\ 80 & \textit{при}\ \ n = 3, \\ 334 & \textit{при}\ \ n = 4, \\ 2818 & \textit{при}\ \ n = 6, \\ 3 \cdot 2^n + 2 & \textit{при}\ \ n \geq 5, n\ \textit{нечетно}, \\ (n+3)2^n + 2 & \textit{при}\ \ n \geq 8, n\ \textit{четно}. \end{cases}$$

Глава 7 посвящена результатам исследований инвариантных классов дискретных функций. Инвариантные классы булевых функций были введены С. В. Яблонским в работе[48], но более известна его последующая работа[49]. В этой главе рассматриваются не только инвариантные классы булевых функций, но и классы функций, заданных на двоичных наборах и принимающих k значений. Булевы функции из инвариантных классов не являются, вообще говоря, функциями с равномерно распределенными единичными значениями. Однако, тем не менее, многие рассматриваемые в предыдущих главах работы классы функций с равномерно распределенными единичными значениями являются инвариантными. Так, инвариантными являются класс $(n-k)$-устойчивых функций от n переменных (для заданного k) и класс l-уравновешенных функций (для заданного l). Тут, впрочем, надо сделать оговорку, что эти классы не являются инвариантными по классическому определению

[48] Яблонский С. В. О классах функций алгебры логики, допускающих простую схемную реализацию, Успехи матем. наук, 1957, Т. 12, №6, с. 189–196.

[49] Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем, Проблемы кибернетики, вып. 2, М.: Физматгиз, 1959, с. 75–121.

С. В. Яблонского, потому что они не замкнуты относительно добавления фиктивных переменных. Поэтому надо или делать оговорку о том, что включаем вместе с функцией в класс все функции, получающиеся из нее добавлением фиктивной переменной, или просто исключить такое добавление из определения инвариантного класса. Этим главным образом и объясняется то, что наряду с классическим определением инвариантного класса по С. В. Яблонскому в этой главе рассматриваются и неклассические определения инвариантного класса, в которых операция добавления несущественной переменной не учитывается.

Помимо того, что некоторые классы функций с равномерно распределенными единичными значениями являются инвариантными, важна также и общность методов и подходов. Так во многих рассуждениях предыдущих глав являлось важным, что если мы перейдем от функции к ее подфункции, подставив, например, вместо переменной константу, или удалив линейную переменную из ее полинома, то мы получим снова функцию из того же класса. Этим и вызван интерес к инвариантным классам в данной работе, для которой, таким образом, инвариантные классы являются идейно близким объектом.

В параграфе 7.1 дается общее понятие инвариантного класса и некоторые определения, в том числе обсуждаются различные способы определения инвариантного класса.

В параграфе 7.2 даются краткие сведения из теории слов, избегающих запреты.

В параграфе 7.3 предлагается критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов. Задание инвариантных классов через множества запрещенных подфункций использовалось уже при введении инвариантных классов С. В. Яблонским, однако до работы автора[50] та-

[50]Таранников Ю. В. О критериях бесконечности инвариантных классов дискретных функций, Математические вопросы кибернетики, Вып. 9, М., Физматлит, 2000, с. 59–78.

кой критерий предложен не был.

В параграфе 7.4 рассматриваются минимальные бесконечные инвариантные классы функций, т. е. такие классы, что при добавлении к множеству запрещенных функций любой функции из класса класс перестает быть бесконечным. Представлено описание всех минимальных бесконечных инвариантных классов и доказательство теоремы, что число таких классов — континуум.

Степень достоверности и апробация результатов. Достоверность полученных результатов обеспечивается строгими математическими выкладами и доказательствами утверждений, апробацией на конференциях и семинарах, а также публикациями в рецензируемых журналах. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Результаты диссертации математически строго доказаны. Они неоднократно докладывались на научных семинарах «Булевы функции в криптологии», «Математические вопросы кибернетики», «Синтез и сложность управляющих систем» на механико-математическом факультете МГУ, «Теория кодирования», «2022-арные квазигруппы и смежные вопросы» в ИМ им. С. Л. Соболева, семинаре по теории кодирования Института проблем передачи информации им. А. А. Харкевича, научных семинарах в Индийском статистическом институте (Колката), Институте индустриальных наук университета Токио, технологическом университете Квинсленда, на конференциях «Синтез и сложность управляющих систем», «Проблемы теоретической кибернетики», «Межгосударственный семинар по дискретной математике и ее приложениям», «Математика и безопасность информационных технологий», «Международная научная конференция по проблемам безопасности и противодействия терроризму», «Сибирская конференция по исследованию операций», «Институт продвинутого изучения по разностным множествам, последовательностям и их корреляционным свойствам» (Германия), «Институт продвинутого изучения по булевым функциям в криптологии», «Индо-российская конференция по алгебре, теории чисел и дискретной матема-

тике», Международная конференция «Графы и группы, спектры и симметрии», «Международный симпозиум по комбинаторной оптимизации», Международный семинар «Алгебраическая и комбинаторная теория кодирования» (Болгария), «Индокрипт», «Азиякрипт», Семинар «Быстрое программное шифрование» (Япония).

Структура и объем работы.

Диссертация состоит из введения, семи глав, разбитых на параграфы, заключения и списка литературы из 189 наименований. Работа изложена на 287 страницах.

ЗАКЛЮЧЕНИЕ

Изложенные в работе основные результаты автора состоят в следующем.

1. Установлена теорема, что для m-устойчивой неоптимальной булевой функции f при $m \leq n-3$ выполнено $nl(f) \leq 2^{n-1} - 2^{m+2}$. Корреляционно-иммунные и устойчивые булевы функции активно изучались, были получены некоторые описания, но оставалась, в частности, непроясненной связь с нелинейностью. Оценки $nl(f) \leq 2^{n-1} - 2^{m+1}$ для m-устойчивых и $nl(f) \leq 2^{n-1} - 2^{m+1}$ были получены автором, а также независимо в параллельных работах Саркара–Майтры и Зенга–Занга. В каждой из этих работ есть дополнительные результаты, не содержащиеся в других работах. В частности, установленная теорема о верхней оценке нелинейности m-устойчивой неоптимальной булевой функции в параллельных работах Саркара–Майтры и Зенга–Занга получена не была.

2. Разработаны методы построения m-устойчивых функций от n переменных с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$, в частности, с использованием введенных подходящих и обобщенных подходящих матриц, что решило вопросы о существовании m-устойчивых функций, достигающих оценки нелинейности $nl(f) \leq 2^{n-1} - 2^{m+1}$ и эффективном построения таких функций.

3. С помощью этих разработанных автором методов построены m-устойчивые функции от n переменных с нелинейностью $2^{n-1} - 2^{m+1}$ при

всех парах (m, n), удовлетворяющих неравенству $0{,}6n - 1 \leq m \leq n - 2$, а асимптотически при $0,5789\ldots(1 + o(1)) \leq m/n$. Также автором разработаны эффективные методы схемной и программной реализации m-устойчивых функций от n переменных для криптографических примитивов и систем защиты информации.

4. Получена новая рекордная при $m > (n-3)/2$ нижняя оценка для абсолютной автокорреляционной характеристики m-устойчивой функции от n переменных: $\Delta_f \geq \left(\frac{2m-n+3}{n+1}\right) 2^n$. Важное значение имеют связи корреляционной иммунности с другими криптографически важными параметрами булевых функций; в частности, с ее автокорреляционными характеристиками. До автора уже было известно несколько оценок на глобальную автокорреляционную характеристику корреляционно-иммунных и m-устойчивых булевых функций.

5. Получен вид формул для числа корреляционно-иммунных и устойчивых порядка $m = n - k$ булевых функций от n переменных; доказано, что эта формула является полиномом степени $p(k)$; получены оценки на величину $p(k)$. Автор не ограничился получением собственно оценок на автокорреляционные характеристики, но и использовал автокорреляционные коэффициенты как мощное средство для получения других результатов. В частности, автор с их помощью получил верхнюю оценки на число нелинейных переменных в $(m = n - k)$-устойчивых булевых функциях высокого порядка: $n \leq (k-1)2^{k-2}$. Этот результат позволил в свою очередь получить вид формул для числа корреляционно-иммунных и устойчивых порядка $m = n - k$ булевых функций от n переменных; формула оказалась полиномом степени $p(k)$; были также получены оценок на величину $p(k)$. Заметим, что ранее были получены асимптотики лишь для числа корреляционно-иммунных функций малого порядка (константного или медленно растущего).

6. Построены платовидные функции с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$ для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1} - 2$. Платовидные функции представляют большой интерес сами по себе и для построения различных

классов криптографически важных функций. Так, бент-функции можно рассматривать как частный случай платовидных. Также платовидными неизбежно должны быть функции ограниченной алгебраической степенью с максимальной при этом устойчивостью. Шарпин и Карле исследовали кубические функции с максимальной устойчивостью (которые должны быть платовидными с мощностью носителя спектра 16) и получили некоторые оценки на их аффинный ранг. Автор нашел все возможные значения аффинного ранга платовидной функции с носителем спектра мощности 16: а именно 4, 5 и 6, в то время как оценка французов для подмножества функций давала более широкий диапазон. Автор пошел в этом направлении еще дальше и построил для любого натурального $\mathbf{k}$, удовлетворяющего неравенствам $2h \leq \mathbf{k} \leq 2^{h+1}-2$, платовидную функцию с носителем спектра мощности 4^h и аффинным рангом $\mathbf{k}$. До сих пор неизвестно, существует ли платовидная функция с параметрами вне этого диапазона.

7. Установлен факт, что при q, равном степени простого числа, для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$. Получены нижние и верхние оценки на величину $N_q(m)$, найдено точное значение $N_q(2) = q+1$; результаты того же типа получены для разбиений на грани. Среди конструкций платовидных вообще и бент-функций в частности, есть конструкции, в которых функция строится путем сборки из подфункций с непересекающимися носителями спектра. Если все исходные функции являются платовидными с одинаковым значением модуля ненулевых коэффициентов Уолша, то полученная функция снова будет платовидной. Если при этом объединение носителей спектра подфункций есть все пространство $\mathbf{F}_2^n$, то получается бент-функция. Однако проблемой является нахождение подходящего множества платовидных функций с непересекающимися носителями спектра. Оказывается, что если взять в качестве носителя спектра аффинное подпространство, то каждая платовидная функция с таким носителем спектра эквивалентна бент-функции

от числа переменных, равных размерности аффинного подпространства; более того, между множествами таких функций существует взаимно-однозначное соответствие, которое задается аффинным преобразованием носителя спектра. В связи со сказанным выше, стала актуальной задача о разбиении пространства $\mathbf{F}_2^n$ на аффинные подпространства и подсчете числа таких разбиений. Поскольку существуют обобщения бент-функций с двоичного на q-ичный случай, автор также рассматривал разбиения пространства $\mathbf{F}_q^n$. Автор установил и доказал тот факт, что при q, равном степени простого числа, для любого натурального m существует наименьшее натуральное $N = N_q(m)$, что при $n > N$ не существует примитивных по Агиевичу разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Автор также получил нижние и верхние оценки на величину $N_q(m)$, нашел точное значение $N_q(2) = q+1$; получил результаты того же типа для разбиений на грани. С помощью этих результатов автор получил вид асимптотических формул для числа разбиений (не обязательно примитивных по Агиевичу) пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств и граней при $m = \mathrm{const}$, $n \to \infty$.

8. Установлен факт, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1. Корреляционно-иммунные и устойчивые булевы функции являются функциями, единичные значения которых абсолютно равномерно распределены по подкубам заданной размерности $n - m$. Не всегда такое абсолютно равномерное распределение достижимо, особенно когда оно должно удовлетворять каким-то дополнительным требованиям. В то же время с практической точки зрения часто достаточно иметь не абсолютно равномерное, а почти равномерное распределение. Поэтому автор рассмотрел также булевы функции, количество единичных значений которых в однотипных подмножествах (подкубах и шарах) одинакового размера (но зато любого) различается не более чем на заданную величину l. Автор установил и доказал тот факт, что при больших n плотности l-уравновешенных функций близки к одному из следующих пяти чисел: 0, 1/3, 1/2, 2/3 или 1. Автор описал все булевы функции,

равномерно распределенные по шарам со степенью 1, и точно подсчитал их количество.

9. Получен критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов. Инвариантные классы булевых функций были введены С. В. Яблонским. Булевы функции из инвариантных классов не являются, вообще говоря, функциями с равномерно распределенными единичными значениями. Однако, тем не менее, многие рассматриваемые в предыдущих главах работы классы функций с равномерно распределенными единичными значениями являются инвариантными. Так, инвариантными являются класс $(n-k)$-устойчивых функций от n переменных (для заданного k) и класс l-уравновешенных функций (для заданного l). Тут, впрочем, надо сделать оговорку, что эти классы не являются инвариантными по классическому определению С. В. Яблонского, потому что они не замкнуты относительно добавления фиктивных переменных. Поэтому надо или делать оговорку о том, что включаем вместе с функцией в класс все функции, получающиеся из нее добавлением фиктивной переменной, или просто исключить такое добавление из определения инвариантного класса. Этим главным образом и объясняется то, что наряду с классическим определением инвариантного класса по С. В. Яблонскому автор рассматривал и неклассические определения инвариантного класса, в которых операция добавления несущественной переменной не учитывается. Помимо того, что некоторые классы функций с равномерно распределенными единичными значениями являются инвариантными, важна также и общность методов и подходов. Так во многих рассуждениях предыдущих глав являлось важным, что если мы перейдем от функции к ее подфункции, подставив, например, вместо переменной константу, или удалив линейную переменную из ее полинома, то мы получим снова функцию из того же класса. Этим и вызван интерес автора к инвариантным классам в данной работе, для которой,

таким образом, инвариантные классы являются идейно близким объектом. Автор получил критерий, позволяющий по системе запрещенных подфункций, задающих инвариантный класс, определить, содержит ли этот класс бесконечное число существенно разных функций. Критерий сводит рассматриваемую задачу для функций к соответствующей задаче для множеств слов. Автор описал все минимальные бесконечные инвариантные классы и доказано, что число таких классов — континуум.

Таким образом, полученные автором в диссертации результаты, являются существенными продвижениями по широкому фронту направлений в решении проблемы обеспечения стойкости систем защиты информации против криптографических атак, среди которых выделяются различные виды корреляционных атак.

Благодарность. Благодарю профессорско-преподавательский состав механико-математического факультета за полученное образование и сотрудников кафедры дискретной математики за внимание к работе.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, RSCI

[1] Таранников Ю. В. О числе единичных значений l-уравновешенных булевых функций, Дискретный анализ и исследование операций. 1995. Т. 2, N 1. с. 80–81 (РИНЦ 0.535).

[2] Таранников Ю. В. О некоторых оценках для веса l-уравновешенных булевых функций, Дискретный анализ и исследование операций. 1995. Т. 2, N 4. с. 80–96 (РИНЦ 0.535). [Перевод на английский язык: Tarannikov Yu. V. On certain bounds for the weight of l-balanced Boolean functions. Mathematics and Its Applications, V. 391, Korshunov

A. D. (ed.), Operation Research and Discrete Analysis, 1997, 285–299.]

[3] Тарannиков Ю. В. О классе булевых функций, равномерно распределенных по шарам со степенью 1, М., — Издательство Московского университета, Вестник Московского университета, Серия 1, Математика, Механика, 1997, N 5, с. 17–21 (РИНЦ 0.472). [Перевод на английский язык: Tarannikov Yu. A class of Boolean functions homogeneously distributed over balls with degree 1. Moscow University Mathematics Bulletin. — 1997. — Vol. 52, №. 5. — pp. 18–22 (SJR 0.417).]

[4] Carlet C., Tarannikov Yu. Covering sequences of Boolean functions and their cryptographic significance, Designs, Codes and Cryptography, V. 25, 2002, pp. 263–279 (JIF 1.397, SJR 1.122) / Ю. В. Тарannиковым получены результаты разделов 5 и 6 (по тексту статьи).

[5] Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Lecture Notes in Computer Science, V. 2247, pp. 254–266, Springer-Verlag, 2001 (SJR 0.407) / Ю. В. Тарannиков получил результаты разделов 5, 6 и 7 (по тексту статьи).

[6] Tarannikov Yu. On the structure and numbers of higher order correlation-immune functions, Proceedings of 2000 IEEE International Symposium on Information Theory ISIT2000, Sorrento, Italy, June 25–30, 2000, p. 185 (SJR 0.872).

[7] Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity, Proceedings of Indocrypt 2000, Lecture Notes in Computer Science, V. 1977, pp. 19–30, Springer-Verlag, 2000 (SJR 0.407).

[8] Tarannikov Yu., Kirienko D. Spectral analysis of high order correlation immune functions, Proceedings of 2001 IEEE International Symposium on Information Theory ISIT2001, Washington, DC, USA, June 2001, p. 69 (SJR 0.872) / Ю. В. Тарannиковым доказаны теоремы 1, 2, 3 и частично теорема 4, за исключением исследования случаев $n = 11, 12$ (по тексту статьи).

[9] Tarannikov Yu., Korolev P., Botev A. Autocorrelation coefficients and correlation immunity of Boolean functions, Proceedings of Asiacrypt 2001,

Gold Coast, Australia, December 9–13, 2001, Lecture Notes in Computer Science, V. 2248, pp. 460–479, Springer-Verlag, 2001 (SJR 0.407) / Ю. В. Таранников получил результаты разделов 3, 4 и 7 (по тексту статьи).

[10] Tarannikov Y. New constructions of resilient Boolean functions with maximal nonlinearity, Fast Software Encryption, 8th International Workshop, FSE 2001, Yokohama, Japan, April 2–4, 2001. Revised Papers. Lecture Notes in Computer Science. Vol. 2355, pp. 66–77, Springer-Verlag, 2002 (SJR 0.407).

[11] Fedorova M., Tarannikov Yu. On impossibility of uniform distribution of codewords over spheres in some cases, Proceedings of 2002 IEEE International Symposium on Information Theory ISIT2002, Lausanne, Switzerland, June 30 – July 05, 2002. — 2002. — p. 344 (SJR 0.872) / Ю. В. Таранниковым предложены постановка задачи, методика исследований, а также получены результаты при $l = 1$.

[12] Таранников Ю. В. О значениях аффинного ранга носителя спектра платовидной функции. Дискретная математика. — 2006. — Т. 18, №3. — с. 120–137 (РИНЦ 0.624). [Перевод на английский язык: Tarannikov Yu. V. On values of the affine rank of the support of spectrum of a plateaued function. Discrete Mathematics and Applications. — 2006. — Vol. 16, №. 4. — pp. 401–421 (SJR 0.226).]

[13] Tarannikov Yu. Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters. Siberian electronic mathematical reports. — 2014. — Vol. 11. — pp. 229–245 (SJR 0.516).

[14] Таранников Ю. В. О рангах подмножеств пространства двоичных векторов, допускающих встраивание системы Штейнера $S(2, 4, v)$. Прикладная дискретная математика. — 2014. — №1 (23). — с. 73–76 (SJR 0.214, РИНЦ 0.368).

[15] Sauskan A. V., Tarannikov Y. V. On packings of (n, k)-products. Siberian electronic mathematical reports. — 2016. — Vol. 13. — pp. 888–896 (SJR 0.516) / А. В. Саускан выдвинул идею рекурсивной конструкции в доказательстве теоремы 2 (по тексту статьи), Ю. В. Таранников офор-

мил математически строгое доказательство теоремы 2, а также получил другие результаты статьи.

[16] Khalyavin A. V., Lobanov M. S., Tarannikov Yu. V. On plateaued Boolean functions with the same spectrum support. Siberian electronic mathematical reports. —2016. — Vol. 13. — pp. 1346–1368 (SJR 0.516) / Ю. В. Таранников получил результаты раздела 3, написал обзор в разделе 1, а также принял участие в математически строгом оформлении некоторых результатов раздела 2 (по тексту статьи).

[17] Баксова И. П., Таранников Ю. В. Оценки числа разбиений пространства $\mathbf{F}_2^m$ на аффинные подпространства размерности k. Вестник Московского университета. Серия 1: Математика. Механика. — 2022. — №3. — с. 21–25 (РИНЦ 0.472). [Перевод на английский язык: Baksova I. P., Tarannikov Yu. V. The bounds on the number of partitions of the space $\mathbf{F}_2^m$ into $\boldsymbol{k}$-dimensional affine subspaces. Moscow University Mathematics Bulletin. — 2022. — Vol. 77, №. 3. — pp. 131–135 (SJR 0.417).] / Ю. В. Таранниковым предложены постановка задачи и методика исследований.

[18] Таранников Ю. В. О существовании разбиений, примитивных по Агиевичу. Дискретный анализ и исследование операций. — 2022. — Т. 29, №4. — с. 104–123 (РИНЦ 0.535). [Перевод на английский язык: Tarannikov Y. V. On the existence of Agievich-primitive partitions. Journal of Applied and Industrial Mathematics. — 2022. — Vol. 16, №. 4 (SJR 0.391).]

Публикации в рецензируемых научных изданиях, входивших в перечень ВАК Минобрнауки России

[19] Таранников Ю. В. О критериях бесконечности инвариантных классов дискретных функций, Математические вопросы кибернетики, Вып. 9, М., Физматлит, 2000, с. 59–78.

[20] Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях, Математические вопросы кибернетики / Под ред. О. Б. Лупанов. — Т. 11 из Математические вопросы кибернетики. — М.:

Физматлит, 2002. — С. 91–148.

Другие публикации

[21] Тарannиков Ю. В. Класс 1-РРШ функций и сложность его реализации, Материалы XI Международной конференции «Проблемы теоретической кибернетики», 10–14 июня 1996 г., М., Рос. гос. гуманит. ун-т, 1996, с. 189–190.

[22] Тарannиков Ю. В. О весах l-уравновешенных булевых функций. В сб. Материалы VII межгосударственной школы-семинара «Синтез и сложность управляющих систем», Минск, 13–16/XI 1995. М: изд-во механико-математич. ф-та МГУ, 1996, с. 28.

[23] Тарannиков Ю. В. О классах булевых функций, единичные значения которых равномерно распределены по однотипным подмножествам. Второй Сибирский Конгресс по Прикладной и Индустриальной Математике, тезисы докладов, Новосибирск, Институт математики СО РАН, 1996, с. 126.

[24] Kasim-Zadeh O. M., Tarannikov Yu. V., Zykov K. A. Complexity and combinatorial aspects of informatics systems. In: Applied mathematics and computer science. Proceedings of the Conference on Applied Mathematics and Computer Science, 28–29 October 1996, Moscow, Russia. M: изд-во механико-математич. ф-та МГУ, 1997, p. 82–90.

[25] Тарannиков Ю. В. Однородные булевы наборы и функции. Материалы Международных научных чтений по аналитической теории чисел и ее приложениям, состоявшихся на механико-математическом факультете МГУ им. М. В. Ломоносова 3–6 февраля 1997 года. М: изд-во механико-математич. ф-та МГУ, 1997, с. 31–33.

[26] Tarannikov Yu. Limit values for the density of l-balanced k-valued functions defined over the Boolean cube, International Symposium on Combinatorial Optimization, Bruxelles, 15–17 April 1998, p. 191.

[27] Тарannиков Ю. В. О предельных значениях плотности l-уравно-

вешенных k-значных функций, заданных на булевом кубе, Международная Сибирская конференция по исследованию операций, Новосибирск, 22–27 июня 1998 г., с. 140.

[28] Тарannиков Ю. В. О корреляционно-иммунных булевых функциях наивысших порядков, Проблемы теоретической кибернетики. Тезисы докладов XII Международной конференции. (Нижний Новгород, 17–22 мая 1999 г.), Москва, Изд-во механико-математического факультета МГУ, 1999, с. 223.

[29] Тарannиков Ю. В. О структуре и числе корреляционно-иммунных функций наивысших порядков, Материалы IX Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 16–19 декабря 1998 г.), Москва, Изд-во механико-математического факультета МГУ, 1999, с. 81–92.

[30] Tarannikov Yu. Ramsey-like theorems on the structure and numbers of higher order correlation-immune functions, Moscow State University, French-Russian Institute of Applied Mathematics and Informatics, Preprint No 5, Moscow, October 1999, 20 pp.

[31] Tarannikov Yu. On a method for the constructing of cryptographically strong Boolean functions, Moscow State University, French-Russian Institute of Applied Mathematics and Informatics. Preprint No 6, Moscow, October 1999, 24 pp.

[32] Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/005, March 2000, 18 pp.

[33] Tarannikov Yu. On some connections between codes and cryptographic properties of Boolean functions, Proceedings of Seventh International Workshop on Algebraic and Combinatorial Coding Theory, Bansko, Bulgaria, June 18–24, 2000, pp. 299–304.

[34] Tarannikov Yu., Kirienko D. Spectral analysis of high order correlation immune functions, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/050, October 2000, 8 pp.

[35] Tarannikov Yu. New constructions of resilient Boolean functions with

maximal nonlinearity, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/069, December 2000, 11 pp.

[36] Тарannиков Ю. В. Одно естественное обобщение теоремы о максимальном паросочетании в двух соседних слоях булева куба является неверным, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 173–176.

[37] Тарannиков Ю. В., Кириенко Д. П. Спектральный анализ корреляционно-иммунных функций высокого порядка, Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем», Нижний Новгород, 20–25 ноября 2000 г., М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 177–189.

[38] Тарannиков Ю. В. Числовые характеристики булевых функций, Дискретная математика и ее приложения. Сборник лекций молодежных научных школ по дискретной математике и ее приложениям, М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 1, с. 129–144.

[39] Тарannиков Ю. В. Об автокорреляционных свойствах корреляционно-иммунных функций, Материалы VII международного семинара «Дискретная математика и ее приложения» (29 января — 2 февраля 2001 г.), М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 3, с. 331–333.

[40] Тарannиков Ю. В. Несуществование неуравновешенных неконстантных корреляционно-иммунных порядка m булевых функций от n переменных при $m > 0.75n - 1.25$, Материалы XII Международной школы-семинара «Синтез и сложность управляющих систем», Пенза, 15–21 октября 2001 г, М., Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2001, Ч. 2, с. 212–218.

[41] Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2001/083, October 2001, 16 pp.

[42] Тарannиков Ю. В. Теорема типа теоремы Симона–Вегенера для регулярных булевых функций. Проблемы теоретической кибернетики. Тезисы докладов XIII Международной конференции (Казань, 27–31 мая 2002 г.). — Проблемы теоретической кибернетики. — М.: Изд-во центра прикладных исследований при мех.-мат. ф-те МГУ, 2002. — с. 175.

[43] Тарannиков Ю. В. О построении корреляционно-иммунных и устойчивых булевых функций. Труды V Международной конференции «Дискретные модели в теории управляющих систем» (26–29 мая 2003 г.). — М.: МАКС Пресс Москва, 2003. — с. 84–85.

[44] Тарannиков Ю. В. Об аффинном ранге платовидных функций. Труды VI Международной конференции «Дискретные модели в теории управляющих систем» (7–11 декабря 2004 г.). — М.: МАКС Пресс, 2004. – с. 259–262.

[45] Тарannиков Ю. В. О платовидных устойчивых булевых функциях. Материалы VIII Международного семинара «Дискретная математика и ее приложения», 2–6 февраля 2004 г., Москва, —М.: МГУ, 2004. — с. 431–435.

[46] Тарannиков Ю. В. О новых конструкциях нелинейных фильтров для поточных шифраторов и их устойчивости против стандартных и новых криптографических атак. Математика и безопасность информационных технологий. Материалы конференции в МГУ 23–24 октября 2003 г. — М.: МЦНМО, 2004. — с. 160–164.

[47] Тарannиков Ю. В. О значениях аффинного ранга носителя спектра платовидных функций. Математика и безопасность информационных технологий. Материалы конференции в МГУ 28–29 октября 2004 г. — М.: МЦНМО, 2005. — с. 226–231.

[48] Tarannikov Yu. On affine rank of spectrum support for plateaued function. Cryptology ePrint archive (http://eprint.iacr.org/), Report 2005/399, November 2005, 22 pp.

[49] Тарannиков Ю. В. Алгебраические атаки на потоковые шифры и алгебраическая иммунность булевых функций. Материалы международной научной конференции по проблемам безопасности и противодействия

тероризму. — М.: МНЦМО, 2006. — с. 132–140.

[50] Tarannikov Yu. On correlation immune Boolean functions. Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, Amsterdam: IOS Press, 2008. P. 219–231. (NATO science for peace and security Series D: Information and communication security, Vol. 18).

[51] Тарапников Ю. В. Описание одного класса рекурсивных конструкций булевых функций. Современные проблемы математики, механики и их приложений. Материалы международной конференции, посвященной 70-летию ректора МГУ академика В. А. Садовничего. — М.: Университетская книга, 2009. — с. 401.

[52] Тарапников Ю. В. Корреляционная иммунность и другие криптологические свойства булевых функций. Современные проблемы математики и механики. Т. III. Математика. Вып. 3. Дискретная математика. — М.: Изд-во Московского университета, 2009. — с. 95–142.

[53] Тарапников Ю. В. О верхней оценке аффинного ранга носителя спектра платовидной функции. Материалы X Международного семинара «Дискретная математика и ее приложения» (Москва, 1–6 февраля 2010 г.). — М.: Изд-во механико-математического факультета МГУ, 2010. — с. 529–531.

[54] Тарапников Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.: МЦНМО, 2011. — 152 с.

[55] Тарапников Ю. В. О булевых функциях из пересечения нескольких специальных классов. Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2012 г.). — М.: Изд-во мех.-мат. ф-та МГУ, 2012. — с. 433–436.

[56] Tarannikov Yu. Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters. Cryptology ePrint archive (http://eprint.iacr.org/), Report 2014/164, March 2014, 19 pp.

[57] Тарапников Ю. В. Несократимые разложения однородных про-

изведений двучленов для построения m-устойчивых функций с максимально возможной нелинейностью. Проблемы теоретической кибернетики. Материалы XVII Международной конференции (Казань, 16–20 июня 2014 г.). — Проблемы теоретической кибернетики. — Казань: Отечество, 2014. — с. 271–272.

[58] Тарannиков Ю. В. О возможности построения m-устойчивых функций с оптимальной нелинейностью в рамках одного метода. Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.). — М.: Изд-во механико-математического факультета МГУ Москва, 2016. — с. 394–397.

[59] Тарannиков Ю. В. On plateaued Boolean functions with the same spectrum support. Graphs and Groups, Spectra and Symmetries, 2016: Abstracts of the International Conference and PhD-Master Summer School on Graphs and Groups, Spectra and Symmetries. Novosibirsk: Sobolev Institute of Mathematics, 2016. — p. 38.

[60] Баксова И. П., Тарannиков Ю. В. Об одной конструкции бент-функций. Обозрение прикладной и промышленной математики. — 2020. — Т. 27, №1. — с. 64–66.

[61] Potapov V. N., Taranenko A. A., Tarannikov Yu. V. Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces. Ithaca, NY: Cornell Univ., 2021. (Cornell Univ. Libr. e-Print Archive; arXiv:2108.00232).

[62] Тарannиков Ю. В. О существовании A-примитивных разбиений. Материалы XIV Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2022 г.). — М., 2022. — с. 285–288.