ОТЗЫВ

официального оппонента

на диссертационную работу Таранникова Юрия Валерьевича «Конструкции и свойства корреляционно-иммунных и платовидных булевых функций», представленную на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность

Актуальность темы. В связи с большими потоками конфиденциальной информации в различных сетях актуальной является проблема защиты этой информации. Основным механизмом такой защиты является шифрование, то есть преобразование информации по определенным алгоритмам. Составной частью таких преобразований часто являются операторы, реализующие булевы функции от некоторых битов текущей информации, например, нелинейный фильтр в системах поточного шифрования. Для того, чтобы противостоять атакам противника, пытающегося по зашифрованным сообщениям понять алгоритмы шифрования или использованные ключи, от применяемых булевых функций требуют обычно наличия определенных свойств. При этом сразу возникают вопросы о существовании булевых функций с такими свойствами, об их количестве, об их возможных и наилучших параметрах, о методах построения функций с оптимальными или близкими к оптимальным параметрами. Именно таким крайне актуальным вопросам и посвящена диссертация Таранникова Ю.В.

Научная новизна. В основной части диссертации, состоящей из 7 глав, рассматриваются различные научные проблемы, относящиеся к общей теме диссертации – исследованию свойств и методов построения корреляционно-иммунных и платовидных булевых функций, которые обладают хорошими свойствами с точки зрения криптографии.

Корреляционно-иммунные булевы функции — это функции, в которых доля наборов, на которых функция равна 0, и доля наборов, на которых функция равна 1, совпадают с соответствующими долями у любой подфункции данной функции, полученной подстановкой ограниченного числа констант вместо переменных. Если дополнительно требуется, чтобы указанные доли равнялись ½,

а число переменных, вместо которых можно подставлять константы, ограничено целым числом m, то функция называется m-устойчивой.

Общие вопросы, связанные с корреляционно-иммунными функциями, исследуются в главах 1-3. В главе 1 даются необходимые определения и приводятся базовые результаты. Также указана связь исследуемых функций с кодами и ортогональными массивами. Одним из главных результатов здесь является верхняя оценка нелинейности m-устойчивой булевой функции от n переменных, полученная диссертантом и, независимо, Саркаром и Майтрой. Дополнительно только диссертантом доказано, что эта оценка достижима, только если достижима оценка в неравенстве Зигенталера.

Хотя основу диссертации составляют глубокие теоретические результаты, наиболее близкой к приложениям является глава 2, в которой излагаются найденные диссертантом методы построения m-устойчивых булевых функций с максимально возможной нелинейностью. Эта глава и по объему самая большая (55 страниц, 12 параграфов).

Существование m-устойчивых булевых функций, на которых достигается верхняя оценка для нелинейности, было установлено до диссертанта только для очень узкого интервала значений m (в зависимости от числа переменных n). Основным достижением диссертанта стало резкое расширение этого интервала. В параграфе 2.1 показано, что такие функции существуют при всех натуральных m от (2n-7)/3 до n-2. Важным является то, что не просто доказано существование таких функций, но предложены алгоритмы их построения.

Результаты параграфа 2.1 усиливаются в параграфе 2.2. А именно, предлагаются методы построения m-устойчивых булевых функций, для которых верхняя оценка для нелинейности достигается не только для функции в целом, но и для каждой переменной. Показано, что такие функции существуют почти для всего интервала значений m, указанного выше (немного понижается верхняя граница).

Общая конструкция из параграфа 2.2 применяется в параграфе 2.3 для построения регулярных булевых функций с высокой степенью нелинейности. В результате установлена максимальная нелинейность c-регулярных функций от n переменных при c или n-c, лежащем на отрезке от 1 до (n/4)+1 (теорема 2.5).

С точки зрения приложений важна сложность схемной реализации построенных функций. В маленьком параграфе 2.4 показано, что некоторые из предлагаемых функций допускают

схемную реализацию со сложностью, линейной по числу переменных n.

В параграфах 2.5-2.8 предложены более изощренные методы построения m-устойчивых булевых функций, на которых достигается верхняя оценка для нелинейности. С помощью этих методов диссертанту удалось расширить интервал значений m, для которых такие функции существуют. А именно, в нижней границе интервала коэффициент при n удалось понизить с 2/3 до примерно 0,5789. Полученные результаты основаны на подходе, который позволяет строить системы функций с требуемым распределением линейных и квазилинейных переменных. Этот общий подход представлен в параграфе 2.5 (теорема 2.6). Подход опирается, в частности, на существование «подходящих матриц» с заданными параметрами.

В параграфе 2.6 приведены конструкции некоторых подходящих матриц. С помощью этих матриц, используя общий подход, диссертант строит новые примеры m-устойчивых булевых функций, на которых достигается верхняя оценка для нелинейности, что позволяет ему в нижней границе интервала для m понизить коэффициент при n с 2/3 сначала до 5/8 (теорема 2.7), а затем до 0.6 (теорема 2.8).

В параграфах 2.7 и 2.8 конструкция еще усиливается с привлечением «обобщенных подходящих матриц». Теорема 2.9 сводит задачу построения m-устойчивых булевых функций, на которых достигается верхняя оценка для нелинейности, к задаче построения обобщенных подходящих матриц с заданными параметрами. Четыре конструкции, приведенные в параграфах 2.7 и 2.8, позволили диссертанту понизить нижнюю границу в интервале для m примерно до 0.5789n (теорема 2.10).

В небольших параграфах 2.9-2.12 (все вместе 11 страниц) обсуждается вопрос о вычислительной сложности построенных функций и некоторые вопросы, связанные с существованием и построением подходящих матриц.

Глава 3 посвящена исследованию свойств корреляционно-иммунных и устойчивых функций, а более точно, связи этих понятий с другими важными для криптографии свойствами. В разделе 3.1 получена нижняя оценка (лучшая из известных) для абсолютной автокорреляционной характеристики m-устойчивой булевой функции от n переменных.

Наличие переменных, от которых функция зависит линейно, рассматривается как криптографическая слабость. Поэтому важно, чтобы используемые булевы функции имели как можно больше переменных, от которых функция зависит нелинейно. Однако

диссертантом доказано, что для устойчивых функций высокого порядка это недостижимо. А именно, показано, что для любого натурального k существует минимальное неотрицательное число p(k) такое, что любая (n-k)-устойчивая функция от n переменных зависит нелинейно не более чем от p(k) переменных. В разделе 3.2 получены достаточно близкие нижняя и верхняя оценки для p(k). А также получены верхние оценки (зависящие от k) на число переменных n для любой (n-k)-устойчивой функции, которая от всех переменных зависит нелинейно.

В разделе 3.3 получен еще один результат о несуществовании корреляционно-иммунных булевых функций с заданными свойствами. А именно, доказано, что при $m > 0.75n - 1.25$ не существует неуравновешенной неконстатной корреляционно-иммунной порядка m булевой функции от n переменных. В разделе 3.4 доказан ряд утверждений, устанавливающих связи свойств корреляционно-иммунных булевых функций со свойствами матрицы ненулевых коэффициентов Уолша этих функций.

В разделе 3.5 получены результаты о числе корреляционно-иммунных и устойчивых булевых функций, в частности, получена асимптотика числа булевых функций от n переменных, корреляционно-иммунных порядка n-4.

В разделе 3.6 рассмотрена величина c(n) – минимальное значение c, при котором существует c-регулярная булева функция, существенно зависящая от n переменных. Получено асимптотическое равенство, выражающее c(n) через n.

Важное внимание в диссертции уделяется исследованию платовидных функций — функций, у которых коэффициенты Уолша принимают ровно 3 значения: 0, r и -r, где r — некоторая степень 2. Платовидные функции довольно тесно связаны с корреляционно-иммунными функциями, поскольку, например, любая m-устойчивая функция с максимальной (для данного m) нелинейностью является платовидной. В главе 4 изучается аффинный ранг носителя спектра платовидных функций. Получена верхняя оценка аффинного ранга произвольной платовидной функции в зависимости от мощности ее носителя спектра (теорема 4.3), для широкого интервала значений аффинного ранга доказано существование платовидных функций с заданной мощностью ее носителя спектра (теорема 4.2). Для платовидных функций с мощностью носителя спектра 16 доказано, что аффинный ранг может принимать только значения 4, 5 и 6.

Тематика корреляционно-иммунных функций тесно связана с другими задачами. Так, например, некоторые методы построения платовидных функций и, в частности, бент-функций опираются на

специальные разбиения n-мерного пространства над конечным полем мощности q на линейные или аффинные подпространства. В главе 5 диссертации рассматриваются специальные (A-примитивные) разбиения такого пространства на аффинные подпространства. Доказано, что для фиксированного q и любого натурального m существует наименьшее натуральное N=N(m) такое, что при n>N не существует A-примитивных разбиений такого пространства на аффинные подпространства размерности n-m. Подобный результат получен и для разбиений на грани.

Глава 6 посвящена исследованию свойств булевых функций, в которых единичные значения достаточно равномерно распределены по подфункциям или шарам. В параграфе 6.2 изучаются l-уравновешенные булевы функции, в которых число единиц в подкубах одинаковой размерности не может отличаться более чем на l. Основной здесь является теорема 6.5, которая показывает, что при большом числе переменных в l-уравновешенных функциях либо мало нулей, либо мало единиц, либо доля единиц близка к одной из дробей 1/3, ½ или 2/3. Можно отметить здесь интересную технику доказательства, связанную с исследованием и использованием свойств периодических симметрических функций.

В параграфе 6.3 изучаются булевы функции, в которых число единиц в шарах одинакового радиуса не может отличаться более чем на l. Основной здесь является теорема 6.6, которая показывает, что таких функций очень мало. В частности, в ней утверждается, что при числе переменных больше 4 у такой функции либо не более 2 единиц, либо не более 2 нулей. В теореме 6.7 установлено точное значение числа таких функций для произвольного числа переменных n.

В главе 7 диссертации автор излагает свои результаты, посвященные исследованию инвариантных классов. Здесь рассматриваются не только булевы функции, но и функции на булевом кубе, принимающие k значений. Эти результаты связаны с общей темой диссертации скорее не по объекту исследования, объявленному в названии диссертации, а по подходам и методам, поскольку в обоих случаях изучается связь функций и их подфункций. В параграфе 7.3 диссертант устанавливает критерии бесконечности инвариантных классов, заданных системой запрещенных подфункций. Здесь можно отметить удачный переход к рассмотрению только симметрических запрещенных подфункций, что позволяет перейти далее к рассмотрению их характеристических последовательностей и связать рассматриваемую задачу с известной задачей о блокирующих множествах слов. В параграфе 7.4 полученные результаты применяются для описания минимальных

бесконечных инвариантных классов (теорема 7.4). В частности, доказано, что мощность множества бесконечных инвариантных классов равна континууму (теорема 7.5).

Общая характеристика работы. Объем диссертации — 287 страниц. Диссертация состоит из «Введения», 7 глав, «Заключения» и списка литературы. Во «Введении», объемом 28 страниц, подробно обоснована актуальность диссертации, ее научная новизна, и сформулированы основные результаты диссертации. Также указаны теоретическая значимость и возможные практические применения. Учитывая, что диссертация достаточно объемная, подробное введение позволяет хорошо осознать актуальность исследований, историю вопроса и структуру диссертации. В разделе «Заключение» на 5 страницах сформулированы основные результаты диссертации (9 пунктов). Список литературы и соответствующие ссылки в диссертации показывают глубокую проработку диссертантом имеющихся результатов (список литературы содержит 189 пунктов).

Диссертация соответствует паспорту научной специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», по которой представлена диссертация, в частности пунктам 1, 9, 10, 15, 19 этого паспорта.

В диссертации проведено глубокое изучение классов булевых функций, имеющих важное значение для процессов защиты информации. Получены глубокие теоретические результаты, а также разработаны методы построения функций из рассматриваемых классов, обладающих другими криптографически важными свойствами.

Применимость результатов диссертации. Разработанные в диссертации методы, построенные с их помощью функции, а также разработанные эффективные схемные и программные реализации этих функций могут найти применение в системах защиты информации, в частности, при поточном шифровании.

Достоверность результатов, полученных в диссертации. Все результаты, полученные в диссертации, имеют корректные формулировки и обоснованы строгими доказательствами. Основные результаты опубликованы в 62 работах. Из них 18 публикаций в изданиях, индексируемых в Web of Science, Scopus, RSCI, и еще 2 публикации в изданиях из перечня ВАК. Результаты неоднократно докладывались на конференциях и научных семинарах.

Замечания по диссертации. По научному содержанию диссертации существенных замечаний нет. В формулировке леммы 6.6 (стр. 209) стоило для большей ясности указать, что

характеристический отрезок один и тот же для всех n. Однако есть замечания по оформлению диссертации.

1) Примерно 40% пунктов в оглавлении не совпадают с названиями глав и разделов в самой диссертации. Возможно, диссертант просто хотел укоротить названия в оглавлении, но, по моему мнению, так поступать не принято.

2) В пункте 1 «Заключения» (стр. 259) в строке 5 вместо второй оценки продублирована первая оценка.

3) Несколько раз, например на стр. 59 и 60, используется некорректная фраза «неравенство может достигаться» (имеется в виду, что нестрогое неравенство может обращаться в равенство).

4) Несколько раз одно и то же слово повторяется в тексте подряд 2 раза (например, «здесь» на стр. 100, «с помощью» на стр. 122, «называется» на стр.152, «причем» на стр. 203).

5) В формулировке леммы 5.2 (стр.182) не определено значение параметра m, хотя смысл понятен и при доказательстве теоремы 5.2 лемма используется корректно.

6) Есть ряд других описок, в частности, некоторое количество неверных окончаний слов.

7) В формулах на стр. 96 в последней строке пропущен знак равенства.

8) На стр. 121 имеется странное неравенство $0.5789...<0.5789...$.

Заключительная оценка. Указанные замечания не являются существенными и не влияют на общую положительную оценку работы. В диссертации разработаны методы построения корреляционно-иммунных и платовидных булевых функций, играющих важную роль в разработке надежных систем защиты информации. При этом проведено глубокое теоретическое исследование различных свойств таких функций, важных для криптографии (особенно свойства нелинейности), и некоторых проблем, близких к проблемам существования и построения корреляционно-иммунных и платовидных булевых функций. Утверждения, выносимые автором на защиту, строго доказаны. По теме диссертации автором опубликованы 20 работ в изданиях, индексируемых в базах данных Web of Science, Scopus, RSCI а также в научных изданиях из списка ВАК. Автореферат правильно отражает содержание диссертации. Считаю, что результаты диссертации Таранникова являются крупным научным достижением в области методов защиты информации.

Диссертация Юрия Валерьевича Таранникова соответствует паспорту научной специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность». Она отвечает требованиям, предъявляемым к докторским диссертациям

Московским государственным университетом имени М.В. Ломоносова, в частности, требованиям пп. 2.1 – 2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

Соискатель Таранников Юрий Валерьевич заслуживает присуждения ему ученой степени доктора физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

доктор физико-математических наук,

профессор кафедры математической кибернетики

факультета ВМК МГУ им. М. В. Ломоносова,

20.09.2023 В. Б. Алексеев

Контактная информация:

Адрес: 119991 ГСП-1 Москва, Ленинские горы, МГУ имени М.В. Ломоносова, 2-й учебный корпус, факультет ВМК

Email: vbalekseev@rambler.ru, тел. 89104502133