# ОТЗЫВ

официального оппонента на диссертацию 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”

Целью диссертационной работы является анализ возможности построения, разработка эффективных конструкций и исследование свойств булевых функций, в первую очередь корреляционно-иммунных и платовидных, для противодействия различным видам корреляционных атак на системы защиты информации. Данное направление, безусловно, является актуальным.

Основное внимание в диссертации уделено корреляционно-иммунным и устойчивым функциям, значения которых равномерно распределены по подкубам двоичного куба и которые обеспечивают наибольшую защищенность от применения корреляционных атак, учитывающих статистические зависимости между входными и выходными последовательностями функциональных схем в системах защиты информации.

Для таких функций в диссертации найдены точные верхние оценки на нелинейность и число существенных нелинейных переменных для функций с высокой степенью корреляционной-иммунности. Предложен оригинальный итеративный способ построения функций с наилучшими параметрами (высокая степень нелинейности и устойчивости), допускающий эффективную схемную и программную реализацию.

Исследовано строение носителя спектра платовидных функций, и предложен способ построения таких функций с носителем спектра мощности $4^h$ и аффинным рангом $\mathbf{k}$ при $2h \leq \mathbf{k} \leq 2^{h+1}-2$ на основе разбиения всего пространства на аффинные подпространства, на которых заданы платовидные подфункции с одинаковыми значениями модуля ненулевых коэффициентов спектра. Отдельно рассмотрена задача о числе разбиений пространства $\mathbf{F}_q^n$ на $q^m$ аффинных подпространств. Получены асимптотические формулы для числа таких разбиений, а также для числа граней при $m = const$ и $n \to \infty$.

Помимо этого изучается класс $l$-уравновешенных функций, представляющих собой некоторое расширение свойства корреляционной иммунности на случай, когда значения функции распределены неравномерно по подкубам, т.е. веса соответствующих подфункций не совпадают, а незначительно

отличаются друг от друга, а также класс функций, равномерно распределенных по шарам со степенью 1.

Обсуждается связь изучаемых классов функций с введенными С.В. Яблонским инвариантными классами.

В данной диссертационной работе автор сосредоточил основное внимание на уточнении и усилении полученных ранее им и многочисленными зарубежными авторами результатов с целью нахождения исчерпывающих точных оценок значений параметров, а также исследовании в общем случае свойств и способов построения функций с наилучшими значениями параметров.

Среди вынесенных на защиту положений наибольшую значимость имеют следующие результаты.

1. Доказана верхняя оценка $nl(f) \le 2^{n-1} - 2^{m+2}$ для неоптимальной, т.е. степени $\deg f \le n - m - 2$, $m$-устойчивой функции $f$ при $m \le n - 3$.

2. Метод построения $m$-устойчивой функции максимально возможной степени нелинейности $nl(f) = 2^{n-1} - 2^{m+1}$ при всех $(n, m)$, удовлетворяющих неравенству $0,6n - 1 \le m \le n - 2$, а также асимптотически при $0,5789\ldots n(1 + o(1)) \le m$.

3. Нижняя оценка $\Delta_f \ge \left(\frac{2m-n+3}{n+1}\right) 2^n$ для абсолютной автокорреляционной характеристики функции $f$ при $m > (n-3)/2$.

4. Верхние оценки на число нелинейных переменных для $(n-k)$-устойчивых функций высокого порядка $n \le (k-1)2^{k-2}$, что дало возможность получить формулы для числа корреляционно-иммунных и устойчивых функций порядка $m = n - k$.

5. Доказательство того, что соотношение веса к общему числу наборов переменных для $l$-уравновешенных функций при больших $n$ стремится к одному из следующих значений: 0, 1/3, 1/2, 2/3, 1.

Основные результаты диссертации опубликованы в 20 рецензируемых печатных работах, из который 18 опубликованы в научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности.

Автореферат правильно и полно отражает содержание диссертации.

Результаты диссертации являются новыми, полученными автором лично. Они четко сформулированы и оформлены в виде строгих математических доказательств.

В качестве замечаний можно высказать следующее.

1. В работе приведены полные доказательства для большого числа простых вспомогательных фактов, что более характерно для учебного пособия, а не квалификационной работы:

— для лемм 1.2, 1.4 – 1.6, 1.8 – 1.10, 1.12, 1.17, 1.18 можно было ограничиться приведенными в тексте ссылками, леммы 1.1, 1.3, 1.15, 1.17, 1.19 – 1.21, 1.25 — очевидны;

— для теоремы 3.1 на стр. 125 достаточно было ограничиться приведенными ссылками и не приводить доказательства;

— утверждение о том, что функция имеет нечетный вес тогда и только тогда, когда ее степень максимальна, очевидно. Тем не менее оно дважды сформулировано как лемма 4.10 на стр. 160 и как лемма 1.15 на стр. 46;

— леммы 4.1 – 4.3 общеизвестны. Поэтому можно было бы не приводить доказательства, а ограничиться ссылками;

— лемма 5.1 на стр. 181 очевидна, так как скалярное произведение задает гомоморфизм линейного пространства.

2. Имеются неточности в формулах:

— на стр. 52 в 10 строке снизу в формуле пропущен символ $x_i$;

— на стр. 65 в формулировке следствия 1.8 пропущен символ $f$;

— на стр. 66 в лемме 1.27 вместо $f(x_1, \ldots, x_n)$ следует писать $g(x_1, \ldots, x_n)$;

— на стр. 67 вместо $\alpha = (\alpha_1, \alpha_n, \delta)$ должно быть $\alpha = (\alpha_1, \ldots, \alpha_n, \delta)$, а также в формуле $wt(f_\alpha)2wt(g') \geq nl(g)$ пропущен знак равенства;

— на стр. 68 в формулировке следствия 1.12 пропущен символ $f$;

— на стр. 132 в 10 строке в формуле пропущен знак равенства.

3. К лемме 1.24 желательно сделать комментарий, оговорив случай, когда переменная $x_i$ является несущественной, так как формула (1.13) в этом случае принимает вид:

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) \oplus x_j.$$

4. На стр. 88 в формулировке леммы 2.5 не определен символ $s$.

5. На стр. 121 в 4 строке снизу вместо $0.5789\ldots < 0.5789\ldots$, по-видимому, следует писать $0.5789\ldots < 0.5902\ldots$

6. На стр. 152–153 приведенный абзац полностью повторяется на стр. 158–159.

7. Скалярное произведение векторов над $\mathbf{F}_2$ на стр. 42 определяется над $\mathbb{Z}$, а для $q > 2$ на стр. 181 — над $\mathbf{F}_q$. В первом случае оно является положительно определенным и соответствует определению скалярного произведения. Во втором случае лучше говорить о внутреннем произведении.

Имеются опечатки (стр. 10, 100, 158, 189, 197, 241).

Оценивая диссертационную работу в целом, считаю, что отмеченные недостатки относятся в основном к оформлению работы и не снижают общего положительного впечатления.

Автор предпринял разностороннее исследование проблем построения классов функций для возможного применения в системах защиты информации, обладающих высокой степенью противодействия корреляционным атакам. При этом он использовал методы алгебры, комбинаторики, математической логики, дискретной математики и др.

Содержание диссертации соответствует ее названию и поставленным задачам, и обладает внутренним единством. Основные выводы и заключения сформулированы достаточно полно и отражают суть полученных результатов. Диссертация представляет собой завершенную научно-исследовательскую работу, в которой на основании выполненных автором исследований разработаны теоретические положения, совокупность которых можно квалифицировать как научное достижение.

Считаю, что диссертационная работа Таранникова Юрия Валерьевича "Конструкции и свойства корреляционно-иммунных и платовидных булевых функций" удовлетворяет критериям, определенным в пп. 2.1–2.5 «Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова», предъявляемым к докторским диссертациям, соответствует специальности 2.3.6 "Методы и системы защиты информации, информационная безопасность", а ее автор заслуживает присуждения ученой степени доктора физико-математических наук.

Официальный оппонент
д.ф.-м.н, профессор, действительный член
Академии криптографии Российской Федерации

12.09.2023 А.В. Черемушкин

тел.: 8(499)162-2968
e-mail: avc238@mail.ru