МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

На правах рукописи

Баев Владимир Валерьевич

Эффективные алгоритмы получения оценок алгебраической иммунности булевых функций

Специальность 01.01.09 – дискретная математика
и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва – 2008

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

Научный руководитель: кандидат физико-математических наук, старший научный сотрудник Логачёв О.А.

Официальные оппоненты: доктор физико-математических наук, профессор Гашков С.Б.

кандидат физико-математических наук Ролдугин П.В.

Ведущая организация: Российский государственный гуманитарный университет

Защита диссертации состоится 15 февраля 2008 года в 11:00 на заседании диссертационного совета Д 501.001.44 при Московском государственном университете им. М. В. Ломоносова по адресу: 119991, ГСП-1, Москва, Ленинские горы, МГУ, 2-й учебный корпус, факультет ВМиК, аудитория 685.

С диссертацией можно ознакомиться в библиотеке факультета ВМиК МГУ. С текстом автореферата можно ознакомиться на официальном сайте факультета ВМиК МГУ: http://www.cmc.msu.ru в разделе «Наука» – «Работа диссертационных Советов» – «Д 501.001.44»

Автореферат разослан «____» января 2008 г.

Учёный секретарь диссертационного совета, профессор Трифонов Н.П.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В теории конечных автоматов, теории кодирования и криптологии возникают задачи решения систем булевых уравнений, имеющих определённую структуру. Как известно, задача решения произвольной системы полиномиальных булевых уравнений является NP-трудной, и в настоящее время для решения таких систем не известно алгоритма, который бы имел сложность по порядку меньшую, чем $2^{O(n)}$, где n — число булевых переменных в системе. Однако, для конкретных классов систем булевых уравнений иногда удаётся разработать более эффективные алгоритмы.

Одним классом конечных автономных автоматов, [3], являются *фильтрующие генераторы*. Они используются для генерации псевдослучайных последовательностей. Непосредственным применением таких генераторов являются потоковые шифры, [1]. Фильтрующий генератор выдаёт двоичную последовательность, зависящую от начального состояния (секретного ключа). При побитовом сложении этой последовательности с открытым текстом получается зашифрованное сообщение. Функция выхода фильтрующего генератора называется также *фильтрующей функцией*.

В 2003 г. в работе [12] был предложен метод анализа фильтрующих генераторов (а также других классов псевдослучайных генераторов), основанный на понижении степени исходной совместной системы полиномиальных булевых уравнений относительно начального состояния генератора. Этот метод был назван авторами *алгебраической атакой*.

Основным требованием для эффективного применения метода алгебраических атак является существование (по крайней мере, одной) ненулевой булевой функции g низкой степени (степени многочлена Жегалкина) d, которая является обнуляющим множителем либо для самой фильтрующей функции f, либо для её отрицания $f+1$, то есть $fg = 0$ или $(f+1)g = 0$.

Метод алгебраических атак позволяет (в некоторых случаях) по части выходной последовательности находить начальное состояние фильтрующего генератора за время $O(n^{3d})$, где n — длина регистра состояния генератора (число булевых переменных фильтрующей функции f), а $d = \deg g$ — степень обнуляющего множителя g (*аннигилятора*) функции f или $f+1$.

Таким образом, возникает задача поиска ненулевых аннигиляторов низкой степени для булевой функции выхода фильтрующего генератора. В 2004 г. в работе [18] был представлен алгоритм, находящий базис пространства аннигиляторов степени $\leqslant d$ со сложностью $O(\left|\mathrm{supp}(f)\right| \cdot n^{2d})$. Булева функция f задаётся на входе этого алгоритма списком элементов множества $\mathrm{supp}(f) = \{x \mid f(x) = 1\}$ — носителя функции f. Затем, в 2006 г. в работе [15] этот алгоритм был немного улучшен, но общая оценка сложности осталась прежней. Одним из основных требований для двоичных псевдослучайных генераторов является равенство частот встречаемости 0 и 1 в выходной последовательности. Это требование налагает на фильтрующую функцию условие *уравновешенности*, то есть вектор значений функции содержит одинаковое количество нулей и единиц, равное $\left|\mathrm{supp}(f)\right| = 2^{n-1}$. Как видно, для таких функций алгоритм, предложенный в [18] имеет экспоненциальную (относительно числа переменных функции f) сложность. Поэтому актуальна задача разработки более эффективных алгоритмов поиска низкостепенных аннигиляторов для функций, используемых в качестве фильтрующей, в том числе и для уравновешенных. Если при этом представлять функцию вектором значений или носителем, то экспоненциальной сложности избежать не удастся. Значит, нужно использовать другие представления функции, желательно именно те, которые фигурируют в описании анализируемых генераторов.

В той же работе [18] было введено понятие *алгебраической иммунности* булевой функции. Значение алгебраической иммунности $AI(f)$ булевой функции f равно минимальному значению числа d, для которого существует ненулевая булева функция g степени d такая, что $fg = 0$ или $(f+1)g = 0$. Значение алгебраической иммунности фильтрующей функции характеризует сложность применения метода алгебраических атак для анализа фильтрующего генератора.

Метод алгебраических атак использует представления аннигиляторов фильтрующей функции в виде многочленов Жегалкина. При больших значениях алгебраической иммунности ненулевой аннигилятор наименьшей степени может иметь многочлен Жегалкина с очень большим количеством мономов, а значит, вычисление этого аннигилятора является очень трудоёмкой алгоритмической задачей, даже если исходить только из размера ответа. С другой стороны, применение аннигилятора высокой степени в методе алгебраических

атак будет неоправданно сложным, даже если многочлен Жегалкина этого аннигилятора содержит мало мономов. То есть, неформально, отсутствие ненулевых аннигиляторов низкой степени у функций f и $f+1$ является показателем иммунности данного фильтрующего генератора к анализу методом алгебраических атак.

Как было отмечено выше, в случае большого значения алгебраической иммунности функции f достаточно найти лишь само значение $AI(f)$ либо как-то его оценить. В работах [12] и [18] было доказано, что для любой булевой функции f от n переменных имеет место оценка $AI(f) \leqslant \lceil n/2 \rceil$. В работах [18] и [14] было исследовано, распределение значения алгебраической иммунности на множестве уравновешенных функций. В частности в [14] доказано, что доля уравновешенных функций f от n переменных, для которых выполнены неравенства $\frac{n}{2} - \sqrt{\frac{n}{2}\ln n} \leqslant AI(f) \leqslant \frac{n+1}{2}$, стремится к единице при $n \to \infty$. То есть алгебраическая иммунность почти всех уравновешенных булевых функций от n переменных имеет асимптотический порядок $n/2$ — максимально возможный.

В 2005 и 2006 годах был опубликован ряд работ, [8], [13], [9], [7], в которых описываются конструкции классов булевых функций, имеющих максимальное значение алгебраической иммунности, равное $\lceil n/2 \rceil$. В [2] доказано, что для конструкций последовательностей функций, построенных в работах [5] и [2], имеет место нижняя оценка их алгебраической иммунности вида $\Omega(\sqrt{n})$.

Задачи вычисления значения алгебраической иммунности и построения классов булевых функций, имеющих общие оценки алгебраической иммунности, активно исследуются специалистами по дискретным функциям и связаны, в основном, с разработкой и анализом потоковых шифров.

В 2003 г. в работе [11] был предложен метод *быстрых алгебраических атак*, являющийся усовершенствованием метода алгебраических атак. Он в ряде случаев работает эффективнее и предполагает существование более общего вида тождеств низкой степени, связывающих значения фильтрующей функции f и значения её аргументов. Метод быстрых алгебраических атак был в дальнейшем улучшен в работах [6] и [17]. В работах [10] и [16] предложены алгоритмы поиска для фильтрующей функции f так называемых *статических соотношений*:

$$fg = h, \quad \deg g \leqslant e, \deg h \leqslant d.$$

для малых значений чисел $e < d$. Эти алгоритмы оперируют с табличными представлениями функций, и их сложность зависит линейно от 2^n. В связи с этим возникает задача более эффективного поиска подобных тождеств для других способов представления функций.

Цель диссертации. Первая цель работы состоит в разработке эффективных алгоритмов поиска ненулевых аннигиляторов (обнуляющих множителей) низкой степени для булевых функций. Алгоритмы должны работать с несколькими представлениями функций, подающихся на вход этих алгоритмов. Для каждого алгоритма должна быть получена оценка сложности.

Вторая цель диссертации состоит в разработке эффективных алгоритмов поиска для фильтрующей функции f тождеств низкой степени, обобщающих тождество $fg = 0$ и пригодных для использования в методе быстрых алгебраических атак.

Третьей целью работы является описание новых классов булевых функций, для которых могут быть получены оценки (как верхние, так и нижние) алгебраической иммунности.

Научная новизна. Результаты, полученные в диссертации, являются новыми. Основные из них состоят в следующем:

1. Исследована задача существования и нахождения аннигиляторов низкой степени для булевых функций. Для поиска аннигиляторов низкой степени разработаны алгоритмы, которые оперируют со следующими представлениями входной булевой функции: многочлен Жегалкина, ДНФ, трэйс представление ([4]), СФЭ и формула в базисе булевых операций конъюнкции, дизъюнкции и отрицания. Причём, для представления булевой функции в виде многочлена Жегалкина, ДНФ и трэйс представления разработанные алгоритмы вычисляют базис пространства аннигиляторов степени $\leqslant d$. Доказано, что такая же алгоритмическая задача для представления булевой функции в виде КНФ (а также формулы и СФЭ) является NP-трудной. Для представления в виде СФЭ получен рекурсивный алгоритм, который находит базис некоторого подпространства аннигиляторов степени $\leqslant d$. Для каждого алгоритма получена полиномиальная верхняя оценка сложности. Более того, все эти оценки зависят линейно от длины соответствующего представления булевой функции.

2. Для поиска тождеств низкой степени, которым удовлетворяет булева функция выхода фильтрующего генератора, разработаны полиномиальные алгоритмы, на вход которым булева функция подаётся в виде многочлена Жегалкина или трэйс представления.
3. Найдены некоторые классы булевых функций f, для которых получены асимптотики значения алгебраической иммунности $AI(f) \sim 2\sqrt{n}$ при числе переменных $n \to \infty$. Найденные классы задаются в виде параметрических семейств трэйс представлений.

Методы исследования. В диссертации используются методы линейной алгебры, комбинаторики, теории множеств, алгебры многочленов и конечных полей, а также асимптотические методы математического анализа.

Теоретическая и практическая ценность. Работа носит теоретический характер. В ней представлен широкий набор эффективных алгоритмов вычисления алгебраических характеристик булевых функций, таких как пространство низкостепенных аннигиляторов и алгебраическая иммунность. Результаты диссертации могут быть использованы для дальнейшего развития теории булевых функций, поиска связей между различными представлениями булевых функций, а также при разработке и криптографическом анализе потоковых шифров.

Апробация работы. Результаты диссертации докладывались на семинаре механико-математического факультета МГУ «Булевы функции в криптологии» под руководством О.А. Логачёва и Ю.В. Таранникова, на семинаре по теории кодирования Института проблем передачи информации РАН под руководством Л.А. Бассалыго, на 1-й и 2-й международных научных конференциях по проблемам безопасности и противодействия терроризму (2005, 2006, Москва), на VII международной конференции «Дискретные модели в теории управляющих систем» (2006, Покровское), на VI молодёжной научной школе по дискретной математике и её приложениям (2007, Москва), на IX международном семинаре «Дискретная математика и её приложения» (2007, Москва), на международной научной школе «Булевы функции в криптологии и информационной безопасности» (2007, Звенигород).

Публикации. Результаты диссертации опубликованы в 8 работах, две из которых — в рецензируемом журнале, входящем в список ВАК.

Структура и объём работы. Диссертация состоит из введения, трёх глав и списка литературы, включающего 53 наименования. Общий объём диссертации составляет 101 страницу.

КРАТКОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ.

Во **введении** даются основные определения, делается краткий обзор работ, связанных с темой диссертации. Излагаются основные результаты диссертации с указанием их дополняющего места в общей картине достижений в данной области исследования булевых функций. В конце введения приведён полный список основных результатов диссертации.

Глава 1 посвящена алгоритмическим вопросам поиска аннигиляторов булевых функций. Эта глава имеет трёхуровневую древовидную структуру разделов.

В **разделе 1.1** разработаны алгоритмы поиска аннигиляторов для различных способов представления булевых функций, подаваемых на вход этим алгоритмам.

Введём обозначения. $\mathbb{F}_2$ — поле из 2-х элементов. $\mathcal{F}_n$ — множество всех отображений $\mathbb{F}_2^n \to \mathbb{F}_2$ (множество всех булевых функций от n переменных). Для булевой функции $f \in \mathcal{F}_n$ введём обозначение для линейного пространства её аннигиляторов степени $\leqslant d$:

$$A_d(f) \coloneqq \{g \in \mathcal{F}_n \mid fg = 0, \deg g \leqslant d\}.$$

Введём обозначение для суммы биномиальных коэффициентов

$$S_n^d \coloneqq \sum\nolimits_{k=0}^{d} \binom{n}{k}.$$

Раздел 1.1.1 посвящён алгоритмам, работающим с представлением булевой функции в виде многочлена Жегалкина.

В **разделе 1.1.1.1** предложен алгоритм AM1 поиска базиса пространства $A_d(f)$. На вход алгоритму подаётся многочлен Жегалкина функции f. На выходе — многочлены Жегалкина базисных функций пространства $A_d(f)$. Оценка сложности алгоритма AM1 — $O(M_f (S_n^d)^3)$, где M_f — длина многочлена Жегалкина функции f (количество мономов). Алгоритм AM1 составляет и решает однородную систему линейных уравнений, задающей пространство $A_d(f)$. В **разделе 1.1.1.2** получен явный вид этой системы.

В **разделе 1.1.1.3** предложен алгоритм АМ1Б поиска базиса пространства

$$A_{d,e}(f) \coloneqq \{(g,h) \in \mathcal{F}_n^2 \mid fg = h, \deg g \leqslant e, \deg h \leqslant d\}.$$

Как отмечалось выше, тождества вида $fg = h$ при малых значениях степеней функций g и h используются в методе быстрых алгебраических атак. На вход алгоритму АМ1Б подаётся многочлен Жегалкина функции f. На выходе — пары многочленов Жегалкина базиса пространства $A_{d,e}(f)$. Сложность алгоритма АМ1Б имеет оценку $O(M_f(S_n^e)^3)$.

В **разделе 1.1.1.4** изложен приём, позволяющий для некоторых входных функций f существенно сократить вычисления. Результатом применения этого приёма к алгоритму АМ1 является алгоритм АМ12, который, однако, имеет такую же общую оценку сложности, что и алгоритм АМ1.

В **разделе 1.1.2** предложен алгоритм АД1, получающий на входе ДНФ функции f. Он вычисляет многочлены Жегалкина базисных функций пространства $A_d(f)$ за время $O(D_f(S_n^d)^3)$, где D_f — количество элементарных конъюнкций в ДНФ, задающей функцию f. Также доказана следующая теорема.

Теорема 1.14. *Для любых чисел $n, d \in \mathbb{Z}$ таких, что $0 \leqslant d \leqslant n$, задача вычисления базиса линейного пространства $A_d(f)$ для функции f, заданной в виде КНФ, является NP-трудной.*

В **разделе 1.1.3.1** предложены алгоритмы АФ1 и АС1, которые соответственно по формуле и схеме из функциональных элементов в базисе операций $\{\neg, \&, \vee\}$ находят многочлены Жегалкина базисов пары пространств $G \subset A_d(f+1)$, $H \subset A_d(f)$. Однако, при этом пространства G и H могут оказаться тривиальными, в то время, как пространства $A_d(f)$ и $A_d(f+1)$ могут содержать ненулевые функции. Аналогично теореме **1.14** доказывается, что задача вычисления базиса линейного пространства $A_d(f)$ для функции f, заданной в виде формулы или СФЭ в базисе операций $\{\neg, \&, \vee\}$, является *NP*-трудной. Сложность алгоритмов АФ1 и АС1 — $O(C_f(S_n^d)^3)$, где C_f — длина формулы или размер СФЭ, задающей функцию f.

В **разделе 1.1.3.2** доказаны следующие две теоремы о пространствах аффинных аннигиляторов произведения булевых функций.

Теорема 1.16. *Пусть* $f_1, f_2 \in \mathcal{F}_n$ *— ненулевые функции степени* $\leqslant 1$ *(аффинные), причём* $f_1 \neq f_2$ *и* $f_1 \neq f_2 + 1$. *Тогда пространство* $A_1(f_1 \cdot f_2)$ *представимо в виде прямой суммы*

$$A_1(f_1 \cdot f_2) = A_1(f_1) \oplus A_1(f_2).$$

Теорема 1.17. *Пусть* $f_1, f_2 \in \mathcal{F}_n \setminus 0$. *Первые* m *переменных фиктивны для функции* f_2, *а остальные переменные фиктивны для функции* f_1. *Тогда пространство* $A_1(f_1 \cdot f_2)$ *представимо в виде прямой суммы*

$$A_1(f_1 \cdot f_2) = A_1(f_1) \oplus A_1(f_2).$$

В **разделе 1.1.3.3** доказана следующая теорема про структуру пространства $A_d(f)$ для функции f, имеющей фиктивные переменные.

Теорема 1.18. *Пусть для некоторого* $k : k \leqslant n$ *переменные* x_i $(k \leqslant i \leqslant n)$ *фиктивны для ненулевой функции* $f \in \mathcal{F}_n$. *Для каждого* $m \in \{k-1, \ldots, n\}$ *рассмотрим функцию* $f_m \in \mathcal{F}_m$, *положив* $f_m(x_1, \ldots, x_m) \coloneqq f(x_1, \ldots, x_m, \underbrace{0, \ldots, 0}_{n-m})$. *В частности,* $f = f_n$. *Мы будем подразумевать вложения* $A_i(f_m) \subset \mathcal{F}_m \subset \mathcal{F}_n$. *Под произведением* $A_i(f_{m-1}) \cdot x_m$ *будем понимать множество произведений каждой функции из* $A_i(f_{m-1})$ *на «селекторную» функцию* $\left[(x_1, \ldots, x_m) \mapsto x_m\right]$. *В указанных обозначениях пространство* $A_d(f)$ *представимо в виде следующей прямой суммы линейных пространств:*

$$A_d(f) = \bigoplus_{\substack{u=(u_k,\ldots,u_n)\in\mathbb{F}_2^{n-k+1}: \\ \mathrm{wt}(u)<d}} A_{d-\mathrm{wt}(u)}(f_{k-1}) \cdot \underbrace{x_k^{u_k} \cdot \ldots \cdot x_n^{u_n}}_{n-k+1},$$

где $\mathrm{wt}(u)$ *— количество единиц в векторе* $u \in \mathbb{F}_2^{n-k+1}$, *а* $x_i^1 = x_i$, $x_i^0 = 1$.

Раздел 1.1.4 посвящён алгоритмам, работающим с трэйс представлением булевой функции. Поле Галуа $GF(2^n)$ из 2^n элементов является линейным пространством над полем $\mathbb{F}_2$. Зафиксируем произвольный изоморфизм $\varphi : GF(2^n) \to \mathbb{F}_2^n$ линейных пространств над полем $\mathbb{F}_2$. φ задаёт также отождествление функционального пространства $\mathcal{F}_n$ с пространством функций $GF(2^n) \to \mathbb{F}_2$. Функции $f \in \mathcal{F}_n$ взаимно однозначно соответствует функция $f \circ \varphi : GF(2^n) \to \mathbb{F}_2$.

Трэйс представление функции $f : GF(2^n) \to \mathbb{F}_2$ задаётся формулой следующего вида

$$f(x) = \sum_{s=0}^{2^n-1} Tr_n(a_s \cdot x^s), \quad Tr_n(x) = \sum_{k=0}^{n-1} x^{2^k}, \quad a_s \in GF(2^n).$$

Любую функцию $f : GF(2^n) \to GF(2^n)$ можно представить единственным (интерполяционным) многочленом степени $\leqslant 2^n - 1$ с коэффициентами из поля $GF(2^n)$. Тот факт, что эта функция f принимает только значения из подполя $\mathbb{F}_2 \subset GF(2^n)$, задаёт некоторое условие на коэффициенты интерполяционного многочлена. Фактически, такой многочлен также является трэйс представлением функции $f : GF(2^n) \to \mathbb{F}_2$.

В **разделе 1.1.4.1** разработан алгоритм АТ1, на вход которому подаётся трэйс представление булевой функции f. Этот алгоритм вычисляет трэйс представления базисных функций пространства $A_d(f)$ за время $O(T_f(nS_n^d)^3)$, где T_f — длина трэйс представления функции f — количество ненулевых коэффициентов интерполяционного многочлена.

В **разделе 1.1.4.2** предложен алгоритм АТ1Б поиска базиса пространства $A_{d,e}(f)$. На вход алгоритму АТ1Б подаётся трэйс представление функции f. На выходе — пары трэйс представлений базиса пространства $A_{d,e}(f)$. Сложность алгоритма АТ1Б имеет оценку $O(T_f(nS_n^e)^3)$.

В **разделе 1.1.4.3** разработан алгоритм АТК1, вычисляющий значение $AI(f)$ для функции $f \in \mathcal{F}_n$, заданной трэйс представлением. Алгоритм АТК1 представляет собой итерационный процесс. Сложность каждой итерации есть $O(n^2 T_f S_n^d \log(n T_f S_n^d))$, где T_f — длина трэйс представления функции f, а $d = AI(f)$. Чем короче трэйс представление функции f, тем меньше итераций потребуется совершить алгоритму АТК1.

В **разделе 1.1.4.4** проведён анализ фильтрующего генератора WG, который был представлен в 2005 г. на конкурсе потоковых шифров eSTREAM в Интернете, [19]. Десятки учёных, занимающихся анализом потоковых шифров, публиковали на сайте конкурса свои статьи, в которых они анализировали ту или иную систему шифрования, представленную на этом конкурсе. Было доказано, что генератор

WG обладает рядом хороших характеристик, но про значение алгебраической иммунности фильтрующей функции $f_{WG} \in \mathcal{F}_{29}$ авторами генератора высказывались только предположения и приводились некоторые оценки. Функция f_{WG} задана трэйс представлением, длина которого равна $T_{f_{WG}} = 5 \cdot 29 = 145$. С помощью алгоритма АТК1 удалось вычислить значение $AI(f_{WG}) = \deg f_{WG} = 11$. Алгоритм совершил 6 итераций. На вычислительной машине с процессором IBM Power4 1,3 ГГц программе понадобилось около 2 ГБ оперативной памяти. Время работы программы составило 250 секунд (≈ 4 минуты).

В **разделе 1.1.5** показано, что дают алгоритмы АМ1 и АТ1 для частично определённых функций $f : \mathbb{F}_2^n \setminus 0 \to \mathbb{F}_2$ выхода фильтрующего генератора. Для таких функций расширяется понятие аннигилятора: функция $g \in \mathcal{F}_n$ является аннигилятором функции f, если $f(x)g(x) = 0$ для любого ненулевого вектора x. В соответствии с этим определяется линейное пространство аннигиляторов степени $\leqslant d$:

$$A_d^*(f) \coloneqq \{g \in \mathcal{F}_n \mid \deg g \leqslant d, \;\; f(x)g(x) = 0 \;\; \forall x \in \mathbb{F}_2^n \setminus 0\} \supset A_d(f).$$

Получены некоторые достаточные условия равенства пространств $A_d^*(f) = A_d(f)$. Причём эти условия легко вычислимы в процессе выполнения алгоритмов АМ1 и АТ1. В частности, доказаны следующие утверждения.

Следствие 1.28. *Пусть M_f — количество мономов в многочлене Жегалкина функции $f \in \mathcal{F}_n$, и пусть имеет место неравенство $M_f S_n^d < 2^n$. Тогда $A_d^*(f) = A_d(f)$.*

Следствие 1.30. *$A_d^*(f) = A_d(f)$ для любой функции $f \in \mathcal{F}_n$ и любого числа $d < n - \deg f$.*

Среди алгоритмов получения оценок алгебраической иммунности булевых функций мы выделим класс алгоритмов, которые предназначены для проверки тривиальности пространства $A_d(f)$. Коротко будем называть их *алгоритмами проверки*. Эти алгоритмы выдают один из двух ответов: «$A_d(f) = 0$» или «неопределённость». Причём первый ответ выдаётся только в тех случаях, когда вычисления, проделанные алгоритмом проверки, доказывают тривиальность пространства $A_d(f)$. В случаях, когда не удаётся это доказать, выдаётся второй ответ. Преимущество такого класса алгоритмов над описан-

ными выше алгоритмами вычисления базиса пространства $A_d(f)$ заключается в том, что сложность алгоритмов проверки гораздо меньше. Недостатки же очевидны. Если $A_d(f) \neq 0$, то алгоритм проверки обязательно выдаст ответ «неопределённость» и не найдёт ни одного ненулевого аннигилятора. Более того, не всегда, когда пространство $A_d(f)$ тривиально, алгоритм проверки может вычислительно это доказать. Доля тех функций, для которых выдаётся первый ответ, характеризует *качество алгоритма проверки*.

Алгоритм 1 из [15], предложенный в 2006 г., также относится к классу алгоритмов проверки тривиальности пространства $A_d(f)$ для табличного представления функции $f \in \mathcal{F}_n$. Про этот детерминированный алгоритм была доказана следующая теорема.

Теорема ([15], Theorem 2). *Пусть случайная величина F_n равномерно распределена на множестве всех уравновешенных булевых функций от n переменных. Тогда математическое ожидание времени работы алгоритма 1 для входной функции F_n можно оценить $O(n^d)$, а вероятность того, что на выходе будет ответ «неопределённость» оценивается $O(e^{-2^d n(1+o(1))})$. В указанных оценках d считается константой, а асимптотика рассматривается при $n \to \infty$.*

В **разделе 1.2** предложены алгоритмы проверки АМ2 и АД2, являющиеся модификациями алгоритма 1 из [15] для представления входной функции в виде многочлена Жегалкина и в виде ДНФ соответственно. Сложность этих двух алгоритмов есть $O(M \cdot n^d)$ при $M, n \to \infty$, где M — количество мономов в многочлене Жегалкина (для алгоритма АМ2) или количество элементарных конъюнкций в ДНФ (для алгоритма АД2). Причём, в отличие от оценки сложности алгоритма 1 из [15] оценка сложности алгоритмов АМ2 и АД2 имеет место для каждой входной функции, размер представления которой равен M. Алгоритмы АМ2, АД2 и алгоритм 1 из [15] устроены так, что получая на вход соответствующие представления одной и той же булевой функции все 3 алгоритма выдают одинаковые ответы. Это значит, что доля уравновешенных функций из $\mathcal{F}_n$, для которых алгоритмы АМ2 и АД2 выдают ответ «неопределённость», также, как и для алгоритма 1 из [15], оценивается $O(e^{-2^d n(1+o(1))})$.

Глава 2 посвящена получению верхних и нижних оценок алгебраической иммунности некоторых классов булевых функций, заданных в виде трэйс представления.

В **разделе 2.1** доказаны следующие ключевые утверждения.

Следствие 2.9. $\forall n \geqslant 5, \forall a \in GF(2^n) \setminus 0$, *для функции* $f(x) = Tr_n(a \cdot x^{-1})$ *имеет место оценка* $AI(f) \geqslant \left\lfloor 2\sqrt{n+4} \right\rfloor - 4$.

Следствие 2.11. *В работе [20] было доказано, что* $AI(Tr_n(x^{-1})) \leqslant \lfloor \sqrt{n} \rfloor + \left\lceil n / \lfloor \sqrt{n} \rfloor \right\rceil - 2$ *для любого* $n \geqslant 2$. *Объединяя этот результат со следствием* ***2.9****, получаем асимптотику алгебраической иммунности следа от инверсии:* $AI(Tr_n(x^{-1})) \sim 2\sqrt{n}$ *при* $n \to \infty$.

В **разделах 2.2** и **2.3** дальше развивается техника получения нижних и верхних оценок алгебраической иммунности. Доказаны следующие 4 теоремы.

Теорема 2.12. $\forall k \in \mathbb{N} \ \ \exists n_0 : \ \forall n \geqslant n_0, \ \forall \alpha_1, \ldots, \alpha_{k-1} \in \{0,1\} \subset \mathbb{Z}$, $\forall a \in GF(2^n) \setminus 0$, *для числа* $m = 2^n - 2^{k+1} + \sum_{i=1}^{k-1} \alpha_i \cdot 2^i$, *для функции* $f(x) = Tr_n(a \cdot x^m)$ *имеет место оценка*

$$AI(f) \geqslant \min\left\{ \left\lfloor \frac{n}{k + \overline{l}\,(m) + 4} \right\rfloor, \left\lfloor 2\sqrt{n+k+5} \right\rfloor - k - 6 \right\} + 1,$$

где $\overline{l}\,(m)$ *— максимальное число последовательно стоящих единиц в наборе из* k *чисел:* $1, \alpha_1, \ldots, \alpha_{k-1}$.

Теорема 2.20. $\forall k \in \mathbb{N} \ \ \exists n_0 : \forall n \geqslant n_0$, *для любых различных чисел* $m_1, \ldots, m_M \in \mathbb{N}$, *которые удовлетворяют предикату*

$$\forall r \in \{1, \ldots, M\} \ \exists \alpha_{r,1}, \ldots, \alpha_{r,k} \in \{0,1\} : m_r = 2^n - 2^{k+1} + \sum_{i=1}^{k} \alpha_{r,i} \cdot 2^i,$$

для любых $a_1, \ldots, a_M \in GF(2^n) \setminus 0$, *для любой функции* $h \in \mathcal{F}_n : \deg h \leqslant k$, *для произвольного изоморфизма* $\varphi : GF(2^n) \to \mathbb{F}_2^n$, *для функции* $f : GF(2^n) \to \mathbb{F}_2$, *заданной формулой* $f(x) = \sum_{r=1}^{M} Tr_n(a_r \cdot x^{m_r}) + h \circ \varphi(x)$, *имеет место оценка*

$$AI(f) \geqslant \min\left\{ \left\lfloor \frac{n}{2k+4} \right\rfloor, \left\lfloor 2\sqrt{n+k+5} \right\rfloor - k - 6 \right\} + 1.$$

Теорема 2.24. *Для каждой пары чисел* (n,k) *и для каждой функции* $f : GF(2^n) \to \mathbb{F}_2$ *из условия теоремы* **2.12** *имеет место оценка*

$$AI(f) \leqslant \lfloor \sqrt{n} \rfloor + \left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil + \sum_{i=1}^{k-1} \alpha_i - 1.$$

Теорема 2.25. *Для каждой пары чисел* (n,k) *и для каждой функции* $f : GF(2^n) \to \mathbb{F}_2$ *из условия теоремы* **2.20** *имеет место оценка*

$$AI(f) \leqslant \lfloor \sqrt{n} \rfloor + \left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil + k - 2.$$

Из этих 4-х теорем следует, что для всех рассмотренных в них последовательностей классов функций имеет место асимптотика значения алгебраической иммунности: $AI(f) \sim 2\sqrt{n}$ при $n \to \infty$. k при этом считается константой.

Глава 3 посвящена систематическому подходу к поиску низкостепенных тождеств, которым удовлетворяет фильтрующая функция и которые могут быть использованы в методе быстрых алгебраических атак при анализе фильтрующих генераторов, [11].

В **разделе 3.1** даны необходимые определения и приведены вспомогательные утверждения.

Для фильтрующего генератора с функцией выхода $f \in \mathcal{F}_n$ изоморфизм $\varphi : GF(2^n) \to \mathbb{F}_2^n$ называется *специальным*, если выходная последовательность этого генератора представляется в виде $\{f \circ \varphi(a^k s)\}_{k \in \mathbb{N}}$, где $a \in GF(2^n)$ — некоторый элемент, а $s \in GF(2^n)$ — начальное состояние генератора.

Для фиксированной функции $f \in \mathcal{F}_n$ и фиксированных чисел N, d, e, r множество всех тождеств следующего вида

$$h(x) = \sum_{\substack{u=(u_0,\ldots,u_N) \in \mathbb{F}_2^{N+1} \setminus 0: \\ \mathrm{wt}(u) \leqslant r}} g_u(x) \cdot \prod_{i=0}^{N} \Big(f \circ \varphi(a^i x) \Big)^{u_i}, \quad \forall x \in GF(2^n),$$

$$\deg(h \circ \varphi^{-1}) \leqslant d, \quad \deg(g_u \circ \varphi^{-1}) \leqslant e \quad \forall u,$$

образует линейное пространство $R_{N,d,e,r}(f)$ над полем $\mathbb{F}_2$. При малых значениях чисел N, d, e, r такие тождества, называемые *динамическими соотношениями*, также могут быть эффективно использованы в методе быстрых алгебраических атак. Нетрудно видеть, что динами-

ческие соотношения являются обобщением статических соотношений и в отличие от статических соотношений используют несколько последовательных значений выходной последовательности генератора, а именно $N+1$ значение.

В **разделе 3.2** разработан алгоритм БААТ1, вычисляющий базис линейного пространства $R_{N,d,e,r}(f)$ для фильтрующей функции $f \in \mathcal{F}_n$. На входе этот алгоритм получает числа N, d, e, r и трэйс представление функции $f \circ \varphi$, где φ — специальный изоморфизм фильтрующего генератора. На выходе — список трэйс представлений базисных наборов функций $(h, g_u \mid \mathrm{wt}(u) \leqslant r)$. Время работы алгоритма БААТ1 ограничивается сверху некоторым многочленом от следующих трёх параметров: длины трэйс представления функции f и чисел n, N. При этом числа d, e, r считаются константами, от них зависит степень многочлена, ограничивающего время работы алгоритма БААТ1.

Частным случаем динамических соотношений являются *нелинейные рекуррентные соотношения* на выходную последовательность $\{f \circ \varphi(a^k s)\}_{k \in \mathbb{N}}$ фильтрующего генератора:

$$f \circ \varphi(a^N x) = \tilde{g}(f \circ \varphi(a^0 x), \ldots, f \circ \varphi(a^{N-1} x)), \ \ \forall x \in GF(2^n), \deg \tilde{g} \leqslant r.$$

Множество $R_{N,r}(f)$ функций $\tilde{g} \in \mathcal{F}_n$, удовлетворяющих этому тождеству (в случае, если $R_{N,r}(f)$ не пусто) соответствует аффинному подпространству в линейном пространстве $R_{N,0,0,r}(f)$.

В **разделе 3.3** предложена модификация алгоритма БААТ1 — алгоритм РТ1, вычисляющий рекуррентные соотношения степени r. На вход алгоритму РТ1 подаётся то же, что и алгоритму БААТ1. На выходе — многочлены Жегалкина функций, порождающих аффинное пространство $R_{N,r}(f)$. Время работы алгоритма РТ1 также ограничивается сверху некоторым многочленом от длины трэйс представления функции f и чисел n, N. При этом r считается константой, от которой зависит степень ограничивающего многочлена.

СПИСОК ЛИТЕРАТУРЫ

[1] Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В.: *Основы криптографии*. М.: издательство «Гелиос АРВ», 2001 г.

[2] Ботев А.А.: *О свойствах корреляционно-иммунных функций с высокой нелинейностью*, дис. канд. физ.-мат. наук, МГУ им. М.В. Ломоносова, мех.-мат. фак. М., 2005

[3] Кудрявцев В.Б., Алёшин С. В., Подколзин А. С.: *Введение в теорию автоматов*. — М.: Наука, 1985.

[4] Логачёв О. А., Сальников А. А., Ященко В. В.: *Булевы функции в теории кодирования и криптологии* — М.: МЦНМО, 2004.

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

[6] Armknecht F.: *Improving Fast Algebraic Attacks*, Fast Software Encryption 2004, LNCS 3017, pp. 65–82, Springer, 2004

[7] Armknecht F., Krause M.: *Constructing Single- and Multi-output Boolean Functions with Maximal Algebraic Immunity*, International Conference on Automata, Languages and Programming, ICALP 2006, Part II, LNCS 4052, pp. 180–191, Springer, 2006.

[8] Braeken A., Preneel B.: *On the Algebraic Immunity of Symmetric Boolean Functions*, Indocrypt 2005, LNCS 3797, pp. 35–48, Springer 2005.

[9] Carlet C.: *A method of construction of balanced functions with optimum algebraic immunity*, Cryptology ePrint Archive, http://eprint.iacr.org/2006/149

[10] Courtois N.: *Cryptanalysis of SFINKS*. Information Security and Cryptology, ICISC 2005, LNCS 3935, pp. 261–269, Springer, 2005.

[11] Courtois N.: *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback*, Crypto 2003, LNCS 2729, pp. 177–194, Springer, 2003

[12] Courtois N., Meier W.: *Algebraic Attacks on Stream Ciphers with Linear Feedback*, Eurocrypt 2003, LNCS 2656, pp. 345–359, Springer, 2003

[13] Dalai D.K., Maitra S.: *Balanced Boolean Functions with (more than) Maximum Algebraic Immunity*, Cryptology ePrint Archive: Report 2006/434, http://eprint.iacr.org/2006/434

[14] Didier F.: *A new bound on the block error probability after decoding over the erasure channel.*, IEEE Trans. on Information Theory, vol. IT-52, No. 10, 2006.

[15] Didier F., Tillich J.-P.: *Computing the Algebraic Immunity Efficiently*, Fast Software Encryption 2006, LNCS 4047, pp. 359–374, Springer, 2006.

[16] Gong G.: *On Existence and Invariant of Algebraic Attacks*, CACR online archive, Technical report 2004-17, 2004.
http://www.cacr.math.uwaterloo.ca/techreports/2004/corr2004-17.pdf

[17] Hawkes P., Rose G.: *Rewriting Variables: the Complexity of Fast Algebraic Attacks on Stream Ciphers*, Crypto 2004, LNCS 3152, pp. 390-406, Springer, 2004

[18] Meier W., Pasalic E., Carlet C.: *Algebraic Attacks and Decomposition of Boolean Functions*, Eurocrypt 2004, LNCS 3027, pp. 474–491, Springer, 2004

[19] Nawaz Y., Gong G.: *The WG Stream Cipher*, eSTREAM, ECRYPT Stream Cipher Project, Report 2005/033, 2005. http://www.ecrypt.eu.org/stream/

[20] Nawaz Y., Gong G., Gupta K.C.: *Upper Bounds on Algebraic Immunity of Boolean Power Functions*, Fast Software Encryption 2006, LNCS 4047, pp. 375–389, Springer, 2006.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ.

[21] Баев В.В.: *Алгебраическая иммунность фильтрующей функции генератора WG*, Материалы IX Международного семинара «Дискретная математика и её приложения». (Москва, МГУ, 18–23 июня 2007 г.) / Под редакцией О.М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2007. стр. 418–420.

[22] Баев В.В.: *Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими трэйс формами*, Дискретные модели в теории управляющих систем: VII Международная конференция, Покровское, 4–6 марта 2006 г.: Труды. — М.: МАКС Пресс, 2006. стр. 25–29.

[23] Баев В.В.: *О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций*, ж. Дискретная математика, том 18, выпуск 3, 2006. стр. 138–151.

[24] Баев В.В.: *О сложности поиска аннигиляторов низкой степени для булевых функций*, Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2–3 ноября 2005 г. — М: МЦНМО, 2006. стр. 198–204.

[25] Баев В.В.: *Рекуррентные соотношения на выходную последовательность фильтрующего генератора и их обобщения*, Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М.В. Ломоносова, 25–26 октября 2006 г. — М: МЦНМО, 2007. стр. 249–254.

[26] Баев В.В.: *Структура пространства аннигиляторов для булевых функций с фиктивными переменными*, Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М.В. Ломоносова, 25–26 октября 2006 г. — М: МЦНМО, 2007. стр. 255–258.

[27] Баев В.В.: *Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина*, ж. Дискретная математика, том 19, выпуск 4, 2007. стр. 132–138.

[28] Баев В.В.: *Эффективная проверка нижней границы алгебраической иммунности многочлена Жегалкина и ДНФ*, Материалы VI молодёжной научной школы по дискретной математике и её приложениям (Москва, 16–21 апреля 2007 г.). Часть I. Под редакцией А.В. Чашкина. 2007. стр. 8–12.