МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

ОТ КРИПТОАНАЛИЗА ШИФРА К КРИПТОГРАФИЧЕСКОМУ СВОЙСТВУ БУЛЕВОЙ ФУНКЦИИ[1]

А. А. Городилова

Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

Настоящий обзор посвящён описанию основных криптографических свойств булевых функций, таких, как высокая алгебраическая степень, уравновешенность и совершенная уравновешенность, лавинные характеристики, отсутствие линейных структур, корреляционная иммунность и устойчивость, высокая нелинейность, статистическая независимость, алгебраическая иммунность, уровень аффинности и k-нормальность, дифференциальная равномерность, разложимость в сумму специальных функций, мультипликативная сложность, высокие мощности линеаризационных множеств. Исследуются вопросы формирования данных свойств на основе атак на блочные и поточные шифры, использующих определённые уязвимости булевых функций, являющихся компонентами шифров; приводятся основные идеи данных атак. Кратко рассмотрены базовые теоретические результаты, полученные для каждого из свойств, и сформулированы открытые проблемы в данной области.

Ключевые слова: *булева функция, поточный шифр, блочный шифр, алгебраическая степень, уравновешенность, совершенная уравновешенность, лавинные характеристики, линейная структура, корреляционная иммунность, устойчивость, нелинейность, статистическая независимость, алгебраическая иммунность, уровень аффинности, k-нормальность, дифференциальная равномерность, пороговое разбиение, мультипликативная сложность, линеаризационное множество, линейная сложность, корреляционный криптоанализ, быстрая корреляционная атака, линейный криптоанализ, статистический аналог, алгебраический криптоанализ, дифференциальный криптоанализ, атаки по сторонним каналам, линеаризационная атака.*

DOI 10.17223/20710410/33/2

FROM CRYPTANALYSIS TO CRYPTOGRAPHIC PROPERTY OF A BOOLEAN FUNCTION

A. A. Gorodilova

Sobolev Institute of Mathematics, Novosibirsk, Russia

E-mail: gorodilova@math.nsc.ru

The survey is devoted to description of basic, but not all, cryptographic properties of Boolean functions: algebraic degree, balancedness and perfect balancedness, avalanche

[1]Работа поддержана грантом РФФИ № 15-07-01328.

characteristics, non-existence of linear structures, correlation immunity and resiliency, high nonlinearity, statistical independence, algebraic immunity, affinity level and k-normality, differential uniformity, threshold implementation, multiplicative complexity, high cardinality of linearization sets. The questions about these properties formation are studied based on the attacks on stream and block ciphers that exploit the vulnerabilities of Boolean functions used in ciphers as components. The ideas of such attacks are given. We briefly describe the basic theoretical results obtained for each of the properties and formulate open problems in this area.

Keywords: *Boolean function, stream cipher, block cipher, algebraic degree, balancedness, perfect balancedness, avalanche characteristics, linear structure, correlation immunity, resiliency, nonlinearity, statistical independence, algebraic immunity, affinity level, k-normality, differential uniformity, threshold implementation, multiplicative complexity, linearization set, linear complexity, correlation attack, fast correlation attack, linear cryptanalysis, statistical analogue, differential cryptanalysis, side-channel attacks, linearization attack.*

Введение

На протяжении полувека сформировалось достаточно много требований к булевым функциям, использующимся в системах шифрования. Функции, удовлетворяющие данным требованиям, стали называть «криптографическими булевыми функциями».

Основная задача работы — привести исходные связи между различными методами криптоанализа шифров и математическими требованиями, которые накладываются на булевы функции, используемые в этих шифрах, для противодействия этим атакам. Таблица отражает основное содержание настоящей работы. Для более основательного знакомства с теоретическими результатами в области различных криптографических свойств можно рекомендовать работы О. А. Логачева, А. А. Сальникова, С. В. Смышляева, В. В. Ященко [11], Г. П. Агибалова [1], И. А. Панкратовой [14], Ю. В. Таранникова [19], Н. Н. Токаревой [42], C. Carlet [24, 25], T. W. Cusick, P. Stanica [30], A. Braeken [23].

Рассматриваемые криптографические свойства и их назначение

№ п/п	Свойство	Цель
1	Высокая алгебраическая степень	Повышение линейной сложности генерируемой последовательности; повышение степени системы нелинейных уравнений, описывающих шифр
2	Уравновешенность	Улучшение статистических свойств последовательностей, вырабатываемых поточными генераторами
3	Совершенная уравновешенность	
4	Лавинные характеристики	Обеспечение изменения значений большого числа выходных переменных при изменении значений малого числа входных переменных
5	Отсутствие линейных структур	Улучшение нелинейных свойств функций
6	Корреляционная иммунность, устойчивость	Препятствие проведению корреляционной атаки на поточные шифры
7	Высокая нелинейность	Препятствие проведению быстрой корреляционной атаки на поточные шифры и линейного криптоанализа блочных шифров
8	Статистическая независимость	Препятствие проведению статистических методов криптоанализа шифров

Окончание таблицы

№ п/п	Свойство	Цель
9	Алгебраическая иммунность	Препятствие проведению алгебраического криптоанализа шифров
10	Уровень аффинности и k-нормальность	Препятствие методу линеаризации без введения новых переменных для решения булевых уравнений
11	Дифференциальная равномерность	Препятствие проведению дифференциального криптоанализа блочных шифров
12	Разложимость в сумму специальных функций	Маскирование данных с целью защиты от атак по сторонним каналам
13	Мультипликативная сложность	Минимизация размера и стоимости аппаратной реализации криптоалгоритмов
14	Высокие мощности линеаризационных множеств	Препятствие линеаризационной атаке

1. Основные определения и обозначения

1.1. Булевы функции

Введём обозначения: n — натуральное число; $\mathbb{F}_2$ — множество, состоящее из 0 и 1; $x = (x_1, \ldots, x_n)$ — двоичный вектор с координатами из $\mathbb{F}_2$; $\mathbb{F}_2^n$ — множество всех двоичных векторов длины n; $\mathbf{0} = (0, \ldots, 0)$ — нулевой вектор; $\oplus$ — сложение по модулю 2.

Весом Хэмминга $\mathrm{wt}(x)$ двоичного вектора x называется количество единиц, содержащихся в x: $\mathrm{wt}(x) = \sum\limits_{i=1}^{n} x_i$. *Расстоянием Хэмминга* $\mathrm{d}(x, y)$ между двумя векторами x, y называется число позиций, в которых они различаются, или, что эквивалентно, $\mathrm{d}(x, y) = \mathrm{wt}(x \oplus y)$. *Скалярное произведение* $\langle x, y\rangle$ двоичных векторов x, y определяется как $\langle x, y\rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n$.

Векторной булевой функцией ((n, m)-функцией) F называется произвольное отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. В случае $m = 1$ говорят, что F — *булева функция* от n переменных. Можно рассматривать (n, m)-функцию как набор из m координатных булевых функций от n переменных: $F = (f_1, \ldots, f_m)$. *Компонентной функцией* называется любая ненулевая линейная комбинация координатных функций, т. е. булева функция $\langle b, F\rangle$, где $b \in \mathbb{F}_2^m$, $b \neq \mathbf{0}$.

Вес функции $\mathrm{wt}(f)$ равен мощности её носителя $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. *Расстоянием Хэмминга* $\mathrm{d}(f, g)$ между булевыми функциями f и g является расстояние Хэмминга между векторами их значений: $\mathrm{d}(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$. Пусть $\mathcal{M}_n$ — некоторое множество булевых функций от n переменных. Расстояние от функции g до множества функций $\mathcal{M}_n$ определяется как $\mathrm{d}(g, \mathcal{M}_n) = \min\{d(f, g) : f \in \mathcal{M}_n\}$. Для любой булевой функции f *производная по направлению* a, где $a \in \mathbb{F}_2^n$, определяется следующим образом: $D_a f(x) = f(x) \oplus f(x \oplus a)$.

Любую (n, m)-функцию можно единственным образом записать в виде *полинома Жегалкина*, или *алгебраической нормальной формы* (АНФ): $F(x_1, \ldots, x_n) = \bigoplus\limits_{k=0}^{n} \bigoplus\limits_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} x_{i_1} \ldots x_{i_k} \oplus a_0$, где $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $a_{i_1, \ldots, i_k} \in \mathbb{F}_2^m$.

Алгебраической степенью $\deg(F)$ функции F называется количество переменных в самом длинном слагаемом АНФ, при котором коэффициент не равен нулевому вектору. Функция степени не выше 1 называется *аффинной*. В случае $a_0 = \mathbf{0}$ функция *линейна*.

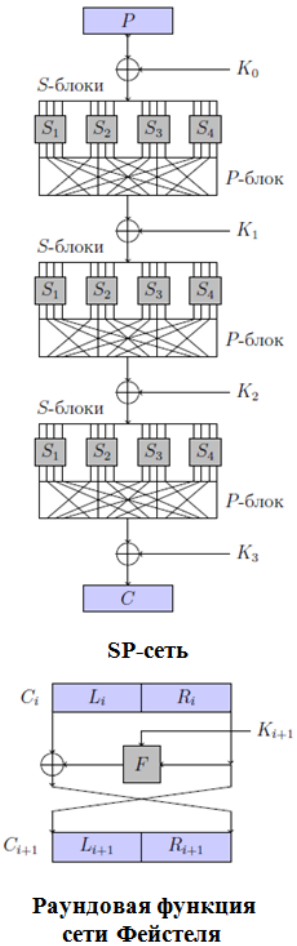
Для каждого $y \in \mathbb{F}_2^n$ *коэффициентом Уолша — Адамара* $W_f(y)$ булевой функции f от n переменных называется величина, определяемая равенством $W_f(y) =$

$= \sum\limits_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle x,y\rangle}$. Набор коэффициентов $W_f(y)$ по всем $y\in\mathbb{F}_2^n$ называется *спектром Уолша — Адамара* булевой функции f. Справедливо *равенство Парсеваля*: $\sum\limits_{y\in\mathbb{F}_2^n} W_f^2(y) = 2^{2n}$. Спектр Уолша — Адамара векторной функции состоит из всех коэффициентов Уолша — Адамара всех её компонентных булевых функций: $W_F(u,v) = \sum\limits_{x\in\mathbb{F}_2^n} (-1)^{\langle v,F(x)\rangle\oplus\langle u,x\rangle}$.

1.2. Блочные шифры

Блочный шифр преобразует блок открытого текста (сообщения) длины N в блок шифртекста также длины N с использованием некоторого секретного ключа. Процесс шифрования состоит из нескольких повторяющихся раундов, определяющихся, как правило, одинаковой раундовой функцией, зависящей от раундового подключа K_i, вырабатываемого по специальному правилу из исходного ключа K.

Наиболее распространённые типы блочных шифров, *SP-сеть* и *сеть Фейстеля*, схематично приведены на рис. 1 [20]. Обе эти схемы отражают в себе два принципа построения шифрующих преобразований, которые определил в своей работе Клод Шеннон, — *рассеивание* и *перемешивание*. Приведём объяснение этих принципов по работе [5]: «Качественно можно сказать, что перемешивание усложняет восстановление взаимосвязи статистических и аналитических свойств открытого и шифрованного текстов, а рассеивание распространяет влияние одного знака открытого текста на большое число знаков шифртекста, что позволяет сгладить влияние статистических свойств открытого текста на свойства шифртекста». На примере SP-сети хорошо видно, что P-блок обеспечивает рассеивание, а набор небольших S-блоков — перемешивание. В то время как в качестве P-блока обычно выбирается линейная функция, S-блоки составляют нелинейные преобразования шифра.



SP-сеть

Раундовая функция сети Фейстеля

Рис. 1

По сути, S-блок — это векторная (n,m)-функция, причём значения n и m небольшие, например 4, 6, 8 битов. Несмотря на столь небольшой размер, найти такой S-блок с «хорошими» криптографическими свойствами достаточно трудно. Для наглядности заметим, что всевозможных отображений из $\mathbb{F}_2^8$ в себя существует 2^{2048}, что в настоящее время не поддаётся полному перебору! При этом даже аналитические рассуждения пока не могут привести к ответу на некоторые важные для криптографических приложений вопросы. Например, не известно, существуют ли взаимно однозначные почти совершенно нелинейные отображения из $\mathbb{F}_2^n$ в себя при чётных $n \geqslant 8$, подробнее об этом сказано в п. 12.

1.3. Поточные шифры

Приведём широко используемую модель поточного шифра — шифр гаммирования [5]. В основе таких систем лежит метод «наложения» (например, сложение по модулю 2) ключевой последовательности (гаммы) на открытый текст (шифруемое сообщение). Из работ Клода Шеннона следует, что если ключ имеет такую же длину, как и сообщение, выбирается случайно и равновероятно и при этом используется только

один раз, то данная система шифрования является абсолютно стойкой к атакам на основе шифртекста. Поскольку такая модель неприменима для широкого распространения в силу того, что затруднительно генерировать такой же объём ключа, как и сообщения, а тем более его передавать, перед разработчиками стоит задача получать из короткой случайной последовательности битов ключа некоторую длинную последовательность (гамму), которая будет близка к случайной. Заметим, что именно от свойств данной последовательности зависит криптографическая стойкость шифра.

Часто в качестве компонент поточного шифра используются регистры сдвига с обратной связью. Общая схема их работы приведена на рис. 2, где f — булева функция от n переменных, являющаяся *функцией обратной связи* [20].

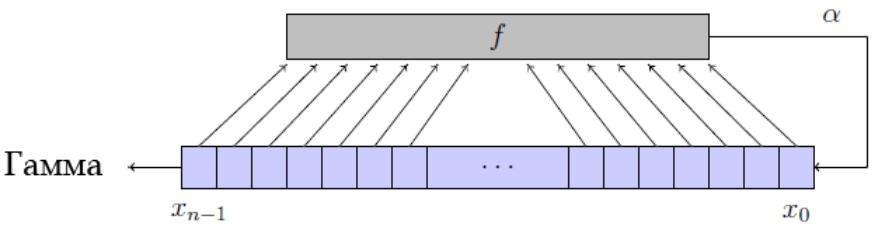


Рис. 2

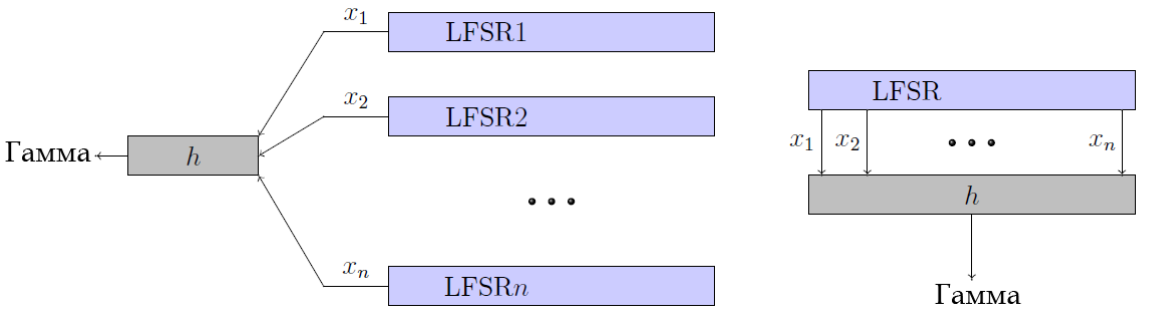
Перед стартом работы происходит начальное заполнение состояния регистра некоторыми n битами. Далее на каждом такте работы вычисляется очередное значение $\alpha = f(x_{n-1}, \ldots, x_0)$, затем все биты регистра сдвигаются влево, при этом в крайний правый бит записывается значение α, а крайний левый бит становится очередным битом выходной последовательности $u = \{u_0, u_1, u_2 \ldots\}$.

Наибольшее распространение получили регистры сдвига с линейной обратной связью (LFSR), т. е. те, в которых f линейна, скажем, $f(x_{n-1}, \ldots, x_0) = \langle c, x\rangle$, где $c \in \mathbb{F}_2^n$. Заметим, что последовательность, порождаемая любым регистром с обратной связью, всегда периодическая. Легко видеть, что на самом деле любую периодическую последовательность можно породить LFSR подходящей длины. При этом *линейной сложностью* $\mathcal{L}^u$ последовательности u называют минимальную длину LFSR, который её порождает. Линейная сложность последовательности — это основной параметр, характеризующий сложность её аналитического строения [5].

Напомним, что для генерации «хорошей» гаммы не используется лишь один LFSR. Действительно, если мы знаем функцию обратной связи $f(x) = \langle c, x\rangle$, $c \in \mathbb{F}_2^n$, то достаточно лишь n подряд идущих битов последовательности для того, чтобы восстановить начальное состояние регистра путём решения системы линейных уравнений. А начальное состояние, как правило, и является секретным ключом шифра.

Кроме того, известен более сильный результат, который позволяет найти линейную функцию обратной связи для любой периодической последовательности. Допустим, что мы перехватили достаточно длинный отрезок некоторой периодической последовательности. Тогда с помощью широко известного алгоритма Берлекэмпа — Месси можно за полиномиальное от длины конечной последовательности время найти закон рекурсии, её порождающий, что эквивалентно нахождению линейного регистра, который вырабатывает данный отрезок последовательности. При этом если длина последовательности не меньше $2\mathcal{L}$, где $\mathcal{L}$ — её линейная сложность, то найденный LFSR вырабатывает и всю бесконечную последовательность, отрезок которой нам известен.

С другой стороны, линейная сложность вырабатываемой последовательности должна быть высокой при почти любом начальном состоянии регистра — неизвестном ключе. В силу этого используют некоторые усложнения. Выделяют две основные модели генераторов, построенных на основе регистров сдвига с линейной обратной связью [20] (рис. 3). Булева функция h называется соответственно *комбинирующей* и *фильтрующей*.



Комбинирующий генератор **Фильтрующий генератор**

Рис. 3

2. Высокая алгебраическая степень

Опишем, опираясь на обзор C. Carlet [24], теоретические результаты, которые показывают, что в качестве комбинирующей и фильтрующей функции h следует выбирать те, чья алгебраическая степень не мала. Рассмотрим сначала комбинирующий генератор, состоящий из n регистров с линейной обратной связью длин $L_1, \ldots, L_n$. Пусть комбинирующая функция h задана в виде алгебраической нормальной формы $h(x_1, \ldots, x_n) = \bigoplus\limits_{k=1}^{n} \bigoplus\limits_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} x_{i_1} \ldots x_{i_k}$, где $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $a_{i_1,\ldots,i_k} \in \mathbb{F}_2$. Тогда линейная сложность $\mathcal{L}$ вырабатываемой последовательности оценивается сверху через длины регистров следующим образом:

$$\mathcal{L} \leqslant \sum_{k=1}^{n} \sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} L_{i_1} \ldots L_{i_k},$$

при этом известны условия, при которых данная оценка достигается: если L_i совпадает с линейной сложностью генерируемой LFSR_i последовательности для любого i и числа $L_1, \ldots, L_n$ попарно взаимно просты. Можно видеть, что чем выше степень АНФ, тем большую линейную сложность можно получить.

В случае фильтрующей модели аналогичного точного результата нет, хотя также известна оценка линейной сложности $\mathcal{L}$ генерируемой последовательности через степень фильтрующей функции $\deg(h)$, а именно: $\mathcal{L} \leqslant \sum\limits_{i=0}^{\deg(h)} C_L^i$, где L — длина регистра, а C_L^i — биномиальный коэффициент. Кроме того, если L — простое число, то верна оценка снизу: $\mathcal{L} \geqslant C_L^{\deg(h)}$.

В блочных шифрах следует также выбирать функции с достаточно большой степенью. «Параметр $\deg(F)$ булевой функции должен быть большим. Для блочных шифров это условие накладывается, как правило, для того, чтобы система уравнений на биты ключа, построенная путём анализа структуры шифра — в том числе функции F, использующейся в качестве его компоненты, — имела высокую степень. Чем выше степень системы, тем сложнее её решить, а значит, определить ключ» [20].

3. Уравновешенность

Определение 1. Булева функция f от n переменных называется *уравновешенной*, если её вес равен 2^{n-1}, т. е. функция принимает значения 0 и 1 одинаково часто.

Это, пожалуй, одно из самых естественных необходимых свойств, накладываемых на булевы функции, использующиеся в поточных шифрах. Если булева функция уравновешена, то вероятность того, что она примет значение 0 или 1, одинакова и равна 1/2. Это позволяет ослабить статистические зависимости между входом функции и её выходом. В противном случае у криптоаналитика есть возможность, используя вероятностное соотношение, провести криптоанализ шифра.

Данное определение обобщается на векторный случай.

Определение 2. Векторная (n, m)-функция F называется *уравновешенной*, если $|F^{-1}(y)| = |\{x \in \mathbb{F}_2^n : F(x) = y\}| = 2^{n-m}$ для любого $y \in \mathbb{F}_2^m$.

При этом справедливо следующее

Утверждение 1. Векторная (n, m)-функция F уравновешена тогда и только тогда, когда уравновешены все её компонентные функции $\langle v, F\rangle$, $v \in \mathbb{F}_2^m$, $v \neq \mathbf{0}$.

Заметим, что при $n = m$ класс уравновешенных векторных функций совпадает с классом взаимно однозначных функций. Как правило, именно они представляют наибольший интерес для использования в блочных шифрах в качестве S-блоков для обеспечения однозначного расшифрования.

4. Совершенная уравновешенность

Свойство совершенной уравновешенности булевой функции является естественным обобщением обычной уравновешенности, когда данная функция выступает, например, в качестве фильтрующей функции генератора. Данное свойство было формализовано С. Н. Сумароковым [18] .

Пусть f — фильтрующая функция генератора от n переменных, $x = (x_1, \ldots, x_{\ell+n-1})$ — отрезок входной последовательности длины $\ell + n - 1$, где ℓ — некоторое натуральное число. Тогда генератор выработает по нему отрезок последовательности $u = (u_1, \ldots, u_\ell)$ длины ℓ, где $u_i = f(x_i, x_{i+1}, \ldots, x_{i+n-1})$, $i = 1, \ldots, \ell$. Определим для функции f и числа ℓ векторную $(\ell + n - 1, \ell)$-функцию f_ℓ, сопоставляющую вектору x вектор u по описанному выше правилу.

Определение 3. Булева функция f называется *совершенно уравновешенной*, если для любого натурального числа ℓ функция f_ℓ уравновешена.

В частности, если функция совершенно уравновешена, то она уравновешена и в обычном смысле. Обратное неверно.

Запретом булевой функции f называется такой вектор $u = (u_1, \ldots, u_\ell)$ для некоторого ℓ, для которого множество прообразов $f_\ell^{-1}(u)$ пусто. Следующая теорема отражает критерий совершенной уравновешенности в терминах запретов функции.

Теорема 1. Булева функция совершенно уравновешена тогда и только тогда, когда она является функцией без запрета.

Интуитивно понятно, что наличие запрета у фильтрующей функции генератора делает её «слабее» с точки зрения порождения последовательностей с хорошими статистическими свойствами. Однако следует быть осторожными, поскольку совершенно уравновешенная фильтрующая функция в том или ином виде переносит свойства входной последовательности в свойства генерируемой последовательности [11]. Например, С. В. Смышляевым в работе [17] установлен новый критерий, который идейно говорит

следующее: «фильтрующая функция сохраняет запреты (в соответствующем смысле) тогда и только тогда, когда она совершенно уравновешена». Соответственно если на вход функции поступает «далёкая» от случайной последовательность, то и на выходе её статистические свойства будут плохие.

Заметим, что если фильтрующая функция линейна по своей первой и/или последней существенной переменной, то она совершенно уравновешена. Но в обратную сторону это неверно, поскольку найдены конструкции совершенно уравновешенных функций, нелинейно зависящих от своих крайних переменных (ссылки можно найти в [11]). Актуальность поиска широкого класса таких функций подтверждается тем, что известна так называемая инверсионная атака на фильтрующие генераторы, использующие линейные по первой или последней существенной переменной функции в качестве фильтрующих. Данную атаку предложил J. Dj. Golić [34].

5. Лавинные характеристики

Концепция лавинных характеристик булевой функции отражает один из принципов Шеннона построения шифрующих преобразований, сформулированных в п. 1.2, а именно принцип рассеивания. Следующее определение ввели A. F. Webster, S. E. Tavares в работе [43].

Определение 4. Булева функция f от n переменных удовлетворяет *строгому лавинному критерию* (SAC), если для любого направления $a \in \mathbb{F}_2^n$, где $\mathrm{wt}(a) = 1$, производная $D_a(f)$ уравновешена.

Если все координатные функции векторной (n, m)-функции удовлетворяют SAC, то при изменении одного входного бита с вероятностью $1/2$ изменится каждый из выходных битов. Следовательно, можно ожидать, что примерно половина выходных битов изменится.

Обобщением данного критерия является следующий, который стали рассматривать B. Preneel и др. [39].

Определение 5. Булева функция f от n переменных удовлетворяет *критерию распространения степени* k (PC(k)), если для любого направления $a \in \mathbb{F}_2^n$, где $1 \leqslant \leqslant \mathrm{wt}(a) \leqslant k$, производная $D_a(f)$ уравновешена.

По определению PC(1) совпадает с SAC. Забегая вперёд, можно отметить, что функции, удовлетворяющие PC(n), — это в точности бент-функции (см. определение 11, п. 8 и теорему 16, п. 12). Если функция удовлетворяет данным критериям, то это означает, что изменение входного вектора в нескольких битах меняет значение функции с вероятностью $1/2$.

Как отмечается в [11], строгий лавинный критерий и его обобщения «явились в конечном счёте индикаторами локальных свойств для исследуемых криптографических функций». Более правильно требовать, чтобы в среднем у функции были «хорошие» лавинные характеристики, которые выражаются в том, что модуль функции автокорреляции $\Delta_f(a) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus a)}$ был равен или близок к нулю для большинства векторов $a \in \mathbb{F}_2^n$. Такой подход предложили X.-M. Zhang и Y. Zheng в работе [45].

Определение 6. *Глобальными лавинными характеристиками* (GAC) булевой функции f от n переменных называются числа $\sigma_f = \sum\limits_{a \in \mathbb{F}_2^n} \Delta_f^2(a)$ и $\Delta_f = \max\limits_{a \in \mathbb{F}_2^n, a \neq \mathbf{0}} \Delta_f(a)$.

Понятно, что чем меньше данные величины, тем лучше функция для использования в шифре, поскольку GAC отражают лавинные показатели в среднем. В [11] можно найти основные свойства GAC произвольной функции, а также их некоторые связи

с другими криптографическими свойствами, в частности с нелинейностью и порядком устойчивости.

6. Линейные структуры

Определение 7. Векторная (n, m)-функция *обладает линейной структурой*, если существует вектор $a \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, такой, что $D_a(F) \equiv \text{const}$.

В качестве компонент шифра следует выбирать функции, которые не обладают линейной структурой [32], несмотря на то, что, как отмечается в [24], к настоящему моменту данные слабости не были использованы в атаках. Действительно, наличие линейной структуры у функции свидетельствует о её «похожести» на линейную функцию в том смысле, что она линейно эквивалентна функции, у которой есть переменная, от которой она зависит линейно или фиктивно. Как уже отмечалось, близость функций в различных смыслах к линейным неприемлема для использования в криптографических системах.

7. Корреляционная иммунность и устойчивость

Рассматриваемые здесь свойства возникли из разных прикладных задач, но, как оказалось, тесно связаны. Термин корреляционной иммунности ввёл T. Siegenthaler в работе [40]. Он показал, что функции с высоким порядком корреляционной иммунности, используемые в качестве комбинирующей функции генератора в поточном шифре, делают шифр стойким к корреляционной атаке. Суть атаки состоит в поиске подмножества переменных комбинирующей функции, о значениях которых можно получить информацию, зная значение функции. Устойчивые функции были введены в открытой литературе также в 1980-х годах, но, как отмечается в [11], «были связаны с такими областями исследований, как распределённые вычисления, устойчивые относительно ошибок, и выработка общих ключей для квантово-криптографических каналов связи». Из работы К. Н. Панкова [13] известно, что в СССР аналогичные функции исследовались Л. В. Ларионовым в 1970-х годах.

В качестве комбинирующей функции генератора в поточном шифре необходимо использовать функции, обладающие свойством устойчивости. При этом чем выше порядок устойчивости, тем выше стойкость шифра к корреляционному криптоанализу.

Приведём формальные определения данных свойств на языке комбинаторики. Определим сначала понятие подфункции. *Подфункцией* булевой функции f от переменных $x_1, \ldots, x_n$ называется булева функция, полученная из f подстановкой вместо переменных $x_{i_1}, \ldots, x_{i_k}$ конкретных констант $a_1, \ldots, a_k$, принимающих значения 0 или 1. Такая подфункция обозначается $f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k}$.

Определение 8. Булева функция f называется *корреляционно-иммунной порядка* k, если вес подфункций $f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k}$ удовлетворяет соотношению $\text{wt}(f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k}) = \text{wt}(f)/2^k$ для любого набора индексов $1 \leqslant i_1 < \ldots < i_k \leqslant n$ и любых значений $a_1, \ldots, a_k \in \mathbb{F}_2$.

Другими словами, булева функция f называется корреляционно-иммунной порядка k, если $\mathsf{P}[f = 1] = \mathsf{P}[f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k} = 1]$, где P — функция вероятности, т. е. знание некоторых входных битов не даёт статистической информации о значении функции.

Определение 9. Булева функция f называется *k-устойчивой* (*k-эластичной*), если любая её подфункция, полученная фиксацией не более k переменных, является уравновешенной.

Нетрудно убедиться, что булева функция f является k-устойчивой тогда и только тогда, когда она уравновешена и корреляционно-иммунна порядка k.

7.1. Идея корреляционной атаки

Рассмотрим общую идею данного криптоанализа, следуя [14].

Пусть f — комбинирующая функция генератора, LFSR_1, …, LFSR_n — его регистры сдвига с линейной обратной связью длин $L_1, \dots, L_n$ соответственно, а $u = u_0, u_1, u_2, \dots$ — выходная последовательность регистра. Трудоёмкость криптоанализа «грубой силой», т. е. полного перебора всех начальных состояний регистров, оценивается как $2^{L_1+\dots+L_n}$. Если регистр построен «правильно», то последовательность u очень близка к случайной, поэтому можно считать, что $\mathsf{P}[u_i = 0] \approx 1/2$. Следовательно, если $z = z_0, z_1, z_2, \dots$ — произвольная не зависящая от u последовательность, то можно считать, что $\mathsf{P}[u_i = z_i] \approx 1/2$, поскольку $\mathsf{P}[u_i = z_i] = \mathsf{P}[u_i = 0]\,\mathsf{P}[z_i = 0] + \mathsf{P}[u_i = 1]\,\mathsf{P}[z_i = 1] \approx 1/2\,(\mathsf{P}[z_i = 0] + \mathsf{P}[z_i = 1]) = 1/2$.

Предположим, что функция f *коррелирует* с функцией $\ell(x_1, \dots, x_n) = x_1$, что означает $\mathsf{P}[f = \ell] = 1/2 + \varepsilon \neq 1/2$. Тогда утверждается, что можно восстановить неизвестное начальное состояние регистра LFSR_1. Для этого будем перебирать все возможные начальные состояния первого регистра (их 2^{L_1}), для каждого из них генерировать выходную последовательность данного регистра $z = z_0, z_1, z_2, \dots$ и считать, сколько раз выполнено $z_i = u_i$. Тогда если начальное состояние было предположено неправильно, то $\mathsf{P}[z_i = u_i] \approx 1/2$, а если правильно, то $\mathsf{P}[z_i = u_i] \approx 1/2 + \varepsilon$. Таким образом, чем больше значение корреляции $|\varepsilon|$, тем с большей вероятностью мы найдём правильное состояние регистра. Тем самым мы уменьшили сложность перебора до $2^{L_1} + 2^{L_2+\dots+L_n}$. Если при этом есть корреляция f и других переменных, то сложность можно ещё понижать. Если же у f нет корреляции с функциями $\ell(x) = x_i$, можно искать корреляции с другими линейными функциями $\langle c, x\rangle$, у которых $\mathrm{wt}(c) = k$ мал, скажем, $c = (1, \dots, 1, 0, \dots, 0)$. Тогда сложность перебора уменьшается до $2^{L_1+\dots+L_k} + 2^{L_{k+1}+\dots+L_n}$. Но если k достаточно большое, то особого выигрыша для криптоаналитика может и не быть.

Заметим, что в [11] приводятся также известные результаты о том, что фильтрующий генератор с функцией f можно свести к специально построенному комбинирующему генератору с той же функцией f, выступающей уже в качестве комбинирующей. При этом новый генератор вырабатывает ту же последовательность при определённом начальном заполнении состояний его регистров. Следовательно, корреляционную атаку можно обобщать и на случай фильтрующих генераторов.

7.2. Основные теоремы и связь с нелинейностью

Утверждение 2. Корреляционно-иммунная порядка k булева функция является также корреляционно-иммунной порядка ℓ для всех $\ell < k$.

В силу этого утверждения естественно ввести определение *порядка* корреляционной иммунности $\mathrm{cor}(f)$ функции f как

$$\mathrm{cor}(f) = \max\{0 \leqslant k \leqslant n : f \text{ — корреляционно-иммунная порядка } k\}.$$

Следующая широко известная теорема даёт спектральную характеризацию корреляционно-иммунных и устойчивых функций.

Теорема 2 (спектральная характеризация). Пусть f — булева функция от n переменных. Справедливо $\mathrm{cor}(f) = k$ тогда и только тогда, когда $W_f(y) = 0$ для всех векторов y, таких, что $1 \leqslant \mathrm{wt}(y) \leqslant k$. Кроме того, f является уравновешенной тогда и только тогда, когда $W_f(\mathbf{0}) = 0$.

Данная теорема наглядно связывает определение корреляционно-иммунных порядка k функций и способность противостоять корреляционной атаке при использова-

нии их в качестве комбинирующих функций поточного генератора. Действительно, для проведения атаки необходимо найти линейную функцию $\ell(x) = \langle c, x\rangle$, с которой есть корреляция у комбинирующей функции f, т. е. $\mathsf{P}[f = \ell] \neq 1/2$. Так как $\mathsf{P}[f = \ell] = (2^n - \mathrm{d}(f, \ell))/2^n = 1/2 + (2^{n-1} - \mathrm{d}(f, \ell))/2^n \neq 1/2$, это эквивалентно тому, что $\mathrm{d}(f, \ell) \neq 2^{n-1}$. Кроме того, легко получить, что расстояние между f и линейной функцией $\ell(x) = \langle c, x\rangle$ выражается как $\mathrm{d}(f, \ell) = 2^{n-1} - W_f(c)/2$. Таким образом, $\mathrm{d}(f, \ell) \neq 2^{n-1}$ тогда и только тогда, когда $W_f(c) \neq 0$. Следовательно, если порядок устойчивости комбинирующей функции достаточно высокий, то корреляционную атаку на данный шифр провести будет сложно.

Связь порядка $\mathrm{cor}(f)$ и степени функции $\deg(f)$ отражается в следующей теореме.

Теорема 3 (Siegenthaler). Пусть f — булева функция от n переменных.

1. Если $\mathrm{cor}(f) = k$, то выполняется $\deg(f) + k \leqslant n$.
2. Если $\mathrm{cor}(f) = k$, f уравновешена и $k \leqslant n - 2$, то выполняется $\deg(f) + k \leqslant n - 1$.

Из теоремы следует, что чем выше степень функции, тем меньше порядок её корреляционной иммунности, и наоборот. Но, как мы видели, оба этих параметра должны быть высокими для функций усложнения криптографических генераторов.

Следствие 1. Пусть f — булева функция от n переменных. Если $\mathrm{cor}(f) = n$, то $f \equiv \mathrm{const}$. Если $\mathrm{cor}(f) = n - 1$, то $f(x) = x_1 \oplus \ldots \oplus x_n \oplus \mathrm{const}$.

Известна следующая оценка $\mathrm{cor}(f)$, полученная Д. Г. Фон-дер-Флаассом [33].

Теорема 4 (Фон-дер-Флаасс). Пусть f — неуравновешенная булева функция от n переменных. Тогда $\mathrm{cor}(f) \leqslant (2n/3) - 1$.

Здесь естественно также упомянуть про нелинейность N_f (см. определение 10, п. 8) корреляционно-иммунных функций.

Теорема 5 (связь $\mathrm{cor}(f)$ и N_f). Пусть f — булева функция от n переменных.

1. Если $\mathrm{cor}(f) = k$, $k \leqslant n - 1$, то выполняется $N_f \leqslant 2^{n-1} - 2^k$.
2. Если $\mathrm{cor}(f) = k$, f уравновешена и $k \leqslant n - 2$, то выполняется $N_f \leqslant 2^{n-1} - 2^{k+1}$.

Как видно из теоремы, нелинейность функции с ростом порядка устойчивости падает. Это интуитивно понятно из того, что с ростом $\mathrm{cor}(f)$ становится всё больше нулевых коэффициентов Уолша — Адамара функции f, что ведёт к увеличению максимального значения $|W_f(a)|$ в силу равенства Парсеваля, а следовательно, к снижению нелинейности. При этом интересен и актуален вопрос о достижимости оценок из теоремы 5. Известно, что если оценка для k-устойчивых функций достигается, то $(n - 3)/2 \leqslant k \leqslant n - 2$, но примеров для всех таких возможных параметров пока не найдено. Ю. В. Таранниковым [41] разработан и обобщён метод, который в настоящий момент позволяет строить k-устойчивые функции с нелинейностью $2^{n-1} - 2^{k+1}$ для всех $k \geqslant cn(1 + \mathrm{o}(1))$, где $c = 0{,}5789\ldots$

8. Высокая нелинейность

Определение 10. *Нелинейностью* булевой функции f от n переменных называется величина N_f, равная расстоянию Хэмминга от f до множества $\mathcal{A}_n$ всех аффинных функций от n переменных.

В п. 7.2 мы уже упоминали связь расстояния между произвольной функцией и линейной функцией $\mathrm{d}(f, \langle c, x\rangle) = 2^{n-1} - W_f(c)/2$. Основываясь на ней, легко получить, что нелинейность f выражается через её коэффициенты Уолша — Адамара следующим образом: $N_f = \mathrm{d}(f, \mathcal{A}_n) = 2^{n-1} - \max\limits_{c \in \mathbb{F}_2^n} |W_f(c)|/2$. Более того, из равенства Парсеваля

можно найти оценку снизу: $\max\limits_{c\in\mathbb{F}_2^n}|W_f(c)|\geqslant 2^{n/2}$. Таким образом, нелинейность функции всегда удовлетворяет неравенству $N_f\leqslant 2^{n-1}-2^{n/2-1}$.

Определение 11. *Максимально нелинейной* называется функция, нелинейность которой достигает максимально возможного значения. В случае чётного числа переменных максимально нелинейные функции также называются *бент-функциями*.

Вопрос о том, кто первым начал изучение максимально нелинейных функций, остаётся открытым. Признанный авторитет в ответе на этот вопрос имеет Oscar S. Rothaus. В 1960-х годах он работал математиком в Институте оборонного анализа США и в то же время написал свою первую работу о бент-функциях, которая появилась в открытой печати лишь в 1976 г. Однако с недавнего времени стало известно [8], что бент-функции также изучались в Советском Союзе в 1960-х годах. Среди первых исследователей — В. А. Елисеев и О. П. Степченков, но их работы по-прежнему засекречены. Известно, что они называли бент-функции *минимальными функциями* и получили ряд утверждений о их свойствах, а также предложили аналог известной конструкции Майорана — МакФарланда. Подробно с историей изучения максимально нелинейных функций, их связи с различными комбинаторными объектами, применении в криптографии, известными конструкциями и открытыми вопросами можно познакомиться по работе Н. Н. Токаревой [42], посвящённой бент-функциям.

Чем выше значение нелинейности булевой функции, тем предпочтительнее её использовать как в поточных, так и в блочных шифрах. Приведём далее две атаки на различные виды шифров.

8.1. Идея быстрой корреляционной атаки

Данный вид атаки на комбинирующий генератор появился вскоре после простой корреляционной атаки (рассмотренной в п. 7.1). Опишем её основную идею, не вдаваясь в подробности теории кодов, исправляющих ошибки [24].

Будем оперировать с тем же комбинирующим генератором, что был описан в п. 7.1. Как и для корреляционной атаки, для быстрой корреляционной атаки необходимо найти линейную функцию $\ell(x)=\langle c,x\rangle$, с которой у f есть корреляция, т. е. $\mathsf{P}[f=\ell]=1/2+\varepsilon\neq 1/2$. Отличие в том, что нам теперь не важно, каково значение $\mathrm{wt}(c)$, а важно лишь, чтобы значение корреляции $|\varepsilon|$ было как можно больше.

Будем считать далее, что $\varepsilon>0$ (иначе вместо ℓ рассмотрим функцию $\ell\oplus 1$). Пусть $u=u_0,u_1,u_2,\ldots$ — последовательность, вырабатываемая генератором. Тогда можно представить, что эта «правильная» последовательность (т. е. которую мы можем действительно наблюдать) является результатом внесения помех в «неправильную» последовательность $z=z_0,z_1,z_2,\ldots$ с вероятностью ошибки $1/2-\varepsilon$, где z получена тем же генератором, но с комбинирующей функцией ℓ вместо f. Так как мы выбрали ε достаточно большим, вероятность ошибки будет маленькой.

Допустим, мы можем наблюдать отрезок последовательности $u_k,\ldots,u_{k+N-1}$. Множество всевозможных значений $z_k,\ldots,z_{k+N-1}$ является линейным кодом длины N. Тогда, наблюдая фрагмент последовательности u, путём исправления ошибок можно восстановить последовательность z. А это даёт выигрыш в том, что линейная сложность z гораздо ниже линейной сложности u, и достаточно отрезка последовательности гораздо меньшей длины, чтобы восстановить закон рекурсии и начальное состояние регистра с помощью алгоритма Берлекэмпа — Месси.

Отметим здесь сразу, что значение корреляции ε функции f с аффинными функциями можно оценить снизу через её нелинейность: $|\varepsilon|\leqslant 2^n-2N_f$. Следовательно, чем

выше нелинейность, тем меньше максимальная корреляция, а значит, больше вероятность ошибки в моделируемом канале с шумом, что делает менее возможным проведение быстрой корреляционной атаки на комбинирующий генератор с комбинирующей функцией f.

8.2. Идея линейного криптоанализа

В 1993 г. японский криптограф M. Matsui предложил статистический метод анализа шифра DES, названный *линейным криптоанализом*. Опишем идею самой простой его модификации по работе [20] (алгоритм 1).

Пусть P, C, K — блоки открытого текста, шифртекста и ключа некоторого блочного шифра. *Линейным приближением* шифра называется соотношение $\langle \alpha, P\rangle \oplus \langle \beta, C\rangle = \langle \gamma, K\rangle$, выполняющее с некоторой вероятностью $1/2+\varepsilon$, $\varepsilon \neq 0$, где α, β, γ — некоторые двоичные вектора соответствующих длин.

Алгоритм 1. Линейный криптоанализ

1: Находим линейное приближение шифра, для которого $|\varepsilon|$ как можно больше.
2: При фиксированном неизвестном ключе K набираем выборку из N пар (P, C).
3: Для каждой пары выборки вычисляем значение левой части выбранного на шаге 1 соотношения. Пусть N_0 — количество полученных нулей, а N_1 — единиц, $N_0 + N_1 = N$.
4: Полагаем $\langle \gamma, K\rangle = 0$, если $(N_0 - N_1)\varepsilon > 0$, и $\langle \gamma, K\rangle = 1$ иначе.

В результате находим одно линейное соотношение на биты неизвестного ключа, следовательно, можем сократить полный перебор с 2^k до 2^{k-1}, где k — количество бит ключа K. Существуют более сильные модификации линейного криптоанализа, которые позволяют находить сразу группу неизвестных битов ключа, но суть остаётся прежней — поиск линейного приближения, но уже не всего шифра, а его части.

Основная сложность метода в том, как находить линейное приближение. На практике поступают так: анализируют соотношения, которые выполняются для S-блоков, а затем расширяют их на несколько раундов и на большую часть битов P, C, K.

Пусть S-блок шифра задан векторной (n, m)-функцией F. Требуется найти соотношение вида $\langle a, x\rangle \oplus \langle b, F(x)\rangle = 0$, выполняющееся с некоторой вероятностью $p = 1/2+\varepsilon$, где $\varepsilon \neq 0$. Распишем $p = \mathsf{P}[\langle a, x\rangle = \langle b, F(x)\rangle] = 1/2 + \left(2^{n-1} - \mathrm{d}(\langle a, x\rangle, \langle b, F(x)\rangle)\right)/2^n$. Опять, как и для поточного шифра, для того чтобы успешно провести атаку, т. е. максимизировать $|\varepsilon|$, необходимо минимизировать расстояние $\mathrm{d}(\langle a, x\rangle, \langle b, F(x)\rangle)$ по всем возможным ненулевым $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^m$. Соответственно противодействием данной атаке является выбор в качестве S-блоков таких векторных функций, у которых минимальное расстояние $\mathrm{d}(\langle a, x\rangle, \langle b, F(x)\rangle)$ по всем возможным ненулевым a, b как можно больше. Заметим, что это эквивалентно рассмотрению нелинейности компонентных функций $\langle b, F\rangle$ функции F.

8.3. Теоретические результаты и открытые вопросы

Приведём некоторые факты, опираясь на работы [42, 25]. Пусть f — булева функция от n переменных. Ранее мы получили оценку нелинейности $N_f \leqslant 2^{n-1} - 2^{n/2-1}$, которая достигается при чётном n для бент-функций. Для нечётного числа переменных точного значения максимальной нелинейности в общем случае не известно. Например, установлено, что при $n = 1, 3, 5, 7$ для f от n переменных $N_f \leqslant 2^{n-1} - 2^{(n-1)/2}$, и данная оценка достигается для квадратичных функций; но при нечётных $n > 7$ существуют функции, нелинейность которых строго больше $2^{n-1} - 2^{(n-1)/2}$.

Теорема 6 (нелинейность случайной функции). Существует константа c, такая, что для почти всех булевых функций от n переменных $N_f \geqslant 2^{n-1} - 2c\sqrt{n}2^{n/2-1}$.

Данный результат говорит о том, что нелинейность произвольной функции близка к верхней границе, но, как это часто бывает, нахождение конкретных функций с высокой нелинейностью является нетривиальной задачей.

В следующей теореме приведём некоторые известные факты о бент-функциях.

Теорема 7.

1. Бент-функции существенно зависят от всех своих переменных.
2. Для бент-функции f от n переменных верно $\mathrm{wt}(f) = 2^{n-1} \pm 2^{n/2-1}$.
3. Для бент-функции f от n переменных верно $\deg(f) \leqslant n/2$.
4. Конструкция Мэйорана — МакФарланда. Пусть π — любая перестановка на множестве $\mathbb{F}_2^{n/2}$; h — произвольная булева функция от $n/2$ переменных. Тогда $f(x', x'') = \langle x', \pi(x'')\rangle \oplus h(x'')$ является бент-функцией от n переменных.

Из утверждений 3 и 4 теоремы 7 можно получить оценки мощности класса $\mathcal{B}_n$ бент-функций от n переменных.

Утверждение 3 (оценки $|\mathcal{B}_n|$). Справедливо: $2^{2^{n/2}}(2^{n/2})! \leqslant |\mathcal{B}_n| \leqslant 2^{2^{n-1}+C_n^{n/2}/2}$.

Известны некоторые улучшения данных оценок, но на качественном уровне они остаются такими же. Видно, что с ростом n разрыв в оценках становится очень большим. Самым насущным открытым вопросом в этой области является установление точного количества бент-функций или хотя бы нахождение более приемлемых оценок мощности класса бент-функций. А это, в свою очередь, связано с поиском новых конструкций. Более подробно об этом можно найти в [42].

Рассмотрим теперь случай векторной булевой (n, m)-функции F. Как мы видели, для того чтобы противостоять линейному криптоанализу, следует выбирать в качестве S-блоков функции, нелинейность компонентных функций которых высока. Поэтому нелинейность векторной функции определяется как $N_F = \min\limits_{v\in\mathbb{F}_2^m, v\neq\mathbf{0}} N_{\langle v,F\rangle}$. Следовательно, также справедлива оценка $N_F \leqslant 2^{n-1} - 2^{n/2-1}$. Функции, нелинейность которых достигает данной оценки, также называются *векторными бент-функциями*. Вопрос состоит в том, а всегда ли они существуют?

Теорема 8 (существование бент-функций). Векторные бент-функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$ существуют только при $m \leqslant n/2$, где n чётно.

Теорема 9 (Сидельников). При $m \geqslant n-1$ для нелинейности произвольной векторной (n, m)-функции F верна оценка $N_F \leqslant 2^{n-1} - \dfrac{1}{2}\sqrt{3\cdot 2^n - 2 - 2\dfrac{(2^n-1)(2^{n-1}-1)}{2^m-1}}$.

При $n = m$ из оценки Сидельникова следует, что $N_F \leqslant 2^{n-1} - 2^{(n-1)/2}$. При этом известно, что оценка точная. Максимально нелинейные (n, n)-функции существуют при нечётных n и называются *почти бент-функциями* (AB-функциями). Но до сих пор остаётся открытым вопрос о максимальной нелинейности в случаях, если:

а) n нечётное и $m < n-1$;

б) n чётное и $n/2 < m < n-1$.

9. Статистическая независимость

Понятие статистической независимости введено в [4] в связи с рассмотрением статистических аналогов функций.

Определение 12. Булева функция f от n переменных *статистически не зависит* от подмножества своих переменных $U = \{x_{i_1}, \ldots, x_{i_k}\}$, если выполнено: $\mathsf{P}[f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k} = 0] = \mathsf{P}[f = 0]$ для любых значений $a_1, \ldots, a_k \in \mathbb{F}_2$.

Справедлив конструктивный тест на проверку статистической независимости [4].

Теорема 10 (критерий статистической независимости). Булева функция $f(x, y)$ от $n + m$ переменных, где $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$, статистически не зависит от переменных в x, если и только если $W_f(u, \mathbf{0}) = 0$ для любого $u \in \mathbb{F}_2^n$.

9.1. Статистические аналоги

Пусть $F : \mathbb{F}_2^n \times \mathbb{F}_2^r \to \mathbb{F}_2^m$. Данная функция может представлять собой, например, преобразование блока открытого текста длины n с помощью ключа длины r в блок шифртекста длины m.

Определение 13. *Статистическим аналогом* функции F называется уравнение $\varphi(x, y, k) = 0$, где $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$, $k \in \mathbb{F}_2^r$ связаны соотношением $y = F(x, k)$ и $\varphi : \mathbb{F}_2^n \times \mathbb{F}_2^m \times \mathbb{F}_2^r \to \mathbb{F}_2$ такая, что функция $\varphi_F(x, k) = \varphi(x, F(x, k), k)$ статистически не зависит от переменных в x. Число $p = \mathsf{P}[\varphi_F = 0]$ называется *вероятностью* данного статистического аналога, при $p \neq 1/2$ аналог *эффективен*.

Эффективные статистические аналоги рассматриваются с той же целью, что и линейные приближения шифра, рассмотренные в п. 8.2, — смоделировать шифр некоторыми упрощёнными уравнениями, связывающими биты открытого текста, шифртекста и ключа, выполняющимися с некоторой вероятностью. Но существенное их отличие заключается в том, что ассоциированные с данными уравнениями функции статистически не зависят от переменных символов открытого текста, что гарантирует сохранение вероятности выполнения данного уравнения при подстановке в них любых значений открытых текстов и соответствующих шифртекстов.

В работе [4] рассматриваются также вопросы построения статистических аналогов аналогично методу «от простого с сложному», т. е. как строить статистические аналоги всего шифра, отталкиваясь от статистических аналогов его простых компонент. Например, «для суперпозиции двух дискретных функций определяется суперпозиция одной из них (внутренней) и статистического аналога другой (внешней) и показывается, что в случае аддитивности внутренней функции полученная суперпозиция является функцией статистического аналога для первой суперпозиции с вероятностью статистического аналога её внешней функции» [4]. Кроме того, приводятся алгоритмы криптоанализа блочных шифров путём решения систем линейных и нелинейных статистических аналогов функций шифрования методом максимального правдоподобия, которые подкрепляются примерами для шифра DES.

10. Алгебраическая иммунность

Пусть задана булева функция f от n переменных. Булева функция g от n переменных называется *аннулятором* функции f, если выполнено равенство $fg = 0$.

Определение 14. *Алгебраической иммунностью* $\mathrm{AI}(f)$ функции f называется такое наименьшее число d, что существует аннулятор g степени d, не тождественно равный нулю, либо для функции f, либо для $f \oplus 1$.

10.1. Идея алгебраической атаки

Перед тем как давать пояснение определению алгебраической иммунности булевой функции, необходимо сказать следующее. Вообще говоря, любой шифр, как поточный, так и блочный, можно описать в виде системы булевых уравнений, в которой

участвуют биты ключа, открытого текста и шифртекста. Таким образом, если мы знаем несколько пар открытого текста и шифртекста, полученных на одном неизвестном ключе, то, подставив их в данную систему, можно попытаться её решить и найти ключ. Отличительная особенность такой системы в том, что она гарантированно совместна, но для реальных шифров её решение представляется затруднительным. Известно, что задача решения систем нелинейных булевых уравнений в общем случае NP-трудна.

Существуют некоторые подходы к решению систем нелинейных булевых уравнений (подробно с ними можно познакомиться по работе Г. П. Агибалова [2]). Опишем один из них. Поскольку для решения линейных булевых систем существует эффективный метод Гаусса, то естественной идеей в общем случае является попытка сделать нелинейную систему линейной, но уже от большего числа переменных. Такой метод называется методом *линеаризации*. Однако чем выше алгебраическая степень системы, тем больше переменных придётся вводить в общем случае.

Соответственно промежуточным вопросом является следующий: а можно ли сначала уменьшить степень системы, не потеряв её решений, а уже затем применять метод линеаризации? В 2003 г. N. Courtois и W. Meier [29] предложили алгебраический криптоанализ фильтрующего генератора, основанный на понижении степени системы уравнений. Позже данный подход был обобщён и для комбинирующих генераторов и блочных шифров, а также сформировано итоговое понятие алгебраической иммунности булевой функции. Опишем идею алгебраического криптоанализа фильтрующего генератора по пособию [14].

Рассмотрим фильтрующий генератор с функцией h от n переменных. Если $f(x) = \langle c, x\rangle$ — закон рекурсии использующегося LFSR, где $c \in \mathbb{F}_2^n$, то на очередном i-м такте работы, $i = 1, 2, \ldots$, на вход фильтрующей функции подаётся значение векторной линейной функции $L^i(K)$, где $L(x_{n-1}, \ldots, x_0) = (x_{n-2}, \ldots, x_0, f(x_{n-1}, \ldots, x_0))$ и $K = (k_{n-1}, \ldots, k_0)$ — начальное состояние регистра.

Если $u_0, u_1, u_2, \ldots$ — выходная последовательность генератора, то

$$\begin{cases} u_0 = & h(k_{n-1}, \ldots, k_0), \\ u_1 = & h\big(L(k_{n-1}, \ldots, k_0)\big), \\ \vdots & \\ u_i = & h\big(L^i(k_{n-1}, \ldots, k_0)\big), \\ \vdots & \end{cases}$$

Из этих равенств строится нелинейная система булевых уравнений от неизвестных битов ключа K, если известен фрагмент последовательности $\{u_i\}$. Попытаемся теперь понизить степень уравнений данной системы. Предположим, что выполнены одно или оба из следующих условий:

1) существует функция g, такая, что $h(x)g(x) = t(x) \not\equiv 0$ и степень t мала;
2) существует функция $g \not\equiv 0$ малой степени, такая, что $h(x)g(x) \equiv 0$.

Тогда можем понизить степени уравнений системы следующим образом:

— если $u_i = 0$, то вместо $h\big(L^i(k_{n-1}, \ldots, k_0)\big) = 0$ рассмотрим уравнение $t\big(L^i(k_{n-1}, \ldots, k_0)\big) = 0$ при выполнении условия 1;
— если $u_i = 1$, то вместо $h\big(L^i(k_{n-1}, \ldots, k_0)\big) = 1$ рассмотрим уравнение $g\big(L^i(k_{n-1}, \ldots, k_0)\big) = 0$ при выполнении условия 2.

Обратим внимание на условие 1. Имеем $hg = t$; домножая равенство на h, получаем $hg = th$. Следовательно, $t = th$, или $(h \oplus 1)t = 0$. Перефразируя условие 1, получаем:

1') существует функция $t \not\equiv 0$ малой степени, такая, что $(h(x) \oplus 1)t(x) \equiv 0$.

Таким образом, чтобы препятствовать проведению алгебраического криптоанализа фильтрующего генератора с функцией h, необходимо, чтобы для всех функций g, таких, что $hg = 0$ или $(h \oplus 1)g = 0$, степень $\deg(g)$ была достаточно большой. Алгебраической иммунностью функции h назвали минимальную степень такой функции g.

10.2. Базовые результаты и связь с нелинейностью

Приведём некоторые известные факты, следуя обзору [24].

Легко видеть, что степень $\deg(f)$ служит естественной верхней оценкой алгебраической иммунности функции. Кроме того, справедлива следующая верхняя оценка алгебраической иммунности, зависящая только от числа переменных n.

Теорема 11 (верхняя оценка AI). Для произвольной булевой функции f от n переменных выполнено $\mathrm{AI}(f) \leqslant \lceil n/2 \rceil$, где $\lceil k \rceil$ — целая часть сверху числа k.

При этом известно, что данная оценка достижима, что подтверждается примерами в следующей теореме.

Теорема 12 (функции с максимальной AI). Следующие функции от n переменных имеют максимальную алгебраическую иммунность $\lceil n/2 \rceil$:

1) для нечётного n: $f(x) = \begin{cases} 0, & \text{если } \mathrm{wt}(x) < \lceil n/2 \rceil, \\ 1, & \text{если } \mathrm{wt}(x) \geqslant \lceil n/2 \rceil; \end{cases}$

2) для чётного n: $f(x) = \begin{cases} 0, & \text{если } \mathrm{wt}(x) < n/2, \\ b \in \{0,1\}, & \text{если } \mathrm{wt}(x) = n/2, \\ 1, & \text{если } \mathrm{wt}(x) > n/2. \end{cases}$

Хотя существуют примеры функций с максимальной алгебраической иммунностью, известно про этот класс функций очень мало. Любопытным также является следующий факт, который показывает, что алгебраическая иммунность произвольной функции достаточно высока.

Теорема 13 (AI случайной функции). Для любого $a < 1$ и для почти всех булевых функций f от n переменных выполнено $\mathrm{AI}(f) > n/2 - \sqrt{n/2 \cdot \ln\big(n/(2a \ln 2)\big)}$.

С обобщениями понятия алгебраической иммунности на случай (n, m)-функций можно познакомиться по работе [25].

Приведём также известную точную нижнюю оценку нелинейности функции через её алгебраическую иммунность, полученную М. С. Лобановым [10].

Теорема 14 (связь AI и N_f). Для булевой функции f от n переменных справедлива оценка $N_f \geqslant 2 \sum\limits_{i=0}^{\mathrm{AI}(f)-2} C_{n-1}^{i}$.

Несмотря на то, что по этой оценке нелинейность и порядок алгебраической иммунности функции «не противоречат» друг другу, высокая алгебраическая иммунность совсем не гарантирует высокой нелинейности. Действительно, при оптимальной алгебраической иммунности $\lceil n/2 \rceil$ данная оценка принимает следующий вид: $N_f \geqslant 2^{n-1} - C_{n-1}^{(n-1)/2}$ при нечётном n и $N_f \geqslant 2^{n-1} - C_n^{n/2}$ при чётном n. Как мы видели в п. 8.3, данная оценка далека от максимального значения нелинейности функции $2^{n-1} - 2^{n/2-1}$ и, более того, далека и от нелинейности случайной функции (теорема 6).

11. Уровень аффинности и k-нормальность

Определение 15. Булева функция f от n переменных называется *k-аффинной*, $0 \leqslant k \leqslant n-1$, если существует набор индексов $1 \leqslant i_1 < \ldots < i_k \leqslant n$ и значения $a_1, \ldots, a_k \in \mathbb{F}_2$, такие, что подфункция $f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}$ является аффинной.

Определение 16. *Уровнем аффинности* $\mathrm{la}f$ булевой функции f называется минимальное неотрицательное целое число k, для которого f является k-аффинной.

Данный параметр булевой функции стал рассматриваться в связи с предложенной О. А. Логачевым, А. А. Сальниковым, В. В. Ященко атакой на комбинирующий генератор [12]. Он связан с возможностью применения метода линеаризации без введения новых переменных для системы булевых уравнений, описывающей работу генератора. Чем ниже уровень аффинности комбинирующей функции, тем эффективнее криптоанализ. Подробное изучение $\mathrm{la}f$ представлено в работе М. Л. Бурякова [6], где, в частности, исследована связь данного параметра с другими основными криптографическими свойствами. Отметим, что известно асимптотическое поведение уровня аффинности, которое показывает, что он высокий.

Теорема 15 ($\mathrm{la}f$ случайной функции). При $n \to \infty$ для почти всех булевых функций f от n переменных верно $n - \lfloor \log_2 n \rfloor \leqslant \mathrm{la}f \leqslant n - \lceil \log_2 n \rceil + 1$.

В зарубежной литературе [27, 31] введено схожее понятие — k-нормальность.

Определение 17. Булева функция f от n переменных *k-нормальна*, если существует аффинное подпространство размерности k, на котором функция f постоянна.

Известен один пример успешного криптоанализа поточного шифра Grain [36], который как раз основан на том, что используемая в нём фильтрующая функция от 5 переменных имеет низкий порядок нормальности, а именно она 2-нормальная.

12. Дифференциальная равномерность

Принято считать, что определение дифференциально равномерных функций появилось в работах K. Nyberg [38] в начале 1990-х годов в связи с появлением дифференциального криптоанализа блочных шифров, предложенного E. Biham, A. Shamir для шифра DES в 1990 г. Однако необходимо отметить, что подход, который заложен в данном понятии, на самом деле рассматривался уже в 1960-х годах в Советском Союзе, как отмечается в [7].

Определение 18. Векторная булева (n, m)-функция F называется *дифференциально δ-равномерной*, если для любых $a \neq \mathbf{0}$, b уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений.

Легко видеть, что минимальное такое δ равно 2^{n-m}.

Определение 19. Векторная булева (n, m)-функция F называется *совершенно нелинейной* (PN-функцией), если она дифференциально 2^{n-m}-равномерна.

Эквивалентным определением PN-функций является следующее:

Определение 19'. F — PN-функция, если её производные $D_a F$ уравновешены по всем ненулевым направлениям $a \in \mathbb{F}_2^n$, т. е. $|\{x \in \mathbb{F}_2^n : D_a F(x) = y\}| = 2^{n-m}$ для всех $y \in \mathbb{F}_2^m$.

Заметим, что при $m = n$ PN-функций не существует, поскольку если x — решение уравнения $F(x) \oplus F(x \oplus a) = b$, то и $x \oplus a$ также является его решением.

Определение 20. Векторная булева (n, n)-функция F называется *почти совершенно нелинейной* (APN-функцией), если она дифференциально 2-равномерна.

12.1. Идея дифференциального криптоанализа

Опишем идею дифференциального криптоанализа блочного шифра, следуя работе [20] (алгоритм 2). Рассмотрим итеративный блочный шифр, состоящий из r раундов. Обозначим открытые тексты P, P', промежуточные шифртексты после i-го раунда — C_i, C_i' и итоговые шифртексты — C, C' соответственно. Пара векторов $(a, b)_i$ называется i-м дифференциалом шифра, если существуют открытые тексты P, P', такие, что $P \oplus P' = a$ и $C_i \oplus C_i' = b$. При этом вероятностью i-го дифференциала $(a, b)_i$ является величина $\mathsf{P}[C_i \oplus C_i' = b \mid P \oplus P' = a]$.

Алгоритм 2. Дифференциальный криптоанализ

1: Выбираем наиболее вероятный $(r-1)$-дифференциал шифра.
2: При фиксированном неизвестном ключе K набираем выборку из N четвёрок $\{P, P', C, C'\}$, таких, что $P \oplus P' = a$.
3: Перебирая раундовые подключи K_r, расшифровываем каждую из N пар C, C' до C_{r-1}, C_{r-1}' и проверяем, выполнено ли $C_{r-1} \oplus C_{r-1}' = b$.
4: Ключ, для которого равенство из п. 3 выполняется чаще всего, полагаем за верный.

Поскольку искать наиболее вероятные дифференциалы для всего шифра сразу, т. е. для функций, переводящих, например, 64 бита в 64 бита, представляется очень трудным, поступают так же, как и в линейном криптоанализе: действуют методом «от простого к сложному», а именно: анализируют сначала S-блоки, а затем расширяют дифференциалы на весь шифр. Таким образом, выбирая S-блоки, дифференциалы которых почти равновероятны, можно сделать весь шифр устойчивым к дифференциальному криптоанализу. Следовательно, интересен вопрос построения дифференциально δ-равномерных функций с как можно меньшим значением δ.

12.2. Связь PN- и бент-функций, открытые вопросы о APN-функциях

Отметим в первую очередь тесную связь совершенно нелинейных функций с максимально нелинейными, рассмотренными в п. 8.

Во-первых, само название «совершенно нелинейные» отражает то, что такие функции тоже сильно отличаются в некотором смысле от самых простых — линейных. Действительно, если L — линейная (n, m)-функция, то уравнение $L(x) \oplus L(x \oplus a) = b$ всегда имеет 2^n решений при $b = L(a)$, что далеко от оптимального значения 2^{n-m}.

Во-вторых, как оказалось, класс PN-функций совпадает с классом бент-функций! Согласно обзору [22], понятие совершенной нелинейности ввели W. Meier, O. Staffelbach для булевой функции. Вскоре было обнаружено, что совершенно нелинейные функции полностью совпадают с бент-функциями, которые ввёл уже в 1970-х годах O. S. Rothaus, что отражено в следующей теореме.

Теорема 16 (бент-функции и её производные). Булева функция f от n переменных — бент-функция тогда и только тогда, когда производные $D_a f$ уравновешены по всем ненулевым направлениям $a \in \mathbb{F}_2^n$.

Из определения векторной бент-функции, утверждения 1 (см. п. 3) и теоремы 16 следует, что классы PN-функций и векторных бент-функций совпадают. Следовательно, PN-функции существуют только при $m \leqslant n/2$.

Таким образом, PN- или бент-функции обладают наилучшей стойкостью как к линейному, так и к дифференциальному криптоанализу. Однако на практике более интересным является случай, когда $n = m$. Как уже отмечалось, при данных парамет-

рах оптимальными с точки зрения дифференциальных характеристик являются APN-функции, т. е. дифференциально 2-равномерные. В связи с тем, что APN-функции представляют большой интерес для использования в шифрах, их изучению уделяется огромное внимание. Несмотря на это, APN-функции остаются «загадочными», поскольку о них больше открытых вопросов, чем известных фактов. Прежде всего, это построение новых APN-функций, описание класса APN-функций, поиск оценок количества APN-функций от произвольного числа переменных и др. Все известные конструкции почти совершенно нелинейных функций получены с помощью алгебраического представления, при котором функция рассматривается как функция над конечным полем. Однако таких конструкций крайне мало. В данном небольшом обзоре упомянем лишь некоторые проблемы.

Интересным открытым вопросом является следующий: верно ли, что нелинейность APN-функций так же высока? Известно следующее утверждение.

Утверждение 4. Функция F — APN тогда и только тогда, когда её коэффициенты Уолша — Адамара удовлетворяют тождеству $\sum\limits_{u,v\in\mathbb{Z}_2^n} \big(W_F(u,v)\big)^4 = 3\cdot 2^{4n} - 2\cdot 2^{3n}$.

Данное тождество не позволяет получить оценок нелинейности APN-функции, но из него следует, что любая AB-функция является APN. Таким образом, AB-функции, так же как и бент, являются оптимальными с точки зрения двух криптографических критериев. Но большой минус AB-функций в том, что они существуют только для нечётного числа переменных, что неудобно для применения на практике. Про нелинейность APN-функций можно наверняка сказать только то, что она не равна нулю. Все известные примеры APN-функций показывают, что их нелинейность достаточно высока, но её нетривиальных оценок снизу или сверху нет даже для случая квадратичных функций.

Стоит отметить про случай нечётного числа переменных ещё и то, что существуют APN-функции, которые не являются AB. Известным примером такой функции является взаимно однозначная функция обращения элемента в конечном поле $\mathbb{F}_{2^n}$: $F(x) = x^{2^n-2}$. Как упоминается в обзоре М. М. Глухова [7], оптимальное свойство данной функции было указано В. А. Башевым и исследовано Б. А. Егоровым ещё в 1968 г. Б. А. Егоровым показано также, что для чётного n соответствующая подстановка не является APN-функцией, но дифференциально 4-равномерна. Именно эта функция от восьми переменных используется в качестве S-блока известного шифра AES.

Таким образом, мы подошли ко второй насущной проблеме в области APN-функций: существованию APN-подстановок при чётном числе переменных. Вычислительно было проверено для функций от двух и четырёх переменных, что ответ на вопрос о существовании APN-подстановок отрицательный, даже высказывалось предположение, что такой ответ верен и в общем случае. Можно представить, каким было удивление, когда в 2009 г. на криптографической конференции J. F. Dillon и др. предъявили взаимно однозначную APN-функцию от шести переменных. «The discovery in 2009 of an APN permutation in a field of characteristic 2 and even dimension has brought new motivation and new ideas to this field of research» [22]. В настоящее время все усилия направлены на поиск ответа на этот вопрос, в частности, для восьми переменных — случая, который является принципиальным для криптографии. Отметим, что в работе [15] В. Н. Сачков развивает новый комбинаторный подход к исследованию и методам построения взаимно однозначных APN-функций.

Упомянем ещё один любопытный открытый вопрос. В работе [26] для (n,n)-функции F определена ассоциированная булева функция γ_F от $2n$ переменных по следую-

щему правилу: $\gamma_F(a,b)=1$, где $a,b\in\mathbb{F}_2^n$, если $a\neq\mathbf{0}$ и уравнение $F(x)\oplus F(x\oplus a)=b$ имеет решение, и $\gamma_F(a,b)=0$ иначе. Там же установлена следующая связь.

Утверждение 5. Пусть F — (n,n)-функция. Справедливы утверждения:
1) F — APN-функция тогда и только тогда, когда $\mathrm{wt}(\gamma_F)=2^{2n-1}-2^{n-1}$;
2) F — AB-функция тогда и только тогда, когда γ_F — бент-функция.

Функции F и G называются *дифференциально эквивалентными* [35], если $\gamma_F=\gamma_G$. Как оказалось, описать классы дифференциальной эквивалентности APN-функций — очень непростая задача. Изучение данного вопроса начато автором в работах [9, 35], где, в частности, установлено на примере известных APN-функций Голда, что существуют APN-функции, классы дифференциальной эквивалентности которых нетривиальные, а именно: полностью описаны аффинные функции, прибавление которых к APN-функциям Голда не выводит за рамки их классов дифференциальной эквивалентности. Получены вычислительные результаты о таких аффинных функциях для известных квадратичных APN-функций от малого числа переменных 2, ..., 8. Отметим, что полное решение вопроса об описании дифференциально эквивалентных APN-функций может потенциально привести к новым конструкциям APN-функций.

13. Разложимость в сумму специальных функций

Такое свойство векторных булевых функций связано с решением задачи *маскирования данных*, которая возникла в связи с появлением атак по сторонним каналам. Криптографические алгоритмы оказались уязвимы к таким атакам, направленным на слабости в практической реализации алгоритма. Криптоаналитик исследует специфические для данной реализации параметры, например такие, как потребляемая мощность, время выполнения операций, электромагнитное излучение. Сравнив их на разных входных данных и набрав некоторую статистику, он может получить информацию о секретном ключе, выполняемых в устройстве операциях и их параметрах. В качестве мер противодействия используются методы, маскирующие входные данные так, чтобы вычисления не зависели от них в явном виде.

Рассмотрим одну идею достаточно нового метода реализации векторных булевых функций с целью маскирования данных. Данный метод порогового разбиения (threshold implementation) получил своё начало в работе бельгийских авторов [37].

Определение 21. Пороговым разбиением (n,m)-функции S на r частей называется такой набор (nr,m)-функций S_j, $j=1,\dots,r$, для которого выполняются следующие свойства:

Корректность. Для всех $x=(x_1,\dots,x_n)$ верно: $S(x_1,\dots,x_n)=\bigoplus\limits_{j=1}^{r}S_j(\mathbf{x}^1,\dots,\mathbf{x}^r)$ для любых $\mathbf{x}^i=(x_1^i,\dots,x_n^i)\in\mathbb{F}_2^n$, удовлетворяющих условию $x=\mathbf{x}^1\oplus\ldots\oplus\mathbf{x}^r$.

Неполнота. Каждая функция S_j, $j=1,\dots,r$, не зависит от переменных $\mathbf{x}^j$.

Равномерность. Для любых векторов $y,y^1,\dots,y^r\in\mathbb{F}_2^m$, таких, что $\bigoplus\limits_{j=1}^{r}y^j=y$, справедливо $|S_j^{-1}(y^j)|=2^{(r-1)(m-n)}|S^{-1}(y)|$ для любого $j=1,\dots,r$.

Теоретически доказано, что если вместо векторной функции реализовать её пороговое разбиение в криптосистеме, то это сделает систему стойкой к дифференциальной атаке по энергопотреблению первого порядка (first-order differential power analysis) даже при наличии импульсных помех (glitches). Интуитивно, пороговое разбиение функции на r частей представляет собой некоторую схему разделения секрета — входного значения функции x — между r игроками — векторами $\mathbf{x}^j$, $j=1,\dots,r$. При этом ни-

какие $r-1$ игроков не могут восстановить секрет, что обеспечивается требованием неполноты разбиения: каждая из S_j не зависит от переменных $\mathbf{x}^j$, следовательно, даже узнав её, мы не сможем восстановить исходное входное значение x. Требование корректности естественно: пороговое разбиение реализует то же преобразование, что и исходная функция. Требование равномерности необходимо для того, чтобы обеспечивать «правильный переход» между раундами, т. е. чтобы на вход очередного раунда преобразования поступало равномерно распределённое значение.

Естественным вопросом является следующий: каково минимальное значение r для функции S, для которого существует пороговое разбиение S на r частей? Вопрос актуален с практической точки зрения, поскольку напрямую связан с размерами и стоимостью реализации всего криптоалгоритма. Известно, что для функций алгебраической степени d минимальное такое r не меньше $d+1$. При этом всегда легко построить такое пороговое разбиение, удовлетворяющее только свойствам корректности и неполноты, сложнее обеспечить равномерность. Более того, как показали исследования для взаимно однозначных функций от малого числа переменных [21], не для всех функций степени d можно построить пороговое разбиение на $d+1$ частей (назовём его *минимальным*). Следовательно, формулируется открытая математическая задача: можно ли выделить некоторую легко проверяемую отличительную особенность тех функций, для которых минимальное пороговое разбиение существует? И если не существует минимального, то какое существует?

Поскольку эти вопросы пока открыты, разработчики данного метода пошли по пути, что называется, наименьшего сопротивления: не можем найти минимальное разбиение — будем искать пороговое разбиение на большее число частей. Так, например, вычислительно показано, что любую взаимно однозначную функцию от не более чем пяти переменных можно представить пороговым разбиением на 5 частей. Но необходимо находить компромисс между размерами и стоимостью реализации. Поэтому получила распространение и другая идея: те функции S, для которых не получается найти минимальное разбиение, представлять в виде композиции двух или более других функций, например $S = F \circ G$, которые, во-первых, меньшей степени, а во-вторых, для них легко строятся минимальные пороговые разбиения.

14. Мультипликативная сложность

Коротко упомянем ещё один аспект, связанный с использованием булевых функций в качестве криптографических элементов.

Определение 22. *Мультипликативной* (*конъюнктивной*) *сложностью* $MC(F)$ векторной булевой (n,m)-функции F называется минимальное число умножений в $\mathbb{F}_2$, необходимое и достаточное для вычисления $F(x)$ для любого $x \in \mathbb{F}_2^n$ в базисе $\{\cdot, \oplus, 1\}$.

Мультипликативная сложность функций связана с размерами и стоимостью аппаратной реализации шифров, которые их используют. Чем меньше мультипликативная сложность функции, тем проще её схемная реализация. Особенно это актуально для так называемой легковесной (или малоресурсной) криптографии.

В булевом случае ($m = 1$) данная сложность изучается ещё с 1960-х годов, позднее целый ряд работ был посвящён исследованию мультипликативной сложности различных классов функций: квадратичных, симметрических и др. (см., например, [16]). В векторном случае особый интерес представляют взаимно однозначные (n,n)-функции. Однако для произвольного n результатов известно мало. В работе [44] исследована мультипликативная сложность для малых значений n равных 3 и 4.

Как уже упоминалось в п. 13, в современных аппаратных реализациях требуется маскировать производимые вычисления с целью защиты от атак по сторонним каналам, причём важно накладывать различные маски именно на выполняемые нелинейные преобразования. Соответственно чем их меньше, тем дешевле это сделать. Хотя, как отмечается в [44], сложность реализаций взаимно однозначных (n, n)-функций в данном случае рассматривается обычно как число умножений над полем $\mathbb{F}_{2^n}$, а не $\mathbb{F}_2$, остаётся открытым вопрос, а не эффективнее ли в данном случае использовать именно мультипликативную сложность.

Отметим также, что существует предположение [28], что низкая мультипликативная сложность преобразования, реализующего весь шифр, может, наоборот, свидетельствовать о его слабости, в частности, приводить к возможности применения алгебраического криптоанализа шифра.

15. Линеаризационные множества

Рассматриваемый подход предложен Г. П. Агибаловым в работе [3].

Пусть имеется некоторая система S булевых уравнений.

Определение 23. Подмножество X переменных системы S называется *линеаризационным*, если при любой фиксации значений этих переменных в системе последняя превращается в линейную систему уравнений.

Заметим, что мощность линеаризационного множества переменных системы можно понизить путём введения вспомогательных переменных.

Пусть $x_1, \ldots, x_k$ — переменные системы S. Если набор значений $a_1, \ldots, a_k$ является полным решением системы S, то любой поднабор $a_{j_1}, \ldots, a_{j_i}$ значений переменных $x_{j_1}, \ldots, x_{j_i}$ соответственно, где $1 \leqslant j_1 \leqslant \ldots \leqslant j_i \leqslant k$, называется *частичным решением* системы. Частичное решение *квазиполное*, если его подстановка в систему делает её линейной.

15.1. Идея линеаризационной атаки

Работу генератора ключевого потока можно описать в виде системы булевых уравнений от неизвестных битов ключа, если известен некоторый конечный отрезок выходной последовательности. Суть линеаризационной атаки [3] состоит в поиске линеаризационного множества переменных как можно меньшей мощности для данной системы и соответствующего ему квазиполного решения системы. Действительно, осуществляя перебор значений переменных из некоторого линеаризационного множества и проверяя, будет ли совместной линейная система уравнений, полученная при подстановке данных значений, можно найти квазиполное решение системы, а следовательно, и полное, решив с полиномиальной сложностью полученную линейную систему уравнений. При этом сложность атаки оценивается величиной $2^{|X|}$, где $|X|$ — мощность линеаризационного множества переменных системы.

В качестве иллюстрации работы данной атаки приведём комбинирующий генератор Geffe, который состоит из трёх LFSR максимального периода длин L_1, L_2, L_3 соответственно и комбинирующей функции $f(x, y, z) = xy \oplus yz \oplus z$. Система булевых уравнений, описывающая работу генератора, следующая:

$$\begin{cases} u_t = x_t^1 x_t^2 \oplus x_t^2 x_t^3 \oplus x_t^3,\ t = 0, 1, \ldots, m-1, \\ x_{L_1+t}^1 = \bigoplus\limits_{j=0}^{L_1-1} c_j^1 x_{t+j}^1,\ t = 0, 1, \ldots, m-1-L_1, \\ x_{L_2+t}^2 = \bigoplus\limits_{j=0}^{L_2-1} c_j^2 x_{t+j}^2,\ t = 0, 1, \ldots, m-1-L_2, \\ x_{L_3+t}^3 = \bigoplus\limits_{j=0}^{L_3-1} c_j^3 x_{t+j}^3,\ t = 0, 1, \ldots, m-1-L_3, \end{cases}$$

где $m \geqslant \max\{L_1, L_2, L_3\}$; $u_0, u_1, \ldots, u_{m-1}$ — известный начальный отрезок выходной последовательности; c_j^i — некоторые заданные константы. Переменными неизвестных битов ключа являются $x_0^1, \ldots, x_{L_1-1}^1$, $x_0^2, \ldots, x_{L_2-1}^2$, $x_0^3, \ldots, x_{L_3-1}^3$. При этом множество $X = \{x_0^2, \ldots, x_{L_2-1}^2\}$ образует линеаризационное множество переменных системы. Следовательно, линеаризационную атаку на данный генератор можно реализовать со сложностью не выше 2^{L_2} путём опробования наборов значений переменных в X. Сложность такой атаки оказывается ниже, чем корреляционной (см. п. 7.1), сложность которой $2^{L_1} + 2^{L_2} + 2^{L_3}$.

Аналогичные результаты справедливы и для генератора с альтернативным управлением, мультиплексорного генератора и генератора скалярного умножения [3].

Заключение

В качестве заключения хотелось бы отметить красоту математики, которая скрыта в криптографических булевых функциях, особенно в нелинейных в разных смыслах. Казалось бы, определения бент-функций или APN-функций может понять и школьник, а полностью описать их классы (даже найти приемлемые оценки мощностей данных классов) не представляется возможным известным математикам! Вполне вероятно, что ответы на эти вопросы (а они рано или поздно все равно появятся) окажутся не такими важными с прикладной точки зрения, однако они будут очень любопытными для математики как таковой.

В данном обзоре мы очень мало осветили связи между различными криптографическими свойствами. Практика показывает, что в качестве компонент шифра необходимо выбирать «хорошие со всех сторон» функции, что на самом деле очень непростая задача, поскольку многие свойства порой противоречат друг другу. Хотя, как мы видели, теоретические результаты показывают, что у случайной функции многие криптографические параметры близки к оптимальным. Вопрос в том, а как её выбрать, случайную?

И наконец, хотелось бы отметить другую важную сторону, касающуюся исследований в области математической криптографии: историю изучения различных свойств булевых функций. К сожалению, многие работы советских математиков-криптографов до сих пор остаются опубликованными лишь в специальных сборниках, в то время как аналогичные работы, полученные за рубежом, известны и считаются основополагающими. И лишь постепенно начинают появляться упоминания о первых авторах-исследователях криптографических булевых функций в статьях и докладах конференций в России, посвящённых криптографической тематике.

Автор выражает благодарность рецензентам за ценные замечания и дополнения.

ЛИТЕРАТУРА

1. *Агибалов Г. П.* Избранные теоремы начального курса криптографии: учеб. пособие. Томск: Изд-во НТЛ, 2005. 116 с.
2. *Агибалов Г. П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 4–9.
3. *Агибалов Г. П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского государственного университета. Приложение. 2003. № 6. С. 31–41.
4. *Агибалов Г. П., Панкратова И. А.* Элементы теории статистических аналогов дискретных функций с применением в криптоанализе итеративных блочных шифров // Прикладная дискретная математика. 2010. № 3. С. 51–68.
5. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.
6. *Буряков М. Л.* Алгебраические, комбинаторные и криптографические свойства параметров аффинных ограничений булевых функций: дис. . . . канд. физ.-мат. наук. М., 2007.
7. *Глухов М. М.* О совершенно и почти совершенно нелинейных функциях // Математические вопросы криптографии. 2016. (в печати)
8. *Глухов М. М.* Планарные отображения конечных полей и их обобщения. Презентация для конф. «Алгебра и логика, теория и приложения». Красноярск, 21–27 июля, 2013.
9. *Городилова А. А.* Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. Т. 27. Вып. 3. С. 3–16.
10. *Лобанов М. С.* Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. Т. 18. Вып. 3. С. 152–159.
11. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
12. *Логачев О. А., Сальников А. А., Ященко В. В.* Корреляционная иммунность и реальная секретность // Математика и безопасность информационных технологий. Материалы конф. в МГУ 23–24 октября 2003 г. М.: МЦНМО, 2004. С. 165–171.
13. *Панков К. Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. Т. 5. Вып. 4. С. 73–97.
14. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.
15. *Сачков В. Н.* Комбинаторные свойства дифференциально 2-равномерных подстановок // Математические вопросы криптографии. 2015. Т. 6. Вып. 1. С. 159–179.
16. *Селезнева С. Н.* Мультипликативная сложность некоторых функций алгебры логики // Дискретная математика. 2014. Т. 26. Вып. 4. С. 100–109.
17. *Смышляев С. В.* О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. 2010. № 1. С. 5–15.
18. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики. 1994. Т. 1. Вып. 1. С. 33–55.
19. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математич. вопросы кибернетики. 2002. Вып. 11. С. 91–148.
20. *Токарева Н. Н.* Симметричная криптография. Краткий курс: учеб. пособие. Новосибирск: Новосибирский государственный университет, 2012. 232 с.
21. *Bilgin B., Nikova S., Nikov V., et al.* Threshold implementations of small S-boxes // Cryptography and Communications. 2015. V. 7. No. 1. P. 3–33.

22. *Blondeau C. and Nyberg K.* Perfect nonlinear functions and cryptography // Finite Fields and their Applications. 2015. V. 32. P. 120–147.
23. *Braeken A.* Cryptographic Properties of Boolean Functions and S-boxes. PhD Thesis, Katholieke Universiteit Leuven, 2006.
24. *Carlet C.* Boolean functions for cryptography and error correcting codes // Ch. 8 of the Monograph "Boolean Methods and Models in Mathematics, Computer Science, and Engineering", Cambridge Univ. Press, 2010. P. 257–397.
25. *Carlet C.* Vectorial Boolean functions for cryptography // Ch. 9 of the Monograph "Boolean Methods and Models in Mathematics, Computer Science, and Engineering", Cambridge Univ. Press, 2010. P. 398–472.
26. *Carlet C., Charpin P., and Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Des. Codes Cryptogr. 1998. V. 15. P. 125–156.
27. *Charpin P.* Normal Boolean functions // J. Complexity. 2004. V. 20. P. 245–265.
28. *Courtois N., Hulme D., and Mourouzis T.* Solving Circuit Optimisation Problems in Cryptography and Cryptanalysis. Cryptology ePrint Archive. Report 2011/475 (2011).
29. *Courtois N. and Meier W.* Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345–359.
30. *Cusick T. W. and Stănică P.* Cryptographic Boolean Functions and Applications. Acad. Press. Elsevier, 2009. 245 p.
31. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // FSE'95. LNCS. 1995. V. 1008. P. 61–74.
32. *Evertse J. H.* Linear structures in block ciphers // EUROCRYPT'87. LNCS. 1988. V. 304. P. 249–266.
33. *Fon-Der-Flaass D. G.* A bound on correlation immunity // Siberian Elektron. Mat. Izv. 2007. No. 4. P. 133–135.
34. *Golić J. Dj.* On the security of nonlinear filter generators // FSE'96. LNCS. 1996. V. 1039. P. 173–188.
35. *Gorodilova A.* On a Remarkable Property of APN Gold Functions. Cryptology ePrint Archive. Report 2016/286 (2016).
36. *Mihaljevic M., Gangopadhyay S., Paul G., and Imai H.* An algorithm for the internal state recovery of Grain-v1 // Proc. CECC'2011. Debrecen, Hungary, June 30–July 2, 2011. P. 7–20.
37. *Nikova S., Rechberger C., and Rijmen V.* Threshold implementations against side-channel attacks and glitches // LNCS. 2006. V. 4307. P. 529–545.
38. *Nyberg K.* Differentially uniform mappings for cryptography // Eurocrypt'93. LNCS. 1994. V. 765. P. 55–64.
39. *Preneel B., Van Leekwijck W., Van Linden L., et al.* Propagation characteristics of Boolean functions // Eurocrypt'90. LNCS. 1991. V. 473. P. 161–173.
40. *Siegenthaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. V. 30. No. 5. P. 776–780.
41. *Tarannikov Y. V.* Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters // Siberian Elektron. Mat. Izv. 2014. No. 11. P. 229–245.
42. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015. 220 p.
43. *Webster A. F. and Tavares S. E.* On the design of S-boxes // Crypto'85. LNCS. 1986. V. 218. P. 523–534.

44. *Zajac P. and Jokay M.* Multiplicative complexity of bijective 4×4 S-boxes // Cryptography and Communications. 2014. V. 6. No. 3. P. 255–277.

45. *Zhang X.-M. and Zheng Y.* GAC — the criterion for Global Avalanche Characteristics of cryptographic functions // J. Universal Computer Science. 1995. V. 1. No. 5. P. 320–337.

REFERENCES

1. *Agibalov G. P.* Izbrannye teoremy nachal'nogo kursa kriptografii: ucheb. posobie [Selected Theorems of Basic Cryptography Course: Tutorial]. Tomsk, NTL Publ., 2005. (in Russian)

2. *Agibalov G. P.* Metody resheniya sistem polinomial'nykh uravneniy nad konechnym polem [Methods for solving systems of polynomial equations over a finite field]. Vestnik Tomskogo Gosudarstvennogo Universiteta. Prilozhenie, 2006, no. 17, pp. 4–9. (in Russian)

3. *Agibalov G. P.* Logicheskie uravneniya v kriptoanalize generatorov klyuchevogo potoka [Logical equations in cryptanalysis of key stream generators]. Vestnik Tomskogo Gosudarstvennogo Universiteta. Prilozhenie, 2003, no. 6, pp. 31–41. (in Russian)

4. *Agibalov G. P. and Pankratova I. A.* Elementy teorii statisticheskikh analogov diskretnykh funktsiy s primeneniem v kriptoanalize iterativnykh blochnykh shifrov [Statistical approximation theory for discrete functions with application in cryptanalysis of iterative block ciphers]. Prikladnaya Diskretnaya Matematika, 2010, no. 3, pp. 51–68. (in Russian)

5. *Alferov A. P., Zubov A. Yu., Kuz'min A. S., and Cheremushkin A. V.* Osnovy Kriptografii [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2002. (in Russian)

6. *Buryakov M. L.* Algebraicheskie, kombinatornye i kriptograficheskie svoystva parametrov affinnykh ogranicheniy bulevykh funktsiy [Algebraic, Combinatorial, and Cryptographic properties of Parameters of Boolean Functions Affine Restrictions]. PhD Thesis, Moscow, 2007. (in Russian)

7. *Glukhov M. M.* O sovershenno i pochti sovershenno nelineynykh funktsiyakh [About perfectly and almost perfectly non-linear functions]. Matematicheskie Voprosy Kriptografii, 2016. (to be published) (in Russian)

8. *Glukhov M. M.* Planarnye otobrazheniya konechnykh poley i ikh obobshcheniya [On planar maps and their generalisation to finite fields]. Pres. conf. "Algebra and Logic, Theory and Applications", Krasnoyarsk, 21–27 July 2013.

9. *Gorodilova A. A.* Kharakterizatsiya pochti sovershenno nelineynykh funktsiy cherez podfunktsii [Characteristics of almost perfectly non-linear functions by subfunctions]. Diskr. Mat., 2015, vol. 27, no. 3, pp. 3–16. (in Russian)

10. *Lobanov M. S.* Tochnoe sootnoshenie mezhdu nelineynost'yu i algebraicheskoy immunnost'yu [Exact relation between nonlinearity and algebraic immunity]. Diskr. Mat., 2006, vol. 18, no. 3, pp. 152–159. (in Russian)

11. *Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2012. (in Russian)

12. *Logachev O. A., Sal'nikov A. A., and Yashchenko V. V.* Korrelyatsionnaya immunnost' i real'naya sekretnost' [Correlation immunity and real privacy]. Proc. conf. "Mathematics and Security of Information Technologies", Moscow, MCCME Publ., 2004, pp. 165–171. (in Russian)

13. *Pankov K. N.* Asimptoticheskie otsenki dlya chisel dvoichnykh otobrazheniy s zadannymi kriptograficheskimi svoystvami [Asymptotic estimates for numbers of Boolean mappings with given cryptographic properties]. Mat. Vopr. Kriptogr., 2014, vol. 5, iss. 4, pp. 73–97. (in Russian)

14. *Pankratova I. A.* Bulevy funktsii v kriptografii: ucheb. posobie [Boolean Functions in Cryptography: Tutorial]. Tomsk, TSU Publ., 2014. (in Russian)

15. *Sachkov V. N.* Kombinatornye svoystva differentsial'no 2-ravnomernykh podstanovok [Combinatorial properties of differentially 2-uniform substitutions]. Mat. Vopr. Kriptogr., 2015, vol. 6, iss. 1, pp. 159–179. (in Russian)
16. *Selezneva S. N.* Mul'tiplikativnaya slozhnost' nekotorykh funktsiy algebry logiki [Multiplicative complexity of some Boolean functions]. Diskr. Mat., 2014, vol. 26, iss. 4, pp. 100–109. (in Russian)
17. *Smyshlyaev S. V.* O kriptograficheskikh slabostyakh nekotorykh klassov preobrazovaniy dvoichnykh posledovatel'nostey [On cryptographic weaknesses of some classes of binary sequence transformations]. Prikladnaya Diskretnaya Matematika, 2010, no. 1, pp. 5–15. (in Russian)
18. *Sumarokov S. N.* Zaprety dvoichnykh funktsiy i obratimost' dlya odnogo klassa kodiruyushchikh ustroystv [Prohibitions of binary functions and reversibility for a class of encoders]. Obozrenie Prikladnoy i Promyshlennoy Matematiki, 1994, vol. 1, no. 1, pp. 33–55. (in Russian)
19. *Tarannikov Yu. V.* O korrelyatsionno-immunnykh i ustoychivykh bulevykh funktsiyakh [On correlation-immune and resilient Boolean functions]. Mat. Voprosy Kibernetiki, 2002, vol. 11, pp. 91–148. (in Russian)
20. *Tokareva N. N.* Simmetrichnaya kriptografiya. Kratkiy kurs: ucheb. posobie. [Symmetric Cryptography. Short Course: Tutorial]. Novosibirsk, NSU Publ., 2012. (in Russian)
21. *Bilgin B., Nikova S., Nikov V., et al.* Threshold implementations of small S-boxes. Cryptography and Communications, 2015, vol. 7, no. 1, pp. 3–33.
22. *Blondeau C. and Nyberg K.* Perfect nonlinear functions and cryptography. Finite Fields and their Applications, 2015, vol. 32, pp. 120–147.
23. *Braeken A.* Cryptographic Properties of Boolean Functions and S-boxes. PhD Thesis, Katholieke Universiteit Leuven, 2006.
24. *Carlet C.* Boolean functions for cryptography and error correcting codes. Ch. 8 of the Monograph "Boolean Methods and Models in Mathematics, Computer Science, and Engineering", Cambridge Univ. Press, 2010, pp. 257–397.
25. *Carlet C.* Vectorial Boolean functions for cryptography. Ch. 9 of the Monograph "Boolean Methods and Models in Mathematics, Computer Science, and Engineering", Cambridge Univ. Press, 2010, pp. 398–472.
26. *Carlet C., Charpin P., and Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr., 1998, vol. 15, pp. 125–156.
27. *Charpin P.* Normal Boolean functions. J. Complexity, 2004, vol. 20, pp. 245–265.
28. *Courtois N., Hulme D., and Mourouzis T.* Solving Circuit Optimisation Problems in Cryptography and Cryptanalysis. Cryptology ePrint Archive. Report 2011/475 (2011).
29. *Courtois N. and Meier W.* Algebraic attack on stream ciphers with linear feedback. LNCS, 2003, vol. 2656, pp. 345–359.
30. *Cusick T. W. and Stănică P.* Cryptographic Boolean Functions and Applications. Acad. Press. Elsevier, 2009. 245 p.
31. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity. FSE'95, LNCS, 1995, vol. 1008, pp. 61–74.
32. *Evertse J. H.* Linear structures in block ciphers. EUROCRYPT'87, LNCS, 1988, vol. 304, pp. 249–266.
33. *Fon-Der-Flaass D. G.* A bound on correlation immunity. Siberian Elektron. Mat. Izv., 2007, no. 4, pp. 133–135.
34. *Golić J. Dj.* On the security of nonlinear filter generators. FSE'96, LNCS, 1996, vol. 1039, pp. 173–188.

35. *Gorodilova A.* On a Remarkable Property of APN Gold Functions. Cryptology ePrint Archive. Report 2016/286 (2016).
36. *Mihaljevic M., Gangopadhyay S., Paul G., and Imai H.* An algorithm for the internal state recovery of Grain-v1. Proc. CECC'2011 Debrecen, Hungary, June 30–July 2, 2011, pp. 7–20.
37. *Nikova S., Rechberger C., and Rijmen V.* Threshold implementations against side-channel attacks and glitches. LNCS, 2006, vol. 4307, pp. 529–545.
38. *Nyberg K.* Differentially uniform mappings for cryptography. Eurocrypt'93, LNCS, 1994, vol. 765, pp. 55–64.
39. *Preneel B., Van Leekwijck W., Van Linden L., et al.* Propagation characteristics of Boolean functions. Eurocrypt'90, LNCS, 1991, vol. 473, pp. 161–173.
40. *Siegenthaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, 1984, V. 30, no. 5, pp. 776–780.
41. *Tarannikov Y. V.* Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters. Siberian Elektron. Mat. Izv., 2014, no. 11, pp. 229–245.
42. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015. 220 p.
43. *Webster A. F. and Tavares S. E.* On the design of S-boxes. Crypto'85, LNCS, 1986, vol. 218, pp. 523–534.
44. *Zajac P. and Jokay M.* Multiplicative complexity of bijective 4×4 S-boxes. Cryptography and Communications, 2014, vol. 6, no. 3, pp. 255–277.
45. *Zhang X.-M. and Zheng Y.* GAC — the criterion for Global Avalanche Characteristics of cryptographic functions. J. Universal Computer Science, 1995, vol. 1, no. 5, pp. 320–337.