

О квадратичных аппроксимациях в блочных шифрах<sup>1</sup>

Н. Н. Токарева

Рассматриваются квадратичные аппроксимации (булевых функций) специального вида и их возможные приложения в криптоанализе блочных шифров. Показано, что использование  $k$ -бент-функций в качестве функций шифрования предельно повышает стойкость шифра к таким аппроксимациям. Рассмотрены примеры четырехразрядных подстановок, рекомендованных для использования в S-блоках алгоритмов ГОСТ 28147-89, DES,  $s^3$ DES; показано, что практически во всех случаях существуют более вероятные (по сравнению с линейными) квадратичные соотношения специального вида на входные и выходные биты этих подстановок.

## § 1 Введение

**Линейный криптоанализ.** Метод линейного криптоанализа (ЛК) для блочного шифра FEAL был предложен М. Мацуи и А. Ямагиши [1] в 1992 году, для шифра DES — М. Мацуи [2] в 1993 году; в настоящее время этот метод наряду с методом дифференциального криптоанализа [3] считается одним из наиболее эффективных. Идея метода состоит в следующем. Вначале для известного алгоритма шифрования определяется линейное соотношение  $L$  на биты открытого текста, шифротекста и ключа, выполняющееся с вероятностью  $p = 1/2 + \varepsilon$ , достаточно сильно отличающейся от  $1/2$ . Затем при фиксированном неизвестном ключе  $K$  криптоаналитиком собирается статистика из  $N$  пар {открытый текст — соответствующий шифротекст}, и на ее основе с учетом знака  $\varepsilon$  производится различение двух простых статистических гипотез: выполняется ли соотношение  $L$  для данного неизвестного ключа  $K$  или нет. В результате для битов ключа  $K$  устанавливается новое вероятностное соотношение. Для надежной работы этого метода мощность статистики  $N$  должна быть пропорциональна величине  $|\varepsilon|^{-2}$ .

Большое число работ посвящено различным обобщениям и применениям метода ЛК. Перечислим некоторые из них. Детальное исследование метода ЛК (в частности для DES) провела К. Ниберг [4]; см. также работы [5–8]. Для повышения эффективности метода ЛК в [9] было предложено для одной комбинации битов ключа рассматривать одновременно несколько линейных аппроксимаций; эту тему продолжает работа [10]. Авторы [11] привели способ улучшения метода ЛК (в частности для шифра LOKI91), предложив учитывать при аппроксимации вероятностное поведение некоторых битов вместо их фиксированных значений. К числу последних работ о развитии метода ЛК можно отнести [12] и [13].

Серия работ посвящена вопросам стойкости различных алгоритмов шифрования к методу линейного криптоанализа. Л. Кнудсен [14] рассматривал вопросы построения схем шифрования типа Фейстеля, стойких к методам линейного и дифференциального криптоанализа. В. В. Шорин, В. В. Железняков, Э. М. Габидулин [15] доказали в 2001 году стойкость к этим методам российского алгоритма ГОСТ 28147-89 (с не менее, чем

<sup>1</sup>Исследование выполнено при финансовой поддержке интеграционного проекта СО РАН N 35 «Древовидный каталог математических Интернет-ресурсов mathtree.ru», Российского фонда фундаментальных исследований (проекты 07-01-00248, 08-01-00671) и Фонда содействия отечественной науке.

пятью раундами шифрования — при линейном криптоанализе и семью раундами — при дифференциальном). Исследования стойкости шифров RC5, RC6, IDEA, Serpent, AES, Blowfish, Khufu к методу ЛК см. в работах [16–20].

Другие работы посвящены исследованию различных классов аппроксимирующих функций и построению функций наиболее плохо поддающихся таким аппроксимациям. В этих работах рассматриваются *бент-функции* [21] — булевы функции от четного числа переменных, максимально удаленные в метрике Хэмминга от множества всех линейных функций, см. обзоры [22–23], и их обобщения: *полу-бент-функции* [24], *частично бент-функции* [22],  $\mathbb{Z}$ -*бент-функции* [25], *однородные бент-функции* [26], *гипер-бент-функции* [27–31], *нега-бент-функции* [32] и др.

**Нелинейный криптоанализ.** Общий подход к использованию в линейном криптоанализе нелинейных аппроксимаций предложили в 1996 году Л. Кнудсен и М. Робшау [33]. Основная идея его проста: обогатить класс аппроксимирующих функций (от  $m$  переменных) нелинейными функциями и за счет этого повысить качество аппроксимации. Но при этом криптоаналитику придется столкнуться со следующими трудностями:

*Как эффективно выбрать хорошую нелинейную аппроксимацию?* В линейном случае возможно решение такой задачи перебором всех  $2^m$  линейных функций. В общем случае полный перебор  $2^{2^m}$  булевых функций неосуществим даже при малых значениях  $m$ .

*Как объединить нелинейные аппроксимации отдельных раундов?* Рассмотрим простой пример. Пусть  $i$ -й раунд шифрования, переводящий промежуточный шифротекст  $C^{(i-1)}$  в  $C^{(i)}$ , устроен таким образом:  $C^{(i)} = S^i(C^{(i-1)} \oplus K^{(i)})$ , где  $K^{(i)}$  — подключ  $i$ -го раунда,  $S^i$  — известное нелинейное преобразование. Пусть, криптоаналитик установил приближение преобразования  $S^i$  функцией  $f^i$ , т. е. с достаточно высокой вероятностью выполняется равенство  $S^i(\mathbf{x}) = f^i(\mathbf{x})$  для произвольного  $\mathbf{x}$ . Тогда, если функция  $f^i$  линейна, то для  $i$ -го раунда имеем приближение  $C^{(i)} = f^i(C^{(i-1)} \oplus K^{(i)}) = f^i(C^{(i-1)}) \oplus f^i(K^{(i)})$ . Поскольку зависимость от блока  $C^{(i-1)}$  и подключа  $K^{(i)}$  здесь выделена явно, такое приближение  $i$ -го раунда может участвовать в общей цепочке раундовых приближений. В общем случае объединение раундовых приближений затруднено.

В направлении решения первой проблемы можно отметить исследования Т. Симоямы и Т. Канеко [34], связанные с поиском квадратичных соотношений для конкретных подстановок, использующихся в S-блоках DES; экспериментальные исследования Дж. Накахары и др. [35]; работу Ж. Тапиадора и др. [36] по применению эвристических алгоритмов для поиска хороших нелинейных аппроксимаций (с примерами для S-блоков шифра MARS). Вероятностные аспекты приближения случайной булевой функции множеством всех квадратичных функций исследовались в [37]. Вопросы нелинейных аппроксимаций булевых функций (с использованием их приведенного представления) рассматривались А. В. Ивановым [38]. Работы, направленные на решение второй проблемы, автору не известны.

В целом метод нелинейного криптоанализа не получил пока должного развития.

**Квадратичный криптоанализ.** В данной статье исследуются возможности квадратичного криптоанализа блочных шифров, в основу которого положены квадратичные аппроксимации специального вида. А именно, в работе [39] для каждого целого  $k$ ,  $1 \leq k \leq m/2$ , была определена бинарная операция  $\langle \cdot, \cdot \rangle_k$  на множестве векторов  $\mathbb{Z}_2^m$ , которую, исходя из ее свойств, можно считать аналогом скалярного произведения векторов над  $\mathbb{Z}_2$ . Определение было дано в рамках теоретико-кодového подхода; при этом по существу использовалась классификация  $\mathbb{Z}_4$ -линейных кодов типа Адамара, полу-

ченная Д. С. Кротовым [40], [41]. При фиксированном векторе  $\mathbf{u} \in \mathbb{Z}_2^m$  функция  $\langle \mathbf{u}, \mathbf{v} \rangle_k$  от переменных  $v_1, \dots, v_m$  является линейной или квадратичной (см. § 2). В работе предлагается вести аппроксимацию всеми функциями вида  $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$ , где  $\pi$  — любая перестановка на  $m$  координатах, параметры  $\mathbf{u}, k$  произвольны. Множество таких функций состоит из  $2^m$  (т.е. всех) линейных функций и не более чем  $2^{m(1+\log_2 m)}$  квадратичных функций, что не ограничивает криптоаналитика в возможности их полного перебора (см. § 3). Выбор таких функций обусловлен наличием простых формул для вычисления расстояния Хэмминга от произвольной булевой функции до класса функций  $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$  при фиксированных  $\pi$  и  $k$ , а также свойствами таких функций, близкими к линейным.

Работа носит теоретический характер. Предложены модификации алгоритмов 1 и 2 линейного криптоанализа Мацуи [2] для расширенного класса аппроксимирующих функций. Приведены формулы для вычисления абсолютных значений преобладаний и надежности алгоритмов. Показано, что использование  $k$ -бент-функций в качестве функций шифрования позволяет снижать максимальное абсолютное значение преобладания до его минимального значения, а следовательно предельно повышать стойкость шифра к данным квадратичным аппроксимациям (см. § 4). Рассмотрены примеры четырехразрядных подстановок, рекомендованных для применения в узлах замены (S-блоках) алгоритмов ГОСТ 28147-89, DES,  $s^3$ DES; с помощью компьютера показано, что для всех этих подстановок (кроме одной) существуют более вероятные (по сравнению с линейными) квадратичные соотношения специального вида на входные и выходные биты этих подстановок (см. § 5). Свойства аппроксимирующих функций, которые могут быть использованы при согласовании нелинейных раундовых аппроксимаций рассмотрены в § 6. Практические результаты по применению квадратичных аппроксимаций в криптоанализе будут представлены в одной из следующих публикаций автора.

## § 2 Операция $\langle \cdot, \cdot \rangle_k$

В данном параграфе, следуя [39], приведем ряд необходимых определений. Пусть  $m$  — целое,  $\mathfrak{F}_m$  — класс всех булевых функций от  $m$  переменных. Двоичные векторы будем выделять полужирным шрифтом. Пусть  $\mathbf{v} = (v_1, \dots, v_m)$ ,  $\mathbf{u} = (u_1, \dots, u_m)$ , где  $u_i, v_i \in \mathbb{Z}_2$ . Определим бинарную операцию  $\langle \cdot, \cdot \rangle_k : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$  при любом целом  $k$ ,  $1 \leq k \leq m/2$ , следующим образом:

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \left( \bigoplus_{i=1}^k \bigoplus_{j=i}^k (u_{2i-1} \oplus u_{2i})(u_{2j-1} \oplus u_{2j})(v_{2i-1} \oplus v_{2i})(v_{2j-1} \oplus v_{2j}) \right) \oplus \langle \mathbf{u}, \mathbf{v} \rangle, \quad (1)$$

где  $\langle \cdot, \cdot \rangle$  — обычное скалярное произведение двоичных векторов над  $\mathbb{Z}_2$ , т.е.

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 \oplus \dots \oplus u_m v_m,$$

и символ  $\oplus$  обозначает сложение по модулю 2. Заметим, что координаты  $u_1, \dots, u_m$  (также как и  $v_1, \dots, v_m$ ) участвуют в операции  $\langle \cdot, \cdot \rangle_k$  неравноправно. А именно при данном  $k$  в точности  $2k$  первых координат каждого из векторов  $\mathbf{u}, \mathbf{v}$  входят в квадратичные и линейные слагаемые; остальные координаты — только в линейные. Из определения следует, что

$$\langle \mathbf{u}, \mathbf{v} \rangle_1 = \langle \mathbf{u}, \hat{\mathbf{v}} \rangle, \quad (2)$$

где  $\hat{\mathbf{v}}$  получен из вектора  $\mathbf{v}$  перестановкой координат  $v_1$  и  $v_2$ . Очевидно также, что  $\langle \mathbf{u}, \mathbf{v} \rangle_k = \langle \mathbf{v}, \mathbf{u} \rangle_k$  и  $\langle a\mathbf{u}, \mathbf{v} \rangle_k = a\langle \mathbf{v}, \mathbf{u} \rangle_k$  для любого  $a \in \mathbb{Z}_2$ . В качестве примера приведем выражение для операции  $\langle \mathbf{u}, \mathbf{v} \rangle_2$  при  $m = 4$ :

$$\langle \mathbf{u}, \mathbf{v} \rangle_2 = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1 \oplus v_2)(v_3 \oplus v_4) \oplus u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4. \quad (3)$$

Бинарная операция  $\langle \cdot, \cdot \rangle_k$  была определена в работе [39], там же исследованы ее свойства, позволяющие считать эту операцию аналогом скалярного произведения. Целочисленная функция  $W_f^{(k)}$ , заданная на множестве  $\mathbb{Z}_2^m$  равенством

$$W_f^{(k)}(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus f(\mathbf{u})} \text{ для любого } \mathbf{v} \in \mathbb{Z}_2^m,$$

называется  $k$ -преобразованием Уолша—Адамара булевой функции  $f \in \mathfrak{F}_m$ . Для  $W_f^{(k)}$  согласно [39] имеет место аналог равенства Парсеваля:

$$\sum_{\mathbf{v} \in \mathbb{Z}_2^m} \left( W_f^{(k)}(\mathbf{v}) \right)^2 = 2^{2m}, \text{ при любой } f \in \mathfrak{F}_m,$$

и следовательно, при любом  $k$  и любой  $f \in \mathfrak{F}_m$  справедливо

$$\max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f^{(k)}(\mathbf{v})| \geq 2^{m/2}. \quad (4)$$

Напомним, что расстояние Хэмминга  $\text{dist}(\cdot, \cdot)$  между булевыми функциями от  $m$  переменных определяется как число позиций, в которых различаются их векторы значений. Если функция  $g_{\mathbf{u}}^{(k)}$  задана равенством  $g_{\mathbf{u}}^{(k)}(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k$ , то справедливы равенства:

$$\text{dist}(f, g_{\mathbf{u}}^{(k)}) = 2^{m-1} - \frac{1}{2} W_f^{(k)}(\mathbf{u}),$$

$$\text{dist}(f, g_{\mathbf{u}}^{(k)} \oplus 1) = 2^{m-1} + \frac{1}{2} W_f^{(k)}(\mathbf{u}).$$

Расстояние между функцией  $f$  и множеством функций  $\{\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a \mid \mathbf{u} \in \mathbb{Z}_2^m, a \in \mathbb{Z}_2\}$  от переменных  $v_1, \dots, v_m$  называется  $k$ -нелинейностью функции  $f$ ; обозначим его через  $N_f^{(k)}$ . Имеет место формула

$$N_f^{(k)} = 2^{m-1} - \frac{1}{2} \max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f^{(k)}(\mathbf{v})|,$$

а значит  $k$ -нелинейность функции  $f$  не превышает величины  $2^{m-1} - 2^{(m/2)-1}$ . При четном  $m$  булева функция  $f \in \mathfrak{F}_m$  называется  $k$ -бент-функцией, если все коэффициенты  $W_f^{(j)}(\mathbf{v})$ ,  $j = 1, \dots, k$ ,  $\mathbf{v} \in \mathbb{Z}_2^m$ , равны  $\pm 2^{m/2}$ . Другими словами,  $k$ -бент-функция — это функция, у которой каждый параметр нелинейности  $N_f^{(j)}$ ,  $j = 1, \dots, k$ , принимает свое максимальное возможное значение  $2^{m-1} - 2^{(m/2)-1}$ . Пусть  $\mathfrak{B}_m^k$  — класс всех  $k$ -бент-функций от  $m$  переменных. Нетрудно показать, что  $\mathfrak{B}_m^1$  совпадает с классом обычных бент-функций. Справедливы строгие включения  $\mathfrak{B}_m^1 \supset \dots \supset \mathfrak{B}_m^{m/2}$ , причем множество  $\mathfrak{B}_m^{m/2}$  непусто. Методы построения  $k$ -бент-функций можно найти в [39], [42].

### § 3 Класс аппроксимирующих функций

Рассмотрим следующий класс булевых функций от переменных  $v_1, \dots, v_m$ , где  $m$  четно. Для любого  $k$ ,  $1 \leq k \leq m/2$ , и произвольной перестановки  $\pi \in S_m$  на  $m$  переменных пусть

$$\mathfrak{A}_{m,0}^k(\pi) = \{\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k \mid \mathbf{u} \in \mathbb{Z}_2^m\}.$$

Заметим, что для любой перестановки  $\pi \in S_m$  множество  $\mathfrak{A}_{m,0}^1(\pi)$  состоит из всех линейных функций. Булевы функции от переменных  $v_1, \dots, v_m$ , используемые при шифровании, будем аппроксимировать функциями из множества

$$\Delta_m = \bigcup_{1 \leq k \leq m/2} \bigcup_{\pi \in S_m} \mathfrak{A}_{m,0}^k(\pi),$$

которое всюду далее называем *классом аппроксимирующих функций*. Говоря неформально, за счет произвольных перестановок  $\pi$  переменных  $v_1, \dots, v_m$  мы снимаем «неравноправие» этих переменных в функции  $\langle \mathbf{u}, \mathbf{v} \rangle_k$ .

Определим мощность класса  $\Delta_m$  и способ перечисления его элементов. Основную трудность здесь представляет тот факт, что множества  $\mathfrak{A}_{m,0}^{k'}(\pi')$  и  $\mathfrak{A}_{m,0}^{k''}(\pi'')$ , вообще говоря, имеют непустое пересечение.

Для булевой функции  $f \in \mathfrak{F}_m$  пусть множество АНФ( $f$ ) состоит из всех одночленов ее алгебраической нормальной формы (иначе ее называют *полиномиальной формой* или *многочленом Жегалкина* функции). Например, для функции  $g(v_1, v_2, v_3, v_4) = v_1 v_2 \oplus v_1 v_3 \oplus v_1 v_4 \oplus v_2 v_3 \oplus v_3 v_4 \oplus v_2 \oplus v_3 \oplus 1$  имеем  $\text{АНФ}(g) = \{v_1 v_2, v_1 v_3, v_1 v_4, v_2 v_3, v_3 v_4, v_2, v_3, 1\}$ . При фиксированной перестановке  $\pi \in S_m$  через  $f^\pi$  обозначим булеву функцию, заданную равенством  $f^\pi(\mathbf{v}) = f(\pi(\mathbf{v}))$ . Переменные булевой функции  $f \in \mathfrak{F}_m$  разобьем на пары; паре  $\{v_{2i-1}, v_{2i}\}$  сопоставим номер  $i$ . Через  $\text{Act}(f)$  обозначим подмножество максимальной мощности множества  $\{1, 2, \dots, m/2\}$  такое, что для любых различных элементов  $i, j$  из  $\text{Act}(f)$  одночлены  $v_{2i-1} v_{2j-1}$ ,  $v_{2i-1} v_{2j}$ ,  $v_{2i} v_{2j-1}$ ,  $v_{2i} v_{2j}$  принадлежат множеству АНФ( $f$ ). Будем говорить, что пара переменных с номером  $i$  *активна* для  $f$ , если  $i \in \text{Act}(f)$ . Заметим, что мощность  $\text{Act}(f)$  для любой функции  $f$  либо нулевая, либо не меньше двух. Через  $\rho = \rho(f)$  обозначим любую перестановку из  $S_m$  такую, что  $|\text{Act}(f^\rho)| = \max_{\pi \in S_m} |\text{Act}(f^\pi)|$ . Рассмотрим, например, множество  $\text{Act}(g)$  для функции  $g$ , заданной выше. Поскольку одночлены  $v_1 v_3$ ,  $v_1 v_4$ ,  $v_2 v_3$  принадлежат АНФ( $g$ ), а одночлен  $v_2 v_4$  — нет, имеем  $\text{Act}(g) = \emptyset$ . Однако, при  $\rho = (1, 3, 2, 4)$  имеем  $\text{Act}(g^\rho) = \{1, 2\}$ .

**Теорема 1.** *Булева функция  $f \in \mathfrak{F}_m$ , степени не больше двух, такая что  $f(\mathbf{0}) = 0$ , принадлежит классу  $\Delta_m$  тогда и только тогда, когда  $f$  удовлетворяет условиям*

- 1) для любых различных чисел  $i, j$  ( $1 \leq i, j \leq m/2$ ) одночлены

$$v_{2i-1} v_{2j-1}, v_{2i-1} v_{2j}, v_{2i} v_{2j-1}, v_{2i} v_{2j}$$

*одновременно либо принадлежат, либо не принадлежат множеству АНФ( $f^\rho$ );*

- 2) *множество АНФ( $f^\rho$ ) не содержит одночленов вида  $v_{2i-1} v_{2i}$ ;*

3) *если пара  $i$  активна для  $f^\rho$ , то в точности одна из переменных  $v_{2i-1}$ ,  $v_{2i}$  принадлежит АНФ( $f^\rho$ ).*

**Доказательство.** ( $\Leftarrow$ ) Пусть функция  $f$  степени не больше двух,  $f(\mathbf{0}) = 0$ , удовлетворяет условиям 1), 2), 3) теоремы. Если множество  $\text{Act}(f^\rho)$  пусто, то функция  $f$ , согласно 1) и 2) линейна и, следовательно, принадлежит множеству  $\Delta_m$ .

Предположим далее, что  $\text{Act}(f^\rho)$  не пусто и имеет вид  $\text{Act}(f^\rho) = \{i_1, \dots, i_k\}$ , где  $2 \leq k \leq m/2$ . Пусть  $j_1, \dots, j_{(m/2)-k}$  — номера неактивных пар переменных функции  $f^\rho$ . Рассмотрим перестановку  $\tau \in S_m$  такую, что  $\tau(i_s) = s$  для любого  $s = 1, \dots, k$  и  $\tau(j_s) = k + s$  для любого  $s = 1, \dots, (m/2) - k$ . Переставим пары переменных функции  $f^\rho$  согласно  $\tau$ . А именно рассмотрим функцию  $f^{\rho \circ \pi}$  (здесь и далее запись  $\rho \circ \pi$  означает, что сначала применяется перестановка  $\rho$ , а затем  $\pi$ ), где  $\pi \in S_m$  задается с помощью  $\tau$  следующим образом:  $\pi(2s - 1) = 2\tau(s) - 1$ ,  $\pi(2s) = 2\tau(s)$  для любого  $s = 1, \dots, m/2$ . Нетрудно заметить, что условия 1), 2), 3) после замены в каждом из них функции  $f^\rho$  на  $f^{\rho \circ \pi}$  остаются справедливыми, причем множество  $\text{Act}(f^{\rho \circ \pi}) = \{1, \dots, k\}$  также как и  $\text{Act}(f^\rho)$  имеет мощность  $k$ . Поэтому далее, без ограничения общности, считаем, что  $\text{Act}(f^\rho) = \{1, \dots, k\}$ .

Заметим, что число  $k$  согласно условиям 1) и 2) однозначно определяет квадратичную часть функции  $f^\rho$ , которая имеет вид

$$\bigoplus_{i=1}^{k-1} \bigoplus_{j=i+1}^k (v_{2i-1}v_{2j-1} \oplus v_{2i-1}v_{2j} \oplus v_{2i}v_{2j-1} \oplus v_{2i}v_{2j}). \quad (5)$$

Покажем, что функция  $f^\rho$  принадлежит множеству  $\mathfrak{A}_{m,0}^k$ . Рассмотрим вектор  $\mathbf{u} \in \mathbb{Z}_2^m$  такой, что

$$u_t = 1 \iff \begin{cases} v_t \notin \text{АНФ}(f^\rho), & \text{при } t = 1, \dots, 2k; \\ v_t \in \text{АНФ}(f^\rho), & \text{при } t = 2k + 1, \dots, m. \end{cases}$$

Тогда  $f^\rho(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k$ . Действительно, по определению  $\langle \mathbf{u}, \mathbf{v} \rangle_k$  имеем

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \left( \bigoplus_{i=1}^{k-1} \bigoplus_{j=i+1}^k Y_i Y_j \right) \oplus \left( \bigoplus_{i=1}^k (u_{2i}v_{2i-1} \oplus u_{2i-1}v_{2i}) \right) \oplus \left( \bigoplus_{i=k+1}^{m/2} (u_{2i-1}v_{2i-1} \oplus u_{2i}v_{2i}) \right), \quad (6)$$

где  $Y_i = (u_{2i-1} \oplus u_{2i})(v_{2i-1} \oplus v_{2i})$ . Используя условие 3) и определение вектора  $\mathbf{u}$ , получаем  $u_{2i-1} \oplus u_{2i} = 1$  при  $i = 1, \dots, k$ , а значит  $Y_i Y_j = v_{2i-1}v_{2j-1} \oplus v_{2i-1}v_{2j} \oplus v_{2i}v_{2j-1} \oplus v_{2i}v_{2j}$ , где  $1 \leq i < j \leq k$ . Таким образом, квадратичная часть функции  $\langle \mathbf{u}, \mathbf{v} \rangle_k$  совпадает с (5). Непосредственно из (6) получаем, что линейные части функций  $f^\rho$  и  $\langle \mathbf{u}, \mathbf{v} \rangle_k$  также совпадают. Следовательно, поскольку  $f^\rho(\mathbf{0}) = \langle \mathbf{u}, \mathbf{0} \rangle_k = 0$ , и обе функции  $f^\rho$  и  $\langle \mathbf{u}, \mathbf{v} \rangle_k$  имеют степень 2, они равны. Итак, мы показали, что функция  $f^\rho$  принадлежит классу  $\mathfrak{A}_{m,0}^k(\text{id})$ , где  $\text{id}$  обозначает тождественную перестановку. Осталось заметить, что справедливо

$$f^\sigma \in \mathfrak{A}_{m,0}^k(\text{id}) \iff f \in \mathfrak{A}_{m,0}^k(\sigma^{-1}), \text{ для любой перестановки } \sigma \in S_m,$$

что вытекает из следующей эквивалентности:

$$\exists \mathbf{u} : f^\sigma(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k \iff \exists \mathbf{u} : f(\mathbf{v}) = \langle \mathbf{u}, \sigma^{-1}(\mathbf{v}) \rangle_k.$$

Отсюда, наконец, заключаем, что функция  $f$  принадлежит классу  $\mathfrak{A}_{m,0}^k(\rho^{-1})$ , а следовательно и классу  $\Delta_m$ .

( $\implies$ ) Если функция  $f$  линейна, то выполнение условий 1), 2), 3) очевидно. Пусть  $f$  имеет нетривиальную квадратичную часть. Тогда, поскольку  $f$  принадлежит некоторому классу  $\mathfrak{A}_{m,0}^k(\pi)$ , мощность квадратичной части  $f$  равна  $4 \cdot \binom{s}{2}$  для подходящего  $s$ ,  $2 \leq s \leq k$ , что непосредственно следует из определения  $\langle \mathbf{u}, \mathbf{v} \rangle_k$ . Так как  $f^\rho$  также

содержится в классе  $\Delta_m$ , то  $|\text{Act}(f^\rho)| = s$  (например, в качестве  $\rho$  можно взять перестановку  $\pi^{-1}$ ). Тогда квадратичная часть  $\text{АНФ}(f^\rho)$  исчерпывается одночленами вида  $v_{2i-1}v_{2j-1}$ ,  $v_{2i-1}v_{2j}$ ,  $v_{2i}v_{2j-1}$ ,  $v_{2i}v_{2j}$  для любых различных  $i, j \in \text{Act}(f^\rho)$ , и следовательно выполнены условия 1) и 2). Справедливость 3) вытекает из определения  $\langle \mathbf{u}, \mathbf{v} \rangle_k$ .  $\blacktriangle$

**Следствие 1.** Для любого четного  $m$  справедливо равенство

$$|\Delta_m| = 2^m \left( 1 + \sum_{k=2}^{m/2} \binom{m}{2k} \frac{(2k-1)!!}{2^k} \right).$$

**Доказательство.** Класс  $\Delta_m$  содержит ровно  $2^m$  линейных булевых функций. С помощью теоремы 1 для каждого фиксированного  $k$ ,  $2 \leq k \leq m/2$ , определим число квадратичных функций  $f$  из  $\Delta_m$  таких, что  $|\text{Act}(f^\rho)| = k$ . Каждая такая функция  $f$  однозначно определяется множеством из  $k$  неупорядоченных пар переменных (после действия соответствующей перестановки  $\rho$  все эти пары будут активными) и своей линейной частью. Множество из  $k$  неупорядоченных пар можно выбрать

$$\frac{1}{k!} \binom{m}{2} \binom{m-2}{2} \cdots \binom{m-2k+2}{2} = \frac{m!}{2^k k! (m-2k)!}$$

способами. Для любой выбранной пары переменных в точности одна переменная из пары входит в множество  $\text{АНФ}(f)$  согласно условию 3) теоремы 1. Переменные, не содержащиеся в выбранных парах, входят или не входят в  $\text{АНФ}(f)$  свободно. Таким образом, число функций  $f \in \Delta_m$ ,  $|\text{Act}(f^\rho)| = k$ , равно

$$\frac{m!}{2^k k! (m-2k)!} \cdot 2^k \cdot 2^{m-2k} = \binom{m}{2k} 2^{m-k} (2k-1)!!$$

Суммируя по всем  $k$ ,  $2 \leq k \leq m/2$ , и учитывая линейные функции, получаем требуемое выражение для мощности класса  $\Delta_m$ .  $\blacktriangle$

Например,  $|\Delta_4| = 28$ ,  $|\Delta_6| = 904$ ,  $|\Delta_8| = 28\,816$ , а число линейных функций в каждом из этих классов равно 16, 64 и 256 соответственно. Из следствия 1 несложно вывести, что величина  $|\Delta_m|$  не превышает числа  $e 2^m m!$ , что заведомо меньше, чем  $2^{m(1+\log_2 m)}$ . Отметим, что число всех квадратичных функций от  $m$  переменных пропорционально величине  $2^{m^2}$  и функции вида  $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$  составляют предельно малую их часть при  $m \rightarrow \infty$ .

Теорема 1 и следствие 1 предлагают способ перечисления всех элементов множества  $\Delta_m$  без повторений.

## § 4 Квадратичные аппроксимации в блочных шифрах

Основная идея предлагаемого подхода состоит в расширении области поиска наиболее вероятных соотношений для битов открытого текста, шифротекста и ключа: с множества линейных соотношений на множество линейных и квадратичных соотношений специального вида. В обозначениях будем следовать, в основном, книге [22].

Рассмотрим блочный шифр с  $r$  раундами шифрования. Пусть

$m = m_{\text{text}}$  — длина открытого текста и шифротекста;

$P$  — открытый текст,  $P \in \mathbb{Z}_2^m$ ;

$m_{\text{key}}$  — длина ключа;

$K$  — ключ шифрования,  $K \in \mathbb{Z}_2^{m_{\text{key}}}$ ;

$F : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m_{\text{key}}} \rightarrow \mathbb{Z}_2^m$  — преобразование, взаимно однозначное при любом фиксированном втором аргументе;

$C = F(P, K)$  — шифротекст,  $C \in \mathbb{Z}_2^m$ ;

$m'_{\text{key}}$  — длина раундового подключа;

$K^{(i)}$  — подключ  $i$ -го раунда шифрования,  $K^{(i)} \in \mathbb{Z}_2^{m'_{\text{key}}}$ ,  $1 \leq i \leq r$ , определяемый по ключу  $K$ ;

$F_i : \mathbb{Z}_2^m \times \mathbb{Z}_2^{m'_{\text{key}}} \rightarrow \mathbb{Z}_2^m$  — преобразование  $i$ -го раунда шифрования,  $1 \leq i \leq r$ , взаимно однозначное, если второй аргумент фиксирован;

$C^{(0)} = P$ ;

$C^{(i)} = F_i(C^{(i-1)}, K^{(i)})$  — промежуточный шифротекст,  $C^{(i)} \in \mathbb{Z}_2^m$ ,  $1 \leq i \leq r$ ;

$C = C^{(r)}$  — итоговый шифротекст;

Предполагаем, что все открытые тексты  $P$  (как и ключи  $K$ ) равновероятны. Всюду далее считается, что  $m$ ,  $m_{\text{key}}$ ,  $m'_{\text{key}}$  — четные числа.

**4.1. Первый алгоритм.** В основе алгоритма лежит следующее равенство

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = \langle \mathbf{d}, \tau(K) \rangle_k, \quad (7)$$

где

$\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^m$ ,  $\mathbf{d} \in \mathbb{Z}_2^{m_{\text{key}}}$  — некоторым образом выбранные векторы;

$\pi, \sigma \in S_m$ ,  $\tau \in S_{m_{\text{key}}}$  — фиксированные перестановки;

$i, j, k$  — целые числа такие, что  $1 \leq i, j \leq m/2$ ,  $1 \leq k \leq m_{\text{key}}/2$ .

Считаем, что равенство (7) выполняется с вероятностью  $p = 1/2 + \varepsilon$ , такой, что  $0 < |\varepsilon| \leq 1/2$ . Число  $\varepsilon$  назовем *преобладанием* равенства (7). Отдельной задачей для каждого конкретного алгоритма шифрования является выбор таких значений параметров  $\mathbf{a}, \mathbf{b}, \mathbf{d}, \pi, \sigma, \tau, i, j, k$ , чтобы величина  $|\varepsilon|$  была по возможности максимальной. В данной статье эта задача рассматриваться не будет. Отметим, что выбор параметров  $i, j, k$  отражается на виде соотношения (7) следующим образом. Если данный параметр ( $i, j$  или  $k$ ) равен 1, то биты соответствующего блока (открытого текста  $P$ , шифротекста  $C$  или ключа  $K$ ) входят в соотношение (7) линейно, что может быть использовано при добавлении такого соотношения в линейную систему уравнений. С ростом параметра ( $i, j$  или  $k$ ) пропорционально увеличивается число битов блока, участвующих в нелинейной части соотношения.

Пусть фиксирован ключ шифрования  $K$ . Рассмотрим набор

$$\{(P_t, C_t) \mid t = 1, \dots, N\}$$

известных пар открытого и шифрованного текстов,  $C_t = F(P_t, K)$ . Следующий алгоритм является модификацией алгоритма Мацуи [2] определения одного бита ключа, основанного на принципе максимального правдоподобия.



### Алгоритм 1

- определяем  $N_0 = | \{ t : \langle \mathbf{a}, \pi(P_t) \rangle_i \oplus \langle \mathbf{b}, \sigma(C_t) \rangle_j = 0 \} |$ ;
- полагаем  $\langle \mathbf{d}, \tau(K) \rangle_k = \begin{cases} 0, & \text{если } (N_0 - \frac{N}{2}) \cdot \varepsilon > 0; \\ 1, & \text{в другом случае;} \end{cases}$
- с учетом полученного соотношения подбираем ключ.

### Конец алгоритма

Напомним, что *надежностью*  $\xi_0$  алгоритма, основанного на процедуре статистической классификации, называется математическое ожидание вероятности его корректной работы. В данном случае под корректной работой алгоритма понимается установление верного соотношения на биты ключа. При этом предполагается, что искомый ключ выбран во всем пространстве ключей случайно, равновероятно и независимо от набора открытых текстов (см. подробнее [22]). Таким образом,

$$\xi_0 = \mathbf{E}\{\xi(K)\} = \frac{1}{2^{m_{\text{key}}}} \sum_{K \in \mathbb{Z}_2^{m_{\text{key}}}} \xi(K),$$

где  $\xi(K)$  — вероятность выбора открытых текстов  $P_1, \dots, P_N$  таких, что будет установлено верное соотношение на биты ключа  $K$ . Если  $p(K) = 1/2 + \varepsilon(K)$ , где  $\varepsilon(K) \neq 0$ , — вероятность выполнения равенства (7) для фиксированного ключа  $K$ , то

$$\xi(K) = \sum_{s=0}^{N/2} \binom{N}{s} \left( \frac{1}{2} - |\varepsilon(K)| \right)^s \left( \frac{1}{2} + |\varepsilon(K)| \right)^{N-s}.$$

Надежность  $\xi_0$  алгоритма 1 можно оценить в точности так же как и в случае линейного криптоанализа (с привлечением дополнительных криптографических предположений, см. подробнее [2], [22]) с помощью функции нормального распределения, а именно

$$\xi_0 \simeq \Phi_{0,1}(-2|\varepsilon|\sqrt{N}) = \int_{-2|\varepsilon|\sqrt{N}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy. \quad (8)$$

Приведем формулы для вычисления абсолютных значений преобладаний и выделим те свойства булевых функций, использующихся при шифровании, наличие которых придает шифру стойкость к рассматриваемым квадратичным аппроксимациям.

Для фиксированного ключа  $K$ , для любых целых  $i, j$ , таких что  $1 \leq i, j \leq m/2$ , для произвольных перестановок  $\pi, \sigma \in S_m$  обозначим через  $\varepsilon_{j,\mathbf{b},\sigma}^{i,\mathbf{a},\pi}(K; 0)$  действительное число из отрезка  $[-1/2, 1/2]$  такое, что вероятность выполнения равенства

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(P, K)) \rangle_j = 0 \quad (9)$$

равна  $1/2 + \varepsilon_{j,\mathbf{b},\sigma}^{i,\mathbf{a},\pi}(K; 0)$ .

**Утверждение 1.** Для любого отображения  $F(\cdot, K) : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$  и любых перестановок  $\pi, \sigma \in S_m$  выполняется равенство

$$2^{m+1} \cdot \varepsilon_{j,\mathbf{b},\sigma}^{i,\mathbf{a},\pi}(K; 0) = W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a}).$$

**Доказательство.** Пусть  $\mathbb{Z}_2^m = M_0 \cup M_1$ , где

$$M_x = \{\mathbf{u} \in \mathbb{Z}_2^m \mid \langle \mathbf{a}, \pi(\mathbf{u}) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(\mathbf{u}, K)) \rangle_j = x\}$$

при  $x = 0, 1$ . Из определения  $i$ -коэффициента Уолша — Адамара  $W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a})$  следует, что

$$W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{a}, \pi(\mathbf{u}) \rangle_i \oplus \langle \mathbf{b}, \sigma(F(\mathbf{u}, K)) \rangle_j} = |M_0| - |M_1|.$$

С помощью (9) получаем  $|M_0| = 2^m(1/2 + \varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0))$ , и следовательно

$$|M_0| - |M_1| = 2^{m+1} \cdot \varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0).$$

▲

Напомним, что  $\varepsilon(K)$  обозначает преобладание, с которым выполняется равенство (7) при фиксированном ключе  $K$ . Заметим, что для любых  $k, \mathbf{d}$  и  $\tau$  справедливо

$$|\varepsilon(K)| = |\varepsilon_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K; 0)|. \quad (10)$$

**Теорема 2.** Пусть фиксирован ключ  $K \in \mathbb{Z}_2^{m_{\text{key}}}$ . Если вектор  $\mathbf{b} \in \mathbb{Z}_2^m$ , перестановки  $\pi, \sigma \in S_m$  и параметр  $j$ ,  $1 \leq j \leq m/2$ , таковы что функция

$$\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$$

является  $(m/2)$ -бент-функцией, то справедливо равенство

$$\max_{i, k, \mathbf{a}, \mathbf{d}, \tau} |\varepsilon(K)| = \min_{i, k, \mathbf{a}, \mathbf{d}, \tau} |\varepsilon(K)| = 2^{-(m/2)-1}.$$

**Доказательство.** Поскольку функция  $\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j$  принадлежит классу  $\mathfrak{B}_m^{m/2}$ , имеем  $|W_{\langle \mathbf{b}, \sigma(F(\pi^{-1}(\cdot), K)) \rangle_j}^{(i)}(\mathbf{a})| = \pm 2^{m/2}$  для любого  $\mathbf{a} \in \mathbb{Z}_2^m$  и каждого  $i$ ,  $1 \leq i \leq m/2$ . Тогда из утверждения 1 и равенства (10) сразу следует, что для любых параметров  $k, \mathbf{d}$  и  $\tau$  все значения  $|\varepsilon(K)|$  равны  $2^{-(m/2)-1}$ , откуда и вытекает требуемое. ▲

Из неравенства (4) следует, что  $2^{-(m/2)-1}$  является минимальным возможным значением для  $\max_{\mathbf{a} \in \mathbb{Z}_2^m} |\varepsilon(K)|$  при любых фиксированных  $i, j, k, \mathbf{b}, \mathbf{d}, \pi, \sigma$  и  $\tau$ . Согласно теореме 2 это минимальное значение достижимо только при использовании  $(m/2)$ -бент-функций. Задача построения таких функций представляется автору весьма сложной.

**4.2. Второй алгоритм.** Рассмотрим модификацию улучшенного алгоритма Мацуи [2], основанную на исследовании промежуточных шифротекстов. Пусть выбраны целые числа  $s_1, s_2$ , такие, что  $0 \leq s_1 < s_2 \leq r$ . Рассмотрим равенство

$$\langle \mathbf{a}, \pi(C^{(s_1)}) \rangle_i \oplus \langle \mathbf{b}, \sigma(C^{(s_2)}) \rangle_j = \langle \tau(\mathbf{d}), K \rangle_k, \quad (11)$$

где  $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^m$ ,  $\mathbf{d} \in \mathbb{Z}_2^{m_{\text{key}}}$  — фиксированные векторы;  $\pi, \sigma \in S_m$ ,  $\tau \in S_{m_{\text{key}}}$  — заданные перестановки;  $i, j, k$  — целые числа такие, что  $1 \leq i, j \leq m/2$ ,  $1 \leq k \leq m_{\text{key}}/2$ . Будем считать, что (11) выполняется с вероятностью  $\tilde{p} = 1/2 + \tilde{\varepsilon}$ , такой, что  $0 < |\tilde{\varepsilon}| \leq 1/2$ .

Обозначим через  $\tilde{K}$  часть битов ключа  $K$ , которых достаточно для нахождения значений  $\langle \mathbf{a}, \pi(C^{(s_1)}) \rangle_i$  и  $\langle \mathbf{b}, \sigma(C^{(s_2)}) \rangle_j$  по известным векторам  $P$  и  $C$ . Пусть  $m_{s_1, s_2}$  — число битов в блоке  $\tilde{K}$ .

## Алгоритм 2

- для каждого  $\tilde{K} \in \mathbb{Z}_2^{m_{s_1, s_2}}$  определяем

$$N_0(\tilde{K}) = |\{ t : \langle \mathbf{a}, \pi(C_t^{(s_1)}) \rangle_i \oplus \langle \mathbf{b}, \sigma(C_t^{(s_2)}) \rangle_j = 0 \}|;$$

- упорядочим все векторы из  $\mathbb{Z}_2^{m_{s_1, s_2}} : \tilde{K}_1, \dots, \tilde{K}_{2^{m_{s_1, s_2}}}$ , так, что

$$\left| \frac{N}{2} - N_0(\tilde{K}_1) \right| \geq \dots \geq \left| \frac{N}{2} - N_0(\tilde{K}_{2^{m_{s_1, s_2}}}) \right|;$$

- для каждого  $q$  от 1 до  $2^{m_{s_1, s_2}}$

$$\triangleright \text{ полагаем } \langle \mathbf{d}, \tau(K) \rangle_k = \begin{cases} 0, & \text{если } (N_0(\tilde{K}_q) - \frac{N}{2}) \cdot \tilde{\varepsilon} > 0; \\ 1, & \text{в другом случае;} \end{cases}$$

$\triangleright$  с учетом полученного соотношения подбираем ключ.

## Конец алгоритма

Надежность алгоритма 2 может быть оценена так же как в случае линейного криптоанализа (см. [2], [22]). Для обеспечения требуемой надежности алгоритма размер статистики  $N$  должен быть пропорционален величине  $|\tilde{\varepsilon}|^{-2}$ .

Как и в случае алгоритма 1 имеет место взаимосвязь между абсолютной величиной преобладания  $\tilde{\varepsilon}$ ,  $k$ -коэффициентами Уолша — Адамара и  $k$ -бент-функциями.

Набор подключей  $K^{(s_1+1)}, \dots, K^{(s_2)}$  обозначим через  $K^{(s_1+1, \dots, s_2)}$ . Пусть отображение  $F_{s_1+1, s_2} : \mathbb{Z}_2^m \times (\mathbb{Z}_2^{m'_{\text{key}}})^{s_2-s_1} \rightarrow \mathbb{Z}_2^m$  задано суперпозицией функций  $F_{s_1+1}, \dots, F_{s_2}$ :

$$F_{s_1+1, s_2}(C^{(s_1)}, K^{(s_1+1, \dots, s_2)}) = F_{s_2}(F_{s_2-1}(\dots (F_{s_1+1}(C^{(s_1)}, K^{(s_1+1)}), K^{(s_1+2)}) \dots), K^{(s_2)}).$$

Тогда выполняется

$$C^{(s_2)} = F_{s_1+1, s_2}(C^{(s_1)}, K^{(s_1+1, \dots, s_2)}).$$

Аналогично тому, как это было сделано для первого алгоритма, рассмотрим равенство

$$\langle \mathbf{a}, \pi(C^{(s_1)}) \rangle_i \oplus \langle \mathbf{b}, \sigma(F_{s_1+1, s_2}(C^{(s_1)}, K^{(s_1+1, \dots, s_2)})) \rangle_j = 0 \quad (12)$$

при фиксированном наборе подключей  $K^{(s_1+1, \dots, s_2)}$ . Пусть оно выполняется с вероятностью  $1/2 + \tilde{\varepsilon}_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K^{(s_1+1, \dots, s_2)}; 0)$ , где  $-1/2 \leq \tilde{\varepsilon}_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K^{(s_1+1, \dots, s_2)}; 0) \leq 1/2$ .

Аналогично утверждению 1 несложно доказать

**Утверждение 2.** Для любого отображения  $F_{s_1+1, s_2}(\cdot, K^{(s_1+1, \dots, s_2)}) : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$  имеем

$$2^{m+1} \cdot \tilde{\varepsilon}_{j, \mathbf{b}, \sigma}^{i, \mathbf{a}, \pi}(K^{(s_1+1, \dots, s_2)}; 0) = W_{\langle \mathbf{b}, \sigma(F_{s_1+1, s_2}(\pi^{-1}(\cdot), K^{(s_1+1, \dots, s_2)})) \rangle_j}^{(i)}(\mathbf{a}).$$

Через  $\tilde{\varepsilon}(K)$  обозначим преобладание в равенстве (11) при фиксированном  $K$ . Тогда при любых параметрах  $k, \mathbf{d}$  и  $\tau$  справедливо

$$|\tilde{\varepsilon}(K)| = |\tilde{\varepsilon}_{j,\mathbf{b},\sigma}^{i,\mathbf{a},\pi}(K^{(s_1+1,\dots,s_2)}; 0)|, \quad (13)$$

если  $K^{(s_1+1,\dots,s_2)}$  является набором подключей ключа  $K$ .

**Теорема 3.** Пусть фиксирован ключ  $K \in \mathbb{Z}_2^{m_{\text{key}}}$  и целые числа  $s_1, s_2$ , где  $0 \leq s_1 < s_2 \leq r$ . Пусть  $K^{(s_1+1,\dots,s_2)}$  — набор подключей ключа  $K$ . Пусть вектор  $\mathbf{b} \in \mathbb{Z}_2^m$ , перестановки  $\pi, \sigma \in S_m$  и параметр  $j$ ,  $1 \leq j \leq m/2$ , таковы, что функция

$$\langle \mathbf{b}, \sigma(F_{s_1+1,s_2}(\pi^{-1}(\cdot), K^{(s_1+1,\dots,s_2)})) \rangle_j : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$$

является  $(m/2)$ -бент-функцией. Тогда справедливо равенство

$$\max_{i,k,\mathbf{a},\mathbf{d},\tau} |\tilde{\varepsilon}(K)| = \min_{i,k,\mathbf{a},\mathbf{d},\tau} |\tilde{\varepsilon}(K)| = 2^{-(m/2)-1}.$$

Так же как и для первого алгоритма из теоремы 3 следует, что использование  $(m/2)$ -бент-функций в качестве промежуточных функций шифрования позволяет снижать величину  $\max_{\mathbf{a} \in \mathbb{Z}_2^m} |\tilde{\varepsilon}(K)|$  до минимума.

## § 5 Анализ 4-разрядных подстановок в S-блоках ГОСТ, DES, $s^3\text{DES}$

Известно, что стойкость блочного шифра напрямую зависит от стойкости используемых в нем узлов замены (S-блоков). В данном параграфе рассматриваются примеры четырехразрядных подстановок для S-блоков шифров ГОСТ, DES,  $s^3\text{DES}$ . С помощью компьютера нами показано, что практически во всех случаях существуют более вероятные (по сравнению с линейными) квадратичные соотношения специального вида на входные и выходные биты этих подстановок.

**Пример 5.1.** В книге А. Г. Ростовцева и Е. Б. Маховенко [43] приведена серия экстремальных четырехразрядных подстановок, рекомендованных для S-блоков стандарта ГОСТ 28147-89 (см. подстановки  $S^1, \dots, S^{10}$  в таблице 1). Из каждой подстановки путем умножения ее на аффинные подстановки получается целый класс экстремальных подстановок. Все они выбраны так, чтобы максимально повысить стойкость шифра к методам линейного и дифференциального криптоанализа. Рассмотрим их квадратичные аппроксимации функциями из класса  $\Delta_4$ .

Каждому двоичному вектору  $\mathbf{x} = (x_1, x_2, x_3, x_4)$  сопоставим целое число  $\tilde{x} = 8x_1 + 4x_2 + 2x_3 + x_4$  от 0 до 15. Пусть  $P = (p_1, p_2, p_3, p_4)$  — двоичные входы,  $C = (c_1, c_2, c_3, c_4)$  — двоичные выходы некоторой четырехразрядной подстановки  $S$ , т.е.  $S(\tilde{P}) = \tilde{C}$ . Например, действие подстановки  $S^2$  представлено в таблице 2. Найдем наиболее вероятные квадратичные и линейные зависимости между входными и выходными битами подстановки  $S$ , используя класс функций  $\Delta_4$ . Согласно следствию 1 число функций в  $\Delta_4$  равно 28. Из них 16 — линейные функции, 12 — квадратичные, которые можно перечислить следующим образом:

$$\begin{aligned} &\langle 0101, v_1 v_2 v_3 v_4 \rangle_2, \quad \langle 0110, v_1 v_2 v_3 v_4 \rangle_2, \quad \langle 1001, v_1 v_2 v_3 v_4 \rangle_2, \quad \langle 1010, v_1 v_2 v_3 v_4 \rangle_2, \\ &\langle 0101, v_1 v_3 v_2 v_4 \rangle_2, \quad \langle 0110, v_1 v_3 v_2 v_4 \rangle_2, \quad \langle 1001, v_1 v_3 v_2 v_4 \rangle_2, \quad \langle 1010, v_1 v_3 v_2 v_4 \rangle_2, \\ &\langle 0101, v_1 v_4 v_2 v_3 \rangle_2, \quad \langle 0110, v_1 v_4 v_2 v_3 \rangle_2, \quad \langle 1001, v_1 v_4 v_2 v_3 \rangle_2, \quad \langle 1010, v_1 v_4 v_2 v_3 \rangle_2. \end{aligned}$$

Для этого мы выбрали все различные множества из двух неупорядоченных пар переменных:  $\{\{v_1, v_2\}, \{v_3, v_4\}\}, \{\{v_1, v_3\}, \{v_2, v_4\}\}, \{\{v_1, v_4\}, \{v_2, v_3\}\}$ ; затем для каждого множества составили четыре квадратичные функции, различающиеся только линейной частью.

$S^1 = (0, 13, 11, 8, 3, 6, 4, 1, 15, 2, 5, 14, 10, 12, 9, 7)$   
 $S^2 = (0, 1, 9, 14, 13, 11, 7, 6, 15, 2, 12, 5, 10, 4, 3, 8)$   
 $S^3 = (0, 1, 11, 13, 9, 14, 6, 7, 12, 5, 8, 3, 15, 2, 4, 10)$   
 $S^4 = (0, 1, 2, 4, 3, 5, 8, 10, 7, 9, 6, 13, 11, 14, 12, 15)$   
 $S^5 = (0, 1, 11, 2, 8, 6, 15, 3, 14, 10, 4, 9, 13, 5, 7, 12)$   
 $S^6 = (0, 1, 11, 2, 8, 3, 15, 6, 14, 10, 4, 9, 13, 5, 7, 12)$   
 $S^7 = (0, 4, 11, 2, 8, 6, 10, 1, 14, 15, 3, 9, 13, 5, 7, 12)$   
 $S^8 = (0, 4, 11, 2, 8, 3, 15, 1, 14, 10, 6, 9, 13, 5, 7, 12)$   
 $S^9 = (0, 11, 15, 9, 1, 5, 6, 8, 3, 10, 4, 12, 14, 13, 7, 2)$   
 $S^{10} = (0, 7, 10, 14, 9, 1, 13, 8, 12, 2, 11, 15, 3, 5, 4, 6)$   
 $S^{11} = (4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3)$   
 $S^{12} = (8, 2, 11, 13, 4, 1, 14, 7, 5, 15, 0, 3, 10, 6, 9, 12)$   
 $S^{13} = (10, 5, 3, 15, 12, 9, 0, 6, 1, 2, 8, 4, 11, 14, 7, 13)$   
 $S^{14} = (5, 10, 12, 6, 0, 15, 3, 9, 8, 13, 11, 1, 7, 2, 14, 4)$   
 $S^{15} = (3, 9, 15, 0, 6, 10, 5, 12, 14, 2, 1, 7, 13, 4, 8, 11)$   
 $S^{16} = (15, 0, 10, 9, 3, 5, 4, 14, 8, 11, 1, 7, 6, 12, 13, 2)$   
 $S^{17} = (12, 6, 3, 9, 0, 5, 10, 15, 2, 13, 4, 14, 7, 11, 1, 8)$   
 $S^{18} = (13, 10, 0, 7, 3, 9, 14, 4, 2, 15, 12, 1, 5, 6, 11, 8)$

ВХОДЫ				ВЫХОДЫ			
$p_1$	$p_2$	$p_3$	$p_4$	$c_1$	$c_2$	$c_3$	$c_4$
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	1
0	0	1	1	1	1	1	0
0	1	0	0	1	1	0	1
0	1	0	1	1	0	1	1
0	1	1	0	0	1	1	1
0	1	1	1	0	1	1	0
1	0	0	0	1	1	1	1
1	0	0	1	0	0	1	0
1	0	1	0	1	1	0	0
1	0	1	1	0	1	0	1
1	1	0	0	1	0	1	0
1	1	0	1	0	1	0	0
1	1	1	0	0	0	1	1
1	1	1	1	1	0	0	0

**Таблица 1.** 4-Разрядные подстановки, с предельно высокой нелинейностью  $NL = 4$ .

**Таблица 2.** Подстановка  $S^2$ .

Рассмотрим соотношения

$$\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = 0, \quad (14)$$

где при  $i = 1$  вектору  $\mathbf{a}$  соответствуют числа  $0, \dots, 15$  и тождественная перестановка  $\pi$ ; при  $i = 2$  вектору  $\mathbf{a}$  отвечают числа  $5, 6, 9, 10$  и перестановки  $\pi = \text{id}, (1, 3, 2, 4), (1, 3, 4, 2)$  (аналогично для  $\mathbf{b}$  и  $\sigma$  при  $j = 1, j = 2$ ). При данных условиях функции  $\langle \mathbf{a}, \pi(\cdot) \rangle_i$  и  $\langle \mathbf{b}, \sigma(\cdot) \rangle_j$  пробегают все множество функций  $\Delta_4$  без повторений. Для подстановки  $S$  рассмотрим таблицу, строки которой занумерованы тройками  $(i, \tilde{a}, \pi)$ , а столбцы — тройками  $(j, \tilde{b}, \sigma)$ , такую что на пересечении строки и столбца находится преобладание  $\varepsilon_{j, \tilde{b}, \sigma}^{i, \mathbf{a}, \pi}$  соответствующего равенства (14), умноженное на 16 (т. е. отклонение числа выполнений равенства (14) от половины).

И хотя здесь приводится способ построения таблицы для четырехразрядной подстановки, заметим, что он несложно может быть обобщен на случай произвольной  $t$ -разрядной подстановки или преобразования  $P \rightarrow C$ , где  $P$  и  $C$  имеют разное число битов.

Параметром неквадратичности подстановки  $S$  назовем число

$$NQ(S) = \min_{i, j} \min_{\mathbf{a} \neq \mathbf{0}, \mathbf{b} \neq \mathbf{0}} \min_{\delta \in \mathbb{Z}_2, \pi, \sigma} |\{P : \langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j \neq \delta\}|.$$

Другими словами, величина  $NQ(S)$  равна разности числа 8 и максимальной из абсолютных величин элементов таблицы (кроме элементов первой строки и первого столбца). Соотношение, отвечающее элементу таблицы с абсолютной величиной  $8 - NQ(S)$ , выполняется с вероятностью  $\frac{NQ(S)}{16}$  или  $1 - \frac{NQ(S)}{16}$  (т.е. наименее или наиболее вероятно).

Нелинейностью подстановки  $S$  называется величина

$$NL(S) = \min_{\mathbf{a} \neq \mathbf{0}, \mathbf{b} \neq \mathbf{0}} \min_{\delta, \pi, \sigma} |\{P : \langle \mathbf{a}, \pi(P) \rangle_1 \oplus \langle \mathbf{b}, \sigma(C) \rangle_1 \neq \delta\}|.$$

Величину  $NL(S)$  можно получить как разность числа 8 и максимальной из абсолютных величин элементов той части таблицы, которая соответствует только линейным соотношениям входных и выходных битов, т. е. где  $i = j = 1$  (кроме нулевых комбинаций). Очевидно, что  $NQ(S) \leq NL(S)$ . Согласно [44] справедливо  $NL(S) \leq 4$  для любой четырехразрядной подстановки  $S$ .

$16 \cdot \varepsilon_{j,b,\sigma}^{i,a,\pi}$		$j = 1$ id															$j = 2$ id				$j = 2$ (1,3,2,4)				$j = 2$ (1,3,4,2)				
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	5	6	9	10	5	6	9	10	5	6	9	10
$i = 1$ id	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	-2	0	2	-2	0	-2	4	0	2	0	-2	2	0	2	4	-2	0	0	2	0	2	2	0	0	0	4	0
	2	0	0	0	0	0	4	4	0	2	2	-2	-2	2	-2	2	-2	2	6	0	0	2	4	-2	0	4	2	0	2
	3	0	2	0	-2	-2	0	2	0	-2	4	2	4	0	-2	0	2	0	2	4	2	2	-2	0	0	4	-2	0	2
	4	0	-2	0	-2	0	2	0	2	0	-2	4	2	0	2	4	-2	4	-2	0	2	4	-2	0	2	0	0	-2	-2
	5	0	0	4	0	2	2	-2	2	0	4	0	0	-2	2	-2	-2	-2	2	0	4	0	0	-2	2	0	-4	2	2
	6	0	-2	4	2	0	-2	0	-2	2	0	-2	4	2	0	2	0	-2	0	0	-2	-2	2	2	-2	0	2	2	0
	7	0	4	0	0	2	2	-2	2	-2	-2	-2	2	4	0	0	0	0	0	-4	0	2	4	0	-2	0	2	2	-4
	8	0	0	2	-2	0	0	2	-2	0	0	2	-2	4	4	-2	2	2	0	2	0	4	0	2	-2	4	2	0	-2
	9	0	2	2	4	-2	4	0	-2	0	-2	2	0	-2	0	0	2	4	0	-2	2	0	2	0	6	-4	2	0	2
	10	0	0	-2	2	4	0	-2	-2	2	2	4	0	2	-2	0	0	0	-2	2	4	2	0	4	2	0	0	4	0
	11	0	-2	-2	4	2	0	4	2	-2	0	0	2	0	2	-2	0	2	2	2	-2	-2	2	2	2	0	4	0	4
	12	0	2	2	0	0	-2	2	4	4	-2	2	0	0	-2	-2	0	2	-2	2	-2	0	-2	2	0	0	2	-2	0
	13	0	0	-2	-2	2	2	0	0	4	0	-2	2	-2	2	0	4	0	2	-2	0	0	0	-4	0	0	-2	-2	0
	14	0	2	2	0	4	-2	2	0	-2	0	0	-2	-2	0	4	2	0	0	2	-2	-2	-2	0	0	0	0	-2	2
	15	0	4	-2	2	-2	-2	0	0	2	2	0	0	0	4	2	-2	-2	0	2	0	-2	0	2	0	0	0	2	2
$i = 2$ id	5	0	-2	2	0	4	-2	-2	0	2	4	0	2	2	0	0	-2	-4	0	2	2	0	0	2	-2	2	-2	4	0
	6	0	0	6	2	-2	2	0	0	0	0	-2	2	-2	2	0	0	0	2	-2	0	-2	2	-2	2	-2	0	0	2
	9	0	0	0	4	0	0	0	-4	2	-2	2	2	2	-2	2	2	2	-2	0	0	0	2	4	2	-2	4	2	0
	10	0	2	0	2	2	4	-2	0	0	2	4	-2	-2	0	-2	0	2	0	0	6	2	0	0	6	-2	-2	2	2
$i = 2$ (1,3,2,4)	5	0	0	2	2	4	0	-2	2	4	0	2	-2	0	0	-2	-2	0	-2	0	2	0	0	2	2	-2	0	2	0
	6	0	2	4	-2	-2	0	2	4	0	2	0	2	-2	0	-2	0	0	2	2	0	0	-2	-2	0	2	-2	-2	2
	9	0	2	-2	0	0	-2	2	0	2	0	4	2	2	-4	0	2	2	-2	4	0	2	-2	4	0	2	2	0	0
	10	0	0	0	0	2	2	-2	-2	6	2	2	0	0	0	0	-2	2	2	6	2	0	0	2	2	-4	4	2	
$i = 2$ (1,3,4,2)	5	0	0	4	4	0	0	0	0	4	-4	0	0	0	0	0	2	-2	-2	-2	-2	2	2	2	-4	4	0	0	
	6	0	0	2	-2	0	-4	2	2	2	2	0	4	2	-2	0	0	-2	0	4	-2	0	-2	2	-4	4	0	0	
	9	0	4	0	0	-2	2	2	2	0	0	4	0	-2	-2	-2	2	4	0	2	2	2	-2	0	4	0	0	-2	2
	10	0	0	2	2	-2	2	0	-4	-2	2	0	4	0	0	2	2	0	2	0	2	0	2	0	2	0	0	2	2

Таблица 3. Преобладания для подстановки  $S^2$ .

Для подстановки  $S^2$  имеем  $NL(S^2) = 4$ ,  $NQ(S^2) = 2$  (см. таблицу 3). В таблице 3 элементы с абсолютными значениями 4 и 6 выделены полужирным шрифтом и заключены в кружки соответственно. Любые линейные соотношения на входные и выходные биты  $S^2$  выполняются с вероятностью не большей  $3/4$ , тогда как существуют 7 квадратичных соотношений, вероятность которых составляет  $7/8$ . Выберем из них соотношение при  $i = 2$ ,  $\tilde{a} = 6$ ,  $\pi = \text{id}$ ,  $j = 1$ ,  $\tilde{b} = 2$ ,  $\sigma = \text{id}$ , т.е

$$\langle (0110), (p_1, p_2, p_3, p_4) \rangle_2 \oplus \langle (0010), (c_1, c_2, c_3, c_4) \rangle_1 = 0.$$

Используя формулы (2) и (3), приходим к равенству для входных и выходных битов

$$c_3 = p_1 p_3 \oplus p_1 p_4 \oplus p_2 p_3 \oplus p_2 p_4 \oplus p_1 \oplus p_4,$$

которое выполняется с вероятностью  $(8 + 6)/16$ , т.е.  $7/8$ . Заметим, что полученное соотношение линейно относительно битов  $c_1, c_2, c_3$  и  $c_4$ .

Аналогично, если выбрать соотношение при  $i = 1, \tilde{a} = 9, \pi = \text{id}, j = 2, \tilde{b} = 10, \sigma = (1, 3, 2, 4)$ , а именно

$$\langle (1001), (p_1, p_2, p_3, p_4) \rangle_1 \oplus \langle (1010), (c_1, c_3, c_2, c_4) \rangle_2 = 0,$$

то после преобразования с помощью (2) и (3) получаем соотношение

$$p_2 \oplus p_4 = c_1 c_2 \oplus c_1 c_4 \oplus c_2 c_3 \oplus c_3 c_4 \oplus c_3 \oplus c_4,$$

линейное относительно битов  $p_1, p_2, p_3$  и  $p_4$ , выполняющееся с вероятностью  $7/8$ .

$S$	квадратичные соотношения с вероятностью $7/8$
$S^1$	$C\{1, 3, 4\} = P\{13, 14, 23, 24, 1, 3\},$ $C\{1, 3, 4\} = P\{12, 13, 24, 34, 1, 3\},$ $C\{13, 14, 23, 24, 2, 3\} = P\{3, 4\},$ $C\{12, 14, 23, 34, 2, 3\} = P\{3, 4\},$
$S^2$	$C\{3\} = P\{13, 14, 23, 24, 1, 4\},$ $C\{2, 4\} = P\{12, 14, 23, 34, 3, 4\},$ $C\{13, 14, 23, 24, 1, 4\} = P\{3\},$ $C\{12, 14, 23, 34, 3, 4\} = P\{2, 4\},$ $C\{13, 14, 23, 24, 2, 4\} = P\{13, 14, 23, 24, 2, 4\},$ $C\{12, 14, 23, 34, 3, 4\} = P\{13, 14, 23, 24, 2, 4\},$ $C\{13, 14, 23, 24, 2, 4\} = P\{12, 14, 23, 34, 3, 4\}$
$S^3$	$C\{2\} = P\{13, 14, 23, 24, 1, 4\},$ $C\{1, 2, 3, 4\} = P\{12, 14, 23, 34, 3, 4\},$ $C\{12, 14, 23, 34, 3, 4\} = P\{4\},$ $C\{13, 14, 23, 24, 1, 4\} = P\{1, 2\},$
$S^4$	$C\{12, 13, 24, 34, 1, 3\} = P\{1, 2\}$ $C\{12, 14, 23, 34, 3, 4\} = P\{1, 2, 3, 4\},$ $C\{12, 13, 24, 34, 1, 3\} = P\{12, 13, 24, 34, 1, 3\},$ $C\{12, 14, 23, 34, 1, 4\} = P\{12, 13, 24, 34, 1, 3\},$ $C\{12, 14, 23, 34, 1, 4\} = P\{12, 14, 23, 34, 1, 4\},$
$S^5$	$C\{1, 2\} = P\{12, 14, 23, 34, 2, 3\}$ $C\{12, 14, 23, 34, 2, 3\} = P\{2, 3\},$
$S^6$	$C\{12, 14, 23, 34, 1, 4\} = P\{1, 2, 3, 4\}$
$S^7$	$C\{1, 3\} = P\{13, 14, 23, 24, 2, 4\},$ $C\{12, 13, 24, 34, 1, 2\} = P\{1, 3\} \oplus 1$ $C\{12, 13, 24, 34, 3, 4\} = P\{12, 14, 23, 34, 1, 2\},$ $C\{13, 14, 23, 24, 1, 4\} = P\{12, 13, 24, 34, 3, 4\} \oplus 1,$
$S^8$	$C\{1, 3\} = P\{13, 14, 23, 24, 2, 4\},$ $C\{12, 13, 24, 34, 1, 2\} = P\{1, 3\} \oplus 1$ $C\{12, 13, 24, 34, 3, 4\} = P\{12, 14, 23, 34, 1, 2\},$ $C\{13, 14, 23, 24, 1, 4\} = P\{12, 13, 24, 34, 3, 4\} \oplus 1,$
$S^9$	$C\{1, 2\} = P\{12, 14, 23, 34, 1, 4\}$ $C\{1, 2, 3\} = P\{13, 14, 23, 24, 1, 3\}$ $C\{1, 2, 4\} = P\{12, 13, 24, 34, 1, 3\}$ $C\{13, 14, 23, 24, 2, 3\} = P\{1, 2, 4\},$ $C\{12, 14, 23, 34, 1, 2\} = P\{12, 14, 23, 34, 1, 4\},$ $C\{13, 14, 23, 24, 1, 4\} = P\{12, 13, 24, 34, 1, 2\},$
$S^{10}$	$C\{1, 4\} = P\{13, 14, 23, 24, 1, 3\},$ $C\{1, 2, 3, 4\} = P\{12, 14, 23, 34, 1, 4\},$ $C\{13, 14, 23, 24, 1, 3\} = P\{1, 3\},$ $C\{12, 14, 23, 34, 3, 4\} = P\{1, 3\},$ $C\{13, 14, 23, 24, 2, 4\} = P\{12, 14, 23, 34, 3, 4\},$ $C\{13, 14, 23, 24, 2, 4\} = P\{13, 14, 23, 24, 1, 3\},$

**Таблица 4.** Наиболее вероятные квадратичные соотношения для входных и выходных битов подстановок  $S^1, \dots, S^{18}$  (часть 1).

В таблице 4 приведены наиболее вероятные соотношения на  $P$  и  $C$  для подстановок  $S^1, \dots, S^{10}$ , представленные в компактном виде, который поясним на примере полученных соотношений для  $S^2$ . Одно соотношение представлено в таблице как  $C\{3\} = P\{13, 14, 23, 24, 1, 4\}$ , другое — в виде  $C\{12, 14, 23, 34, 3, 4\} = P\{2, 4\}$ . Заметим, что для каждой из 10 подстановок удастся построить более вероятные (по сравнению с линейными) квадратичные соотношения, используя функции из класса  $\Delta_4$ . Имеем  $NL(S^t) = 4$ ,  $NQ(S^t) = 2$  для каждого  $t = 1, \dots, 10$ .

$S$	квадратичные соотношения с вероятностью 7/8
$S^{11}$	$C\{2, 3\} = P\{13, 14, 23, 24, 1, 3\} \oplus 1,$
	$C\{2, 3\} = P\{12, 13, 24, 34, 1, 3\} \oplus 1,$
	$C\{12, 14, 23, 34, 1, 4\} = P\{1, 4\},$
	$C\{13, 14, 23, 24, 1, 3\} = P\{13, 14, 23, 24, 2, 4\},$
	$C\{13, 14, 23, 24, 1, 3\} = P\{12, 13, 24, 34, 1, 3\} \oplus 1,$
$S^{12}$	$C\{1, 2, 3\} = P\{13, 14, 23, 24, 1, 3\} \oplus 1,$
	$C\{13, 14, 23, 24, 1, 3\} = P\{3, 4\} \oplus 1,$
	$C\{12, 14, 23, 34, 1, 2\} = P\{3, 4\} \oplus 1,$
	$C\{13, 14, 23, 24, 2, 4\} = P\{1, 3, 4\},$
	$C\{12, 14, 23, 34, 3, 4\} = P\{1, 3, 4\},$
	$C\{13, 14, 23, 24, 1, 3\} = P\{12, 14, 23, 34, 2, 3\} \oplus 1,$
	$C\{12, 13, 24, 34, 1, 3\} = P\{12, 14, 23, 34, 2, 3\} \oplus 1,$
$S^{13}$	$C\{12, 14, 23, 34, 1, 4\} = P\{13, 14, 23, 24, 2, 3\} \oplus 1,$
	$C\{12, 13, 24, 34, 1, 3\} = P\{13, 14, 23, 24, 2, 3\} \oplus 1,$
$S^{14}$	$C\{1\} = P\{12, 14, 23, 34, 1, 4\},$
	$C\{3\} = P\{12, 14, 23, 34, 3, 4\},$
	$C\{1, 2\} = P\{12, 14, 23, 34, 2, 3\} \oplus 1,$
	$C\{2, 3\} = P\{12, 14, 23, 34, 1, 2\} \oplus 1,$
	$C\{12, 14, 23, 34, 3, 4\} = P\{12, 14, 23, 34, 1, 2\} \oplus 1,$
	$C\{12, 14, 23, 34, 1, 4\} = P\{12, 14, 23, 34, 2, 3\} \oplus 1,$
$S^{15}$	$C\{1, 2, 3\} = P\{12, 14, 23, 34, 1, 2\} \oplus 1,$
	$C\{12, 13, 24, 34, 1, 3\} = P\{2, 4\},$
	$C\{12, 13, 24, 34, 2, 4\} = P\{1, 2, 4\},$
	$C\{13, 14, 23, 24, 2, 4\} = P\{2, 4\} \oplus 1,$
	$C\{13, 14, 23, 24, 1, 3\} = P\{1, 2, 4\} \oplus 1,$
	$C\{12, 14, 23, 34, 1, 4\} = P\{12, 13, 24, 34, 2, 4\},$
	$C\{12, 13, 24, 34, 1, 3\} = P\{12, 13, 24, 34, 2, 4\},$
$S^{16}$	$C\{12, 13, 24, 34, 1, 2\} = P\{12, 13, 24, 34, 1, 2\},$
	$C\{12, 13, 24, 34, 1, 2\} = P\{13, 14, 23, 24, 2, 3\},$
	$C\{12, 14, 23, 34, 1, 2\} = P\{12, 14, 23, 34, 2, 3\},$
	$C\{12, 14, 23, 34, 1, 4\} = P\{12, 14, 23, 34, 1, 2\},$
	$C\{12, 14, 23, 34, 1, 4\} = P\{13, 14, 23, 24, 1, 3\},$
	$C\{13, 14, 23, 24, 2, 4\} = P\{12, 13, 24, 34, 1, 3\},$
	$C\{13, 14, 23, 24, 1, 4\} = P\{12, 14, 23, 34, 1, 2\},$
	$C\{13, 14, 23, 24, 2, 4\} = P\{12, 14, 23, 34, 2, 3\},$
$S^{17}$	$C\{2, 3\} = P\{12, 13, 24, 34, 1, 3\},$
	$C\{1, 3, 4\} = P\{13, 14, 23, 24, 2, 3\} \oplus 1,$
	$C\{13, 14, 23, 24, 2, 3\} = P\{2\} \oplus 1,$
	$C\{12, 13, 24, 34, 3, 4\} = P\{2\} \oplus 1,$
	$C\{13, 14, 23, 24, 1, 4\} = P\{1, 2\} \oplus 1,$
	$C\{12, 13, 24, 34, 1, 2\} = P\{1, 2\} \oplus 1,$
$S^{18}$	$C\{13, 14, 23, 24, 1, 4\} = P\{12, 13, 24, 34, 1, 3\} \oplus 1,$
	отсутствуют

**Таблица 5.** Наиболее вероятные квадратичные соотношения для входных и выходных битов подстановок  $S^1, \dots, S^{18}$  (часть 2).

На данном примере можно убедиться в том, что использование соотношений вида (14) в составе систем уравнений с неизвестными битами (входными или выходными)



может приводить к более вероятным аппроксимациям неизвестных битов, не усложняя при этом решение системы (система по-прежнему может оставаться линейной относительно неизвестных).

**Пример 5.2.** В книге Б. Шнайера [45] приведены восемь четырехразрядных подстановок, использовавшихся при шифровании методом ГОСТ в приложении для ЦБ РФ, а также в однонаправленной хэш-функции ГОСТ. Все они имеют параметр  $NL$ , равный 2, кроме одной, для которой  $NL = 4$  (см. подстановку  $S^{11}$  в таблице 1). Для каждой подстановки имеем  $NQ = 2$ , и в среднем добавляется 5-6 новых наиболее вероятных квадратичных соотношений специального вида на входные и выходные биты каждой подстановки.

**Пример 5.3.** Для всех 32 подстановок на 16 элементах, используемых в S-блоках алгоритма DES (см. например, [45]), параметры  $NL$  и  $NQ$  совпадают и равны 2. Отметим, что для каждой подстановки добавляется от 0 до 11 (в среднем 4-5) новых наиболее вероятных квадратичных соотношений на входные и выходные биты.

**Пример 5.4.** Рассмотрим 32 подстановки (см. например, [45]) в S-блоках модифицированного алгоритма  $s^3DES$  [46], [47], которые считаются устойчивыми к методам дифференциального и линейного криптоанализа. Среди них только 7 подстановок (это подстановки  $S^{12}, \dots, S^{18}$  в таблице 1) обладают нелинейностью  $NL = 4$ , для 25-ти остальных параметр  $NL$  равен 2. Для шести из семи подстановок с нелинейностью  $NL = 4$  выполняется  $NQ = 2$ , и в среднем для каждой такой подстановки имеется около 6 квадратичных соотношений с вероятностью  $7/8$ . И лишь для одной подстановки  $S^{18}$  имеем  $NL = NQ = 4$ .

Квадратичные соотношения с вероятностью  $7/8$  для подстановок  $S^{11}, \dots, S^{18}$  приведены в таблице 5.

## § 6 Замечания и дополнения

Приведем свойства функций  $\langle \mathbf{u}, \mathbf{v} \rangle_k$ , которые могут быть использованы при согласовании раундовых аппроксимаций в квадратичном криптоанализе конкретных шифров.

Для вектора  $\mathbf{u} = (u_1, \dots, u_m)$  пусть  $\bar{\mathbf{u}}^k = (u_1 \oplus u_2, \dots, u_{2k-1} \oplus u_{2k})$  — вектор длины  $k$ . Через  $*$  обозначим обычное покомпонентное умножение векторов. Пусть  $|\mathbf{u}| = \langle \mathbf{u}, \mathbf{u} \rangle$ . Справедливо

**Утверждение 3.** Для любых векторов  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$ , для любого  $k$ ,  $1 \leq k \leq m/2$ , верно

$$\langle \mathbf{u} \oplus \mathbf{v}, \mathbf{w} \rangle_k = \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \langle \bar{\mathbf{u}}^k, \bar{\mathbf{w}}^k \rangle \cdot \langle \bar{\mathbf{v}}^k, \bar{\mathbf{w}}^k \rangle \oplus |\bar{\mathbf{u}}^k * \bar{\mathbf{v}}^k * \bar{\mathbf{w}}^k|.$$

**Доказательство.** Согласно (1) имеем

$$\begin{aligned} \langle \mathbf{u} \oplus \mathbf{v}, \mathbf{w} \rangle_k &= \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \left( \bigoplus_{i=1}^k \bigoplus_{j=i}^k (\bar{u}_i^k \oplus \bar{v}_i^k)(\bar{u}_j^k \oplus \bar{v}_j^k) \bar{w}_i^k \bar{w}_j^k \right) = \\ &= \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \left( \bigoplus_{i=1}^k \bigoplus_{j=i}^k \bar{u}_i^k \bar{v}_j^k \bar{w}_i^k \bar{w}_j^k \right) \oplus \left( \bigoplus_{i=1}^k \bigoplus_{j=i}^k \bar{u}_j^k \bar{v}_i^k \bar{w}_i^k \bar{w}_j^k \right) = \\ &= \langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \left( \bigoplus_{i=1}^k \bigoplus_{j=1}^k \bar{u}_i^k \bar{v}_j^k \bar{w}_i^k \bar{w}_j^k \right) \oplus \left( \bigoplus_{i=1}^k \bar{u}_i^k \bar{v}_i^k \bar{w}_i^k \right). \end{aligned}$$

Осталось заметить, что третье слагаемое совпадает с  $\langle \bar{\mathbf{u}}^k, \bar{\mathbf{w}}^k \rangle \cdot \langle \bar{\mathbf{v}}^k, \bar{\mathbf{w}}^k \rangle$ , а четвертое равно  $|\bar{\mathbf{u}}^k * \bar{\mathbf{v}}^k * \bar{\mathbf{w}}^k|$ . ▲

Из утверждения 3 следует, что чем меньше значение  $k$ , тем менее существенной является нелинейная «добавка» при переходе от  $\langle \mathbf{u} \oplus \mathbf{v}, \mathbf{w} \rangle_k$  к сумме  $\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k$ . При согласовании раундовых аппроксимаций (см. § 1) такая добавка может быть оценена с некоторой вероятностью по частичной информации о неизвестных битах.

**Аналог линейности.** В основе этого свойства лежит другой подход к определению функций  $\langle \mathbf{u}, \mathbf{v} \rangle_k$  — подход со стороны теории кодирования. Не вдаваясь в подробности, можно сказать, что множество векторов значений всех функций  $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ ,  $\mathbf{u} \in \mathbb{Z}_2^m$ ,  $a \in \mathbb{Z}_2$ , образует двоичный код типа Адамара  $A_m^k$ , на котором можно определить групповую операцию, согласованную с метрикой Хэмминга. Данная операция и позволяет говорить об аналоге линейности для функций  $\langle \mathbf{u}, \mathbf{v} \rangle_k$ . Детально эти свойства функций  $\langle \mathbf{u}, \mathbf{v} \rangle_k$  рассмотрены в [39]. Здесь мы лишь кратко обозначим основные моменты.

Пусть  $m$  — произвольное целое, параметр  $k$ ,  $1 \leq k \leq m/2$ , фиксирован. Пусть  $\mathbf{G}_m^k$  — матрица над  $\mathbb{Z}_4$  размера  $(m - k) \times 2^m$ , состоящая из лексикографически упорядоченных столбцов  $\mathbf{z}^T$ , где  $\mathbf{z} \in \mathbb{Z}_4^k \times (2\mathbb{Z}_4)^{m-2k}$ . Такие матрицы впервые рассматривались Д. С. Кротовым [40], [41] для построения  $\mathbb{Z}_4$ -линейных кодов типа Адамара и совершенных кодов. Например,

$$\mathbf{G}_2^1 = (0123), \mathbf{G}_4^1 = \begin{pmatrix} 0000111122223333 \\ 0022002200220022 \\ 0202020202020202 \end{pmatrix}, \mathbf{G}_4^2 = \begin{pmatrix} 0000111122223333 \\ 0123012301230123 \end{pmatrix}.$$

Пусть далее

$\beta, \gamma : \mathbb{Z}_4^i \rightarrow \mathbb{Z}_2^i$  — покоординатные продолжения отображений  $\beta, \gamma : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$  таких, что  $\beta : 0, 1 \rightarrow 0; 2, 3 \rightarrow 1$  и  $\gamma : 0, 3 \rightarrow 0; 1, 2 \rightarrow 1$  для любого целого  $i$ ;

$\varphi : \mathbb{Z}_4^i \rightarrow \mathbb{Z}_2^{2i}$  — покоординатное продолжение отображения Грея:  $\varphi(a) = (\beta(a), \gamma(a))$  для  $a \in \mathbb{Z}_4$  (см. [48], [49]);

$\varphi_k : \mathbb{Z}_4^k \times \mathbb{Z}_2^{m-2k} \rightarrow \mathbb{Z}_2^m$  — отображение такое, что  $\varphi_k : (\mathbf{u}', \mathbf{u}'') \rightarrow (\varphi(\mathbf{u}'), \mathbf{u}'')$  для любых векторов  $\mathbf{u}' \in \mathbb{Z}_4^k, \mathbf{u}'' \in \mathbb{Z}_2^{m-2k}$  (см. [39]).

Пусть  $\mathbf{h}^{\mathbf{u}} = \varphi_k^{-1}(\mathbf{u}) \cdot \mathbf{G}_m^k$  — вектор длины  $2^m$  над  $\mathbb{Z}_4$ . Рассмотрим квадратную матрицу  $\mathbf{C}_m^k = (c_{\mathbf{u}, \mathbf{v}}^k)$ ,  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ , порядка  $2^m$  над  $\mathbb{Z}_4$ , строками которой являются всевозможные векторы  $\mathbf{h}^{\mathbf{u}}$ , расположенные в порядке лексикографического возрастания векторов  $\varphi_k^{-1}(\mathbf{u})$ . Считаем, что столбцы матрицы  $\mathbf{C}_m^k$  также нумеруются векторами  $\mathbf{v}$  в порядке лексикографического возрастания векторов  $\varphi_k^{-1}(\mathbf{v})$ . Например, векторы  $\mathbf{u}$  для нумерации строк матриц  $\mathbf{C}_4^1$  и  $\mathbf{C}_4^2$  в нужном порядке приведены в таблицах 6 и 7. При этом каждому вектору  $\mathbf{u}$  удобно сопоставлять число  $\tilde{u} = 8u_1 + 4u_2 + 2u_3 + u_4$ .

$\tilde{u}$	$u$	$\varphi_1^{-1}(u)$
0	0000	000
1	0001	001
2	0010	010
3	0011	011
4	0100	100
5	0101	101
6	0110	110
7	0111	111
12	1100	200
13	1101	201
14	1110	210
15	1111	211
8	1000	300
9	1001	301
10	1010	310
11	1011	311

$\tilde{u}$	$u$	$\varphi_2^{-1}(u)$
0	0000	00
1	0001	01
3	0011	02
2	0010	03
4	0100	10
5	0101	11
7	0111	12
6	0110	13
12	1100	20
13	1101	21
15	1111	22
14	1110	23
8	1000	30
9	1001	31
11	1011	32
10	1010	33

**Таблица 6.** Векторы для  $C_4^1$ . **Таблица 7.** Векторы для  $C_4^2$ .

В таблицах 8 и 9 приведены матрицы  $C_4^1$  и  $C_4^2$  вместе с нумерацией их строк и столбцов.

$c_{u,v}^1$	0	1	2	3	4	5	6	7	12	13	14	15	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2
3	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0
4	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
5	0	2	0	2	1	3	1	3	2	0	2	0	3	1	3	1
6	0	0	2	2	1	1	3	3	2	2	0	0	3	3	1	1
7	0	2	2	0	1	3	3	1	2	0	0	2	3	1	1	3
12	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
13	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
14	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0
15	0	2	2	0	2	0	0	2	0	2	2	0	2	0	0	2
8	0	0	0	0	3	3	3	3	2	2	2	2	1	1	1	1
9	0	2	0	2	3	1	3	1	2	0	2	0	1	3	1	3
10	0	0	2	2	3	3	1	1	2	2	0	0	1	1	3	3
11	0	2	2	0	3	1	1	3	2	0	0	2	1	3	3	1

$c_{u,v}^2$	0	1	3	2	4	5	7	6	12	13	15	14	8	9	11	10
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
3	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
2	0	3	2	1	0	3	2	1	0	3	2	1	0	3	2	1
4	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
5	0	1	2	3	1	2	3	0	2	3	0	1	3	0	1	2
7	0	2	0	2	1	3	1	3	2	0	2	0	3	1	3	1
6	0	3	2	1	1	0	3	2	2	1	0	3	3	2	1	0
12	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
13	0	1	2	3	2	3	0	1	0	1	2	3	2	3	0	1
15	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
14	0	3	2	1	2	1	0	3	0	3	2	1	2	1	0	3
8	0	0	0	0	3	3	3	3	2	2	2	2	1	1	1	1
9	0	1	2	3	3	0	1	2	2	3	0	1	1	2	3	0
11	0	2	0	2	3	1	3	1	2	0	2	0	1	3	1	3
10	0	3	2	1	3	2	1	0	2	1	0	3	1	0	3	2

**Таблица 8.** Матрица  $C_4^1$ .

**Таблица 9.** Матрица  $C_4^2$ .

Несложно доказать, что каждая матрица  $C_m^k$  симметрична. Матрицы  $C_m^k$  можно получать итеративно [39]:

$$C_{m+1}^k = (C_m^k \otimes J_2) + (J_n \otimes C_1^0);$$

$$C_{m+2}^{k+1} = (J_4 \otimes C_m^k) + (C_2^1 \otimes J_n),$$

где  $J_s$  — квадратная матрица порядка  $s$  из всех единиц,  $C_1^0 = \begin{pmatrix} 00 \\ 02 \end{pmatrix}$ ,  $A \otimes B$  — кронекерово произведение

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1p}B \\ \dots & \dots & \dots \\ a_{p1}B & \dots & a_{pp}B \end{pmatrix}$$

квадратной матрицы  $A = (a_{ij})$ ,  $1 \leq i, j \leq p$ , на матрицу  $B = (b_{ij})$ ,  $1 \leq i, j \leq q$ .

**Утверждение 4.** (см. [39]) При любых целых  $m, k$ ,  $1 \leq k \leq m/2$ , любых  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$  выполняется  $\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(c_{\mathbf{u}, \mathbf{v}}^k)$ .

Этот факт вместе с итеративными формулами для матриц  $\mathbf{C}_m^k$  можно использовать для быстрого вычисления коэффициентов  $W_f^{(k)}(\mathbf{v})$  и расчета преобладаний.

Пусть  $\star : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$  — бинарная операция, такая что  $\mathbf{u} \star \mathbf{v} = \varphi_k(\varphi_k^{-1}(\mathbf{u}) \dot{+} \varphi_k^{-1}(\mathbf{v}))$  для любых  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ , где  $\dot{+}$  обозначает сложение над  $\mathbb{Z}_4$  для первых  $k$  координат векторов  $\varphi_k^{-1}(\mathbf{u})$ ,  $\varphi_k^{-1}(\mathbf{v})$  и сложение над  $\mathbb{Z}_2$  для  $m - 2k$  последних координат.

**Утверждение 5.** (см. [39]) При любых целых  $m, k$ , любых  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$  справедливо  $c_{\mathbf{u}, \mathbf{w}}^k + c_{\mathbf{v}, \mathbf{w}}^k = c_{\mathbf{u} \star \mathbf{v}, \mathbf{w}}^k$ , где  $+$  обозначает сложение над  $\mathbb{Z}_4$ .

Утверждение 5 вытекает из того, что выполняется  $\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u} \star \mathbf{v}}$  при любых  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ . Из утверждения 4 следует, что вектор значений булевой функции  $\langle \mathbf{u}, \cdot \rangle_k : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$  является образом (под действием отображения  $\beta$ ) вектора значений функции  $\langle \langle \mathbf{u}, \cdot \rangle_k : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_4$ , такой что  $\langle \langle \mathbf{u}, \mathbf{v} \rangle_k = c_{\mathbf{u}, \mathbf{v}}^k$ . Другими словами,  $\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(\langle \langle \mathbf{u}, \mathbf{v} \rangle_k)$ . Заметим, что  $\langle \langle \mathbf{u}, \mathbf{v} \rangle_k = \langle \langle \mathbf{v}, \mathbf{u} \rangle_k$ . Согласно утверждению 5 функции  $\langle \langle \mathbf{u}, \mathbf{v} \rangle_k$ ,  $\mathbf{u} \in \mathbb{Z}_2^m$ , обладают свойством линейности над  $\mathbb{Z}_4$ , т.е.  $\langle \langle \mathbf{u}', \mathbf{v} \rangle_k + \langle \langle \mathbf{u}'', \mathbf{v} \rangle_k = \langle \langle \mathbf{u}' \star \mathbf{u}'', \mathbf{v} \rangle_k$ . Этот факт можно использовать в квадратичном криптоанализе. В частности, заменив основное соотношение  $\langle \mathbf{a}, \pi(P) \rangle_i \oplus \langle \mathbf{b}, \sigma(C) \rangle_j = \langle \mathbf{d}, \tau(K) \rangle_k$  для битов открытого текста, шифротекста и ключа (например, для алгоритма 1) на соотношение над  $\mathbb{Z}_4$  вида  $\langle \langle \mathbf{a}, \pi(P) \rangle_k + \langle \langle \mathbf{b}, \pi(C) \rangle_k = \langle \langle \mathbf{d}, \pi(K) \rangle_k$ , полагая  $i = j = k$ , а также  $\pi = \sigma = \tau$ . В соотношениях такого типа напрямую может использоваться линейность функций  $\langle \langle \mathbf{u}, \mathbf{v} \rangle_k$  над  $\mathbb{Z}_4$ . Однако, этот случай требует дополнительного исследования. В частности, необходимо описать способ выбора по набранной статистике значения  $\langle \langle \mathbf{d}, \pi(K) \rangle_k$  из четырех возможных вариантов 0, 1, 2 и 3 (вместо двух, как было ранее).

Автор искренне признателен рецензентам за ценные замечания, позволившие улучшить изложение статьи.

## Литература

- [1] Matsui M., Yamagishi A. A New Method for Known Plaintext Attack of FEAL Cipher // Advances in Cryptology — EUROCRYPT'92 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Balatonfured, Hungary. May 24–28, 1992). Lecture Notes in Comput. Sci. V. 658. Berlin: Springer, 1993. P. 81–91.
- [2] Matsui M. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology — EUROCRYPT'93 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Lofthus, Norway. May 23–27, 1993). Lecture Notes in Comput. Sci. V. 765. Berlin: Springer, 1994. P. 386–397.
- [3] Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4, N 1. P. 3–72.
- [4] Nyberg K. Linear Approximation of Block Ciphers // Advances in Cryptology — EUROCRYPT'94 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Perugia, Italy. May 9–12, 1994). Lecture Notes in Comput. Sci. V. 950. Berlin: Springer, 1995. P. 439–444.

- [5] *Harpers C., Kramer G.G., Massey J.L.* A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma // Advances in Cryptology — EUROCRYPT '95 (Proc. International Conference on the Theory and Application of Cryptographic Techniques. Saint-Malo, France. May 21–25, 1995). Lecture Notes in Comput. Sci. V. 921. Berlin: Springer, 1995. P. 24–38.
- [6] *Buttyan L., Vajda I.* Searching for the Best Linear Approximation of DES-like Cryptosystems // Electronics Letters. 1995. V. 31. N 11. P. 873–874.
- [7] *Matsui M.* New Structure of Block Ciphers with Provable Security Against Differential and Linear Cryptanalysis // Advances in Cryptology — EUROCRYPT'96 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Saragossa, Spain. May 12–16, 1996). Lecture Notes in Comput. Sci. V. 1070. Springer-Verlag, 1996. P. 205–218.
- [8] *Daemen J., Govaerts R., Vandevall J.* Correlation Matrices // Fast Software Encryption — FSE'95 (Proc. Second International Workshop. Leuven, Belgium. December 14–16, 1994). Lecture Notes in Comput. Sci. V. 1008. Berlin: Springer, 1995. P. 275–285.
- [9] *Kaliski B., Robshaw M.* Linear Cryptanalysis Using Multiple Approximations // Advances in Cryptology — CRYPTO'94 (Proc. 14th Annual International Cryptology Conference. Santa Barbara, California, USA. August 21–25, 1994). Lecture Notes in Comput. Sci. V. 839. Berlin: Springer, 1994. P. 26–39.
- [10] *Biryukov A., De Canniere C., Quisquater M.* On Multiple Linear Approximations // Advances in Cryptology — CRYPTO 2004 (Proc. 24th Annual International Cryptology Conference. Santa Barbara, California, USA. August 15–19, 2004). Lecture Notes in Comput. Sci. V. 3152. Springer-Verlag, 2004. P. 1–22.
- [11] *Sakurai K., Furuya S.* Improving Linear Cryptanalysis of LOKI91 by Probabilistic Counting Method // Fast Software Encryption — FSE'97 (Proc. 4th International Workshop, Haifa, Israel. January 20–22, 1997). Lecture Notes in Comput. Sci. V. 1267. Berlin: Springer, 1997. P. 114–133.
- [12] *Baignères T., Junod P., Vaudenay S.* How Far Can We Go Beyond Linear Cryptanalysis? // Advances in Cryptology — ASIACRYPT '04 (Proc. 10th International Conference on the Theory and Applications of Cryptology and Information Security. Jeju Island, Korea. December 5–9, 2004). Lecture Notes in Comput. Sci. V. 3329. Berlin: Springer, 2004. P. 432–450.
- [13] *Selçuk A. A.* On Probability of Success in Linear and Differential Cryptanalysis // J. Cryptology. 2008. V. 21. N. 1. P. 131–147.
- [14] *Knudsen L.* Practically Secure Feistel Ciphers // Fast Software Encryption — FSE'93 (Proc. the Cambridge Security Workshop. Cambridge, UK. December 9–11, 1993). Lecture Notes in Comput. Sci. V. 809. Springer-Verlag, 1994. P. 211–221.
- [15] *Shorin V.V., Jelezniakov V.V., Gabidulin E.M.* Linear and Differential Cryptanalysis of Russian GOST // WCC'2001 (Proc. International Workshop on Coding and Cryptography. Paris, France. January 8–12, 2001). P. 467–476.
- [16] *Borst J., Preneel B., Vandewalle J.* Linear Cryptanalysis of RC5 and RC6 // Fast Software Encryption — FSE'99 (Proc. 6th International Workshop. Rome, Italy. March 24–26, 1999). Lecture Notes in Comput. Sci. V. 1636. Berlin: Springer, 1999. P. 16–30.
- [17] *Hawkes P., O'Connor L.* On Applying Linear Cryptanalysis to IDEA // Advances in Cryptology — ASIACRYPT '96 (Proc. International Conference on the Theory and Applications of Cryptology and Information Security. Kyongju, Korea. November 3–7, 1996). Lecture Notes in Comput. Sci. V. 1163. Berlin: Springer, 1996. P. 105–115.

- [18] *Biham E., Dunkelman O., Keller N.* Differential-Linear Cryptanalysis of Serpent // Fast Software Encryption — FSE'2003 (Proc. 10th International Workshop. Lund, Sweden. February 24–26, 2003). Lecture Notes in Comput. Sci. V. 2887. Berlin: Springer, 2003. P. 9–21.
- [19] *Mansoori S. D., Bizaki H. K.* On the Vulnerability of Simplified AES Algorithm Against Linear Cryptanalysis // International Journal of Computer Science and Network Security, 2007. V. 7. N 7. P. 257–263.
- [20] *Nakahara J. Jr.* A Linear Analysis of Blowfish and Khufu // Information Security Practice and Experience — ISPEC 2007 (Proc. Third International Conference. Hong Kong, China. May 7–9, 2007). Lecture Notes in Comput. Sci. V. 4464. P. 20–32.
- [21] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. N 3. P. 300–305.
- [22] *Логачев О. А., Сальников А. А., Яценко В. В.* Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004.
- [23] *Dobbertin H., Leander G.* A Survey of Some Recent Results on Bent Functions // Sequences and their applications — SETA 2004 (Proc. Third International Conference. Seoul, Korea. October 24–28, 2004). Lecture Notes in Comput. Sci. V. 3486. Berlin: Springer, 2005. P. 1–29.
- [24] *Chee S., Lee S., Kim K.* Semi-bent Functions // Advances in Cryptology — ASIACRYPT '94 (Proc. 4th International Conference on the Theory and Applications of Cryptology. Wollongong, Australia. November 28 – December 1, 1994). Lecture Notes in Comput. Sci. V. 917. Berlin: Springer, 1995. P. 107–118.
- [25] *Dobbertin H., Leander G.* Cryptographer's Toolkit for Construction of 8-Bit Bent Functions // Cryptology ePrint Archive, Report 2005/089, available at <http://eprint.iacr.org/>.
- [26] *Qu C., Seberry J., Pieprzyk J.* Homogeneous Bent Functions // Discrete Applied Mathematics. 2000. V. 102. N 1–2. P. 133–139.
- [27] *Youssef A., Gong G.* Hyper-bent functions // Advances in cryptology — EUROCRYPT'2001 (Proc. International Conference on the Theory and Application of Cryptographic Techniques. Innsbruck, Austria. May 6–10, 2001). Lecture Notes in Comput. Sci. V. 2045. Berlin: Springer, 2001. P. 406–419.
- [28] *Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б.* Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18. N 1. С. 9–29.
- [29] *Carlet C., Gaborit P.* Hyper-bent functions and cyclic codes // J. Combin. Theory. Ser. A. 2006. V. 113. N 3. P. 466–482.
- [30] *Youssef A.M.* Generalized hyper-bent functions over  $GF(p)$  // Discrete Applied Mathematics. 2007. V. 155. N 8. P. 1066–1070.
- [31] *Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишкин В. А., Шишков А. Б.* Бент-функции и гипербент-функции над полем из  $2^l$  элементов // Пробл. передачи информ. 2008. Т. 44. N 1. С. 15–37.
- [32] *Parker M.G., Pott A.* On Boolean Functions Which Are Bent and Negabent // Sequences, Subsequences, and Consequences — SSC 2007 (Proc. International Workshop. Los Angeles, CA, USA. May 31 – June 2, 2007). Lecture Notes in Comput. Sci. V. 4893. Berlin: Springer, 2007. P. 9–23.
- [33] *Knudsen L. R., Robshaw M. J. B.* Non-linear Approximation in Linear Cryptanalysis // Advances in Cryptology — EUROCRYPT'96 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Saragossa, Spain. May 12–16, 1996). Lecture Notes in Comput. Sci. V. 1070. Springer-Verlag, 1996. P. 224–236.

- [34] *Shimoyama T., Kaneko T.* Quadratic Relation of S-box and its Application to the Linear Attack of Full Round DES // Advances in Cryptology — CRYPTO'98 (Proc. 18th Annual International Cryptology Conference. Santa Barbara, California. USA. August 23–27, 1998). Lecture Notes in Comput. Sci. V. 1462. Berlin: Springer, 1998. P. 200–211.
- [35] *Nakahara J., Preneel B., Vandewalle J.* Experimental Non-Linear Cryptanalysis // COSIC Internal Report. Katholieke Universiteit Leuven. 2003. 17 p.
- [36] *Tapiador J. M. E., Clark J. A., Hernandez-Castro J. C.* Non-linear Cryptanalysis Revisited: Heuristic Search for Approximations to S-Boxes // Proc. 11th IMA International Conference. Cirencester, UK. December 18–20, 2007. Lecture Notes in Comput. Sci. V. 4887. Berlin: Springer, 2007. P. 99–117.
- [37] *Рязанов Б. В., Чечета С. И.* О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. 1995. Т. 7. N 3. С. 129–145.
- [38] *Иванов А. В.* Использование приведенного представления булевых функций при построении их нелинейных аппроксимаций // Вестник Томского госуниверситета. Приложение. 2007. N 23. С. 31–35.
- [39] *Токарева Н. Н.* Бент-функции с более сильными свойствами нелинейности:  $k$ -бент-функции // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14. N 4. С. 76–102.
- [40] *Кротов Д. С.*  $\mathbb{Z}_4$ -линейные совершенные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7. N 4. С. 78–90 (translated at <http://arxiv.org/abs/0710.0198>).
- [41] *Krotov D. S.*  $\mathbb{Z}_4$ -linear Hadamard and extended perfect codes // WCC'2001 (Proc. International Workshop on Coding and Cryptography. Paris, France. January 8–12, 2001). P. 329–334.
- [42] *Токарева Н. Н.* Описание  $k$ -бент-функций от четырех переменных // Дискрет. анализ и исслед. операций. 2008. Т. 15. N 4. (в печати).
- [43] *Ростовцев А. Г., Маховенко Е. Б.* Введение в теорию итерированных шифров // СПб.: НПО «Мир и Семья», 2003.
- [44] *Heys H. M., Tavares S. E.* Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis // J. Cryptology. 1996. V. 9. N 1. P. 1–19.
- [45] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си // М.: Триумф, 2002.
- [46] *Kim K., Park S., Lee S.* Reconstruction of s2DES S-Boxes and their Immunity to Differential Cryptanalysis // Proc. Korea — Japan Workshop on Information Security and Cryptography. Seoul, Korea. October 24–26, 1993. P. 282–291.
- [47] *Biham E., Biryukov A.* How to strengthen DES using existing hardware // Advances in Cryptology — ASIACRYPT '94 (Proc. 4th International Conference on the Theory and Applications of Cryptology. Wollongong, Australia. November 28 – December 1, 1994). Lecture Notes in Comput. Sci. V. 917. Berlin: Springer, 1995. P. 398–412.
- [48] *Нечаев А. А.* Код Кердока в циклической форме // Дискретная математика. 1989. Т. 1. Вып. 4. С. 123–139.
- [49] *Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P.* The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. V. 40. N 2. P. 301–319.

Адрес автора:

Институт математики  
им. С. Л. Соболева СО РАН,  
пр. Академика Коптюга, 4,  
Новосибирский гос. университет,  
ул. Пирогова, 2,  
630090 Новосибирск,  
Россия.  
E-mail: [tokareva@math.nsc.ru](mailto:tokareva@math.nsc.ru)  
Web: [www.math.nsc.ru/~tokareva](http://www.math.nsc.ru/~tokareva)

Статья поступила  
8 февраля 2008 г.