Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Вероятностные характеристики разностных и линейных соотношений для неоднородной линейной среды, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 1, 41–72

DOI: <https://doi.org/10.4213/mvk276>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.166.219.16

26 апреля 2023 г., 13:52:25

**Вероятностные характеристики
разностных и линейных соотношений
для неоднородной линейной среды
Ф. М. Малышев**

Математический институт им. В. А. Стеклова Российской академии наук, Москва

Получено 18.IV.2018

Аннотация. Рассматриваются разностные соотношения для операций циклического сдвига, сложения по модулю 2^n и покомпонентного сложения по модулю 2 элементов пространства $V_n = GF(2)^n$, $n \geq 2$, при различных аддитивных операциях, относительно которых вычисляются разности значений и отдельно разности каждого из аргументов.

Ключевые слова: разностный и линейный криптоанализ, модульное сложение, вероятностные соотношения

**Probabilistic characteristics of differential and linear relations
for nonhomogeneous linear medium**

F. M. Malyshev

Steklov Mathematical Institute of Russian Academy of Sciences, Moscow

Abstract. We consider differential relations for operations of cyclic shift, addition modulo 2^n and coordinate-wise addition modulo 2 on the space $V_n = GF(2)^n$, $n \geq 2$, for different additive operations used to construct differences of values and differences of both arguments.

Key words: differential and linear cryptanalysis, modular addition, probabilistic relations

Введение

В последнее время появилось большое семейство просто реализуемых блочных и поточных шифров, построенных по ARX-технологиям. Как правило, в них используются лишь операции циклических сдвигов машинных слов, модульных сложений слов и покомпонентных сложений машинных слов по модулю 2. Примерами таких шифров служат Simeck [1], Simon и Speck [2], Salsa [3], FEAL [4], Threefish [5]. Стандартная техника криптографического анализа ARX-шифров представлена в [6]. Для таких шифров разрабатываются алгоритмы автоматического поиска линейных и разностных соотношений [7, 8]. К ARX-шифрам применяются также разностный метод с низкими разностными характеристиками [9, 10], метод невозможных переходов разностей [11], усеченный разностный метод [12], интегральный метод [13].

В этой связи могут представлять интерес задачи по нахождению и оптимизации разностных характеристик в самых общих ситуациях. Приведем возникающие при этом задачи, рассматриваемые в настоящей работе и относящиеся к двум видам сложений на множестве V_n : $+$ и $\oplus$. Через $\oplus$ обозначаем покомпонентное сложение векторов по модулю 2, а через $+$ обозначаем сложение по модулю 2^n . В последнем случае векторы пространства V_n рассматриваются (при некоторой упорядоченности их компонент) как стандартные двоичные представления вычетов по модулю 2^n . Считаем, что $V_n = \mathbb{Z}_{2^n}$, и двоичное представление вычета 2^{n-1-i} , $i=0, 1, \dots, n-1$, задается вектором $e_i \in V_n = GF(2)^n$ с единственной ненулевой компонентой с номером i . Нам будет удобно в зависимости от ситуации элементы множества $V_n = \mathbb{Z}_{2^n}$ называть как векторами, так и вычетами. К обозначению $\mathbb{Z}_{2^n}$ прибегаем в ситуациях, когда на первом плане значится операция $+$.

Пусть $(*_1, *_2, *_3)$ — любой из 8 возможных наборов операций из множества $\{+, \oplus\}^3$. Будем рассматривать *разностные характеристики*:

$$\begin{aligned} p_{*_1\alpha; *_2\beta; *_3\gamma}^{\oplus} &= \mathbf{P}\{(x_1 *_1 \alpha) \oplus (x_2 *_2 \beta) = (x_1 \oplus x_2) *_3 \gamma\}, \\ p_{*_1\alpha; *_2\beta; *_3\gamma}^{+} &= \mathbf{P}\{(x_1 *_1 \alpha) + (x_2 *_2 \beta) = (x_1 + x_2) *_3 \gamma\}, \\ p_{*_1\alpha; *_2\gamma}^{\lll s} &= \mathbf{P}\{[(x *_1 \alpha) \lll s] = [x \lll s] *_2 \gamma\}, \\ p_{*_1\alpha; *_2\gamma}^{\text{id}} &= \mathbf{P}\{x *_1 \alpha = x *_2 \gamma\}. \end{aligned}$$

Здесь x, x_1, x_2 — независимые случайные векторы с равномерными распределениями на V_n , $\alpha, \beta, \gamma \in V_n$ — фиксированные векторы, определяющие разностные соотношения, $\lll s$ — циклический сдвиг влево на $s \in \{1, \dots, n-1\}$ позиций, $\text{id}: V_n \rightarrow V_n$ — тождественная подстановка.

Приведем два списка задач: один по нахождению разностных характеристик, другой по максимизации разностных характеристик.

Первый список составляют задачи $\mathcal{A}_i$, $i = 1, \dots, 11$, по нахождению разностных характеристик для конкретных наборов сложений аргументов и значений операций:

$$\begin{aligned}\mathcal{A}_1: p_{+\alpha,+\beta;+\gamma}^{\oplus}, \mathcal{A}_2: p_{+\alpha,+\beta;\oplus\gamma}^{\oplus}, \mathcal{A}_3: p_{\oplus\alpha,\oplus\beta;+\gamma}^{\oplus}, \\ \mathcal{A}_4: p_{+\alpha,+\beta;\oplus\gamma}^+, \mathcal{A}_5: p_{\oplus\alpha,+\beta;+\gamma}^+, \mathcal{A}_6: p_{\oplus\alpha,+\beta;\oplus\gamma}^+, \\ \mathcal{A}_7: p_{\oplus\alpha,\oplus\beta;+\gamma}^+, \mathcal{A}_8: p_{\oplus\alpha,\oplus\beta;\oplus\gamma}^+, \mathcal{A}_9: p_{\oplus\alpha;+\gamma}^{\lll s}, \\ \mathcal{A}_{10}: p_{+\alpha;+\gamma}^{\lll s}, \mathcal{A}_{11}: p_{\oplus\alpha;+\gamma}^{\text{id}}.\end{aligned}$$

Задачи $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$ приведенного списка относятся к операции

$$\oplus: V_n \times V_n \rightarrow V_n.$$

Задачи $\mathcal{A}_4$, $\mathcal{A}_5$, $\mathcal{A}_6$, $\mathcal{A}_7$, $\mathcal{A}_8$ списка относятся к операции

$$+: V_n \times V_n \rightarrow V_n.$$

Серии задач $\mathcal{A}_9$, $\mathcal{A}_{10}$ относятся к операциям

$$\lll s: V_n \rightarrow V_n, \quad s = 1, \dots, n-1.$$

Задачу $\mathcal{A}_{11}$ можно было бы отнести к серии задач $\mathcal{A}_9$ с дополнительным значением параметра $s = n$, но она выделена особо в силу своей уникальности: задача вычисления разностных характеристик для тождественной подстановки оказалась содержательной.

В первый список не вошли тривиальные задачи вычисления разностных характеристик:

$$p_{\oplus\alpha,\oplus\beta;\oplus\gamma}^{\oplus}, \quad p_{+\alpha,+\beta;+\gamma}^+, \quad p_{\oplus\alpha;\oplus\gamma}^{\lll s}, \quad p_{+\alpha;+\gamma}^{\text{id}}, \quad p_{\oplus\alpha;\oplus\gamma}^{\text{id}}.$$

Не приведены также задачи, непосредственно сводящиеся к перечисленным. Например, вычисление

$$p_{+\alpha,\oplus\beta;+\gamma}^{\oplus} = p_{+\alpha,+\gamma;\oplus\beta}^{\oplus}$$

сводится к задаче $\mathcal{A}_2$, а вычисление

$$p_{+\alpha,\oplus\beta;+\gamma}^+ = p_{\oplus\beta,+\alpha;+\gamma}^+$$

сводится к задаче $\mathcal{A}_5$. Аналогично:

$$p_{+\alpha;\oplus\gamma}^{\lll s} = p_{\oplus\gamma;+\alpha}^{\lll (n-s)}, \quad p_{+\alpha;\oplus\gamma}^{\text{id}} = p_{\oplus\gamma;+\alpha}^{\text{id}}.$$

Вероятностные разностные соотношения шифрпреобразований в разностном методе криптографического анализа строятся с помощью цепочек согласованных локальных разностных вероятностных соотношений, относящихся к отдельным операциям [14–16]. Целевая функция в разностном методе, которая максимизируется за счет выбора конкретной цепочки согласованных локальных разностных вероятностных соотношений, является произведением локальных разностных характеристик. По этой причине при построении указанных цепочек часто приходится прибегать к максимизации вероятностей $p_{*1\alpha, *2\beta; *3\gamma}^*$, $*, *1, *2, *3 \in \{+, \oplus\}$, когда заданы один или два из параметров $\alpha, \beta, \gamma \in V_n$, а нужно определить значения оставшихся параметров, при которых достигается максимум рассматриваемой вероятности. Аналогичные максимизации приходится проводить и для вероятностей $p_{*1\alpha; *2\gamma}^{\lll s}$, $s = 1, \dots, n-1, n$, $*1, *2 \in \{+, \oplus\}$ (при $s = n$ для тождественной подстановки это тоже содержательные задачи). Приведем возникающий в связи с этим второй список задач. Как и при составлении первого списка задач $\mathcal{A}_1, \dots, \mathcal{A}_{11}$, из нескольких задач, сводящихся одна к другой, указана только одна:

$$\begin{aligned} \mathcal{B}_1: \max_{\alpha} p_{+\alpha, +\beta; +\gamma}^{\oplus}, \mathcal{B}_2: \max_{\alpha, \beta} p_{+\alpha, +\beta; +\gamma}^{\oplus}, \mathcal{B}_3: \max_{\alpha} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \\ \mathcal{B}_4: \max_{\gamma} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_5: \max_{\alpha, \gamma} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_6: \max_{\alpha, \beta} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \\ \mathcal{B}_7: \max_{\alpha} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \mathcal{B}_8: \max_{\gamma} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \mathcal{B}_9: \max_{\alpha, \beta} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \\ \mathcal{B}_{10}: \max_{\alpha, \gamma} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \mathcal{B}_{11}: \max_{\alpha} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{12}: \max_{\gamma} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \\ \mathcal{B}_{13}: \max_{\alpha, \beta} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{14}: \max_{\alpha, \gamma} p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{15}: \max_{\alpha} p_{\oplus\alpha, +\beta; +\gamma}^{\oplus}, \\ \mathcal{B}_{16}: \max_{\beta} p_{\oplus\alpha, +\beta; +\gamma}^{\oplus}, \mathcal{B}_{17}: \max_{\gamma} p_{\oplus\alpha, +\beta; +\gamma}^{\oplus}, \mathcal{B}_{18}: \max_{\alpha, \beta} p_{\oplus\alpha, +\beta; +\gamma}^{\oplus}, \\ \mathcal{B}_{19}: \max_{\alpha, \gamma} p_{\oplus\alpha, +\beta; +\gamma}^{\oplus}, \mathcal{B}_{20}: \max_{\beta, \gamma} p_{\oplus\alpha, +\beta; +\gamma}^{\oplus}, \mathcal{B}_{21}: \max_{\alpha} p_{\oplus\alpha, +\beta; \oplus\gamma}^{\oplus}, \\ \mathcal{B}_{22}: \max_{\beta} p_{\oplus\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{23}: \max_{\gamma} p_{\oplus\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{24}: \max_{\alpha, \beta} p_{\oplus\alpha, +\beta; \oplus\gamma}^{\oplus}, \\ \mathcal{B}_{25}: \max_{\alpha, \gamma} p_{\oplus\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{26}: \max_{\beta, \gamma} p_{\oplus\alpha, +\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{27}: \max_{\alpha} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \\ \mathcal{B}_{28}: \max_{\gamma} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \mathcal{B}_{29}: \max_{\alpha, \beta} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \mathcal{B}_{30}: \max_{\alpha, \gamma} p_{\oplus\alpha, \oplus\beta; +\gamma}^{\oplus}, \\ \mathcal{B}_{31}: \max_{\alpha} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{32}: \max_{\gamma} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{33}: \max_{\alpha, \beta} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^{\oplus}, \\ \mathcal{B}_{34}: \max_{\alpha, \gamma} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^{\oplus}, \mathcal{B}_{35}: \max_{\alpha} p_{\oplus\alpha; +\gamma}^{\lll s}, \mathcal{B}_{36}: \max_{\gamma} p_{\oplus\alpha; +\gamma}^{\lll s}, \\ \mathcal{B}_{37}: \max_{\alpha} p_{+\alpha; +\gamma}^{\lll s}, \mathcal{B}_{38}: \max_{\alpha} p_{\oplus\alpha; +\gamma}^{\text{id}}, \mathcal{B}_{39}: \max_{\gamma} p_{\oplus\alpha; +\gamma}^{\text{id}}. \end{aligned}$$

Ниже в разделе 1 решаются задачи $\mathcal{A}_{11}$, $\mathcal{B}_{38}$, $\mathcal{B}_{39}$. В качестве следствий получаются решения задач $\mathcal{A}_3, \mathcal{A}_4, \mathcal{A}_5, \mathcal{A}_9, \mathcal{B}_7, \dots, \mathcal{B}_{20}, \mathcal{B}_{35}, \mathcal{B}_{36}$. В разделе 2 решаются задачи $\mathcal{A}_8, \mathcal{B}_{31}, \dots, \mathcal{B}_{34}$. Нерешенными остаются 5 из 11 задач по нахождению разностных характеристик и 17 из 39 задач по максимизации разностных характеристик. Всего в настоящей работе представлено решение 28 задач из 50 сформулированных.

1. Разностные характеристики для тождественной подстановки

В этом разделе решаются три выше заявленные задачи для разностных соотношений тождественной подстановки. Сначала для произвольных $\alpha, \beta \in \mathbb{Z}_{2^n}$ и равновероятных $x \in \mathbb{Z}_{2^n}$ ниже в теореме 1 вычисляются вероятности

$$p_{\oplus\alpha;+\beta}^{\text{id}} = \mathbf{P}\{x \oplus \alpha = x + \beta\}.$$

В качестве следствия к теореме 1 получим значения $\max_{\beta} p_{\oplus\alpha;+\beta}^{\text{id}}$. Наконец, в теореме 2 находится $\max_{\alpha} p_{\oplus\alpha;+\beta}^{\text{id}}$ и определяются все векторы $\alpha \in V_n$, на которых этот максимум достигается. Такие векторы α будем называть *экстремальными*.

1.1

Далее, как уже условились, вычеты $\alpha \in \mathbb{Z}_{2^n}$ представляем в двоичном виде, располагая цифры слева направо в естественном порядке, начиная со старших и заканчивая младшими:

$$\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) = \alpha_0 2^{n-1} + \alpha_1 2^{n-2} + \dots + \alpha_{n-2} 2 + \alpha_{n-1}.$$

Для $\alpha \in \mathbb{Z}_{2^n}$ полагаем

$$[\alpha] = \{i \in \{1, \dots, n-1\} | \alpha_i = 1\} = \{i_1, \dots, i_r\}, \quad i_1 < \dots < i_r, \quad r \geq 0.$$

Определим подмножество $B(\alpha) \subset \mathbb{Z}_{2^n}$ следующим образом:

$$\begin{aligned} B(\alpha) &= B(\alpha_0; [\alpha]) = B(\alpha_0; i_1, \dots, i_r) = \\ &= \left\{ \alpha_0 2^{n-1} + \sum_{i \in [\alpha]} \varepsilon_i 2^{n-1-i} \mid \varepsilon_i \in \{1, -1\} \forall i \in [\alpha] \right\}. \end{aligned}$$

Далее для удобства выписывания формул формально полагаем $i_0 = 0$, $i_{r+1} = n$, $\varepsilon_{i_{r+1}} = \varepsilon_n = 1$.

1.1.1. Индукцией по $r \geq 0$ легко убедиться в том, что $|B(\alpha)| = 2^r$, а векторы β из $B(\alpha)$ естественным образом разбиваются на $r+1$ *подвекторов* $\beta^{(1)}, \dots, \beta^{(r)}, \beta^{(r+1)}$ с номерами компонент $i_{j-1}, i_{j-1}+1, \dots, i_j-1, j=1, \dots, r, r+1$, причем $\beta^{(r+1)} = (1, 0, \dots, 0)$, $\beta^{(1)} \in \{(\alpha_0, 0, \dots, 0), (\alpha_0 \oplus 1, 1, \dots, 1)\}$, $\beta^{(j)} \in \{(1, 0, \dots, 0), (0, 1, \dots, 1)\}, j=2, \dots, r$. (При $r=0$ имеем $\beta = \beta^{(1)} = (\alpha_0, 0, \dots, 0) = \alpha$.) Первый подвектор в паре отвечает значению $\varepsilon_{i_j} = 1$, а второй подвектор — значению $\varepsilon_{i_j} = -1, j=1, \dots, r$.

Этим устанавливается биекция между векторами из $B(\alpha)$ и наборами

$$(\varepsilon_i \mid i \in [\alpha]) = (\varepsilon_{i_1}, \dots, \varepsilon_{i_r}) \in \{1, -1\}^r.$$

Индуктивный переход состоит в построении множества

$$B(\alpha) = B(\alpha_0; i_1, \dots, i_{r-1}, i_r)$$

по множеству

$$B(\alpha \oplus e_{i_r}) = B(\alpha_0; i_1, \dots, i_{r-1}) :$$

для каждого $z \in B(\alpha_0; i_1, \dots, i_{r-1})$ вычисляются $z + 2^{n-1-i_r}$ и $z - 2^{n-1-i_r}$, принадлежащие $B(\alpha_0; i_1, \dots, i_{r-1}, i_r)$. Обратим внимание, что длины 0-серий и 1-серий у подвекторов $\beta^{(j)}$, $j = 1, 2, \dots, r, r+1$, равны $i_j - 1 - i_{j-1}$, и при $i_j = i_{j-1} + 1$ эти серии отсутствуют.

Приведенные выше рассуждения п. 1.1.1 продемонстрируем в формулах (1) на четырех возможных фрагментах последовательностей цифр вычета β для $\varepsilon_{i_1}, \varepsilon_{i_2}, \varepsilon_{i_j}, \varepsilon_{i_{j+1}}, \varepsilon_{i_{r-1}}, \varepsilon_{i_r} \in \{+1, -1\}$. В (1) значение $+1$ обозначено символом $+$, а значение -1 обозначено символом $-$. Значения $\varepsilon_{i_{j-1}} \in \{+1, -1\}$ в (1) не конкретизируются. Значения β_{i_2} и $\beta_{i_{j+1}}$, помеченные символом $*$, зависят соответственно от ε_{i_3} и $\varepsilon_{i_{j+2}}$:

$$\beta_{i_2} = 1 \Leftrightarrow \varepsilon_{i_3} = 1, \quad \beta_{i_{j+1}} = 1 \Leftrightarrow \varepsilon_{i_{j+2}} = 1.$$

$$\begin{array}{cccccccccccc} 0 & 1 & i_1 & i_2 & i_{j-1} & i_j & i_{j+1} & i_{r-1} & i_r & n-1 \\ \text{a) } \alpha_0 & 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[*]} \dots \overset{+}{[1]} 0 \dots 0 & \overset{*}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[*]} \dots & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 \\ \text{b) } \alpha_0 \oplus 1 & (1 \dots 1 \overset{-}{[1]} 0 \dots 0 & \overset{+}{[*]} \dots \overset{*}{[0]} (1 \dots 1 \overset{-}{[1]} 0 \dots 0 & \overset{+}{[*]} \dots & \overset{-}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 & \overset{+}{[1]} 0 \dots 0 \\ \text{c) } \alpha_0 & 0 \dots 0 & \overset{+}{[0]} (1 \dots 1 \overset{-}{[*]} \dots \overset{*}{[1]} 0 \dots 0 & \overset{+}{[0]} (1 \dots 1 \overset{-}{[*]} \dots \overset{+}{[0]} (1 \dots 1 \overset{-}{[*]} \dots \overset{+}{[0]} (1 \dots 1 \overset{-}{[1]} 0 \dots 0 \\ \text{d) } \alpha_0 \oplus 1 & (1 \dots 1 \overset{-}{[0]} (1 \dots 1 \overset{-}{[*]} \dots \overset{*}{[0]} (1 \dots 1 \overset{-}{[0]} (1 \dots 1 \overset{-}{[*]} \dots \overset{-}{[0]} (1 \dots 1 \overset{-}{[1]} 0 \dots 0 \end{array} \quad (1)$$

Скобками в (1) выделены вырожденные интервалы $[i_s, i_s]$ при $\varepsilon_{i_s} = 1$ и полуинтервалы $(i_{s-1}, i_s]$ при $\varepsilon_{i_s} = -1$, $s \in \{1, \dots, r\}$. Напомним, что серии нулей $0 \dots 0$ и единиц $1 \dots 1$ в (1) будут отсутствовать при $i_j = i_{j-1} + 1$, $j = 1, \dots, r, r+1$ (см. ниже (3), (4), (5)).

Теорема 1. Для $\alpha \in \mathbb{Z}_{2^n}$ имеем:

$$p_{\oplus \alpha; +\beta}^{\text{id}} = \begin{cases} 2^{-|\alpha|} & \text{для } \beta \in B(\alpha), \\ 0 & \text{для } \beta \notin B(\alpha). \end{cases}$$

Доказательство. Для $x \in \mathbb{Z}_{2^n}$ положим $\varepsilon_i(x) = 1$, если $x = 0$, и $\varepsilon_i(x) = -1$, если $x = 1$, $i = 0, 1, \dots, n-1$. Равенство $x \oplus \alpha = x + \beta$ означает, что

$$\begin{aligned} \beta &= (x \oplus \alpha) - x = (x \oplus \alpha_0 e_0 \oplus e_{i_1} \oplus \dots \oplus e_{i_r}) - x = \\ &= (\dots ((x \oplus \alpha_0 e_0) \oplus e_{i_1}) \oplus \dots \oplus e_{i_{r-1}}) \oplus e_{i_r} - x = \\ &= (x_0 \oplus \alpha_0) 2^{n-1} + \sum_{i=1}^{n-1} x_i 2^{n-1-i} + \varepsilon_{i_1}(x) 2^{n-1-i_1} + \dots + \varepsilon_{i_r}(x) 2^{n-1-i_r} - \\ &\quad - x_0 2^{n-1} - \sum_{i=1}^{n-1} x_i 2^{n-1-i} = \alpha_0 2^{n-1} + \sum_{i \in [\alpha]} \varepsilon_i(x) 2^{n-1-i}. \end{aligned}$$

В полученном выражении конкретное $\beta \in \mathbb{Z}_{2^n}$ получается ровно для $2^{n-|\alpha|}$ значений $x \in \mathbb{Z}_{2^n}$. Предполагая x случайным с равномерным распределением вероятностей на множестве $\mathbb{Z}_{2^n}$, для $\beta \in B(\alpha)$ получаем $p_{\oplus\alpha;+\beta}^{\text{id}} = 2^{n-|\alpha|}/2^n = 2^{-|\alpha|}$. Теорема 1 доказана. $\square$

Конструктивное задание всех элементов множества $B(\alpha)$, приведенное в п. 1.1.1 перед формулировкой теоремы 1, может оказаться полезным при поиске подходящих вероятностных разностных соотношений путем построения цепочек согласованных локальных разностных соотношений.

1.2

Приступим теперь к задаче по нахождению $\max_{\alpha} p_{\oplus\alpha;+\beta}^{\text{id}}$. Ввиду равенства $p_{\oplus\alpha;+\beta}^{\text{id}} = p_{\oplus(\alpha \oplus 2^{n-1});+(\beta \oplus 2^{n-1})}^{\text{id}}$ можно ограничиться значениями $\beta \in \{1, \dots, 2^{n-1}-1\}$, когда $\beta \neq 0$, а $\beta_0 = 0$. По теореме 1 имеем $p_{\oplus\alpha;+\beta}^{\text{id}} = 2^{-|\alpha|}$ для $\beta \in B(\alpha)$ и $p_{\oplus\alpha;+\beta}^{\text{id}} = 0$ для $\beta \notin B(\alpha)$, поэтому вычисление $\max_{\alpha} p_{\oplus\alpha;+\beta}^{\text{id}}$ при заданном $\beta \in \mathbb{Z}_{2^n}$ отвечает нахождению вектора $\alpha \in V_n$ с минимальным значением $|\alpha|$, для которого $\beta \in B(\alpha)$.

В формулируемой далее теореме 2, в которой кроме указания собственно значения $\max_{\alpha} p_{\oplus\alpha;+\beta}^{\text{id}}$ будут указаны все векторы α , называемые *каноническими*, на которых этот максимум достигается. Знание именно всех экстремальных (канонических) векторов α является важным при построении цепочек согласованных локальных разностных вероятностных соотношений с максимальными произведениями локальных разностных характеристик. При заданном $\beta \in \mathbb{Z}_{2^n}$ множество канонических векторов в общем случае имеет большую мощность и нетривиальное конструктивное задание, связанное с вводимыми далее в пп. 1.2.1, 1.2.3 *каноническими покрытиями* множества $[\beta] = \{i \in \{1, \dots, n-1\} \mid \beta_i = 1\}$ и специальными характеристиками $\mathcal{H} = \mathcal{H}(\beta)$ вычета β . Все эти понятия, естественно, приходится вводить перед формулировкой теоремы 2.

$$\begin{aligned}\beta &= \alpha_\varepsilon = \alpha_0 2^{n-1} + \sum_{j=1}^r \varepsilon_{i_j} 2^{n-1-i_j} = \\ &= \alpha_0 2^{n-1} + \varepsilon_{i_1} 2^{n-1-i_1} + \varepsilon_{i_2} 2^{n-1-i_2} + \dots + \varepsilon_{i_r} 2^{n-1-i_r},\end{aligned}\tag{2}$$

Ниже в формулах (3)–(5) приведены примеры фрагментов последовательностей цифр вычетов $\beta \in \{1, \dots, 2^{n-1} - 1\}$ и векторов $\alpha \in V_n$, для которых $\beta \in B(\alpha)$, $\beta = \alpha_\varepsilon$, $\varepsilon \in \{1, -1\}^{|\alpha|}$. В них указаны полуинтервалы и вырожденные интервалы. Номера из множества $[\alpha]$, как и в (1), выделены знаками «+» и «-». Знак «+» в позиции i означает, что $\alpha_i = 1$, $\varepsilon_i = 1$, а знак «-» в позиции i означает, что $\alpha_i = 1$, $\varepsilon_i = -1$. Для остальных $i \in \{1, \dots, n-1\}$ имеем $\alpha_i = 0$. Проверка равенств $\beta = \alpha_\varepsilon$ в этих примерах осуществляется по формуле (2) добавлением величин $\varepsilon_{i_j} 2^{n-1-i_j}$ в естественном порядке: последовательно для $j = 1, 2, \dots, r$. Так как $\beta_0 = 0$, то значение $\alpha_0 \in \{0, 1\}$ в равенстве (2) однозначно определяется по значению $\varepsilon_{i_1} \in \{1, -1\}$: $\alpha_0 = 1 \Leftrightarrow \varepsilon_{i_1} = -1$.

$$\dots 00[1]_0^+ [0]_1^+ [1]_0^+ [0]_1^+ (10]_1^- (10]_1^- (1110]_1^- (10]_1^- (110]_1^- (10]_1^- (11110]_1^- (10]_1^- (10]_1^- (1]_0^+ [0]_1^+ [0]_1^+ 00 \dots \quad (3)$$

$$\begin{array}{cccccccccccc} - & - & - & - & - & - & - & + & + & & \\ (10) & (10) & (10) & (0) & (10) & (110) & (10) & (111) & 0 & 1 & 0 & 1 & 00 \dots \end{array} \quad (4)$$

$$\begin{aligned}
& (\bar{1}0)(\bar{1}0)(\bar{1})00^+(\bar{1}0)(\bar{1}1\bar{0})(\bar{1}0)(\bar{1}1\bar{1})0[\bar{1}]0[\bar{1}]00\dots \\
& (\bar{1}0)(\bar{1})0[\bar{1}]00^+(\bar{1}0)(\bar{1}1\bar{0})(\bar{1}0)(\bar{1}1\bar{1})0[\bar{1}]0[\bar{1}]00\dots \\
& [\bar{1}]0[\bar{1}]0[\bar{1}]00^+[\bar{1}]0^+(\bar{1}1\bar{0})(\bar{1}0)(\bar{1}11\bar{0})(\bar{1})0[\bar{1}]00\dots
\end{aligned} \tag{5}$$

Отметим, что примеры (4), (5) относятся к одному и тому же вычету β , но к различным покрытиям множества $[\beta]$ полуинтервалами и вырожденными интервалами.

В полуинтервале $(i_{j-1}, i_j]$ точку i_{j-1} назовем *левым концом*, i_j — *правым*. В случае $\varepsilon_{i_j} = \varepsilon_{i_{j+1}} = -1$, $j \in \{1, \dots, r-1\}$, номер i_j называем *точкой соприкосновения* полуинтервалов $(i_{j-1}, i_j]$ и $(i_j, i_{j+1}]$. Для точек соприкосновения i_j , содержащихся в объединении полуинтервалов, обязательно $\beta_{i_j} = 0$, т.е. $i_j \notin [\beta]$. Для всех остальных номеров i из объединения этих полуинтервалов обязательно $\beta_i = 1$, $i \in [\beta]$.

Обозначим

$$B^{[-1]}(\beta) = \{\alpha \in V_n \mid \beta \in B(\alpha)\}.$$

Каждым $\alpha \in B^{[-1]}(\beta)$ и $\varepsilon \in \{1, -1\}^{[\alpha]}$ таким, что $\alpha_\varepsilon = \beta$, отвечает покрытие множества $[\beta]$ полуинтервалами (назовем их α -полуинтервалами) и особыми точками $i_j \in [\alpha]$ с $\varepsilon_{i_j} = \varepsilon_{i_{j+1}} = 1$. (Согласно п. 1.1.1 элементы последовательности $\varepsilon \in \{1, -1\}^{[\alpha]}$ однозначно определяются по α и β . В этом можно убедиться и непосредственно с помощью равенств (1) и (2).) Покрытия множества $[\beta]$, состоящие из вырожденных интервалов и полуинтервалов, отвечающие элементам $\alpha \in B^{[-1]}(\beta)$, назовем α -покрытиями. Подмножество $[\alpha] \subseteq \{1, \dots, n-1\}$ состоит из концов α -полуинтервалов и особых точек α -покрытия. Подмножество $[\beta] \subseteq \{1, \dots, n-1\}$ исчерпывается особыми точками α -покрытия и целочисленными точками из α -полуинтервалов, за исключением точек соприкосновения.

Если $i_j = i_{j-1} + 1$ и $\varepsilon_{i_j} = \varepsilon_{i_{j+1}} = -1$, то полуинтервал $(i_{j-1}, i_j]$ содержит единственную целочисленную точку i_j с $\beta_{i_j} = 0$. Тем не менее такой полуинтервал $(i_{j-1}, i_j]$, называемый далее *вырожденным полуинтервалом*, будем считать α -полуинтервалом, относящимся к α -покрытию, даже если этот полуинтервал и не содержит ни одного номера i из $[\beta]$. Вырожденный полуинтервал имеется в примере (4).

1.2.1. Для определения канонического покрытия множества $[\beta]$ среди элементов последовательности $\beta_1, \dots, \beta_{n-1}$ выделим максимальные серии подряд идущих единиц (*1-серии*) длины $l \geq 1$. Соответствующее подмножество номеров единичных координат в $\{1, \dots, n-1\}$ тоже будем называть *1-серией*. Аналогично номер $i \in \{1, \dots, n-1\}$ в случае $\beta_i = 0$ или $\beta_i = 1$ иногда будем называть соответственно нулевой или единичной точкой. Две соседние 1-серии считаем *связанными*, если между ними располагается ровно один нуль, а если между ними располагается более одного нуля, то эту пару 1-серий считаем просто *соседними*. Множество $[\beta]$ разбивается на компоненты связанных 1-серий, называемых далее просто *компонентами*. Число 1-серий в компоненте K обозначим через h_K , через I_K — минимальный номер в компоненте K , а через J_K — максимальный номер в компоненте K . Множество всех компонент в $[\beta]$ обозначим через $\mathcal{K}$.

Будем различать компоненты типов I, II и III.

К типу I относятся компоненты, в которых все 1-серии имеют длину $l = 1$.

К типу II относятся компоненты, в которых ровно одна 1-серия имеет длину $l = 2$, а остальные 1-серии (если они есть) имеют длину 1.

К типу III относятся все остальные компоненты.

Будем также различать компоненты с параметром $I_K = 1$ и компоненты с параметром $I_K > 1$. Таким образом, предусматривается 6 типов компонент. Компоненты типа I с параметром $I_K > 1$ будем называть *однородными*. Компоненты остальных 5 типов будем называть *неоднородными*. Через $\mathcal{K}_0$ обозначим множество однородных компонент в $[\beta]$, через $\mathcal{K}_1$ — множество неоднородных компонент в $[\beta]$: $\mathcal{K} = \mathcal{K}_0 \sqcup \mathcal{K}_1$.

Приступим теперь непосредственно к заданию канонического покрытия непустого подмножества $[\beta] \subseteq \{1, \dots, n-1\}$, $\beta \in \{1, \dots, 2^{n-1}-1\}$, вырожденными интервалами $[j, j]$, $j \in \{1, \dots, n-1\}$, содержащими единичные точки, и полуинтервалами $(j, k]$ с целочисленными концами $j, k \in \{0, 1, \dots, n-1\}$. Напомним, что номер k для соприкасающихся полуинтервалов $(j, k]$ и $(k, l]$ выше был назван точкой соприкосновения.

Вначале некоторые (не обязательно все) из пар соседних неоднородных компонент $K_1, K_2 \in \mathcal{K}_1$, между которыми располагаются ровно два нуля (т. е. $J_{K_1} + 3 = I_{K_2}$), объявляем *близкими*. Нулевые номера $(J_{K_1} + 1, I_{K_2} - 1)$ при этом будем называть *связующей парой*. (Отношение близости, которое вводится на множестве неоднородных компонент $\mathcal{K}_1$, может быть произвольным. Допускается, например, отсутствие близких пар K_1, K_2 . Напротив, все соседние пары $K_1, K_2 \in \mathcal{K}_1$, разделяющиеся ровно двумя нулями, могут быть объявлены близкими.) Максимальную последовательность из попарно близких неоднородных компонент назовем *блоком*. Неоднородную компоненту, не являющуюся близкой к соседним неоднородным компонентам, тоже будем считать блоком.

Как и для компонент, число 1-серий в блоке B обозначим через h_B , через I_B — минимальный номер в блоке B , а через J_B — максимальный номер в блоке B . Множество всех блоков в $[\beta]$ обозначим через $\mathcal{B}$. Через $\mathcal{K}_B$ обозначим множество компонент в блоке $B \in \mathcal{B}$: $\mathcal{K}_1 = \bigsqcup_{B \in \mathcal{B}} \mathcal{K}_B$, $h_B = \sum_{K \in \mathcal{K}_B} h_K$. Пусть также $\kappa_B = |\mathcal{K}_B|$, $\kappa_1 = |\mathcal{K}_1|$,

$$\mathcal{H} = \mathcal{H}(\beta) = \sum_{K \in \mathcal{K}} h_K + \kappa_1 + \delta, \quad \text{где} \quad \delta = \delta(\beta) = \begin{cases} -1, & \text{если } 1 \in \bigsqcup_{K \in \mathcal{K}_1} K, \\ 0 & \text{иначе.} \end{cases}$$

1.2.2. Все дальнейшие положения определения канонического покрытия полезно проверять на конкретных примерах (3), (4), (5) канонических покрытий соответственно блока из одной неоднородной компоненты, блока из двух компонент, двух различных канонических покрытий тех же двух компонент, но не объявленных близкими. В примерах (4) и (5) левая неоднородная компонента относится к типу I с параметром $I = 1$.

1.2.3. Каноническое покрытие множества $[\beta]$ состоит из канонических покрытий отдельных блоков и однородных компонент.

Каноническое покрытие однородной компоненты состоит только из вырожденных интервалов, содержащих единичные точки.

Каноническое покрытие каждого блока $B \in \mathcal{B}$ состоит из вырожденных интервалов, содержащих единичные точки, и ровно одной *цепи* последовательно соприкасающихся полуинтервалов. (Цепь может состоять только из одного полуинтервала.) В эту цепь входят вырожденные полуинтервалы $(J_{K_1} + 1, I_{K_2} - 1]$ для всех связующих пар $(J_{K_1} + 1, I_{K_2} - 1)$ блока B . Вырожденными интервалами накрываются несколько (не обязательно все) первых и несколько (тоже не обязательно все) последних подряд идущих изолированных точек блока (1-серий длины $l = 1$). Остальные изолированные единичные точки блока накрываются полуинтервалами цепи. Каждая 1-серия накрывается своим полуинтервалом или вырожденным интервалом.

Если параметр $I_B = 1$, то вырожденные интервалы могут накрывать только несколько последних подряд идущих изолированных вершин блока B . Если $I_B = 2$, то цепь в блоке B может начинаться самым левым вырожденным полуинтервалом $(0, 1]$. Общее число невырожденных полуинтервалов и вырожденных интервалов равно числу 1-серий в блоке B , обозначенному выше через h_B . Для точек соприкосновения полуинтервалов $i \in \{1, \dots, n-1\}$ обязательно $\beta_i = 0$. В каждом полуинтервале, кроме самого правого полуинтервала в цепи, имеется ровно один нуль, отвечающий правому концу полуинтервала. Самый правый полуинтервал в цепи состоит только из единиц (из элементов подмножества $[\beta]$). Если блок состоит из одной неоднородной компоненты K типа II с $I_K > 1$ или из одной неоднородной компоненты типа I с $I_K = 1$, то покрытие этого блока соответственно из $h_K + 1$ или h_K вырожденных интервалов, содержащих единичные точки, тоже (как исключение) будем считать каноническим покрытием, хоть в нем и отсутствует цепь из полуинтервалов.

Подмножество $[\alpha] \subseteq \{1, \dots, n-1\}$, задающее соответствующий канонический вектор $\alpha \in B^{[-1]}(\beta)$, состоит из концов (кроме i_0) полуинтервалов (включая вырожденные) и вырожденных интервалов канонического покрытия.

Для выписанного в (2) представления $\beta = \alpha_\varepsilon$, которое будем называть *каноническим представлением* в случае канонического вектора α , следует полагать $\varepsilon_i = 1$ для i из вырожденных интервалов и для $i \neq i_0$, являющихся левыми концами самых левых полуинтервалов в цепях для всех блоков. Для остальных $i \in [\alpha]$ необходимо полагать $\varepsilon_i = -1$. Так как $\beta_0 = 0$, то полагаем

$$\alpha_0 = 1 \Leftrightarrow \varepsilon_{i_1} = -1.$$

Покажем, что из определения канонического вектора α следует принципиально важное равенство

$$|[\alpha]| = \mathcal{H}(\beta). \quad (6)$$

Здесь $|[\alpha]|$ зависит от канонического покрытия множества $[\beta]$, зависящего, в свою очередь, от введенного отношения близости на множестве $\mathcal{K}_1$ и от задаваемого множества вырожденных интервалов, а величина

$$\mathcal{H} = \mathcal{H}(\beta) = \sum_{K \in \mathcal{K}} h_K + \kappa_1 + \delta$$

однозначно определяется по множеству $[\beta]$, является его характеристикой. Если в множестве $\mathcal{K}_1$ отсутствуют близкие пары неоднородных компонент K_1, K_2 , то равенство (6) непосредственно следует из определений канонического покрытия и канонического вектора, поскольку каждой 1-серии в множестве $[\beta]$ отвечает свой полуинтервал или вырожденный интервал в каноническом покрытии, а в множество $[\alpha]$, кроме правых концов полуинтервалов и вырожденных интервалов, дополнительно входят еще отличные от i_0 номера левых концов самых левых полуинтервалов из цепей покрытия неоднородных компонент K для всех $K \in \mathcal{K}_1$. Наличие связующей пары $(J_{K_1} + 1, I_{K_2} - 1)$ не нарушит равенство (6), так как тогда

$$J_{K_1} + 1, I_{K_2} - 1 \in [\alpha] \quad \text{при} \quad J_{K_1} \notin [\alpha].$$

Если пара $(J_{K_1} + 1, I_{K_2} - 1)$ не является связующей, то

$$J_{K_1} \in [\alpha] \quad \text{при} \quad J_{K_1} + 1 \notin [\alpha],$$

а вместо номера $I_{K_2} - 1$ в $[\alpha]$ окажется левый номер самого левого полуинтервала цепи из покрытия блока, содержащего компоненту K_2 .

1.2.4. По завершении определения канонического покрытия и канонического вектора отметим, что различные канонические покрытия одного и того же подмножества $[\beta] \subseteq \{1, \dots, n-1\}$, $\beta \in \{1, \dots, 2^{n-1}-1\}$, получим при различных отношениях близости на множестве неоднородных компонент $\mathcal{K}_1$ и при различных (в покрытиях) множествах вырожденных интервалов, содержащих единичные точки.

Теорема 2. Для произвольного $\beta \in \{1, \dots, 2^{n-1}-1\}$ с характеристикой подмножества $[\beta] \subseteq \{1, \dots, n-1\}$, равной $\mathcal{H}$, имеем $\max_{\alpha} p_{\oplus\alpha;+\beta}^{\text{id}} = 2^{-\mathcal{H}}$. Максимум достигается в точности на канонических векторах $\alpha \in V_n$, отвечающих каноническим покрытиям подмножества $[\beta]$.

Доказательство. По теореме 1

$$p_{\oplus\alpha;+\beta}^{\text{id}} = \begin{cases} 2^{-|\alpha|} & \text{для } \alpha \in B^{[-1]}(\beta) = \{\gamma \in V_n \mid \beta \in B(\gamma)\}, \\ 0 & \text{для } \alpha \notin B^{[-1]}(\beta). \end{cases}$$

Согласно (6) для канонических векторов $\alpha \in B^{[-1]}(\beta)$ имеем

$$|\alpha| = \mathcal{H} = \sum_{K \in \mathcal{K}} h_K + \kappa_1 + \delta,$$

поэтому для экстремальных векторов заведомо $|\alpha| \leq \mathcal{H}$, а для канонических векторов α обязательно $p_{\oplus\alpha;+\beta}^{\text{id}} = 2^{-\mathcal{H}}$. Теорема 2 будет доказана, если показать, что экстремальные векторы $\alpha \in B^{[-1]}(\beta)$ (с минимальным значением $|\alpha|$) являются каноническими.

Из (1) следует, что каждый вектор $\alpha \in B^{[-1]}(\beta)$, в том числе и экстремальный вектор α , задает так называемое α -покрытие множества $[\beta]$ полуинтервалами и вырожденными интервалами. Канонические векторы $\alpha \in B^{[-1]}(\beta)$ задают канонические покрытия множества $[\beta]$.

Далее доказательство теоремы 2 проведем индукцией по величине $\bar{J} = \max\{|\beta|\}$. У нас $\beta \in \{1, \dots, 2^{n-1}-1\}$, поэтому $\bar{J} \geq 1$. При $\bar{J} = 1$ имеем единственную неоднородную компоненту из одной точки: $\beta = 2^{n-2}$, $[\beta] = \{1\}$. Данная компонента K относится к типу I, является неоднородной, содержит номер 1, поэтому $\mathcal{H} = 1 + 1 - 1 = 1$. Векторы $\alpha \in B^{[-1]}(\beta)$ с $|\alpha| \leq \mathcal{H} = 1$ существуют. Например, покрытие $[\beta]$ вырожденным интервалом $[1, 1]$ соответствуют: $\alpha = e_1$, $\beta = 2^{n-2} = 0 \cdot 2^{n-1} + 1 \cdot 2^{n-2}$. Возможно еще покрытие номера 1 полуинтервалом $(0, 1]$, поэтому имеется второй экстремальный вектор $\tilde{\alpha} = e_0 \oplus e_1$, при котором $\beta = 2^{n-2} = 1 \cdot 2^{n-1} - 1 \cdot 2^{n-2}$. Других представлений (1) вычета $\beta = 2^{n-2}$ в виде

$$\alpha_0 \cdot 2^{n-1} + \varepsilon_j \cdot 2^{n-1-j}, \quad \alpha_0 \in GF(2), \quad j \in \{1, \dots, n-1\}, \quad \varepsilon_j \in \{1, -1\},$$

кроме двух выше рассмотренных канонических представлений, нет. Подчеркнем, что нас интересуют представления $\beta = \alpha_{\varepsilon}$, $\varepsilon \in \{-1, +1\}^{|\alpha|}$, только для экстремальных векторов α , поэтому $|\alpha| \leq \mathcal{H}$.

Пусть $\bar{J} = \max\{[\beta]\} > 1$ и $\alpha \in B^{[-1]}(\beta)$ — экстремальный вектор с $[\alpha] = \{i_1, \dots, i_r\}$, $0 = i_0 < i_1 < \dots < i_r < i_{r+1} = n$,

$$\beta = \alpha_0 2^{n-1} + \varepsilon_{i_1} 2^{n-1-i_1} + \dots + \varepsilon_{i_{r-1}} 2^{n-1-i_{r-1}} + \varepsilon_{i_r} 2^{n-1-i_r}, \quad (7)$$

$$\varepsilon_{i_j} \in \{1, -1\}, \quad j = 1, \dots, r.$$

Напомним, что коэффициенты $\alpha_0 \in \{0, 1\}$ и $\varepsilon_{i_j} \in \{1, -1\}$, $j = 1, \dots, r$, при заданных номерах $i_1, \dots, i_r$ однозначно задаются равенством (7) (см. (1), (2) в п. 1.1.1). Для доказательства справедливости индуктивного перехода необходимо убедиться, что экстремальное разложение $\beta = \alpha_\varepsilon$ (самое короткое, с минимально возможным значением $||[\alpha]||$), представленное в (7), является каноническим. В случае $r = 1$ это верно, проверяется непосредственно для $\varepsilon_{i_1} = 1$ (когда $\alpha_0 = 0$) и для $\varepsilon_{i_1} = -1$ (когда $\alpha_0 = 1$). В обоих случаях вектор $\alpha_0 e_0 \oplus e_{i_1}$ канонический, $\mathcal{H} = 1$: подмножество $[\beta] \subseteq \{1, \dots, n-1\}$ состоит из одной изолированной точки i_1 или из одной 1-серии, накрываемой полуинтервалом $(0, i_1]$, содержащим номер 1.

Пусть $r > 1$. Рассмотрим ненулевой вычет

$$\beta' = \beta - \varepsilon_{i_r} 2^{n-1-i_r} = \alpha_0 2^{n-1} + \varepsilon_{i_1} 2^{n-1-i_1} + \dots + \varepsilon_{i_{r-1}} 2^{n-1-i_{r-1}}, \quad (8)$$

для которого величина $\bar{J}' = \max\{[\beta']\} = i_{r-1}$ строго меньше $\bar{J} = i_r$. Рассуждая от противного, убеждаемся, что вектор

$$\alpha' = \alpha \oplus e_{i_r} \quad \text{с} \quad [\alpha'] = [\alpha \oplus e_{i_r}] = \{i_1, \dots, i_{r-1}\}$$

должен быть экстремальным для β' , иначе разложение (7) не было бы экстремальным. По предположению индукции разложение (8) отвечает каноническому покрытию множества $[\beta'] = [\beta - \varepsilon_{i_r} 2^{n-1-i_r}]$. По тем же соображениям вектор $\alpha'' = \alpha' \oplus e_{i_{r-1}}$ будет экстремальным для вычета $\beta'' = \beta' - \varepsilon_{i_{r-1}} 2^{n-1-i_{r-1}}$.

При $r = 2$ имеем

$$\beta'' = \alpha'' = \alpha_0 e_0, \quad \alpha_0 \in \{0, 1\}.$$

Такое значение для β'' не предусмотрено формулировкой теоремы 2, в которой $\beta \in \{1, \dots, 2^{n-1} - 1\}$, $[\beta] \neq \emptyset$, хотя формально теорема 2 справедлива и для $\beta \in \{0, 1, \dots, 2^{n-1} - 1, 2^{n-1}\}$. Тогда для $\beta \in \{0, 2^{n-1}\}$ имеем $[\beta] = \emptyset$, $\mathcal{K} = \emptyset$, $\mathcal{H} = \mathcal{H}(\emptyset) = 0$. Каноническим покрытием пустого множества будет пустое множество полуинтервалов и пустое множество вырожденных интервалов, а соответствующим каноническим вектором будет $\alpha = \beta$ с $[\alpha] = \emptyset$. С учетом сказанного можно считать $\bar{J} \geq \max\{\emptyset\} \stackrel{\text{def}}{=} 0$, а базу индукции можно относить к $\bar{J} \in \{0, 1\}$.

Можно было бы поступить и иначе, считая далее $r \geq 3$, разобрав предварительно случай $r = 2$ в (7) (как и случай $r = 1$) отдельно. Тогда непосредственно проверяется, что для всех четырех вычетов $\beta = \alpha_\varepsilon \in B(\alpha)$ вектор $\alpha \in B^{[-1]}(\alpha_\varepsilon)$ является каноническим. Исключение составят только случаи с $i_1 = 1$, $i_2 - i_1 = 1$ и с $i_1 > 1$, $i_2 - i_1 = 1$, $\varepsilon_{i_1} \neq \varepsilon_{i_2}$, в которых $\mathcal{H} = \mathcal{H}(\beta) = 1 < \|\alpha\|$, из-за чего, вопреки предположению, вектор α и разложение (7) не являются экстремальными.

Далее при $r \geq 2$ доказательство сводится к анализу нескольких случаев, задаваемых, главным образом, условиями $\varepsilon_{i_r} = 1$, $\varepsilon_{i_r} = -1$, $i_r - i_{r-1} = 1$, $i_r - i_{r-1} > 1$. Каждый раз, исходя из канонического разложения (8), необходимо убедиться, что либо разложение (7) является каноническим, либо вектор $\alpha = \alpha' \oplus e_{i_r}$ не является экстремальным для $\beta = \beta' + \varepsilon_{i_r} 2^{n-1-i_r}$. Последнее противоречит исходному предположению об экстремальности вектора α и разложения (7).

Обозначения, относящиеся к вычету β' , далее, как правило, будут сопровождаться штрихом.

Пусть вначале $\varepsilon_{i_r} = 1$. При $i_r - i_{r-1} > 1$ точка i_r является изолированной в множестве $[\beta]$. Тогда разложение (7) отвечает покрытию множества $[\beta]$, получающемуся из канонического покрытия множества $[\beta']$ добавлением вырожденного интервала $[i_r, i_r]$. При таком добавлении получающееся покрытие множества $[\beta]$ тоже будет каноническим.

При $i_r = i_{r-1} + 1$ множество $[\beta]$ получается из множества $[\beta']$ увеличением самой правой 1-серии (в $[\beta']$) на одну единицу с номером i_r . Числа 1-серий $h(\beta)$ и $h(\beta')$ в множествах $[\beta]$ и $[\beta']$ соответственно одинаковы: $h(\beta') = h(\beta)$. Если самая правая компонента $\overline{K}'$ множества $[\beta']$ неоднородна, то самая правая компонента $\overline{K} = \overline{K}' \sqcup \{i_r\}$ в множестве $[\beta]$ тоже неоднородна. Таким образом, $h(\beta') = h(\beta)$, $\kappa'_1 = \kappa_1$, $\delta' = \delta$, поэтому $\mathcal{H}(\beta) = h(\beta) + \kappa_1 + \delta = h(\beta') + \kappa'_1 + \delta' = \mathcal{H}(\beta') = r - 1$, а вектор α не является экстремальным, так как $\|\alpha\| = r > \mathcal{H}(\beta) = r - 1$.

Наконец, если компонента $\overline{K}'$ однородна, т. е. относится к типу I, а $I_{\overline{K}'} > 1$, то самая правая компонента множества $[\beta] = [\beta'] \sqcup \{i_r\}$, равная $\overline{K} = \overline{K}' \sqcup \{i_r\}$, относится к типу II, и тогда $\mathcal{H}(\beta) = \mathcal{H}(\beta') + 1 = r$. В этом случае разложение (7) является каноническим, отвечающим каноническому покрытию множества $[\beta]$, получающемуся из канонического покрытия множества $[\beta']$ добавлением вырожденного интервала $[i_r, i_r]$. Компонента $\overline{K}$ с $I_{\overline{K}} > 1$ накрывается вырожденными интервалами, число которых равно $h_{\overline{K}} + 1 = h_{\overline{K}'} + 1$.

В случае $\varepsilon_{i_r} = -1$ рассмотрим $\beta'' = \beta' - \varepsilon_{i_{r-1}} 2^{n-1-i_{r-1}}$. При $r = 2$ считаем $i_{r-2} = i_0$, $[\beta''] = \emptyset$, $\mathcal{H}(\beta'') = 0$. Прежде всего заметим, что $\beta'_{i_{r-1}} = 1$ (это видно из равенства (8)), а $\beta_{i_{r-1}} = 0$ (это следует из (7)), $\beta_i = 1$ при $i_{r-1}+1 \leq i \leq i_r$, $\beta_i = \beta'_i$ для $i < i_{r-1}$. Отдельно рассмотрим возможности $i_r = i_{r-1} + 1$, $i_r > i_{r-1} + 1$. В свою очередь, для каждой из этих возможностей будем разбирать три случая: $\varepsilon_{i_{r-1}} = 1, \varepsilon_{i_{r-1}} = -1$ с $i_{r-1} = i_{r-2} + 1, \varepsilon_{i_{r-1}} = -1$ с $i_{r-1} > i_{r-2} + 1$. На рис. 1 представлены все 6 ситуаций. Номеру $i_{r-1} \in \{1, \dots, n-1\}$ отвечает пара значений $\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}$: верхнее для $\beta_{i_{r-1}} = 0$, а нижнее для $\beta'_{i_{r-1}} = 1$. В верхних строках располагаются компоненты вектора $(\beta_{i_{r-1}}, \beta_{i_{r-1}+1}, \dots, \beta_{i_r})$, в нижних строках — последние цифры вычета β' . Через $1\dots 1$ на рис. 1 обозначена последовательность из единиц длиной $l \geq 1$. Для вычета β' знаки «+» и «-», выделяющие последний номер подмножества $[\alpha'] \subseteq \{1, \dots, i_{r-1}\}$, указываются снизу, значение $\varepsilon_{i_r} = -1$ указано над β_{i_r} .

$$\begin{array}{lll}
 \text{a) } \dots 0 \begin{smallmatrix} \overline{1} \\ 1 \end{smallmatrix} & \text{b) } \dots 0 \begin{smallmatrix} \overline{1} \\ 1 \end{smallmatrix} & \text{c) } \dots 0 \begin{smallmatrix} \overline{1} \\ 1 \end{smallmatrix} \\
 \text{d) } \dots 0 \begin{smallmatrix} \overline{1\dots 1} \\ 1 \end{smallmatrix} & \text{e) } \dots 0 \begin{smallmatrix} \overline{1} \\ 1 \end{smallmatrix} & \text{f) } \dots 0 \begin{smallmatrix} \overline{1\dots 1} \\ 1 \end{smallmatrix}
 \end{array}$$

Рис. 1

Если в случаях а) и d) $i_{r-1} = 1$, а в случаях б), с), е), f) левый конец нижнего полуинтервала равен 0, то непосредственное выписывание цифр вычета β показывает, что в случаях с), d), е), f) разложение (7) является каноническим, и в обоих случаях а), б) разложение (7) не является экстремальным, так как в каждом из этих случаев $\mathcal{H}(\beta) = |[\beta]| = 1 < r = 2 = |[\alpha]|$. Далее считаем, что в случаях а) и d) $i_{r-1} > 1$, а в случаях б), с), е), f) левый конец нижнего полуинтервала больше 0.

В случае а) заведомо $\beta'_{i_{r-1}-1} \neq 1$, иначе самая правая компонента $\overline{K}'$ подмножества $[\beta'] \subseteq \{1, \dots, n-2\}$ относилась бы к типу II, причем с параметром $I_{\overline{K}'} > 1$. Но тогда самая правая компонента $\overline{K}$ подмножества $\beta \subseteq \{1, \dots, n-1\}$ была бы однородной, причем $h_{\overline{K}} = h_{\overline{K}'} + 1$, $\kappa_1 = \kappa'_1 - 1$. Откуда следовало бы равенство $\mathcal{H}(\beta) = \mathcal{H}(\beta')$, и с учетом экстремальности вектора α' для вычета β' следовало бы неравенство $\mathcal{H}(\beta) = r-1 < r$. Это противоречит свойству экстремальности вектора $\alpha \in B^{[-1]}(\beta)$. Но если $\beta'_{i_{r-1}-1} = \beta_{i_{r-1}-1} = 0$, то ввиду экстремальности вектора α'' для вычета β'' имеем $\mathcal{H}(\beta) = \mathcal{H}(\beta'') + 1 = r-2+1 = r-1$. Снова получаем неравенство $\mathcal{H}(\beta) < r = |[\alpha]|$, доказывающее невозможность случая а) на рис. 1 для экстремального разложения (7).

В случае b) на рис. 1 вычет β' с каноническим представлением (8) не может заканчиваться фрагментом $\dots 0 \overset{+}{\bar{1}}$, поскольку цепь в каноническом представлении, состоящая из единственного полуинтервала, накрывающего ровно одну единицу, может присутствовать только в покрытии блока, состоящего из единственной компоненты типа I с параметром $I = 1$, во всех остальных случаях в цепи обязательно присутствует полуинтервал, накрывающий две или более единиц. Таким образом, вычет β' заканчивается фрагментом $\dots (1 \dots 10) \bar{1}$.

Но тогда

$$\mathcal{H}(\beta) \leq \mathcal{H}(\beta'') + 1 = r - 1 < r = |\alpha|.$$

Полученное неравенство говорит о неэкстремальности разложения (7). Таким образом, случай b) на рис. 1 для экстремального разложения (7) тоже невозможен.

В случаях c) и f) на рис. 1 разложение (7) является каноническим. Соответствующее каноническое покрытие множества $[\beta] \subseteq \{1, \dots, n-1\}$ получается из канонического покрытия множества $[\beta'] \subseteq \{1, \dots, n-2\}$ добавлением полуинтервала $(i_{r-1}, i_r]$.

В случае d) (в отличие от случая a)) для $\beta'_{i_{r-1}-1} = \beta_{i_{r-1}-1}$ возможно значение 1. Тогда компонента $\bar{K}'$ относится к типу II с параметром $I_{\bar{K}'} > 1$, причем левее компоненты $\bar{K}'$ не может быть связующей пары, к ней примыкающей. В этом случае разложение (7) является каноническим, а соответствующее каноническое покрытие множества $[\beta] \subseteq \{1, \dots, n-1\}$ получается из канонического покрытия множества $[\beta'']$ добавлением полуинтервала $(i_{r-1}, i_r]$. Такое же заключение при $\beta'_{i_{r-1}-1} = \beta_{i_{r-1}-1} = 0$ даже не требует дополнительных рассуждений.

В случае e) на рис. 1 вычет β' заканчивается фрагментом

$$\dots (1 \dots 10) \bar{1}$$

(это было установлено выше при рассмотрении случая b)). В результате вычет β заканчивается фрагментом

$$\dots (1 \dots 1 0) \bar{0} \bar{1} \bar{1},$$

поэтому разложение (7) является каноническим. Соответствующее каноническое покрытие подмножества $[\beta]$ получается из канонического покрытия подмножества $[\beta'']$ добавлением вырожденного полуинтервала $(i_{r-1} - 1, i_{r-1}]$ и полуинтервала $(i_{r-1}, i_r]$.

Теорема 2 полностью доказана. $\square$

2. Разностные характеристики модульных сложений

В настоящем разделе, состоящем из четырех частей, изучаются операция

$$+: V_n \times V_n \rightarrow V_n, \quad (x, y) \mapsto x + y \pmod{2^n}, \quad (x, y) \in V_n \times V_n,$$

и разностные характеристики $p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^+$, которые здесь будем обозначать

$$p_{\alpha, \beta; \gamma}^+ = \mathbf{P}\{(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma\}.$$

Вероятность вычисляется в предположении о случайности и равновероятности пар $(x, y) \in V_n \times V_n$.

В п. 2.1 дается общая схема получения разностных и линейных вероятностных соотношений для шифрпреобразования посредством выделения линейной среды в задающей его функциональной схеме. В теореме 5 п. 2.2 приводится решение задачи $\mathcal{A}_8$, а ее следствием обосновывается сведение задач $\mathcal{B}_{31}$ и $\mathcal{B}_{33}$ соответственно к задачам $\mathcal{B}_{32}$ и $\mathcal{B}_{34}$. В п. 2.3 решается задача $\mathcal{B}_{32}$, а в п. 2.4 — задача $\mathcal{B}_{34}$.

2.1

Отображение

$$F : V_N \rightarrow V_M, \quad V_N \ni a \mapsto b = F(a) \in V_M,$$

задаваемое некоторым шифратором при конкретном криптографическом ключе, называем *шифрпреобразованием*. Функциональная схема $\mathcal{F}$, задающая шифрпреобразование F , может представляться последовательностью выполняемых в определенном порядке линейных и нелинейных преобразований. Эту последовательность можно также рассматривать как схему компьютерной программы без циклов.

Пусть нелинейные преобразования $f_i : V_{n_i} \rightarrow V_{m_i}$, $x_i \mapsto y_i = f_i(x_i)$, $i = 1, \dots, k$, выполняются в этой программе в указанном порядке. Через $x_i \in V_{n_i}$ обозначено значение аргумента отображения f_i , которое в конечном счете выражается через $a \in V_N$ и является результатом выполнения некоторых предыдущих операций. В промежутках между нелинейными преобразованиями выполняются линейные преобразования, каждое из которых может быть представлено с помощью суммирований нескольких двоичных слагаемых и с помощью узлов размножения на несколько выходов: $x \mapsto (x, \dots, x)$. Обычно в функциональных схемах узлы размножения не выделяют в отдельные функциональные элементы, хотя они и присутствуют там явным образом (см. [17, с. 243–244]). Но при построении линейных и разностных соотношений узлы размножения играют одинаковую роль с суммированиями (см. [14, 15]), поэтому полезно их выделять особо.

По отдельности линейные операции в шифрпреобразовании выписывать не будем. Ограничимся тем, что для некоторых двоичных матриц c_{ij} размера $m_i \times n_j$, $i=0, 1, \dots, k$, $j=1, \dots, k, k+1$, $m_0=N$, $n_{k+1}=M$, можно записать

$$x_j = a c_{0j} \oplus \bigoplus_{i=1}^{j-1} y_i c_{ij}, \quad j = 1, \dots, k,$$

$$b = a c_{0,k+1} \oplus \bigoplus_{i=1}^k y_i c_{i,k+1}.$$

Полагая $c_{ij} = 0$ при $i \geq j$, из блоков c_{ij} можно составить матрицу C размера

$$\left(N + \sum_{i=1}^k m_i \right) \times \left(\sum_{i=1}^k n_i + M \right),$$

для которой

$$(a, y_1, \dots, y_k) C = (x_1, \dots, x_k, b). \quad (9)$$

Матрица C называется *матрицей линейной среды* функциональной схемы $\mathcal{F}$, в ней аккумулированы все линейные операции шифрпреобразования F . Линейная среда, обозначаемая той же буквой C , сама является функциональной схемой. Она получается удалением из функциональной схемы $\mathcal{F}$ каждого функционального элемента f_i , $i = 1, \dots, k$, с сохранением n_i его двоичных входов, которые превращаются в выходы линейной среды C , и с сохранением m_i его двоичных выходов, которые становятся входами линейной среды C . Линейная среда задает линейное отображение $C : V_{N+\sum_{i=1}^k m_i} \rightarrow V_{\sum_{i=1}^k n_i + M}$ в соответствии с равенством (9).

Главной задачей линейного метода криптографического анализа является построение такой пары вектор-столбцов $L' \in V_N^*$, $L'' \in V_M^* \setminus \{0\}$, для которой абсолютная величина преобладания (иначе, линейная характеристика) $\delta_{L', L''} = \delta_{L', L''}^F = 2 \mathbf{P}\{aL' = bL''\} - 1$ в линейном соотношении $aL' \simeq bL''$ имеет как можно большее значение; здесь $b = F(a)$, а $a \in V_N$ имеет равномерное распределение на V_N .

Вероятностные линейные соотношения $aL' \simeq bL''$, или, в иной записи, $aL' \oplus bL'' \simeq 0$ получаются формальным сложением локальных вероятностных линейных соотношений $x_i l'_i \oplus y_i l''_i \simeq 0$, $l'_i \in V_{n_i}^*$, $l''_i \in V_{m_i}^*$, $y_i = f_i(x_i)$, $i = 1, \dots, k$, характеризующихся преобладаниями

$$\delta_i = \delta_{l'_i, l''_i}^{f_i} = 2 \mathbf{P}\{x_i l'_i = y_i l''_i\} - 1,$$

вычисляемыми для равномерного распределения x_i на V_{n_i} .

Набор $\mathfrak{L} = ((l'_i, l''_i), i = 1, \dots, k)$ должен быть согласованным в том смысле, что при некоторых $L' \in V_N^*$, $L'' \in V_M^*$ имеет место тождество $\bigoplus_{i=1}^k (x_i l'_i \oplus y_i l''_i) = aL' \oplus bL''$, или

$$\begin{aligned} 0 &= \bigoplus_{i=1}^k (x_i l'_i \oplus y_i l''_i) \oplus aL' \oplus bL'' = \\ &= xl' \oplus yl'' \oplus aL' \oplus bL'' = (a, y) \begin{pmatrix} L' \\ l'' \end{pmatrix} \oplus (x, b) \begin{pmatrix} l' \\ L'' \end{pmatrix} = \\ &= (a, y) \begin{pmatrix} L' \\ l'' \end{pmatrix} \oplus (a, y) C \begin{pmatrix} l' \\ L'' \end{pmatrix} = (a, y) \left[\begin{pmatrix} L' \\ l'' \end{pmatrix} \oplus C \begin{pmatrix} l' \\ L'' \end{pmatrix} \right], \end{aligned}$$

здесь a, y_i — **независимые** переменные, $x = (x_1, \dots, x_k)$, $y = (y_1, \dots, y_k)$, $l' \in V_{\sum_{i=1}^k n_i}^*$ — вектор-столбец, составленный из вектор-столбцов l'_i , аналогично $l'' \in V_{\sum_{i=1}^k m_i}^*$ составлен из l''_i , $i = 1, \dots, k$. Таким образом, критерием согласованности набора $\mathfrak{L} = ((l'_i, l''_i), i = 1, \dots, k)$ является равенство

$$C \begin{pmatrix} l' \\ L'' \end{pmatrix} = \begin{pmatrix} L' \\ l'' \end{pmatrix}, \quad (10)$$

выполненное при некоторых $L' = L'_\mathfrak{L} \in V_N^*$ и $L'' = L''_\mathfrak{L} \in V_M^*$.

В качестве грубого приближения для $\delta_{L', L''}$ рассматривают произведение $\tilde{\delta} = \delta_1 \cdots \delta_k$. Это мотивируется следующим рассуждением. Если равновероятность $a \in V_N$ обеспечивает равновероятность $x_i \in V_{n_i}$ для всех $i = 1, \dots, k$ и булевы случайные величины $\eta_i = x_i l'_i \oplus y_i l''_i$, $i = 1, \dots, k$, независимы в совокупности, то $\delta_{L', L''} = \tilde{\delta}$.

Пусть $\mathfrak{W}(L', L'')$ — множество всех решений системы (10) относительно неизвестных $\mathfrak{L} = ((l'_i, l''_i), i = 1, \dots, k)$ при заданных «краевых» вектор-столбцах: вектор-столбце $L' \in V_N^*$ при входе и вектор-столбце $L'' \in V_M^*$ при выходе. Положим

$$\mathfrak{W} = \bigcup_{L' \in V_N^*, L'' \in V_M^*} \mathfrak{W}(L', L'') \quad \text{и} \quad \mathfrak{W}^{(0)} = \{\mathfrak{L} \in \mathfrak{W} \mid l''_i = 0 \Rightarrow l'_i = 0, i = 1, \dots, k\}.$$

Для $\mathfrak{L} \in \mathfrak{W} \setminus \mathfrak{W}^{(0)}$ обязательно $\tilde{\delta}_\mathfrak{L} = \delta_1 \cdots \delta_k = \prod_{i=1}^k \delta_{l'_i, l''_i}^{f_i} = 0$. Искомые линейные соотношения $aL'_\mathfrak{L} \simeq bL''_\mathfrak{L}$ являются результатом поиска $\mathfrak{L} \in \mathfrak{W}^{(0)}$ с максимально возможными значениями $|\tilde{\delta}_\mathfrak{L}|$, $\tilde{\delta}_\mathfrak{L} = \prod_{i=1}^k \delta_{l'_i, l''_i}^{f_i}$.

Точное значение линейной характеристики $\delta_{L'_\mathfrak{L}, L''_\mathfrak{L}}$ вычисляется с помощью следующей теоремы.

Теорема 3 ([16]). Для $L' \in V_N^*$, $L'' \in V_M^*$ справедливо равенство: $\delta_{L', L''} = \sum_{\mathcal{L} \in \mathcal{W}(L', L'')} \tilde{\delta}_{\mathcal{L}}$.

Обратимся теперь к разностному методу криптографического анализа. Рассматривая равенства (9) для двух входов функциональной схемы $a^{(1)}, a^{(2)} \in V_N$ и переходя к разностям (вычитая одно из другого), получим

$$(D', d''_1, \dots, d''_k) C = (d'_1, \dots, d'_k, D''), \quad (11)$$

где

$$\begin{aligned} D' &= a^{(1)} \oplus a^{(2)}, & D'' &= b^{(1)} \oplus b^{(2)}, \\ d''_i &= y_i^{(1)} \oplus y_i^{(2)}, & d'_i &= x_i^{(1)} \oplus x_i^{(2)}, & i &= 1, \dots, k. \end{aligned}$$

Здесь $b^{(1)} = F(a^{(1)})$, $b^{(2)} = F(a^{(2)})$, $x_i^{(1)}, x_i^{(2)}$ — значения аргументов f_i , когда входами всей функциональной схемы являются, соответственно, $a^{(1)}$ и $a^{(2)}$, $y_i^{(1)} = f_i(x_i^{(1)})$, $y_i^{(2)} = f_i(x_i^{(2)})$, $i = 1, \dots, k$; все действия проводятся над полем $GF(2)$, поэтому допустимо вместо $\ominus$ писать $\oplus$.

Главной задачей разностного метода криптографического анализа является построение такой пары векторов $D' \in V_N, D'' \in V_M$, для которой нестрогая импликация

$$a^{(1)} \oplus a^{(2)} = D' \Rightarrow b^{(1)} \oplus b^{(2)} = D'',$$

называемой *разностным соотношением* и обозначаемой записью $D' \rightsquigarrow D''$, отвечает как можно большая разностная характеристика

$$p_{D', D''} = p_{D', D''}^F = \mathbf{P}\{F(a \oplus D') \oplus F(a) = D''\},$$

вычисляемая при равновероятном $a \in V_N$.

Пусть $D' \in V_N$, $D'' \in V_M$, $d'_i \in V_{n_i}$, $d''_i \in V_{m_i}$, $i = 1, \dots, k$, — произвольный набор векторов, удовлетворяющий условию согласованности (11). Матрица C является блочно верхнетреугольной, поэтому из справедливости импликаций $x_i^{(1)} \oplus x_i^{(2)} = d'_i \Rightarrow y_i^{(1)} \oplus y_i^{(2)} = d''_i$ для всех $i = 1, \dots, k$ следует справедливость импликации $a^{(1)} \oplus a^{(2)} = D' \Rightarrow b^{(1)} \oplus b^{(2)} = D''$.

Если набор локальных разностей $\mathfrak{D} = ((d'_i, d''_i), i = 1, \dots, k)$, $d'_i \in V_{n_i}$, $d''_i \in V_{m_i}$, удовлетворяет условию (11) при некоторых краевых значениях $D' = D'_{\mathfrak{D}} \in V_N$, $D'' = D''_{\mathfrak{D}} \in V_M$, то в качестве грубого приближения для разностной характеристики $p_{D', D''}^F$ разностного соотношения $D' \rightsquigarrow D''$ обычно рассматривают произведение $\tilde{p}_{\mathfrak{D}} = \prod_{i=1}^k p_{d'_i, d''_i}^{f_i}$, в котором каждый сомножитель $p_{d'_i, d''_i}^{f_i} = \mathbf{P}\{f_i(x_i^{(1)} \oplus d'_i) \oplus f_i(x_i^{(1)}) = d''_i\}$ является разностной характеристикой локального разностного соотношения $d'_i \rightsquigarrow d''_i$ и вычисляется в условиях равномерного распределения $x_i^{(1)}$ на V_{n_i} .

Использование приближения $\tilde{p}_{\mathfrak{D}}$ для $p_{D',D''}$ мотивируется следующим рассуждением. Если $a^{(2)} = a^{(1)} \oplus D'$, а равновероятность $a^{(1)} \in V_N$ обеспечивает равновероятность $x_i^{(1)} \in V_{n_i}$ для всех $i = 1, \dots, k$, и если события $y_i^{(1)} \oplus y_i^{(2)} = d_i''$, $i = 1, \dots, k$, независимы в совокупности, то, согласно (11),

$$\begin{aligned} p_{D',D''} &\geq \mathbf{P}\{y_i^{(1)} \oplus y_i^{(2)} = d_i'', i = 1, \dots, k\} = \\ &= \prod_{i=1}^k \mathbf{P}\{y_i^{(1)} \oplus y_i^{(2)} = d_i''\} = \prod_{i=1}^k \mathbf{P}\{f_i(x_i^{(1)}) \oplus f_i(x_i^{(2)}) = d_i''\} = \\ &= \prod_{i=1}^k \mathbf{P}\{f_i(x_i^{(1)}) \oplus f_i(x_i^{(1)} \oplus d_i') = d_i''\} = \tilde{p}_{\mathfrak{D}}. \end{aligned}$$

Пусть $W(D', D'')$ — множество всех решений системы (11) относительно неизвестных $\mathfrak{D} = ((d_i', d_i''), i = 1, \dots, k)$ при заданных краевых разностях $D' \in V_N$, $D'' \in V_M$. Положим

$$W = \bigcup_{D' \in V_N, D'' \in V_M} W(D', D'')$$

и

$$W^{(0)} = \{\mathfrak{D} \in W \mid d_i' = 0 \Rightarrow d_i'' = 0, i = 1, \dots, k\}.$$

Для $\mathfrak{D} \in W \setminus W^{(0)}$ обязательно $\tilde{p}_{\mathfrak{D}} = 0$. Искомые разностные соотношения

$$a^{(1)} \oplus a^{(2)} = D'_{\mathfrak{D}} \rightsquigarrow D''_{\mathfrak{D}} = b^{(1)} \oplus b^{(2)}$$

являются результатом поиска $\mathfrak{D} \in W^{(0)}$ с максимально возможными

$$\tilde{p}_{\mathfrak{D}} = \prod_{i=1}^k p_{d_i', d_i''}^{f_i}.$$

Точное значение разностной характеристики $p_{D'_{\mathfrak{D}}, L''_{\mathfrak{D}}}$ вычисляется с помощью следующей теоремы.

Теорема 4 ([16]). Для $D' \in V_N$, $D'' \in V_M$ имеем:

$$\begin{aligned} p_{D',D''} &= \sum_{\mathfrak{D} \in W(D',D'')} \tilde{p}_{\mathfrak{D}} + \\ &+ \frac{1}{2^M} \sum_{(L',L'') \in V_N^* \times V_M^*} (-1)^{D'L' + D''L''} \sum_{\substack{\mathfrak{L}_1, \mathfrak{L}_2 \in \mathfrak{M}(L',L''): \\ \mathfrak{L}_1 \neq \mathfrak{L}_2}} \tilde{\delta}_{\mathfrak{L}_1} \tilde{\delta}_{\mathfrak{L}_2}. \end{aligned}$$

2.2

Применим теорему 4 для получения выражений разностных характеристик $p_{\alpha,\beta;\gamma}^+ = p_{\oplus\alpha,\oplus\beta;\oplus\gamma}^+$. Тройку векторов $\alpha, \beta, \gamma \in V_n$, $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$, $\beta = (\beta_0, \beta_1, \dots, \beta_{n-1})$, $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{n-1})$, будем задавать последовательностью троек компонент

$$(\alpha_0, \beta_0; \gamma_0), (\alpha_1, \beta_1; \gamma_1), \dots, (\alpha_{n-1}, \beta_{n-1}; \gamma_{n-1}). \quad (12)$$

Для $i = 1, 2, \dots, n-2$ положим $I(\alpha_i, \beta_i; \gamma_i) = 0$, если $\alpha_i = \beta_i = \gamma_i$, иначе $I(\alpha_i, \beta_i; \gamma_i) = 1$. Для $i = n-1$ полагаем $I(\alpha_{n-1}, \beta_{n-1}; \gamma_{n-1}) = 0$, если $\alpha_{n-1} = \beta_{n-1} = 0$, иначе $I(\alpha_{n-1}, \beta_{n-1}; \gamma_{n-1}) = 1$.

Теорема 5. Тогда и только тогда $p_{\alpha,\beta;\gamma}^+ > 0$, когда выполняются три следующих условия:

- i) $\alpha_{n-1} \oplus \beta_{n-1} = \gamma_{n-1}$,
- ii) если $\alpha_{n-1} = \beta_{n-1} = 0$, то $\alpha_{n-2} \oplus \beta_{n-2} = \gamma_{n-2}$,
- iii) если $\alpha_i = \beta_i = \gamma_i$, то $\alpha_{i-1} \oplus \beta_{i-1} \oplus \gamma_{i-1} = \alpha_i = \beta_i = \gamma_i$, $i = 1, 2, \dots, n-2$.

Если $p_{\alpha,\beta;\gamma}^+ > 0$, то $p_{\alpha,\beta;\gamma}^+ = \left(\frac{1}{2}\right)^{\sum_{i=1}^{n-1} I(\alpha_i, \beta_i; \gamma_i)}$.

Следствие. Если векторы $\alpha', \beta', \gamma' \in V_n$ получаются из векторов $\alpha, \beta, \gamma \in V_n$ путем независимых перестановок бит в каждой тройке последовательности (12), то $p_{\alpha',\beta';\gamma'}^+ = p_{\alpha,\beta;\gamma}^+$.

Доказательство теоремы 5. В качестве функциональной схемы для операции $+: \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^n}$, $(x_0, x_1, \dots, x_{n-1}) + (y_0, y_1, \dots, y_{n-1}) = (z_0, z_1, \dots, z_{n-1})$, можно рассматривать цепочку функциональных элементов $f_i, i = n-1, n-2, \dots, 1, 0$, реализующих отображения

$$\begin{aligned} f_{n-1}: (x_{n-1}, y_{n-1}) &\mapsto (z_{n-1}, \tau_{n-2}), z_{n-1} = x_{n-1} \oplus y_{n-1}, \tau_{n-2} = x_{n-1} y_{n-1}, \\ f_i: (x_i, y_i, \tau_i) &\mapsto (z_i, \tau_{i-1}), z_i = x_i \oplus y_i \oplus \tau_i, \tau_{i-1} = x_i y_i \oplus (x_i \oplus y_i) \tau_i, \\ &i = n-2, n-3, \dots, 1, \\ f_0: (x_0, y_0, \tau_0) &\mapsto x_0 \oplus y_0 \oplus \tau_0. \end{aligned}$$

Локальные разностные соотношения для $f_{n-1}, f_i (i = n-2, \dots, 1), f_0$ задаем векторами $(\alpha_{n-1}, \beta_{n-1}; \gamma_{n-1}, \kappa_{n-2}), (\alpha_i, \beta_i, \kappa_i; \gamma_i, \kappa_{i-1}) (i = n-2, \dots, 1), (\alpha_0, \beta_0, \kappa_0; \gamma_0)$ соответственно. Непосредственно проверяется, что локальные разностные характеристики равны 1 для f_{n-1} , когда $\alpha_{n-1} = \beta_{n-1} = \gamma_{n-1} = \kappa_{n-2} = 0$, для $f_i, i = n-2, \dots, 1$, когда $\alpha_i = \beta_i = \kappa_i = \gamma_i = \kappa_{i-1}$, и для f_0 , когда вес вектора $(\alpha_0, \beta_0, \kappa_0; \gamma_0)$ четен. Локальные разностные характеристики равны $1/2$ для f_{n-1} , когда в векторе $(\alpha_{n-1}, \beta_{n-1}; \gamma_{n-1}, \kappa_{n-2})$ среди координат $\alpha_{n-1}, \beta_{n-1}, \gamma_{n-1}$ ровно 2 единицы, для $f_i, i = n-2, \dots, 1$, когда в векторе $(\alpha_i, \beta_i, \kappa_i; \gamma_i, \kappa_{i-1})$ среди первых четырех координат ровно 2 единицы. Во всех остальных случаях локальные разностные характеристики равны 0.

Использование одинаковых обозначений $\kappa_i, i = n - 2, \dots, 1, 0$, для выходной компоненты f_{i+1} и для входной компоненты f_i обусловлено согласованностью.

Абсолютные величины локальных линейных характеристик (преобладаний) для $f_{n-1}, f_i, i = n - 2, \dots, 1, f_0$ обозначаем соответственно через

$$\begin{aligned} & \delta_{\alpha_{n-1}, \beta_{n-1}; \gamma_{n-1}, \kappa_{n-2}}^{(n-1)}, \\ & \delta_{\alpha_i, \beta_i, \kappa_i; \gamma_i, \kappa_{i-1}}^{(i)} = 2\mathbf{P}\{x_i\alpha_i \oplus y_i\beta_i \oplus \tau_i\kappa_i = z_i\gamma_i \oplus \tau_{i-1}\kappa_{i-1}\} - 1, \\ & \delta_{\alpha_0, \beta_0, \kappa_0; \gamma_0}^{(0)}. \end{aligned}$$

Непосредственно проверяется, что абсолютные величины локальных линейных характеристик равны 1 для f_{n-1} , когда $\kappa_{n-2} = 0$ и $\alpha_{n-1} = \beta_{n-1} = \gamma_{n-1}$, для $f_i, i = n - 2, \dots, 1$, когда $\kappa_{i-1} = 0$ и $\alpha_i = \beta_i = \kappa_i = \gamma_i$, для f_0 , когда $\alpha_0 = \beta_0 = \kappa_0 = \gamma_0$. Абсолютные величины локальных линейных характеристик равны $1/2$ для $f_i, i = n - 1, n - 2, \dots, 1$, когда $\kappa_{i-1} = 1$ и, кроме того, при $i = n - 2, \dots, 1$ вес вектора $(\alpha_i, \beta_i, \kappa_i; \gamma_i)$ нечетен. Во всех остальных случаях абсолютные величины локальных линейных характеристик равны 0.

В силу перечисленных свойств локальных характеристик имеем: для любых $L' \in V_{2n}^*, L'' \in V_n^*$ условие $\tilde{\delta}_{\mathcal{L}} \neq 0$ выполняется не более чем для одного набора $\mathcal{L} \in \mathfrak{W}(L', L'')$, для любых $D' \in V_{2n}, D'' \in V_n$ условие $\tilde{p}_{\mathfrak{D}} \neq 0$ выполняется тоже не более чем для одного набора $\mathfrak{D} \in W(D', D'')$. Поэтому, применяя для вычисления $p_{\alpha, \beta; \gamma}^+$ теорему 4, убеждаемся, что из двух представленных в теореме сумм в первой сумме только одно ненулевое слагаемое, а вторая сумма равна нулю (в ее внутренних суммах нет ненулевых слагаемых).

Ориентируясь на ненулевые локальные разностные характеристики и проходя по функциональной схеме от f_{n-1} к f_{n-2} и далее от f_i к $f_{i-1}, i = n - 2, \dots, 1$, убеждаемся в необходимости и достаточности совокупности условий i), ii), iii) для выполнения неравенства $p_{\alpha, \beta; \gamma}^+ > 0$.

Теорема 5 доказана. $\square$

Другим способом независимо от автора эквивалентные теореме 5 утверждения были получены А. Е. Тришиным (не опубликовано) и в [18].

Аналогично с помощью теоремы 3 можно получить простые выражения для линейных характеристик

$$\delta_{\alpha, \beta; \gamma}^+ = 2\mathbf{P}\{x\alpha \oplus y\beta = (x + y)\gamma\} - 1, \quad \alpha, \beta, \gamma \in V_n^*.$$

Доказательства следующих приводимых ниже предложений проводятся совершенно по той же схеме, что и доказательство теоремы 5, поэтому их приводить не будем.

Для формулировки этих предложений поставим в соответствие последовательности (12), задающей вектор-столбцы $\alpha, \beta, \gamma \in V_n^*$, какую-либо последовательность

$$v_0, v_1, \dots, v_{n-1}, \quad (13)$$

в которой $v_i \in V_2, i=0, 1, \dots, n-1$, — вершины графа де Брейна на множестве V_2 с дугами $(u_1, u_2) \rightarrow (\varepsilon, u_1), \varepsilon, u_1, u_2 \in GF(2)$. Если $\alpha_i = \beta_i = \gamma_i = 0$, то $v_i \in \{(0, 0), (1, 1)\}$. Если $\alpha_i = \beta_i = \gamma_i = 1$, то $v_i \in \{(1, 0), (0, 1)\}$. В других случаях, когда $(\alpha_i, \beta_i, \gamma_i) \in V_3 \setminus \{(0, 0, 0), (1, 1, 1)\}$, соответствие однозначно. Если вес $\|(\alpha_i, \beta_i, \gamma_i)\|$ четен, то $v_i = (1, 1)$, а если нечетен, то $v_i = (0, 1)$. Таким образом, если $v_i = (0, 0)$, то $(\alpha_i, \beta_i, \gamma_i) = (0, 0, 0)$. Если $v_i = (1, 0)$, то $(\alpha_i, \beta_i, \gamma_i) = (1, 1, 1)$. Если $v_i = (1, 0)$, то вес $\|(\alpha_i, \beta_i, \gamma_i)\|$ четен. Если $v_i = (0, 1)$, то вес $\|(\alpha_i, \beta_i, \gamma_i)\|$ нечетен.

Последовательность (13) называем *монотонной*, если $v_0 \in \{(0, 0), (1, 0)\}$ и для всех $i = 0, 1, \dots, n-2$ вершина v_i является началом, а v_{i+1} — концом некоторой дуги графа де Брейна.

Предложение 1. Любой тройке векторов $\alpha, \beta, \gamma \in V_n^*$ последовательности (12) соответствует не более одной монотонной последовательности (13).

Монотонную последовательность (13) можно представлять в виде

$$\{t_0\}, (1, 0), [n_1], (0, 1), \{t_1\}, (1, 0), [n_2], (0, 1), \{t_2\}, (1, 0), [n_3], (0, 1), \dots, \quad (14)$$

где через $\{t_i\}, i \geq 0$, обозначена серия вершин $(0, 0)$ длины $t_i \geq 0$, а через $[n_j], j \geq 1$, обозначена серия вершин $(1, 1)$ длины $n_j \geq 0$. Последовательность (14) может заканчиваться любой из 4 вершин графа де Брейна.

В формулировке следующего предложения полагаем:

r — номер j последней $(1, 1)$ -серии в последовательности (14),

$a = |\{i \in \{0, 1, \dots, n-1\} : (\alpha_i, \beta_i, \gamma_i) \in \{(0, 0, 1), (1, 1, 0)\}\}|$,

$b = 2$, если последней вершиной в последовательности (13) является $(1, 1)$, иначе $b=1$.

Предложение 2. Тогда и только тогда $\delta_{\alpha, \beta, \gamma}^+ \neq 0$, когда последовательности (12) можно поставить в соответствие монотонную последовательность (13), при этом

$$\delta_{\alpha, \beta, \gamma}^+ = (-1)^a \cdot \prod_{j=1}^r \left(\frac{1}{2}\right)^{n_j+1} \cdot b.$$

В качестве следствий предложения 2 получаем следующие предложения.

Предложение 3. Если вектор-столбцы $\alpha', \beta', \gamma' \in V_n^*$ получаются из вектор-столбцов $\alpha, \beta, \gamma \in V_n^*$ путем независимых перестановок бит в каждой тройке последовательности (12), то $|\delta_{\alpha', \beta', \gamma'}^+| = |\delta_{\alpha, \beta, \gamma}^+|$.

Предложение 4. Неравенство $|\delta_{\alpha,\beta;\gamma}^+| > 0$ при заданных $\alpha, \beta \in V_n^*$ имеет место тогда и только тогда, когда либо $\alpha = \beta = 0$, либо

$$\min \{i \in \{0, 1, \dots, n-1\} \mid \alpha_i = 1\} = \min \{i \in \{0, 1, \dots, n-1\} \mid \beta_i = 1\}.$$

Ясно, что обязательно $\max_{(\alpha,\beta) \in V_n^* \times V_n^*} |\delta_{\alpha,\beta;\gamma}^+| > 0$ при любом заданном $\gamma \in V_n^*$.

2.3

Приведем алгоритм решения задачи $\mathcal{B}_{32}$ по нахождению $\max_{\gamma} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^+$ при заданных $\alpha, \beta \in V_n$.

Функциональную схему для отображения $+: V_n \times V_n \rightarrow V_n$ будем представлять диаграммой в виде n горизонтально расположенных вершин, соединенных отрезками и занумерованных числами $0, 1, \dots, n-2, n-1$ слева направо. Вершины $i \in \{0, 1, \dots, n-1\}$ отвечают функциональным элементам f_i , введенным в п. 2.2. Считаем еще, что между соседними вершинами на диаграмме располагается прямоугольная ячейка с основанием в виде отрезка, соединяющего эти вершины. Номер ячейки совпадает с номером левой вершины. Пример фрагмента этой диаграммы приведен на рис. 2.

Рис. 2

Нахождение $\max_{\gamma} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^+$ сводится к расстановке специальных значений $\kappa_0, \kappa_1, \dots, \kappa_{n-2}$ над горизонтальными отрезками диаграммы (κ_i над отрезком $[i, i+1]$), по которым (в силу равенств $z_i = x_i \oplus y_i \oplus \tau_i$, $i = 0, 1, \dots, n-2$, $z_{n-1} = x_{n-1} \oplus y_{n-1}$) однозначно восстанавливаются $\gamma_0, \gamma_1, \dots, \gamma_{n-2}, \gamma_{n-1}$:

$$\gamma_i = \alpha_i \oplus \beta_i \oplus \kappa_i \quad \text{при} \quad i = 0, 1, \dots, n-2, \quad \gamma_{n-1} = \alpha_{n-1} \oplus \beta_{n-1}. \quad (15)$$

Таким образом, γ_{n-1} однозначно определяется по α и β , и, согласно указанной в (15) биекции между векторами

$$(\gamma_0, \gamma_1, \dots, \gamma_{n-2}) \in V_{n-1} \quad \text{и} \quad \kappa = (\kappa_0, \kappa_1, \dots, \kappa_{n-2}) \in V_{n-1},$$

задача по нахождению $\max_{\gamma \in V_n} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^+$ равносильна задаче по нахождению $\max_{\kappa \in V_{n-1}} p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^+$.

Из теоремы 5 и ее доказательства следует, что

$$p_{\oplus\alpha, \oplus\beta; \oplus\gamma}^+ = \mathbf{P} \{(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma\} = p_0 \cdot p_1 \cdot \dots \cdot p_{n-1}, \quad (16)$$

где вероятность вычисляется при независимых равновероятных $x, y \in V_n$.

Сомножители в правой части (16) для $i = 1, \dots, n-1$ равны

$$p_i = p_{\alpha_i, \beta_i, \kappa_i, \gamma_i, \kappa_{i-1}}^{f_i} = \mathbf{P}\{f_i(x_i \oplus \alpha_i, y_i \oplus \beta_i, \tau_i \oplus \kappa_i) = f_i(x_i, y_i, \tau_i) \oplus (\gamma_i, \kappa_i)\},$$

причем вероятности вычисляются при независимых равновероятных $x_i, y_i, \tau_i \in GF(2)$. Аналогично вычисляются $p_{n-1} = p_{\alpha_{n-1}, \beta_{n-1}, \gamma_{n-1}, \kappa_{n-2}}^{f_{n-1}}$, $p_0 = p_{\alpha_0, \beta_0, \kappa_0, \gamma_0}^{f_0}$. Вероятности p_i , $i = n-1, \dots, 1, 0$, как следует из доказательства теоремы 5, могут принимать значения 1, $1/2$, 0. Конкретно,

$$p_{n-1} = 1, \quad \text{когда} \quad \alpha_{n-1} = \beta_{n-1} = \gamma_{n-1} = \kappa_{n-2} = 0,$$

$$p_i = 1, \quad i = 1, \dots, n-2, \quad \text{когда} \quad \alpha_i = \beta_i = \kappa_i = \gamma_i = \kappa_{i-1},$$

$$p_0 = 1, \quad \text{когда вес} \quad \|(\alpha_0, \beta_0, \kappa_0, \gamma_0)\| \quad \text{четен,}$$

$$p_{n-1} = 1/2, \quad \text{когда} \quad \|(\alpha_{n-1}, \beta_{n-1}, \gamma_{n-1})\| = 2,$$

$$p_i = 1/2, \quad i = 1, \dots, n-2, \quad \text{когда} \quad \|(\alpha_i, \beta_i, \kappa_i, \gamma_i)\| = 2.$$

Во всех остальных случаях $p_i = 0$, $i = 0, 1, \dots, n-2, n-1$.

Поскольку далее решается задача максимизации произведения $p_0 p_1 \dots p_{n-2} p_{n-1}$ по всем $\kappa \in V_{n-1}$, то наличие координат вектора $\gamma \in V_n$ в представленных выше условиях нежелательно. Эти условия, принимая во внимание равенства (15), можно переписать без координат вектора γ в виде

$$p_0 = 1 \quad \text{всегда,}$$

$$p_i = 1, \quad i = 1, \dots, n-2, \quad \text{когда} \quad \alpha_i = \beta_i = \kappa_i = \kappa_{i-1},$$

$$p_i = 1/2, \quad \text{когда} \quad \|(\alpha_i, \beta_i, \kappa_i)\| \in \{1, 2\}, \quad (17)$$

$$p_{n-1} = 1, \quad \text{когда} \quad \alpha_{n-1} = \beta_{n-1} = \kappa_{n-2} = 0,$$

$$p_{n-1} = 1/2, \quad \text{когда} \quad (\alpha_{n-1}, \beta_{n-1}) \neq (0, 0).$$

Во всех остальных случаях, которые не будут допускаться при выборе векторов $\kappa = (\kappa_0, \kappa_1, \dots, \kappa_{n-2}) \in V_{n-1}$, обязательно $p_i = 0$, $i = 1, \dots, n-2, n-1$. Равенства (17) легко проверяются исходя из формул для вероятностей $p_i = \mathbf{P}\{(x \oplus \alpha_i)(y \oplus \beta_i) \oplus (x \oplus y \oplus \alpha_i \oplus \beta_i)(\tau \oplus \kappa_i) = xy \oplus (x \oplus y)\tau \oplus \kappa_{i-1}\}$, $i = 1, \dots, n-2$, $p_{n-1} = \mathbf{P}\{(x \oplus \alpha_{n-1})(y \oplus \beta_{n-1}) = xy \oplus \kappa_{n-2}\}$, вычисляемых при независимых равновероятных $x, y, \tau \in GF(2)$. Далее в рассуждениях каждый раз при выписывании значения вероятности $p_i \in \{1, 1/2\}$, $i = 0, 1, \dots, n-1$, будет подразумеваться ссылка на формулы (17).

Независимо от κ_0 имеем $p_0 = 1$. Возникает свобода в выборе конкретного значения координаты κ_0 , которое, до поры, конкретизировать не будем. Это обстоятельство будем записывать в виде $\kappa_0 = *$. Далее, если $\hat{i} \in \{1, \dots, n-1\}$ — максимальное, для которого либо $\alpha_{\hat{i}} \neq 0$, либо $\beta_{\hat{i}} \neq 0$, то $\kappa_{\hat{i}} = \dots = \kappa_{n-2} = 0$, и независимо от $\kappa_{\hat{i}-1}$ имеем $p_{\hat{i}} = 1/2$, $1p_{\hat{i}+1} = \dots = p_{n-1} = 1$, т. е. произведение $n - \hat{i}$ сомножителей в (16), начиная с $\hat{i}$ -го, равно $1/2$.

Значение $\kappa_{\hat{i}-1}$ тоже не конкретизируем: $\kappa_{\hat{i}-1} = *$. Ситуацию, когда такого номера $\hat{i}$ не существует, не рассматриваем как тривиальную. Наконец, если $\alpha_i \neq \beta_i$, $i \in \{1, \dots, n-2\}$, то независимо от κ_{i-1} и κ_i имеем $p_i = 1/2$, поэтому и для таких номеров i считаем $\kappa_{i-1} = *$, $\kappa_i = *$. После этих замечаний задача $\mathcal{B}_{32}$ по максимизации произведения (16) из n сомножителей сводится к независимым максимизациям произведений подмножеств из этих сомножителей, относящихся к отдельным фрагментам нашей диаграммы (см. рис. 2), на которые она разбивается после выявления всех номеров $i \in \{1, \dots, n-2\}$, для которых $\alpha_i \neq \beta_i$. Для каждого фрагмента нужно максимизировать произведения вида

$$p_{i_0} p_{i_0+1} p_{j_0-1} p_{j_0}, \quad (18)$$

где $1 \leq i_0 < j_0 \leq n-2$, $\kappa_{i_0-1} = *$, $\kappa_{j_0} = *$, $\alpha_s = \beta_s$, $s = i_0, i_0+1, \dots, j_0$. Здесь для $i = i_0, i_0+1, \dots, j_0$ имеем:

$$p_i = \begin{cases} 1, & \text{если } \kappa_{i-1} = \alpha_i = \kappa_i, \\ \frac{1}{2}, & \text{если } \kappa_{i-1} = \alpha_i \neq \kappa_i, \\ \frac{1}{2}, & \text{если } \kappa_{i-1} \neq \alpha_i \neq \kappa_i. \end{cases} \quad (19)$$

Оставшаяся логическая возможность $\kappa_{i-1} \neq \alpha_i = \kappa_i$ при выборе вектора $\kappa \in V_{n-1}$ не допускается, так как тогда $p_i = 0$, что приводит к нулевому произведению (16), а оно подлежит максимизации. Вектор

$$\bar{\kappa}_{i_0, j_0} = (\kappa_{i_0}, \kappa_{i_0+1}, \dots, \kappa_{j_0-2}, \kappa_{j_0-1}) \in V_{j_0-i_0} \quad (20)$$

будем называть *допустимым*, если нет таких номеров $i \in \{i_0+1, \dots, j_0-1\}$, что $\kappa_{i-1} \neq \alpha_i = \kappa_i$. В случае допустимых векторов (20) произведение (18), обозначаемое далее $p(\bar{\kappa}_{i_0, j_0})$, обязательно больше нуля: $p(\bar{\kappa}_{i_0, j_0}) > 0$. Допустимый вектор $\bar{\kappa}_{i_0, j_0} \in V_{j_0-i_0}$ будем характеризовать величиной

$$\mathcal{N} = \mathcal{N}(\bar{\kappa}_{i_0, j_0}) = |\mathcal{M}(\bar{\kappa}_{i_0, j_0})|,$$

где $\mathcal{M}(\bar{\kappa}_{i_0, j_0}) = \{i \in \{i_0, i_0+1, \dots, j_0\} : \kappa_{i-1} \neq \alpha_i \text{ или } \kappa_i \neq \alpha_i\}$, для которой после уточнения κ_{i_0-1} и κ_{j_0} получим $p(\bar{\kappa}_{i_0, j_0}) = 2^{-\mathcal{N}(\bar{\kappa}_{i_0, j_0})}$.

Нам нужно найти все допустимые векторы (20) с минимальным значением $\mathcal{N}(\bar{\kappa}_{i_0, j_0})$, или, иначе, с максимальным числом вершин $i \in \{i_0, i_0+1, \dots, j_0\}$, для которых $\kappa_{i-1} = \alpha_i = \kappa_i$. Согласно (19) для $i \in \{i_0, i_0+1, \dots, j_0\}$ с такими условиями в произведении (18) имеем сомножитель $p_i = 1$. Для минимизации $\mathcal{N}(\bar{\kappa}_{i_0, j_0})$ рассмотрим последовательность

$$\varpi_{i_0}, \varpi_{i_0+1}, \dots, \varpi_{j_0-1}, \quad (21)$$

где $\varpi_i = \bullet$, если $\alpha_i \neq \alpha_{i+1}$, и $\varpi_i = \emptyset$, если $\alpha_i = \alpha_{i+1}$, $i = i_0, i_0+1, \dots, j_0-1$.

Элементы последовательности (21) помещаем в ячейки диаграммы на рис. 2. В ячейку между вершинами i и $i+1$, $i = i_0, i_0+1, \dots, j_0-1$, помещаем $\bullet$ или оставляем пустой в зависимости от ϖ_i . Если $\varpi_i = \bullet$, то независимо от выбора $\kappa_i \in GF(2)$ либо $\alpha_i \neq \kappa_i$, либо $\alpha_i = \kappa_i$, т.е. либо $i \in \mathcal{M}(\bar{\kappa}_{i_0, j_0})$, либо $i+1 \in \mathcal{M}(\bar{\kappa}_{i_0, j_0})$. Значок $\bullet$ называем *помехой* минимизации величины $\mathcal{N}(\bar{\kappa}_{i_0, j_0}) = |\mathcal{M}(\bar{\kappa}_{i_0, j_0})|$. (При наличии помехи в ячейке i в произведении (18), которое мы хотим максимизировать, один из сомножителей p_i или p_{i+1} обязательно равен $1/2$.) В случае уже заданных κ_i , $i = i_0, i_0+1, \dots, j_0-1$, при $\varpi_i = \bullet$ помеху отнесем к одной из вершин i или $i+1$ (см. рис. 3): к i , если $\kappa_i \neq \alpha_i$, и к $i+1$, если $\kappa_i \neq \alpha_{i+1}$. Если далее по каким-то причинам будет осуществлен «противоестественный» выбор κ_i при $\varpi_i = \emptyset$, т.е. $\kappa_i \neq \alpha_i$, то в i -ю ячейку будем помещать два значка $\bullet$, считая $\varpi_i = \{\bullet, \bullet\}$. Тогда $\kappa_i \neq \alpha_i$ и $\kappa_i \neq \alpha_{i+1}$, поэтому одну помеху отнесем к вершине i , а другую — к вершине $i+1$.

При $\varpi_i = \{\bullet, \bullet\}$ помехи направляем в обе эти вершины.

Рис. 3

Задача по нахождению всех векторов (20) с минимальной величиной $\mathcal{N}(\bar{\kappa}_{i_0, j_0})$ сводится к такому дополнительному введению двойных помех и последующему распределению всех образовавшихся помех по вершинам диаграммы рис. 2, при которых число вершин с помехами будет минимальным. Вершины с помехами могут быть четырех типов (см. рис. 4): а) i_0 с помехой справа; б) i , $i_0 < i < j_0$, с помехой справа; в) j_0 с помехой слева; г) i , $i_0 < i < j_0$, с двумя помехами слева и справа. Вершин i , $i_0 < i < j_0$, типа д) с помехой слева быть не должно, потому что тогда соответствующий (такому распределению помех по вершинам) вектор $\bar{\kappa}_{i_0, j_0} \in V_{j_0-i_0}$ не является допустимым, так как тогда (см. (19)) имели бы $p_i = 0$ и $p(\bar{\kappa}_{i_0, j_0}) = 0$.

Рис. 4

Согласно (19) каждая единичная помеха $\varpi_i = \bullet$ дает вклад в $\mathcal{N}(\bar{\kappa}_{i_0, j_0})$, равный 1 в случае вершин типа а), б), в), и вклад, равный $1/2$ в случае вершин типа г). Включение дополнительных помех $\{\bullet, \bullet\}$ над некоторыми интервалами $[i, i+1]$ с $\alpha_i = \alpha_{i+1}$, $i = i_0, \dots, j_0-1$, допустимо только в случае когда их вклад в $\mathcal{N}(\bar{\kappa}_{i_0, j_0})$ равен нулю. Теперь мы располагаем всем необходимым, чтобы сформулировать алгоритм получения всех допустимых векторов $\bar{\kappa}_{i_0, j_0} \in V_{j_0-i_0}$, на которых достигается минимум для $\mathcal{N}(\bar{\kappa}_{i_0, j_0})$.

После расстановки единичных помех $\varpi_i = \bullet$ над интервалами $[i, i+1]$ с $\alpha_i \neq \alpha_{i+1}$, $i = i_0, \dots, j_0$, в последовательности (21) выделяем все $\bullet$ -серии, граничащие с ячейками без помех. Помехи $\bullet$ -серии четной длины s объединяем в $s/2$ пар к вершинам типа г) на рис. 4. В сериях нечетной длины s производится аналогичное объединение помех в $(s-1)/2$ пар, кроме одной помехи (любой из $(s+1)/2$ допустимых), которая переходит либо к правой вершине, либо к левой, лишь бы соответствующая вершина с помехой относилась к типам а), б), в) на рис. 4. После этого в качестве $\kappa_{i_0-1} \in GF(2)$ предусматриваем оба значения, если вершина i_0 с помехой. В противном случае полагаем $\kappa_{i_0-1} = \alpha_{i_0}$, тогда $p_{i_0} = 1$. Полагаем также $\kappa_{j_0} = \alpha_{j_0} \oplus 1$, если вершина j_0 с помехой, иначе $\kappa_{j_0} = \alpha_{j_0}$, $p_{j_0} = 1$. Если $\varpi_i = \emptyset$, $i = i_0, \dots, j_0-1$, то полагаем $\kappa_i = \alpha_i = \alpha_{i+1}$. Значения остальных координат κ_i , $i = i_0, \dots, j_0-1$, полагаем, как указано на рис. 3. При таких действиях будут исчерпаны все векторы $\kappa_{i_0-1}, \kappa_{i_0}, \dots, \kappa_{j_0}$ с максимальным произведением (18), равным $p(\bar{\kappa}_{i_0, j_0}) = 2^{-\mathcal{N}(\bar{\kappa}_{i_0, j_0})}$, но только в случае когда вектор (20) не допускает двойных помех. (Если экстремальный вектор (20) допускает двойные помехи, то после их удаления получим другую последовательность (20) с прежней (минимальной) характеристикой $\mathcal{N}$.)

Каждая пустая ячейка, в которую можно поместить пару помех, не увеличивая характеристику $\mathcal{N}$, должна находиться между двумя $\bullet$ -сериями нечетной длины. В этой связи две $\bullet$ -серии нечетной длины назовем связанными, если между ними ровно одна пустая ячейка. Множество всех $\bullet$ -серий нечетной длины фрагмента на рис. 2 разбивается на блоки — компоненты связности. В каждом блоке выделим несколько непересекающихся связанных пар, называемых близкими. В пустые ячейки между близкими $\bullet$ -сериями помещаем две помехи. Далее помехи во всех $\bullet$ -сериях распределяем по вершинам диаграммы, как и в предыдущем абзаце, только в $\bullet$ -сериях нечетной длины из близких пар одна крайняя помеха встречается с помехой из сближающей ячейки в вершине типа г) на рис. 4.

По индукции устанавливается, что число способов выделения близких пар в блоке из k $\bullet$ -серий нечетной длины равно $(k+2)$ -му числу Фибоначчи.

Например, для блока из 4 •-серий нечетной длины $\mathfrak{W}_1, \mathfrak{W}_2, \mathfrak{W}_3, \mathfrak{W}_4$ имеем следующие 5 способов выделения (стрелками) близких пар:

- 1) $\mathfrak{W}_1 \longleftrightarrow \mathfrak{W}_1 \quad \mathfrak{W}_3 \longleftrightarrow \mathfrak{W}_4,$
- 2) $\mathfrak{W}_1 \longleftrightarrow \mathfrak{W}_1 \quad \mathfrak{W}_3 \quad \mathfrak{W}_4,$
- 3) $\mathfrak{W}_1 \quad \mathfrak{W}_2 \longleftrightarrow \mathfrak{W}_3 \quad \mathfrak{W}_4,$
- 4) $\mathfrak{W}_1 \quad \mathfrak{W}_2 \quad \mathfrak{W}_3 \longleftrightarrow \mathfrak{W}_4,$
- 5) $\mathfrak{W}_1 \quad \mathfrak{W}_2 \quad \mathfrak{W}_3 \quad \mathfrak{W}_4.$

Последний способ не предусматривает наличия близких пар.

Компоненты вектора $\gamma \in V_n$ восстанавливаются по последовательностям $\kappa_{i_0-1}, \kappa_{i_0}, \dots, \kappa_{j_0}$ для всех фрагментов диаграммы с помощью равенств (15).

2.4

Обратимся теперь к задаче по нахождению

$$\max_{(\beta, \gamma)} p_{\oplus \alpha, \oplus \beta; \oplus \gamma}^+ \quad (22)$$

с указанием, как и в п. 2.3, всех экстремальных пар (β, γ) . За счет подробных рассуждений предыдущего подраздела решение данной задачи существенно упрощается. Теперь задан только вектор $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$. Требуется определить векторы $\beta = (\beta_0, \beta_1, \dots, \beta_{n-1})$ и $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{n-1})$, при которых произведение $P = p_0 p_1 \dots p_{n-1}$ (см. (16)) максимально. Как и в предыдущем пункте, с помощью равенств (15) вектор γ исключаем из рассмотрения, максимизируя вероятность P по векторам β и $(\kappa_0, \kappa_1, \dots, \kappa_{n-2})$.

Независимо от κ_0 и β_0 имеем $p_0 = 1$. Пусть, далее, $\alpha_{\tilde{i}} = 1$ и $\alpha_i = 0$ для $i > \tilde{i}$. Тогда независимо от $\kappa_{\tilde{i}-1}$ имеем $p_{\tilde{i}} p_{\tilde{i}+1} \dots p_{n-1} \leq 1/2$, и равенство достигается только когда $\kappa_i = 0$ для всех $i \geq \tilde{i}$ и $\beta_i = 0$ для всех $i \geq \tilde{i} + 1$, а при $\kappa_{\tilde{i}-1} = 1$ еще и при $\beta_{\tilde{i}} = \kappa_{\tilde{i}} = \beta_{\tilde{i}+1} = 1, \kappa_i = 0$ ($i \geq \tilde{i} + 1$), $\beta_i = 0$ ($i \geq \tilde{i} + 2$). Ситуации, когда $\tilde{i}$ не существует или $\tilde{i} \in \{0, 1\}$, далее не рассматриваем как тривиальные.

В отличие от предыдущего пункта здесь ограничиваемся одним фрагментом на нашей диаграмме (см. рис. 2) с параметрами $i_0 = 1, j_0 = \tilde{i} - 1$. Формирование последовательности помех (21), введение двойных помех и распределение этих помех по вершинам (иначе, задание координат вектора (20)) происходит по тем же правилам, что и в п. 2.3, только здесь вершины типа д) на рис. 4 допускаются. После расстановки помех для вершин i без помех полагаем $\beta_i = \alpha_i$, а для вершин типа д) полагаем $\beta_i = \alpha_i \oplus 1$. Для остальных вершин i фрагмента на рис. 2 значение β_i задаем произвольным образом. При заданных векторах $(\beta_0, \beta_1, \dots, \beta_{n-1}), (\kappa_0, \kappa_1, \dots, \kappa_{n-2})$ вектор $(\gamma_0, \gamma_1, \dots, \gamma_{n-1})$ определяется с помощью равенств (15).

Автор благодарен А. А. Дмуху и А. М. Зубкову за важные критические замечания.

Список литературы

- [1] Yang G., Zhu B., Suder V., Aagaard M.D., Gong G., “The Simeck family of lightweight block ciphers”, CHES, Lect. Notes Comput. Sci., **9293**, 2015, 307–329.
- [2] Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L., “The Simon and Speck families of lightweight block ciphers”, IACR Cryptology ePrint Archive, 2013/404, 2013.
- [3] Bernstein D., “Salsa20/8 and Salsa20/12” (2006 <http://cr.yp.to/snuffle/812.pdf>).
- [4] Shimizu A., Miyaguchi S., “Fast data encipherment algorithm FEAL”, Lect. Notes Comput. Sci., **304**, 1988, 267–278.
- [5] Ferguson N., Lucks S., Schneier B., Whiting D., Bellare M., Kohno T., Callas J., Walker J., “The Skein hash family” (2010 <http://dx.doi.org/10.1007/978-3-642-45239-0-15>).
- [6] Leurent G., “Construction of differential characteristics in ARX designs application to Skein”, CRYPTO 2013, Lect. Notes Comput. Sci., **8042**, 2013, 241–258.
- [7] Biryukov A., Velichkov V., “Automatic search for differential trails in ARX ciphers”, Lect. Notes Comput. Sci., **8366**, 2014, 227–250.
- [8] Biryukov A., Roy A., Velichkov V., “Differential analysis of block ciphers Simon and Speck”, Lect. Notes Comput. Sci., **8540**, 2014, 525–545.
- [9] Blondeau C., “Improbable differential from impossible differential: on the validity of the model”, Lect. Notes Comput. Sci., **8250**, 2013, 149–160.
- [10] Tezcan C., “The improbable differential attack: cryptanalysis of reduced round CLEFIA”, Lect. Notes Comput. Sci., **6498**, 2010, 197–209.
- [11] Tolba M., Abdelkhalek A., Youssef M., “Impossible differential cryptanalysis of reduced-round SKINNY”, Cryptology ePrint Archive, 2016/1115, 2016.
- [12] Blondeau C., Peyrin T., Wang L., “Known-key distinguisher on full PRESENT”, Lect. Notes Comput. Sci., **9215**, 2015, 455–474.
- [13] Knudsen L. R., Wagner D., “Integral cryptanalysis”, FSE 2002, Lect. Notes Comput. Sci., **2365**, 2002, 112–127.
- [14] Малышев Ф. М., “Двойственность разностного и линейного методов в криптографии”, *Математические вопросы криптографии*, **5:3** (2014), 35–47.
- [15] Малышев Ф. М., Трифионов Д. И., “Рассеивающие свойства XSLP-шифров”, *Математические вопросы криптографии*, **7:3** (2016), 47–60.
- [16] Малышев Ф. М., Тришин А. Е., “Линейный и разностный методы в криптографии (другой взгляд)”, В сб.: *Алгебра, теория чисел и дискретная геометрия: Современные проблемы и приложения*, Матер. XV Междунар. конф., посвященной столетию со дня рождения профессора Н. М. Коробова (Тула), Тула: ТГПУ им. Л. Н. Толстого, 2018, 42–45.
- [17] Яблонский С. В., *Введение в дискретную математику*, М.: Наука, 1979, 272 с.
- [18] Wallén, “On the differential and linear properties of addition”, Helsinki Univ. of Technology, Lab. Theor. Comput. Sci., HUT-TCS-A84, Espoo 2003.