Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Разностные характеристики основных операций ARX-шифров, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 4, 97–105

DOI: <https://doi.org/10.4213/mvk342>

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: 54.162.85.209

26 апреля 2023 г., 18:28:50

Разностные характеристики основных операций ARX-шифров

Ф. М. Малышев

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

Получено 20.V.2020

Аннотация. Изучаются вероятностные разностные соотношения для операций циклического сдвига, сложения по $\text{mod } 2^n$ и покомпонентного сложения по $\text{mod } 2$ над элементами пространства $V_n = GF(2)^n$, $n \geq 2$. Разности между значениями операции и разности между ее аргументами, связанные конкретным вероятностным разностным соотношением, могут вычисляться с помощью не одинаковых аддитивных операций.

Ключевые слова: разностный криптоанализ, модульное сложение, вероятностные соотношения

Differential characteristics of base operations in ARX-ciphers

F. M. Malyshev

Steklov Mathematical Institute of Russian Academy of Sciences, Moscow

Abstract. Probabilistic difference relations for operations of cyclic shift, addition modulo 2^n and component-wise addition modulo 2 over elements of the space $V_n = GF(2)^n$, $n \geq 2$, are considered. Differences between results of the operation and differences between its arguments connected by the concrete probabilistic difference relation may be computed by different addition operations.

Keywords: differential cryptanalysis, modular addition, probabilistic relations

1. Постановка задач

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 над машинными словами, модульных сложений слов и покомпонентных сложений машинных слов по mod 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 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 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 mod 2, а через $+$ обозначаем сложение по mod 2^n . В последнем случае векторы пространства V_n рассматриваются (при некоторой упорядоченности их компонент) как стандартные двоичные представления вычетов по mod 2^n . Считаем, что $V_n = \mathbb{Z}_{2^n}$, и двоичное представление вычета $2^{n-1-i} \in \mathbb{Z}_{2^n}$, $i = 0, 1, \dots, n-1$, задается вектором $e_i \in V_n = GF(2)^n$ с единственной ненулевой компонентой с номером i . Нам будет удобно в зависимости от ситуации называть элементы множества $V_n = \mathbb{Z}_{2^n}$ 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*:

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

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 основной список задач $\mathcal{A}_i$, $i = 1, \dots, 11$, по нахождению разностных характеристик:

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

Задачи $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ первой строки приведенного списка относятся к операции $\oplus: V_n \times V_n \rightarrow V_n$. Задачи $\mathcal{A}_4, \mathcal{A}_5, \mathcal{A}_6, \mathcal{A}_7, \mathcal{A}_8$ второй строки списка относятся к операции $+: V_n \times V_n \rightarrow V_n$. Серии задач $\mathcal{A}_9, \mathcal{A}_{10}$ третьей строки относятся к операциям $\lll s: V_n \rightarrow V_n$, $s = 1, \dots, n-1$. Задачу $\mathcal{A}_{11}$ третьей строки 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.

Вообще говоря, в этом списке вместо 11 должно было бы быть $2^4 + 2^2 + 2^2 = 24$ задачи по вычислению соответственно $p_{*1\alpha,*2\beta;*3\gamma}^*$, $* \in \{+, \oplus\}$, $p_{*1\alpha;*2\gamma}^{\lll s}$, $s = 1, \dots, n-1$, и $p_{*1\alpha;*2\gamma}^{\text{id}}$. В приведенный список не вошли тривиальные задачи вычисления разностных характеристик: $p_{\oplus\alpha,\oplus\beta;\oplus\gamma}^{\oplus}$, $p_{+\alpha,+\beta;+\gamma}^+$, $p_{\oplus\alpha;\oplus\gamma}^{\lll s}$, $p_{+\alpha;+\gamma}^{\text{id}}$, $p_{\oplus\alpha;\oplus\gamma}^{\text{id}}$. 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: $p_{+\alpha;\oplus\gamma}^{\lll s} = p_{\oplus\gamma;+\alpha}^{\lll (n-s)}$, $p_{+\alpha;\oplus\gamma}^{\text{id}} = p_{\oplus\gamma;+\alpha}^{\text{id}}$.

В [14] были решены задачи $\mathcal{A}_3, \mathcal{A}_4, \mathcal{A}_5, \mathcal{A}_8, \mathcal{A}_9, \mathcal{A}_{11}$. Остались нерешенными задачи $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_6, \mathcal{A}_7, \mathcal{A}_{10}$. Для решения задач $\mathcal{A}_2, \mathcal{A}_6, \mathcal{A}_7$ в настоящей работе будет использоваться приведенная ниже теорема 1 из [14], в которой указаны значения $p_{\oplus\alpha;+\beta}^{\text{id}} = \mathbf{P}\{x \oplus \alpha = x + \beta\}$ для произвольных $\alpha, \beta \in \mathbb{Z}_{2^n}$ и равновероятных $x \in \mathbb{Z}_{2^n}$ (задача $\mathcal{A}_{11}$).

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:

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

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

Конкретный элемент $\beta = \alpha_0 2^{n-1} + \sum_{i \in [\alpha]} \varepsilon_i 2^{n-1-i} \in B(\alpha_0; i_1, \dots, i_r)$, задаваемый последовательностью $(\varepsilon_{i_1}, \dots, \varepsilon_{i_r}) \in \{1, -1\}^r$, можно получать исходя из записи

$$\beta = \alpha_0 2^{n-1} + \varepsilon_{i_1} 2^{n-1-i_1} + \varepsilon_{i_2} 2^{n-1-i_2} + \dots + \varepsilon_{i_r} 2^{n-1-i_r}, \quad (1)$$

в которой сложения естественно выполнять в порядке слева направо.

Вектор β удобно разбивать на подвекторы $\beta^{(1)}, \dots, \beta^{(r)}, \beta^{(r+1)}$: подвектор $\beta^{(j)}$ состоит из компонент с номерами $i_{j-1}, i_{j-1} + 1, \dots, i_j - 1$, $j = 1, \dots, r, r+1$. Выполняя сложения в (1) в порядке слева направо, убеждаемся, что после j -го сложения, $j = 1, \dots, r$, компонента текущей суммы с номером i_j равна 1, а подвектор $\beta^{(j)} = (\beta_{i_{j-1}}, \beta_{i_{j-1}+1}, \dots, \beta_{i_j-1})$ однозначно определяется значением ε_{i_j} и при $j \in \{2, \dots, r\}$ равен либо $(1; 0, \dots, 0)$ (если $\varepsilon_{i_j} = 1$), либо $(0; 1, \dots, 1)$ (если $\varepsilon_{i_j} = -1$). При $j = 1$ подвектор $\beta^{(1)}$ равен либо $(\alpha_0; 0, \dots, 0)$ (если $\varepsilon_{i_1} = 1$), либо $(\alpha_0 \oplus 1; 1, \dots, 1)$ (если $\varepsilon_{i_1} = -1$). При последующих сложениях в (1) (после j -го сложения) подвектор $\beta^{(j)}$ не будет изменяться из-за единицы в компоненте с номером i_j , установившейся в результате j -го сложения. Для $j = r+1$ при $r > 0$ имеем $\beta^{(r+1)} = (1, 0, \dots, 0)$. Таким образом, для различных последовательностей $(\varepsilon_{i_1}, \dots, \varepsilon_{i_r}) \in \{1, -1\}^r$ соответствующие вычеты $\beta \in B(\alpha)$ являются различными, поэтому $|B(\alpha)| = 2^r$.

Обратим внимание, что длины 0-серий и 1-серий компонент подвекторов $\beta^{(j)}$ с номерами $i_{j-1} + 1, \dots, i_j - 1$, $j = 1, 2, \dots, r, r+1$, равны $i_j - 1 - i_{j-1}$, и при $i_j = i_{j-1} + 1$ эти серии отсутствуют.

Приведенные выше рассуждения проиллюстрируем четырьмя примерами (см. формулу (2) ниже), соответствующими

$$\alpha = \alpha_0 2^{n-1} + \varepsilon_{i_1} 2^{n-1-i_1} + \varepsilon_{i_2} 2^{n-1-i_2} + \dots + \varepsilon_{i_{j-1}} 2^{n-1-i_{j-1}} + \varepsilon_{i_j} 2^{n-1-i_j} \\ + \varepsilon_{i_{j+1}} 2^{n-1-i_{j+1}} + \dots + \varepsilon_{i_{r-1}} 2^{n-1-i_{r-1}} + \varepsilon_{i_r} 2^{n-1-i_r},$$

для четырех различных последовательностей $(\varepsilon_{i_1}, \varepsilon_{i_2}, \dots, \varepsilon_{i_{j-1}}, \varepsilon_{i_j}, \varepsilon_{i_{j+1}}, \dots, \varepsilon_{i_{r-1}}, \varepsilon_{i_r}) \in \{-1, +1\}^r$.

В (2) значение $+1$ для ε_{i_s} , $s = 1, \dots, r$, помечено знаком $+$, а значение -1 — знаком $-$. Значения $\varepsilon_{i_{j-1}}$ в (2) не конкретизируются, они могут быть любыми из множества $\{+1, -1\}$, поэтому используем значок $\pm$. Значения β_{i_2} и $\beta_{i_{j+1}}$, помеченные знаком $*$, зависят соответственно от ε_{i_3} и $\varepsilon_{i_{j+2}}$: $\varepsilon_{i_3} = 1 \Rightarrow \beta_{i_2} = 1$, $\varepsilon_{i_3} = -1 \Rightarrow \beta_{i_2} = 0$, $\varepsilon_{i_{j+2}} = 1 \Rightarrow \beta_{i_{j+1}} = 1$, $\varepsilon_{i_{j+2}} = -1 \Rightarrow \beta_{i_{j+1}} = 0$.

$$\begin{array}{cccccccccccccccc}
 & 0 & 1 & i_1 & i_2 & i_{j-1} & i_j & i_{j+1} & i_{r-1} & i_r & & n-1 \\
 \text{a)} & \alpha_0 & 0\dots 0 & \overset{+}{1} & 0\dots 0 & \overset{+}{*} \dots \overset{\pm}{1} & 0\dots 0 & \overset{+}{1} & 0\dots 0 & \overset{+}{*} \dots \overset{+}{1} & 0\dots 0 & \overset{+}{1} & 0 \dots 0 \\
 \text{b)} & \alpha_0 \oplus 1 & 1\dots 1 & \bar{1} & 0\dots 0 & \overset{+}{*} \dots \overset{\pm}{0} & 1\dots 1 & \bar{1} & 0\dots 0 & \overset{+}{*} \dots \bar{1} & 0\dots 0 & \overset{+}{1} & 0 \dots 0 \\
 \text{c)} & \alpha_0 & 0\dots 0 & \overset{+}{0} & 1\dots 1 & \bar{*} \dots \overset{\pm}{1} & 0\dots 0 & \overset{+}{0} & 1\dots 1 & \bar{*} \dots \overset{+}{0} & 1\dots 1 & \bar{1} & 0 \dots 0 \\
 \text{d)} & \alpha_0 \oplus 1 & 1\dots 1 & \bar{0} & 1\dots 1 & \bar{*} \dots \overset{\pm}{0} & 1\dots 1 & \bar{0} & 1\dots 1 & \bar{*} \dots \bar{0} & 1\dots 1 & \bar{1} & 0 \dots 0
 \end{array} \quad (2)$$

Теорема 1 ([14]). Если $\alpha \in \mathbb{Z}_{2^n}$, то $p_{\oplus\alpha;+\beta}^{\text{id}} = 2^{-|\alpha|}$ для $\beta \in B(\alpha)$ и $p_{\oplus\alpha;+\beta}^{\text{id}} = 0$ для $\beta \notin B(\alpha)$.

Приводимые далее теоремы относятся соответственно к задачам $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_6$, $\mathcal{A}_7$. На настоящий момент вопрос о вероятностях $p_{+\alpha,+\beta;+\gamma}^{\oplus}$ и $p_{+\alpha;+\gamma}^{\ll s}$, $s = 1, \dots, n-1$, является открытым. Нерешенными задачами полного списка остаются $\mathcal{A}_1$ и $\mathcal{A}_{10}$.

Теорема 2. Пусть $p_{\alpha,\beta;\gamma}$, $\alpha, \beta, \gamma \in V_n = \mathbb{Z}_{2^n}$, — любая из вероятностей $p_{+\alpha,+\beta;+\gamma}^{\oplus}$, $p_{+\alpha,+\beta;\oplus\gamma}^{\oplus}$, $p_{\oplus\alpha,+\beta;\oplus\gamma}^+$, $p_{\oplus\alpha,\oplus\beta;+\gamma}^+$. Тогда

$$p_{\alpha,\beta;\gamma} = 1 \Leftrightarrow (\alpha_0 \oplus \beta_0 = \gamma_0, \alpha_i = \beta_i = \gamma_i = 0, i = 1, \dots, n-1).$$

В остальных случаях $p_{\alpha,\beta;\gamma} \leq \frac{1}{2}$.

Теорема 3. Справедливы равенства:

$$p_{+\alpha,+\beta;\oplus\gamma}^{\oplus} = \sum_{\delta \in V_n} (p_{+\alpha;+\delta}^{\text{id}} \cdot p_{+\beta;\oplus(\delta \oplus \gamma)}^{\text{id}}), \quad (3)$$

$$p_{\oplus\alpha,+\beta;\oplus\gamma}^+ = \sum_{\delta \in \mathbb{Z}_{2^n}} (p_{\oplus\alpha;+\delta}^{\text{id}} \cdot p_{+(\delta+\beta);\oplus\gamma}^{\text{id}}), \quad (4)$$

$$p_{\oplus\alpha,\oplus\beta;+\gamma}^+ = \sum_{\delta \in \mathbb{Z}_{2^n}} (p_{\oplus\alpha;+\delta}^{\text{id}} \cdot p_{\oplus\beta;+(\gamma-\delta)}^{\text{id}}). \quad (5)$$

2. Доказательства теорем

2.1. Доказательство теоремы 2.

При доказательстве будем использовать обозначение $\tau_j^*(X, A)$ для знака переноса из $(j+1)$ -го разряда в j -й в результате сложения $X * A$, $*$ $\in \{+, \oplus\}$, где X, A — переменные, представляющие n -разрядные двоичные числа. Ясно, что $\tau_j^\oplus(X, A) \equiv 0$.

Обозначим через $j \in \{0, 1, \dots, n-1\}$ максимальный номер, при котором вектор $(\alpha_j, \beta_j, \gamma_j)$ из V_3 ненулевой.

Если $j = 0$, то суммы $(x *_1 \alpha) * (y *_2 \beta)$ и $(x * y) *_3 \gamma$ совпадают во всех разрядах кроме, быть может, старшего, причем $\tau_0^*(x *_1 \alpha, y *_2 \beta) = \tau_0^*(x, y)$, поэтому соответствующее вероятности $p_{\alpha, \beta; \gamma}$ условие

$$(x *_1 \alpha) * (y *_2 \beta) = (x * y) *_3 \gamma \quad (6)$$

равносильно равенству в старшем разряде

$$(x_0 \oplus \alpha_0) \oplus (y_0 \oplus \beta_0) \oplus \tau_0^*(x *_1 \alpha, y *_2 \beta) = (x_0 \oplus y_0) \oplus \tau_0^*(x, y) \oplus \gamma_0.$$

Поэтому $p_{\alpha, \beta; \gamma} = 1$ при $\alpha_0 \oplus \beta_0 = \gamma_0$, а в противном случае $p_{\alpha, \beta; \gamma} = 0$.

Далее докажем, что при $j > 1$ во всех задачах $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_6, \mathcal{A}_7$ обязательно $p_{\alpha, \beta; \gamma} \leq \frac{1}{2}$. Прежде всего, как и выше при $j = 0$, обращаясь к j -м компонентам левой и правой частей в (6), заключаем, что для неравенства $p_{\alpha, \beta; \gamma} > 0$ необходимо условие $\gamma_j = \alpha_j \oplus \beta_j$. После этого неравенство $p_{\alpha, \beta; \gamma} \leq \frac{1}{2}$ для задач $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_6, \mathcal{A}_7$ будем доказывать отдельно, предполагая каждый раз, что

$$\gamma_j = \alpha_j \oplus \beta_j, \quad (\alpha_j, \beta_j) \in V_2 \setminus \{0\}. \quad (7)$$

2.1.1. Для задачи $\mathcal{A}_1$ условие (6) принимает вид

$$(x + \alpha) \oplus (y + \beta) = (x \oplus y) + \gamma. \quad (8)$$

Для $(j-1)$ -го разряда это равенство означает, что

$$x_{j-1} \oplus \alpha_{j-1} \oplus x_j \alpha_j \oplus y_{j-1} \oplus \beta_{j-1} \oplus y_j \beta_j = x_{j-1} \oplus y_{j-1} \oplus \gamma_{j-1} \oplus (x_j \oplus y_j) \gamma_j. \quad (9)$$

Ввиду (7) равенства (9) и $\alpha_j y_j \oplus \beta_j x_j \oplus \alpha_{j-1} \oplus \beta_{j-1} \oplus \gamma_{j-1} = 0$ равносильны. В последнем равенстве (см. (7)) по крайней мере один из коэффициентов α_j, β_j ненулевой. Поэтому условию (8) удовлетворяет не более половины векторов $(x, y) \in V_n \times V_n$.

2.1.2. Для задачи $\mathcal{A}_2$ условие (6) принимает вид

$$(x + \alpha) \oplus (y + \beta) = x \oplus y \oplus \gamma. \quad (10)$$

Для $(j - 1)$ -го разряда это равенство означает, что

$$x_{j-1} \oplus \alpha_{j-1} \oplus x_j \alpha_j \oplus y_{j-1} \oplus \beta_{j-1} \oplus y_j \beta_j = x_{j-1} \oplus y_{j-1} \oplus \gamma_{j-1}. \quad (11)$$

Равенство (11) равносильно равенству $\alpha_j x_j \oplus \beta_j y_j \oplus \alpha_{j-1} \oplus \beta_{j-1} \oplus \gamma_{j-1} = 0$. В этом равенстве (см. (7)) по крайней мере один из коэффициентов α_j, β_j ненулевой. Поэтому условию (10) удовлетворяет не более половины векторов $(x, y) \in V_n \times V_n$.

2.1.3. Для задачи $\mathcal{A}_6$ условие (6) принимает вид

$$(x \oplus \alpha) + (y + \beta) = (x + y) \oplus \gamma. \quad (12)$$

Положим $\tau = \tau_j^+(x, y)$. Это функция от переменных $x_{j+1}, \dots, x_n, y_{j+1}, \dots, y_n$. Для $(j - 1)$ -го разряда равенство (12) означает, что

$$\begin{aligned} & x_{j-1} \oplus \alpha_{j-1} \oplus y_{j-1} \oplus \beta_{j-1} \oplus y_j \beta_j \oplus (x_j \oplus \alpha_j)(y_j \oplus \beta_j) \\ & \oplus (x_j \oplus \alpha_j \oplus y_j \oplus \beta_j)\tau = x_{j-1} \oplus y_{j-1} \oplus x_j y_j \oplus (x_j \oplus y_j)\tau \oplus \gamma_{j-1}. \end{aligned} \quad (13)$$

Равенство (13) равносильно равенству

$$(\alpha_j \oplus \beta_j)y_j \oplus \beta_j x_j \oplus \alpha_j \beta_j \oplus (\alpha_j \oplus \beta_j)\tau \oplus \alpha_{j-1} \oplus \beta_{j-1} \oplus \gamma_{j-1} = 0.$$

В этом равенстве (см. (7)) по крайней мере один из коэффициентов $(\alpha_j \oplus \beta_j), \beta_j$ ненулевой. Поэтому условию (12) удовлетворяет не более половины векторов $(x, y) \in V_n \times V_n$.

2.1.4. Для задачи $\mathcal{A}_7$ условие (6) принимает вид

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) + \gamma. \quad (14)$$

Снова рассмотрим функцию τ от переменных $x_{j+1}, \dots, x_n, y_{j+1}, \dots, y_n$: $\tau = \tau_j^+(x, y)$. Для $(j - 1)$ -го разряда равенство (14) означает, что

$$\begin{aligned} & x_{j-1} \oplus \alpha_{j-1} \oplus y_{j-1} \oplus \beta_{j-1} \oplus (x_j \oplus \alpha_j)(y_j \oplus \beta_j) \oplus (x_j \oplus \alpha_j \oplus y_j \oplus \beta_j)\tau \\ & = x_{j-1} \oplus y_{j-1} \oplus x_j y_j \oplus (x_j \oplus y_j)\tau \oplus \gamma_{j-1} \oplus (x_j + y_j + \tau)\gamma_j. \end{aligned} \quad (15)$$

Ввиду (7) равенство (15) равносильно равенству

$$\alpha_j x_j \oplus \beta_j y_j \oplus \alpha_j \beta_j \oplus \alpha_{j-1} \oplus \beta_{j-1} \oplus \gamma_{j-1} = 0.$$

В этом равенстве (см. (7)) по крайней мере один из коэффициентов α_j, β_j ненулевой. Поэтому условию (14) удовлетворяет не более половины векторов $(x, y) \in V_n \times V_n$.

Теорема 2 доказана.

2.2. Доказательство теоремы 3.

2.2.1. Доказательство равенства (3). В определении вероятностей $p_{*1\alpha, *2\beta; *3\gamma}^*$, $*, *1, *2, *3 \in \{+, \oplus\}$, исходили из того, что $z = x * y$, а случайный вектор $(x, y) \in V_n \times V_n$ имеет равновероятное распределение. Величина $p_{+\alpha, +\beta; \oplus\gamma}^{\oplus}$ является вероятностью события (10). Рассмотрим разбиение

$$V_n \times V_n = \bigcup_{\delta \in V_n} X_\delta, \quad X_\delta = \{(x, y) \in V_n \times V_n \mid x + \alpha = x \oplus \delta\}.$$

Если $(x, y) \in X_\delta$, то согласно (10) имеем $y + \beta = y \oplus \gamma \oplus \delta$. Используя независимость событий $\{(x, y) \in V_n \times V_n \mid x + \alpha = x \oplus \delta\}$ и $\{(x, y) \in V_n \times V_n \mid y + \beta = y \oplus \gamma \oplus \delta\}$, по формуле полной вероятности получаем $p_{+\alpha, +\beta; \oplus\gamma}^{\oplus} = \sum_{\delta \in V_n} (p_{+\beta; \oplus(\delta \oplus \gamma)}^{\text{id}} \cdot p_{+\alpha; \oplus\delta}^{\text{id}})$.

Равенство (3) доказано.

2.2.2. Доказательство равенства (4). Снова исходим из того, что $z = x + y$, а случайный вектор $(x, y) \in V_n \times V_n$ имеет равновероятное распределение. Величина $p_{\oplus\alpha, +\beta; \oplus\gamma}^+$ является вероятностью события (12). Рассмотрим разбиение

$$V_n \times V_n = \bigcup_{\delta \in V_n} Y_\delta, \quad Y_\delta = \{(x, y) \in V_n \times V_n \mid x \oplus \alpha = x + \delta\}.$$

Если $(x, y) \in Y_\delta$, то согласно (12) имеем $(x + y) + (\delta + \beta) = (x + y) \oplus \gamma$. Используя независимость событий $\{(x, y) \in V_n \times V_n \mid x \oplus \alpha = x + \delta\}$ и $\{(x, y) \in V_n \times V_n \mid (x + y) + (\delta + \beta) = (x + y) \oplus \gamma\}$, по формуле полной вероятности получаем $p_{\oplus\alpha, +\beta; \oplus\gamma}^+ = \sum_{\delta \in \mathbb{Z}_2^n} (p_{+(\delta+\beta); \oplus\gamma}^{\text{id}} \cdot p_{\oplus\alpha; +\delta}^{\text{id}})$.

Равенство (4) доказано.

2.2.3. Доказательство равенства (5). Здесь также исходили из того, что $z = x + y$, а случайный вектор $(x, y) \in V_n \times V_n$ имеет равновероятное распределение. Величина $p_{\oplus\alpha, \oplus\beta; +\gamma}^+$ является вероятностью события (14). Рассмотрим разбиение

$$V_n \times V_n = \bigcup_{\delta \in V_n} Z_\delta, \quad Z_\delta = \{(x, y) \in V_n \times V_n \mid x \oplus \alpha = x + \delta\}.$$

Если $(x, y) \in Z_\delta$, то согласно (14) имеем $y \oplus \beta = y + (\gamma - \delta)$. Используя независимость событий $\{(x, y) \in V_n \times V_n \mid x \oplus \alpha = x + \delta\}$ и $\{(x, y) \in$

$V_n \times V_n \mid y \oplus \beta = y + (\gamma - \delta)\}$, по формуле полной вероятности получаем $p_{\oplus\alpha, \oplus\beta; +\gamma}^+ = \sum_{\delta \in \mathbb{Z}_{2^n}} \left(p_{\oplus\beta; +(\gamma-\delta)}^{\text{id}} \cdot p_{\oplus\alpha; +\delta}^{\text{id}} \right)$.

Равенство (5) доказано.

Теорема 3 полностью доказана.

Список литературы

- [1] Yang G., Zhu B., Suder V., Aagaard M.D., Gong G., “The SIMECK family of lightweight block ciphers”, CHES 2015, 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*, 2013, <http://eprint.iacr.org/2013/404>.
- [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*, 2016, <http://eprint.iacr.org/2013/115>.
- [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., “Вероятностные характеристики разностных и линейных соотношений для неоднородной линейной среды”, *Математические вопросы криптографии*, **10:1** (2019), 41–72.