

ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 31 № 4 2024

Новосибирск
Издательство Института математики

ЧИСЛО НЕВОЗМОЖНЫХ РАЗНОСТЕЙ ПО МОДУЛЮ 2^n КОМПОЗИЦИИ XOR И ЦИКЛИЧЕСКОГО СДВИГА БИТОВ

Н. А. Коломеец

Институт математики им. С. Л. Соболева,
пр. Акад. Коптюга, 4, 630090 Новосибирск, Россия
E-mail: nkolomeec@gmail.com

Аннотация. Для преобразования $(x \oplus y) \lll r$, $x, y \in \mathbb{Z}_2^n$, $1 \leq r < n$, исследуются невозможные разности по модулю 2^n . Они представляют интерес в контексте разностных атак на шифры, схемы которых состоят из сложений по модулю 2^n , побитовых XOR ($\oplus$) и циклических сдвигов битов на r позиций ($\lll r$). В работе найдено число всех невозможных разностей при всех возможных значениях n и r . В качестве следствия показано, что оно больше $\frac{38}{245}8^n$, причём эта оценка асимптотически точна при r , $n - r \rightarrow \infty$. При фиксированном n число невозможных разностей монотонно убывает с ростом r от 1 до $\lceil n/2 \rceil$ ($n/2 + 1$ при $n \in \{4, 6, 8, 10, 12\}$), а далее — монотонно возрастает. Приведено более компактное описание всех невозможных разностей с точностью до известных симметрий. Табл. 10, библиогр. 25.

Ключевые слова: ARX, разностная характеристика, XOR, сложение по модулю, циклический сдвиг битов, невозможная разность.

Введение

Примитивы симметричной криптографии, ориентированные на программную реализацию, могут быть представлены в виде схем, состоящих только из сложений по модулю 2^n ($\boxplus$), побитовых исключающих «или» (XOR, $\oplus$) и циклических сдвигов битов на r позиций в сторону старших разрядов ($\lll r$). Такие конструкции называются ARX-шифрами (см. Speck [1], CHAM [2], Salsa20 [3], ChaCha [4], Sparkle [5], Chaskey [6] и многие др.). Построение оценок их стойкости к разностным атакам [7] приводит к необходимости анализа разностных характеристик преобразований в этом базисе. Далее будем рассматривать разности относительно операции $\boxplus$, в общем же они могут быть выбраны и иными способами (см. [8–12]).

Значение разностной характеристики adp^f по модулю 2^n (т. е. относительно $\boxplus$) для преобразования $f: (\mathbb{Z}_2^n)^k \rightarrow \mathbb{Z}_2^n$ на наборе разностей $\alpha^1, \dots, \alpha^{k+1} \in \mathbb{Z}_2^n$ определяется следующим образом:

$$\begin{aligned} \text{adp}^f(\alpha^1, \dots, \alpha^k \rightarrow \alpha^{k+1}) &= \\ &= \Pr_{(x^1, \dots, x^k) \in (\mathbb{Z}_2^n)^k} [f(x^1 \boxplus \alpha^1, \dots, x^k \boxplus \alpha^k) = f(x^1, \dots, x^k) \boxplus \alpha^{k+1}], \end{aligned}$$

где $x^1, \dots, x^k$ независимы и равномерно распределены на $\mathbb{Z}_2^n$. Таким образом, это вероятность преобразования функцией f входных разностей $\alpha^1, \dots, \alpha^k$ в выходную разность α^{k+1} . Например, свойства разностной характеристики по модулю 2^n функции $x \mapsto x \lll r$ исследовались в [13, 14], функции $(x, y) \mapsto x \oplus y$ — в [15–17], а функции $(x, y) \mapsto (x \lll r) \oplus y$ — в [18–20]. Обозначим через adp^{XR} разностную характеристику для XR-преобразования $(x, y) \mapsto (x \oplus y) \lll r$, где $x, y \in \mathbb{Z}_2^n$ и $1 \leq r < n$, а через $\mathcal{N}_n^r$ — число невозможных разностей этого преобразования (вероятность возникновения которых равна 0). В [19] найдены все невозможные разности XR-преобразования в виде шаблонов — регулярных выражений (см. разд. 1). В настоящей работе продолжены исследования в этом направлении: приводится точная формула для $\mathcal{N}_n^r$, устанавливаются его свойства и упрощается список невозможных разностей с применением известных симметрий adp^{XR} . Отметим, что все невозможные разности также известны для базовых операций и композиций нескольких XOR [21]. Они наиболее интересны в контексте атак, предложенных в [22, 23].

Разд. 1 содержит базовые определения и обозначения. В разд. 2 приведено описание всех невозможных разностей XR-преобразования (утверждение 1 и табл. 2), полученное в [19]. Точная формула для $\mathcal{N}_n^r$ найдена в разд. 3 (теорема 1). В разд. 4 рассматриваются свойства $\mathcal{N}_n^r$. Нижняя оценка $\mathcal{N}_n^r > \frac{38}{245}8^n$, асимптотически точная при $r, n - r \rightarrow \infty$, доказана в п. 4.1. В п. 4.2 установлено, что

$$\mathcal{N}_n^1 > \mathcal{N}_n^2 > \dots > \mathcal{N}_n^s < \mathcal{N}_n^{s+1} < \dots < \mathcal{N}_n^{n-1},$$

где $s = \lceil n/2 \rceil$ при $n \notin \{4, 6, 8, 10, 12\}$ и $s = n/2 + 1$ иначе (теорема 2). Как следствие, справедливы следующие оценки:

$$\mathcal{N}_n^s \leq \mathcal{N}_n^r \leq \mathcal{N}_n^{n-1} < \mathcal{N}_n^2 < \mathcal{N}_n^1 \quad \text{при } 3 \leq r < n.$$

Оценка $\mathcal{N}_n^r \leq \mathcal{N}_n^{n-1}$ при $r \geq 3$ точнее, чем $\mathcal{N}_n^r < \mathcal{N}_n^1$ из [19], в виду равенств

$$\mathcal{N}_n^1 = \frac{5}{14}8^n - \frac{6}{7}, \quad \mathcal{N}_n^{n-1} = \frac{3}{14}8^n + \frac{2}{3}4^n - \frac{50}{21}.$$

Известно, что преобразование $(x, y) \mapsto x \oplus y$ имеет ровно $\frac{4}{7}8^n - \frac{4}{7}$ невозможных разностей [15]. Таким образом, добавление циклического сдвига существенно снижает их число. В разд. 5 приводится описание всех

невозможных разностей XR-преобразования с точностью до симметрий, сохраняющих значение adp^{XR} (теорема 3 и табл. 10). В отличие от табл. 2, такое описание содержит 10 пар шаблонов, что существенно компактнее.

Заметим, что полученные результаты применимы к преобразованиям RX: $(x, y) \mapsto (x \lll r) \oplus y$, ARX: $(x, y, z) \mapsto ((x \boxplus y) \lll r) \oplus z$ и аналогичным, поскольку их разностные характеристики прямо выражаются через adp^{XR} , а именно: при любых $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_2^n$ имеем

$$\begin{aligned}\text{adp}^{\text{RX}}(\alpha, \beta \xrightarrow{r} \gamma) &= \text{adp}^{\text{XR}}(\gamma, \beta \xrightarrow{n-r} \alpha), \\ \text{adp}^{\text{ARX}}(\alpha, \beta, \gamma \xrightarrow{r} \delta) &= \text{adp}^{\text{RX}}(\alpha \boxplus \beta, \gamma \xrightarrow{r} \delta)\end{aligned}$$

и т. д.

Задачи, связанные с ARX-схемами, встречаются и на криптографических олимпиадах (см. NSUCRYPTO [24, 25]).

1. Определения

Пусть $\mathbb{Z}_2^n$ — линейное пространство двоичных векторов размерности n . Поскольку ARX-схемы комбинируют операции $\oplus$ и $\boxplus$, сопоставим вектору $x = (x_1, \dots, x_n) \in \mathbb{Z}_2^n$ целое число

$$2^{n-1}x_1 + 2^{n-2}x_2 + \dots + 2^0x_n,$$

т. е. x_1 является *наиболее значимым* битом. Под суммой $x + y$ векторов $x, y \in \mathbb{Z}_2^n$ будем подразумевать сложение соответствующих им целых чисел по модулю 2^n , тем самым $x + y \in \{0, \dots, 2^n - 1\}$. Аналогично $-x$ обозначает противоположное относительно сложения по модулю 2^n число к числу, соответствующему x . Обозначим через $(x, z) = (x_1, \dots, x_n, z_1, \dots, z_m)$ *конкатенацию* вектора x с вектором $z \in \mathbb{Z}_2^m$. Положим также $\bar{x} = (x_1 \oplus 1, x_2 \oplus 1, \dots, x_n \oplus 1)$.

Рассматриваемая в работе разностная характеристика относительно сложения по модулю 2^n для XR-преобразования $(x, y) \mapsto (x \oplus y) \lll r$, где $1 \leq r < n$, определяется как

$$\begin{aligned}\text{adp}^{\text{XR}}(\alpha, \beta \xrightarrow{r} \gamma) &= \frac{1}{4^n} |\{(x, y) \in (\mathbb{Z}_2^n)^2 \mid \\ &\quad ((x + \alpha) \oplus (y + \beta)) \lll r = \gamma + ((x \oplus y) \lll r)\}|,\end{aligned}$$

а число его невозможных разностей — как

$$\mathcal{N}_n^r = |\{(\alpha, \beta, \gamma) \in (\mathbb{Z}_2^n)^3 \mid \text{adp}^{\text{XR}}(\alpha, \beta \xrightarrow{r} \gamma) = 0\}|.$$

Для удобства представим тройки $(\alpha, \beta, \gamma) \in (\mathbb{Z}_2^n)^3$ в виде восьмеричного слова $\omega \in \{0, \dots, 7\}^n$, определив

$$\omega(\alpha, \beta, \gamma) = (4\alpha_1 + 2\beta_1 + \gamma_1, \dots, 4\alpha_n + 2\beta_n + \gamma_n).$$

Для $\omega(\alpha, \beta, \gamma)_i$, $i \in \{1, \dots, n\}$, используем как численное $4\alpha_i + 2\beta_i + \gamma_i$, так и векторное $(\alpha_i, \beta_i, \gamma_i)$ обозначения.

Таблица 1

Символы в шаблонах

Символ	Значение
[	начало (наиболее значимые биты)
]	конец (наименее значимые биты)
.	0, 1, 2, 3, 4, 5, 6, 7 (любое значение)
e и d	0, 3, 5, 6 и 1, 2, 4, 7 соответственно
$\hat{t}$	$t, t \oplus 3, t \oplus 5$
α_0 и α_1	0, 1, 2, 3 и 4, 5, 6, 7 соответственно
β_0 и β_1	0, 1, 4, 5 и 2, 3, 6, 7 соответственно
γ_0 и γ_1	0, 2, 4, 6 и 1, 3, 5, 7 соответственно
0_6 и 1_7	0, 6 и 1, 7 соответственно
s*	пусто, s, ss, sss, ssss, ...

Для описания слов будем использовать шаблоны — регулярные выражения. В табл. 1 приведены элементы шаблонов и их значения. Пусть $\omega = \omega(\alpha, \beta, \gamma)$ для $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$. Запись $\omega \in \xi$ означает, что ω удовлетворяет шаблону ξ . Приведём примеры:

- $\omega \in [.*d]$ означает $\omega_n \in \{1, 2, 4, 7\}$;
- $\omega \in [.*e11*]$ означает, что $\omega = (\omega_1, \dots, \omega_k, 1, \dots, 1)$, $\omega_k \in \{0, 3, 5, 6\}$ для некоторого $1 \leq k \leq n-1$;
- $\omega \in [00*2\alpha_0*]$ означает равенство $\omega = (0, \omega_2, \dots, \omega_k, 2, \omega_{k+2}, \dots, \omega_n)$, где $\omega_2, \dots, \omega_k \in \{0, 3, 5\}$, $\omega_{k+2}, \dots, \omega_n \in \{0, 1, 2, 3\}$, $1 \leq k \leq n-1$. Отметим, что $\omega = (0, 2, \omega_3, \dots, \omega_n)$ при $k = 1$, а при $k = n-1$ имеем $\omega = (0, \omega_2, \dots, \omega_{n-1}, 2)$, т. е. одна из обозначенных частей слова ω может быть пустой.

Удобно также использовать следующие симметрии.

- 1) Шаблоны ξ и ζ назовём $\alpha\beta$ -эквивалентными, если $\omega(\alpha, \beta, \gamma) \in \xi$ тогда и только тогда, когда $\omega(\beta, \alpha, \gamma) \in \zeta$, для любых $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$;
- 2) Шаблоны ξ и ζ назовём $\overline{\gamma}$ -эквивалентными, если $\omega(\alpha, \beta, \gamma) \in \xi$ тогда и только тогда, когда $\omega(\alpha, \beta, \overline{\gamma}) \in \zeta$, для любых $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$.

Шаблон ξ удовлетворяет шаблону ζ (пишем $\xi \subseteq \zeta$), если для любого $\omega \in \xi$ имеет место $\omega \in \zeta$. Шаблоны ξ и ζ не пересекаются, если не существует слова, удовлетворяющего им обоим.

2. Невозможные разности XR-преобразования

Невозможные разности XR-преобразования описаны в [19, теорема 9]. Шаблоны таких разностей представлены в табл. 2. Через $X.Y$ обозначим шаблон в столбце X и строке Y табл. 2. Будем говорить, что пара (ω, ω')

Таблица 2

Невозможные разности XR-функции

№ пп	1 [.*d00*]	2 [.*e22*]	3 [.*e44*]	4 [.*d66*]	5 [.*d]	6 [.*]	7 [γ ₀ *]
1	[α ₀ *]	[α ₀ *]	[β ₀ *]	[66̂*7.*]	[0*]	[.*d00*]	[.*d]
2	[β ₀ *]	[22̂*]	[44̂*]	[66̂*1γ ₁ *1 ₇]	[1*]	[.*e11*]	
3	[00̂*]	[22̂*3.*]	[44̂*5.*]	[77̂*6.*]			
4	[00̂*1.*]	[22̂*0α ₀ *]	[44̂*0β ₀ *]	[77̂*0γ ₀ *0 ₆]			
5	[00̂*2α ₀ *]	[22̂*5γ ₁ *1 ₇]	[44̂*3γ ₁ *1 ₇]				
6	[00̂*4β ₀ *]	[33̂*]	[55̂*]				
7	[00̂*7]	[33̂*2.*]	[55̂*4.*]				
8	[00̂*7γ ₁ *1 ₇]	[33̂*1α ₀ *]	[55̂*1β ₀ *]				
9	[11̂*]	[33̂*4γ ₀ *0 ₆]	[55̂*2γ ₀ *0 ₆]				
10	[11̂*0.*]						
11	[11̂*3α ₀ *]						
12	[11̂*5β ₀ *]						
13	[11̂*6]						
14	[11̂*6γ ₀ *0 ₆]						

удовлетворяет шаблону $X.Y$, если $\omega \in X.Y$, а ω' удовлетворяет метке столбца X . Например, запись $\omega \in 7.1$ равносильна тому, что $\omega \in [.*d]$, а $(\omega, \omega') \in 7.1$ означает, что $\omega \in [.*d]$ и $\omega' \in [\gamma_0*]$.

Утверждение 1 [19]. Если $\omega = \omega(\alpha, \beta, \gamma)$, $\omega' = \omega(\alpha', \beta', \gamma')$ для некоторых $\alpha, \beta, \gamma \in \mathbb{Z}_2^{n-r}$, $\alpha', \beta', \gamma' \in \mathbb{Z}_2^r$, то $\text{adp}^{\text{XR}}((\alpha', \alpha), (\beta', \beta) \xrightarrow{r} (\gamma, \gamma')) = 0$ тогда и только тогда, когда $(\omega, \omega') \in X.Y$ для некоторых столбца X и строки Y табл. 2.

Таблица 3

Символы, удовлетворяющие $\hat{\mathbf{t}}$

$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$	$\hat{7}$
0, 3, 5	1, 2, 4	1, 2, 7	0, 3, 6	1, 4, 7	0, 5, 6	3, 5, 6	2, 4, 7
$\mathbf{e} \setminus \{6\}$	$\mathbf{d} \setminus \{7\}$	$\mathbf{d} \setminus \{4\}$	$\mathbf{e} \setminus \{5\}$	$\mathbf{d} \setminus \{2\}$	$\mathbf{e} \setminus \{3\}$	$\mathbf{e} \setminus \{0\}$	$\mathbf{d} \setminus \{1\}$

Далее будем работать только с шаблонами из табл. 2 и их пересечениями. Поскольку они содержат выражения вида $\mathbf{t}\hat{\mathbf{t}}*$, приведём в явном виде очевидные свойства $\hat{\mathbf{t}}$.

Утверждение 2. Значения $\hat{\mathbf{t}}$ для всех $t \in \mathbb{Z}_2^3$ приведены в табл. 3. Кроме того,

- 1) $\hat{\mathbf{t}} \subseteq \mathbf{e}$ ($\hat{\mathbf{t}} \subseteq \mathbf{d}$) тогда и только тогда, когда $t \in \mathbf{e}$ ($t \in \mathbf{d}$), причём $\hat{\mathbf{t}} = \mathbf{e} \setminus \{t \oplus 6\}$ ($\hat{\mathbf{t}} = \mathbf{d} \setminus \{t \oplus 6\}$);
- 2) $\hat{\mathbf{t}} \oplus \hat{\mathbf{s}} = \hat{\mathbf{t}} \oplus s$ для $s \in \mathbb{Z}_2^3$.

Отметим, что в [19, следствия 5, 6] доказано, что

$$\mathcal{N}_n^r < \mathcal{N}_n^1 = \frac{5}{14}8^n - \frac{6}{7}, \quad 2 \leq r < n. \quad (1)$$

3. Число невозможных разностей

Здесь найдём $\mathcal{N}_n^r$, т. е. число невозможных разностей XR-преобразования, разбив раздел на три части. В п. 3.1 столбцы 1–6 табл. 2 представлены в более удобном виде. П. 3.2 классифицирует шаблоны столбцов 1–4 (которые и составляют основную массу шаблонов), а также их пересечения с шаблонами столбца 6. В п. 3.3 получим итоговую формулу для $\mathcal{N}_n^r$.

Для подсчёта числа слов, удовлетворяющих рассматриваемым шаблонам, используется

Лемма 1. Для любых попарно различных целых $a, b, c > 0$ и любого целого $m > 0$ справедливы равенства

$$\begin{aligned} 1) \quad & \sum_{i=0}^m a^i b^{m-i} = \frac{1}{a-b}(a^{m+1} - b^{m+1}); \\ 2) \quad & \sum_{i=0}^m \sum_{j=0}^{m-i} a^i b^j c^{m-i-j} = \frac{a^{m+2}}{(a-b)(a-c)} + \frac{b^{m+2}}{(b-a)(b-c)} + \frac{c^{m+2}}{(c-a)(c-b)}. \end{aligned}$$

Доказательство. П. 1 очевиден в силу формулы

$$(a-b)(a^m b^0 + a^{m-1} b^1 + \dots + a^0 b^m) = a^{m+1} - b^{m+1}.$$

Для доказательства п. 2 воспользуемся п. 1:

$$\begin{aligned} \sum_{i=0}^m \sum_{j=0}^{m-i} a^i b^j c^{m-i-j} &= \sum_{i=0}^m a^i \sum_{j=0}^{m-i} b^j c^{m-i-j} = \\ &= \frac{1}{b-c} \sum_{i=0}^m a^i (b^{m-i+1} - c^{m-i+1}) = \frac{b}{b-c} \sum_{i=0}^m a^i b^{m-i} + \\ &+ \frac{c}{c-b} \sum_{i=0}^m a^i c^{m-i} = \frac{b(a^{m+1} - b^{m+1})}{(b-c)(a-b)} + \frac{c(a^{m+1} - c^{m+1})}{(c-b)(a-c)} = \\ &= \frac{ba^{m+1}}{(a-b)(b-c)} + \frac{ca^{m+1}}{(a-c)(c-b)} + \frac{b^{m+2}}{(b-c)(b-a)} + \frac{c^{m+2}}{(c-a)(c-b)}, \end{aligned}$$

при этом сумма первых двух слагаемых в последней строке равна

$$\begin{aligned} \frac{a^{m+1}}{b-c} \left(\frac{b}{a-b} - \frac{c}{a-c} \right) &= \frac{a^{m+1}(ba - bc - ca + cb)}{(b-c)(a-b)(a-c)} = \\ &= \frac{a^{m+2}(b-c)}{(b-c)(a-b)(a-c)} = \frac{a^{m+2}}{(a-b)(a-c)}. \end{aligned}$$

Лемма 1 доказана.

3.1. Упрощение таблицы 2. Начнём со следующей леммы.

Лемма 2. Пусть $\omega = \omega(\alpha, \beta, \gamma)$ для $\alpha, \beta, \gamma \in \mathbb{Z}_2^{n-r}$. Тогда

- 1) если $\omega \in [0\hat{0}*\alpha_0*] ([1\hat{1}*\alpha_0*])$, то ω удовлетворяет 1.3, 1.4 или 1.5 (1.9, 1.10 или 1.11);
- 2) если $\omega \in [0\hat{0}*\beta_0*] ([1\hat{1}*\beta_0*])$, то ω удовлетворяет 1.3, 1.4 или 1.6 (1.9, 1.10 или 1.12);
- 3) если $\omega \in [2\hat{2}*\alpha_0*] ([3\hat{3}*\alpha_0*])$, то ω удовлетворяет 2.2, 2.3 или 2.4 (2.6, 2.7 или 2.8);
- 4) если $\omega \in [4\hat{4}*\beta_0*] ([5\hat{5}*\beta_0*])$, то ω удовлетворяет 3.2, 3.3 или 3.4 (3.6, 3.7 или 3.8).

ДОКАЗАТЕЛЬСТВО. 1) Если $\omega \notin 1.3$, то определим ω^α как часть ω , идущую после $0\hat{0}*$ и удовлетворяющую α_0* , причём $\omega_0^\alpha \notin \hat{0}$. В этом случае $\omega_0^\alpha \in \{1, 2\}$, так как 0 и 3 удовлетворяют $\hat{0}$ (см. табл. 3), но тогда ω удовлетворяет либо 1.4, либо 1.5.

Шаблон $[1\hat{1}*\alpha_0*]$ $\bar{\gamma}$ -эквивалентен уже рассмотренному, поэтому удовлетворяет шаблонам, $\bar{\gamma}$ -эквивалентным 1.3, 1.4 и 1.5, которыми являются 1.9, 1.10 и 1.11 соответственно.

2) Достаточно заметить, что шаблоны $[0\hat{0}*\beta_0*] ([1\hat{1}*\beta_0*])$ $\alpha\beta$ -эквивалентны рассмотренным в п. 1, а шаблоны 1.3, 1.4 и 1.6 (1.9, 1.10 и 1.12) $\alpha\beta$ -эквивалентны 1.3, 1.4 и 1.5 (1.9, 1.10 и 1.11) соответственно.

3) Аналогично п. 1, если $\omega \notin 2.2$, определим ω^α такое, что $\omega_0^\alpha \notin \hat{2}$, т. е. $\omega_0^\alpha \in \{0, 3\}$, поскольку 1 и 2 удовлетворяют $\hat{2}$, но тогда ω удовлетворяет либо 2.4, либо 2.3.

4) Шаблоны этого пункта $\alpha\beta$ -эквивалентны соответствующим шаблонам п. 3 (см. также столбцы 2, 3 табл. 2). Лемма 2 доказана.

Лемма 3. Если $\omega = \omega(\alpha, \beta, \gamma)$, $\omega' = \omega(\alpha', \beta', \gamma')$ для $\alpha, \beta, \gamma \in \mathbb{Z}_2^{n-r}$, $\alpha', \beta', \gamma' \in \mathbb{Z}_2^r$, то (ω, ω') удовлетворяет шаблону из столбцов 1–6 табл. 2 тогда и только тогда, когда либо (ω, ω') , либо $(\omega(\alpha, \beta, \bar{\gamma}), \omega')$ удовлетворяет некоторому шаблону из табл. 4. Более того, среди шаблонов одного столбца табл. 4 и $\bar{\gamma}$ -эквивалентных к ним никакие два не пересекаются.

ДОКАЗАТЕЛЬСТВО. Ввиду условия леммы из пары $\bar{\gamma}$ -эквивалентных шаблонов одного столбца табл. 2 достаточно рассмотреть только один. Таким образом, удаляем шаблоны 1.9–14, 2.6–9, 3.6–9, 4.3–4, 5.2 и 6.2. Замыкание оставшихся шаблонов относительно $\bar{\gamma}$ -эквивалентности составит столбцы 1–6 табл. 2.

По лемме 2 шаблон 1.1 можно преобразовать в $[2\alpha_0*]$ и $\bar{\gamma}$ -эквивалентный последнему $[3\alpha_0*]$ (слова, удовлетворяющие $[0_1\alpha_0*]$, удовлетворяют одному из 1.3–1.14); шаблон 1.2 — в $[4\beta_0*]$ и $\bar{\gamma}$ -эквивалентный

Таблица 4

Шаблоны столбцов 1–6 табл. 2 с точностью до $\bar{\gamma}$ -эквивалентности

№ пп	1 [. *d00*]	2 [. *e22*]	3 [. *e44*]	4 [. *d66*]	5 [. *d]	6 [. *]
1	$[2\alpha_0*]$	$[0\alpha_0*]$	$[0\beta_0*]$	$[6\hat{6}*7.*]$	$[0*]$	$[. *d00*]$
2	$[4\beta_0*]$	$[2\hat{2}*]$	$[4\hat{4}*]$	$[6\hat{6}*1\gamma_1*1_7]$		
3	$[0\hat{0}*]$	$[2\hat{2}*3.*]$	$[4\hat{4}*5.*]$			
4	$[0\hat{0}*1.*]$	$[2\hat{2}*0\alpha_0*]$	$[4\hat{4}*0\beta_0*]$			
5	$[0\hat{0}*2\alpha_0*]$	$[2\hat{2}*5\gamma_1*1_7]$	$[4\hat{4}*3\gamma_1*1_7]$			
6	$[0\hat{0}*4\beta_0*]$					
7	$[0\hat{0}*7]$					
8	$[0\hat{0}*7\gamma_1*1_7]$					

ему $[5\beta_0*]$; шаблон 2.1 — в $[0\alpha_0*]$ и $\bar{\gamma}$ -эквивалентный ему $[1\alpha_0*]$; шаблон 3.1 — в $[0\beta_0*]$ и $\bar{\gamma}$ -эквивалентный ему $[1\beta_0*]$.

Таким образом, шаблоны одного столбца табл. 4 попарно не пересекаются, что также имеет место при добавлении $\bar{\gamma}$ -эквивалентных им шаблонов: любые два отличаются как минимум одним фиксированным символом. Лемма 3 доказана.

3.2. Классификация шаблонов из столбцов 1–4 таблицы 2.

Скомбинируем шаблоны столбцов 1–4 табл. 2 и их пересечения с шаблонами 6.1 и 6.2, объединяя те из них, которым удовлетворяет одинаковое число слов. В результате получим табл. 5 и 6, каждая строка которых содержит тип шаблона, число шаблонов этого типа в табл. 2, число слов, удовлетворяющих шаблону этого типа, и ограничение, при котором указанная формула справедлива. Если ограничение не выполняется, то не существует слов длины $n - r$, удовлетворяющих соответствующему шаблону. Отметим, что табл. 5 почти совпадает с [19, табл. 5].

Лемма 4. Табл. 5 классифицирует шаблоны из столбцов 1–4 табл. 2.

ДОКАЗАТЕЛЬСТВО. Будем пользоваться табл. 4, умножая итоговое число шаблонов на 2 в силу $\bar{\gamma}$ -эквивалентности (см. лемму 3). Также если слово удовлетворяет некоторому из шаблонов, то все «звёздочки» расставляются однозначно. Действительно, после $t\hat{t}*$ всегда идёт символ, не удовлетворяющий t (либо его нет).

1. Тип $[2\alpha_0*]$. К нему относятся 1.1, 1.2, 2.1 и 3.1, что даёт $2 \cdot 4$ шаблонов, каждому из которых удовлетворяет 4^{n-r-1} слов.

2. Тип $[0\hat{0}*1.*]$. К нему относятся 1.4, 2.3, 3.3 и 4.1, что даёт $2 \cdot 4$ шаблонов. Каждому из них удовлетворяет

Таблица 5

Классификация шаблонов из столбцов 1–4 табл. 2

№	Тип шаблона	#	Число слов	Ограничение
1	$[2\alpha_0*]$	8	4^{n-r-1}	$n-r \geq 1$
2	$[0\hat{0}*1.*]$	8	$\frac{1}{5}(8^{n-r-1} - 3^{n-r-1})$	$n-r \geq 1$
3	$[0\hat{0}*2\alpha_0*]$	8	$4^{n-r-1} - 3^{n-r-1}$	$n-r \geq 1$
4	$[0\hat{0}*7\gamma_1*1_7]$	8	$2(4^{n-r-2} - 3^{n-r-2})$	$n-r \geq 2$
5	$[0\hat{0}*]$	6	3^{n-r-1}	$n-r \geq 1$
6	$[0\hat{0}*7]$	2	3^{n-r-2}	$n-r \geq 2$

$$8^0 \cdot 3^{n-r-2} + 8^1 \cdot 3^{n-r-3} + \dots + 8^{n-r-2} \cdot 3^0 = \sum_{i=0}^{n-r-2} 8^i \cdot 3^{n-r-2-i}$$

слов, что по лемме 1 равно $\frac{1}{5}(8^{n-r-1} - 3^{n-r-1})$. Если $n-r < 2$, то шаблону не может удовлетворять ни одно слово. Однако $\frac{1}{5}(8^{1-1} - 3^{1-1}) = 0$, поэтому можно считать, что $n-r \geq 1$.

3. Тип $[0\hat{0}*2\alpha_0*]$. К нему относятся 1.5, 1.6, 2.4 и 3.4, что даёт 2·4 шаблонов. Каждому удовлетворяет $\sum_{i=0}^{n-r-2} 4^i \cdot 3^{n-r-2-i}$ слов, что по лемме 1 равно $4^{n-r-1} - 3^{n-r-1}$. Аналогично при $n-r < 2$ шаблону не удовлетворяет ни одно слово. Однако $4^{1-1} - 3^{1-1} = 0$, поэтому формула верна при $n-r \geq 1$.

4. Тип $[0\hat{0}*7\gamma_1*1_7]$. К нему относятся 1.8, 2.5, 3.5 и 4.2, что даёт 2·4 шаблонов. Каждому удовлетворяет $2 \cdot \sum_{i=0}^{n-r-3} 4^i \cdot 3^{n-r-3-i}$ слов (делим шаблон на два, заканчивающихся на 1 и 7). По лемме 1 получаем $2(4^{n-r-2} - 3^{n-r-2})$ слов. При $n-r < 3$ шаблону не удовлетворяет ни одно слово. Однако $2(4^{2-2} - 3^{2-2}) = 0$, поэтому формула верна при $n-r \geq 2$.

Таблица 6

Классификация пересечений шаблонов из столбцов 1–4 с шаблонами столбца 6 табл. 2

№	Тип шаблона	#	Число слов	Ограничение
1	$[2\alpha_0*1_200*]$	16	$\frac{2}{3}(4^{n-r-2} - 1)$	$n-r \geq 2$
2	$[200*]$	8	1	$n-r \geq 2$
3	$[0\hat{0}*1.*d00*]$	16	$\frac{4}{35}8^{n-r-2} - \frac{2}{5}3^{n-r-2} + \frac{2}{7}$	$n-r \geq 2$
4	$[0\hat{0}*100*]$	22	$\frac{1}{2}(3^{n-r-2} - 1)$	$n-r \geq 2$
5	$[0\hat{0}*11*]$	6	$\frac{1}{2}(3^{n-r-1} - 1)$	$n-r \geq 1$
6	$[0\hat{0}*2\alpha_0*1_200*]$	24	$\frac{2}{3}4^{n-r-2} - 3^{n-r-2} + \frac{1}{3}$	$n-r \geq 2$

5. Тип $[0\hat{0}*]$. К нему относятся 1.3, 2.2 и 3.2, что даёт $2 \cdot 3$ шаблона. Ему удовлетворяет 3^{n-r-1} слов, где $n - r \geq 1$.

6. Тип $[0\hat{0}*7]$. К нему относится 1.7, которому удовлетворяет 3^{n-r-2} слов, где $n - r \geq 2$.

Все шаблоны столбцов 1–4 табл. 4 рассмотрены. Лемма 4 доказана.

Лемма 5. *Табл. 6 содержит классификацию пересечений шаблонов из столбцов 1–4 с шаблонами столбца 6 табл. 2.*

ДОКАЗАТЕЛЬСТВО. Метки столбцов 1–4 не пересекаются друг с другом, при этом все они удовлетворяют метке $[.*]$ столбца 6, поэтому при классификации можно рассматривать шаблоны независимо друг от друга, как непересекающиеся (что верно с учётом ω' -частей).

Классификацию пересечений проведём по табл. 5, но в некоторых случаях будем обращаться и к табл. 2. Нас интересуют пересечения шаблонов из столбцов 1–4 с шаблонами $[.*d00*]$ (6.1) и $[.*e11*]$ (6.2). Отметим также следующие равенства (см. табл. 1):

$$\begin{aligned}\alpha_0 \cap e &= 0_3, & \beta_0 \cap e &= 0_5, & \gamma_0 \cap e &= 0_6, & \gamma_1 \cap e &= 3_5, \\ \alpha_0 \cap d &= 1_2, & \beta_0 \cap d &= 1_4, & \gamma_0 \cap d &= 2_4, & \gamma_1 \cap d &= 1_7.\end{aligned}$$

1. $[2\alpha_0*]$. Пересечения: $[2\alpha_0*1_200*]$, $[2\alpha_0*0_311*]$ и $[200*]$, других пересечений здесь нет. Таким образом, добавляем $8 \cdot 2$ шаблонов в строку 1 и 8 шаблонов в строку 2.

Далее заметим, что в $[.*d00*]$ и $[.*e11*]$ имеется смена чётности e/d со стороны младших разрядов: $1 \in d$ и $0 \in e$. При этом все оставшиеся шаблоны из классификации в старших битах содержат подстроку $\hat{t}\hat{t}*$, символы которой удовлетворяют либо e , либо d (см. утверждение 2). Это означает, что шаблоны типа 5 табл. 5 не пересекаются с 6.1 и 6.2. Также все шаблоны типа 6, содержащиеся в табл. 2, не заканчиваются ни на 0, ни на 1, т. е. также не имеют пересечений с 6.1 и 6.2. Все оставшиеся шаблоны после $\hat{t}\hat{t}*$ имеют смену чётности e/d или d/e , поэтому e/d из 6.1 и 6.2 может соответствовать символ, начиная с последнего в части $\hat{t}\hat{t}*$.

2. $[0\hat{0}*1.*]$. Пересечения: $[0\hat{0}*1.*d00*]$, $[0\hat{0}*1.*e11*]$ и $[0\hat{0}*100*]$, т. е. добавляем $8 \cdot 2$ шаблонов в строку 3 и 8 шаблонов в строку 4. Однако если шаблон типа 2 содержит после $\hat{t}\hat{t}*$ символы 0 или 1, то появится ещё один тип пересечения: $[0\hat{0}*11*]$. В табл. 2 таких шаблонов два: 1.4 и 1.10, т. е. добавляем 2 шаблона в строку 5.

3. $[0\hat{0}*2\alpha_0*]$. Пересечениями в этом случае являются $[0\hat{0}*2\alpha_0*0_311*]$, $[0\hat{0}*2\alpha_0*1_200*]$ и $[0\hat{0}*200*]$, что добавляет $8 \cdot 2$ шаблонов в строку 6 и 8 шаблонов в строку 4. Аналогично если шаблон типа 3 содержит после подстроки $\hat{t}\hat{t}*$ символы 0 или 1, то появится ещё один тип пересечения: $[2\hat{2}*00*]$. В табл. 2 таких шаблонов четыре: 2.4, 2.8, 3.4 и 3.8, т. е. добавляем 4 шаблона в строку 5.

4. $[0\hat{0}*7\gamma_1*1_7]$. Пересечение — $[0\hat{0}*7\gamma_1*3_511*]$, так как он не пересекается с 6.1. Добавляем 8 шаблонов в строку 6. Если шаблон типа 4 после подстроки $\hat{t}\hat{t}*$ содержит символ из e/d и оканчивается на $1/0$, то появится пересечение $[2\hat{2}*511*]$. В табл. 2 таких шаблонов четыре: 2.5, 2.9, 3.5 и 3.9, т. е. добавляем 4 шаблона в строку 4. Ещё один случай дают шаблоны 4.2 и 4.4, в которых после $\hat{t}\hat{t}*$ и в конце стоит 1 (4.2) и 0 (4.4). Это даёт 2 пересечения вида $[6\hat{6}*111*]$, которые добавляются в строку 4.

Тем самым перечислены все типы шаблонов и их число. Они представлены в столбцах 2 и 3 табл. 6. Далее найдём число слов, удовлетворяющих каждому из указанных типов шаблонов. Отметим, что «звёздочки» $*$ в таких словах расставляются однозначно. Действительно, «звёздочка» после $\hat{t}\hat{t}$ всегда оканчивается символом, не принадлежащим $\hat{t}$. «Звёздочка» со стороны младших разрядов также оканчивается символом, отличным от $0/1$. С учётом фиксированной длины слов $n - r$ даже при наличии в шаблоне третьей «звёздочки» её элементы определяются однозначно. Далее будем пользоваться леммой 1: п. 1 в случае двух «звёздочек» и п. 2 в случае трёх.

Шаблон $[2\alpha_0*1_200*]$ разбивается на два непересекающихся подшаблона $[2\alpha_0*100*]$ и $[2\alpha_0*200*]$. Здесь три фиксированных символа, т. е. взяв $m = n - r - 3$, получим, что число слов, удовлетворяющих каждому из шаблонов, равно $\sum_{i=0}^m 4^i \cdot 1^{m-i}$. В силу леммы 1 получаем $\frac{1}{4-1}(4^{m+1} - 1) = \frac{1}{3}(4^{n-r-2} - 1)$ слов на каждый подшаблон. Однако, несмотря на ограничение $n - r \geq 3$ (в шаблоне три фиксированных символа), $\frac{1}{3}(4^{n-r-2} - 1) = 0$ при $n - r = 2$, т. е. указанная формула справедлива при $n - r \geq 2$.

Шаблону $[200*]$ удовлетворяет ровно одно слово с условием $n - r \geq 2$, поскольку здесь имеется два фиксированных символа.

Шаблон $[0\hat{0}*1.*d00*]$ по значению d разделим на 4 непересекающихся подшаблона, в каждом из которых 4 фиксированных символа. При $m = n - r - 4$ получим $\sum_{i=0}^m \sum_{j=0}^{m-i} 8^i \cdot 3^j \cdot 1^{m-i-j}$ слов на каждый подшаблон равно.

По лемме 1 получим следующее число слов на подшаблон:

$$\frac{8^{m+2}}{(8-3)(8-1)} + \frac{3^{m+2}}{(3-8)(3-1)} + \frac{1^{m+2}}{(1-8)(1-3)} = \frac{8^{n-r-2}}{35} - \frac{3^{n-r-2}}{10} + \frac{1}{14}.$$

При $n - r \in \{2, 3\}$ эта сумма обращается в нуль: $\frac{8}{35} - \frac{3}{10} + \frac{1}{14} = \frac{16-21+5}{35 \cdot 2} = 0$ и $\frac{1}{35} - \frac{1}{10} + \frac{1}{14} = \frac{2-7+5}{35 \cdot 2} = 0$, так что ограничение можно ослабить, взяв $n - r \geq 2$.

Аналогично для шаблонов $[0\hat{0}*100*]$ и $[0\hat{0}*11*]$ получаем $\frac{1}{2}(3^{n-r-2} - 1)$ и $\frac{1}{2}(3^{n-r-1} - 1)$ слов с ограничениями $n - r \geq 2$ и $n - r \geq 1$ соответственно.

Шаблон $[0\widehat{0}*2\alpha_0*1_200*]$ разделим на два подшаблона по значению символа 1_2 и аналогично рассмотренному случаю для каждого из них по лемме 1 получим $\frac{1}{3}4^{n-r-2} - \frac{1}{2}3^{n-r-2} + \frac{1}{6}$ слов. Эта сумма также равна нулю при $n - r \in \{2, 3\}$, так что $n - r \geq 2$. Лемма 5 доказана.

3.3. Число невозможных разностей. В следующей теореме приводится точное значение $\mathcal{N}_n^r$ для всех возможных n и r .

Теорема 1. Пусть $n \geq 2$ и $1 \leq r < n$. Тогда

$$\begin{aligned} \mathcal{N}_n^r = & \frac{1}{7}8^n + \frac{3}{7}4^r \cdot 8^{n-r} - \frac{1}{7}8^r + \frac{1}{14}4^r + \\ & + \left(\frac{6}{35}8^{n-r} + \frac{10}{3}4^{n-r} - \frac{8}{5}3^{n-r} + \frac{2}{21} \right) \left(\frac{1}{14}8^r - \frac{1}{12}4^r - \frac{5}{21} \right). \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Пусть $T_{j_1, \dots, j_s}^{i_1, \dots, i_t}(n, r)$, $t \geq 1$, $s \geq 0$, — множество слов (ω, ω') , $\omega = \omega(\alpha, \beta, \gamma)$, $\omega' = \omega(\alpha', \beta', \gamma')$, $\alpha, \beta, \gamma \in \mathbb{Z}_2^{n-r}$, $\alpha', \beta', \gamma' \in \mathbb{Z}_2^r$, удовлетворяющих шаблону из столбцов $i_1, \dots, i_t \in \{1, \dots, 7\}$ и не удовлетворяющих шаблону из столбцов $j_1, \dots, j_s \in \{1, \dots, 7\}$ табл. 2. Вычислим $\mathcal{N}_n^r$ по формуле

$$\mathcal{N}_n^r = |T^6(n, r)| + |T^7(n, r)| + |T_{6,7}^5(n, r)| + |T_{5,6,7}^{1-4}(n, r)|.$$

1. $|T^6(n, r)|$. По лемме 1 число различных ω -частей у 6.1 и 6.2 равно $2 \cdot 4 \cdot \frac{1}{8-1}(8^{n-r-1} - 1)$. Это выражение равно нулю при $n - r = 1$, поэтому его можно использовать без ограничений. Таким образом,

$$|T^6(n, r)| = 8^r \cdot \frac{8}{7}(8^{n-r-1} - 1) = \frac{1}{7}8^n - \frac{8}{7}8^r.$$

2. $|T^7(n, r)|$. Заметим, что $|T^7(n, r)| = 4^r \cdot 4 \cdot 8^{n-r-1} = \frac{1}{2}4^r \cdot 8^{n-r}$. Осталось найти пересечение $T^7(n, r)$ и $T^6(n, r)$. Их ω' -части пересекаются по $[\gamma_0*]$, а ω -части — по $[.*e11*]$. Таким образом,

$$\begin{aligned} |T^7(n, r)| &= |T^7(n, r)| - |T^7(n, r) \cap T^6(n, r)| = \\ &= \frac{1}{2}4^r \cdot 8^{n-r} - \frac{4^r \cdot 4}{7}(8^{n-r-1} - 1) = \frac{3}{7}4^r \cdot 8^{n-r} + \frac{4}{7}4^r. \end{aligned}$$

Формула верна при всех $r \geq 1$ и $n - r \geq 1$, т. е. без ограничений.

3. $|T_{6,7}^5(n, r)|$. Поскольку ω -части 5.1 и 5.2 не пересекаются ни с 6.1, ни с 6.2, то $T_{6,7}^5(n, r) = T_7^5(n, r)$. При этом $|T^5(n, r)| = 4 \cdot 8^{r-1} \cdot 2 = 8^r$. Найдём $T^5(n, r) \cap T^7(n, r)$: их ω' -части пересекаются по $[\gamma_0*2_4]$ (пересечение γ_0 и d равно 2_4), а ω -части — по $[1*]$. Тем самым

$$\begin{aligned} |T_{6,7}^5(n, r)| &= |T_7^5(n, r)| = |T^5(n, r)| - |T^5(n, r) \cap T^7(n, r)| = \\ &= 8^r - 2 \cdot 4^{r-1} \cdot 1 = 8^r - \frac{1}{2}4^r. \end{aligned}$$

В итоге получаем первую часть формулы для $\mathcal{N}_n^r$:

$$|T^6(n, r)| + |T^7(n, r)| + |T_{6,7}^5(n, r)| = \frac{1}{7}8^n + \frac{3}{7}4^r \cdot 8^{n-r} - \frac{1}{7}8^r + \frac{1}{14}4^r.$$

4. Осталось показать, что $|T_{5,6,7}^{1-4}(n, r)|$ равна произведению скобок в формуле для $\mathcal{N}_n^r$. Обозначим через $P(r)$ число слов, удовлетворяющих метке каждого из столбцов 1–4, т. е. $P(r) = \frac{4}{7}(8^{r-1} - 1)$ по лемме 1. Дополнительных ограничений на r нет, так как $P(1) = 0$. Найдём число $|T_{5,6,7}^{1-4}(n, r)|$ в несколько шагов. Положим $n - r \geq 2$, а случай $r = n - 1$ рассмотрим в конце доказательства.

4.1. $|T^{1-4}(n, r)|$. Применим классификацию из табл. 5 (см. лемму 4):

$$\begin{aligned} |T^{1-4}(n, r)| &= P(r) \left(8 \cdot 4^{n-r-1} + 8 \cdot \frac{1}{5}(8^{n-r-1} - 3^{n-r-1}) + 2 \cdot 3^{n-r-2} + \right. \\ &\quad \left. + 8(4^{n-r-1} - 3^{n-r-1}) + 8 \cdot 2(4^{n-r-2} - 3^{n-r-2}) + 6 \cdot 3^{n-r-1} \right) = \\ &= \frac{1}{5}P(r)(8^{n-r} + 25 \cdot 4^{n-r} - 124 \cdot 3^{n-r-2}). \end{aligned}$$

4.2. $|T_6^{1-4}(n, r)|$. Метки столбцов 1–4 удовлетворяют метке $[.*]$ столбца 6, поэтому применим классификацию пересечений из табл. 6:

$$\begin{aligned} |T_6^{1-4}(n, r)| &= |T^{1-4}(n, r)| - P(r) \left(16 \cdot \frac{2}{3}(4^{n-r-2} - 1) + 8 \cdot 1 + \right. \\ &\quad \left. + 16 \cdot \frac{2}{35}(2 \cdot 8^{n-r-2} - 7 \cdot 3^{n-r-2} + 5) + 22 \cdot \frac{1}{2}(3^{n-r-2} - 1) + \right. \\ &\quad \left. + 6 \cdot \frac{1}{2}(3^{n-r-1} - 1) + 24 \cdot \frac{1}{3}(2 \cdot 4^{n-r-2} - 3^{n-r-1} + 1) \right) = \\ &= P(r) \left(\frac{6}{35}8^{n-r} + \frac{10}{3}4^{n-r} - \frac{8}{5}3^{n-r} + \frac{86}{21} \right). \end{aligned}$$

4.3. $|T_{5,6}^{1-4}(n, r)|$. Метки столбцов 1 и 4 не пересекаются с меткой столбца 5, а метки столбцов 2 и 3 удовлетворяют метке столбца 5. Далее, ω -части $[0*]$ (5.1) и $[1*]$ (5.2) удовлетворяют 2.1 и 3.1. Таким образом,

$$|T_{5,6}^{1-4}(n, r)| = |T^{1-4}(n, r)| - 2 \cdot 2 \cdot P(r) = |T^{1-4}(n, r)| - 4P(r).$$

Более того, шаблоны из столбцов 5 и 6 не пересекаются, поэтому такой способ подсчёта работает и для $|T_{5,6}^{1-4}(n, r)|$:

$$|T_{5,6}^{1-4}(n, r)| = |T_6^{1-4}(n, r)| - 4P(r) = P(r) \left(\frac{6}{35}8^{n-r} + \frac{10}{3}4^{n-r} - \frac{8}{5}3^{n-r} + \frac{2}{21} \right).$$

4.4. $|T_{5,6,7}^{1-4}(n, r)|$. Пусть $|T_{5,6}^{1-4}(n, r)| = P(r)Q(n - r)$, где

$$Q(n - r) = \frac{6}{35}8^{n-r} + \frac{10}{3}4^{n-r} - \frac{8}{5}3^{n-r} + \frac{2}{21}.$$

Метка $[\gamma_0*]$ столбца 7 имеет пересечения типа $[\gamma_0*2_400*]$ с метками любого из столбцов 1–4, что даёт $\frac{2}{3}(4^{r-1} - 1)$ слов (лемма 1).

Далее покажем, что $(\omega, \omega') \in T_{5,6}^{1-4}(n, r)$ тогда и только тогда, когда $(\omega(\alpha, \beta, \bar{\gamma}), \omega') \in T_{5,6}^{1-4}(n, r)$. Действительно, ω -части шаблонов из столбцов 1–6 замкнуты относительно $\bar{\gamma}$ -эквивалентности (лемма 3), а значит, замкнуты и их объединения, пересечения и разности. Пусть $(\omega, \omega') \in T_{5,6}^{1-4}(n, r)$. Тогда одно из слов ω и $\omega(\alpha, \beta, \bar{\gamma})$ будет удовлетворять ω -части $[.*d]$ 7.1, а второе — нет. Действительно, инвертировав γ -бит у символа, удовлетворяющего e , получим символ, удовлетворяющий d (и наоборот). Таким образом, среди всех слов из $T_{5,6}^{1-4}(n, r)$, ω' -части которых удовлетворяют ω' -части 7.1, ω -части 7.1 удовлетворяет ровно $\frac{1}{2}Q(n - r)$ ω -частей слов. Следовательно,

$$\begin{aligned} |T_{5,6,7}^{1-4}(n, r)| &= P(r)Q(n - r) - \frac{2}{3}(4^{r-1} - 1) \cdot \frac{1}{2}Q(n - r) = \\ &= \left(\frac{4}{7}(8^{r-1} - 1) - \frac{1}{3}(4^{r-1} - 1) \right) Q(n - r) = \\ &= \left(\frac{1}{14}8^r - \frac{1}{12}4^r - \frac{5}{21} \right) Q(n - r). \end{aligned}$$

Тем самым получена искомая формула для $\mathcal{N}_n^r$.

Осталось разобрать случай $n - r = 1$, от которого зависит только $|T_{5,6,7}^{1-4}(n, r)|$. Отметим, что в этом случае нет слов, удовлетворяющих шаблонам из столбца 6, т. е. достаточно найти $|T_5^{1-4}(n, n - 1)|$ и далее воспользоваться п. 4.4 для нахождения числа $|T_{5,6,7}^{1-4}(n, n - 1)|$, которое зависит только от мощности $T_{5,6}^{1-4}(n, n - 1) = T_5^{1-4}(n, n - 1)$. Нетрудно видеть, что из ω -частей столбца 1 подходят $[0_1]$, $[2_3]$ и $[4_5]$ (6 слов), а также $[2_3]$ из столбца 2 (2 слова) и $[4_5]$ из столбца 3 (2 слова), исключаем $[0_1]$ из столбцов 2 и 3, потому что они удовлетворяют 5.1 или 5.2. Итого,

$$|T_5^{1-4}(n, n - 1)| = 6P(n - 1) + 2P(n - 1) + 2P(n - 1) = 10P(n - 1),$$

что также совпадает с $|T_{5,6}^{1-4}(n, n - 1)|$. Однако

$$\begin{aligned} Q(1) &= \frac{6}{35} \cdot 8 + \frac{10}{3} \cdot 4 - \frac{8}{5} \cdot 3 + \frac{2}{21} = \frac{48 \cdot 3 + 40 \cdot 35 - 24 \cdot 21 + 10}{3 \cdot 5 \cdot 7} = \\ &= \frac{144 + 1400 - 504 + 10}{105} = \frac{1050}{105} = 10, \end{aligned}$$

так что формула $|T_{5,6}^{1-4}(n, r)| = P(r)Q(n-r)$ справедлива и при $n-r=1$, а значит, 4.4 даст то же самое $|T_{5,6,7}^{1-4}(n, r)|$. Теорема 1 доказана.

Зафиксировав r или $n-r$, можно получить более простое выражение для $\mathcal{N}_n^r$. Напомним также, что $\mathcal{N}_n^1 = \frac{5}{14}8^n - \frac{6}{7}$ (см. (1)).

Следствие 1. *Имеют место следующие равенства:*

$$\begin{aligned}\mathcal{N}_n^2 &= \frac{289}{1120}8^n + \frac{5}{8}4^n - \frac{8}{15}3^n - \frac{54}{7}, \quad n \geq 3, \\ \mathcal{N}_n^3 &= \frac{1853}{8960}8^n + \frac{155}{96}4^n - \frac{248}{135}3^n - \frac{1378}{21}, \quad n \geq 4, \\ \mathcal{N}_n^{n-3} &= \frac{5}{28}8^n + \frac{99}{32}4^n - \frac{430}{7}, \quad n \geq 4, \\ \mathcal{N}_n^{n-2} &= \frac{11}{56}8^n + \frac{35}{24}4^n - \frac{250}{21}, \quad n \geq 3, \\ \mathcal{N}_n^{n-1} &= \frac{3}{14}8^n + \frac{2}{3}4^n - \frac{50}{21}, \quad n \geq 2.\end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Заметим, что

$$\frac{1}{14}8^r - \frac{1}{12}4^r - \frac{5}{21} = \begin{cases} 3 & \text{при } r = 2, \\ 31 & \text{при } r = 3, \end{cases}$$

поэтому

$$\begin{aligned}\mathcal{N}_n^2 &= \left(\frac{1}{7} + \frac{3}{7 \cdot 4} + \frac{9}{7 \cdot 4 \cdot 40}\right)8^n + \frac{5}{8}4^n - \frac{8}{15}3^n - \\ &\quad - \frac{8^2}{7} + \frac{4^2}{7 \cdot 2} + \frac{2}{7} = \frac{289}{1120}8^n + \frac{5}{8}4^n - \frac{8}{15}3^n - \frac{54}{7}, \\ \mathcal{N}_n^3 &= \left(\frac{1}{7} + \frac{3}{7 \cdot 8} + \frac{6 \cdot 31}{5 \cdot 7 \cdot 8^3}\right)8^n + \frac{10 \cdot 31}{3 \cdot 4^3}4^n - \frac{8 \cdot 31}{5 \cdot 27}3^n - \\ &\quad - \frac{8^3}{7} + \frac{4^3}{7 \cdot 2} + \frac{62}{21} = \frac{1853}{8960}8^n + \frac{155}{96}4^n - \frac{248}{135}3^n - \frac{1378}{21}.\end{aligned}$$

Аналогично

$$\frac{6}{35}8^{n-r} + \frac{10}{3}4^{n-r} - \frac{8}{5}3^{n-r} + \frac{2}{21} = \begin{cases} 2 \cdot 3 \cdot 43 = 258 & \text{при } r = n-3, \\ 50 & \text{при } r = n-2, \\ 10 & \text{при } r = n-1, \end{cases}$$

поэтому

$$\begin{aligned}\mathcal{N}_n^{n-3} &= \left(\frac{1}{7} - \frac{1}{7 \cdot 8^3} + \frac{129}{7 \cdot 8^3}\right)8^n + \left(\frac{3 \cdot 8}{7} + \frac{1}{14 \cdot 4^3} - \frac{43}{2 \cdot 4^3}\right)4^n - \frac{430}{7}, \\ \mathcal{N}_n^{n-2} &= \left(\frac{1}{7} - \frac{1}{7 \cdot 8^2} + \frac{25}{7 \cdot 8^2}\right)8^n + \left(\frac{3 \cdot 4}{7} + \frac{1}{14 \cdot 16} - \frac{25}{6 \cdot 16}\right)4^n - \frac{250}{21},\end{aligned}$$

$$\mathcal{N}_n^{n-1} = \left(\frac{1}{7} - \frac{1}{7 \cdot 8} + \frac{5}{7 \cdot 8}\right) 8^n + \left(\frac{6}{7} + \frac{1}{14 \cdot 4} - \frac{5}{6 \cdot 4}\right) 4^n - \frac{50}{21}.$$

Следствие 1 доказано.

Значения $\mathcal{N}_n^r$ при $n \leq 9$ представлены в табл. 7, где также приведены доли невозможных разностей по отношению ко всем 8^n разностям.

Таблица 7

Значения $\mathcal{N}_n^r$ при $2 \leq n \leq 9$

n	r	$\mathcal{N}_n^r$	$\mathcal{N}_n^r/8^n, \%$	n	r	$\mathcal{N}_n^r$	$\mathcal{N}_n^r/8^n, \%$
2	1	22	34,37500	7	4	425118	20,27121
3	1	182	35,54688		5	435822	20,78161
	2	150	29,29688		6	460310	21,94929
4	1	1462	35,69336	8	1	5991862	35,71428
	2	1166	28,46680		2	4366574	26,02681
	3	1046	25,53711		3	3563358	21,23927
5	1	11702	35,71167		4	3232014	19,26430
	2	8958	27,33765		5	3198622	19,06527
	3	7918	24,16382		6	3391086	20,21245
	4	7702	23,50464		7	3638806	21,68897
6	1	93622	35,71396	9	1	47934902	35,71429
	2	69806	26,62888		2	34786302	25,91781
	3	59422	22,66769		3	28144334	20,96916
	4	57454	21,91696		4	25110494	18,70878
	5	58902	22,46933		5	24182542	18,01740
7	1	748982	35,71424		6	24778398	18,46135
	2	550206	26,23587		7	26746478	19,92768
	3	456078	21,74749		8	28935702	21,55878

4. Свойства чисел невозможных разностей

В этом разделе найдём оценки для чисел $\mathcal{N}_n^r$ и проведём их сравнительный анализ при фиксированном n . П. 4.1 содержит нижнюю оценку, асимптотически точную при $n, n-r \rightarrow \infty$. В п. 4.2 числа $\mathcal{N}_n^1, \dots, \mathcal{N}_n^{n-1}$ упорядочены по величине. Как следствие, получен ряд точных оценок для $\mathcal{N}_n^r$ при некоторых ограничениях на r . Результаты также показывают примерное отношение числа невозможных разностей к числу всех разностей. Например, в табл. 8 приведены такие отношения при самом востребованном с точки зрения практических приложений значении $n = 32$.

4.1. Нижняя оценка $\mathcal{N}_n^r$. Для доказательства дальнейших утверждений преобразуем формулу из теоремы 1.

Таблица 8

Отношение $\mathcal{N}_{32}^r/8^{32}$ при $1 \leq r < 32$

r	$\mathcal{N}_{32}^r/8^{32}, \%$	r	$\mathcal{N}_{32}^r/8^{32}, \%$	r	$\mathcal{N}_{32}^r/8^{32}, \%$
1	35,71429	12	15,52034	23	15,55504
2	25,80357	13	15,51531	24	15,59874
3	20,68080	14	15,51282	25	15,68429
4	18,09849	15	15,51165	26	15,85039
5	16,80472	16	15,51120	27	16,16909
6	16,15751	17	15,51124	28	16,76897
7	15,83386	18	15,51180	29	17,85714
8	15,67204	19	15,51316	30	19,64286
9	15,59112	20	15,51597	31	21,42857
10	15,55067	21	15,52161		
11	15,53044	22	15,53284		

Следствие 2. Пусть $n \geq 2$ и $1 \leq r < n$. Тогда

$$\begin{aligned} \mathcal{N}_n^r = & \frac{38}{245}8^n - \frac{5}{18}4^n + \frac{5}{21}8^r \cdot 4^{n-r} + \frac{29}{70}4^r \cdot 8^{n-r} - \frac{4}{35}8^r \cdot 3^{n-r} + \\ & + \frac{2}{15}4^r \cdot 3^{n-r} - \frac{20}{147}8^r + \frac{4}{63}4^r - \frac{6}{147}8^{n-r} - \frac{50}{63}4^{n-r} + \frac{8}{21}3^{n-r} - \frac{10}{441}. \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Раскрывая скобки в формуле для $\mathcal{N}_n^r$ из теоремы 1, получаем

$$\begin{aligned} & \left(\frac{6}{35}8^{n-r} + \frac{10}{3}4^{n-r} - \frac{8}{5}3^{n-r} + \frac{2}{21} \right) \left(\frac{1}{14}8^r - \frac{1}{12}4^r - \frac{5}{21} \right) = \\ & = \frac{3}{35 \cdot 7}8^n + \frac{5}{3 \cdot 7}8^r \cdot 4^{n-r} - \frac{4}{5 \cdot 7}8^r \cdot 3^{n-r} + \frac{1}{21 \cdot 7}8^r - \\ & - \frac{1}{35 \cdot 2}4^r \cdot 8^{n-r} - \frac{5}{3 \cdot 6}4^n + \frac{2}{5 \cdot 3}4^r \cdot 3^{n-r} - \frac{1}{21 \cdot 6}4^r - \\ & - \frac{6}{7 \cdot 21}8^{n-r} - \frac{10 \cdot 5}{3 \cdot 21}4^{n-r} + \frac{8}{21}3^{n-r} - \frac{10}{21 \cdot 21}, \end{aligned}$$

поэтому

$$\begin{aligned} \mathcal{N}_n^r = & \frac{35+3}{35 \cdot 7}8^n - \frac{5}{6 \cdot 3}4^n + \frac{5}{3 \cdot 7}8^r \cdot 4^{n-r} + \frac{30-1}{2 \cdot 35}4^r \cdot 8^{n-r} - \\ & - \frac{4}{5 \cdot 7}8^r \cdot 3^{n-r} + \frac{2}{15}4^r \cdot 3^{n-r} - \frac{21-1}{21 \cdot 7}8^r + \frac{9-1}{2 \cdot 7 \cdot 9}4^r - \\ & - \frac{6}{7 \cdot 21}8^{n-r} - \frac{10 \cdot 5}{3 \cdot 21}4^{n-r} + \frac{8}{21}3^{n-r} - \frac{10}{21 \cdot 21}. \end{aligned}$$

Следствие 2 доказано.

Используя полученную формулу, несложно доказать следующую нижнюю оценку для чисел $\mathcal{N}_n^r$.

Следствие 3. Пусть $n \geq 2$ и $1 \leq r < n$. Тогда

$$\mathcal{N}_n^r > \frac{38}{245} 8^n.$$

ДОКАЗАТЕЛЬСТВО. Ясно, что $\mathcal{N}_n^{n-1}, \mathcal{N}_n^{n-2} > \frac{38}{245} 8^n$ (см. следствие 1). Далее положим $n - r \geq 3$ и воспользуемся следствием 2:

$$\begin{aligned} \mathcal{N}_n^r &= \frac{38}{245} 8^n - \frac{5}{18} 4^n + \frac{5}{21} 8^r \cdot 4^{n-r} + \frac{29}{70} 4^r \cdot 8^{n-r} - \frac{4}{35} 8^r \cdot 3^{n-r} + \\ &+ \frac{2}{15} 4^r \cdot 3^{n-r} - \frac{20}{147} 8^r + \frac{4}{63} 4^r - \frac{6}{147} 8^{n-r} - \frac{50}{63} 4^{n-r} + \frac{8}{21} 3^{n-r} - \frac{10}{441}. \end{aligned}$$

Докажем оценку в три шага. Во-первых, отметим, что

$$\frac{5}{21} 8^r \cdot 4^{n-r} > \frac{4}{35} 8^r \cdot 3^{n-r} + \frac{20}{147} 8^r,$$

поскольку

$$\frac{4}{35} 8^r \cdot 3^{n-r} + \frac{20}{147} \cdot \frac{4^{n-r}}{4^{n-r}} 8^r \leq \left(\frac{4}{35} + \frac{20}{4^3 \cdot 147} \right) 8^r \cdot 4^{n-r} < \frac{5}{21} 8^r \cdot 4^{n-r}.$$

Во-вторых,

$$\frac{29}{70} 4^r \cdot 8^{n-r} > \frac{5}{18} 4^n + \frac{6}{147} 8^{n-r} + \frac{50}{63} 4^{n-r},$$

так как

$$\begin{aligned} \frac{5}{18} \cdot \frac{8^{n-r}}{2^{n-r}} 4^r + \frac{6}{147} \cdot \frac{4^r}{4^r} 8^{n-r} + \frac{50}{63} \cdot \frac{4^r \cdot 8^{n-r}}{4^r \cdot 2^{n-r}} &\leq \\ &\leq \left(\frac{5}{8 \cdot 18} + \frac{6}{4 \cdot 147} + \frac{50}{2^5 \cdot 63} \right) 4^r \cdot 8^{n-r} = \\ &= \left(\frac{5 \cdot 2 \cdot 49 + 8 \cdot 3 \cdot 6 + 7 \cdot 50}{32 \cdot 9 \cdot 49} \right) 4^r \cdot 8^{n-r} = \\ &= \frac{984}{14112} 4^r \cdot 8^{n-r} < \frac{29}{70} 4^r \cdot 8^{n-r}. \end{aligned}$$

В-третьих,

$$\frac{8}{21} 3^{n-r} > \frac{10}{441}.$$

Суммируя сказанное, получаем требуемое неравенство для числа $\mathcal{N}_n^r$. Утверждение 2 доказано.

Доказанная оценка лучше, чем $\mathcal{N}_n^r \geq \frac{1}{7} 8^n - \frac{1}{7} 8^r$, которая была предложена в [19]. Более того, она асимптотически точна при удалении от крайних значений r . Непосредственно из следствия 2 вытекает

Следствие 4. Справедливо равенство $\lim_{\substack{r \rightarrow \infty \\ n-r \rightarrow \infty}} \frac{\mathcal{N}_n^r}{8^n} = \frac{38}{245}$, т. е.

$$\lim_{\substack{r \rightarrow \infty \\ n-r \rightarrow \infty}} \frac{\mathcal{N}_n^r}{\frac{38}{245} 8^n} = 1.$$

Отметим также, что $\frac{38}{245} \approx 15,51020\%$. В то же время доля невозможных разностей по модулю 2^n для преобразования $(x, y) \mapsto x \oplus y$ примерно равна $\frac{4}{7}$ (см. [15]), что составляет около $57,14286\%$. Следовательно, добавление циклического сдвига с далёким от крайних значением в несколько раз снижает число невозможных разностей.

4.2. Соотношения чисел $\mathcal{N}_n^r$ и точные оценки. Докажем неравенства для полученных в следствии 1 формул.

Лемма 6. При $n \geq 7$ имеем $\mathcal{N}_n^1 > \mathcal{N}_n^2 > \mathcal{N}_n^3$ и $\mathcal{N}_n^{n-3} < \mathcal{N}_n^{n-2} < \mathcal{N}_n^{n-1}$.

ДОКАЗАТЕЛЬСТВО. Пользуясь формулами из следствия 1, получаем

$$\frac{5}{14} 8^n > \frac{289}{1120} 8^n > \frac{1853}{8960} 8^n, \quad \frac{5}{28} 8^n < \frac{11}{56} 8^n < \frac{3}{14} 8^n.$$

Несложно проверить, что при $n \geq 7$ другие слагаемые не нарушают этих неравенств. Лемма 6 доказана.

Теперь можем упорядочить числа $\mathcal{N}_n^1, \dots, \mathcal{N}_n^{n-1}$.

Теорема 2. Если $n \geq 2$, $r = n/2 + 1$ при $n \in \{4, 6, 8, 10, 12\}$ и $r = \lceil n/2 \rceil$ иначе, то

$$\mathcal{N}_n^1 > \mathcal{N}_n^2 > \dots > \mathcal{N}_n^r < \mathcal{N}_n^{r+1} < \dots < \mathcal{N}_n^{n-1}.$$

ДОКАЗАТЕЛЬСТВО. Из табл. 7 вытекает утверждение теоремы при $n \leq 6$. Далее пусть $n \geq 7$. Положим $\Delta_{n,r} = \mathcal{N}_n^r - \mathcal{N}_n^{r+1}$ для любого r , $1 \leq r \leq n-2$. Для доказательства необходимо показать, что

- 1) $\Delta_{n,r} > 0$ при $r < n/2$,
- 2) $\Delta_{n,r} < 0$ при $r > n/2$,
- 3) $\Delta_{n,n/2} < 0$ для чётного $n \geq 14$,
- 4) $\Delta_{n,n/2} > 0$ для $n \in \{8, 10, 12\}$.

Из леммы 6 следует, что $\Delta_{n,1}$ и $\Delta_{n,2}$ положительны, а $\Delta_{n,n-3}$ и $\Delta_{n,n-2}$ отрицательны. Таким образом, можем полагать, что $3 \leq r \leq n-4$.

Все значения $\mathcal{N}_n^r$ и $\mathcal{N}_n^{r+1}$ могут быть вычислены с помощью следствия 2:

$$\begin{aligned} \mathcal{N}_n^r = & \frac{38}{245} 8^n - \frac{5}{18} 4^n + \frac{5}{21} 8^r \cdot 4^{n-r} + \frac{29}{70} 4^r \cdot 8^{n-r} - \frac{4}{35} 8^r \cdot 3^{n-r} + \\ & + \frac{2}{15} 4^r \cdot 3^{n-r} - \frac{20}{147} 8^r + \frac{4}{63} 4^r - \frac{6}{147} 8^{n-r} - \frac{50}{63} 4^{n-r} + \frac{8}{21} 3^{n-r} - \frac{10}{441}. \end{aligned}$$

Отметим, что для любых чисел a и b справедливо равенство

$$a^r b^{n-r} - a^{r+1} b^{n-(r+1)} = a^r b^{n-r-1} (b - a),$$

поэтому

$$\begin{aligned} \Delta_{n,r} = & -\frac{4 \cdot 5}{21} 8^r \cdot 4^{n-r-1} + \frac{4 \cdot 29}{70} 4^r \cdot 8^{n-r-1} + \\ & + \frac{5 \cdot 4}{35} 8^r \cdot 3^{n-r-1} - \frac{2}{15} 4^r \cdot 3^{n-r-1} + \frac{7 \cdot 20}{147} 8^r - \frac{3 \cdot 4}{63} 4^r - \\ & - \frac{7 \cdot 6}{147} 8^{n-r-1} - \frac{3 \cdot 50}{63} 4^{n-r-1} + \frac{2 \cdot 8}{21} 3^{n-r-1}. \end{aligned}$$

Следовательно,

$$\begin{aligned} \frac{21}{8^n} \Delta_{n,r} = & -5 \cdot 8^{-n} \cdot 8^r \cdot 4^{n-r} + \frac{87}{20} 8^{-n} \cdot 4^r \cdot 8^{n-r} + 4 \cdot 8^{-n} \cdot 8^r \cdot 3^{n-r} + \\ & + T_{n,r} - S_{n,r} = \frac{87}{20} 2^{-r} - S_{n,r} - \left(5 \cdot 2^{r-n} - T_{n,r} - 4 \left(\frac{8}{3} \right)^{r-n} \right), \quad (2) \end{aligned}$$

где

$$\begin{aligned} T_{n,r} = & 20 \cdot 8^{-n} \cdot 8^r - 4 \cdot 8^{-n} \cdot 4^r = \frac{20}{4^{n-r}} 2^{r-n} - \frac{4}{2^r \cdot 4^{n-r}} 2^{r-n}, \\ S_{n,r} = & \frac{14}{15} 8^{-n} \cdot 4^r \cdot 3^{n-r} + 6 \cdot 8^{-n} \cdot 8^{n-r-1} + \\ & + 50 \cdot 8^{-n} \cdot 4^{n-r-1} - 16 \cdot 8^{-n} \cdot 3^{n-r-1} = \\ = & \frac{14}{15} \left(\frac{3}{8} \right)^{n-r} 2^{-r} + \frac{3}{4^{r+1}} 2^{-r} + \frac{25}{4^r \cdot 2^{n-r+1}} 2^{-r} - \frac{16}{3 \cdot 4^r} \left(\frac{3}{8} \right)^{n-r} 2^{-r}. \end{aligned}$$

В то же время $r \geq 3$ и $n - r \geq 4$, поэтому

$$\begin{aligned} 0 < T_{n,r} & < \frac{20}{4^4} 2^{r-n} = \frac{5}{64} 2^{r-n}, \\ 0 < S_{n,r} & < \frac{14}{15} \left(\frac{3}{8} \right)^4 2^{-r} + \frac{3}{4^4} 2^{-r} + \frac{25}{4^3 \cdot 2^5} 2^{-r} = \\ & = \frac{7 \cdot 27 + 3 \cdot 5 \cdot 2^3 + 25 \cdot 5}{5 \cdot 2^{11}} 2^{-r} = \frac{189 + 120 + 125}{5 \cdot 2^{11}} 2^{-r} = \frac{217}{5120} 2^{-r}. \end{aligned}$$

Для удобства можем считать, что

$$0 < T_{n,r} < \frac{1}{10} 2^{r-n} < \frac{13}{40} 2^{r-n}, \quad (3)$$

$$0 < S_{n,r} < \frac{1}{20} 2^{-r}. \quad (4)$$

Будем использовать эти неравенства совместно с (2) для $\Delta'_{n,r} = \frac{21}{8^n} \Delta_{n,r}$. Отметим, что $\Delta_{n,r}$ и $\Delta'_{n,r}$ имеют одинаковый знак.

1. Докажем, что $\Delta'_{n,r} > 0$ при $r < n/2$. В силу (3) и (4) достаточно проверить, что $5 \cdot 2^{r-n} \leq \frac{87-1}{20} 2^{-r}$. Действительно, имеем $n-r > n/2$, или $n-r \geq r+1$, что влечёт

$$5 \cdot 2^{r-n} \leq 5 \cdot 2^{-r-1} = \frac{5}{2} 2^{-r} = \frac{50}{20} 2^{-r} < \frac{86}{20} 2^{-r}.$$

2. Докажем, что $\Delta'_{n,r} < 0$ при $r > n/2$. В силу (4) достаточно показать, что

$$5 \cdot 2^{r-n} - T_{n,r} - 4 \left(\frac{8}{3} \right)^{r-n} \geq \frac{87}{20} 2^{-r}. \quad (5)$$

Аналогично п. 1 справедливо $r \geq n-r+1$. Это означает, что

$$\frac{87}{20} 2^{-r} \leq \frac{87}{20} 2^{r-n-1} = \frac{87}{40} 2^{r-n}.$$

Таким образом, (3) обеспечивает оценку

$$5 \cdot 2^{r-n} - T_{n,r} - \frac{87}{20} 2^{-r} > \frac{200 - 13 - 87}{40} 2^{r-n} = \frac{5}{2} 2^{r-n}.$$

Осталось заметить, что $\frac{5}{2} 2^{r-n} \geq 4 \left(\frac{8}{3} \right)^{r-n}$. Это эквивалентно неравенству $\frac{5}{8} 8^{n-r} \geq 3^{n-r} \cdot 2^{n-r}$, которое имеет место, поскольку $5 \cdot 8^{n-r-1} \geq 6^{n-r}$ при $n-r \geq 2$.

3. Докажем, что $\Delta'_{n,n/2} < 0$ для чётных $n \geq 14$. Аналогично п. 2, покажем, что справедливо неравенство (5). Поскольку $r = n-r = n/2$, оно эквивалентно

$$\left(5 - \frac{87}{20} \right) \cdot 2^{-n/2} - T_{n,r} \geq 4 \left(\frac{8}{3} \right)^{-n/2}.$$

В то же время в силу (3) достаточно доказать, что

$$\frac{11}{20} 2^{-n/2} \geq 4 \left(\frac{8}{3} \right)^{-n/2}.$$

Это эквивалентно неравенству $11 \cdot 4^{n/2-2} \geq 5 \cdot 3^{n/2}$, которое имеет место при $n/2 \geq 7$. Действительно, $11 \cdot 4^5 = 11264$ и $5 \cdot 3^7 = 10935$.

Таблица 9

Значения $\mathcal{N}_n^{n/2}$ и $\mathcal{N}_n^{n/2+1}$ при чётных n , $4 \leq n \leq 12$

n	$\mathcal{N}_n^{n/2}$	$\mathcal{N}_n^{n/2}/8^n, \%$	$\mathcal{N}_n^{n/2+1}$	$\mathcal{N}_n^{n/2+1}/8^n, \%$
4	1166	28,46680%	1046	25,53711%
6	59422	22,66769%	57454	21,91696%
8	3232014	19,26430%	3198622	19,06527%
10	187255262	17,43951%	186758926	17,39328%
12	11332868174	16,49149%	11329597918	16,48673%

4. Табл. 9 показывает, что $\mathcal{N}_n^{n/2} > \mathcal{N}_n^{n/2+1}$ при $n \in \{8, 10, 12\}$. Теорема 2 доказана.

Прямым следствием теоремы 2 является точная нижняя оценка для числа $\mathcal{N}_n^r$.

Следствие 5. При $1 \leq r < n$ справедливо неравенство

$$\mathcal{N}_n^r \geq \begin{cases} \mathcal{N}_n^{n/2+1}, & \text{если } n \in \{4, 6, 8, 10, 12\}, \\ \mathcal{N}_n^{\lceil n/2 \rceil} & \text{иначе.} \end{cases}$$

Рассмотрим верхние оценки чисел $\mathcal{N}_n^r$. Согласно (1)

$$\mathcal{N}_n^r < \mathcal{N}_n^1, \quad 2 \leq r < n.$$

Однако $\mathcal{N}_n^1$ заметно больше всех других $\mathcal{N}_n^2, \dots, \mathcal{N}_n^{n-1}$. При этом теорема 2 позволяет получить другие оценки при дополнительных ограничениях на r .

Следствие 6. При $3 \leq r < n$

$$\mathcal{N}_n^r \leq \mathcal{N}_n^{n-1} = \frac{3}{14}8^n + \frac{2}{3}4^n - \frac{50}{21} < \mathcal{N}_n^2 < \mathcal{N}_n^1.$$

ДОКАЗАТЕЛЬСТВО. Из следствия 1 вытекает, что $\mathcal{N}_n^3 < \mathcal{N}_n^{n-1} < \mathcal{N}_n^2$. Действительно, $\frac{1853}{8960} < \frac{3}{14} < \frac{289}{1120}$, остальные слагаемые не нарушат это неравенство (при малых значениях n можно воспользоваться табл. 7). Для $4 \leq r \leq n-2$ неравенства следуют из теоремы 2. Следствие 6 доказано.

Рассмотренные оценки можно назвать точными, так как они представляют собой одно из чисел $\mathcal{N}_n^1, \dots, \mathcal{N}_n^{n-1}$.

5. Невозможные разности с точностью до симметрий

Наиболее многочисленны в табл. 2 шаблоны столбцов 1–4. При этом согласно доказательству теоремы 1 и следствию 4 доля слов, удовлетворяющих шаблону столбцов 1–4 и не удовлетворяющих шаблону столбцов 5–7, составляет $\frac{6}{35 \cdot 14} \cdot \frac{245}{38} = \frac{3}{38}$ при $r, n-r \rightarrow \infty$. Таким образом, эти столбцы нельзя игнорировать. Однако можно сократить число шаблонов за счёт преобразований аргументов, сохраняющих значение adr^{XR} .

Через $\mathcal{S}$ обозначим множество всех композиций преобразований

- $(\alpha, \beta, \gamma) \mapsto (\beta, \alpha, \gamma)$,
- $(\alpha, \beta, \gamma) \mapsto (-\alpha, \beta, \gamma)$, $(\alpha, \beta, \gamma) \mapsto (\alpha, -\beta, \gamma)$, $(\alpha, \beta, \gamma) \mapsto (\alpha, \beta, -\gamma)$,

где $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$.

Отметим, что $\mathcal{S}$ образует группу относительно композиции преобразований. Известно, что перечисленные преобразования сохраняют значение adr^{XR} (см. [19, теорема 5]). Для множества $V \subseteq (\mathbb{Z}_2^n)^3$ положим $\mathcal{S}(V) = \{s(v) \mid s \in \mathcal{S}, v \in V\}$.

Таблица 10

Невозможные разности с точностью
до преобразований из $\mathcal{S}$

№	ω	ω'	№	ω	ω'
1	$[\alpha_0*]$	$[.*d00*]$	6	$[0\hat{0}*7\gamma_1*1_7]$	$[.*d00*]$
2	$[0\hat{0}*]$	$[.*d00*]$	7	$[12_4*0_6\gamma_0*]$	$[\gamma_0*2_400*]$
3	$[0\hat{0}*1.*]$	$[.*d00*]$	8	$[.*d]$	$[\gamma_0*]$
4	$[0\hat{0}*2\alpha_0*]$	$[.*d00*]$	9	$[0*]$	$[.*d]$
5	$[0\hat{0}*7]$	$[.*d00*]$	10	$[.*d00*]$	$[.*]$

Теорема 3. Пусть множество $I \subseteq (\mathbb{Z}_2^n)^3$ содержит все тройки $((\alpha', \alpha), (\beta', \beta), (\gamma, \gamma'))$, где $\alpha, \beta, \gamma \in \mathbb{Z}_2^{n-r}$, $\alpha', \beta', \gamma' \in \mathbb{Z}_2^r$, такие, что $\omega = \omega(\alpha, \beta, \gamma)$ и $\omega' = \omega(\alpha', \beta', \gamma')$ удовлетворяют некоторой паре из табл. 10. Для векторов $x, y, z \in \mathbb{Z}_2^n$ имеет место $\text{adr}^{\text{XR}}(x, y \xrightarrow{r} z) = 0$ тогда и только тогда, когда $(x, y, z) \in \mathcal{S}(I)$.

ДОКАЗАТЕЛЬСТВО. Для шаблона ξ через $\xi^{-\alpha}$ обозначим множество шаблонов таких, что $\omega(\alpha, \beta, \gamma)$ удовлетворяет ξ тогда и только тогда, когда $\omega(-\alpha, \beta, \gamma)$ удовлетворяет некоторому шаблону из $\xi^{-\alpha}$. Аналогично определим $\xi^{-\gamma}$. Напомним, что

$$-(\alpha', \alpha) = \begin{cases} (\bar{\alpha}', -\alpha), & \text{если } \alpha \neq 0, \\ (-\alpha', 0) & \text{иначе,} \end{cases}$$

$$-0 = 0, \quad -(\alpha_1, \dots, \alpha_k, 1, 0, \dots, 0) = (\bar{\alpha}_1, \dots, \bar{\alpha}_k, 1, 0, \dots, 0),$$

где $k \in \{0, \dots, n-r-1\}$ можно подобрать для любого $\alpha \neq 0$. Другими словами, чтобы найти $\xi^{-\alpha}$ для некоторого ξ , сначала пересекаем ξ с шаблоном $[.*\alpha_1\alpha_0*]$, при необходимости разделив ξ на несколько подшаблонов, а затем к части ξ , соответствующей $.*$ в $[.*\alpha_1\alpha_0*]$, применяем преобразование $\bar{\alpha}$. Если ξ имеет непустое пересечение с $[\alpha_0*]$ (случай $\alpha = 0$), то оно тоже будет частью $\xi^{-\alpha}$. Например,

$$[.*e11*]^{-\alpha} = [.*e11*], \quad [.*d00*]^{-\alpha} = [.*d00*], \quad (6)$$

так как при $\alpha \neq 0$ будут инвертированы биты внутри $.*$, а при $\alpha = 0$ изменений не будет.

Начнём с преобразования шаблонов столбцов 2–4 в шаблоны из столбцов 1, 5 и 6, используя преобразование $-(\alpha', \alpha)$, а также меняя местами (α', α) и (β', β) . Обратим внимание, что ω -части из столбцов 1–6 замкнуты относительно $\bar{\gamma}$ -эквивалентности, при этом применяемые преобразования не зависят от γ . Таким образом, на данном этапе достаточно рассматривать только шаблоны из табл. 4 (см. лемму 3).

Столбец 4. Таким шаблонам не удовлетворяют слова с $\alpha = 0$, так как наиболее значимый символ в ω -части всегда $6 = (1, 1, 0)$. Таким образом, $-(\alpha', \alpha) = (\bar{\alpha}', -\alpha)$ и $\omega(\bar{\alpha}', \beta', \gamma')$ будет соответствовать метке столбца 2. Пересечём шаблоны с $[.*\alpha_1\alpha_0*]$. Далее будем часто использовать табл. 3 (см. утверждение 2).

4.1	$[\widehat{66}*7.*]$	4.2	$[\widehat{66}*1\gamma_1*1_7]$
4.1a	$[\widehat{66}*7.*\alpha_1\alpha_0*]$	4.2a	$[\widehat{66}*1\gamma_1*7]$
4.1b	$[\widehat{66}*7\alpha_0*]$	4.2b	$[\widehat{66}*1\gamma_1*5_71_3*1]$
		4.2c	$[\widehat{66}*11_3*1]$

Шаблон $4.1a^{-\alpha} = [2\widehat{2}*3.*\alpha_1\alpha_0*]$ удовлетворяет 2.3. Шаблон $4.1b^{-\alpha} = [2\widehat{2}*7\alpha_0*]$ удовлетворяет $[2\widehat{2}*\alpha_0*]$ (7 удовлетворяет $\widehat{2}$ согласно табл. 3). Значит, по лемме 2 он удовлетворяет одному из шаблонов столбца 2. Аналогично $4.2a^{-\alpha}$ удовлетворяет $[2\widehat{2}*5\gamma_1*7]$, а значит, и 2.5; $4.2b^{-\alpha} = [2\widehat{2}*5\gamma_1*5_71_3*1]$ также удовлетворяет 2.5. Поскольку 4.2c удовлетворяет $[.*e11*]$, в силу (6) все слова, удовлетворяющие $4.2c^{-\alpha}$, также будут удовлетворять $[.*e11*]$, т. е. 6.2 (с учётом и ω' -части).

Столбец 3. Здесь $\alpha = 0$ могут иметь только слова, удовлетворяющие $[0\beta_1*]$ (3.1), ω -части которых удовлетворяют $[00_1*]$. Такие слова удовлетворяют 5.1 (ω' -часть столбца 4 удовлетворяет $[.*d]$), 6.1 или 6.2.

Пусть $\alpha \neq 0$. Таким образом, $\omega(\bar{\alpha}', \beta', \gamma')$ будет удовлетворять метке столбца 1. Пересечём шаблоны с $[.*\alpha_1\alpha_0*]$:

3.1	$[0\beta_0*]$	3.2	$[\widehat{44}*]$	3.4	$[\widehat{44}*0\beta_0*]$
3.1a	$[0\beta_0*4_50_1*]$	3.2a	$[\widehat{44}*4_71*]$	3.4a	$[\widehat{44}*0\beta_0*4_50_1*]$
3.1b	$\emptyset$	3.2b	$[\widehat{41}*]$	3.4b	$[\widehat{44}*00_1*]$

Шаблон $3.1a^{-\alpha} = [4\beta_0*4_50_1*]$ удовлетворяет шаблону 1.2. Шаблон $3.2a^{-\alpha} = [0\widehat{0}*4_71*]$ удовлетворяет либо шаблону $[0\widehat{0}*4\beta_0*]$ (1.6), либо одному из двух: $[0\widehat{0}*7]$ или $[0\widehat{0}*7\gamma_1*1_7]$ (1.7 или 1.8). Шаблон $3.4a^{-\alpha} = [0\widehat{0}*4\beta_0*4_50_1*]$ удовлетворяет $[0\widehat{0}*4\beta_0*]$ (1.6). Шаблон 3.4b удовлетворяет $[.*d00*]$ или $[.*e11*]$, а значит, $3.4b^{-\alpha}$ удовлетворяет 6.1 или 6.2 в силу (6). Шаблоны 3.3 и 3.5 рассматриваются аналогично 4.1 и 4.2.

Столбец 2 можно не рассматривать, так как и его метка, и его элементы $\alpha\beta$ -эквивалентны шаблонам столбца 3.

Заполним табл. 10. Здесь возвращаемся к табл. 2, в которой достаточно рассмотреть столбцы 1, 5, 6 и 7. Добавим шаблоны 7.1 (строка 8), 6.1 (строка 9), 5.1 (строка 10), а также 1.1, 1.3–5, 1.7, 1.8 (строки 1–6). При этом не добавляем 1.2 и 1.6, так как они $\alpha\beta$ -эквивалентны 1.1 и 1.5 (с учётом ω' -части). Таким образом, осталось разобраться с 1.9–14, 5.2 и 6.2. Используем подстановку $-(\gamma, \gamma')$ вместо (γ, γ') .

Пусть $\gamma' \neq 0$, тогда $-(\gamma, \gamma') = (\bar{\gamma}, -\gamma')$. Отметим также, что метки столбцов 1, 5 и 6 симметричны относительно подстановки $-\gamma'$, т. е. слово $\omega(\alpha', \beta', \gamma')$ удовлетворяет одной из этих меток тогда и только тогда, когда слово $\omega(\alpha', \beta', -\gamma')$ удовлетворяет той же самой метке (используем (6) с $-\gamma$ вместо $-\alpha$). Поскольку ω -части 1.9–14, 5.2 и 6.2 $\bar{\gamma}$ -эквивалентны 1.3–8, 5.1 и 6.1, в табл. 10 ничего добавлять не требуется.

Пусть $\gamma' = 0$, тогда $-(\gamma, \gamma') = (-\gamma, 0)$. Значит, ω' -часть слов удовлетворяет $[\gamma_0*]$. Таким образом, нужно понять, какие шаблоны из 1.9, 1.10, 1.11, 1.13 и 1.14 (1.12 $\alpha\beta$ -эквивалентен 1.11) удовлетворяют 1.3–1.8 после преобразования $\omega(\alpha, \beta, -\gamma)$. Рассматриваем только ω -части, удовлетворяющие $[.*e]$, так как иначе получится подслучай 7.1. Например, в 7.1 укладываются исключённые из списка выше 5.2 и 6.2. Получаем, что ω' -части всех оставшихся слов должны удовлетворять и $[.*d00*]$, и $[\gamma_0*]$, т. е. $[\gamma_0*2_400*]$. Как и в случае с α , пересечём все шаблоны с $[.*\gamma_1\gamma_0*]$. Также можем заменить шаблоны 1.13 и 1.14 «расширенным» $[1\hat{1}*6\gamma_0*]$ (1.14). Действительно, добавили только $[1\hat{1}*6\gamma_0*2_4]$, который удовлетворяет 7.1. Также можно не рассматривать 1.9: его ω -часть удовлетворяет $[.*d]$, а значит, $1.9^{-\gamma}$ удовлетворяет 7.1.

1.10	$[1\hat{1}*0.*]$	1.11	$[1\hat{1}*3\alpha_0*]$	$\widetilde{1.14}$	$[1\hat{1}*6\gamma_0*]$
1.10a	$[1\hat{1}*0.*\gamma_1\gamma_0*]$	1.11a	$[1\hat{1}*3\alpha_0*1_30_2*]$	$\widetilde{1.14a}$	$[1\hat{1}*12_4*6\gamma_0*]$
1.10b	$[1\hat{1}*12_4*0\gamma_0*]$	1.11b	$[1\hat{1}*30_2*]$	$\widetilde{1.14b}$	$[12_4*6\gamma_0*]$
1.10c	$[12_4*0\gamma_0*]$				

Шаблон $1.10a^{-\gamma} = [0\hat{0}*1.*\gamma_1\gamma_0*]$ удовлетворяет 1.4, как и $1.10b^{-\gamma} = [0\hat{0}*12_4*0\gamma_0*]$. Далее, шаблон $1.11a^{-\gamma} = [0\hat{0}*2\alpha_0*1_30_2*]$ удовлетворяет 1.5, а $1.11b^{-\gamma} = [0\hat{0}*30_2*] - [0\hat{0}*\alpha_0*]$ ($3 \in \hat{0}$), слова которого по лемме 2 удовлетворяют 1.3, 1.4 или 1.5. Шаблон $\widetilde{1.14a}^{-\gamma} = [0\hat{0}*12_4*6\gamma_0*]$ удовлетворяет 1.4. Шаблоны $1.10c^{-\gamma} = 1.10c$ и $\widetilde{1.14b}^{-\gamma} = \widetilde{1.14b}$ объединены в один шаблон и добавлены в табл. 10 (строка 7).

Табл. 10 заполнена. Указанные в ней шаблоны порождают невозможные разности, и с помощью преобразований из $\mathcal{S}$ к ним сводятся все шаблоны табл. 2. При этом преобразования из $\mathcal{S}$ сохраняют значение разностной характеристики adr^{XR} . Теорема 3 доказана.

Таким образом, применяя преобразования из $\mathcal{S}$ (перестановка первых двух аргументов adp^{XR} и замена любого аргумента противоположным по модулю 2^n), невозможные разности XR-преобразования можно описать 10-ю парами шаблонов. Отметим, что одновременная инверсия старших битов первых двух аргументов adp^{XR} также не изменяет её значения, при этом все шаблоны табл. 2 (учитывая метки) изначально замкнуты относительно этого преобразования.

Финансирование работы

Исследование выполнено в рамках государственного задания Института математики им. С. Л. Соболева (проект № FWNF-2022-0019). Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Автор заявляет, что у него нет конфликта интересов.

Литература

1. **Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L.** The SIMON and SPECK families of lightweight block ciphers. San Diego: Univ. California, 2013. 45 p. (Cryptol. ePrint Archive; Paper ID 2013/404). URL: eprint.iacr.org/2013/404 (accessed: Dec. 9, 2024).
2. **Roh D., Koo B., Jung Y., Jeong I. W., Lee D.-G., Kwon D., Kim W.-H.** Revised version of block cipher CHAM // Information security and cryptology — ICISC 2019. Rev. Sel. Pap. 22th Int. Conf. (Seoul, South Korea, Dec. 4–6, 2019). Cham: Springer, 2020. P. 1–19. (Lect. Notes Comput. Sci.; V. 11975). DOI: 10.1007/978-3-030-40921-0_1.
3. **Bernstein D. J.** The Salsa20 family of stream ciphers. Chicago: Univ. Ill. Chic., 2007. 15 p. URL: cr.yp.to/snuffle/salsafamily-20071225.pdf (accessed: Dec. 9, 2024).
4. **Bernstein D. J.** ChaCha, a variant of Salsa20. Chicago: Univ. Ill. Chic., 2008. 6 p. URL: cr.yp.to/chacha/chacha-20080128.pdf (accessed: Dec. 9, 2024).
5. **Beierle C., Biryukov A., Cardoso dos Santos L. [et al.]** Lightweight AEAD and hashing using the sparkle permutation family // IACR Trans. Symmetric Cryptol. 2020. V. 2020, Suppl. 1. P. 208–261. DOI: 10.13154/tosc.v2020.iS1.208-261.
6. **Mouha N., Mennink B., Van Herrewege A., Watanabe D., Preneel B., Verbauwhede I.** Chaskey: An efficient MAC algorithm for 32-bit microcontrollers // Selected areas in cryptography — SAC 2014. Rev. Sel. Pap. 21th Int. Conf. (Montreal, Canada, Aug. 14–15, 2014). Cham: Springer, 2014. P. 306–323. (Lect. Notes Comput. Sci.; V. 8781). DOI: 10.1007/978-3-319-13051-4_19.
7. **Biham E., Shamir A.** Differential cryptanalysis of DES-like cryptosystems // J. Cryptol. 1991. V. 4. P. 3–72.

8. **Biryukov A., Velichkov V.** Automatic search for differential trails in ARX ciphers // Topics in cryptology — CT-RSA 2014. Proc. Cryptographer's Track at the RSA Conf. (San Francisco, USA, Feb. 25–28, 2014). Cham: Springer, 2014. P. 227–250. (Lect. Notes Comput. Sci.; V. 8366). DOI: 10.1007/978-3-319-04852-9_12.
9. **Leurent G.** Analysis of differential attacks in ARX constructions // Advances in cryptology — ASIACRYPT 2012. Proc. 18th Int. Conf. Theory and Application of Cryptology and Information Security (Beijing, China, Dec. 2–6, 2012). Heidelberg: Springer, 2012. P. 226–243. (Lect. Notes Comput. Sci.; V. 7658).
10. **Leurent G.** Construction of differential characteristics in ARX designs application to Skein // Advances in cryptology — CRYPTO 2013. Proc. 33rd Annu. Cryptology Conf. (Santa Barbara, USA, Aug. 18–22, 2013). Heidelberg: Springer, 2013. P. 241–258. (Lect. Notes Comput. Sci.; V. 8042). DOI: 10.1007/978-3-642-40041-4_14.
11. **Малышев Ф. М.** Вероятностные характеристики разностных и линейных соотношений для неоднородной линейной среды // Мат. вопрос. криптографии. 2019. Т. 10, № 1. С. 41–72. DOI: 10.4213/mvk276.
12. **Малышев Ф. М.** Разностные характеристики основных операций ARX-шифров // Мат. вопрос. криптографии. 2020. Т. 11, № 4. С. 97–105. DOI: 10.4213/mvk342.
13. **Berson T. A.** Differential cryptanalysis mod 2^{32} with applications to MD5 // Advances in cryptology — EUROCRYPT'92. Proc. Workshop Theory and Application of Cryptographic Techniques (Balatonfüred, Hungary, May 24–28, 1992). Heidelberg: Springer, 1992. P. 71–80. (Lect. Notes Comput. Sci.; V. 658). DOI: 10.1007/3-540-47555-9_6.
14. **Daum M. A.** Cryptanalysis of hash functions of the MD4-family: PhD Thesis. Bochum: Ruhr-Univ. Bochum, 2005.
15. **Lipmaa H., Wallén J., Dumas P.** On the additive differential probability of exclusive-or // Fast software encryption. Rev. Pap. 11th Int. Workshop (Delhi, India, Feb. 5–7, 2004). Heidelberg: Springer, 2004. P. 317–331. (Lect. Notes Comput. Sci.; V. 3017). DOI: 10.1007/978-3-540-25937-4_20.
16. **Mouha N., Velichkov V., De Cannière C., Preneel B.** The differential analysis of S-functions // Selected areas in cryptography. Rev. Sel. Pap. 17th Int. Workshop (Waterloo, Canada, Aug. 12–13, 2010). Heidelberg: Springer, 2011. P. 36–56. (Lect. Notes Comput. Sci.; V. 6544). DOI: 10.1007/978-3-642-19574-7_3.
17. **Mouha N., Kolomeec N. A., Akhtiamov D.** [et al.]. Maximums of the additive differential probability of exclusive-or // IACR Trans. Symmetric Cryptol. 2021. V. 2021, No. 2. P. 292–313. DOI: 10.46586/tosc.v2021.i2.292-313.
18. **Velichkov V., Mouha N., De Cannière C., Preneel B.** The additive differential probability of ARX // Fast software encryption. Rev. Sel. Pap. 18th Int. Workshop (Lyngby, Denmark, Feb. 13–16, 2011). Heidelberg: Springer, 2011. P. 342–358. (Lect. Notes Comput. Sci.; V. 6733). DOI: 10.1007/978-3-642-21702-9_20.

19. Kolomeec N. A., Sutormin I. A., Bykov D. A., Panferov M. A., Bonich T. A. On additive differential probabilities of the composition of bitwise exclusive-or and a bit rotation. Ithaca, NY: Cornell Univ., 2023. 35 p. (Cornell Univ. Libr. e-Print Archive; arXiv:2303.04097). DOI: 10.48550/arXiv.2303.04097.
20. Мокроусов А. С., Коломеец Н. А. Разности по модулю 2^n для ARX-преобразований, вероятность которых больше $1/4$ // Дискрет. анализ и исслед. операций. 2024. Т. 31, № 2. С. 108–135. DOI: 10.33048/daio.2024.31.769.
21. Sutormin I. A., Kolomeec N. A. On additive differential probabilities of a composition of bitwise XORs // Прикл. дискрет. математика. 2023. № 60. С. 59–75. DOI: 10.17223/20710410/60/5.
22. Knudsen L. DEAL — A 128-bit block cipher. Tech. Rep. No. 151. Bergen: Univ. Bergen, 1998. 9 p.
23. Biham E., Biryukov A., Shamir A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // Advances in cryptology — EUROCRYPT'99. Proc. Int. Conf. Theory and Application of Cryptographic Techniques (Prague, Czech Republic, May 2–6, 1999). Heidelberg: Springer, 1999. P. 12–23. (Lect. Notes Comput. Sci.; V. 1592). DOI: 10.1007/3-540-48910-X_2.
24. Agievich S. V., Gorodilova A. A., Kolomeec N. A. [et al.]. Problems, solutions and experience of the First International Student's Olympiad in Cryptography // Прикл. дискрет. математика. 2015. № 3. С. 41–62. DOI: 10.17223/20710410/29/4.
25. Gorodilova A. A., Tokareva N. N., Agievich S. V. [et al.]. An overview of the Eight International Olympiad in Cryptography «Non-Stop University Crypto» // Сиб. электрон. мат. изв. 2022. Т. 19, № 1. С. A9–A37. DOI: 10.33048/semi.2022.19.023.

Коломеец Николай Александрович

Статья поступила

9 апреля 2024 г.

После доработки —

10 мая 2024 г.

Принята к публикации

22 июня 2024 г.

THE NUMBER OF IMPOSSIBLE ADDITIVE DIFFERENTIALS FOR THE COMPOSITION OF XOR AND BIT ROTATION

N. A. Kolomeec

Sobolev Institute of Mathematics,
4 Acad. Koptuyug Avenue, 630090 Novosibirsk, Russia
E-mail: nkolomeec@gmail.com

Abstract. Additive differentials of the function $(x \oplus y) \lll r$ whose probability is 0 are considered, where $x, y \in \mathbb{Z}_2^n$ and $1 \leq r < n$. They are called impossible differentials and are interesting in the context of differential cryptanalysis of ciphers whose schemes consist of additions modulo 2^n , bitwise XORs ($\oplus$), and bit rotations ($\lll r$). The number of all such differentials is calculated for all possible r and n . It is also shown that this number is greater than $\frac{38}{245}8^n$. Moreover, the estimate is asymptotically tight for $r, n-r \rightarrow \infty$. For any fixed n the number of all impossible differentials decreases as r goes from 1 to $\lceil n/2 \rceil$ (to $n/2 + 1$ in the case of $n \in \{4, 6, 8, 10, 12\}$) and then increases monotonically as r goes to $n - 1$. A simplified description of all impossible differentials is obtained up to known symmetries. Tab. 10, bibliogr. 25.

Keywords: ARX, differential probability, XOR, modular addition, bit rotation, impossible differential.

References

1. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, The SIMON and SPECK families of lightweight block ciphers (Univ. California, San Diego, 2013) (Cryptol. ePrint Archive; ID 2013/404), URL: eprint.iacr.org/2013/404 (accessed: Dec. 9, 2024).
2. D. Roh, B. Koo, Y. Jung, I. W. Jeong, D.-G. Lee, D. Kwon, and W.-H. Kim, Revised version of block cipher CHAM, in *Information Security and Cryptology — ICISC 2019* (Rev. Sel. Pap. 22th Int. Conf., Seoul, South Korea, Dec. 4–6, 2019) (Springer, Cham, 2020), pp. 1–19 (Lect. Notes Comput. Sci., Vol. 11975), DOI: 10.1007/978-3-030-40921-0_1.

3. **D. J. Bernstein**, The Salsa20 family of stream ciphers (Univ. Ill. Chic., Chicago, 2007), URL: cr.yp.to/snuffle/salsafamily-20071225.pdf (accessed: Dec. 9, 2024).
4. **D. J. Bernstein**, ChaCha, a variant of Salsa20 (Univ. Ill. Chic., Chicago, 2008), URL: cr.yp.to/chacha/chacha-20080128.pdf (accessed: Dec. 9, 2024).
5. **C. Beierle, A. Biryukov, L. Cardoso dos Santos**, [et al.]. Lightweight AEAD and hashing using the sparkle permutation family, *IACR Trans. Symmetric Cryptol.* **2020** (Suppl. 1), 208–261 (2020), DOI: 10.13154/tosc.v2020.iS1.208-261.
6. **N. Mouha, B. Mennink, A. Van Herrewege, D. Watanabe, B. Preneel**, and **I. Verbauwhede**, Chaskey: An efficient MAC algorithm for 32-bit microcontrollers, in *Selected Areas in Cryptography — SAC 2014* (Rev. Sel. Pap. 21th Int. Conf., Montreal, Canada, Aug. 14–15, 2014) (Springer, Cham, 2014), pp. 306–323 (Lect. Notes Comput. Sci., Vol. 8781), DOI: 10.1007/978-3-319-13051-4_19.
7. **E. Biham** and **A. Shamir**, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.* **4**, 3–72 (1991).
8. **A. Biryukov** and **V. Velichkov**, Automatic search for differential trails in ARX ciphers, in *Topics in Cryptology — CT-RSA 2014* (Proc. Cryptographer’s Track at the RSA Conf., San Francisco, USA, Feb. 25–28, 2014) (Springer, Cham, 2014), pp. 227–250 (Lect. Notes Comput. Sci., Vol. 8366), DOI: 10.1007/978-3-319-04852-9_12.
9. **G. Leurent**, Analysis of differential attacks in ARX constructions, in *Advances in Cryptology — ASIACRYPT 2012* (Proc. 18th Int. Conf. Theory and Application of Cryptology and Information Security, Beijing, China, Dec. 2–6, 2012) (Springer, Heidelberg, 2012), pp. 226–243 (Lect. Notes Comput. Sci., Vol. 7658).
10. **G. Leurent**, Construction of differential characteristics in ARX designs application to Skein, in *Advances in Cryptology — CRYPTO 2013* (Proc. 33rd Annu. Cryptology Conf., Santa Barbara, USA, Aug. 18–22, 2013) (Springer, Heidelberg, 2013), pp. 241–258 (Lect. Notes Comput. Sci., Vol. 8042), DOI: 10.1007/978-3-642-40041-4_14.
11. **F. M. Malyshev**, Probabilistic characteristics of differential and linear relations for nonhomogeneous linear medium, *Mat. Vopr. Kriptogr.* **10** (1), 41–72 (2019), DOI: 10.4213/mvk276 [Russian].
12. **F. M. Malyshev**, Differential characteristics of base operations in ARX-ciphers, *Mat. Vopr. Kriptogr.* **11** (4), 97–105 (2020), DOI: 10.4213/mvk342 [Russian].
13. **T. A. Berson**, Differential cryptanalysis mod 2^{32} with applications to MD5, in *Advances in Cryptology — EUROCRYPT’92* (Proc. Workshop Theory and Application of Cryptographic Techniques, Balatonfüred, Hungary, May 24–28, 1992) (Springer, Heidelberg, 1992), pp. 71–80 (Lect. Notes Comput. Sci., Vol. 658), DOI: 10.1007/3-540-47555-9_6.

14. **M. A. Daum**, Cryptanalysis of hash functions of the MD4-family, *PhD Thesis* (Ruhr-Univ. Bochum, Bochum, 2005).
15. **H. Lipmaa, J. Wallén and P. Dumas**, On the additive differential probability of exclusive-or, in *Fast Software Encryption* (Rev. Pap. 11th Int. Workshop, Delhi, India, Feb. 5–7, 2004) (Springer, Heidelberg, 2004), pp. 317–331 (Lect. Notes Comput. Sci., Vol. 3017), DOI: 10.1007/978-3-540-25937-4_20.
16. **N. Mouha, V. Velichkov, C. De Cannière and B. Preneel**, The differential analysis of S-functions, in *Selected Areas in Cryptography* (Rev. Sel. Pap. 17th Int. Workshop, Waterloo, Canada, Aug. 12–13, 2010) (Springer, Heidelberg, 2011), pp. 36–56 (Lect. Notes Comput. Sci., Vol. 6544), DOI: 10.1007/978-3-642-19574-7_3.
17. **N. Mouha, N. A. Kolomeec, D. Akhtiamov**, [et al.]. Maximums of the additive differential probability of exclusive-or, *IACR Trans. Symmetric Cryptol.* **2021** (2), 292–313 (2021), DOI: 10.46586/tosc.v2021.i2.292-313.
18. **V. Velichkov, N. Mouha, C. De Cannière and B. Preneel**, The additive differential probability of ARX, in *Fast Software Encryption* (Rev. Sel. Pap. 18th Int. Workshop, Lyngby, Denmark, Feb. 13–16, 2011) (Springer, Heidelberg, 2011), pp. 342–358 (Lect. Notes Comput. Sci., Vol. 6733), DOI: 10.1007/978-3-642-21702-9_20.
19. **N. A. Kolomeec, I. A. Sutormin, D. A. Bykov, M. A. Panferov**, and **T. A. Bonich**, On additive differential probabilities of the composition of bitwise exclusive-or and a bit rotation (Cornell Univ., Ithaca, NY, 2023) (Cornell Univ. Libr. e-Print Archive, arXiv:2303.04097), DOI: 10.48550/arXiv.2303.04097.
20. **A. S. Mokrousov and N. A. Kolomeec**, Additive differentials for ARX mappings with probability exceeding $1/4$, *Diskretn. Anal. Issled. Oper.* **31** (2), 108–135 (2024), DOI: 10.33048/daio.2024.31.769 [Russian] [*J. Appl. Ind. Math.* **18** (2), 294–311 (2024), DOI: 10.1134/S199047892402011X].
21. **I. A. Sutormin and N. A. Kolomeec**, On additive differential probabilities of a composition of bitwise XORs, *Prikl. Diskretn. Mat.*, No. 60, 59–75 (2023), DOI: 10.17223/20710410/60/5.
22. **L. Knudsen**, DEAL — A 128-bit block cipher, *Tech. Rep. No. 151* (Univ. Bergen, Bergen, 1998).
23. **E. Biham, A. Biryukov**, and **A. Shamir**, Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials, in *Advances in Cryptology — EUROCRYPT’99* (Proc. Int. Conf. Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2–6, 1999) (Springer, Heidelberg, 1999), pp. 12–23 (Lect. Notes Comput. Sci., Vol. 1592), DOI: 10.1007/3-540-48910-X_2.
24. **S. V. Agievich, A. A. Gorodilova, N. A. Kolomeec**, [et al.]. Problems, solutions, and experience of the First International Student’s Olympiad in Cryptography, *Prikl. Diskretn. Mat.*, No. 3, 41–62 (2015), DOI: 10.17223/20710410/29/4.

-
- 25. A. A. Gorodilova, N. N. Tokareva, S. V. Agievich**, [et al.]. An overview of the Eight International Olympiad in Cryptography “Non-Stop University Crypto”, *Sib. Elektron. Mat. Izv.* **19** (1), A9–A37 (2022), DOI: 10.33048/semi.2022.19.023.

Nikolay A. Kolomeec

Received April 9, 2024

Revised May 10, 2024

Accepted June 22, 2024