МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 003.26.09+004.021 DOI 10.17223/20710410/58/5

О ПОИСКЕ РАЗНОСТНЫХ СООТНОШЕНИЙ ДЛЯ ПОДСТАНОВКИ ALZETTE С МАКСИМАЛЬНЫМ ИЛИ БЛИЗКИМ К НЕМУ ЗНАЧЕНИЕМ РАЗНОСТНОЙ ХАРАКТЕРИСТИКИ

А. А. Дмух, Д. О. Пасько

Академия криптографии Российской Федерации, г. Москва, Россия

E-mail: graphin@rambler.ru, pasko.do@yandex.ru

Предлагается подход «разностная встреча посередине» для построения согласованных систем локальных разностных соотношений для подстановки Alzette, который позволяет получать системы с максимальными или близкими к максимальным разностными характеристиками. С помощью этого подхода расширены результаты по оценке разностных характеристик подстановки Alzette, полученные разработчиками подстановки, при этом с меньшей трудоёмкостью.

Ключевые слова: *подстановка, Alzette, разностная характеристика, разностный метод.*

SEARCH FOR DIFFERENCES FOR ALZETTE S-BOX WITH MAXIMUM OR CLOSE TO MAXIMUM DIFFERENTIAL CHARACTERISTIC PROBABILITY

A. A. Dmukh, D. O. Pasko

Academy of Cryptography of the Russian Federation, Moscow, Russia

In this paper, we describe a “differential meet-in-the-middle” method for obtaining differences for 64-bit ARX permutation Alzette with maximum or close to maximum differential characteristic probability (DCP). The method is based on testing the high-probability differences in the middle rounds of Alzette and extending them to the previous and following rounds. Using this method, we obtain 7 differences for 4-rounds Alzette with DCP 2^{-6}, 1 difference for 5-rounds Alzette with DCP 2^{-10}, and 1 difference for 6-rounds Alzette with DCP 2^{-18}. Same differences for 4 and 5 rounds were obtained by the developers of Alzette as the differences with maximum DCP, but our method has lower complexity: taking the calculation of probability for a round difference as a single operation, it’s 36 operations (4 rounds), 135 operations (5 rounds) and 486 operations (6 rounds) for our method and more than $1.29 \cdot 10^8$ operations (4 rounds), $2 \cdot 1.29 \cdot 10^8$ operations (5 rounds) and $1.03 \cdot 10^{14}$ operations (6 rounds) for Alzette developers’ method. Also, we obtain 6 differences for 7-rounds Alzette with DCP 2^{-27} and 11 differences for 8-rounds Alzette with DCP 2^{-35} with complexity $\leqslant 5 \cdot 10^{13}$ operations for both cases. For these number of rounds by the developers of Alzette were obtained only the higher bounds for maximum DCP: 2^{-24} (7 rounds) and 2^{-32} (8 rounds). Our estimations of Alzette developers’ method complexity is

$\geqslant 2.97 \cdot 10^{16}$ operations for 7-rounds Alzette and $\geqslant 2.97 \cdot 10^{16} + 4.75 \cdot 10^{12}$ operations for 8-rounds Alzette.

Keywords: *permutation, Alzette, differential characteristic, differential method.*

Введение

В ноябре 2019 г. коллективом авторов в работе [1] была предложена подстановка Alzette, действующая на двоичных векторах длины 64 и предназначенная к использованию в низкоресурсных блочных шифрах и криптографических примитивах на их основе. Подстановка Alzette представляет собой итеративную ARX-конструкцию, т. е. в ней на каждой итерации (раунде) используются лишь следующие операции над двоичными векторами длины 32: модульного сложения по $\bmod 2^{32}$ ($\boxplus$), циклического сдвига ($\ggg\ a$ — в данном случае циклический сдвиг вправо на a позиций, Rotation) и побитового сложения ($\oplus$, XOR). Выбор ARX-конструкции для построения подстановки обусловлен удобством и эффективностью реализации указанных операций на платформах с ограниченными ресурсами.

Конкретный выбор количества итераций и значений циклических сдвигов для подстановки Alzette в [1], по словам авторов, был сделан для достижения разумного баланса между эффективностью реализации и приемлемыми криптографическими характеристиками. Таким образом, в [1] для подстановки Alzette остановились на количестве итераций, равном 4, и значениях циклических сдвигов, приведённых на рис. 1, где $x, y, u, v, c \in V_{32}$.

Подстановка Alzette из $\mathrm{S}_{V_{64}}$ является дальнейшим развитием ARX-конструкций, предназначенных для использования в низкоресурсных криптографических примитивах: подстановки из криптопримитива SATURNIN [2] (используется подстановка из $\mathrm{S}_{V_{16}}$, получаемая из нескольких слоев 4-битных подстановок, перемежаемых слоями максимально рассеивающих линейных преобразований соответствующей размерности) и подстановки SPARX [3] (ARX-конструкция, реализующая подстановку из $\mathrm{S}_{V_{32}}$).

В отличие от подстановок из [2, 3], для которых некоторые (в работе [2] — все) криптографические характеристики подсчитаны точно на ЭВМ, для подстановки Alzette в работе [1] ряд характеристик, в частности разностные и линейные, оценены на ЭВМ с применением подхода, предложенного в [4]. Данный подход использует ряд предположений и допущений. В частности, предполагается марковость ARX-конструкции, хотя сами же авторы работы [4] показывают, что алгоритм Speck, для которого получены значения для оценок наилучших разностных и линейных характеристик для некоторого числа итераций, свойством марковости не обладает. Таким образом, строгих теоретических обоснований полученных в [1] оценок для наилучших разностных и линейных характеристик не приводится.

В данной работе с использованием результатов [5, 6] предложен подход по проверке оценок максимального значения разностной характеристики подстановки Alzette, полученных в [1], который, помимо прочего, позволяет предъявлять согласованные системы локальных разностных соотношений [5] (далее — с.с.л.р.с.), соответствующие заданным разностным соотношениям, с максимальными значениями разностных характеристик.

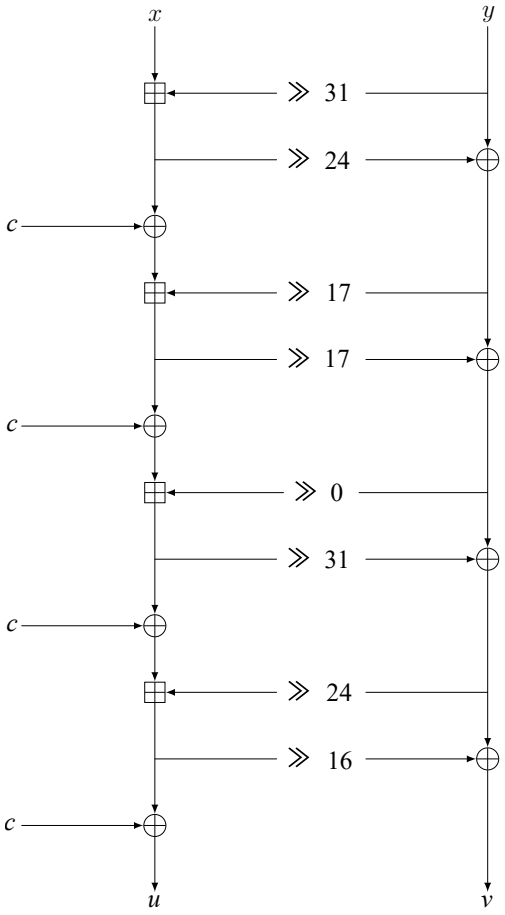

Рис. 1. Подстановка Alzette

1. Разностные характеристики подстановки Alzette

Как и в [1], будем искать разностные соотношения для подстановки Alzette $(A, B) \in \in V_{64} \times V_{64}$ с максимально возможными значениями разностной характеристики $P^{\mathrm{ALZ}}_{A,B} = \mathsf{P}[\mathrm{ALZ}(x) \oplus \mathrm{ALZ}(x \oplus A) = B]$, где вероятность $\mathsf{P}[\dots]$ вычисляется в предположении случайного равновероятного распределения x на V_{64}, а $\mathrm{ALZ}(x) \in V_{64}$ — результат применения подстановки Alzette к вектору x.

Представим подстановку Alzette как четыре итерации блочного ARX-шифра. В таком случае, в соответствии с [5], с.с.л.р.с. можно строить последовательно, например от первой итерации к последней. При этом необходимо строить локальные разностные соотношения (относительно побитового сложения $\oplus$) для всех трёх используемых операций: $\boxplus$, $\ggg a$ и $\oplus$. Если для последних двух операций построение таких соотношений (в том числе удовлетворяющих условию согласованности и имеющих значение разностной характеристики 1) — тривиальная задача, то для построения локальных вероятностных соотношений модульного сложения (и, главное, оценки их разностных характеристик) воспользуемся результатами, полученными в [5, 6]. В соответствии с [5], вместо точного значения вероятности $P^{\mathrm{ALZ}}_{A,B}$ рассматривается её оценка — разностная характеристика $\tilde{P}^{\mathrm{ALZ}}_{A,B}$ с.с.л.р.с. подстановки Alzette, равная произведению разностных характеристик локальных разностных соотношений, приходящихся на каждой итерации на модульное сложение.

На рис. 2 дано альтернативное (более удобное для построения с.с.л.р.с.) представление итерации с номером i, $i = 1, \dots, 4$, подстановки Alzette. Здесь сложе-

ние с константой $c \in V_{32}$ не изображено, так как оно не влияет ни на построение локальных разностных соотношений, ни на значения разностных характеристик; $X_L^{(i-1)}, X_R^{(i-1)}, X_L^{(i)}, X_R^{(i)}, Z^{(i-1)} \in V_{32}$ — промежуточные разности; r_i, s_i — значения циклических сдвигов влево (они приведены в табл. 1).

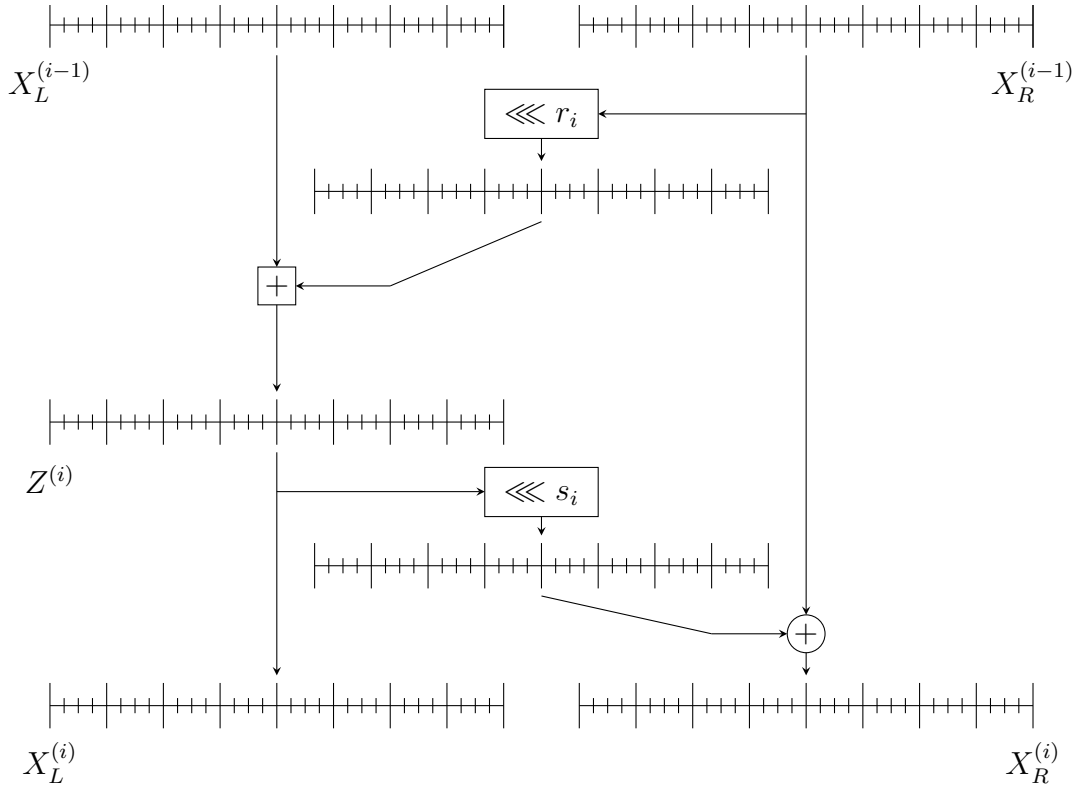

Рис. 2. Альтернативное представление i-й итерации подстановки Alzette

Таблица 1
Значения сдвигов

i	r_i	s_i
1	1	8
2	15	15
3	0	1
4	8	16

Определим, следуя [6], разностную характеристику для модульного сложения ($xdp^+(\alpha, \beta \to \gamma)$ — exclusive-or differential probability):

$$xdp^+(\alpha, \beta \to \gamma) = \mathsf{P}\left[\alpha, \beta \xrightarrow{\boxplus} \gamma\right] = \mathsf{P}\left[((x \oplus \alpha) \boxplus (y \oplus \beta)) \oplus (x \boxplus y) = \gamma\right],$$

где вероятность $\mathsf{P}[\dots]$ вычисляется в предположении случайного равновероятного распределения x, y на V_n; $x = (x_{n-1}, \dots, x_0)$, $y = (y_{n-1}, \dots, y_0)$. Отметим, что в обозначениях работы [5] $xdp^+(\alpha, \beta \to \gamma) = p^+_{\oplus\alpha, \oplus\beta, \oplus\gamma}$.

Для вычисления конкретных значений разностных характеристик локальных разностных соотношений, приходящихся в подстановке Alzette на модульное сложение, удобно воспользоваться результатами работы [6], в которой приводится представление вероятности $xdp^+(\alpha, \beta \to \gamma)$ как формального ряда над моноидом восьмеричных слов

с коэффициентами из поля действительных чисел. Для заданных $\alpha, \beta, \gamma \in V_n$ обозначим $w = (w_{n-1}, \ldots, w_0)$, где $w_i = \alpha_i \cdot 4 + \beta_i \cdot 2 + \gamma_i$, $i = 0, 1, \ldots, n-1$. Таким образом, можно задать $xdp^+(\alpha, \beta \to \gamma)$ как функцию от множества всех восьмеричных слов длины n в интервал $[0, 1] \subset \mathbb{R}$

Теорема 1 [6, теорема 2.1]. Для любого набора $(\alpha, \beta, \gamma) \in V_{3n}$

$$xdp^+(\alpha, \beta \to \gamma) = \overrightarrow{L} \cdot A_{w_{n-1}} \cdot A_{w_{n-2}} \cdot \ldots \cdot A_{w_0} \cdot C^{\downarrow},$$

где $\overrightarrow{L} = (1, 1)$; $C^{\downarrow} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; $A_1 = A_2 = A_4 = \begin{pmatrix} 0 & 1/2 \\ 0 & 1/2 \end{pmatrix}$; $A_3 = A_5 = A_6 = \begin{pmatrix} 1/2 & 0 \\ 1/2 & 0 \end{pmatrix}$; $A_7 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Из теоремы 1, в частности, следует, что $xdp^+(\alpha, \beta \to \gamma) = 1$ только в одном из четырёх случаев, приведённых в табл. 2 (e_{n-1} — вектор из V_n, у которого единственная координата с номером $n-1$ равна единице, все остальные — нулю).

Таблица 2

Разностные соотношения сложения $\boxplus$, имеющие вероятность 1

α	0	e_{n-1}	e_{n-1}	0
β	e_{n-1}	0	e_{n-1}	0
γ	e_{n-1}	e_{n-1}	0	0

Так как для подстановки Alzette $n = 32$ (т. е. достаточно велико), то при расчёте разностных характеристик с использованием теоремы 1 для уменьшения трудоёмкости их вычисления полезно использовать следующие свойства матриц A_k, $k = 0, \ldots, 7$.

Утверждение 1. Для матриц A_k, $k = 0, \ldots, 7$:

1) $A_0^t = A_0$, $A_7^t = A_7$ для любого $t \geqslant 1$;
2) если обозначить $A_{124} = A_1 = A_2 = A_4 = \begin{pmatrix} 0 & 1/2 \\ 0 & 1/2 \end{pmatrix}$ и $A_{356} = A_3 = A_5 = A_6 = \begin{pmatrix} 1/2 & 0 \\ 1/2 & 0 \end{pmatrix}$, то $A_{124}^t = \begin{pmatrix} 0 & 1/2^t \\ 0 & 1/2^t \end{pmatrix}$, $A_{356}^t = \begin{pmatrix} 1/2^t & 0 \\ 1/2^t & 0 \end{pmatrix}$ для любого $t \geqslant 1$;
3) $A_0^s \cdot A_7^t = A_7^t \cdot A_0^s = A_{124}^s \cdot A_0^t = A_{356}^s \cdot A_7^t = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ для любых $s, t \geqslant 1$;
4) $A_{124} \cdot A_7^t = A_{124}$, $A_{356} \cdot A_0^t = A_{356}$ для любого $t \geqslant 1$;
5) $A_0^t \cdot A_{356} = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix}$, $A_7^t \cdot A_{356} = \begin{pmatrix} 0 & 0 \\ 1/2 & 0 \end{pmatrix}$, $A_0^t \cdot A_{124} = \begin{pmatrix} 0 & 1/2 \\ 0 & 0 \end{pmatrix}$, $A_7^t \cdot A_{124} = \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix}$ для любого $t \geqslant 1$;
6) $A_{124}^s \cdot A_{356}^t = \begin{pmatrix} 1/2^{s+t} & 0 \\ 1/2^{s+t} & 0 \end{pmatrix}$, $A_{356}^t \cdot A_{124}^s = \begin{pmatrix} 0 & 1/2^{s+t} \\ 0 & 1/2^{s+t} \end{pmatrix}$ для любых $s, t \geqslant 1$.

Доказательство.

Пункт 1 доказывается индукцией по $i \geqslant 2$ с базисом индукции при $i = 2$: $A_0^2 = A_0$, $A_7^2 = A_7$.

Пункт 2 доказывается индукцией по $i \geqslant 2$ с базисом индукции при $i = 2$: $A_{124}^2 = \begin{pmatrix} 0 & 1/4 \\ 0 & 1/4 \end{pmatrix}$, $A_{356}^2 = \begin{pmatrix} 1/4 & 0 \\ 1/4 & 0 \end{pmatrix}$.

Пункт 3 следует из пп. 1 и 2.

Пункт 4 следует из п. 1 и легко проверяемых равенств $A_{124} \cdot A_7 = A_{124}$ и $A_{356} \cdot A_0 = A_{356}$.

Пункт 5 следует из п. 1 и легко проверяемых равенств $A_0 \cdot A_{356} = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix}$, $A_7 \cdot A_{356} = \begin{pmatrix} 0 & 0 \\ 1/2 & 0 \end{pmatrix}$, $A_0 \cdot A_{124} = \begin{pmatrix} 0 & 1/2 \\ 0 & 0 \end{pmatrix}$, $A_7 \cdot A_{124} = \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix}$.

Пункт 6 следует из п. 2. ■

Замечание 1. Если через A обозначить $A_{w_{n-1}} \cdot A_{w_{n-2}} \cdot \ldots \cdot A_{w_0} = A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$, то $\overrightarrow{L} \cdot A \cdot C^{\downarrow} = a_{1,1} + a_{2,1}$, следовательно, при построении разностного соотношения при заданных α и β для выполнения условия $xdp^{+}(\alpha, \beta \to \gamma) \neq 0$ необходимо выбирать вектор γ таким образом, чтобы избегать в произведении $A_{w_{n-1}} \cdot A_{w_{n-2}} \cdot \ldots \cdot A_{w_0}$ сомножителей, которые приводят к одновременному обнулению элементов в первом столбце.

Замечание 2. В работе [1] с использованием подхода из [4], реализованного на ЭВМ, найдены семь разностных соотношений для подстановки Alzette (четыре итерации) с максимальным значением разностной характеристики соответствующей с.с.л.р.с., равной 2^{-6}, а также одно разностное соотношение для подстановки Alzette на пять итераций (четыре итерации плюс дополнительная первая итерация) с максимальным значением разностной характеристики с.с.л.р.с., равной 2^{-10}. Эти разностные соотношения приведены в шестнадцатеричном виде в табл. 3.

Таблица 3

Разностные соотношения подстановки Alzette, найденные в [1]

№ п/п	Число итераций	$A \in V_{64}$	$B \in V_{64}$	$-\log_2\left(\tilde{P}^{\mathrm{ALZ}}_{A,B}\right)$
1	4	(8000010000000080)	(8040410041004041)	6
2	4	(8000010000000080)	(80C04100410040C1)	6
3	4	(0080400180400000)	(8000018081808001)	6
4	4	(0080400180400000)	(8000008080808001)	6
5	4	(A0008140000040A0)	(8000010001008001)	6
6	4	(8002010000010080)	(0101000000030101)	6
7	4	(8002010000010080)	(0301000000030301)	6
8	5	(A0008140000040A0)	(8201010200018283)	10

2. Разностная встреча посередине

Для построения с.с.л.р.с. с максимальным (или близким к нему) значением разностной характеристики для подстановки Alzette на четыре, пять и шесть итераций в соответствии с теоремой 1 и замечанием 1 предложим следующий подход, который условно назовём «разностная встреча посередине». На второй (или на третьей) итерации подстановки Alzette в качестве промежуточных разностей $X_L^{(1)}$, $X_R^{(1)} \lll r_2$, $Z^{(2)}$ (или $X_L^{(2)}$, $X_R^{(2)} \lll r_3$, $Z^{(3)}$) будем брать только векторы из табл. 1 с дальнейшим достраиванием системы локальных разностных соотношений «вверх» и «вниз», пытаясь одновременно максимизировать разностные характеристики с.с.л.р.с. на других итерациях с учётом уже сделанного выбора промежуточных разностей. При этом следует отметить, что хотя при равенстве $\alpha = \beta = \gamma = 0$ (столбец 5 табл. 1) также достигается максимальное значение локальной разностной характеристики (равное 1), такие варианты мы рассматривать не будем, так как это означает, что $X_L^{(i-1)} = X_R^{(i-1)} = 0$ при

$i = 2$ или 3, что, в свою очередь, приводит к тривиальному (нулевая разность на входе с вероятностью 1 переходит в нулевую разность на выходе) разностному соотношению для всей подстановки Alzette.

Используя подход «разностная встреча посередине» без применения ЭВМ, удалось получить все семь разностных соотношений на четыре итерации с максимальным значением разностной характеристики с.с.л.р.с., равной 2^{-6}, приведённых в [1], одно разностное соотношение на пять итераций с максимальным значением разностной характеристики с.с.л.р.с., равной 2^{-10} (также найденное в [1]), и одно разностное соотношение на шесть итераций с максимальным значением разностной характеристики с.с.л.р.с., равной 2^{-18}. Отметим, что в [1] только упоминается, что максимальное значение разностной характеристики с.с.л.р.с. на шести итерациях равно 2^{-18}, но ни одной с.с.л.р.с., на которой оно достигается, не приведено. При этом для меньшего числа итераций — четыре и пять — все соответствующие разностные соотношения приведены. Вероятно, для шести итераций авторы [1] получили не точное значение максимальной разностной характеристики с.с.л.р.с., а лишь её оценку сверху, потому что, начиная с семи итераций, в работе [1] прямо указывается, что предъявленные максимальные значения разностных характеристик (также без указания соответствующих им разностных соотношений) являются лишь оценками сверху.

3. Разностная встреча посередине для шести итераций подстановки Alzette

Подробно распишем построение и получение значений разностных характеристик с.с.л.р.с. для разностного соотношения на шесть итераций. Для оставшихся разностных соотношений на четыре итерации приведём с.с.л.р.с. вида

$$X_L^{(0)}, X_R^{(0)}, X_L^{(1)}, X_R^{(1)}, X_L^{(2)}, X_R^{(2)}, X_L^{(3)}, X_R^{(3)}, X_L^{(4)}, X_R^{(4)},$$

по которым с использованием теоремы 1 можно проверить равенство разностной характеристики максимальному значению 2^{-6}.

Начнём с разностного соотношения на шесть итераций. На рис. 3–8 во всех двоичных векторах длины 32 для простоты отмечены (символом «•») только единичные координаты. С учётом замечания 1 значение $xdp^+(\alpha, \beta \to \gamma)$ будем характеризовать в виде произведения 32 матриц (без дополнительного умножения на $\overrightarrow{L}$ и $C^{\downarrow}$), помня, что для получения значения $xdp^+(\alpha, \beta \to \gamma)$ необходимо сложить строки результирующей матрицы и выбрать старшую координату.

На рис. 3 и 8 над $X_L^{(0)}, X_R^{(0)}$ и $X_L^{(6)}, X_R^{(6)}$ записаны их шестнадцатеричные представления. Из построения с.с.л.р.с. на шесть итераций видно, что она содержит в себе с.с.л.р.с. на четыре итерации с максимальным значением разностной характеристики 2^{-6} (№ 5 из табл. 3), а также с.с.л.р.с. на пять итераций (№ 8 из табл. 3), значения $X_L^{(4)}, X_R^{(4)}$ и $X_L^{(5)}, X_R^{(5)}$ для которого записаны на рис. 6 и 7 в шестнадцатеричном виде.

Таким образом, для разностного соотношения на шесть итераций получаем, что $P^{\mathrm{ALZ}}_{(\mathrm{A0008140000040A0,434081024080A323})} = \frac{1}{16}\cdot\frac{1}{2}\cdot 1\cdot\frac{1}{2}\cdot\frac{1}{16}\cdot\frac{1}{256} = 2^{-18}$, а для разностного соотношения на пять и четыре итерации $P^{\mathrm{ALZ}}_{(\mathrm{A0008140000040A0,8201010200018283})} = \frac{1}{16}\cdot\frac{1}{2}\cdot 1\cdot\frac{1}{2}\cdot\frac{1}{16} = 2^{-10}$, $P^{\mathrm{ALZ}}_{(\mathrm{A0008140000040A0,8000010001008001})} = \frac{1}{16}\cdot\frac{1}{2}\cdot 1\cdot\frac{1}{2} = 2^{-6}$ соответственно.

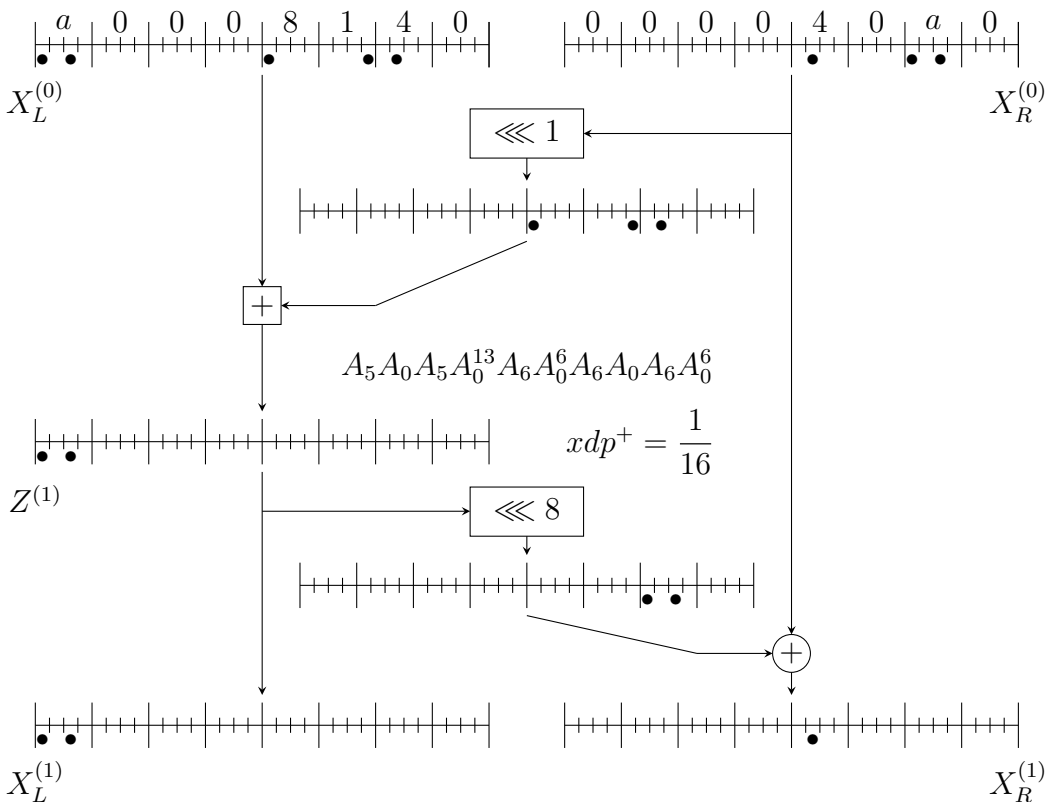

Рис. 3. Итерация 1

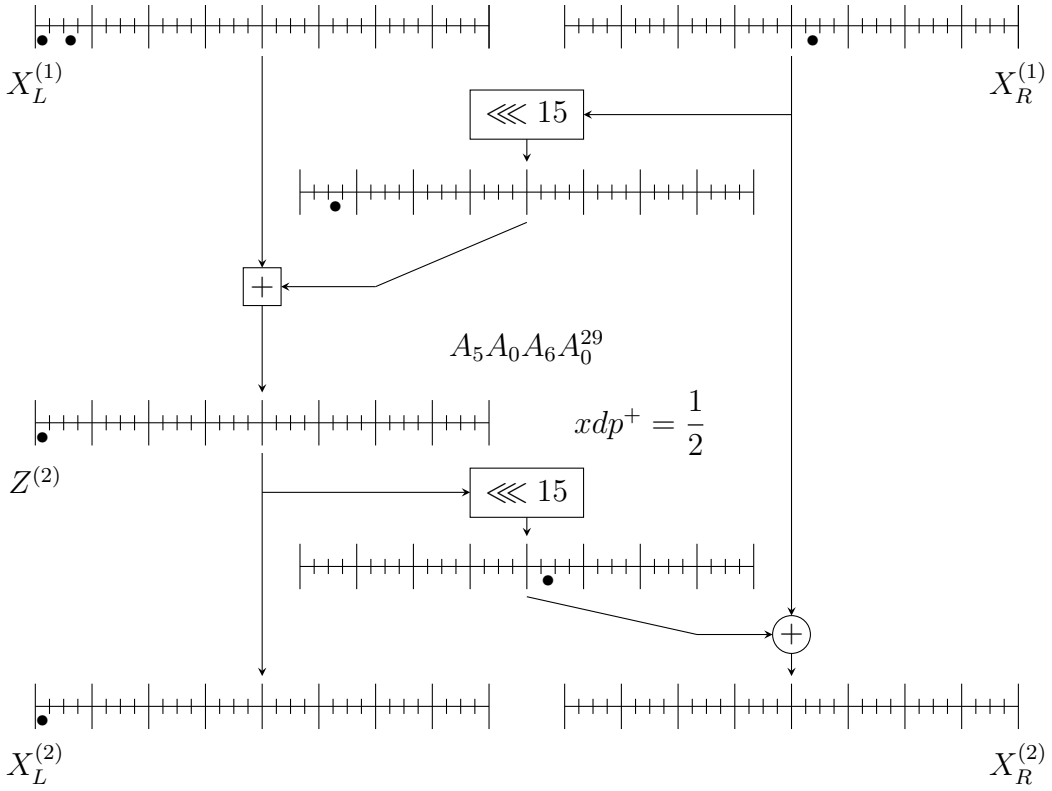

Рис. 4. Итерация 2

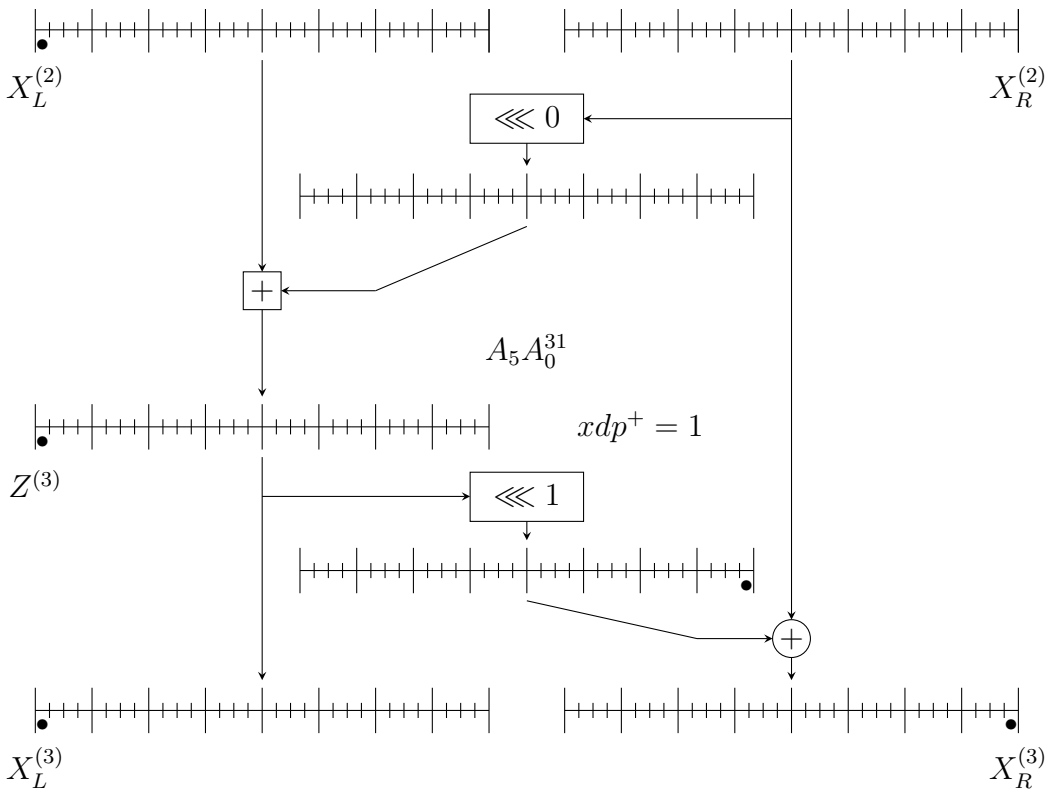

Рис. 5. Итерация 3

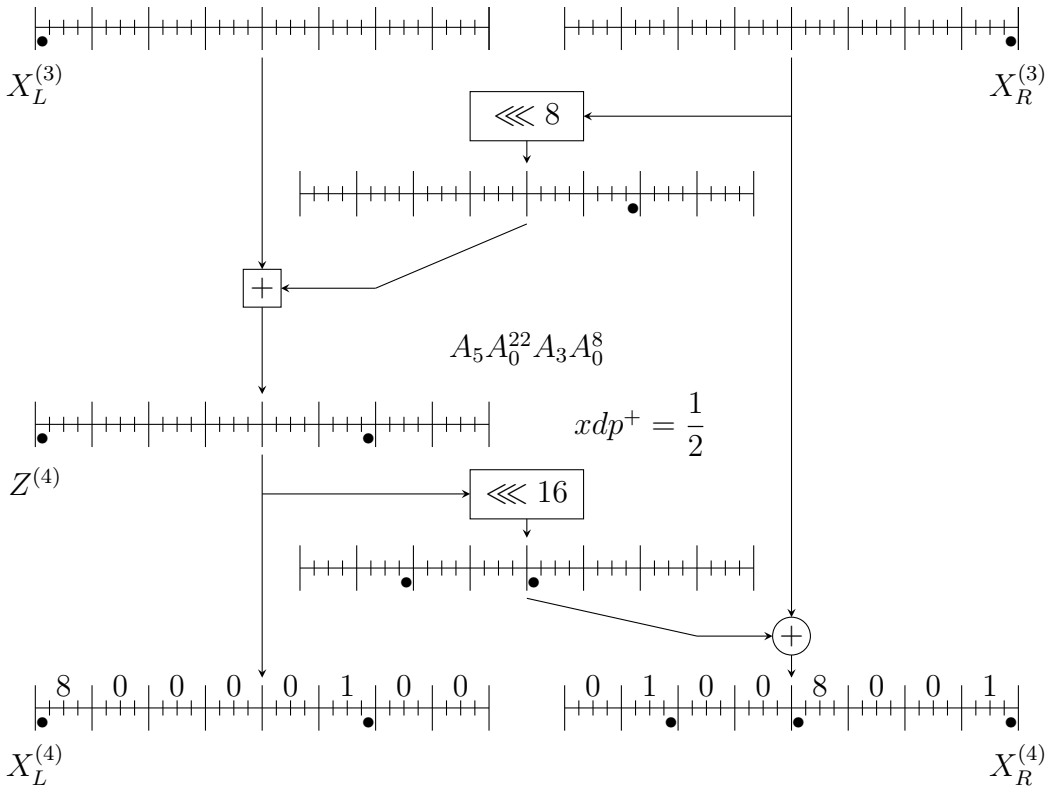

Рис. 6. Итерация 4

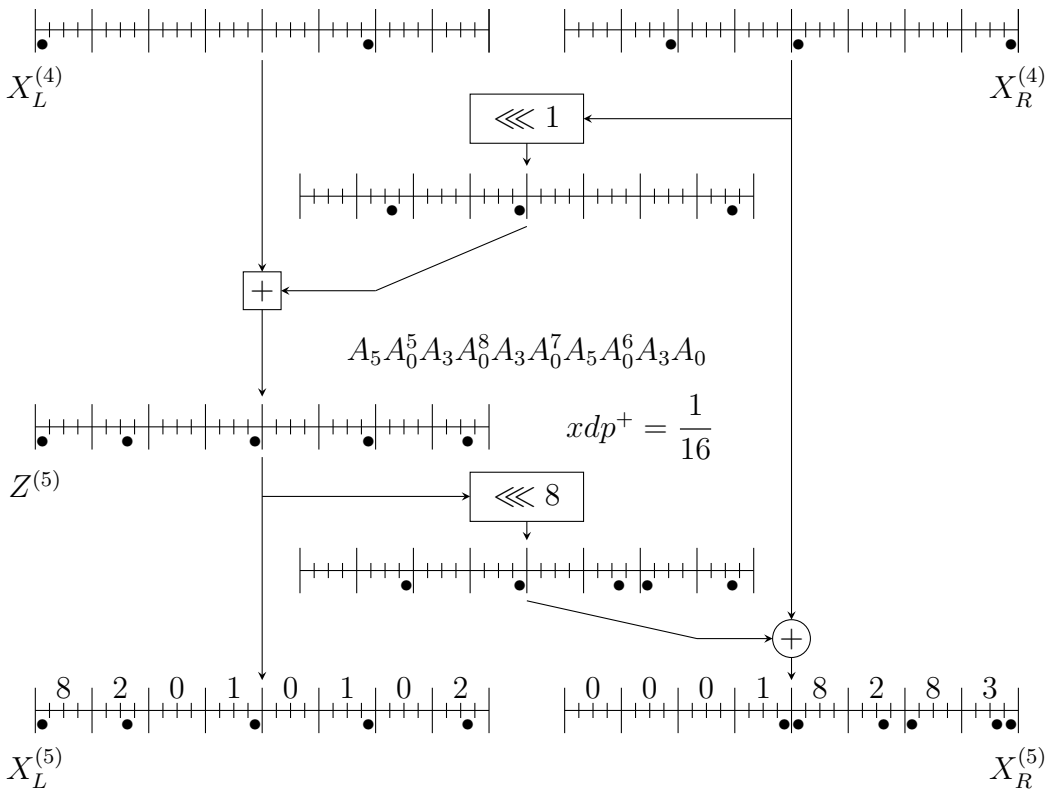

Рис. 7. Итерация 5

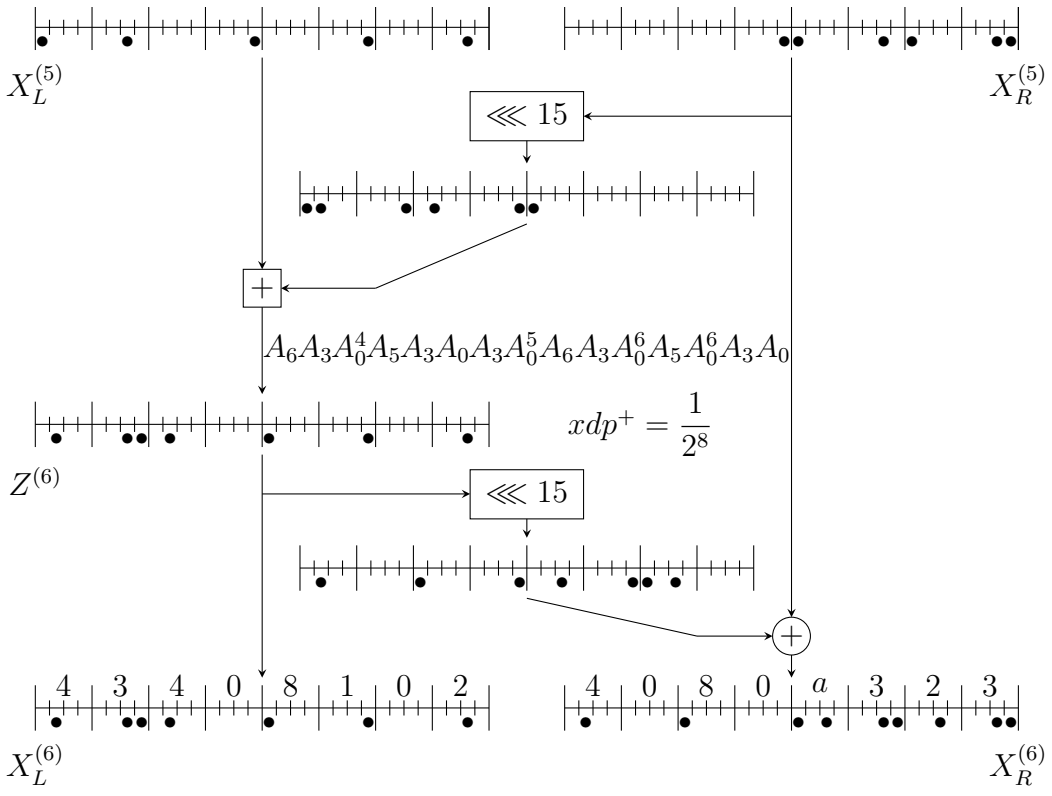

Рис. 8. Итерация 6

В табл. 4 приведены в шестнадцатеричном виде с.с.л.р.с. для оставшихся разностных соотношений с максимальным значением разностной характеристики (№ 1–4, 6, 7 из табл. 3).

Таблица 4

Разностные соотношения подстановки Alzette на четыре итерации

Соотношение № 1	Соотношение № 2
$\left(X_L^{(0)}, X_R^{(0)}\right) = (80000100, 00000080)$ $Z^{(1)} = X_L^{(1)} = (80000000), X_R^{(1)} = (00000000)$ $Z^{(2)} = X_L^{(2)} = (80000000), X_R^{(2)} = (00004000)$ $Z^{(3)} = X_L^{(3)} = (80004000), X_R^{(3)} = (0000C001)$ $Z^{(4)} = X_L^{(4)} = (80404100), X_R^{(4)} = (41004041)$ $\tilde{P}^{\mathrm{ALZ}}_{\left(x_L^{(0)}, x_R^{(0)}\right), \left(x_L^{(4)}, x_R^{(4)}\right)} = \frac{1}{2} \cdot 1 \cdot \frac{1}{2} \cdot \frac{1}{16} = 2^{-6}$	$\left(X_L^{(0)}, X_R^{(0)}\right) = (80000100, 00000080)$ $Z^{(1)} = X_L^{(1)} = (80000000), X_R^{(1)} = (00000000)$ $Z^{(2)} = X_L^{(2)} = (80000000), X_R^{(2)} = (00004000)$ $Z^{(3)} = X_L^{(3)} = (80004000), X_R^{(3)} = (0000C001)$ $Z^{(4)} = X_L^{(4)} = (80C04100), X_R^{(4)} = (410040C1)$ $\tilde{P}^{\mathrm{ALZ}}_{\left(x_L^{(0)}, x_R^{(0)}\right), \left(x_L^{(4)}, x_R^{(4)}\right)} = \frac{1}{2} \cdot 1 \cdot \frac{1}{2} \cdot \frac{1}{16} = 2^{-6}$
Соотношение № 3	Соотношение № 4
$\left(X_L^{(0)}, X_R^{(0)}\right) = (00804001, 80400000)$ $Z^{(1)} = X_L^{(1)} = (00004000), X_R^{(1)} = (80000000)$ $Z^{(2)} = X_L^{(2)} = (00000000), X_R^{(2)} = (80000000)$ $Z^{(3)} = X_L^{(3)} = (80000000), X_R^{(3)} = (80000001)$ $Z^{(4)} = X_L^{(4)} = (80000180), X_R^{(4)} = (81808001)$ $\tilde{P}^{\mathrm{ALZ}}_{\left(x_L^{(0)}, x_R^{(0)}\right), \left(x_L^{(4)}, x_R^{(4)}\right)} = \frac{1}{8} \cdot \frac{1}{2} \cdot 1 \cdot \frac{1}{4} = 2^{-6}$	$\left(X_L^{(0)}, X_R^{(0)}\right) = (00804001, 80400000)$ $Z^{(1)} = X_L^{(1)} = (00004000), X_R^{(1)} = (80000000)$ $Z^{(2)} = X_L^{(2)} = (00000000), X_R^{(2)} = (80000000)$ $Z^{(3)} = X_L^{(3)} = (80000000), X_R^{(3)} = (80000001)$ $Z^{(4)} = X_L^{(4)} = (80000080), X_R^{(4)} = (80808001)$ $\tilde{P}^{\mathrm{ALZ}}_{\left(x_L^{(0)}, x_R^{(0)}\right), \left(x_L^{(4)}, x_R^{(4)}\right)} = \frac{1}{8} \cdot \frac{1}{2} \cdot 1 \cdot \frac{1}{4} = 2^{-6}$
Соотношение № 5	Соотношение № 6
$\left(X_L^{(0)}, X_R^{(0)}\right) = (80020100, 00010080)$ $Z^{(1)} = X_L^{(1)} = (80000000), X_R^{(1)} = (00010000)$ $Z^{(2)} = X_L^{(2)} = (00000000), X_R^{(2)} = (00010000)$ $Z^{(3)} = X_L^{(3)} = (00010000), X_R^{(3)} = (00030000)$ $Z^{(4)} = X_L^{(4)} = (01010000), X_R^{(4)} = (00030101)$ $\tilde{P}^{\mathrm{ALZ}}_{\left(x_L^{(0)}, x_R^{(0)}\right), \left(x_L^{(4)}, x_R^{(4)}\right)} = \frac{1}{4} \cdot 1 \cdot \frac{1}{2} \cdot \frac{1}{8} = 2^{-6}$	$\left(X_L^{(0)}, X_R^{(0)}\right) = (80020100, 00010080)$ $Z^{(1)} = X_L^{(1)} = (80000000), X_R^{(1)} = (00010000)$ $Z^{(2)} = X_L^{(2)} = (00000000), X_R^{(2)} = (00010000)$ $Z^{(3)} = X_L^{(3)} = (00010000), X_R^{(3)} = (00030000)$ $Z^{(4)} = X_L^{(4)} = (03010000), X_R^{(4)} = (00030301)$ $\tilde{P}^{\mathrm{ALZ}}_{\left(x_L^{(0)}, x_R^{(0)}\right), \left(x_L^{(4)}, x_R^{(4)}\right)} = \frac{1}{4} \cdot 1 \cdot \frac{1}{2} \cdot \frac{1}{8} = 2^{-6}$

4. Разностная встреча посередине для семи и восьми итераций подстановки Alzette

С использованием ЭВМ проведён поиск с.с.л.р.с. для семи (4 плюс 3 первых итерации) и восьми (4 плюс 4) итераций подстановки Alzette. Непосредственно поиск проводился для восьми итераций, а системы для семи итераций строились из найденных систем. В [1] для такого числа итераций приведены только оценки сверху на минус двоичный логарифм максимума разностной характеристики — соответственно 24 и 32.

Алгоритм является разновидностью описанной «разностной встречи посередине». Предварительно были сформированы наборы разностей для сложения $\boxplus$, имеющие вероятности 1, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}. Алгоритм состоит из трёх этапов. Результатами первого и второго этапов являются частичные системы для итераций с третьей по шестую и с третьей по восьмую соответственно. На третьем этапе системы, прошедшие первые два этапа, достраиваются до полных систем для итераций с первой по восьмую.

Первый этап. Фиксируем значения $p_3, p_6 \in \{2^{-k} : k = 0, \ldots, 4\}$. На итерации 3 перебираем все разности, имеющие вероятность p_3, а на итерации 6 — все разности, имеющие вероятность p_6. При их фиксации разности на итерациях 4 и 5 вычисляются однозначно. Таким образом получаем с.с.л.р.с. на итерациях 3–6. Проверяем, что вероятность этой системы больше $p_{\max}$. Если условие не выполняется, то выбираем

следующую пару разностей на третьей и шестой итерациях. Системы, для которых условие выполняется, переходят на второй этап.

В т о р о й э т а п. Для каждой из систем, полученных на первом этапе, перебираем все возможные выходные разности сложения $\boxplus$ на седьмой итерации (входные разности определяются по выходным разностям шестой итерации). Полученные системы на итерации 3–7, разностная характеристика которых превышает $p_{\max}$, достраиваются до системы на восемь итераций так, чтобы максимизировать вероятность системы на итерациях 3–8. Полученные системы на итерации 3–8, разностная характеристика которых превышает $p_{\max}$, переходят на третий этап.

Т р е т и й э т а п аналогичен второму, только перебираются все возможные разности на второй итерации и достраивается (исходя из максимизации разностной характеристики результирующей системы) разность на первой итерации. Построенные таким образом системы, имеющие вероятность больше $p_{\max}$, являются результатом работы алгоритма.

В качестве $p_{\max}$ была выбрана полученная в [1] граница на разностную характеристику системы локальных разностных соотношений на девять итераций, равная 2^{-36}. В табл. 5 приведены сочетания вероятностей p_3, p_6 опробованных пар разностей.

Т а б л и ц а 5

$-\log_2(p_3)\,(-\log_2(p_6))$	$-\log_2(p_6)\,(-\log_2(p_3))$
0 и 1	0 и 1
0 и 1	2
0 и 1	3
0 и 1	4
2	0 и 1
2	2
2	3
2	4

Системы на семь итераций строятся из систем на восемь итераций следующим образом: отбрасывается локальное разностное соотношение восьмой итерации, а соотношение на седьмой итерации заменяется соотношением с максимальной вероятностью выполнения.

Всего получено 11 с.с.л.р.с. на восемь итераций, имеющих разностную характеристику 2^{-35}. Из них построено 6 с.с.л.р.с. на семь итераций, имеющих разностную характеристику 2^{-27}. Полученные соотношения приведены в табл. 6. В табл. 7 в качестве примера приведена одна из полученных систем на восемь итераций.

Таблица 6

Разностные соотношения подстановки Alzette на семь и восемь итераций

№ п/п	Число итераций	$A \in V_{64}$	$B \in V_{64}$	$-\log_2 \tilde{P}^{\mathrm{ALZ}}_{A,B}$
1	7	(00A1508020508040)	(10102080507001A0)	27
2	7	(0021108060108040)	(10102080507001A0)	27
3	7	(00A1508020508040)	(10102080507001A0)	27
4	7	(0021108060108040)	(10102080507001A0)	27
5	7	(210002410080C121)	(410020200340A0E0)	27
6	7	(210002410080C121)	(410020200340A0E0)	27
7	8	(A080410180C000A0)	(81804140C1418141)	35
8	8	(210002410080C121)	(002040204060A0C0)	35
9	8	(210002410080C121)	(00A0002000602040)	35
10	8	(2101000001810020)	(0181018081010080)	35
11	8	(00A1508020508040)	(2010001050602030)	35
12	8	(00A1508020508040)	(0010005010200030)	35
13	8	(0021108060108040)	(0010005010200030)	35
14	8	(4200028501008142)	(0040804080C14180)	35
15	8	(4200028501008142)	(0140004000C04080)	35
16	8	(80001081801000C0)	(80C000C080404080)	35
17	8	(0021108060108040)	(2010001050602030)	35

Таблица 7

Пример системы локальных разностных соотношений на восемь итераций

№ итерации i	$X^{(i-1)} = \left(X_L^{(i-1)}, X_R^{(i-1)}\right)$	$X^{(i-1)} = \left(X_L^{(i)}, X_R^{(i)}\right)$	$-\log_2 P\left(X^{(i-1)} \to X^{(i)}\right)$
1	(21000241, 0080C121)	(20008001, 0000C001)	8
2	(20008001, 0000C001)	(80000001, 00000001)	4
3	(80000001, 00000001)	(80000000, 00000000)	1
4	(80000000, 00000000)	(80000000, 00008000)	0
5	(80000000, 00008000)	(80010000, 01008080)	1
6	(80010000, 01008080)	(C0410080, 8140E0A0)	4
7	(C0410080, 8140E0A0)	(40802020, 0040A0E0)	10
8	(40802020, 0040A0E0)	(00204020, 4060A0C0)	7

5. Оценка трудоёмкости построения разностных соотношений для подстановки Alzette

Трудоёмкость предложенного подхода «разностная встреча посередине» для четырёх итераций подстановки Alzette равна $3^2 \cdot 4 = 36$ вычислений (в соответствии с теоремой 1) вероятностей локальных разностных соотношений на двоичных векторах длины 32 (существенно менее трудоёмкими операциями циклического сдвига и сложения по $\bmod 2$ двоичных векторов длины 32 мы пренебрегаем), для пяти и шести итераций указанная трудоёмкость равна $3^3 \cdot 5 = 135$ и $3^4 \cdot 6 = 486$ операций соответственно (причём это максимальная трудоёмкость — без учёта уже известных результатов по локальным разностным соотношениям для четырёх итераций).

Трудоёмкость алгоритма для восьми итераций в основном определяется трудоёмкостью первого этапа. Для каждой пары опробуемых локальных разностных соотношений необходимо вычислить вероятности локальных разностных соотношений для итераций 4 и 5. Число опробуемых пар рассчитаем при помощи формулы из [6, теорема 2.3]. Если обозначить через $D_n(j)$ число разностных соотношений разрядности n,

имеющих вероятность 2^{-j}, $j \in \{0, \ldots, n\}$, то

$$D_n(j) = 4 \cdot 6^j \binom{n-1}{j}.$$

Тогда общее число опробуемых пар равно

$$\sum_{p_3, p_6} D_{32}(-\log_2(p_3)) D_{32}(-\log_2(p_6)) \approx 2{,}26 \cdot 10^{13}.$$

С учётом двух операций для каждой разности и этапов 2 и 3 общую трудоёмкость нахождения с.с.л.р.с. на восемь итераций можно оценить сверху величиной $5 \cdot 10^{13}$.

Системы на семь итераций строятся из систем на восемь итераций фактически вручную, поэтому в качестве оценки трудоёмкости их построения можно использовать оценку для восьми итераций.

Для сравнения оценим трудоёмкость алгоритма поиска/оценки максимальных разностных характеристик, которым пользовались авторы работы [1]. В [1] не описан алгоритм и не оценена его трудоёмкость, поэтому все выводы сделаны на основе анализа программной реализации [8].

Суть алгоритма состоит в следующем. Последовательно, от младшего разряда к старшему, опробуются локальные разностные соотношения первой итерации и для каждого «частичного» соотношения вычисляется его вероятность. Далее эта вероятность умножается на разностную характеристику наилучшей с.с.л.р.с. на оставшийся «хвост» из итераций 2, 3 и т. д. — таким образом получается оценка сверху на характеристику наилучшей системы локальных разностных соотношений на заданное число итераций, имеющей опробуемое в данный момент начало. Если эта оценка меньше заданной границы p_b, то мы опробуем следующее значение текущего разряда «частичного» локального соотношения или возвращаемся на один разряд назад. Если же оценка не меньше границы p_b, то переходим к следующем разряду. После получения полного локального соотношения на первой итерации повторяем аналогичный процесс на второй итерации с той разницей, что в качестве оценки характеристики текущей опробуемой системы используется произведение вероятности (уже полной) локального соотношения на первой итерации, вероятность «частичного» соотношения на второй итерации и разностная характеристика наилучшей системы на «хвост» из итераций 3, 4 и т. д. Ещё одно отличие: на первой итерации перебираются все три вектора α, β, γ, а на последующих — только γ. В конце концов мы или получаем систему на заданное число итераций с разностной характеристикой не меньше p_b, или убеждаемся, что систем с такой характеристикой на заданное число итераций нет. В последнем случае уменьшаем p_b в 2 раза и повторяем весь алгоритм. В качестве начального значения p_b для r итераций используется значение характеристики наилучшей системы на $(r-1)$ итераций.

Описанный алгоритм предназначен для обоснования криптографических свойств подстановки Alzette при криптографическом синтезе, то есть в случае нахождения системы разностных соотношений с разностной характеристикой p_b утверждается, что систем с бóльшей разностной характеристикой (для данного числа итераций) не существует. Алгоритм разностной встречи посередине ориентирован на криптографический анализ, то есть на нахождение системы разностных соотношений с как можно большей разностной характеристикой за как можно меньшее число операций. Поэтому чтобы сравнить трудоёмкости этих двух алгоритмов, будем рассчитывать трудоёмкость алгоритма из [1], исходя из поиска конкретных систем разностных соотношений.

Оценим снизу трудоёмкость алгоритма из работы [1] следующим образом. Зафиксируем число итераций r. Пусть вероятность искомой системы разностных соотношений на r-й итераций составляет $p^{(1)}$, а наибольшая вероятность разностного соотношения на $(r-1)$ итераций, начиная со второй, — $p^{(2)}$. Это означает, что прежде чем мы дойдём до искомого разностного соотношения, имеющего вероятность $p^{(1)}$, мы должны будем проверить $k = -\log_2\left(p^{(1)}\right) + \log_2\left(p^{(2)}\right)$ ложных границ $p_b = p^{(2)}$, $p^{(2)}/2$, $p^{(2)}/4$, $\ldots$, $p^{(2)}/2^{k-1}$. Для каждой из этих ложных границ мы будем как минимум перебирать все разности первой итерации, имеющие «разрешённую» вероятность $p_1 \in \left\{1, 1/2, \ldots, p^{(1)}/p^{(2)}\right\}$, и для каждой из них вычислять эту вероятность 32 раза (при добавлении каждого разряда разности). Таким образом, будет произведено не менее $S(k)$ вычислений вероятности разностного соотношения, где

$$S(k) = 32 \sum_{i=0}^{k-1} \sum_{j=0}^{i} D_{32}(j). \tag{1}$$

Как видно из формулы (1), величина $S(k)$ зависит только от k, по сути — от отношения $p^{(1)}/p^{(2)}$, поэтому если при разных r значения k одинаковые, то и величины $S(k)$ тоже одинаковы. В этом случае чтобы подчеркнуть, что $S(k)$ больше при большем r, будем учитывать, что значение $p^{(2)}$ должно быть определено по аналогичному алгоритму с использованием значения $p^{(3)}$ — наибольшей вероятности разностного соотношения на $(r-2)$ итераций, начиная с третьей. Соответствующая трудоёмкость будет не меньше чем $S(k')$, где $k' = -\log_2\left(p^{(2)}\right) + \log_2\left(p^{(3)}\right)$.

В табл. 8 приведены значения $-\log_2\left(p^{(i)}\right)$, $i = 1, 2, 3$. В ней:

— значения $p^{(1)}$ — разностные характеристики конкретных найденных систем разностных соотношений;
— значения $p^{(2)}$ для четырёх, пяти и шести итераций и $p^{(3)}$ для пяти и восьми итераций взяты из [1, табл. 2] (см. табл. 3 и 6);
— в качестве $p^{(2)}$ для восьми итераций взято значение границы из [1, табл. 2];
— значения k — разности значений второй и третьей колонок;
— значения k' — разности значений третьей и четвёртой колонок;
— значения $p^{(3)}$ и k' приведены только для такого числа итераций, у которых k совпадает с k для предыдущего числа.

Таблица 8

Число итераций	$-\log_2(p^{(1)})$	$-\log_2(p^{(2)})$	$-\log_2(p^{(3)})$	k	k'
4	6	2	–	4	–
5	10	6	2	4	4
6	18	10	–	8	–
7	27	17	–	10	–
8	35	25	18	10	7

Окончательно получаем: если обозначить через S_r оценку снизу трудоёмкости алгоритма из работы [1], то имеет место следующее выражение:

$$S_r = \begin{cases} S(k), & r \in \{4, 6, 7\}, \\ S(k) + S(k'), & r \in \{5, 8\}, \end{cases}$$

где k, k' зависят от r и берутся из табл. 8. Численные значения S_r и оценки сверху на трудоёмкость разностной встречи посередине приведены в табл. 9.

Таблица 9

Число итераций r	S_r	Трудоёмкость РВП (оценка сверху)
4	$1{,}29 \cdot 10^8$	36
5	$2 \cdot 1{,}29 \cdot 10^8$	135
6	$1{,}03 \cdot 10^{14}$	486
7	$2{,}97 \cdot 10^{16}$	$5 \cdot 10^{13}$
8	$2{,}97 \cdot 10^{16} + 4{,}75 \cdot 10^{12}$	$5 \cdot 10^{13}$

Заключение

В работе с использованием предложенного подхода «разностная встреча посередине» для подстановки Alzette с четырьмя и пятью итерациями получены все согласованные системы локальных разностных соотношений, соответствующие максимальному значению разностной характеристики этой подстановки. Для подстановки Alzette с шестью итерациями получена одна система с максимальной разностной характеристикой. Разностные соотношения для четырёх и пяти итераций, соответствующие данным согласованным системам (без указания самих этих систем), получены ранее разработчиками подстановки Alzette с использованием вычислений на ЭВМ.

Построены согласованные системы локальных разностных соотношений для семи и восьми итераций подстановки Alzette, разностные характеристики которых лишь незначительно отличаются от оценок сверху, полученных в [1]. Показано, что в задаче построения разностного соотношения с как можно бóльшим значением разностной характеристики за как можно меньшее число операций разностная встреча посередине обладает меньшей трудоёмкостью, чем алгоритм, использованный в [1] для обоснования криптографических характеристик подстановки Alzette.

Подход «разностная встреча посередине», использующий математический аппарат формальных рядов с коэффициентами из поля действительных чисел, позволяет относительно просто находить согласованные системы локальных разностных соотношений, имеющие максимальное значение разностной характеристики. Полученные результаты могут быть использованы, например, при оценке характеристик криптографических примитивов, построенных с использованием подстановки Alzette.

ЛИТЕРАТУРА

1. *Beierle C., Biryukov A., Cardoso dos Santos L., et al.* Alzette: A 64-bit ARX-box. Cryptology ePrint Archive. Report 2019/1378. 2019. `https://eprint.iacr.org/2019/1378`.
2. *Canteaut A., Duval S., Leurent G., et al.* Saturnin: a suite of lightweight symmetric algorithms for post-quantum security. `https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/saturnin-spec-round2.pdf`.
3. *Dinu D., Perrin L., Udovenko A., et al.* Design strategies for ARX with provable bounds: Sparx and LAX // LNCS. 2016. V. 10031. P. 484–513.
4. *Biryukov A., Velichkov V., and Corre Y. L.* Automatic search for the best trails in ARX: Application to block cipher Speck // LNCS. 2016. V. 9783. P. 289–310.
5. *Малышев Ф. М.* Вероятностные характеристики разностных и линейных соотношений для неоднородной линейной среды // Математические вопросы криптографии. 2019. Т. 10. Вып. 1. С. 41–72.
6. *Wallèn J.* On the differential and linear properties of addition. Research Report A84. Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, 2003. 58 p.

7. *Малышев Ф. М., Трифонов Д. И.* Рассеивающие свойства XSLP-шифров // Математические вопросы криптографии. 2016. Т. 7. Вып. 3. С. 47–60.
8. https://github.com/cryptolu/sparkle.

REFERENCES

1. *Beierle C., Biryukov A., Cardoso dos Santos L., et al.* Alzette: A 64-bit ARX-box. Cryptology ePrint Archiv, Report 2019/1378, 2019. https://eprint.iacr.org/2019/1378.
2. *Canteaut A., Duval S., Leurent G., et al.* Saturnin: a suite of lightweight symmetric algorithms for post-quantum security. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/saturnin-spec-round2.pdf.
3. *Dinu D., Perrin L., Udovenko A., et al.* Design strategies for ARX with provable bounds: Sparx and LAX. LNCS, 2016, vol. 10031, pp. 484–513.
4. *Biryukov A., Velichkov V., and Corre Y. L.* Automatic search for the best trails in ARX: Application to block cipher Speck. LNCS, 2016, vol. 9783, pp. 289–310.
5. *Malyshev F. M.* Veroyatnostnye kharakteristiki raznostnykh i lineynykh sootnosheniy dlya neodnorodnoy lineynoy sredy [Probabilistic characteristics of differential and linear relations for nonhomogeneous linear medium]. Matematicheskie Voprosy Kriptografii, 2019, vol. 10, iss. 1, pp. 41–72. (in Russian)
6. *Wallèn J.* On the differential and linear properties of addition. Research Report A84, Helsinki University of Technology, Laboratory for Theoretical Computer Science, Espoo, Finland, 2003. 58 p.
7. *Malyshev F. M. and Trifonov D. I.* Rasseivayushchie svoystva XSLP-shifrov [Diffusion properties of XSLP-ciphers]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, iss. 3, pp. 47–60. (in Russian)
8. https://github.com/cryptolu/sparkle.