конференция
РусКрипто

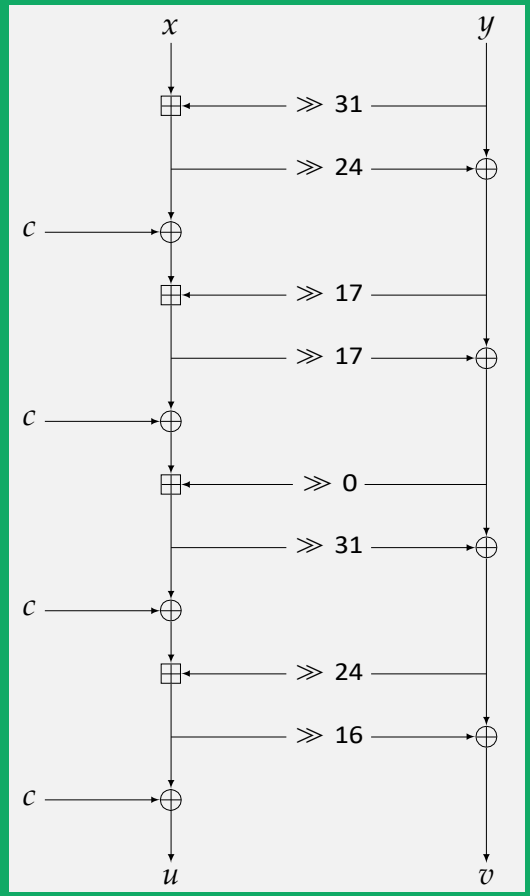
Ежегодная международная научно-практическая конференция
«РусКрипто'2022»

О поиске разностных соотношений для подстановки ALZETTE с максимальным или близким к нему значением разностной характеристики

Андрей Александрович Дмух, Дмитрий Олегович Пасько
Академия криптографии Российской Федерации

Подстановка ALZETTE

- Beierle, C., Biryukov, A., Cardoso dos Santos, L., Grosschadl, J., Perrin, L., Udovenko, A., Velichkov, V., Wang, Q. Alzette: A 64-bit ARX-box. Cryptology ePrint Archive, Report 2019/1378, https://eprint.iacr.org/2019/1378
- Увеличение числа итераций производится по циклу: 1,2,3,4,1,2,3,4….



Разностные характеристики

- Точное значение вероятности выполнения разностного соотношения $A, B \in V_{64} : P_{A,B}^{ALZ} = P_x\left(ALZ\left(x\right) \oplus ALZ\left(x \oplus A\right) = B\right)$
- Вычислять точное значение сложно, поэтому в качестве приближения используем оценку $P_{A,B}^{ALZ} = \prod p_i$, где p_i – вероятность выполнения локального соотношения на i-й итерации
- Локальные соотношения на разных итерациях должны быть *согласованы,* т.е. входная разность следующей итерации должна быть равна выходной разности предыдущей итерации
- $\max\limits_{A,B \in V_{64}} P_{A,B}^{ALZ}$ будем называть разностной характеристикой подстановки ALZETTE
- F.M. Malyshev, A.E. Trishin. Linear and differential cryptanalysis: Another viewpoint. Mat. Vopr. Kriptogr., 2020, Volume 11, Issue 2, pp. 83-98.

Разностные характеристики

- Вероятность выполнения разностного соотношения для линейного преобразования вычисляется тривиально и равна либо 0, либо 1
- Единственное нелинейное преобразование в подстановке ALZETTE – сложение по модулю 2^{32}
- Wallèn, J. «On the differential and linear properties of addition» – вычисление точного значения вероятности выполнения разностного соотношения для сложения по модулю 2^{32} с использованием математического аппарата формальных рядов с коэффициентами из поля действительных чисел

Решаемые задачи

- Апробация метода разностной встречи посередине
- Построение полных согласованных систем локальных разностных соотношений на 4, 5 и 6 итераций без вычислений на компьютере.
- Построение полных согласованных систем локальных разностных соотношений на 7 и 8 итераций с характеристиками, близкими к максимальным

Разностные характеристики подстановки ALZETTE

- Разработчиками подстановки ALZETTE с использованием компьютера получены некоторые значения разностных характеристик
- Для 4 и 5 итераций приведены конкретные разностные соотношения, для 6 и далее - нет.

Число итераций	$-\log_2 P_{A,B}^{ALZ}$
1	0
2	1
3	2
4	6
5	10
6	18
7	≥ 24
8	≥ 32

Метод разностной встречи посередине

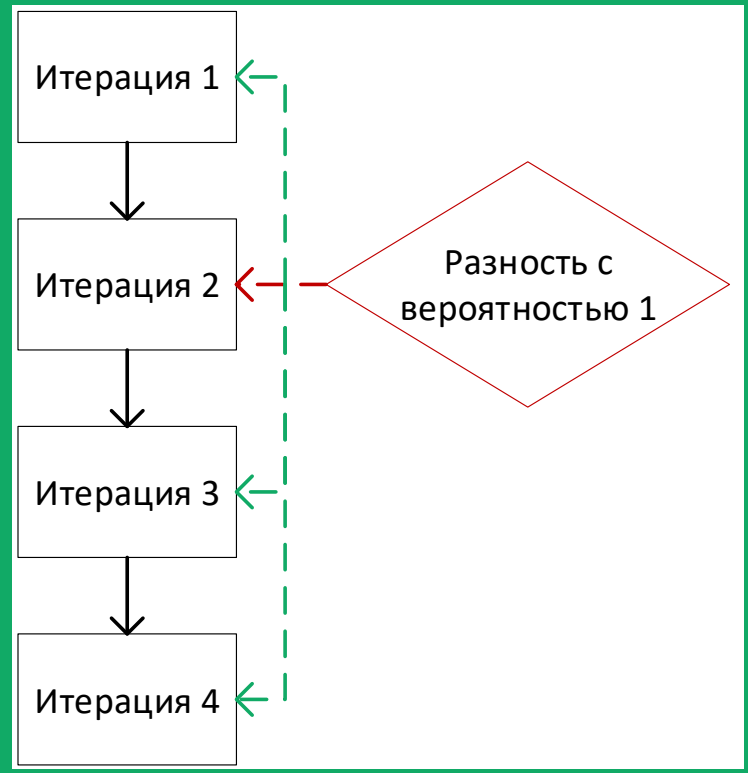
- Цель разработчиков ALZETTE – криптографический синтез, оценка криптографической стойкости «снизу»
- Наша цель – криптографический анализ, поиск разностного соотношения с как можно бо̀льшим значением разностной характеристики за как можно меньшее число операций

Метод разностной встречи посередине

- Опробуем на средних итерациях подстановки ALZETTE локальные разностные соотношения, имеющие высокую вероятность выполнения
- Протягиваем эти соотношения на первые и последние итерации таким образом, чтобы получать на этих итерациях локальные разностные соотношения с максимально возможными вероятностями выполнения

Разностная встречи посередине на 4 итерации подстановки ALZETTE

- Опробуем на второй (или на третьей) итерации разностные соотношения, имеющие вероятность выполнения 1
- Достраиваем эти соотношения на первую и последние итерации локально-оптимально , т.е. максимизируя вероятность выполнения разностного соотношения на каждой итерации отдельно



Полученные разностные соотношения на 4, 5 и 6 итераций

№	Число итераций	$A \in V_{64}$	$B \in V_{64}$	$-\log_2 P_{A,B}^{ALZ}$
1	4	(8000010000000080)	(804041041004041)	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
9	6	(a0008140000040a0)	(43408102408 0a323)	18

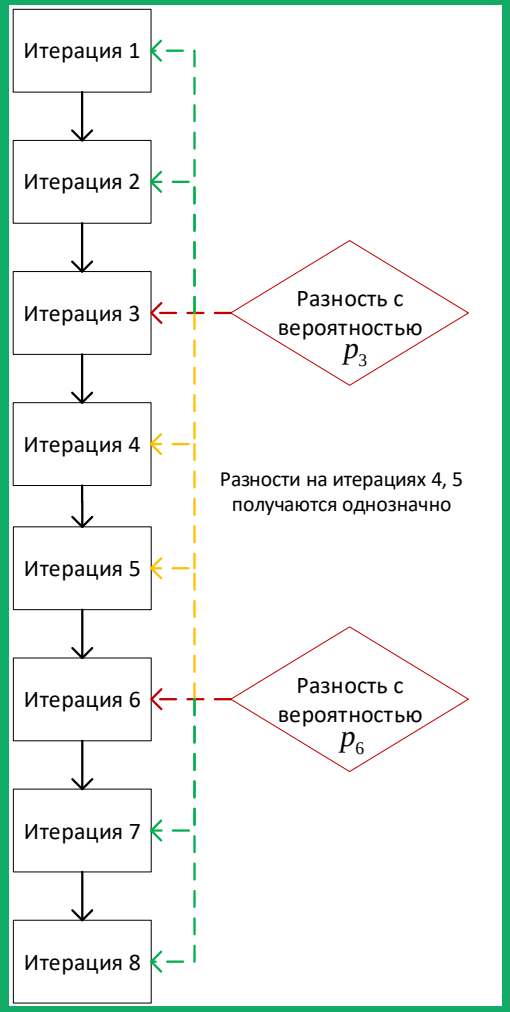
- Также получены соответствующие согласованные системы локальных разностных соотношений

Разностная встреча посередине на 8 итерации подстановки ALZETTE

- Вероятности $p_3, p_6 \in \left\{1, \frac{1}{2}, \ldots, \frac{1}{2^4}\right\}$

$-\log(p_3)(-\log p_6)$	$-\log(p_6)(-\log p_3)$
0 и 1	0 и 1
…	…
0 и 1	4
2	0 и 1
…	…
2	4

- На 2-й и 7-й итерациях перебираются все разности, согласованные с системой 3-6
- На 1-й и 8-й максимизируем вероятность



Полученные разностные соотношения на 8 итераций

№	$A \in V_{64}$	$B \in V_{64}$	$-\log_2 P_{A,B}^{ALZ}$
1	(a080410180c000a0)	(81804140c1418141)	35
2	(210002410080c121)	(00204020406 0a0c0)	35
3	(210002410080c121)	(00a000200602040)	35
4	(210100001810020)	(018101808 1010080)	35
5	(00a1508020508040)	(2010001050602030)	35
6	(00a1508020508040)	(0010005010200030)	35
7	(002110806 0108040)	(0010005010200030)	35
8	(420002850 1008142)	(0040804080c14180)	35
9	(420002850 1008142)	(0140004000c04080)	35
10	(8000108 1801000c0)	(80c000c080404080)	35
11	(002110806 0108040)	(2010001050602030)	35

- Также получены соответствующие согласованные системы локальных разностных соотношений

Полученные разностные соотношения на 7 итераций

- Системы на 7 итераций строятся из систем на 8 итераций, достаточно отбросить соотношение на 8-й итерации и максимизировать вероятность соотношения на 7-й итерации

№	$A \in V_{64}$	$B \in V_{64}$	$-\log_2 P_{A,B}^{ALZ}$
1	(00a1508020508040)	(1010208050700 1a0)	27
2	(002110806010 8040)	(1010208050700 1a0)	27
3	(00a1508020508040)	(1010208050700 1a0)	27
4	(002110806010 8040)	(1010208050700 1a0)	27
5	(210002410080c121)	(410020200340a0e0)	27
6	(210002410080c121)	(410020200340a0e0)	27

- Также получены соответствующие согласованные системы локальных разностных соотношений

Трудоемкость разностной встречи посередине на 4, 5 и 6 итераций

- За одну операцию считаем вычисление вероятности выполнения локального разностного соотношения
- Для 4-х итераций – 36 операций
- Для 5-и итераций – 135 операций
- Для 6-и итераций – 486 операций
- Это максимальная трудоемкость, на практике все приведенные разностные соотношения были построены вручную, без вычислений на компьютере

Трудоемкость разностной встречи посередине на 8 итераций

- В работе Wallèn, J. «On the differential and linear properties of addition» приведена формула для вычисления количества разностных соотношений, имеющих заданную вероятность выполнения
- Общее число опробованных разностей $\sim 2.26 \cdot 10^{13}$ пар
- Для получения системы локальных разностных соотношений на итерации 3-6 необходимо 2 раза вычислить вероятность выполнения локального соотношения (на 4-й и 5-й итерациях)
- Трудоемкость достраивания системы на итерации 1, 2, 7 и 8 пренебрежимо мала по сравнению с числом опробуемых разностей
- Общая трудоемкость - не более $5 \cdot 10^{13}$ операций

Трудоемкость разностной встречи посередине на 7 итераций

- Системы на 7 итераций вычислялись из систем на 8 итераций вручную – трудоемкость низкая

Оценка трудоемкости алгоритма разработчиков подстановки ALZETTE

- В исходной работе трудоемкость алгоритма не оценивается
- Наша оценки на основе анализа программы

Число итераций	Трудоемкость, операций	Трудоемкость РВП, операций
4	$>1.29\cdot10^{8}$	36
5	$>2\cdot1.29\cdot10^{8}$	135
6	$>1.03\cdot10^{14}$	486
7	$>2.97\cdot10^{16}$	$\leq 5\cdot10^{13}$
8	$>2.97\cdot10^{16}+4.75\cdot10^{12}$	$\leq 5\cdot10^{13}$

- Для 5 и 8 итераций учтено, что для работы алгоритма необходимо получить системы с наибольшей разностной характеристикой для 4 и 7 итераций соответственно, начиная со 2-й

Выводы

- С использованием подхода «разностная встреча посередине» без вычислений на компьютере получены все разностные соотношения с максимальной разностной характеристикой для подстановки ALZETTE с 4 и 5 итерациями, а также одно разностное с максимальной разностной характеристикой для подстановки с 6 итерациями.
- Для подстановки ALZETTE с 7 и 8 итерациями получены разностные соотношения с разностными характеристиками, близкими к верхними границам, полученным разработчиками подстановки
- Подход «разностной встречи посередине» при криптографическом анализе имеет меньшую трудоемкость, чем подход разработчиков подстановки ALZETTE, использованный для обоснования криптографических качеств подстановки

Вопросы

???