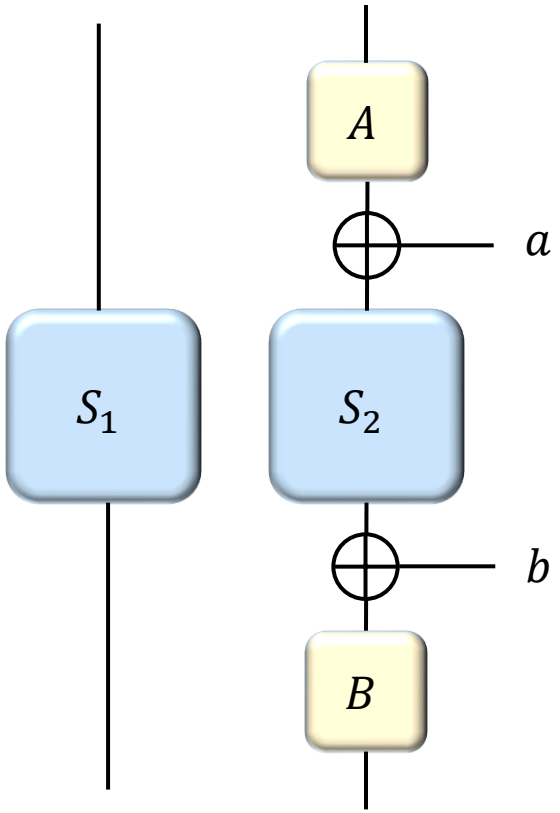
КРИПТОНИТ

Поиск эффективно реализуемых подстановок с оптимальными криптографическими характеристиками

Чичаева Анастасия

Две подстановки S_1 и S_2 называются аффинно эквивалентными если существуют такие линейные отображения A, B и константы a и b, что:

$$S_1(x) = B(S_2(Ax \oplus a) \oplus b),$$
$$\forall x \in \{0,1\}^n$$



- Линейная характеристика:

$$l_s = \max_{\substack{\alpha,\beta \neq 0^n, \\ \alpha,\beta \in V_n}} |2 \cdot P\{(S(x), \beta) = (x, \alpha)\} - 1|$$

- Дифференциальная характеристика:

$$\Delta_s = \max_{\substack{\alpha,\beta \neq 0^n, \\ \alpha,\beta \in V_n}} P\{S(x) \oplus S(x \oplus \alpha) = \beta\}$$

- Алгебраическая степень:

$$\lambda_s = \min_{\substack{\beta \neq 0^n, \\ \beta \in V_n}} \deg(S(x), \beta)$$

4-битовые подстановки

- 4-битовые подстановки разбиваются на 302 класса аффинной эквивалентности

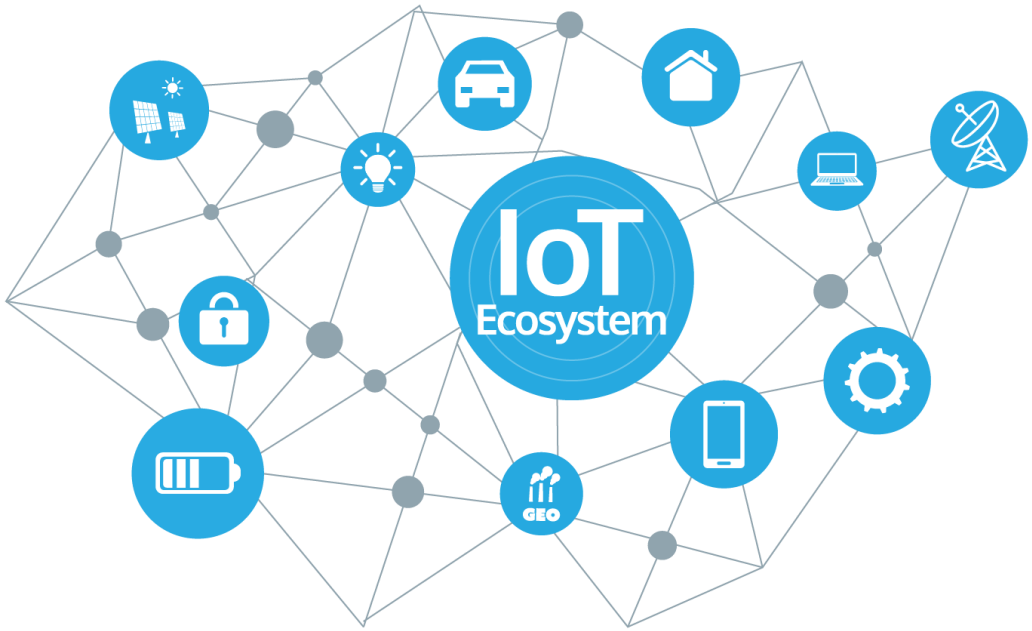
- Оптимальные характеристики 4-битовых подстановок:

$$l_s = \frac{1}{2}, \qquad \Delta_s = \frac{1}{4}, \qquad \lambda_s = 3$$

- 16 оптимальных классов

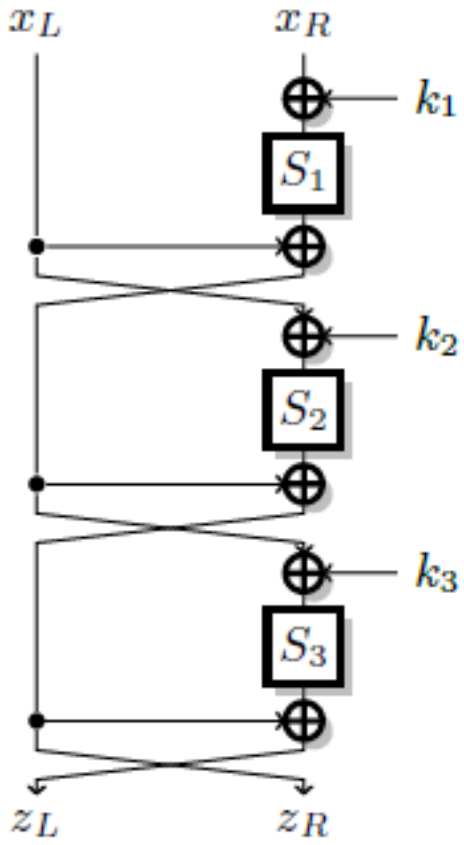
4-битовые подстановки используются в алгоритмах:

- Магма
- LUFFA
- Serpent
- Present
- ...

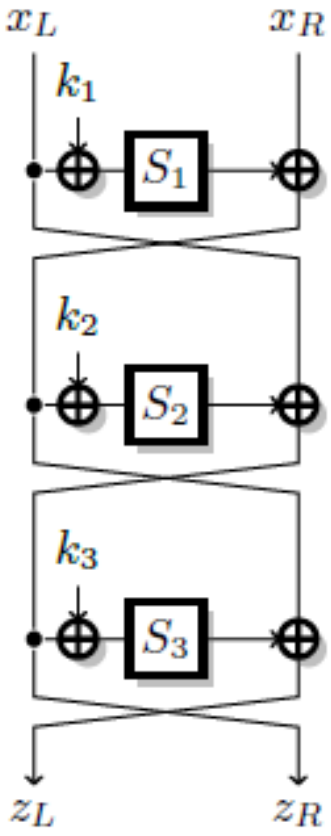


Более 22 кандидатов конкурса NIST низкоресурсных криптографических механизмов используют 4-битовые подстановки

4-битовые подстановки



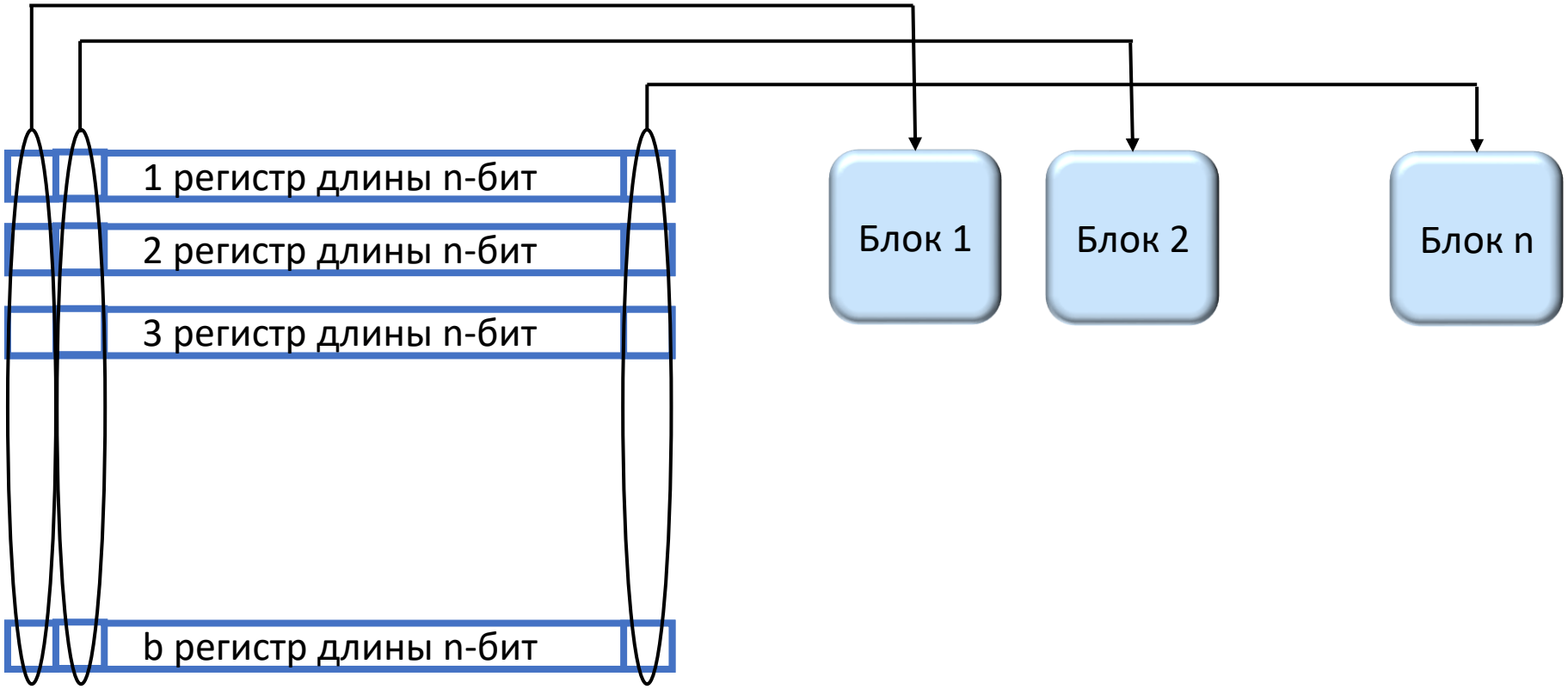
3-раундовая сеть MISTY



3-раундовая сеть Фейстеля

[1] Canteaut A., Duval S., Leurent G. Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version) //IACR Cryptol. ePrint Arch. – 2015. – Т. 2015. – С. 711.

Bitslice реализация



n: размер регистра = число блоков
b: размер блока = число регистров

Поиск битового представления подстановок

В работе [2] проведен систематический поиск эффективных представителей классов аффинной эквивалентности 4-битовых подстановок

Были найдены эффективные представители для 272 из 302 классов эквивалентности

Класс	**Представитель**	Δ_s	l_s	λ_s	Число инструкций
1	?	1/4	1/2	3	?
2	?	1/4	1/2	3	?
3	?	1/4	1/2	3	?
4	?	1/4	1/2	3	?
5	?	1/4	1/2	3	?
6	?	1/4	1/2	3	?
7	?	1/4	1/2	3	?
8	?	1/4	1/2	3	?
9	0cabf9d4e8635172	1/4	1/2	3	11
10	01298bd7cfe654a3	1/4	1/2	3	12
11	0a43562edfb1c789	1/4	1/2	3	13
12	?	1/4	1/2	3	?
13	086d5f7c4e2391ba	1/4	1/2	3	9
14	086c7e5f4d21b39a	1/4	1/2	3	10
15	0845d7fec6a391b2	1/4	1/2	3	10
16	01a2987cdef4563b	1/4	1/2	3	11

[2] Markus Ullrich, Christophe De Canni`ere, Sebastiaan Indesteege, Nicky Mouha, and Bart Preneel, Finding Optimal Bitsliced Implementations of4 x 4-bit S-boxes

Поиск битового представления подстановок

В работе [3] ведётся поиск подстановок, представимых с помощью инструкций AND и XOR

Использование только инструкций AND и XOR облегчает создание «пороговой» реализации, предназначенной для противостояния атакам, использующим информацию, полученную из побочных каналов

Авторы довели поиск до 8 инструкций

[3] Clavier C., Reynaud L. Systematic and Random Searches for Compact 4-Bit and 8-Bit Cryptographic S-Boxes : дис. – IACR Cryptology ePrint Archive, 2019.

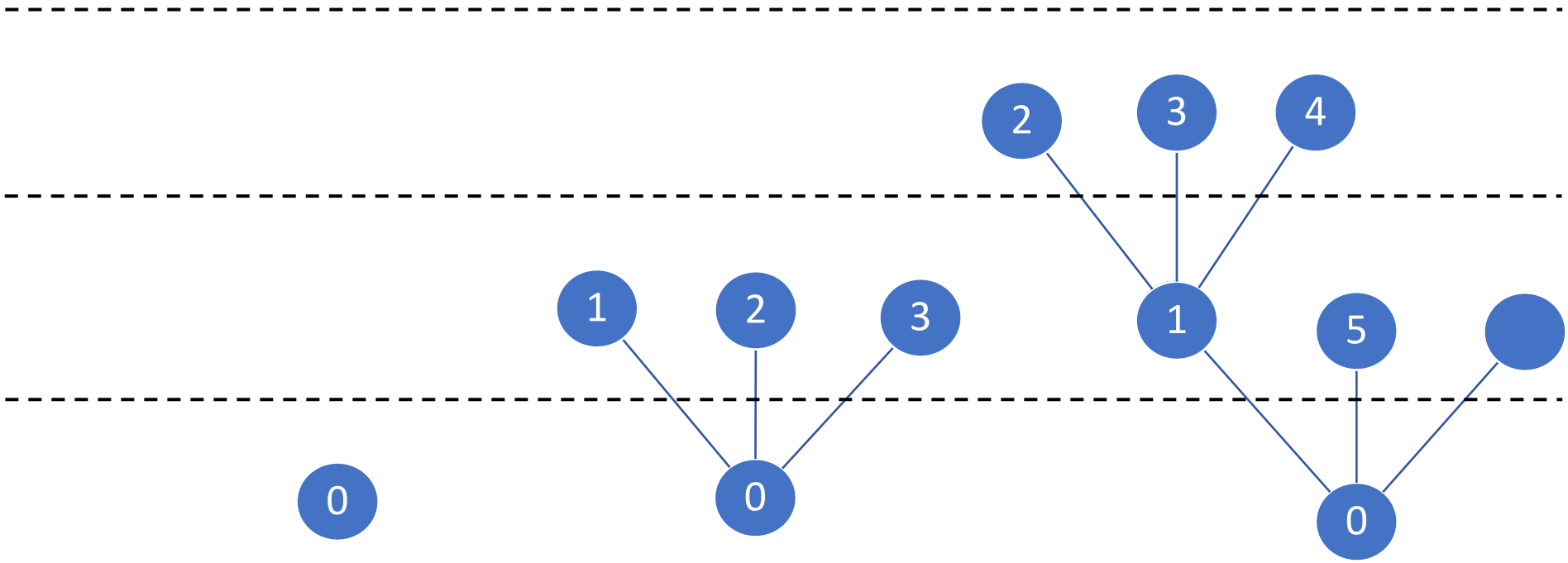
Процедура поиска эффективно реализуемых подстановок из 30 классов разделяется на два этапа:

Первый этап

- На первом этапе используется подход из работы [3]
- Ведётся систематический перебор всех возможных комбинаций инструкций AND, XOR
- Рассматриваются комбинации из 1 - 8 инструкций
- Для представления подстановок используются 5 регистров длины 16 бит

[3] Clavier C., Reynaud L. Systematic and Random Searches for Compact 4-Bit and 8-Bit Cryptographic S-Boxes : дис. – IACR Cryptology ePrint Archive, 2019.

Обход графа в глубину с итеративным углублением



Второй этап поиска

Поиск подстановок из искомых классов аффинной эквивалентности, представимых 11, 12, 13 и более инструкциями.

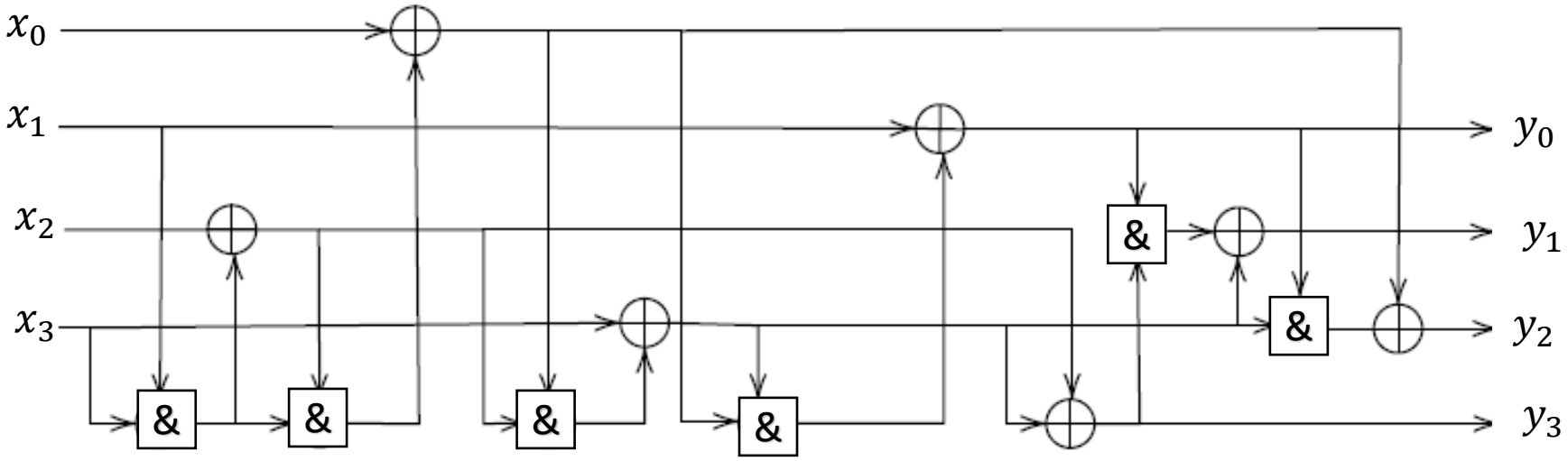
Для этого берутся преобразования, полученные за 8 и меньше инструкций, и рассматривается их суперпозиция

Результат суперпозиции проверяется на аффинную эквивалентность подстановкам из 30 целевых классов

Результаты

№ класса	Представитель	δ_s	l_s	λ_s	Число инструкций
22	095d23b8471a6cef	$\frac{3}{8}$	$\frac{1}{2}$	3	10
74	031ec2fb45a786d9	$\frac{3}{8}$	$\frac{3}{4}$	3	11
12	071e283b4a95dcf6	$\frac{1}{4}$	$\frac{1}{2}$	3	11
42	083e2d1a4c57f9b6	$\frac{3}{8}$	$\frac{3}{4}$	3	11
1	012385be47dfc6a9	$\frac{1}{4}$	$\frac{1}{2}$	3	12
4	0ef285b74613c9da	$\frac{1}{4}$	$\frac{1}{2}$	3	12
2	041583b6a9f72cde	$\frac{1}{4}$	$\frac{1}{2}$	3	13
5	0958a23e4cbf6d17	$\frac{1}{4}$	$\frac{1}{2}$	3	13
7	05932f7c8d61b4ae	$\frac{1}{4}$	$\frac{1}{2}$	3	13
8	095d723f461ebc8a	$\frac{1}{4}$	$\frac{1}{2}$	3	13

Класс 2 041583b6a9f72cde



КРИПТОНИТ

Спасибо за внимание!

Чичаева Анастасия,

Электронная почта: a.chichaeva@kryptonite.ru