ИСПОЛЬЗОВАНИЕ АЛГОРИТМА ПОИСКА ПРЕДСТАВИТЕЛЯ МНОЖЕСТВА АФФИННО-ЭКВИВАЛЕНТНЫХ S-БЛОКОВ ДЛЯ ОЦЕНКИ ИХ КАЧЕСТВА

Н.П. Борисенко
Б.Д. Дударев
Email: npbor@yandex.ru

Алгоритм поиска представителя множества аффинно-эквивалентных S-блоков

X8	X4	X2	X1	Y8	Y4	Y2	Y1
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	1
0	0	1	1	1	1	1	0
0	1	0	0	1	1	0	1
0	1	0	1	1	0	1	1
0	1	1	0	0	1	1	1
0	1	1	1	0	1	1	0
1	0	0	0	1	1	1	1
1	0	0	1	0	0	1	0
1	0	1	0	1	1	0	0
1	0	1	1	0	1	0	1
1	1	0	0	1	0	1	0
1	1	0	1	0	1	0	0
1	1	1	0	0	0	1	1
1	1	1	1	1	0	0	0

Для поиска представителя, алгоритм, описанный в [Alex Birykov, Christophe De Cannere**, An Braeken**, and Barn Prenell. A Toolbox for Cryptanalysis: Linear and Affine Equivalent Algorithms* - In Advances in Cryptology - EUROCRYPT 2003, volume 2656, pages 33–50. Springer, 2003], использует следующий подход:

Исходный S-блок, имеющий n входов, представляется в виде таблиц истинности составляющих его компонентных функций. Каждая строка полученной таблицы рассматривается как число, что позволяет решить задачу поиска представителя путем перестановки строк данной таблицы.

Пусть R_0 – представитель класса S^0 аффинно-эквивалентных S-блоков. Любой S-блок из класса S^0 можно задать двумя преобразованиями A и B из аддитивной группы преобразований (*Affine General Linear Group*, *AGL*).

$$S = B \circ R_0 \circ A$$

Зная R_0 можно получить любой S-блок из S^0. Соответственно, каждому S-блоку данного множества можно сопоставить уникальную комбинацию невырожденных матриц A и B. Сгруппировав S-блоки, получаемые из R_0 аффинно-эквивалентными преобразованиями по значениям матриц A и B, составим модель представления множества аффинно-эквивалентных S-блоков.

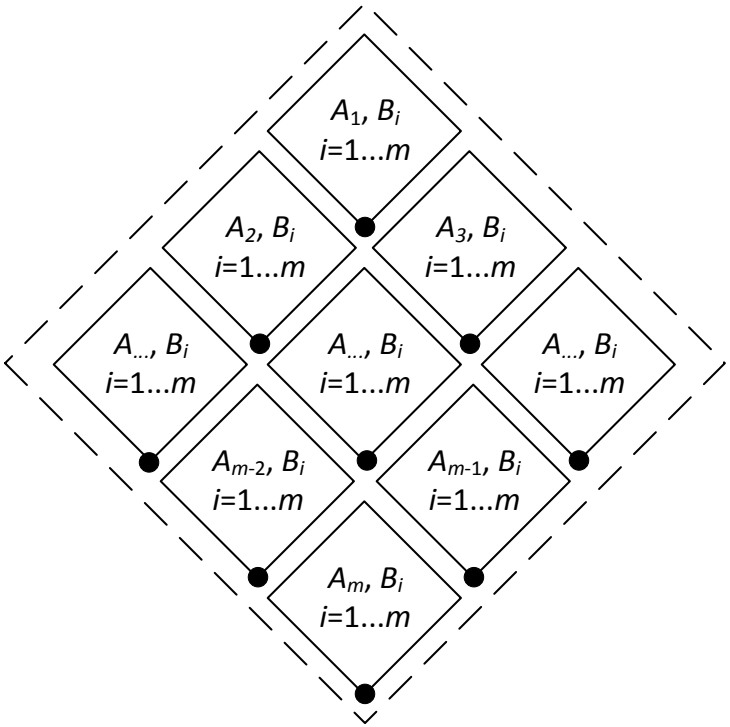
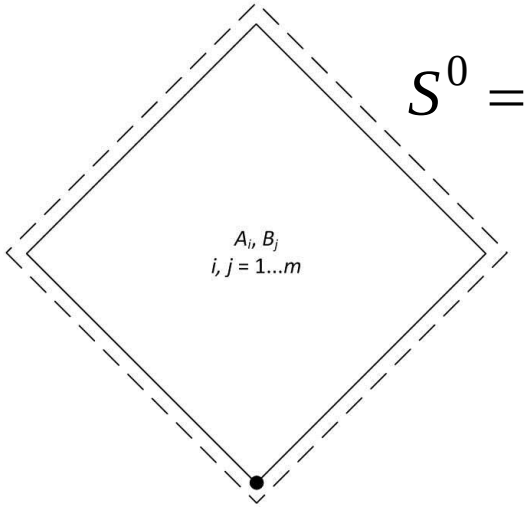


Рис.1. Модель представления множества аффинно-эквивалентных S-блоков.

На данном рисунке все множество аффинно-эквивалентных S-блоков показано пунктирной линией. Ромбами внутри данного множества показаны подмножества S-блоков, имеющие при получении из R_0 одинаковые матрицы A и все возможные значения матрицы B. Точки внизу ромбов – минимальные представители данных подмножеств или локальные представители всего множества. Точка внизу рисунка – искомый представитель R_0.

Множества аффинно-эквивалентных S-блоков



$$S^0 = \prod_{i=1}^{n} (2^{n+1} - 2^i)$$

Рис. 2. Линейный S-блок

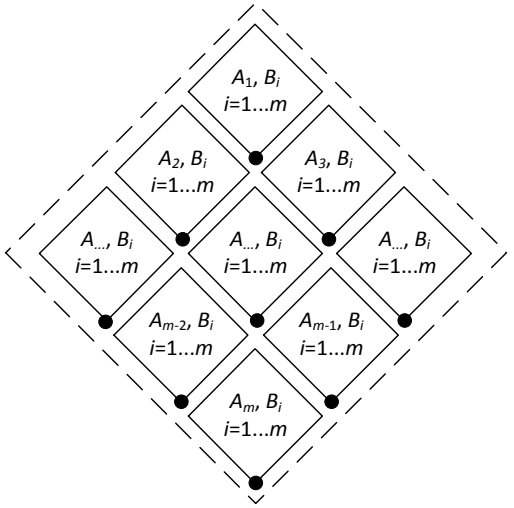
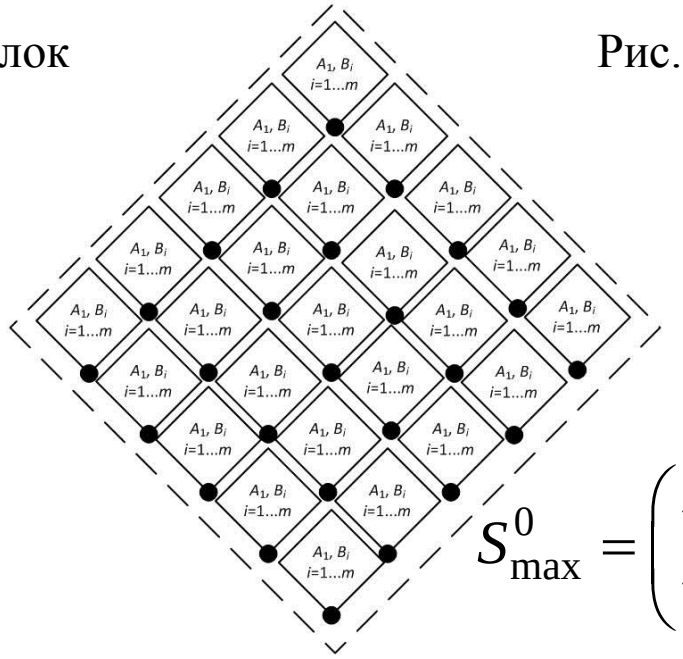


Рис. 3. Слабо нелинейный S-блок



$$S^0_{\max} = \left(\prod_{i=1}^{n} (2^{n+1} - 2^i) \right)^2$$

Рис. 3. Существенно нелинейный S-блок

Формальная постановка задачи

Исходные данные:

S-блок произвольной структуры.

Требуется разработать алгоритм поиска (оценки) количества подмножеств различных аффинно-эквивалентных подстановок (количество различных представителей) во всем множестве S-блоков, получаемых за счет применения аффинных преобразований на входе и выходе заданного S-блока и на его основе:

1) сформулировать показатель(и) оценки качества S-блоков;

2) сравнить характеристики различных S-блоков на основе этого(этих) показателя(ей);

3) оценить значимость полученных результатов.

X8	X4	X2	X1	Y8	Y4	Y2	Y1
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	1
0	0	1	1	1	1	1	0
0	1	0	0	1	1	0	1
0	1	0	1	1	0	1	1
0	1	1	0	0	1	1	1
0	1	1	1	0	1	1	0
1	0	0	0	1	1	1	1
1	0	0	1	0	0	1	0
1	0	1	0	1	1	0	0
1	0	1	1	0	1	0	1
1	1	0	0	1	0	1	0
1	1	0	1	0	1	0	0
1	1	1	0	0	0	1	1
1	1	1	1	1	0	0	0

1. Для поиска представителя, S-блок, имеющий n входов, представляется в виде таблиц истинности составляющих его компонентных функций. В отличие от алгоритма описанного в [A Toolbox for Cryptanalysis: Linear and Affine Equivalent Algorithms*], таблица истинности, формирующая S-блок, рассматривается по столбцам, то есть, как n чисел системы счисления с основанием:

$$M = 2^{2^n}$$

2. На следующем этапе для компонентных функций, составляющих S-блок, строится множество линейных комбинаций и их инверсий (L). Мощность которого равна:

$$\#L = 2^{n+1}-2$$

3. Для каждого элемента данного множества в соответствии с вышеописанными соображениями рассчитывается вес.

4. Далее из полученного множества выбирается n минимальных линейно-независимых функций для построения нового S-блока. Перед выбором очередной минимальной функции из множества L необходимо исключить линейные комбинации и их инверсии для минимальных функций, отобранных ранее, за счет чего, собственно, и достигается линейная независимость компонентных булевых функций, составляющих новый S-блок.

5. Рассчитывается вес полученного S-блока.

Пример поиска представителя

Исходный S-блок, записанный в виде таблицы истинности компонентных функций:

X8	X4	X2	X1	Y8	Y4	Y2	Y1
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	1
0	0	1	1	1	1	1	0
0	1	0	0	1	1	0	1
0	1	0	1	1	0	1	1
0	1	1	0	0	1	1	1
0	1	1	1	0	1	1	0
1	0	0	0	1	1	1	1
1	0	0	1	0	0	1	0
1	0	1	0	1	1	0	0
1	0	1	1	0	1	0	1
1	1	0	0	1	0	1	0
1	1	0	1	0	1	0	0
1	1	1	0	0	0	1	1
1	1	1	1	1	0	0	0

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Вес
0	0	1	1	1	1	0	0	1	0	1	0	1	0	0	1	15529
0	0	0	1	1	0	1	1	1	0	1	1	0	1	0	0	7092
0	0	0	1	0	1	1	1	1	1	0	0	1	0	1	0	6090
0	1	1	0	1	1	1	0	1	0	0	1	0	0	1	0	28306

Множество линейных комбинаций и их инверсий компонентных функций S-блока:

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1
0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	1	1	0	0	1	1	1	1	0
0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	1	0	1
0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	0	1	1	0	0	1	1
0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1
1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1
1	1	0	0	1	1	0	0	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1	1	1	0	0	1	1	0
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0
1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

Пример поиска представителя

X8	X4	X2	X1	Y8	Y4	Y2	Y1
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	0
0	0	1	1	0	1	0	0
0	1	0	0	1	0	0	0
0	1	0	1	1	1	1	1
0	1	1	0	0	1	1	0
0	1	1	1	0	1	1	1
1	0	0	0	0	1	0	1
1	0	0	1	1	1	0	1
1	0	1	0	1	0	0	1
1	0	1	1	1	0	1	1
1	1	0	0	1	1	1	0
1	1	0	1	1	0	1	0
1	1	1	0	1	1	0	0
1	1	1	1	0	0	1	1

Соответствие номера линейной комбинации и веса:

№	1	2	3	4	5	6	7	8	9	10
Вес	28306	6090	31064	7092	29990	3198	25324	15529	21051	11107
№	11	12	13	14	15	17	18	19	20	21
Вес	17905	10013	18831	12503	24133	37229	59445	34471	58443	35545
№	22	23	24	25	26	27	28	29	30	31
Вес	62337	40211	50006	44484	54428	47630	55522	46704	53032	41402

№	6	2	4	12	10	14	8	11	13	9
Вес	3198	6090	7092	10013	11107	12503	15529	17905	18831	21051
№	15	7	1	5	3	19	21	17	23	31
Вес	24133	25324	28306	29990	31064	34471	35545	37229	40211	41402
№	25	29	27	24	30	26	28	20	18	22
Вес	44484	46704	47630	50006	53032	54428	55522	58443	59445	62337

Выбор минимальных линейно-независимых комбинаций:

1) Выбирается: №6, исключается: № 6, 22;
2) Выбирается: №2, исключаются: № 2, 4, 18, 20;
3) Выбирается: №12, исключаются: №8, 10, 12, 14, 24, 26, 28, 30;
4) Выбирается: №11.

Полученный S-блок (представитель с наименьшим весом):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Вес
0	0	0	0	1	1	0	0	0	1	1	1	1	1	1	0	3198
0	0	0	1	0	1	1	1	1	1	0	0	1	0	1	0	6090
0	0	1	0	0	1	1	1	0	0	0	1	1	1	0	1	10013
0	1	0	0	0	1	0	1	1	1	1	1	0	0	0	1	17905

Определение числа представителей

Далее перебираются все возможные значения невырожденной матрицы A, для каждого из полученных значений ищется представитель.

Количество различных представителей из всех полученных предлагается использовать в качестве показателя оценки качества S-блока. Обозначим это число N_{lm}, обозначающее число локальных представителей.

Теоретически возможное количество подмножеств множества аффинно-эквивалентных S-блоков, а, следовательно, и представителей, рассчитывается по формуле:

$\max N_{lm}$

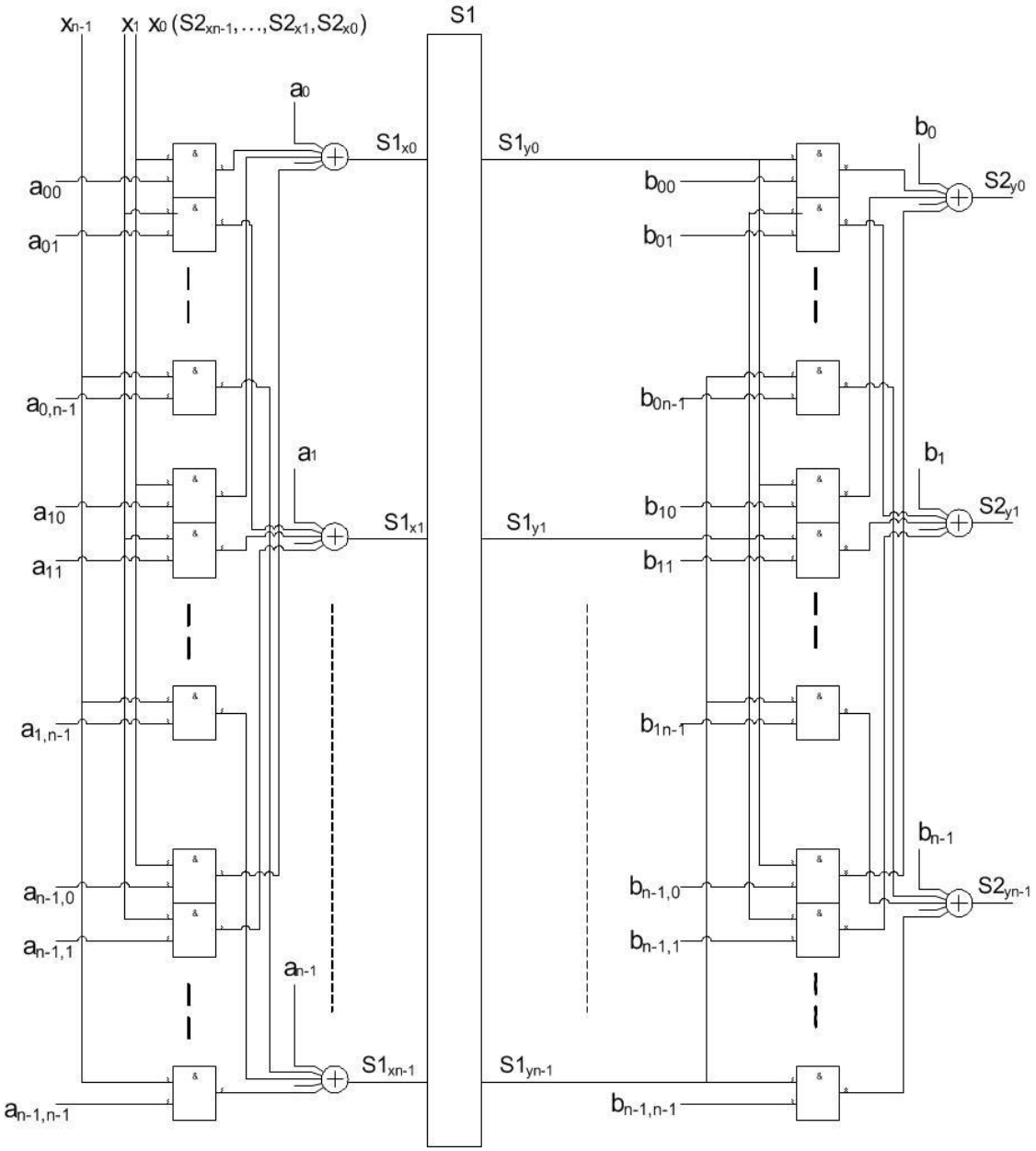
$$N_{lm} \le \prod_{i=1}^{n} (2^{n+1} - 2^{i})$$

N	Количество представителей
4	322560
5	319979520
6	1290157424640
7	2097279909494784 0
8	1369104324918194995200
15	5,10259969886794669593834275239 76e+71

Результаты экспериментов для различных аффинно-неэквивалентных S-блоков

S-блок	Нелинейность	Число представителей
D2781EB45AF0963C	0	1
0FA5C369872D4BE1	0	1
01C86F4E3DBA2975	2	5376
019EDB76F2C5A438 (AES)	4	5376
0123468A5BCF7E9D	4	80640
C462A5B9У8D703F1 (ГОСТ)	4	322560

Аппаратная реализация аффинно-эквивалентных преобразований



Связь аффинно-эквивалентных преобразований и структуры блочного шифра

Вывод

Оптимальной следует считать такую структуру блочного шифра, которая позволяет на каждом раунде и в каждом S-блоке размера *n*, с одинаковой вероятностью
реализовать одну из множества $S^0 = \left(\prod_{i=1}^{n} (2^{n+1} - 2^i) \right)^2$
подстановок!

Спасибо за внимание!

ИСПОЛЬЗОВАНИЕ АЛГОРИТМА ПОИСКА ПРЕДСТАВИТЕЛЯ МНОЖЕСТВА АФФИННО-ЭКВИВАЛЕНТНЫХ S-БЛОКОВ ДЛЯ ОЦЕНКИ ИХ КАЧЕСТВА

Н.П. Борисенко
Б.Д. Дударев
Email: npbor@yandex.ru