**Лекция 11.** Дифференциальный криптоанализ S блоки алгоритмов DES, AES, ГОСТ 28147-89, ГОСТ Р 34.13.2015.

На данный момент изучение свойств S–блоков и способов их усовершенствования является одной из главнейших задач в области симметричных алгоритмов блочного шифрования.

Размер S-блока является одной из важных характеристик. S-блок размером предполагает -битовые значения и -битовые выходные. Устойчивость алгоритма определяется размером S-блока, чем больше тем выше по отношению к методам линейного и дифференциального криптоанализа, а также ее равномерностью. В зависимости от размера S-блока, усложняется его проектирование. Исходя из практических соображений, значение , как правило, выбирают в диапазоне от 8 до 10. Об этом написано в книгах В. Столлингс и Л.К. Бабенко. (1, стр 18).

Найберг предложил использовать следующие подходы при разработке S-блоков:

1. **Случайный выбор**. Элементы S–блоков выбираются с помощью генератора или специальных таблиц псевдослучайных чисел. В случае небольшого размера (6х4) такой способ может привести к созданию S-блоков с нежелательными характеристиками, но для больших блоков (8х32) он должен быть вполне приемлемым.
2. **Случайный выбор с проверкой**. Элементы S-блока выбираются случайным образом, но после этого полученные результаты должны провериться на соответствие различным критериям, описанным выше, с отсеиванием тех матриц, которые не выдержали такой проверки.
3. **Выбор вручную**. Элементы S-блока выбираются практически вручную с использованием элементарных математических преобразований. Для больших Sблоков использование данного подхода сопряжено с немалыми трудностями.
4. **Математический подход**. Элементы S-блока генерируются на основе тех или иных математических принципов. Такой подход обеспечивает S–блоки, гарантирующие заданный уровень надежности по отношению к методам линейного и дифференциального криптоанализа, а также хорошие показатели диффузии (то есть рассеивания статистических особенностей открытого текста по широкому диапазону статистических характеристик шифрованного текста).

Разработана программа по проведению линейного и дифференциального криптоанализа для любых S-блоков симметричного алгоритма. С помощью этой программы проводились анализы S-блоков DES, ГОСТ 28147-89, ГОСТ Р 34.13-2015, AES (Rijndael). А также проведено линейный и дифференциалный криптоанализ на умножение многочленов в НПСС (таблица 1).

Таблица 1 - Интервал результатов линейного и дифференциалного криптоанализа

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Наименование | | Минимум | максимум | средний минимум | средний максимум | Хи-квадрат | степень свободы |
| DES | линейный | 12 | 48 | 15,5 | 46,25 | 480 | 944 |
| дифференциалный | 0 | 16 | 0 | 16 | 20514 | 1007 |
| ГОСТ 28147-89 | линейный | 2 | 14 | 2,75 | 13,75 | 120 | 224 |
| дифференциалный | 0 | 8 | 0 | 6,25 | 480 | 239 |
| ГОСТ Р 34.13-2015 | линейный | 100 | 156 |  |  | 32640 | 65024 |
| дифференциалный | 0 | 8 |  |  | 111297 | 65279 |
| AES-128 (Rijndael) | линейный | 111 | 145 |  |  | 32639 | 65024 |
| дифференциалный | 0 | 5 |  |  | 67125 | 65279 |
| НПСС | линейный | 128 | 256 |  |  | 32640 | 65024 |
|  | дифференциалный | 0 | 256 |  |  | 16646400 | 65279 |

Во время проведения анализа мы прослеживаем всевозможные комбинации двоичных векторов. Каждую пару векторов мы используем в качестве маски, которую накладываем на всевозможные пары вход-выход блока замены. Эти маски указывают нам биты входа и выхода соответственно, которые необходимо сложить по модулю два, а затем сравнить полученные результаты (считывается количество 0, либо 1). Результаты полученные программой приведены ниже. В связи с большим размером полученных таблиц, приведен пример анализа для алгоритма ГОСТ 28147-89 (таблицы 2, 3). Таблицы результатов анализа S-блоков DES совпадает с результатами в литературах.

Одной из функции программы является разработка S-блоков с хорошим характеристиками. Проверили полученные *S-*блоки всех неприводимых многочленов восьмого степени основанных получением обратного элемента относительно умножения в поле GF(28). Убедились, что такие S-блоки одинаково стойки для дифференциального и линейного криптоанализа.

Криптостойкость к дифференциальному и линейному криптоанализу *S*-блока должен удовлетворять следующие требования:

-для линейного криптоанализа *S-*блока с определенной размерностью и относящиеся к нему элементы матрицы, в котором входные и выходные данные соответствуют между собой, должны распределятся равномерно считанных количеств 0 и 1 ко всей матрицы элементов;

-для дифференциального криптоанализа *S-*блока с определенной размерностью и относящиеся к нему элементы матрицы должны распространятся равномерно.

Таблица 3 - Дифференциалный криптоанализ S-блоков алгоритма шифровании ГОСТ 28147-89(а, б, в, г, д, е, ж, з)

Дифференциалный анализ 1-блока (а)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 4 | 4 | 0 |
| 2 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 0 | 2 | 4 | 0 | 0 |
| 3 | 0 | 0 | 0 | 4 | 2 | 0 | 2 | 0 | 2 | 0 | 6 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 2 | 2 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 |
| 5 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 4 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 4 | 6 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 4 | 2 |
| 8 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 |
| 9 | 0 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 4 |
| 10 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 2 |
| 11 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 2 | 2 |
| 12 | 0 | 4 | 2 | 4 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 2 |
| 14 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 0 |
| 15 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 2 |

Дифференциалный анализ 2-блока (б)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 |
| 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 4 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 0 |
| 3 | 0 | 0 | 6 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 0 | 2 |
| 4 | 0 | 0 | 2 | 0 | 2 | 0 | 4 | 0 | 4 | 0 | 0 | 2 | 0 | 2 | 0 | 0 |
| 5 | 0 | 2 | 0 | 6 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 |
| 6 | 0 | 6 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 2 | 0 | 0 | 4 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 |
| 8 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 4 | 0 | 4 | 2 | 0 | 0 |
| 9 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 2 |
| 10 | 0 | 0 | 0 | 2 | 2 | 0 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 4 |
| 11 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 0 | 2 | 4 |
| 12 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 4 | 0 |
| 13 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 2 | 0 | 2 | 2 | 2 |
| 14 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 4 | 2 | 2 | 2 | 0 |
| 15 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 4 | 2 | 0 | 0 | 0 | 4 | 0 | 2 | 0 |

Дифференциалный анализ 3-блока (в)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 2 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 0 |
| 2 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 2 |
| 3 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 4 | 6 | 0 | 0 | 0 | 2 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 6 |
| 5 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 |
| 6 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | 0 | 4 | 2 | 0 | 0 | 2 | 0 |
| 7 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 2 | 4 | 0 | 0 |
| 9 | 0 | 2 | 0 | 0 | 0 | 2 | 4 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 2 |
| 10 | 0 | 0 | 6 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 4 |
| 11 | 0 | 2 | 2 | 2 | 6 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 |
| 12 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 6 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 4 | 0 |
| 14 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 4 | 0 | 0 |
| 15 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 2 | 2 | 2 | 2 |

Дифференциалный анализ 4-блока (г)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 6 | 2 | 0 | 0 | 0 | 0 |
| 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 2 | 2 | 2 | 0 |
| 3 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 4 | 0 | 0 | 0 | 4 | 0 | 4 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 |
| 5 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 4 |
| 6 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 2 | 4 | 0 |
| 7 | 0 | 4 | 2 | 0 | 4 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 2 | 2 | 6 | 2 | 0 | 0 |
| 9 | 0 | 0 | 2 | 6 | 0 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 4 | 2 | 0 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 |
| 11 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 6 | 0 | 2 | 2 | 2 |
| 12 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 2 | 6 |
| 13 | 0 | 0 | 0 | 0 | 4 | 4 | 4 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 2 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 |
| 15 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |

Дифференциалный анализ 5-блока (д)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 0 |
| 2 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 4 | 0 | 0 |
| 3 | 0 | 0 | 4 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 |
| 4 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 2 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 2 |
| 6 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 2 | 2 |
| 7 | 0 | 4 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 4 | 0 |
| 8 | 0 | 0 | 2 | 0 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 2 |
| 9 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 4 | 2 | 0 | 0 | 2 | 0 | 0 | 4 |
| 10 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 2 | 2 |
| 11 | 0 | 0 | 0 | 0 | 2 | 4 | 0 | 2 | 4 | 0 | 0 | 0 | 0 | 2 | 2 | 0 |
| 12 | 0 | 2 | 0 | 2 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 |
| 13 | 0 | 2 | 0 | 2 | 0 | 4 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 2 |
| 14 | 0 | 2 | 4 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 0 |
| 15 | 0 | 2 | 0 | 0 | 4 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 |

Дифференциалный анализ 6-блока (е)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 0 | 0 | 0 | 6 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 2 |
| 2 | 0 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 2 |
| 3 | 0 | 2 | 0 | 4 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 |
| 4 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 4 | 4 | 0 | 2 | 0 | 0 |
| 5 | 0 | 2 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 4 |
| 6 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 4 | 2 | 0 | 2 | 2 | 0 | 0 |
| 8 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 6 | 0 |
| 9 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 4 | 0 | 0 | 0 | 4 |
| 10 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 4 | 2 | 0 | 0 | 4 | 0 | 2 | 0 |
| 11 | 0 | 2 | 0 | 4 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 4 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 2 | 0 |
| 13 | 0 | 4 | 2 | 0 | 4 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 14 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 2 |
| 15 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 0 |

Дифференциалный анализ 7-блока (ж)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 0 | 4 | 0 |
| 2 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 |
| 3 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 8 | 0 | 2 | 0 | 0 | 2 |
| 4 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 |
| 5 | 0 | 0 | 4 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 2 | 2 | 0 | 0 |
| 6 | 0 | 0 | 4 | 0 | 0 | 0 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 2 | 2 |
| 7 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 |
| 8 | 0 | 2 | 0 | 0 | 0 | 4 | 2 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 |
| 9 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 4 | 0 | 6 | 0 | 0 | 0 | 2 |
| 10 | 0 | 4 | 0 | 6 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 |
| 11 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 4 | 2 | 4 |
| 12 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 0 |
| 13 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 2 |
| 14 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 2 |
| 15 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 |

Дифференциалный анализ 8-блока (з)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 6 | 4 | 0 |
| 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 4 | 0 | 2 | 4 |
| 3 | 0 | 6 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 |
| 4 | 0 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 2 |
| 5 | 0 | 0 | 2 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 4 | 0 | 0 | 0 | 0 | 2 |
| 6 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 0 | 2 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 8 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 2 | 2 | 4 | 0 |
| 9 | 0 | 2 | 0 | 6 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 |
| 10 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 2 |
| 11 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 6 |
| 12 | 0 | 0 | 0 | 0 | 2 | 4 | 0 | 2 | 0 | 2 | 2 | 0 | 4 | 0 | 0 | 0 |
| 13 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 0 |
| 14 | 0 | 0 | 0 | 4 | 0 | 0 | 4 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 2 | 0 | 4 | 2 | 2 | 0 | 0 | 2 | 0 | 4 | 0 | 0 |