**Лекция 13. Линейный криптоанализ** **S блоки** алгоритмов DES, AES, ГОСТ 28147-89, ГОСТ Р 34.13.2015. Требование для S блоков к устойчивости дифференциального и линейного криптоанализа.

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).
5. 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 |

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

*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.

Таблица 2 - Линейный криптоанализ S-блоков алгоритма шифрования ГОСТ 28147-89(а, б, в, г, д, е, ж, з)

Линейный анализ 1-блока (а)

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

Линейный анализ 2-блока (б)

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

Линейный анализ 3-блока (в)

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

Линейный анализ 4-блока (г)

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

Линейный анализ 5-блока (д)

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

Линейный анализ 6-блока (е)

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

Линейный анализ 7-блока (ж)

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

Линейный анализ 8-блока (з)

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