1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 1**

1. по дисциплине «Основы построения стойких криптопримитивов и псевдослучайных генераторов»
2. Выполнил
3. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Преподаватель д.ф.-м.н. Шенец Н.Н.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Проведение анализа основных свойств s-блока блочной криптосистемы

# Задание

1. Посчитать алгебраическую степень подстановки
2. Посчитать нелинейность подстановки
3. Составить таблицу разностей
4. Составить таблицу линейных аппроксимаций

# Ход работы

Каждый s-блок можно представить в виде m булевых функций:

S-блоки должны обладать свойствами, затрудняющими применение тех или иных методов криптоанализа. Основными критериями выбора S-блоков являются: высокая нелинейность, большие степени координатных функций и их линейных комбинаций, малые значения в таблицах разностей.

Алгебраической степенью функции f называется степень ее многочлена Жегалкина. Алгебраической степенью подстановки называется величина . Поэтому, чтобы посчитать алгебраическую степень подстановки, необходимо задать s-блок в виде m многочленов Жегалкина и затем перебором найти минимальную степень их комбинаций.

Для того, чтобы построить по заданной подстановке многочлены Жегалкина, необходимо построить таблицы истинности для каждой из функций. В таблице 1 представлена таблица истинности для подстановки из моего варианта. X1, X2, X3, X4 – входные данные, столбцы Y1, Y2, Y3, Y4 – таблица истинности для 1, 2, 3, 4 многочлена Жегалкина.

Таблица 1 – входные и выходные данные подстановки

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| X1 | X2 | X3 | X4 | Y1 | Y2 | Y3 | Y4 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |

Далее, по таблице истинности можно построить многочлен Жегалкина по таблице истинности, решив СЛАУ, или по треугольнику Паскаля. В моей реализации решается СЛАУ. На рисунке 1 представлены посчитанные многочлены Жегалкина, являющиеся координатными функциями для s-блока.

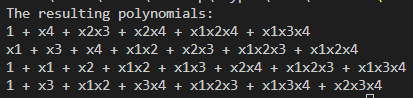


Рисунок 1 – полученные многочлены Жегалкина

Все полученные многочлены Жегалкина имеют степень 3. Однако, если сложить 1, 2, 3 многочлены, то степень итогового многочлена равна 2, следовательно, степень подстановки равна 2.

Нелинейностью функции *f* называется расстояние от нее до множества аффинных функций: . Нелинейность подстановки:

Расстояние между *f* и *l* определяется через коэффициент Уолша-Адамара, поэтому нелинейность функции можно найти следующим образом:

В моей реализации используется именно этот способ поиска нелинейности функции. В результате нелинейность подстановки равна 2.

Линейной аппроксимацией для подстановки называется пара векторов . При случайном равновероятном выборе определяется вероятность аппроксимации . Чем выше эта вероятность, тем с большей точностью можно предсказать линейную комбинацию по линейной комбинации . Качество аппроксимации характеризует абсолютное значение величины , которую называют преобладанием. В моей реализации строиться таблица именно преобладаний, а не аппроксимаций. На рисунке 2 представлена таблица преобладаний, построенная моей реализацией, а на рисунке 3 построенная sagemath.

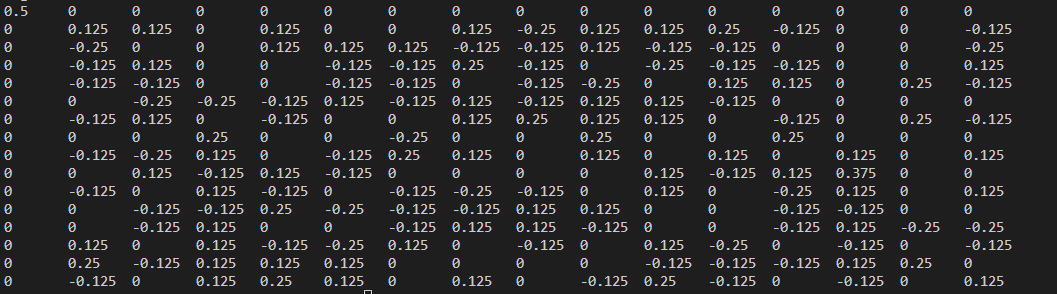


Рисунок 2 – таблица преобладаний моей реализации

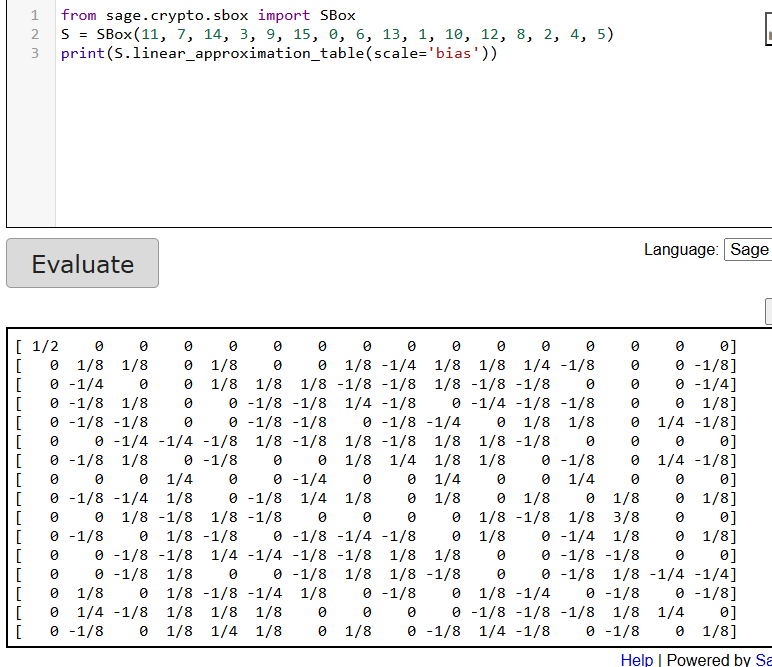


Рисунок 3 – таблица преобладаний sagemath

По преобладанию можно определить нелинейность подстановки, так как преобладание связано с коэффициентами Уолша-Адамара, . Откуда . Максимальное преобладание в построенной таблице равно 0,375, тогда нелинейность подстановки равна 2, как и подсчитано ранее.

На заданной подстановке задана групповая операция XOR. Тогда событие означает, что прообразам *x, x xor a* с разностью *a* соответствуют образы с разностью *b.* Тогда в таблице разностей находятся следующие значения:

На рисунке 4 представлена таблица разностей, построенная моей реализацией, на рисунке 5 построенная sagemath.

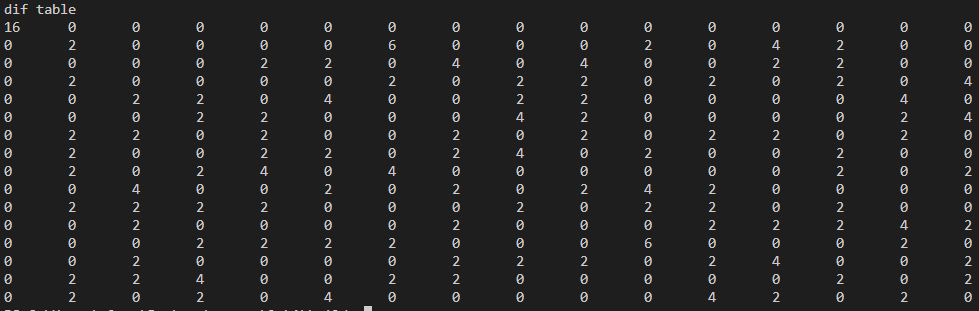


Рисунок 4 – таблица разностей моей реализации

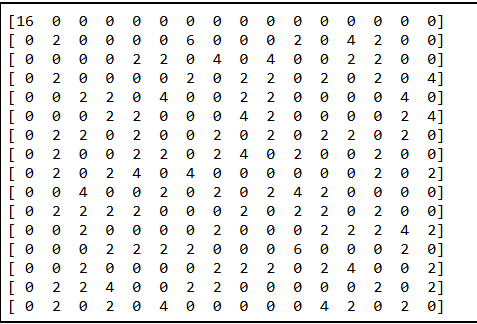


Рисунок 5 – таблица разностей sagemath

# Вывод

В результате данной работы были изучены основные свойства s-блока и способы их подсчета. Для заданной подстановки были подсчитаны алгебраическая степень, равная 2, нелинейность, равная 2, построены таблицы разности и преобладаний.