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 № 3**

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

Изучение линейного метода криптоанализа, способов оптимизации линейного метода и способа оценки стойкости шифра

# Задание

1. В качестве анализируемой блочной криптосистемы взять свой вариант криптосистемы из курса КМЗИ.
2. Изучить метод оценки стойкости шифра к линейному криптоанализу
3. Составить таблицу преобладаний подстановки
4. Найти характеристику, обладающую наибольшим абсолютным значением преобладания, ее вероятность и оценить стойкость шифра к линейному методу.

# Ход работы

В заданной криптосистеме есть 4 раунда: SP-сеть, подстановка Фейстеля, SP-сеть, подстановка Лай-Месси. Подстановка представлена вектором {11, 7, 14, 3, 9, 15, 0, 6, 13, 1, 10, 12, 8, 2, 4, 5}, Перестановка задана функцией f(x) = 21\*x+23(mod 32), в качестве функции для подстановок Фейстеля и Лай-Месси выступает 16-битная SP-сеть.

Суть линейного метода заключается в поиске линейных над полем F2 равенств, содержащих биты открытого текста x, шифртекста y и ключа k, которые выполняются с вероятностью, заметно большей 0,5, или с вероятностью, заметно меньшей 0,5:

После получения достаточного числа уравнений ключ можно найти решением этой системы, поскольку биты открытого и зашифрованного текста известны. Истинный ключ определяется как наиболее (наименее) вероятный, для которого условия выполняются наиболее (наименее) часто.

Линейной характеристикой назовем последовательность линейных сумм для отдельных раундов шифрования, в которых множество выходных параметров, входящих в линейную сумму предыдущего оператора, совпадает с множеством входных переменных, входящих в линейную сумму последующего оператора.

Вероятность линейной характеристики находится с помощью леммы о набегании знаков: .

Рассмотрим заданную криптосистему. На рисунке 1 представлена структурная схема раундов криптосистемы. На рисунке 2 представлена таблица преобладаний для заданного s-блока.

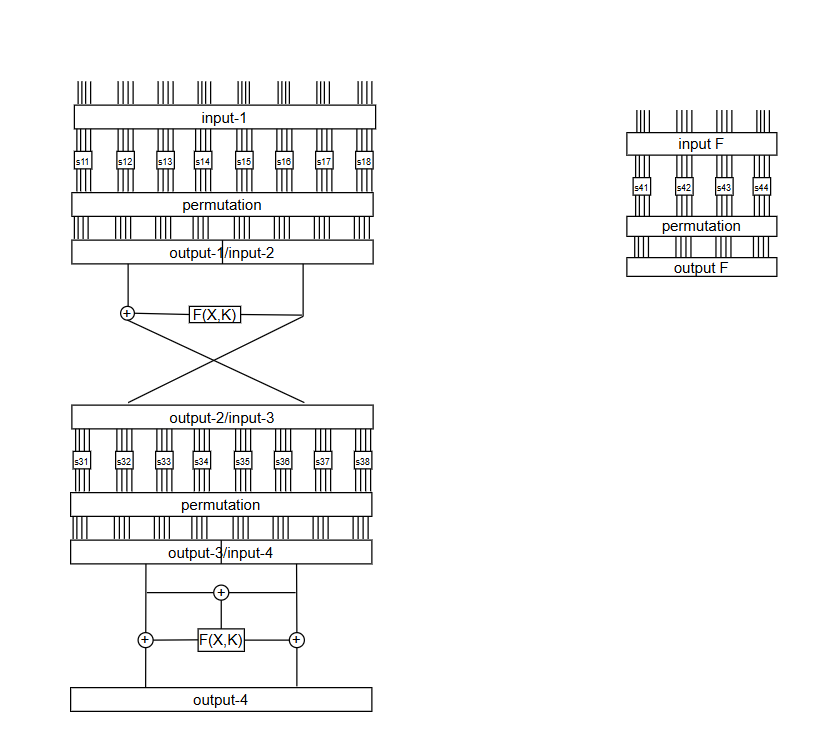


Рисунок 1 – структурная схема криптосистемы

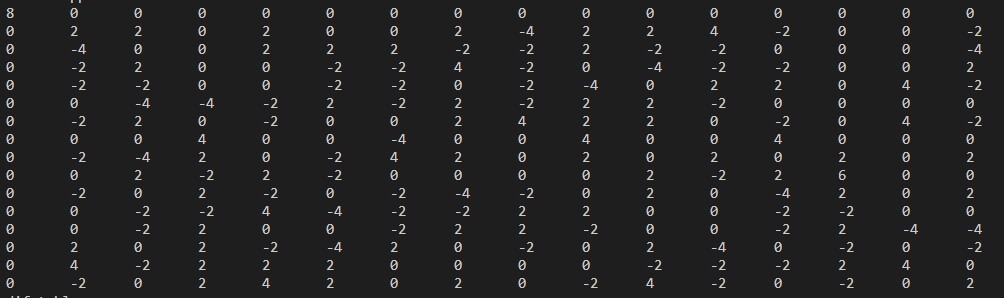


Рисунок 2 – таблица преобладаний

Начнем со стратегии «жадных» алгоритмов. Если на второй раунд придет входной блок X = X1 || 0, тогда с вероятностью 1 на входе будет блок Y = 0 || X1, ключ никак не участвует в раунде, активных s-блоков нет.

Найдем в таблице преобладаний максимальное по абсолютному значению ячейку и подадим ее на вход третьему раунду. Также это значение является выходным значением первого раунда. Рассмотрим первый раунд.

Выходом первого раунда является 0 || 1001 || 0 || 0 || 0 || 0 || 0 || 0, тогда выходом s-блока s15 = 1000, s17 = 0100, тогда входом s15 = 0110, s17 = 1111.

Т.е.

На вход третьему раунду приходит 0 || 0 || 0 || 0 || 0 || 1001 || 0 || 0.

Активным является s36. , подставив вместо входа выход первого раунда, получается :

На вход четвертному раунду приходит 0 || 0 || 0 || 0 || 1000 || 0 || 0011 || 0.

После ксора двух полублоков получится 1000 || 0 || 0011 || 0. Активными являются s41, s43. Результатом является:

На рисунке 3 представлена та же информация, только на картинке.

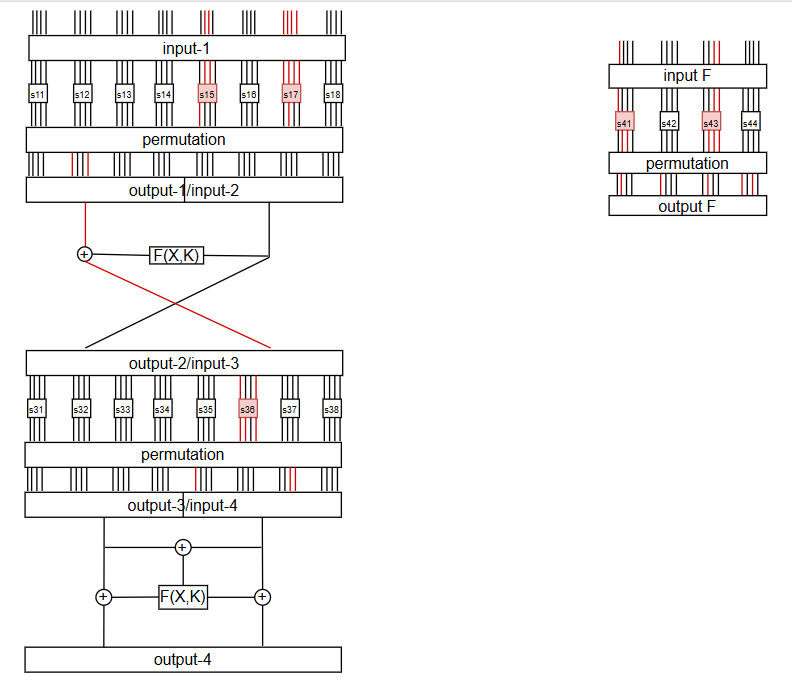


Рисунок 3 – активные s-блоки и биты первой стратегии

Вероятность такой характеристики:

В результате в характеристику вошло много активных s-блоков. Попробуем теперь минимизировать их число. Второй раунд остается тем же. Пусть выход первого раунда 0 || 0001 || 0 || 0 || 0 || 0 || 0 || 0. Тогда

Тогда на вход 3 раунда приходит 0 || 0 || 0 || 0 || 0 || 0001 || 0 || 0. Тогда

или .

На вход 4 раунда 0 || 0 || 0 || 0 || 0 || 0 || 0001 || 0. После ксора получается 0 || 0 || 0001 || 0. Тогда активным s-блоком является s43.

*или*

На рисунке 4 представлены активные s-блоки, входные и выходные биты раундов.

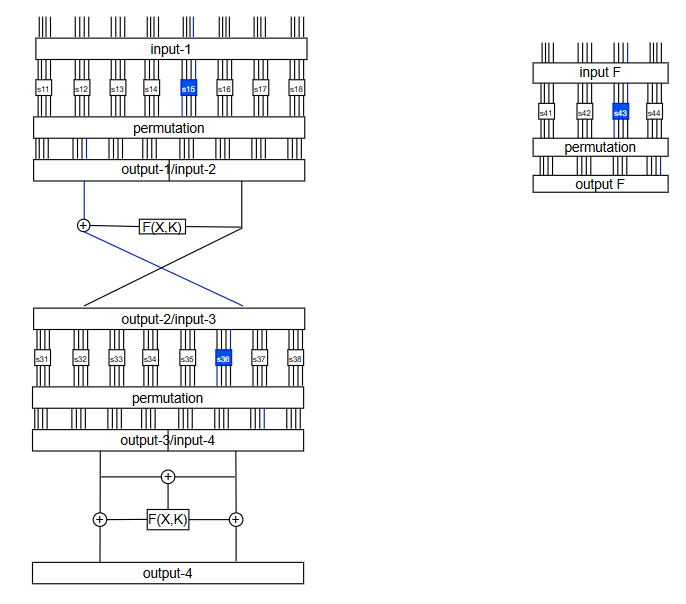


Рисунок 4 – активные s-блоки и биты второй стратегии

В характеристику входит 3 s-блока: s15, s36, s43.

Вероятность такой характеристики:

Для вскрытия ключа необходимо примерно пар открытый текст – шифртекст.

# Контрольные вопросы

1. *Что такое линейная характеристика?*

Линейная характеристика – последовательность линейных сумм для отдельных раундов шифрования, в которых множество выходных параметров, входящих в линейную сумму предыдущего оператора, совпадает с множеством входных переменных, входящих в линейную сумму последующего оператора.

1. *Как можно найти преобладания линейных равенств для подстановки?*

Каждый элемент матрицы преобладаний содержит центрированное число выполнений равенств над полем :

Т.е. число совпадений минус .

1. *Как влияет вес линейных равенств на стойкость шифра?*

Одним из вариантов построения высоковероятностной характеристики является построение, составленное из линейных равенств веса 2, которые обладают ненулевой вероятностью, поскольку число активных s-блоков в такой характеристике минимально. Поэтому желательно, чтобы подстановка имела минимально возможную вероятность дифференциалов веса 2.

# Вывод

В результате данной работы были найдены высоковероятностные 3-х тактовые характеристики для заданной криптосистемы. В первом случае в нее вошло 5 s-блока, преобладание равно 0,0234375, что явно больше чем , поэтому, скорее всего, линейная атака пройдет успешно. Для атаки достаточно около пар открытый текст – шифртекст. Во втором случае в характеристику вошло 3 s-блока, преобладание равно 0,0625, необходимо пар текстов.