Министерство образования и науки Российской Федерации

Санкт-Петербургский государственный политехнический университет

—

Факультет технической кибернетики

**Кафедра «Информационная безопасность компьютерных систем»**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4**

**Линейный криптоанализ подстановочно-перестановочного шифра**

по дисциплине «Теория итерированных шифров»

Выполнил

студент гр. 5088/1 И.И. Сиваков

Проверил

ст. преподаватель О.В. Шемякина

Санкт-Петербург

2011

# задание

1. Изучить метод оценки стойкости шифра к линейному анализу.

2. Найти характеристику, обладающую наибольшим абсолютным значением преобладания, ее вероятность и оценить стойкость шифра к линейному методу.

# Результаты работы

Размер блока исследуемого шифра 32 бита. Зашифрование выполняется на четырех циклах. На каждом цикле используется один и тот же ключ, выполняются действия:

1. XOR блока текста с блоком ключа.
2. Подстановка S блоков по 4 бита.
3. 32-х битовая перестановка P.

После выполнения 4-х циклов выполняется XOR блока текста с блоком ключа.

S: (2, 11, 13, 0, 9, 7, 4, 14, 1, 12, 8, 15, 6, 10, 3, 5)

P:

P: (11, 16, 21, 26, 31, 4, 9, 14, 19, 24, 29, 2, 7, 12, 17, 22, 27, 0, 5, 10, 15, 20, 25, 30, 3, 8, 13, 18, 23, 28, 1, 6)

Таблица линейных сумм:

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

------------------------------------------------------------------

0| 8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1| 0 0 2 -2 2 -2 0 0 2 2 **-4** 0 0 **-4** -2 -2

2| 0 0 -2 -2 2 -2 0 **-4** 0 0 -2 -2 -2 2 **4** 0

3| 0 0 0 **-4** 0 0 4 0 2 2 2 -2 2 2 -2 2

4| 0 0 2 2 2 2 0 0 -2 2 0 **-4** 4 0 2 -2

5| 0 0 0 **-4** 0 **4** 0 0 0 **-4** 0 0 0 0 0 **-4**

6| 0 0 0 0 0 **-4** **-4** 0 2 -2 2 -2 2 2 -2 -2

7| 0 0 -2 2 2 2 0 **-4 4** 0 2 2 2 -2 0 0

8| 0 0 0 0 0 0 0 0 0 **4** 0 **4** 0 **4** 0 **-4**

9| 0 0 2 -2 -2 2 **-4 -4** -2 2 0 0 0 0 -2 2

10| 0 **-4** -2 2 2 2 0 0 0 0 -2 -2 -2 2 **-4** 0

11| 0 **4** 0 0  **4** 0 0 0 -2 -2 -2 2 2 2 -2 2

12| 0 0 -2 -2 2 2 **-4 4** 2 2 0 0 0 0 2 2

13| 0 0 **-4** 0 **-4** 0 0 0 0 0 **-4** 0 **4** 0 0 0

14| 0 **4** **-4** 0 0 0 0 0 -2 2 2 -2 -2 -2 -2 -2

15| 0 **4** 2 2 -2 2 0 0 **4** 0 -2 -2 -2 2 0 0

Построенная таблица распределения линейных сумм с наибольшим абсолютным преобладанием по весам:

|  |  |  |
| --- | --- | --- |
| Вес дифференциала | Наибольшая вероятность | Вид дифференциала |
| 2 | 0.125000 | [1, 2]; [1, 4]; [1, 8]; [2, 2]; [2, 4]; [4, 2]; [4, 4]; [4, 8]; |
| 3 | 0.250000 | [1, 10]; [4, 12]; [8, 9]; [10, 1]; |
| 4 | 0.250000 | [1, 13]; [2, 7]; [2, 14]; [3, 3]; [3, 6];  [4, 11]; [5, 3]; [5, 5]; [5, 9]; [6, 5]; [6, 6];  [7, 8]; [8, 11]; [8, 13]; [9, 6]; [11, 1];[11, 4];  [12, 6]; [13, 2]; [13, 4]; [14, 1]; [14, 2]; |
| 5 | 0.250000 | [8, 15]; [9, 7]; [10, 14]; [12, 7]; [13, 10];  [13, 12]; [15, 1]; [15, 8]; |
| 6 | 0.250000 | [5, 15]; [7, 7]; |
| 7 | 0.125000 | [11, 15]; [14, 15]; [15, 11]; [15, 13]; |
| 8 | 0.000000 |  |

Для вскрытия ключа необходимо построить характеристику, вероятность которой будет максимальна или близка к максимальной. У подстановки есть линейные суммы веса 2 с ненулевым преобладанием.

Для перестановки P никакие два разряда с выхода одного блока подстановки не попадают на вход одного блока подстановки на следующем цикле. Это значит, что если не использовать линейную сумму веса 2, то для характеристики понадобится, как минимум, 4 S-блока.

S11

S12

S13

S14

S15

S16

S17

S18

Сложение с ключом

Перестановка

S21

S22

S23

S24

S25

S26

S27

S28

Сложение с ключом

Перестановка

S31

S32

S33

S34

S35

S36

S37

S38

Сложение с ключом

Перестановка

Рис.1 построенная характеристика

Вероятность характеристики . Преобладание . Построенная характеристика с данным преобладанием не является единственной.

Для трех циклов линейная аппроксимация имеет следующий вид:

u1,12 + u1,14 + u1,15 + u4,7 + u4,22 + k12 + k14 + k15 + k7 + k22 = 0,

где ui,j - j-ый разряд текста на входе i-го цикла. Равенство выполняется с вероятностью 15/32. В зависимости от четности суммы разрядов ключа равенство:

u1,12 + u1,14 + u1,15 + u4,7 + u4,22 = 0

выполняется с вероятностью 15/32 или 17/32.

Вскрытие ключа:

1. Выбирается некоторое число текстов x и соответствующих им шифртекстов y.
2. В четвертом цикле активными являются второй и шестой S-блоки, поэтому делаем перебор по 8 соответствующим битам ключа (256 вариантов). Для каждого из значений части ключа подсчитываем преобладание выполнения вышеприведенного равенства.
3. Выбираем то значение части ключа, чье преобладание наиболее близко к расчетному.
4. Для определения других битов ключа можно использовать аналогичную характеристику с другим активным входным блоком. Всего нужно использовать 4 характеристики.

Для вскрытия необходимо перебрать 8 бит ключа для каждого из текста. Вычислительная сложность . Для вскрытия всего ключа необходимо, используя другие вероятные характеристики повторить операцию 4 раза..

Вычислительная сложность равна .

Число активных S блоков на каждом цикле можно сделать равным одному, используя линейную сумму [1, 2] с весом 2. Ее преобладание равно . Тогда преобладание (k-1)-цикловой характеристики будет равна , где k – число циклов шифрования. Для того чтобы анализ имел сложность большую, чем переборная, необходимо . .

# Выводы

Для вскрытия ключа необходимо около открытых блоков и соответствующих шифртекстов. Характеристика позволяет вскрыть 8 бит ключа.