Отчет по лабораторной работе

«Линейный криптоанализ блочного шифра»

Выполнил студент: Громов А.А.

Группа: ИКТЗ-83

Профессор кафедры ЗСС: д.т.н. проф. Яковлев В.А.

Вероятности появления линейных комбинаций

Произвольно выбраны

X1⊕X3=Y2⊕Y4 вероятность появления = 0.5 перекос= 0

X3= Y2⊕Y4  вероятность появления = 0.5 перекос= 0

X2⊕X3=Y2⊕Y3⊕Y4 вероятность появления = 0.625 перекос= 0.125

X1⊕X2⊕X3= Y2⊕Y3⊕Y4 вероятность появления = 0.625 перекос= 0.125

Заданы

X1⊕X2=Y2  вероятность появления = 0.25 перекос= -0.25

X4=Y1⊕Y2  вероятность появления = 0.625 перекос= 0.125

Генерация ключа

Выбран исходный ключ 1011010

Раундовые ключи

K1 = 1011 0100 1110 0100

K2 = 0010 0101 0010 0110

K3 = 1101 1100 0111 1010

K4 = 0000 1101 0100 0110

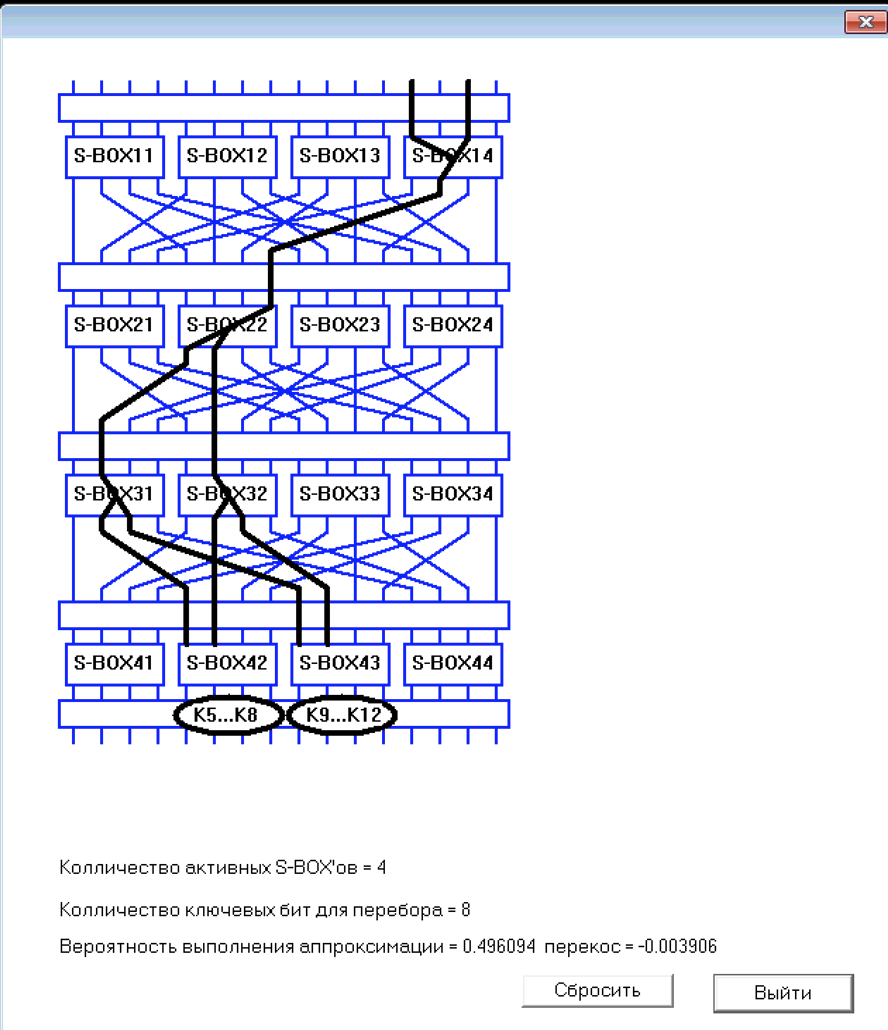
K5 = 0101 1101 1000 0111

Линейный криптоанализ

Вариант № 4 (привести номера S-box)

|  |  |  |  |
| --- | --- | --- | --- |
| № вар. | 1раунд | 2 раунд | 3 раунд |
| 4 | S14 | S22 | S31,S32 |

1. Сквозная линейная аппроксимация

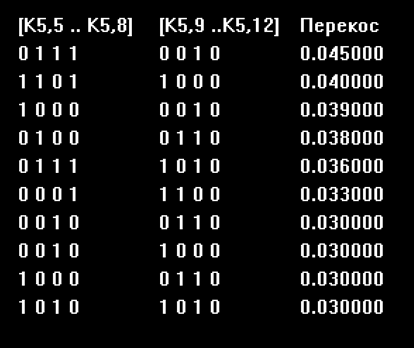


1. Расчет вероятностных характеристик линейных аппроксимаций

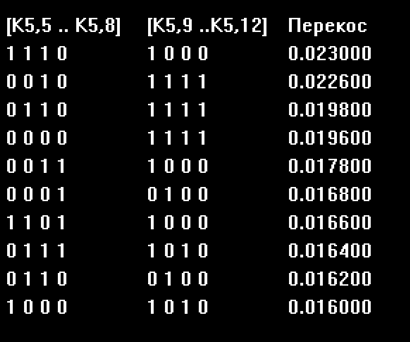
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № раунда | Вероятность  аппрокси-  мации S-блока (блоков) в раунде | Перекос аппрокс-  мации | Вероятность  аппрокси-  мации в 1+2  раунде и перекос | Вероятность  аппрокси-  мации в 1+2+3 раунде и перекос |
| 1 | S14: 1/4 | -1/4 |  |  |
| 2 | S22: 5/8 | 1/8 | ½+2(1/4-1/2)(5/8-1/2)=7/16  перекос (-1/16) |  |
| 3 | S31+ S32: ½+2(3/8-1/2)(3/8-1/2)=17/32 | 1/32 |  | ½+23(1/4-1/2)(5/8-1/2)3=127/256=0,496094  перекос  (-1/256)= -0,00390625 |
| Результаты моделирования для подключа K5i…K5i+4 и K5j…K5j+4 | | | | перекос: -0,003906 |

1. Скриншоты окна подбора ключа для разных N.

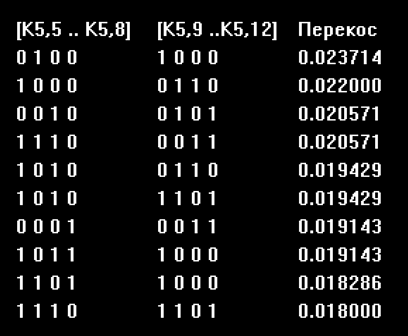
N=1000



N=5000



N=35000



Выводы по работе. Описать суть линейного криптоанализа. Характеристику сквозной линейной аппроксимации, результаты расчета вероятностей по каждому раунду. Принцип подбора ключей и выбора истинного ключа.

**Вывод:**

Шифр SPN уязвим для атаки методом сквозной линейной аппроксимации. Чем больше имеется пар сообщение/криптограмма, тем выше вероятность отыскать верный ключ. Исходя из результатов данной лабораторной работы, можно сделать вывод, что для увеличения достоверности вычисления истинного ключа количество таких пар с каждым разом должно увеличиваться всё больше и больше, то есть нелинейно.