ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. проф. М. А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Дисциплина «Основы криптографии»

# Лабораторная работа № 7

**«ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ БЛОЧНОГО ШИФРА»**

**4 вариант**

Выполнила: Громов А. А.

ИКТЗ-83

Проверил: Яковлев В. А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург

2021

**Цель работы:** Целью данной работы является изучение принципа линейного криптоанализа блочных шифров, реализованных по схеме SPN.

**Ход выполнения работы**

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

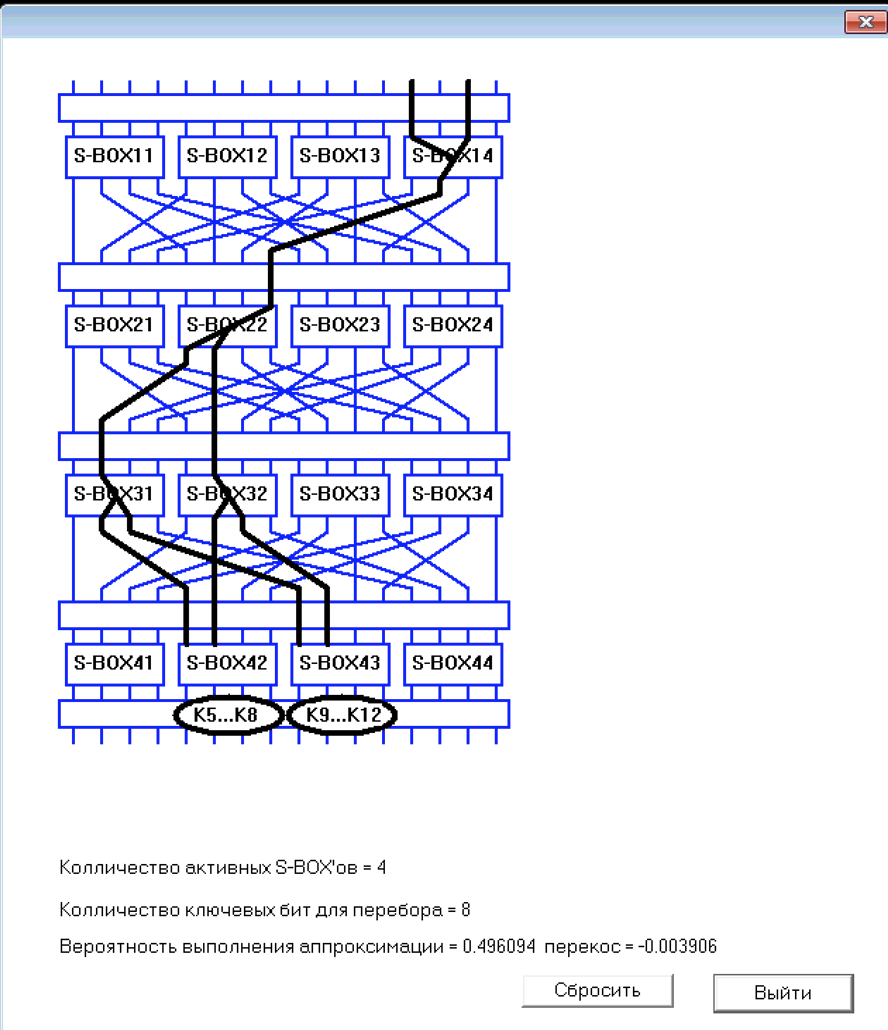
K5 = 0101 1101 1000 0111

Линейный криптоанализ

Вариант № 4

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

1. Сквозная линейная аппроксимация

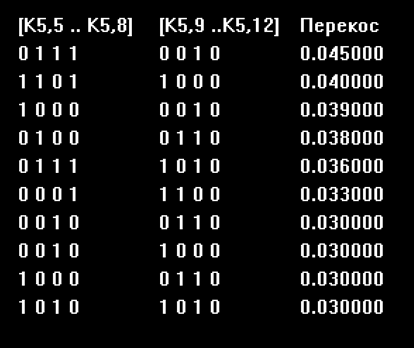


1. Расчет вероятностных характеристик линейных аппроксимаций

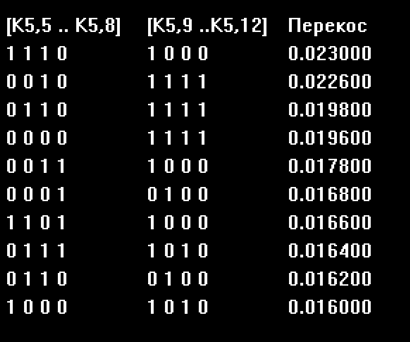
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № раунда | Вероятность  аппрокси-  мации S-блока (блоков) в раунде | Перекос аппрокс-  мации | Вероятность  аппрокси-  мации в 1+2  раунде и перекос | Вероятность  аппрокси-  мации в 1+2+3 раунде и перекос |
| 1 | S14: 1/4 | -1/4 |  |  |
| 2 | S22: 5/8 | 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.

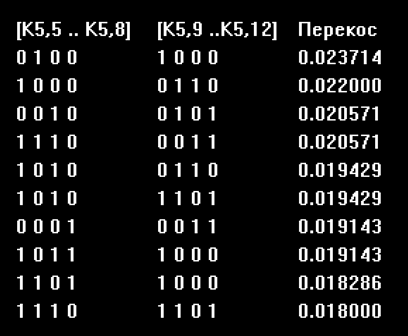
N=1000



N=5000



N=35000



**Вывод:**

Суть линейного криптоанализа заключается в использовании линейных уравнений, связывающих некоторые биты входа и выхода. На вход шифрующего устройства подается N сообщений, они шифруются заданным ключом, а потом проводится криптоанализ и выдается 10 наиболее вероятных значений подключа.

Вероятность нахождения искомого ключа среди предложенных программой тем выше, чем больше N, причем данная зависимость нелинейна.

Принцип выбора ключей состоит в вычислении для каждого из них количества пар сообщение-криптограмма, для которых верна линейная аппроксимация. Тот ключ, для которого отклонение пар от половины их количества наибольшее по абсолютному значению, объявляется наиболее верным.