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⊕X3⊕X4=Y2  вероятность появления = 0.75 перекос= 0.25

X2=Y2⊕Y4  вероятность появления = 0.25 перекос= -0.25

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

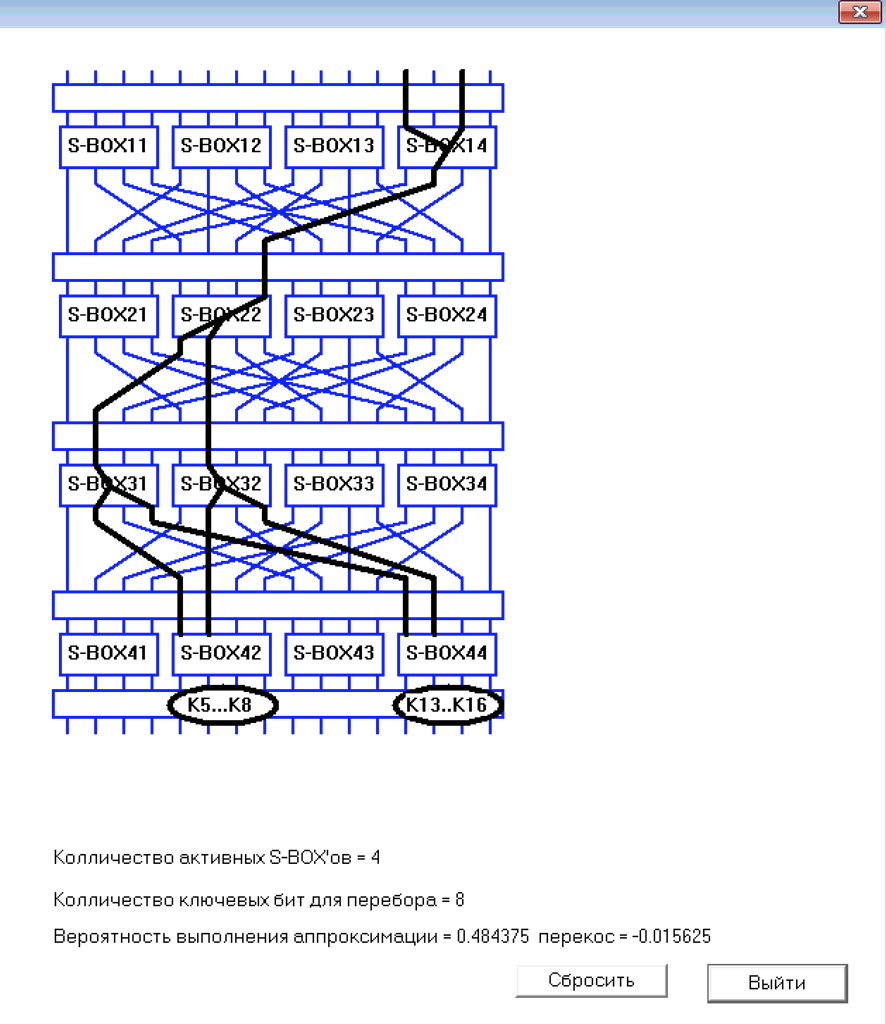
K5 = 0101 1101 1000 0111

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 | S32+ S34: ½+2(1/4-1/2)(1/4-1/2)=5/8 | 1/8 |  | ½+23(3/4-1/2)(1/4-1/2)3=15/32  перекос  (-1/32)= -0,03125 |
| Результаты моделирования для подключа K5i…K5i+4 и K5j…K5j+4 | | | | перекос: 0,0338 |

1. Скриншоты окна подбора ключа для разных N.

N=1000

[K5,5...K5,8] [K5,13...K5,16] Перекос

0001 1111 0.058

1111 0010 0.057

1101 1100 0.055

1111 1111 0.052

1111 1100 0.051

1111 0001 0.049

0001 1100 0.047

0011 1100 0.045

1010 1111 0.045

1101 1111 0.044

N=5000

[K5,5...K5,8] [K5,13...K5,16] Перекос

1111 1111 0.0278

1001 1000 0.0224

1111 0010 0.0216

1000 0010 0.0210

1000 0000 0.0200

1000 1100 0.0198

1010 1100 0.0192

1010 0001 0.0190

1100 0101 0.0178

0001 1011 0.0176

N=35000

[K5,5...K5,8] [K5,13...K5,16] Перекос

1111 1111 0.0391

1111 0010 0.0351

0001 1111 0.0294

1111 0011 0.0283

1110 0110 0.0280

1111 1110 0.0263

0000 0110 0.0257

1101 0101 0.0257

0011 1111 0.0249

1010 1111 0.0243

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

Контрольные вопросы

1.Основной принцип линейного криптоанализа блоковых шифров.

2.Какой тип атаки используется при линейном криптоанализе?

3.Чем определяется сложность линейного криптоанализа?

4.Каким условиям должен удовлетворять шифр для его устойчивости к линейному криптоанализу?

**Литература**

1.В.И.Коржик , В.А. Яковлев ,”Основы криптографии”, Учебное пособие,

ИЦ Интермедиа. 2016.