## **ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО**

###### Кафедра систем сбора и обработки информации



Факультет специальных информационных технологий

###### Практическое занятие № 6

Тема: **Линейный криптоанализ блочных шифров**

по дисциплине   
«Методы и средства криптографической защиты информации»

Вариант № 14

##### Выполнили курсанты 611/12 учебной группы:

|  |  |
| --- | --- |
| сержант | Рябинин И.А. |
| рядовой | Низамидинов М.Ф. |
|  |  |
|  |  |

##### Проверил преподаватель 61 кафедры

|  |  |
| --- | --- |
| подполковник | Д.Нагибин |

Санкт-Петербург

2025 г.

Содержание

[Постановка задачи 3](#_Toc89288778)

[1 Цель работы 3](#_Toc89288779)

[2 Теоретическая часть 3](#_Toc89288780)

[3 Задание 7](#_Toc89288781)

[Решение 8](#_Toc89288782)

[Вывод 13](#_Toc89288783)

# Постановка задачи

## 1. Цель работы

## Приобрести навыки проведения линейного криптоанализа блочных шифров.

## 2. Теоретическая часть

**Анализ полученного алгоритма, определение таблицы   
линейной аппроксимации используемых в нем подстановок.**

Линейный криптоанализ относится к классу вероятностных методов криптоанализа. Он использует данные вида «известный открытый текст / соответствующий ему шифртекст», и в этом отношении менее требовательный чем дифференциальный криптоанализ. Работа линейного криптоанализа основывается на отклонении поведения блочного алгоритма шифрования от случайного поведения. Это отклонение заключается в том, что если составить множество различных булевых функций (линейных выражений) из бит открытого текста и шифртекста перед последним раундом шифрования, то окажется, что некоторые из них выполняются с большей или меньшей вероятностью чем остальные, несмотря на то, что теоретически все такие выражения должны выполняться с вероятностью равной 0.5. Это отклонение для некоторых алгоритмов шифрования позволяет найти часть последнего подключа с невысокой сложностью.

**Определение:** Линейный криптоанализ – это атака на блочные шифры, основанная на существовании линейной зависимости между битами открытого текста и битами шифртекста на входе последнего раунда шифрования.

Пример линейного выражения:

|  | (1) |
| --- | --- |

Линейный криптоанализ был представлен Matsui на Eurocrypt’93 как теоретическая атака на блочный шифр DES.

Сначала рассмотрим построение линейных выражений для нелинейного элемента блочного шифра. Если линейное выражение составлено из булевых переменных, имеющих равномерное распределение, то вероятность выполнения такого выражения будет стремиться к 0.5.

Будем называть величину, на которую вероятность выполнения линейного выражения отклоняется от в сторону 1 или в сторону 0 *смещением вероятности*. Следовательно, если выражение (1) истинно с вероятностью для случайно выбранных открытых текстов и соответствующих им шифртекстов, тогда смещение вероятности равно .

Чем выше величина вероятности отклонения, тем лучше применимость линейного криптоанализа: требуется меньше количество текстов для атаки. Если смещение вероятности равно +-0.5 то это означает что некоторое линейное выражение полностью линейно (афинно) воспроизводит поведение алгоритма, это возможно только для очень слабых блочных шифров.

Целью линейного криптоанализа является построение линейной модели для r-1 раунда r-раундового блочного алгоритма шифрования. Для построения линейной модели блочного шифра необходимо для каждого раунда кроме последнего выбрать линейное выражение с максимально возможным отклонением вероятности. При этом выражения выбираются таким образом, чтобы выход выражения предыдущего раунда (с учетом линейного преобразования) полностью совпадал с входом линейного выражения последующего раунда (так, чтобы не было «висящих ветвей»).

Перед рассмотрением того, как строятся линейные выражения для одного раунда необходимо рассмотреть лемму, в которой говорится о том, как вычислить смещение вероятности линейной модели зная смещения составляющих ее линейных выражений.

Для определения вероятности линейной модели используется лемма о набегании. Рассмотрим две случайные бинарные переменные , тогда , будет линейным выражением, а , будет аффинным выражением.

Предположим, что распределение вероятностей равно:

Если две случайные переменные являются независимыми, тогда:

тогда

.

Обозначим

и получим в результате подстановки

.

Эти рассуждения могут быть расширены более чем на две двоичные переменные. Матсуи предложил следующую лемму, которая предполагает, что все n случайных двоичных переменных являются независимыми:

|  | (2) |
| --- | --- |

или, что эквивалентно

| . | (3) |
| --- | --- |

**Определение:** линейной характеристикой элемента блочного шифра называется **таблица линейной аппроксимации**, которая отражает вероятность выполнения каждого возможного линейного выражения, описываемого произвольной комбинацией входных и выходных бит исследуемой подстановки. Исходя из определения очевидно, что ее размерность составляет , как и размерность таблицы распределения разностей.

Так для случайного блока подстановки размерности 4 бита:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0 | 6 | 7 | 9 | B | 5 | E | 4 | A | 1 | 8 | 2 | F | C | 3 | D |

таблица линейной аппроксимации, вычисленная с использованием программы TSBox, представлена на рисунке 1.



Строки этой таблицы соответствуют всем возможным комбинациям входных бит подстановки, столбцы этой таблицы соответствуют всем возможным комбинациям выходных бит. Значения в строке и столбце представлены в шестнадцатеричной системе. Каждой ячейке этой таблицы соответствует некоторое линейное выражение, описываемое комбинациями входных и выходных бит. Значение в ячейке является количеством случаев, в которых выражение выполняется, из которого вычли . От этого значения легко перейти к смещению вероятности от путем деления числа в ячейке на .

Рисунок 1: Таблица линейной аппроксимации

Для выбора линейных выражений (ячеек) используется два критерия:

1. максимально-возможная по модулю величина отклонения вероятности от ;
2. минимальный (но больше 0) вес Хэмминга выходной комбинации бит в линейном выражении.

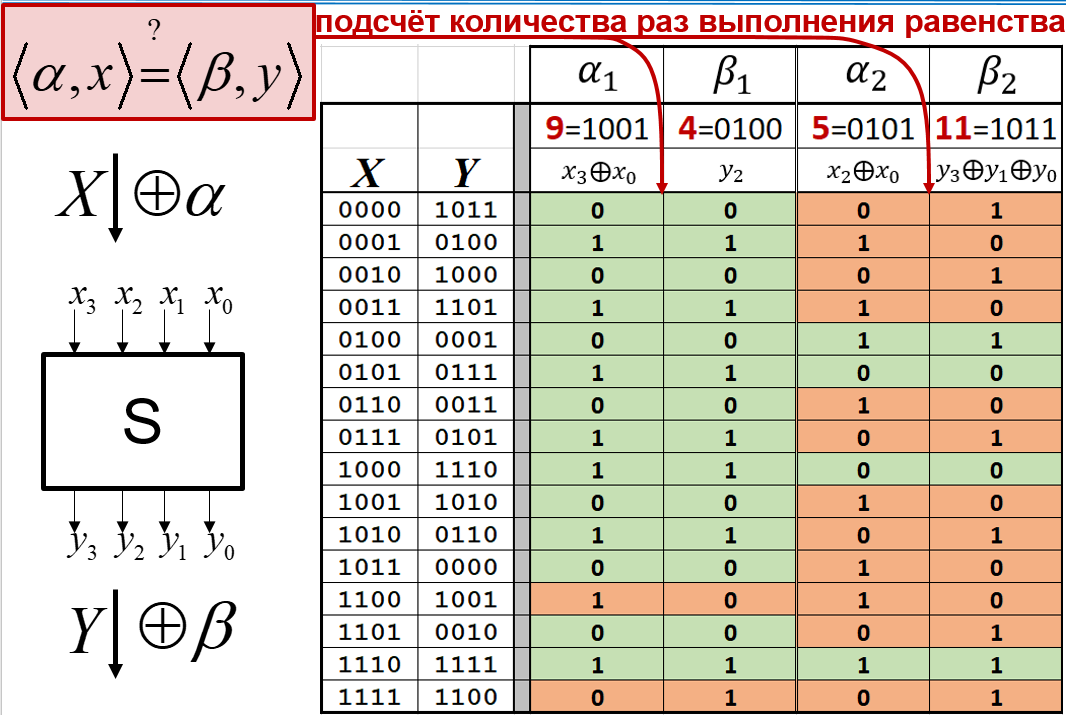
***Вес Хэмминга*** *– это число единиц в двоичном представлении страниц.*

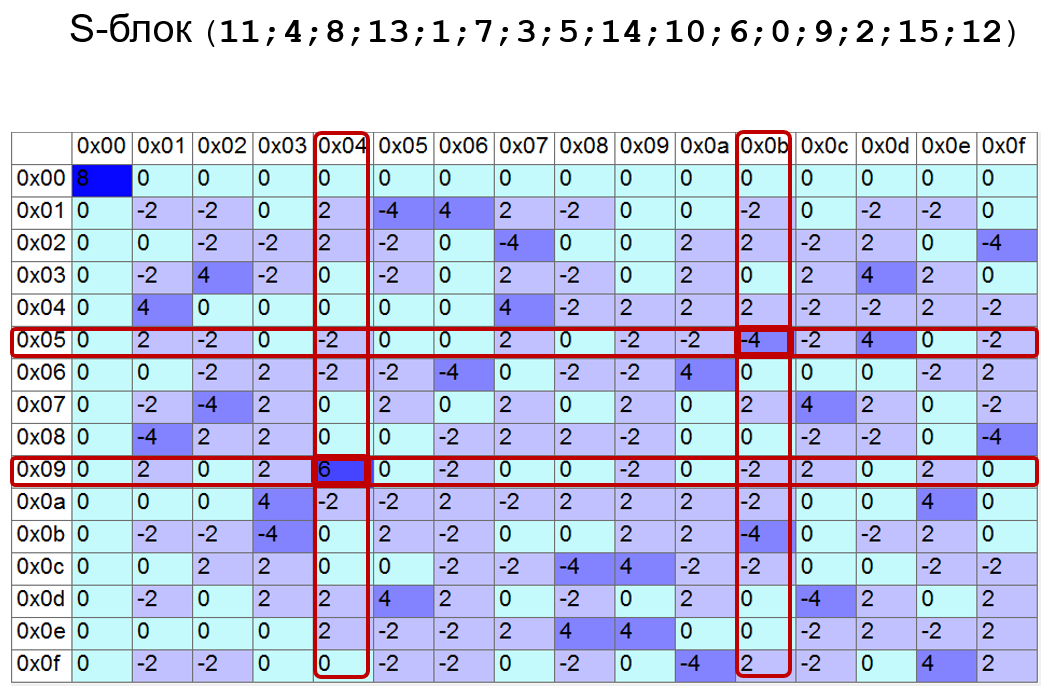
Так, например, выражение , соответствующее ячейке (0x0e, 0x01), согласно таблице линейной аппроксимации имеет отклонение вероятности и так как его выходная разность имеет минимальный вес Хэмминга, равный 1, то это линейное выражение целесообразно использовать для построения линейной характеристики.

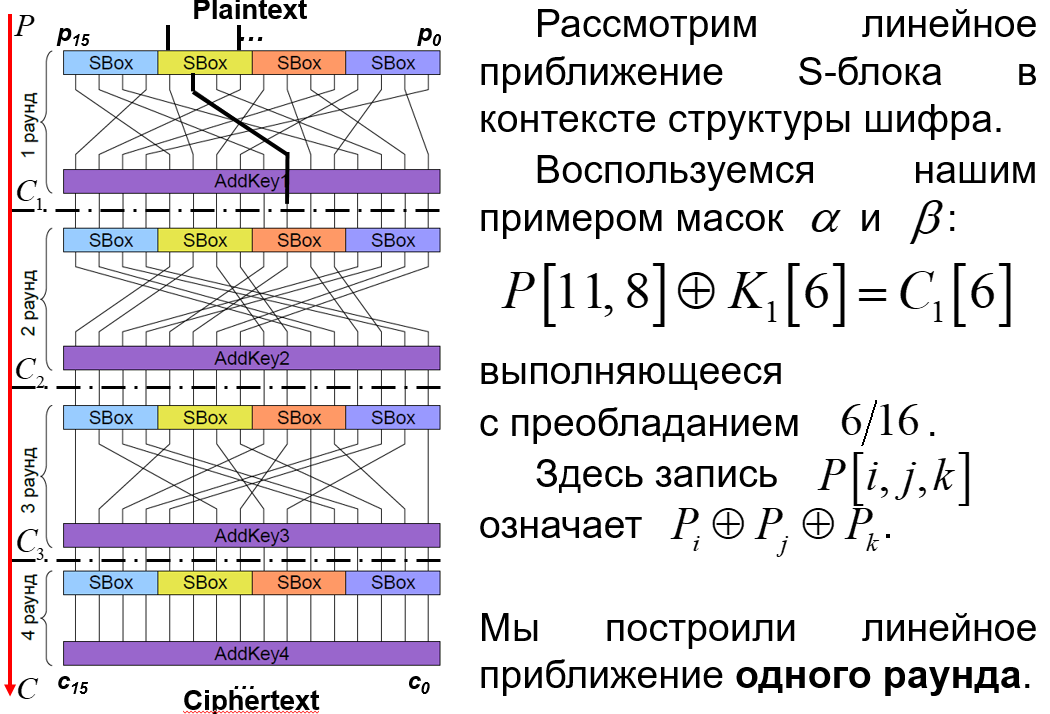
Линейные выражения, смещения вероятностей которых равно 0 при построении линейной модели, использовать нельзя.

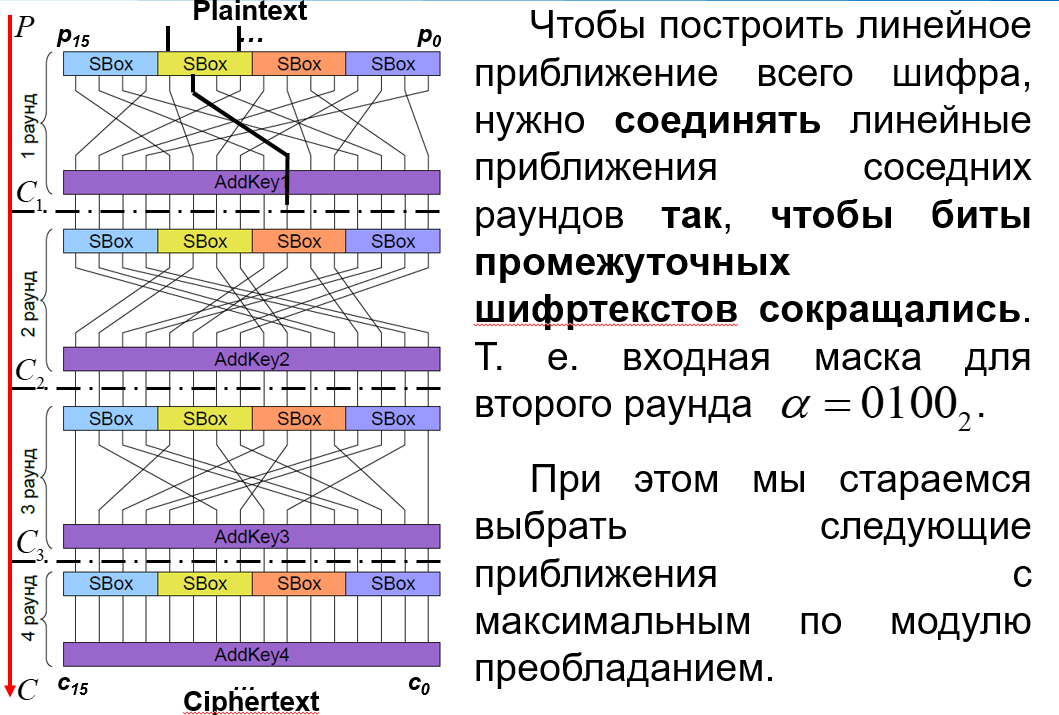
Связывание линейных выражений от одного раунда к другому выполняется так, чтобы ненулевые биты выходного линейного выражения одного раунда были связаны с входными ненулевыми битами линейного выражения следующего раунда. Это позволяет построить линейную модель, состоящую из набора входных переменных и набора выходных переменных, соответствующих значению шифртекстов на входе последнего раунда алгоритма шифрования.

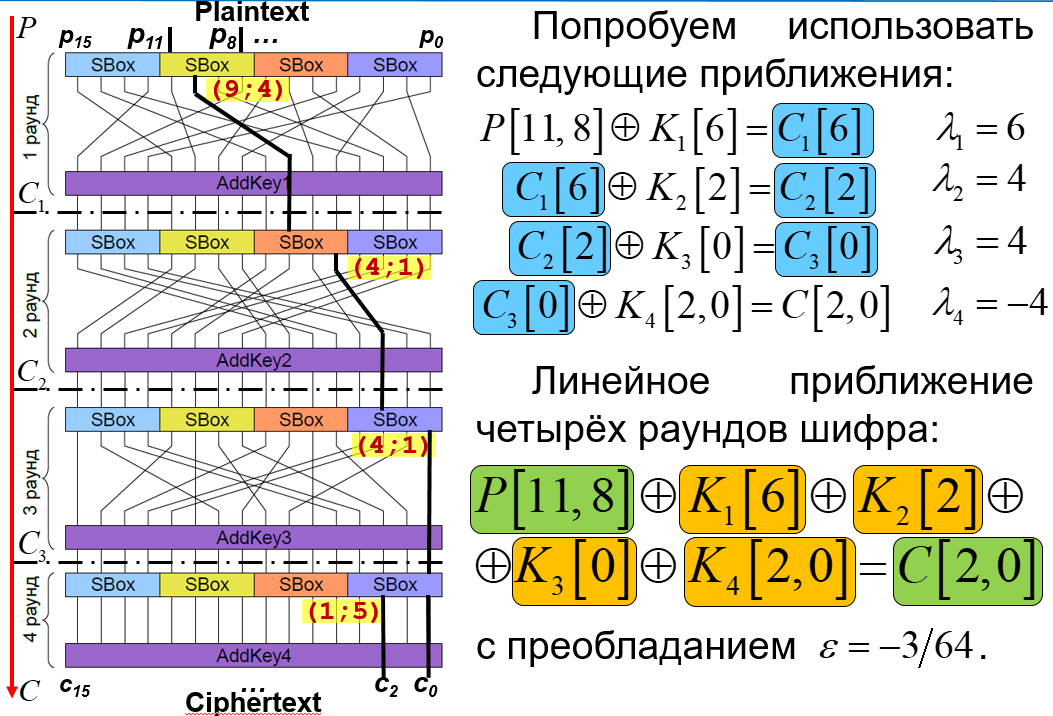
Рассмотрим пример построения линейной модели.

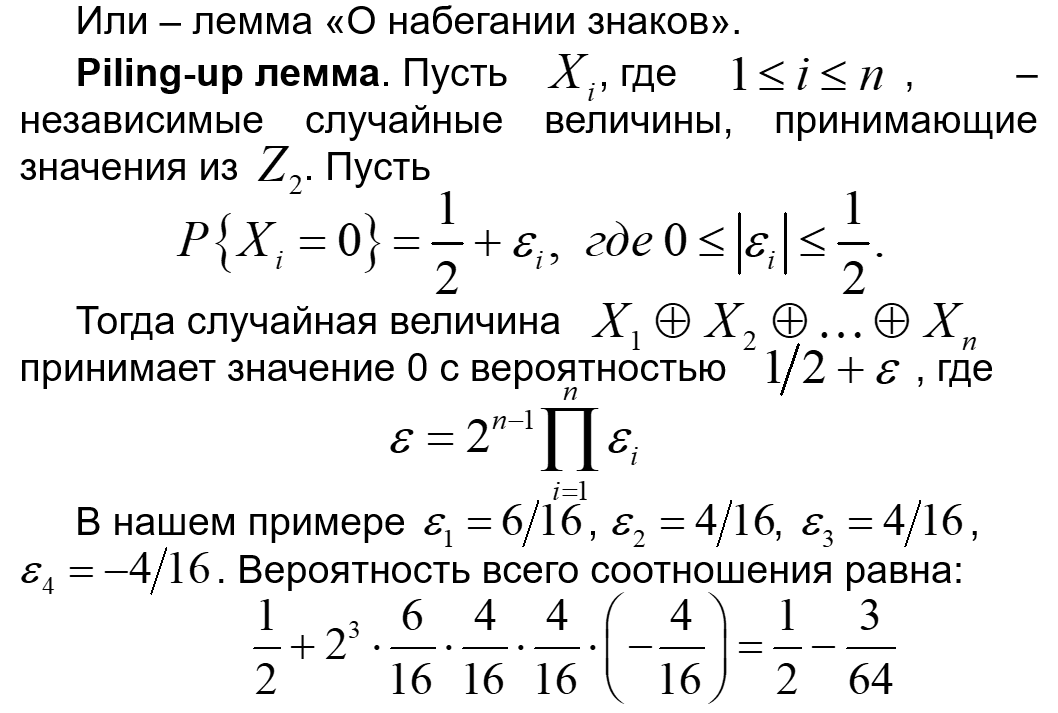


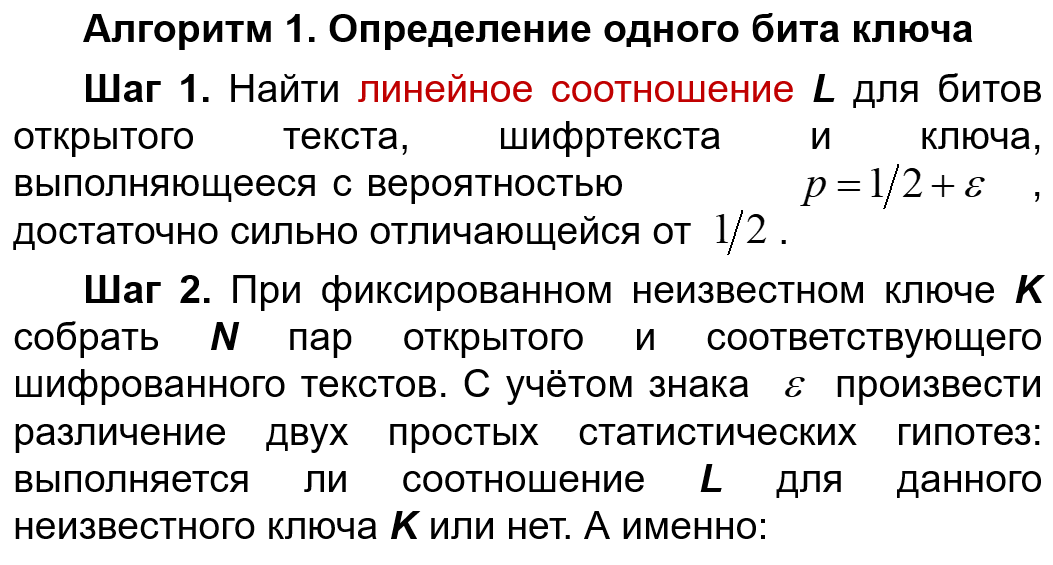


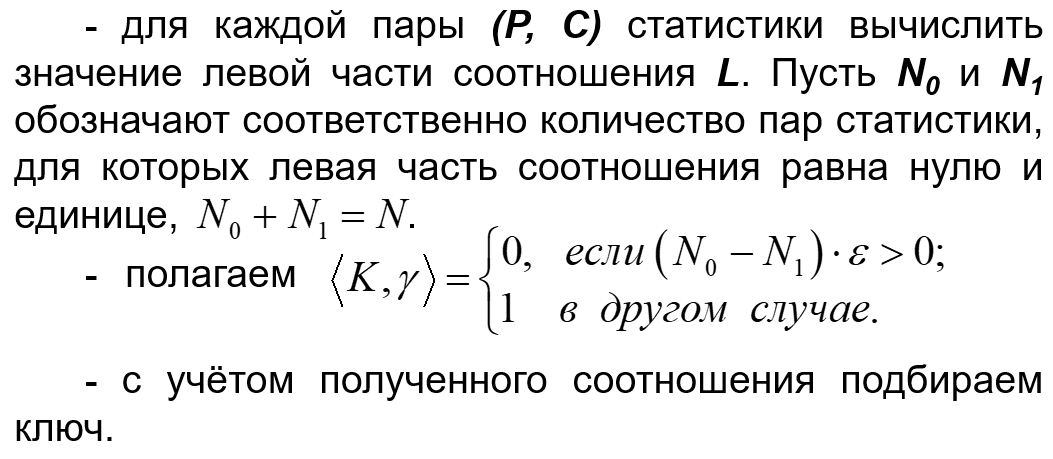


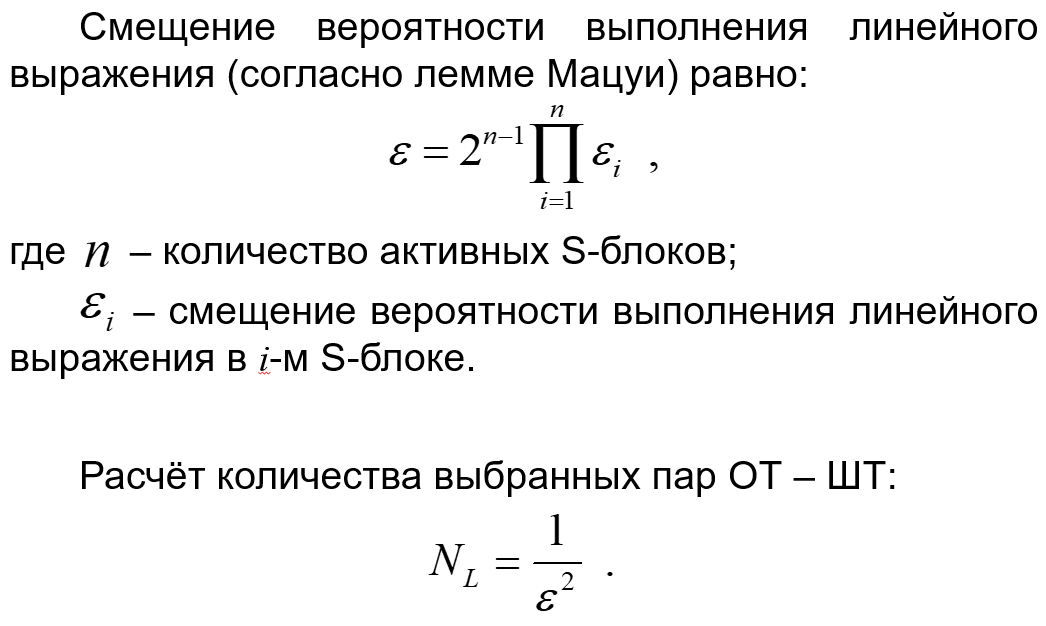












# Задание

В качестве исходного материала для выполнения задания используется учебный блочный шифр. Он имеет размер блока 16 бит и размер ключа 64 бита и состоит из 4 раундов. Каждый раунд состоит из добавления подключа с помощью операции «исключающего или», слоя подстановок, состоящего из 4 одинаковых 4-битных подстановок, и перестановки бит различной для каждого раунда. В последнем раунде битовая перестановка не производится. Схема блочного шифра приведена на рисунке:

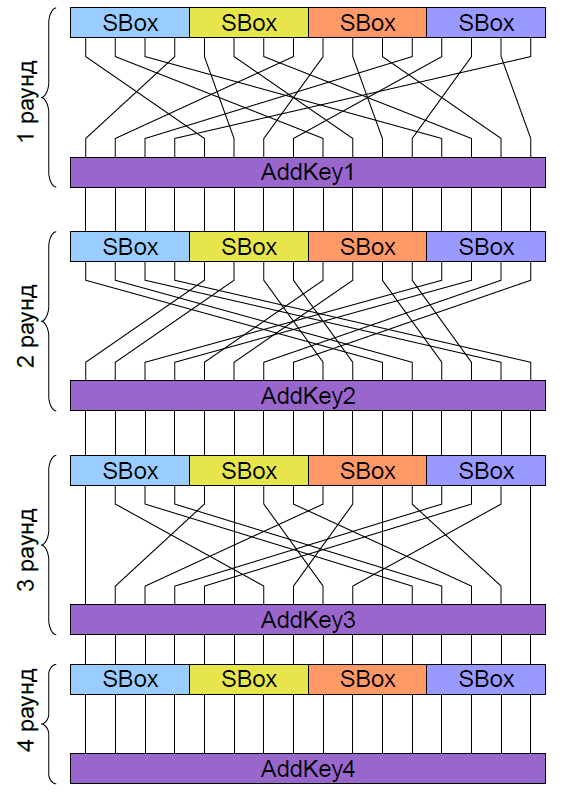


Рисунок 4: Построение одной строки таблицы распределения разностей

Подстановка приведена в таблице:

| 0x00 | 0x01 | 0x02 | 0x03 | 0x04 | 0x05 | 0x06 | 0x07 | 0x08 | 0x09 | 0x0a | 0x0b | 0x0c | 0x0d | 0x0e | 0x0f |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0x09 | 0x0a | 0x0c | 0x04 | 0x00 | 0x08 | 0x01 | 0x06 | 0x0e | 0x0f | 0x07 | 0x0d | 0x03 | 0x02 | 0x05 | 0x0b |

# Решение

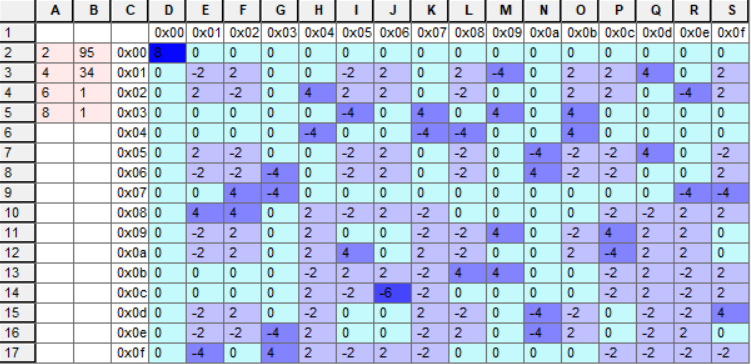


Рисунок 5: Построение таблицы распределения разностей

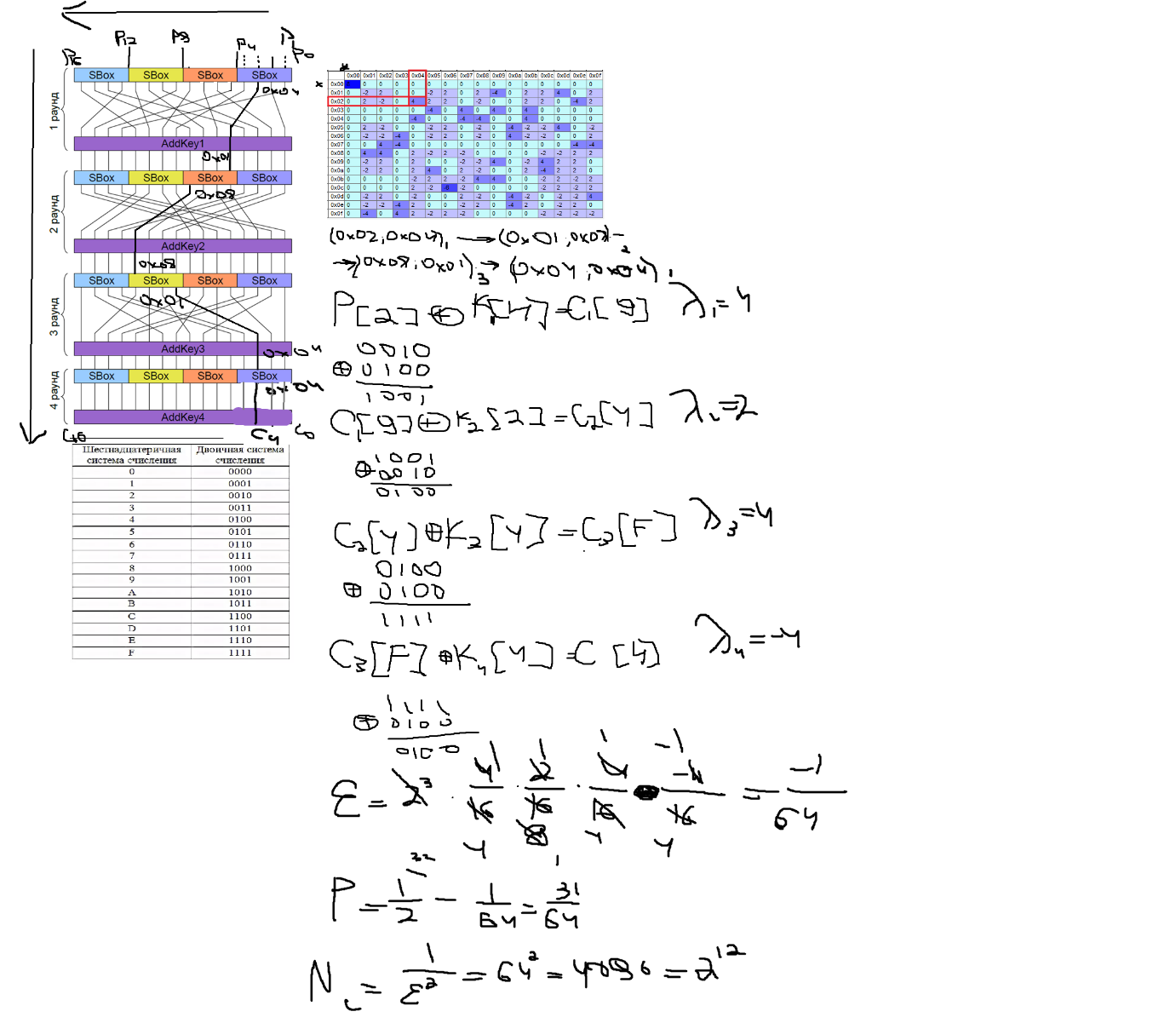


Рисунок 6: Результаты вычислений и дифференциальная модель

# Вывод

В ходе выполнения работы был реализован линейный анализ учебного шифра и получены данные для восстановления ключа.