Министерство образования и науки Российской Федерации

Южный Федеральный Университет

Институт математики, механики и компьютерных наук им. И.И.Воровича

Кафедра алгебры и дискретной математики

Реферат

По курсу «Криптография»

«Шифр Е2 и его криптоанализ»

Выполнил:

Студент 4 курса 1 группы

Пашков Данил

**Введение**

Шифр E2- блочный шифр, с размером блока 128 бит, созданный компанией NTT. Шифр основывается на сети Фейстеля и справочной таблице, не имеет сдвигов и арифметических операций(за исключением произведений в IT-функции(преобразователь начальных данных) и FT-функции (преобразователь конечных данных)). Более того, шифр E2 имеет строго байт-ориентированную структуру; все операции, используемые на фазе рандомизации данных, - это поиск в байтовой таблице и побитовый xor, за исключением 32-битных произведений в IT-функции и FT-функции, что успешно делает шифр E2 быстрым программным шифром независимо от целевой платформы: от 8-битных микропроцессоров до 64-битных компьютеров с архитектурой RISC.

**Алгоритм шифрования**

Работу алгоритма шифрования можно разделить на три основные части: IT-функция, ячейка Фейстеля на базе F-функции, повторяющаяся 12 раз, и FT-функция. Блок алгоритма, отвечающий за планировку ключей (англ. *key sheduling part*), до начала шифрования из секретного ключа К создает шестнадцать подключей {k1,..k16}, каждый из которых является 128-разрядным битовым вектором (элементом поля Галуа(2^128)). Первое преобразование открытого текста M производится с помощью IT-функции и двух сгенерированных ключей под номерами 13 и 14(){\displaystyle k\_{13}}{\displaystyle k\_{14}}.

)

разбивается на два блока  {\displaystyle L\_{0}} и {\displaystyle R\_{0}} равной длины, каждый из элементов {\displaystyle L\_{0}} {\displaystyle L\_{0}} и {\displaystyle R\_{0}} является битовым вектором размерностью 64 бита. Затем выполняются 12 циклов преобразований в ячейке Фейстеля, в которой правый блок на текущей итерации цикла {\displaystyle R\_{0}}  определяется сложением по модулю два левой части предыдущей итерации цикла {\displaystyle R\_{r-1}} и результата функции F, аргументами которой являются правая часть предыдущей итерации {\displaystyle R\_{r-1}} и ключ {\displaystyle k\_{r}}, а левому блоку на **r** шаге цикла присваивается значение правого блока на **r-1** шаге. Цикл повторяется 12 раз, то есть r изменяется от 1 до 12

,{\displaystyle k\_{r}})

Финальный этап шифрования — выполнение FT-функции. Результат FT-функции, аргументами которой являются конкатенация правой {\displaystyle R\_{12}} и левой {\displaystyle L\_{12}} частей на выходе 12 итерации ячейки Фейстеля и ключи {\displaystyle k\_{1},k\_{2}}:

**Алгоритм расшифрования**

Расшифрование происходит по схеме, аналогичной шифрованию. Работу алгоритма шифрования можно разделить на три основные части: IT-функция 12 циклов ячейки Фейстеля с F-функцией и в конце FT-функция Блок алгоритма, отвечающий за планировку ключей из секретного ключа непосредственно перед шифрованием генерирует 16 подключей , которые являются битовыми векторами размерностью 128 (элементом поля Галуа GF(2^128)). На первом этапе происходит выполнение IT-функции, аргументами которой являются криптограмма и два подключа .

Результат IT-функции разбивается на 2 равные части по 64 бита(половина блока): правую и левую ().  Далее выполняются 12 циклов ячейки Фейстеля на базе F-Функции (**{\displaystyle r}r** меняется от 12 до 1).

,{\displaystyle k\_{r}})

По завершении последнего цикла ячейки Фейстеля осуществляется конкатенация половинок блока (). И в конце — финальное преобразование: выполняется FT-функция, аргументами которой являются результат конкатенации  и два ключа . Результатом выполнения FT-функции является открытый текст {\displaystyle M}MM.

)

**Криптоанализ алгоритма**

Сотрудниками компании Information Technology R&D Center Mitsubishi Electric Corporation Мицуру Мацуи (*Mitsuru Matsui*) и Тосио Токита (*Toshio Tokita*) была обнаружена нестойкость шифра к дифференциальному анализу. Несмотря на это шифр (использующий 12 циклов шифрования) остается стойким с практической точки зрения. Хотя Мицуру Мацуи и Тосио Токита удалось показать, что уровень безопасность шифра E2 с меньшим числом циклов шифрования существенно ниже того, что заявлено разработчиками.

**Распределение характеристик байтов раундовой функции**

Шифр E2 был спроектирован таким образом, что для изменения одного любого байта исходных данных раундовой функции,может быть изменено не менее пяти выходных байтов (в частности, пять или шесть байтов). Например, легко проверить, что если мы изменим a1, оставив оставшиеся семь байтов неизменными, то g1, g2, g3, g4, g5 и g7 всегда будут изменяться, в то время как оставшиеся два байта никогда не изменяются.

Очевидно, что эта схема расположения байтов не зависит от количества изменений

в байте a1. Это правило перехода опишем следующим образом:

(10000000)->(11111010) p=1. (1)

Когда же мы одновременно меняем два входных байта раундовой функции, то существует ровно два шаблона изменений выходных байтов. Например, когда мы меняем байты a1 и a5 одновременно, то в случае, если сумма изменения c1 (Δc1) равна сумме изменений c5 (Δc5), тогда только три байта g1, g5 и g8 будут изменены, в противном случае все байты, кроме g6, будут изменены. При условии, что входные значения (от a1 до a8) и величина изменений (Δa1 и Δa5) подаются случайным образом, первый случай случается с приближенной вероятностью (точное значение составляет 1/255). Эти правила перехода описываются следующим образом:

(10001000)->(10001001) p= (2)

(10001000)->(11111011) p=1 (3)

Аналогично мы можем применить это обозначение к произвольному числу байтовых изменений. Одной из наиболее полезных байтовых характеристик раундовой функции шифра E2 является следующий «циклический байт», шаблон входных данных которого совпадает с шаблоном выходных данных. Эта характеристика имеет место, когда

Δc1 = Δc4 = Δc6, с вероятностью = :

(10010100)->(10010100) p= (4)

Кроме того, далее будет использоваться следующая характеристика:

(10110000)->(10000010) p= (5)

**Распределение характеристик байтов шифра Е2**

Используя циклическую характеристику, показанную в (4), можно получить семь раундовых характеристик шифра E2 (без функций IT и FT), как показано на рисунке 5. Нужн отметить, что операция xor вне раундовой функции может аннулировать различия; то есть 1 ⊕ 1 = 0 с вероятностью 1/255 и 1 ⊕ 1 = 1 с вероятностью 254/255. Для простоты

мы будем рассматривать эти вероятности как и 1 соответственно. На рисунке 5, это аннулирование происходит три раза (в трёх байта) в операции xor после шестой раундовой функции. В результате характеристика седьмого раунда сохраняется с приблизительной вероятностью × = .

Это означает, что при одновременном изменении первого, четвертого и шестого байтов блок открытого текста без изменения остальных байтов, после седьмого

раунда, вероятность того, что три байта на соответствующих местах изменятся, а другие байты нет, становится равной . С другой стороны, если раундовая функция является случайной , ожидается, что такое же изменение произойдет снова с вероятностью = , так как число неизмененных байтов составляет тринадцать. Поэтому ожидаемое число «правильных пар» совпадает с ожидаемым числом «неправильных пар».

Правильные пары могут быть обнаружены с вероятностью в предположении, что количество различий указанных входных байт (Δa1, Δa4 и Δa6 в данном случае) задаются случайным образом. Однако, если мы можем задать пары открытого текста с неслучайными различиями в выбранном сценарии открытого текста, то эта вероятность может быть больше. Фактически, когда мы генерируем входные пары открытого текста таким образом, что выполняется уравнение Δa1 = Δa4 = Δa6, то вероятность перехода функции второго раунда возрастает примерно до 9,3 × , а не , что является экспериментальным результатом. Причина этого увеличения основана на том, что следующая вероятность значительно больше , когда Δx = Δy, тогда как ожидается, что оно будет составлять в среднем , когда Δx Δy.

P(Δx Δy)

Точная вероятность P (Δx, Δy) зависит от структуры подстановки в таблице S, но нетрудно доказать, что S P (Δx, Δy) > ,когда Δx = Δy. Также следует отметить, что это может быть использовано в нашем анализе шифра E2, поскольку E2 имеет только одну таблицу замещения в своей раундовой функции. Если функция S левой части отличается от функции S правая части в вышеприведенном определении, то распределение P (Δx, Δy) будет «прямым», не зависящим от Δx и Δy.

**Возможные сценарии атаки шифра E2**

**1)Сокращённый до 7-ми раундов шифр Е2 без функций IT и FT.**

Из выводов предыдущих разделов видно, что для шифра E2, сокращенного до семи раундов, когда для выбранных пар открытого текста, выполняется: ΔP1 = ΔP4 = ΔP6, ожидаемое число пар зашифрованных пар, имеющих разностный шаблон

(10010100 00000000) равный 9.3, где P1, P4 и P6 обозначают первый, четвертый и шестой байты открытого текста, соответственно. Эти пары открытого текста могут быть получены из блоков сообщений открытого текста (97 = 104-8 + 1); например, они даются как набор прямых произведений из всех возможных шаблонов левой части открытых текстов и произвольно выбранных шаблонов правой части.

С другой стороны, для случайной перестановки с теми же выбранным парами открытого текста, ожидаемое число пар зашифрованного текста, которые имеют разностный шаблон

(10010100 00000000) равен 1. Это приводит к следующему сценарию для различия шифра E2, уменьшенного до семи раундов от случайной перестановки:

*Если для данного шифра количество пар зашифрованного текста, которые имеют разностный шаблон (10010100 00000000) больше либо равно заданному значению t, то рассматриваем его как шифр E2, сокращенный до семи раундов, иначе рассматриваем его как случайную перестановку.*

Чтобы оценить соответствующее значение для t, нам понадобится следующая лемма:

**Лемма 1.** Когда проводится испытание, в котором происходит событие с вероятностью p раз, считая p достаточно близким к 0 и i достаточно малым, по отношению к , то вероятность того, что событие произойдет ровно i раз, равна

(7)

Используя эту лемму, мы видим, что t = 4 может быть принято в нашем случае; для шифра E2, уменьшенного до семи раундов, вероятность того, что количество пар зашифрованного текста, имеющих разностный шаблон (10010100 00000000) больше либо равен четырех составляет 98%, тогда как для случайной перестановки вероятность ожидается равной 2%.

**2)Сокращённый до 7-ми раундов шифр Е2 без функций IT и FT.**

Применяя снова семи раундовые характеристики для первых семи раундов шифра E2, сокращенного до восьми раундов без функций IT и FT, мы можем ограничить вероятности подключа окончательного (восьмого) раунда с использованием следующего алгоритма:

*Для каждого кандидата в подключ финального раунда расшифруйте все пары зашифрованного текста за один раунд. Тогда, если количество пар, имеющих разностный шаблон (10010100 00000000) после седьмого раунда меньше предопределенного значения t, отбрасывать неверный подключ как ложного кандидата.*

Рассмотрим = 8 × выбранных пар открытого текста, таких что ΔP1 = ΔP4 =ΔP6. Тогда, если кандидат является правильным подключом,то ожидаемое количество пар, которые имеют разностный шаблон (10010100 00000000) после седьмого раунда, равно 8 × 9,3 = 74,4; однако, если это неправильный подключ, то ожидаемое количество пар равно 8. Эти пары открытого текста могут быть получены с использованием блоков сообщений открытого текста(100 = 107-8 + 1).

Прямое вычисление с использованием леммы 1 показывает, что t = 60, например, может быть достаточно, чтобы сузить вероятности подключа финального раунда. В частности, для правильного подключа, вероятность того, что количество пар, имеющих разностный шаблон (10010100 00000000) после седьмого раунда больше либо равна 60 составляет 96%, тогда как для неправильного подключа ожидается, что вероятность равна

.

Прямой метод реализации алгоритма выше имеет сложность более , но, отбрасывая невозможные пары и вводя метод подключа второго уровня с счетчиками, мы можем уменьшить сложность до < .

**{\displaystyle k\_{13},k\_{14}}{\displaystyle M}**