Пас из-за границы – атака на ГОСТ

Чиликов Алексей Анатольевич,
МГТУ им. Баумана

Краткое содержание

- Алгоритм шифрования ГОСТ 28147-89
- «Японская» атака (T. Isobe, FSE’2011) – основные характеристики
- Детальное описание атаки
  - Reflection Points
  - Разделение ключей
  - Оценки сложности
- Итоговые замечания

ГОСТ 28147-89

- Стандарт шифрования с 1989
- Действует в настоящее время
- Опубликованных атак до сих пор не было!

ГОСТ 28147-89

- Блочный шифр
- Размер ключа – 256 бит
- Размер блока – 64 бита
- Схема Фейстеля

- 32 раунда
- 8 раундовых ключей по 32 бита
- Раундовый ключ испоьзуется 4 раза
- Порядок подключей: 0-7, 0-7, 0-7, 7-0

ГОСТ 28147-89

- Вход: (L[0], R[0]) – 2 слова по 32 бита
- Выход: (R[32], L[32]) – 2 слова по 32 бита
- Описание раунда:
  - L[i+1] = R[i] ^ F(K[i]+L[i])
  - R[i+1] = L[i]
- После последнего раунда меняется порядок L и R
- Расшифрование такое же, но с обратным порядком раундовых ключей
- F – нелинейная функция
- Для атаки достаточно лишь биективности F

Характеристики атаки

- Takanori Isobe, FSE’2011
- Сложность по времени: T ~ 2^225
- Сложность по данным: D ~ 2^32
- Known Plaintext Attack
- Single-Key Model

Reflection Points

- L[i+1] = R[i] ^ f(k, L[i])
- R[i+1] = L[i]

- L[i] = R[i+1]
- R[i] = L[i+1] ^ f(k[i], R[i+1])

- Что если?
  - (L[i], R[i]) = (R[2m-i], L[2m-i])
  - K[i] = K[2m+1-i]

- L[i-1] = R[2m-(i-1)]
- R[i-1] = L[2m-(i-1)]

Reflection Points

- Ключи для раундов 16-31 повторяются и используются в симметричном порядке
- K[24] = K[23], K[25] = K[22], …, K[31] = K[16]

- Если L[24] = R[24], то (L[16], R[16]) = (R[32], L[32])
- Это и есть reflection point
- Количество reflection point – 2^32 (из 2^64)

- P –> (0-15 раунды) –> C –> (16-31 раунды) –> C

- Среди 2^32 пар (P,C) с большой вероятностью найдётся хотя бы один reflection point (неизвестно, какой)

Разделение ключей

- Пусть (P, C) – reflection point
- Обозначим:
  - P –> (K[0..3]) –> S –> (K[4..7]) –> X –> (K[0..3]) –> T –> (K[4..7]) –> C
- S – 2^64 вариантов
- T – 2^64 вариантов
- При известных (P, C):
  - S зависит только от K0 = K[0]||K[1]||K[2]||K[3]
  - T зависит только от K1 = K[4]||K[5]||K[6]||K[7]

Эквивалентность ключей

- Пусть U -> K[0..3] -> V

- Лемма: Для любых (U, V) существует в точности 2^64 ключей K = K[0]||K[1]||K[2]||K[3], таких что U -> V

- Зададим K[0], K[1] произвольно
- U -> K[0..1] -> X -> K[2..3] -> V
- Обозначим U = (Ul, Ur), V = (Vl, Vr), X = (Xl, Xr)
- X легко вычисляется по U, K[0], K[1]

Эквивалентность ключей

- Vr = Xr ^ F(Xl + K[2])
- Vl = Xl ^ F(Vr + K[3])
- =>
- K[3] = F^{-1}(Vl ^ Xl) - Vr
- K[2] = F^{-1}(Vr ^ Xr) – Xl

- => Для любых K[0], K[1] существуют подходящие K[2], K[3]

- Т.о., для любых (U, V) существует в точности 2^64 подходящих ключей

- Такие ключи назовём эквивалентными

Разделение ключей

- Пусть (P, C) – reflection point
  - P -> (K[0..3]) -> S -> (K[4..7]) -> X -> (K[0..3]) -> T -> (K[4..7]) -> C
- Зададим S (2^64 вариантов)
- Построим все эквивалентные K0 для P, S (2^64 вариантов)
- Получаем таблицу S, K0 (2^128 вариантов)
- Аналогично строим таблицу T, K1 (2^128 вариантов)

Разделение ключей

P -> (K[0..3]) -> S -> (K[4..7]) -> X -> (K[0..3]) -> T -> (K[4..7]) -> C

- Задаём пару S, T (2^128 вариантов)

- Выбираем все возможные K0 и вычисляем возможные X (2^64 вариантов) – левая таблица
- Выбираем все возможные K1 и вычисляем возможные X (2^64 вариантов) – правая таблица
- Строим пересечение левой и правой таблиц (~2^64 вариантов)
- Подходящие ключи восстановлены!

- Итого: для всех 2^128 (S,T) по 2^64 ключей – всего 2^192

Схема атаки

- Для каждой пары (P,C) предполагаем, что это reflection point
- Строим по описанной схеме 2^192 ключей
- Каждый из ключей проверяем по другим парам (P’,C’)
- Вероятность ложного срабатывания ~ 2^{-64}
- Достаточно ~ 5 пар для проверки
- Требуется ~ 2^32 пар для попадания в reflection point

Оценка сложности

- Для фиксированной пары (S,T) строятся 2 таблицы по 2^64 элементов и пересекаются
- Сложность по времени ~ 2^64+2^64 = 2^65

- Сложность по памяти ~ 2^65
- Для фиксированной пары (P,C) строятся 2^128 пар (S,T) – 2^128 вызовов проверки
- Сложность по времени ~ 2^128 * 2^65 = 2^193

- Требуется набрать и проверить ~2^32 пар (P,C)
- Общая сложность по времени ~ 2^32*2^193 = 2^225
- Общая сложность по данным ~ 2^32

Заключительные замечания

- Атака основана на reflection point => требуется на менее 2^32 пар (P,C)
- Сама атака использует лишь один блок
- Используются не все соотношения, а лишь соотношения на первые 16 раундов
- Для любой пары (P,C) найдутся примерно 2^{256-64}=2^192 ключа, удовлетворяющие этим соотношениям – т.е., атака оптимальна

- Если использовать соотношения на последние раунды, подходящих ключей будет 2^{256-64-32} = 2^160 для каждой пары (P,C)
- Таким образом, оптимальная атака на основе одного блока потребует 2^32 * 2^160 = 2^192

Заключительные замечания

- Что будет, если использовать несколько пар (P,C)?

- Reflection Points неотличимы от других блоков
- Атака:
  - Выбрать n пар (P[i],C[i])
  - Выявить подходящие ключи
  - Проверить по остальным парам
- Сложность 1 шага: $L1 > 2^{32*n} * n^n / n!$
- Сложность 2 шага: $L2 > 2^{256 - 96*n}$
- Лучший вариант – n = 3, $L > 2^{98}$

Вывод: Атаки такого класса (даже оптимальные) неприменимы на практике!

Вопросы?

- chilikov@passware.com