

9 Разностная атака

9.1 Разностная атака

Пусть F — действующая на $\{0, 1\}^n$ d -тактовая итерационная криптосистема. Разностная атака на F проводится при выбираемом открытом тексте. Противнику разрешено выбирать пары открытых текстов (X, \tilde{X}) и получать соответствующие пары шифртекстов $(F_K(X), F_K(\tilde{X}))$.

Противник выбирает X и \tilde{X} так, что *разность* $\Delta X = X \oplus \tilde{X}$ принимает специальное фиксированное значение.

Эта разность порождает последовательность разностей

$$\Delta Y(1) = Y(1) \oplus \tilde{Y}(1), \dots, \Delta Y(d) = Y(d) \oplus \tilde{Y}(d),$$

где $Y(i), \tilde{Y}(i)$ — результаты выполнения i тактов преобразования $F_K = \Sigma_{\kappa_d} \dots \Sigma_{\kappa_1}$ над X и \tilde{X} соответственно.

Последовательность $(\alpha, \beta(1), \dots, \beta(r))$ возможных значений разностей $\Delta X, \Delta Y(1), \dots, \Delta Y(r)$ называется *r -тактовой характеристикой*, а пара $(\alpha, \beta(r))$ значений $(\Delta X, \Delta Y(r))$ — *r -тактовым дифференциалом*, $1 \leq r \leq d$. Тривиальные характеристики $(0, 0, \dots, 0)$ и дифференциалы $(0, 0)$ в разностном анализе не рассматриваются.

В предположении, что X, \tilde{X} — случайные слова с равномерным на $\{0, 1\}^n$ распределением, а случайные тактовые ключи $\kappa_1, \dots, \kappa_d$ независимы и равномерно распределены на множестве тактовых ключей \mathcal{K} , введем *вероятность характеристики*

$$\mathbf{P} \{ \Delta Y(1) = \beta(1), \dots, \Delta Y(r) = \beta(r) \mid \Delta X = \alpha \}$$

и *вероятность дифференциала*

$$\mathbf{P} \{ \Delta Y(r) = \beta(r) \mid \Delta X = \alpha \}.$$

Цель атаки. Целью атаки является определение последнего тактового ключа κ_d (полностью или частично). Используя оценки $\hat{\kappa}_d$ можно вычислять значения

$$Z(Y, \tilde{Y}; \hat{\kappa}_d) = \Sigma_{\hat{\kappa}_d}^{-1}(Y) \oplus \Sigma_{\hat{\kappa}_d}^{-1}(\tilde{Y}).$$

Предварительный этап. Криптоаналитик находит $(d-1)$ -тактовый дифференциал $(\alpha, \beta(d-1))$ с максимально возможной вероятностью p . Сразу скажем, что для успеха атаки требуется выполнения условия $p > 1/(2^n - 1)$.

Поиск высоковероятного дифференциала — непростая задача, успешное решение которой зависит от квалификации криптоаналитика. Криптоаналитик должен тщательно изучить криптосистему, провести исследование разностных характеристик S -блоков, характеристик перемешивания P -блоков и др.

Обычно вместо высоковероятного дифференциала $(\alpha, \beta(d-1))$ криптоаналитик ищет высоковероятную характеристику $(\alpha, \beta(1), \dots, \beta(d-1))$ и использует оценки:

$$\begin{aligned} p &\geq \mathbf{P} \{ \Delta Y(1) = \beta(1), \dots, \Delta Y(r) = \beta(d-1) \mid \Delta X = \alpha \} \\ &\approx \mathbf{P} \{ \Delta Y(1) = \beta(1) \mid \Delta X = \alpha \} \mathbf{P} \{ \Delta Y(2) = \beta(2) \mid \Delta Y(1) = \beta(1) \} \dots \\ &\quad \mathbf{P} \{ \Delta Y(d-1) = \beta(d-1) \mid \Delta Y(d-2) = \beta(d-2) \}. \end{aligned}$$

Оперативный этап атаки проводится следующим образом:

1. Криптоаналитик случайным образом выбирает открытые тексты $X_t \in \{0, 1\}^n$ и определяет шифртексты $Y_t = F_K(X_t)$, $\tilde{Y}_t = F_K(X_t \oplus \alpha)$, $t = 1, \dots, T$.
2. В качестве оценки κ_d выбирается значение $\hat{\kappa}_d$, доставляющее максимум сумме

$$W(\hat{\kappa}_d) = \sum_{t=1}^T \mathbf{I} \{ Z(Y_t, \tilde{Y}_t; \hat{\kappa}_d) = \beta(d-1) \}.$$

Сложность атаки. Проведем грубый анализ сложности атаки (более тонкий анализ предполагает использование свойств конкретной криптосистемы). Если $\hat{\kappa}_d = \kappa_d$, то

$$\mathbf{E}W(\hat{\kappa}_d) = \sum_{t=1}^T \mathbf{P} \left\{ Z(Y_t, \tilde{Y}_t; \hat{\kappa}_d) = \beta(d-1) \right\} = Tp.$$

Если же $\hat{\kappa}_d \neq \kappa_d$, то естественно считать, что слова $Z(Y_t, \tilde{Y}_t; \hat{\kappa}_d)$ принимают случайные значения из $\{0, 1\}^n \setminus \{0\}$ и в этом случае

$$\mathbf{E}W(\hat{\kappa}_d) = \sum_{t=1}^T \mathbf{P} \left\{ Z(Y_t, \tilde{Y}_t; \hat{\kappa}_d) = \beta(d-1) \right\} = T/(2^n - 1).$$

Для того, чтобы атака приводила в среднем к нужному результату требуется, чтобы

$$Tp - T/(2^n - 1) \geq 1,$$

откуда

$$T \geq \frac{1}{p - 1/(2^n - 1)}.$$

Пример 9.1. Блочная криптосистема DES была принята в качестве стандарта шифрования США в 1977 г. Долгое время не удавалось предложить атаки на DES, сложность которых была бы существенно меньше сложности атаки «грубой силой». Первым успехом явилась как раз разностная атака, предложенная в 1991 г. Бихамом и Шамиром. В предложенной атаке использовались две 13-тактовых разностных характеристики с вероятностью $\approx 2^{-47.2}$. Атака позволяет определить 52 бита информации о двух последних тактовых ключах с вероятностью 0.58 при анализе 2^{47} пар «открытый текст — шифртекст». \square

9.2 Модельная криптосистема \mathbf{G}

Методы криптоанализа мы будем иллюстрировать на примере модельной 8-тактовой криптосистемы Фейстеля \mathbf{G} . Длина ключа \mathbf{G} — 32 бита, длина блока — 16 битов.

Ключу $K = (K_1, K_2, K_3, K_4)$, $K_i \in \{0, 1\}^8$, ставится в соответствие последовательность тактовых ключей

$$\kappa_1 = K_1, \quad \kappa_2 = K_2, \quad \kappa_3 = K_3, \quad \kappa_4 = K_4, \quad \kappa_5 = K_1, \quad \kappa_6 = K_2, \quad \kappa_7 = K_3, \quad \kappa_8 = K_4.$$

Тактовая функция $f_\kappa: \{0, 1\}^8 \rightarrow \{0, 1\}^8$ ставит в соответствие слово x слово

$$f_\kappa(x) = S_1(u_1) \parallel S_2(u_2) \lll 3, \quad u = u_1 \parallel u_2 = x \oplus \kappa.$$

S -блоки действуют на $\{0, 1\}^4 \sim \mathbb{Z}_{16} \sim \mathbb{F}_{17}^*$ по правилам:

$$S_1(x) = ((3^x \bmod 17) + 2) \bmod 16, \quad S_2(x) = ((5^x \bmod 17) + 7) \bmod 16, \quad x = 0, 1, \dots, 15$$

(3 и 5 — примитивные элементы \mathbb{F}_{17}).

Упражнение 9.1. Построить таблицы S -блоков S_1, S_2 . \square

9.3 Разностная атака на криптосистему \mathbf{G}

Проиллюстрируем разностную атаку на примере модельной криптосистемы \mathbf{G} .

Анализ тактовой функции. Рассмотрим тактовую функцию f_κ криптосистемы \mathbf{G} . Анализируя вид f_κ , устанавливаем, что для $\gamma = 10000000$ выполняется:

$$\begin{aligned} \mathbf{P} \{ \Delta f_\kappa = \gamma \mid \Delta x = \gamma \} &= \mathbf{P} \{ S_1(x_1 \oplus \kappa_1) \oplus S_1(x_1 \oplus \kappa_1 \oplus \alpha) = \beta \} = \\ &= \mathbf{P} \{ S_1(x_1) \oplus S_1(x_1 \oplus \alpha) = \beta \} = \\ &= \mathbf{P} \{ \Delta S_1 = \beta \mid \Delta x_1 = \alpha \}. \end{aligned}$$

Здесь $\alpha = 1000$ и $\beta = 0001$.

Напомним, что $S_1(x_1) = ((3^{x_1} \bmod 17) + 2) \bmod 16$. Прямыми расчетами устанавливаем, что $\mathbf{P}\{\Delta S_1 = \beta \mid \Delta x_1 = \alpha\} = \frac{1}{4}$.

Таким образом, $\mathbf{P}\{\Delta f_\kappa = \gamma \mid \Delta x = \gamma\} = \frac{1}{4}$, т. е. f_κ сохраняет разность γ с высокой вероятностью. Подобного рода слабости как раз и позволяют использовать методы разностного анализа.

Характеристика. Для проведения разностной атаки на \mathbf{G} можно использовать 7-тактовую характеристику следующего вида:

$$\begin{aligned}\alpha &= \gamma \parallel \mathbf{0} \\ \beta(1) &= \mathbf{0} \parallel \gamma \quad (\text{с вероятностью } 1) \\ \beta(2) &= \gamma \parallel \gamma \quad (\text{с вероятностью } 1/4) \\ \beta(3) &= \gamma \parallel \mathbf{0} \quad (\text{с вероятностью } 1/4) \\ \beta(4) &= \mathbf{0} \parallel \gamma \quad (\text{с вероятностью } 1) \\ \beta(5) &= \gamma \parallel \gamma \quad (\text{с вероятностью } 1/4) \\ \beta(6) &= \gamma \parallel \mathbf{0} \quad (\text{с вероятностью } 1/4) \\ \beta(7) &= \mathbf{0} \parallel \gamma \quad (\text{с вероятностью } 1),\end{aligned}$$

где $\gamma = 10000000$, а значения вероятностей определялись с помощью предыдущего примера. Вероятность характеристики $p = 2^{-8}$.

Поскольку $p \gg 2^{-n} = 2^{-16}$, найденную характеристику можно использовать для определения последнего тактового ключа $\kappa_8 = K_4$.

Детальный анализ показывает, что имеются *неразличимые* ключи-кандидаты $\hat{\kappa}_8$, которые доставляют одинаковые значения целевой функции $W(\hat{\kappa}_8)$. Поэтому удастся определить только 3 бита κ_8 , для этого требуется обработать ≈ 2000 пар «открытый текст — шифртекст».