

ДУКПТ: Доказательство, Устраняющее Критические Пробелы в Теории

Фомин Денис Бониславович

Рассмотрим противника $\mathcal{A}$, взаимодействующего с оракулом, реализующим либо настоящую схему PRF (гипотеза H_1), либо случайную функцию (гипотеза H_0).

Обозначим через Y вектор всех ответов, полученных нарушителем от оракула в ходе эксперимента. Пусть D_1 и D_0 — распределения Y в случае H_1 и H_0 соответственно.

Определение

Вычислительно ограниченное статистическое расстояние для нарушителя $\mathcal{A}$, имеющего доступ к оракулу в течение времени T и сделавшего не более q запросов, определяется как

$$\delta_{\mathcal{A}}(T, q) := \sup_{A \subseteq \Omega} |\mathbb{P}[Y \in A \mid H_1] - \mathbb{P}[Y \in A \mid H_0]|.$$

Лемма

Пусть $\mathcal{A}$ — произвольный вероятностный нарушитель, Y — наблюдаемый вектор ответов. Тогда:

$$\text{Adv}_{\text{DUKPT}}^{fs\text{-PRF}}(\mathcal{A}) = |\mathbb{P}[Y \in A \mid H_1] - \mathbb{P}[Y \in A \mid H_0]|,$$

где $A = \mathcal{A}^{-1}(1)$ — множество выходов, при которых нарушитель принимает гипотезу H_1 .

Следствие

$$\text{Insec}_{\text{DUKPT}}^{fs\text{-PRF}} = \delta_{\mathcal{A}}(T, q).$$

Понятие вычислительно ограниченного статистического расстояния можно естественным образом воспринимать в соответствии с классической парадигмой теории вероятностей, когда неопределённость, вызванная отсутствием информации, описывается вероятностной моделью.

Если субъект (в данном случае нарушитель) не обладает полной информацией о реализации случайного эксперимента, то его поведение и предположения формализуются в виде случайных величин и вероятностных событий.

δ_A — «мера отличимости» двух распределений, достижимая нарушителем A за время T .

DUKPT вырабатывает множество ключей: $CWK_1, CWK_2, \dots, CWK_n$.

Согласно модели fs-PRF нарушитель может знать все CWK_i , кроме одного, например, CWK_t .

Задачей нарушителя в этом случае является отличить CWK_t от случайной последовательности той же длины.

Пусть $P = (p_1, \dots, p_N)$ — апостериорное распределение ключа CWK_t , как результат действий нарушителя $\mathcal{A}$ за время T .

Тогда:

$$\delta_{\mathcal{A}}(T) := \frac{1}{2} \sum_{i=1}^N \left| p_i - \frac{1}{N} \right|.$$

Используя Proposition 1 из работы¹, можно получить нижнюю границу среднего количества шагов Q , необходимого для нахождения CWK_t методом перебора:

Утверждение (по Proposition 1)

Если $2\delta_{\mathcal{A}}(T) < \pi_0$, где π_0 — фиксированная вероятность успеха атаки, то

$$Q \geq \left(1 - \frac{2\delta_{\mathcal{A}}(T)}{\pi_0}\right) \cdot \frac{N(1 - 8\delta_{\mathcal{A}}(T)) + 1}{2},$$

где $N = 2^k$ — мощность пространства значений ключа CWK_t .

Для практически значимых значений π_0 и полученного значения²
 $\delta_{\mathcal{A}}(T, q) = \text{Insec}_{\text{DUKPT}}^{\text{fs-PRF}}$, а также длины ключа $k = 256$, получаем, что $\log_2(Q) = 255$.

¹Арбеков И.М. *Нижние оценки для практической секретности ключа* // Матем. вопр. криптогр. Т. 8(2), стр. 29–38. — 2017

²И. Махонин, Л. Ахметзянова, С. Смышляев. *О стойкости функции выработки производных ключей DUKPT*. — CTCrypt 2025

**Ты должен был бороться
со злом,**

а не примкнуть к нему