

Лекция №1

Часть 4. Семантическая стойкость.

Елена Киршанова
Курс “Основы криптографии”



Информационно-теоретическая vs. семантическая стойкость

ОТР

любые атакующие

Большие ключи $|\mathcal{K}| = |\mathcal{M}|$

Фиксированная длина t

Вычислительный шифр

вычислительно ограниченные атакующие

несколько сотен бит

Любая длина t



Семантическая безопасность: формальное определение

$$\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$$

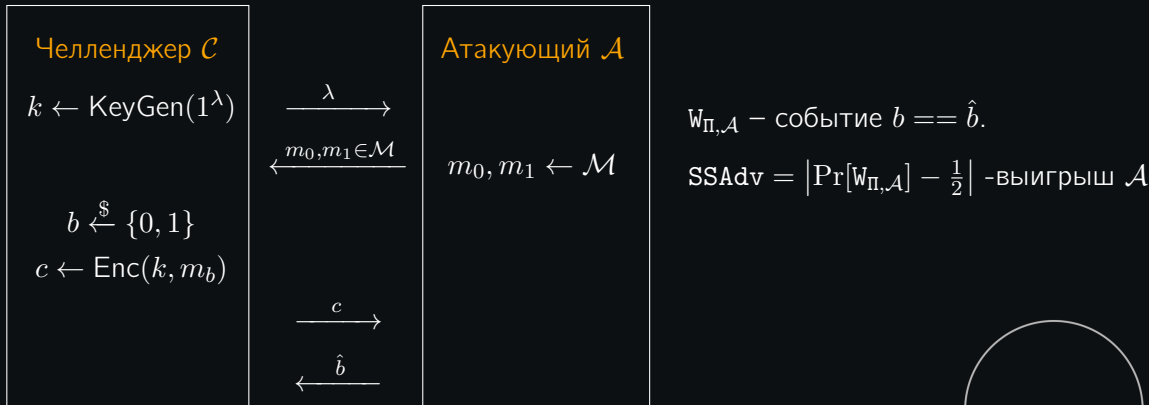


Схема Π –семантически безопасна, если для любого ppt \mathcal{A} :

$$\text{SSAdv} = \text{negl}(\lambda).$$

Семантическая безопасность ОTR

Теорема. Для абсолютно стойкой схемы (ОТР) и для всех атакующих \mathcal{A} выполняется

$$\Pr[w_{\Pi, \mathcal{A}}] = \frac{1}{2}.$$

Эквивалентно

$$\text{SSAdv} = |\Pr[w_{\Pi, \mathcal{A}}] - 1/2| = 0.$$

“Взлом” абсолютно стойкой схемы эквивалентен угадываю ключа.



Следствия семантической безопасности

Теорема.

$\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$ – семантически стойкая схема. Тогда \forall ppt \mathcal{A}

$$\Pr[\mathcal{A}(\text{Enc}(k, m)) \rightarrow m[i]] \leq \frac{1}{2} + \text{negl}(\lambda) \quad \forall i.$$

То есть семантически безопасная схема стойка к угадыванию i -ого бита открытого текста.

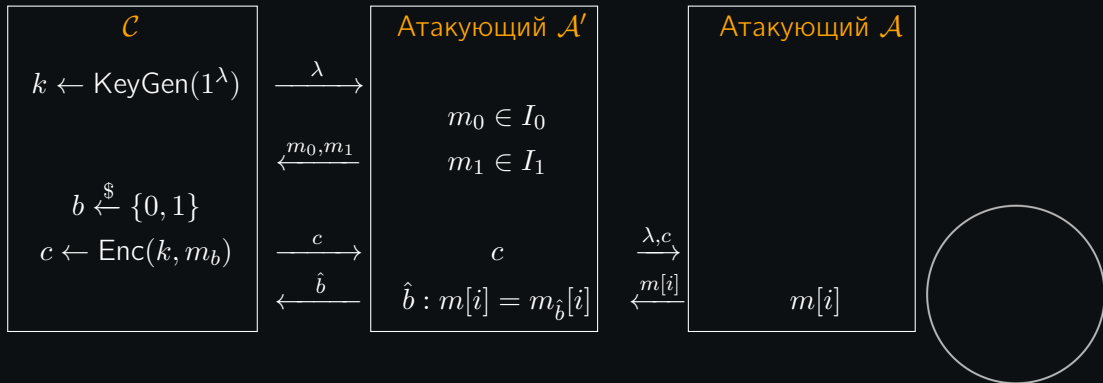


Доказательство редукцией

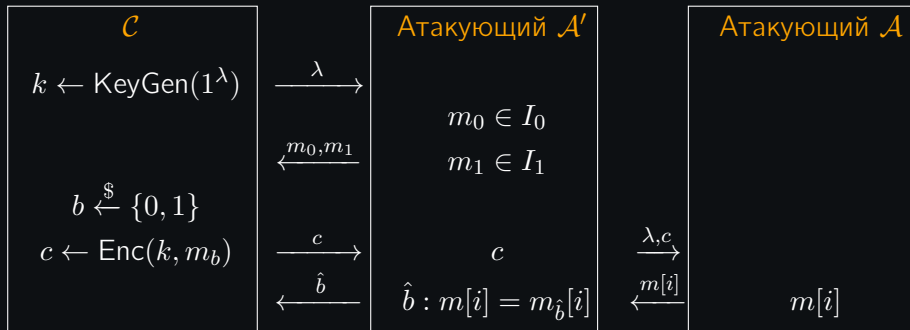
$$I_0 = \{m \in \mathcal{M} \mid m[i] = 0\} \quad I_1 = \{m \in \mathcal{M} \mid m[i] = 1\}$$

$$\Pr[\mathcal{A}(\text{Enc}(k, m)) \rightarrow m[i]] \leq \frac{1}{2} + \text{negl}(\lambda)$$

Построим \mathcal{A}' , отличающий шифр-тексты I_0 от шифр-текстов I_1 .



Доказательство редукцией



Следствия семантической безопасности

Теорема.

$\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$ – семантически стойкая схема. Тогда \forall ppt атакующего \mathcal{A} существует \mathcal{A}' :

$$|\Pr[\mathcal{A}(\lambda, \text{Enc}(k, m)) \rightarrow f(m)] - \Pr[\mathcal{A}'(\lambda) \rightarrow f(m)]| \leq \text{negl}(\lambda).$$

То есть семантически безопасная схема стойка к вычислению *любой* эффективной функции $f(m)$.

