Лекция №1

Часть 4. Семантическая стойкость.

Елена Киршанова

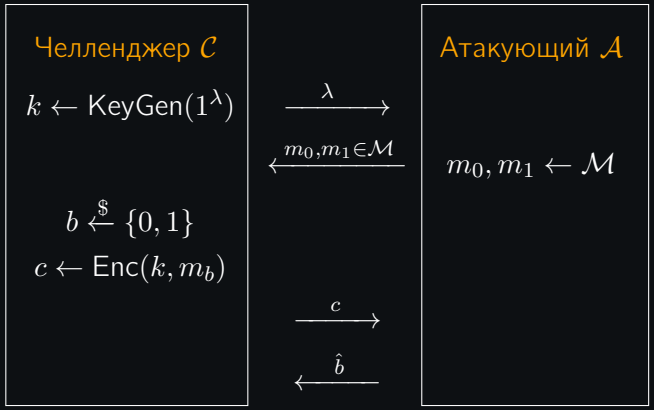
Курс “Основы криптографии”

Информационно-теоретическая vs. семантическая стойкость

OTP	Вычислительный шифр
любые атакующие	вычилительно ограниченные атакующие
Большие ключи $\|\mathcal{K}\| = \|\mathcal{M}\|$	несколько сотен бит
Фиксированная длина m	Любая длина m

Семантическая безопасность: формальное определение

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



$\mathtt{W}_{\Pi,\mathcal{A}}$ – событие $b == \hat{b}$.

$\mathtt{SSAdv} = \left|\Pr[\mathtt{W}_{\Pi,\mathcal{A}}] - \frac{1}{2}\right|$ -выигрыш $\mathcal{A}$

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

$$\mathtt{SSAdv} = \mathrm{negl}(\lambda).$$

Семантическая безопасность OTP

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

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

Эквивалентно

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

“Взлом” абсолютно стойкой схемы эквивалентен угадываю ключа.

Следствия семантической безопасности

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

$$\Pr[\mathcal{A}(\mathsf{Enc}(k, m)) \to m[i]] \leq \frac{1}{2} + \mathrm{negl}(\lambda) \qquad \forall i.$$

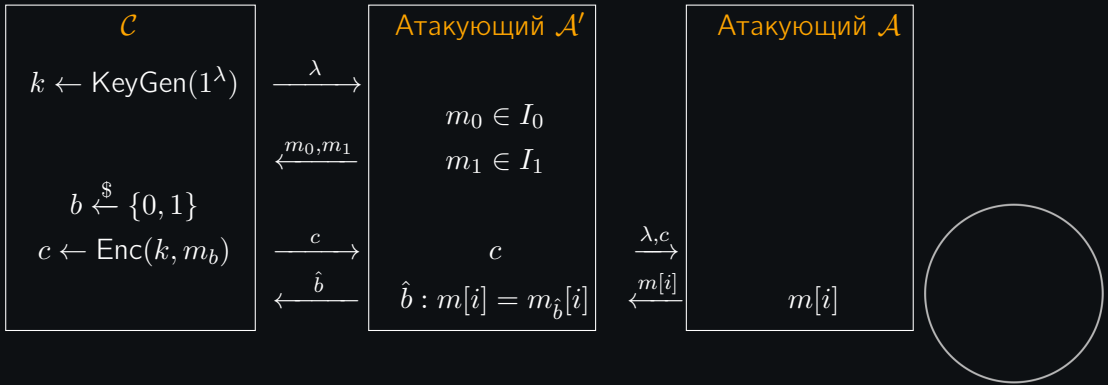
То есть семантически безопасная схема стойка к угадыванию i-ого бита открытого текста.

Доказательство редукцией

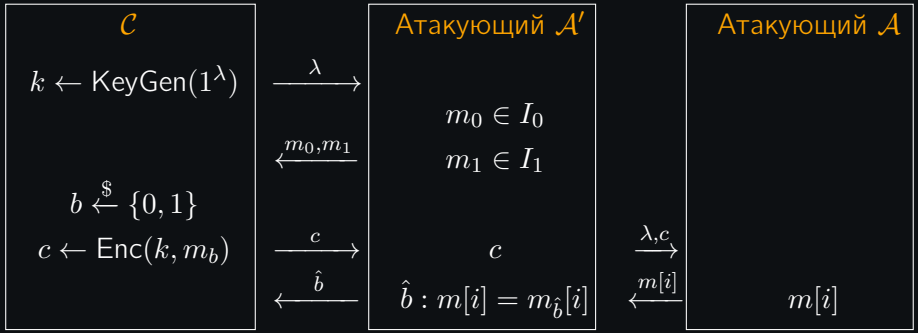
$$I_0 = \{m \in \mathcal{M} \mid m[i] = 0\} \quad I_1 = \{m \in \mathcal{M} \mid m[i] = 1\}$$

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

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



Доказательство редукцией



Следствия семантической безопасности

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

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

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