Прикладная Криптография: Симметричные криптосистемы Абсолютная и Семантическая стойкость (Акт 2)

Макаров Артём

МИФИ 2020

Эквивалентные определения абсолютной стойкости

Теорема 1.4. Пусть $\mathrm{E} = (E, D)$ - шифр Шеннона на (K, M, C). Рассмотрим вероятностный эксперимент для равномерно распределённой $\boldsymbol{k} \in_R K$.

Тогда E – абсолютно стойкий тогда и только тогда, когда для произвольного предиката $\phi: C \to \{0,1\}$ и $\forall m_0, m_1 \in M$

$$\Pr[\phi(E(\boldsymbol{k}, m_0) = 1] = \Pr\left[\phi\left(E(\boldsymbol{k}, m_1)\right) = 1\right]$$

Иными словами: при использовании произвольного предиката на шифртекстах абсолютно стойкого шифра злоумышленник не получает информации об открытом тексте.

Плохие новости

Теорема 1.7 (Шеннона). Пусть $\mathrm{E} = (E, D)$ шифр Шеннона на (K, M, C). Если E – абсолютно стойкий, то

- $|K| \geq |M|$
- $H(\boldsymbol{k}) \geq H(\boldsymbol{m}), \boldsymbol{k} \in_R K, \boldsymbol{m} \in_R M$

Простое объяснение – невозможно получить равномерно распределённую случайную величину длины m, используя детерминированный алгоритм над равномерно распределённой случайной величиной длины $n < m$.

Иными словами, для шифрования 1 Gb данных **любым** абсолютно стойким шифром потребуется ключ размера как минимум 1 Gb.

Вычислимый шифр

Вычислимый шифр на (K, M, C) – пара **эффективных** алгоритмов $\mathrm{E} = (E, D)$, где $E: K \times M \to C$ – вероятностная функция зашифрования, $D: K \times C \to M$ – функция расшифрования.

- Обозначим процедуры зашифрования как $c \overset{R}{\leftarrow} E(k, m)$.
- Обозначим выбор **равномерно распределённого ключа** как $k \overset{R}{\leftarrow} K$.

При этом $\forall k \in K, m \in M, c \overset{R}{\leftarrow} E(\mathrm{k}, \mathrm{m}), m' \leftarrow D(k, c)\ \Pr[m = m'] = 1$ (**свойство корректности**).

Семантическая стойкость

Пусть $\mathrm{E} = (E, D)$ - вычислимый шифр на (K, M, C).

Теорема 1.3 $\Rightarrow E$ – абсолютно стойкий, если $\forall \phi: C \to \{0,1\}, \mathrm{k} \in_R K$ – равномерно распределённый и выполняется

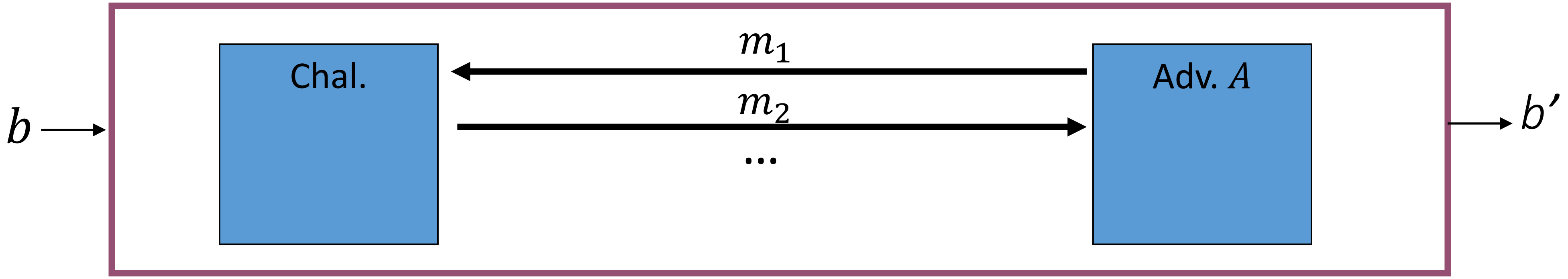
$$\Pr[\phi(E(\boldsymbol{k}, m_0) = 1] = \Pr\big[\phi\big(E(\boldsymbol{k}, m_1)\big) = 1\big]$$

Ослабим свойство абсолютной стойкости: вместо требования равенства вероятностей потребуем чтобы их разность не превосходила величину ϵ:

$$\Pr[\phi(E(\boldsymbol{k}, m_0) = 1] - \Pr\big[\phi\big(E(\boldsymbol{k}, m_1)\big) = 1\big] \le \epsilon$$

Понятие игры

- Игра состоит из двух сторон – **противника** A (**Adversary**) и **претендента** (**Challenger**), моделируемые **эффективными** алгоритмами. При этом алгоритм A – вероятностный
- **Входом** игры называется некоторая величина b
- **Ход игры** – атакующий и претендент обмениваются сообщениями согласно некоторому фиксированному протоколу
- **Результатом** игры называется некоторая величина b'

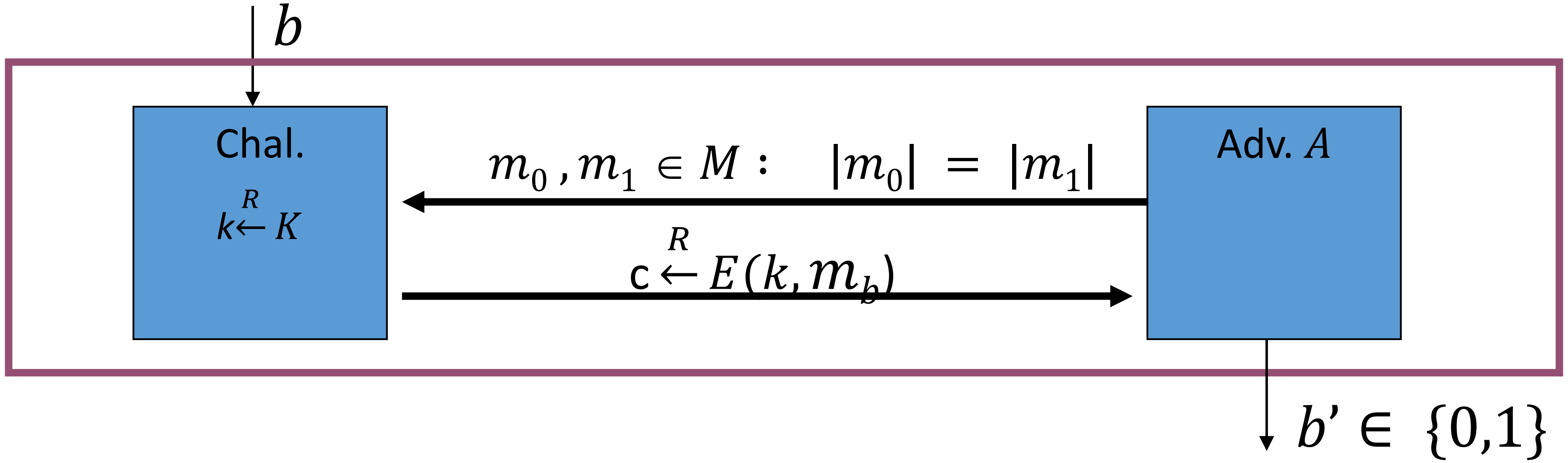


Понятие игры на различимость, определения

- **Входом** игры называется случайное число $b \in \{0,1\}$, неизвестное для атакующего, определяющего эксперимент
- **Экспериментом** $(\mathrm{Exp}\ b)$ называется «режим» претендента при его общении с атакующим
- **Ход игры** – атакующий и претендент обмениваются сообщениями согласно некоторому фиксированному протоколу
- **Цель игры** – атакующий пытается угадать число b (угадать эксперимент)
- **Результатом** игры называется число $b' \in \{0,1\}$ – выход алгоритма A

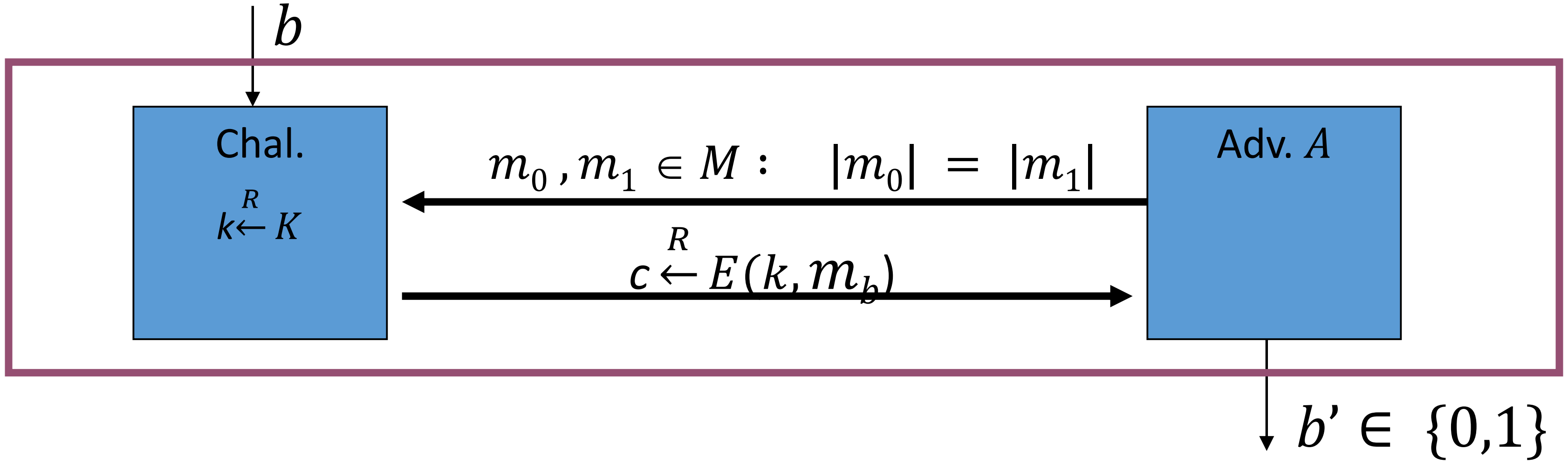
Игра: семантическая стойкость (одноразовое использование ключа)

Для $\mathrm{E} = (E, D)$ - вычислимого шифра на (K, M, C) и противника A определим два эксперимента, Exp. 0 и Exp. 1 следующим образом:



Игра: семантическая стойкость (одноразовое использование ключа)

- Претендент выбирает $k \overset{R}{\leftarrow} K$
- Противник выбирает сообщения $m_0, m_1 \in M$ **одинаковой длины**
- Претендент вычисляет $c \overset{R}{\leftarrow} E(k, m_b)$ и отправляет противнику
- Противник возвращает бит $b' \in \{0,1\}$ как результат игры

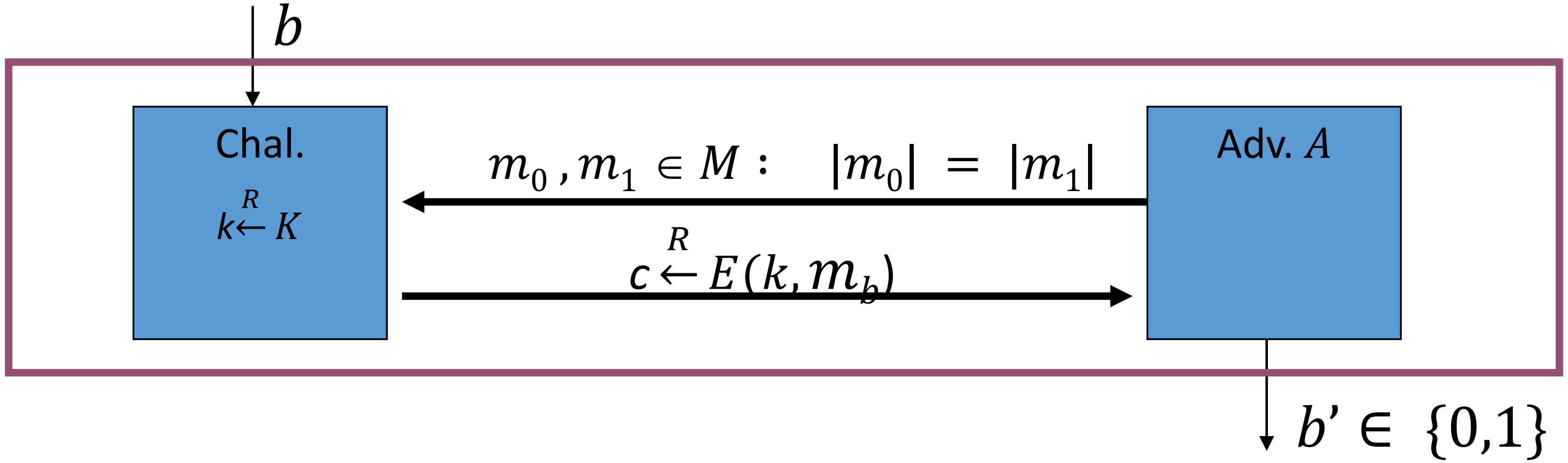


Игра: семантическая стойкость (одноразовое использование ключа)

Пусть W_b - событие того, что $b' = 1$ в эксперименте b.

Преимуществом (**Advantage**) противника A против алгоритма E в игре на семантическую стойкость есть величина:

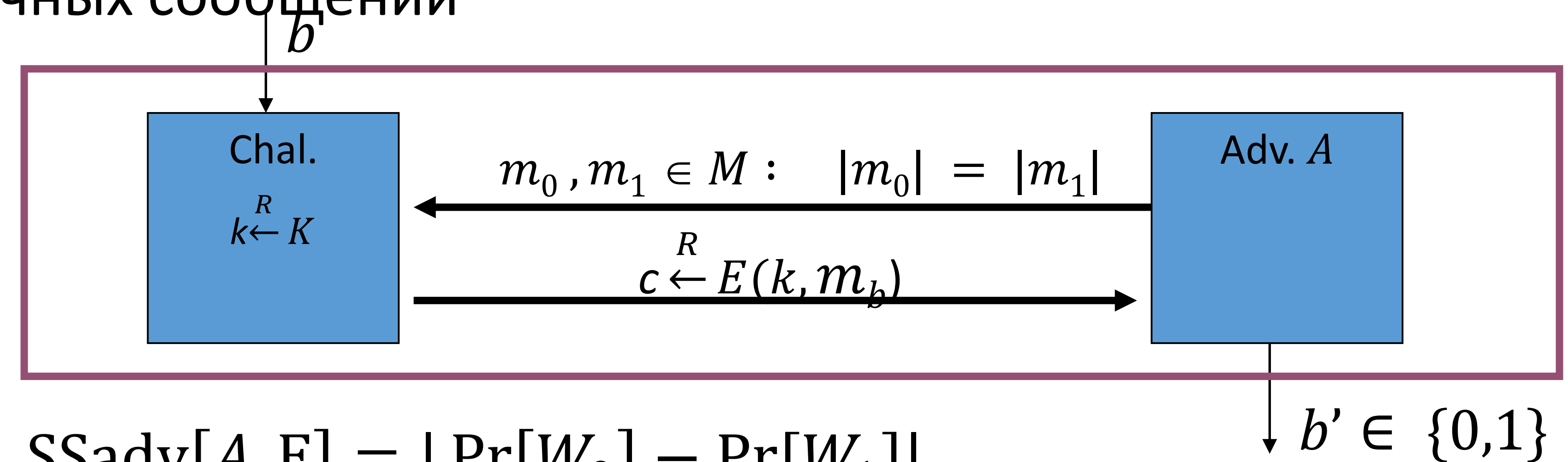
$$\mathrm{SSadv}[A, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]|$$



Семантическая стойкость (одноразовое использование ключа)

Шифр E - (одноразово) **семантически стойкий**, если для всех эффективных противников A величина $\mathrm{SSadv}[A, \mathrm{E}] < \epsilon$ – **пренебрежимо малая величина**

Иными словами – вычислительно невозможно отличить шифррексты различных сообщений



$$\mathrm{SSadv}[A, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]|$$

Семантическая стойкость

- «Ослабленная» версия абсолютной стойкости: только **эффективные противники** и разность вероятностей расшифрования в заданные сообщения **не превосходит** ϵ.
- Позволяет использовать **короткие ключи**

Примеры:

- Одноразовый блокнот – семантически стойкий шифр
- Одноразовый блокнот переменной длины – семантически стойкий шифр
- Шифр подстановки – не семантически стойкий шифр

Построение атаки на семантическую стойкость

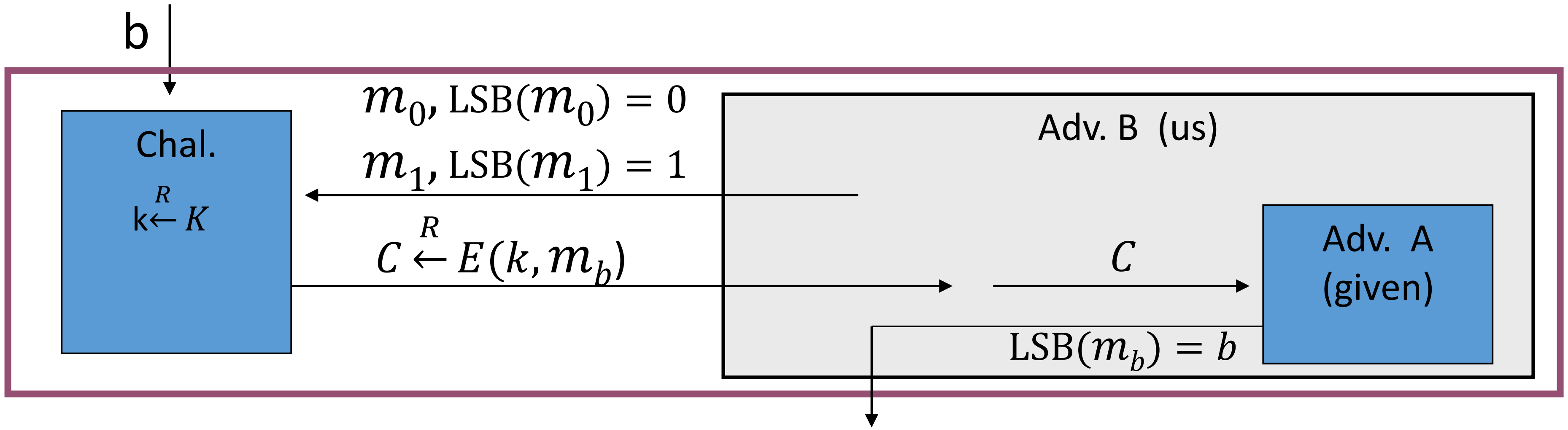
Пусть A – алгоритм позволяющий получить наименее значимый бит (LSB) открытого текста через шифртекст $c \xleftarrow{R} E(k, m)$. Тогда $\mathrm{E} = (E, D)$ – не семантически стойкий шифр.

⊳Построим эффективный алгоритм B, позволяющий выиграть игру на семантическую стойкость.

- Генерация двух сообщений m_0, m_1 с различным наименее значимым битом
- Получение шифртекста c для одного из сообщений
- Передача шифртекста на вход алгоритма A
- Получение наименее значимого бита отрытого текста, определение эксперимента. ⊲

Построение атаки на семантическую стойкость

Пусть A – алгоритм позволяющий получить наименее значимый бит (LSB) открытого текста через шифртекст c $\stackrel{R}{\leftarrow} E(k,m)$. Тогда $\mathrm{E} = (E,D)$ – не семантически стойкий шифр.



$$\mathrm{SSadv}[B, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]| = |1 - 0| = 1$$

Доказательства сведением (Reduction proof)

Пусть $\mathrm{E} = (E, D)$ - вычислимый семантически стойкий шифр на (K, M, C).
Тогда $\mathrm{E}' = (E', D')$: $\begin{cases}(c_0, c_1) = \ E'(k, m) = c||c; c = E(k, m) \\ D'(k, (c_0, c_1)) = D(k, c_0)\end{cases}$ – семантически стойкий шифр.

⊳ От противного. Пусть E' - не семантически стойкий шифр. Тогда $\exists$ противник A: $\mathrm{SSadv}[A, \mathrm{E}'] \geq e$, где e – не пренебрежимо малая величина.

Построим эффективный алгоритм B для игры против семантической стойкости шифра E с использованием алгоритма A, показав тем самым что E – не семантический стойкий ⇒ противоречие ⇒ E' – семантический стойкий. ⊲

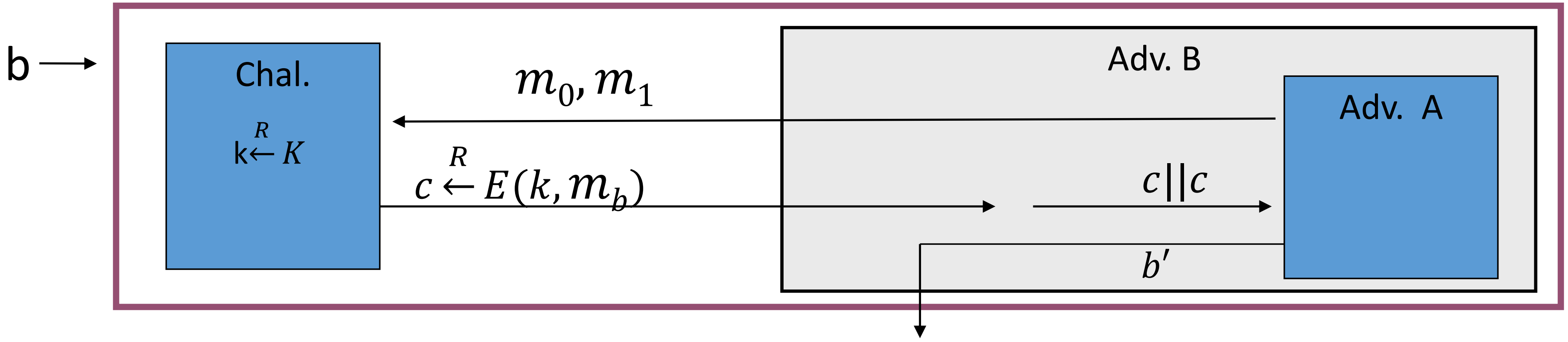
Доказательства сведением (Reduction proof)

Пусть $\mathrm{E} = (E, D)$ - вычислимый семантически стойкий шифр на (K, M, C).

Тогда $\mathrm{E}' = (E', D')$: $\begin{cases} (c_0, c_1) = E'(k, m) = c||c; c = E(k, m) \\ D'(k, (c_0, c_1)) = D(k, c_0) \end{cases}$ –

семантически стойкий шифр.

$\mathrm{SSadv}[A, \mathrm{E}'] \geq e$, где e – не пренебрежимо малая величина.



$$\mathrm{SSadv}[B, \mathrm{E}] = \mathrm{SSadv}[A, \mathrm{E}'] \geq e$$

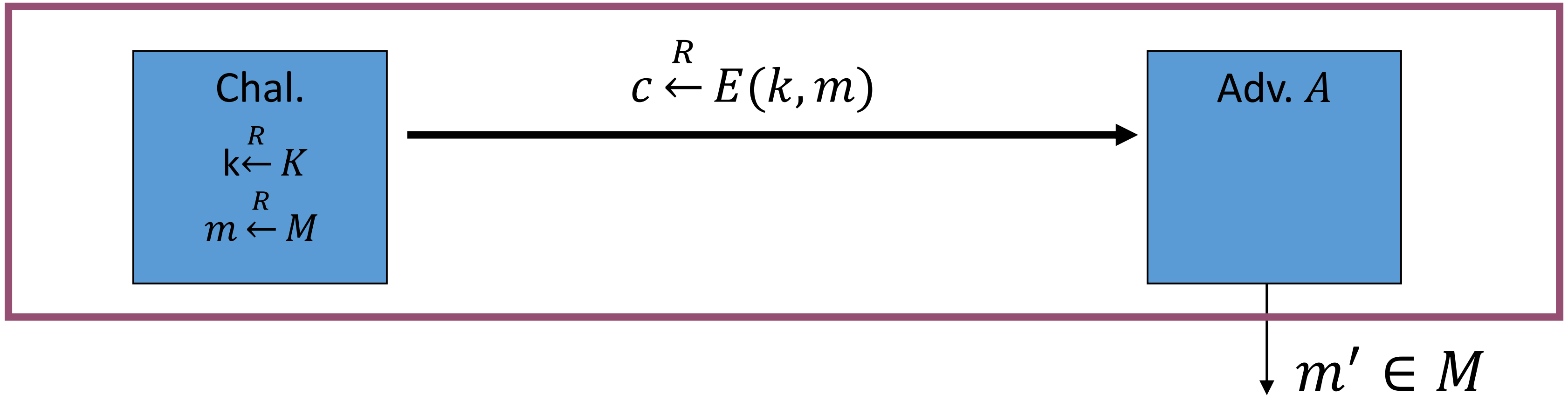
Восстановление сообщений

Атака на восстановление сообщений: имея зашифрованное сообщение $c \leftarrow E(k, m), m \in M$, восстановить сообщение m, с вероятностью больше $1/|M|$.

Опишем игру на восстановление сообщений.

- Претендент вычисляет $m \xleftarrow{R} M, k \xleftarrow{R} K, c \xleftarrow{R} E(k, m)$ и отправляет c противнику.
- Противник возвращает m' как результат игры.

Восстановление сообщений

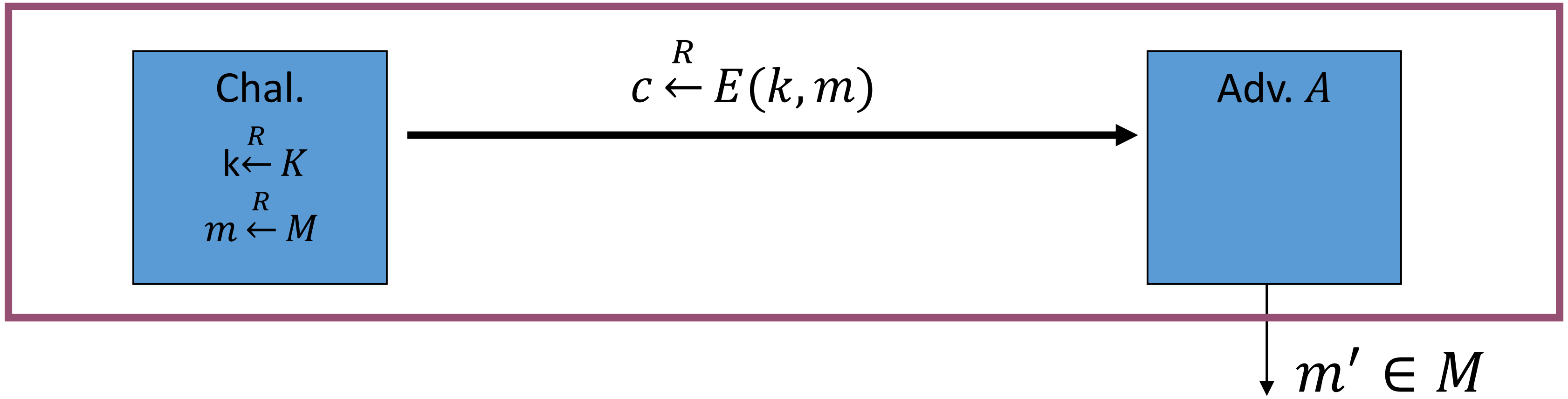


Пусть W – событие, при котором $m' = m$.

Преимуществом алгоритма A против шифра E при атаке на восстановление сообщений является величина

$$\mathrm{MRadv}[A, \mathrm{E}] = \left| \Pr[W] - \frac{1}{|M|} \right|$$

Восстановление сообщений



$$\mathrm{MRadv}[A, \mathrm{E}] = \left| \Pr[W] - \frac{1}{|M|} \right|$$

Шифр E называется **стойким к атаке на восстановление сообщений**, если $\forall A$ величина $\mathrm{MRadv}[A, \mathrm{E}] < \epsilon$, где ϵ - пренебрежимо малая величина.

Восстановление сообщений

Теорема 1.8. Если шифр $\mathrm{E} = (E, D)$ семантически стойкий на (K, M, C), то он стойкий к атаке на восстановление сообщений

⊳ Покажем, что атака на восстановление сообщений даёт атаку на семантическую стойкость.

Пусть A – эффективный алгоритм. Обозначим p – вероятность выиграть игру на восстановление сообщений для алгоритма A:

$$\mathrm{MRadv}[A, \mathrm{E}] = \left| p - \frac{1}{|M|} \right|.$$

Построим эффективный алгоритм B для игры на семантическую стойкость против алгоритма E, для которого

$$\mathrm{MRadv}[A, \mathrm{E}] \leq \mathrm{SSadv}[B, \mathrm{E}].$$

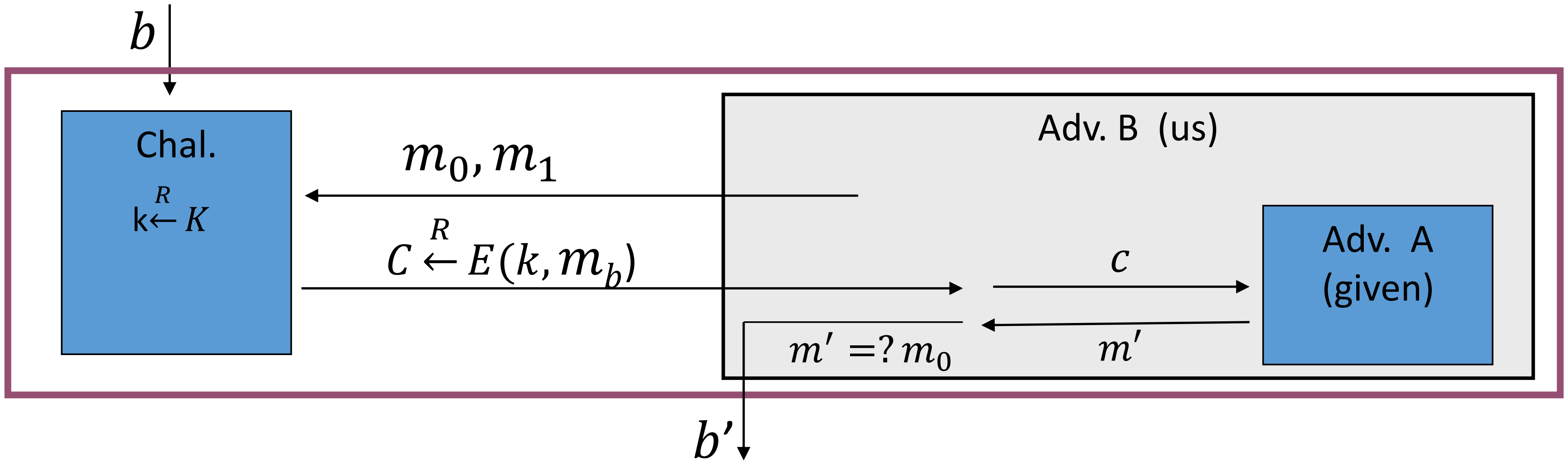
Восстановление сообщений

Теорема 1.8. Если шифр $\mathrm{E} = (E, D)$ семантически стойкий на (K, M, C), то он стойкий к атаке на восстановление сообщений

Построим алгоритм B. Алгоритм B генерирует два сообщения m_0 и m_1и оправляет их претенденту в игре на семантическую стойкость. Претендент отвечает шифртекстом c одного из сообщений, которых алгоритм B пересылает алгоритму A, получая восстановленное сообщение m'. Если $m' = m_0$ то выводит $b' = 0$, иначе $b' = 1$.

Восстановление сообщений

Теорема 1.8. Если шифр $\mathrm{E} = (E, D)$ семантически стойкий на (K, M, C), то он стойкий к атаке на восстановление сообщений



Восстановление сообщений

Теорема 1.8. Если шифр $\mathrm{E} = (E, D)$ семантически стойкий на (K, M, C), то он стойкий к атаке на восстановление сообщений

Для $b = 0{,}1$ пусть p_b - вероятность того, что алгоритм B выдаст значение $b' = 1$, при шифровании сообщения m_b. Тогда $\mathrm{SSadv}[B, \mathrm{E}] = |p_0 - p_1|$. С другой стороны, если c есть зашифрование m_0 то вероятность $p_0 = p$ (Вероятность выиграть игру на восстановление для A). Если же c есть зашифрование m_1, то $p_1 = \Pr[m_1 = m'] = 1/|M|$. Следовательно

$$SSadv[B, \mathrm{E}] = |p_1 - p_0| = \left|\frac{1}{|M|} - p\right| = MRadv[A, \mathrm{E}]$$

⇒ атака на восстановление сообщений даёт атаку на семантическую стойкость. ⊲

Восстановление битов сообщения

Пусть $\mathrm{E} = (E, D)$ шифр на (K, M, C). $M = \{0,1\}^L$. Пусть $par(m)$ – произвольный предикат, вычисляющий 1 бит информации об открытом тексте по шифртексту (Например функция вычисления чётности сообщения $m \in M$).

Определим игру на восстановление битов.

- Претендент вычисляет $m \xleftarrow{R} M, k \xleftarrow{R} K, c \xleftarrow{R} E(k, m)$ и отправляет c противнику.
- Противник возвращает $b' \in \{0,1\}$ как результат игры.

Пусть W – событие, при котором $b' = par(m)$.

Преимуществом алгоритма A против шифра E при атаке на восстановление битов является величина

$$\mathrm{PARadv}[A, \mathrm{E}] = |\Pr[W] - 1/2|$$

Восстановление битов сообщения

Пусть $\mathrm{E} = (E, D)$ шифр на (K, M, C). $M = \{0,1\}^L$. Пусть $par(m)$ – функция вычисления чётности сообщения $m \in M$.

Шифр E называется **стойким к восстановлению битов**, если величина $\mathrm{PARadv}[A, \mathrm{E}] < \epsilon$, где ϵ – пренебрежимо малая величина.

Вычисление индивидуальных битов сообщений

Теорема 1.9. Если шифр $\mathrm{E} = (E, D)$ семантически стойкий на (K, M, C), то он стойкий к атаке на восстановление битов сообщения (Атака на восстановление битов сообщения даёт атаку на семантическую стойкость)

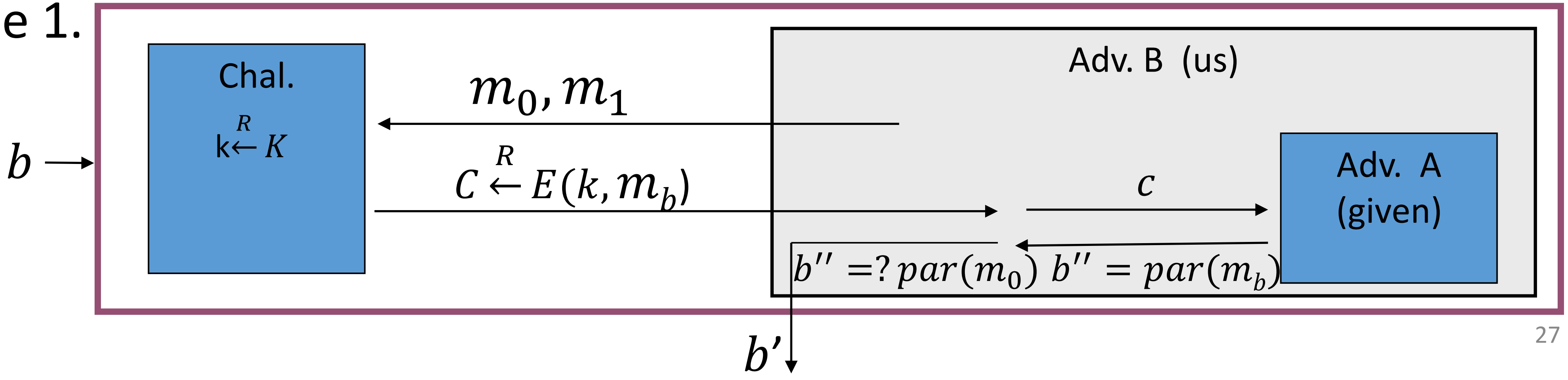
⊳ Построим эффективный алгоритм B для игры на семантическую стойкость простив алгоритма E, для которого

$$\mathrm{PARadv}[A, \mathrm{E}] = \frac{1}{2}\mathrm{SSadv}[B, \mathrm{E}].$$

Вычисление индивидуальных битов сообщений

Теорема 1.9. Если шифр $\mathrm{E} = (E, D)$ семантически стойкий на (K, M, C), то он стойкий к атаке на восстановление битов сообщения (Атака на восстановление битов сообщения даёт атаку на семантическую стойкость)

Противник B генерирует сообщения $m_0, m_1 \leftarrow m_0 \oplus (0^{L-1}1)$ и отправляет претенденту, получая шифртекст c, который он передаёт алгоритму A. После получения значения b'' если $b'' = par(m_0)$ то $b' = 0$, иначе 1.



Вычисление индивидуальных битов сообщений

Теорема 1.9. Если шифр $\mathrm{E} = (E, D)$ семантически стойкий на (K, M, C), то он стойкий к атаке на восстановление битов сообщения (Атака на восстановление битов сообщения даёт атаку на семантическую стойкость)

Пусть A: $\mathrm{PARadv}[A, \mathrm{E}] = \epsilon$, т.е. вероятность угадать чётность есть $\frac{1}{2} + \epsilon$.

Для $b = 0{,}1$ пусть p_b - вероятность того, что алгоритм B выдаст значение $b' = 1$. Тогда $SSadv[B, \mathrm{E}] = |p_1 - p_0| = 2\epsilon = \mathrm{PARadv}[A, \mathrm{E}]$.

$$p_0 = \frac{1}{2} + \epsilon \text{ (верная чётность } m_0\text{)},$$

$$p_1 = 1 - p_0 = \frac{1}{2} - \epsilon \text{(неверная чётность } m_1\text{)}.$$

$\Rightarrow$ атака на восстановление даёт атаку на семантическую стойкость. $\lhd$

Семантическая стойкость (альтернативная формулировка)

Теорема 1.10. (обобщение 1.9) Пусть задана игра на семантическую стойкость для алгоритма A против шифра $\mathrm{E} = (E, D)$ на (K, M, C)**.** Определим $\mathrm{SSadv}^*[A, \mathrm{E}] = \left|\Pr[W] - \frac{1}{2}\right|$, где $\mathrm{W} -$ событие, при котором $\mathrm{b}' = \mathrm{b}$. Тогда $\mathrm{SSadv}\,[A, \mathrm{E}] = 2 * \mathrm{SSadv}^*[A, \mathrm{E}]$

⊳доказательство аналогично **Теореме 1.9.** ⊲

Выводы

- Модель абсолютно стойкого шифра делает его сложно применимым в практическом смысле
  - Требуется размер ключа равный размеру сообщения
  - Невозможно добиться стойкости при переменной длине сообщений
- Семантически стойкий шифр – ослабленная модель абсолютно стойкого шифра, пригодная для практического применения
  - Стойкость к восстановлению сообщений
  - Стойкость к восстановлению битов сообщений
- Игровая модель – модель, позволяющая вводить определения стойкости для криптографический примитивов
  - Доказательства стойкости методом сведения (reduction)
  - Построение атак через моделирование игры