Прикладная Криптография: Симметричные криптосистемы Блочные шифры

Макаров Артём

МИФИ 2018

Блочный шифр

Блочный шифр – детерминированный шифр $\mathrm{E} = (E, D)$ определённый на (E, D): $E: K \times X \to X$.

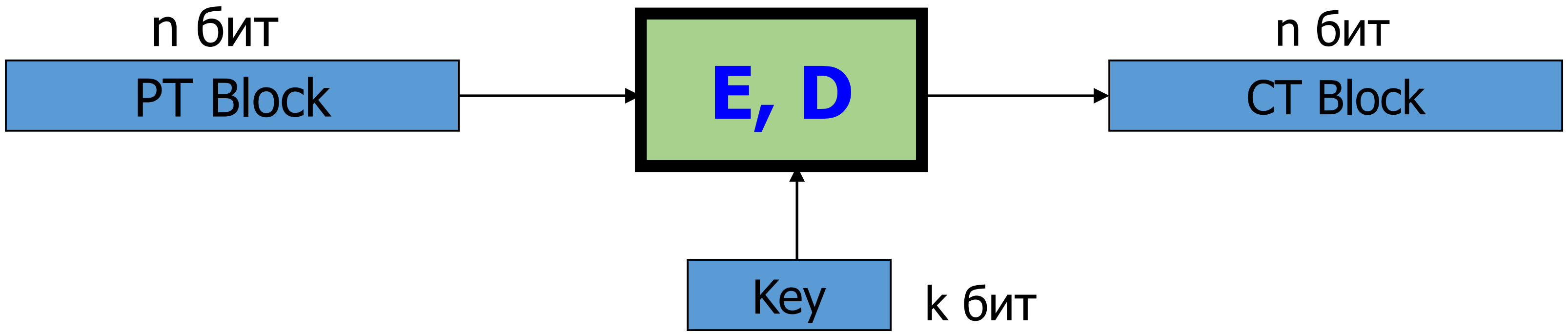
$x \in X$ – блок данных, X – множество блоков, K – множество ключей блочного шифра.

Для ключа $k \in K$ определим функцию $f_k: X \to X: f_k = E(k,*)$. $f_k^{-1}: X \to X: f_k^{-1} = D(k,*)$.

Из свойства корректности имеем f_k, f_k^{-1} - подстановки на множестве X, $f_k f_k^{-1} = e$, где e – тождественная подстановка на X.

Блочный шифр

- Блочные шифры является основным криптографическим примитивом для построения симметричных криптосистем.
- Могут быть использованы для как схем шифрования (в схемах шифрования), так и для обеспечения аутентичности (в кодах аутентичности сообщений.



Понятие стойкости блочного шифры

Для блочных шифров требуют более строгое требование, чем семантическая стойкость: для случайно выбранного ключа $k \in_R K$ перестановка $E_k(*) = f_k$ должна быть псевдослучайной, т.е. выглядеть вычислительно неотличимой от случайной подстановки из $S(X)$.

Идея игры – противник эффективный противник имеет доступ к оракулу, который выбирает функцию f либо случайно, либо использует псевдослучайную функцию на случайном ключе. Противник может получить произвольное число образов функции f на указанных им входах. Задача – различить эксперименты описанной игры.

PRP и PRF

Пусть функция $F: K \times X \to Y$ определена на (K, X, Y).

Тогда F – **псевдослучайная функция (PRF)**, если существует эффективный алгоритм, вычисляющий $F(k, m), k \in K, x \in X$.

Пусть функция $E: K \times X \to X$ определена на (K, X).

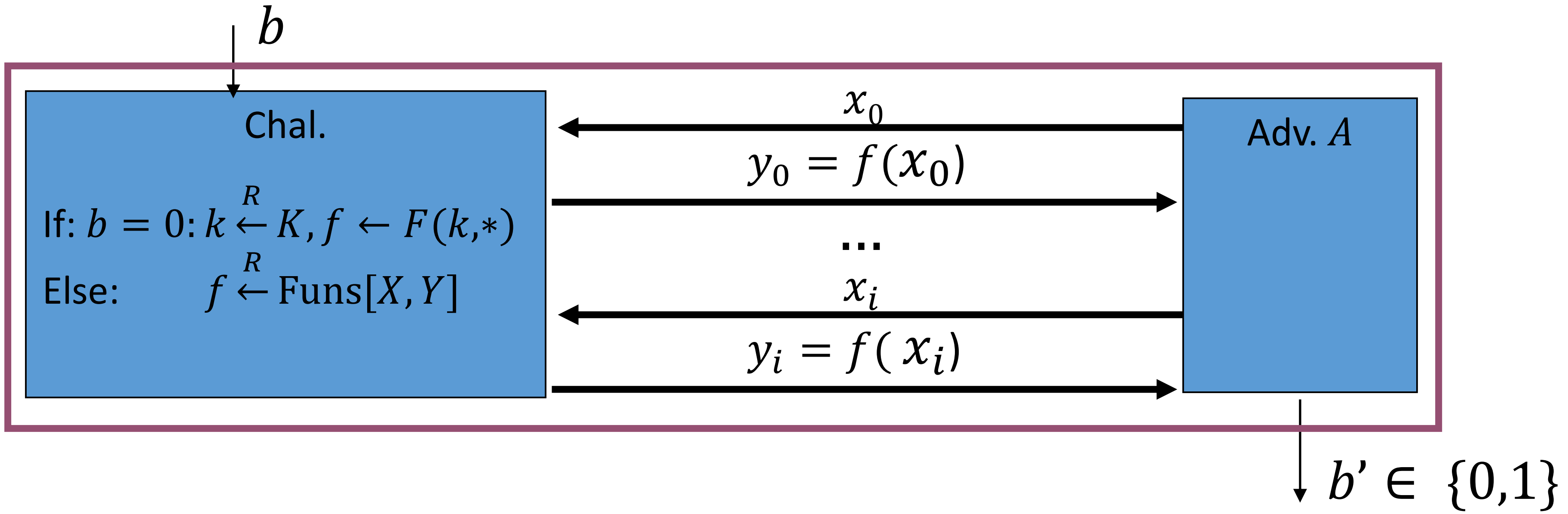
Тогда E – **псевдослучайная подстановка (PRP)**, если

- Существует эффективный алгоритм вычисляющий $E(k, x). k \in K, x \in X$
- Функция $f_k = E(k,*)$ – подстановка.

Игра на стойкость PRF

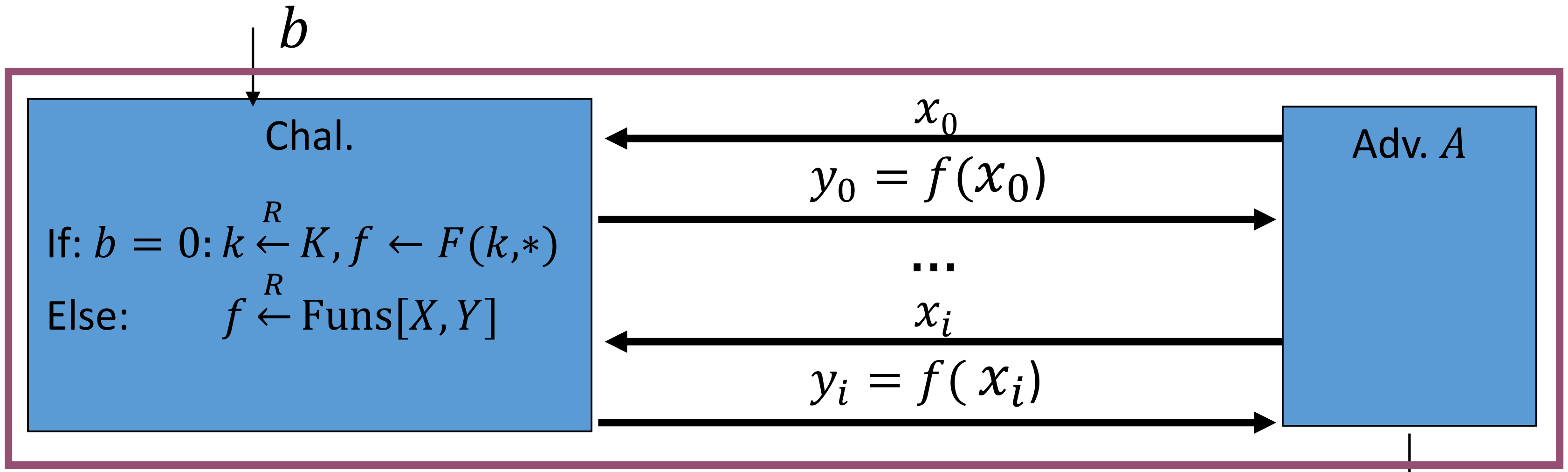
Для $b \in \{0,1\}$ пусть W_b событие того, что b'=1 в эксперименте b.

Тогда преимуществом алгоритма A против блочного шифра $\mathrm{E} = (E, D)$ на (K, X) называется величина $PRF_{adv}[A, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]|$.



Стойкая PRF

PRF F, определённая на (K, X), называется стойкой PRF, если $\forall A$: A – эффективный алгоритм в игре на стойкость PRF величина $PRF_{adv}[A, F] \leq \epsilon$, где ϵ – пренебрежимо малая величина.

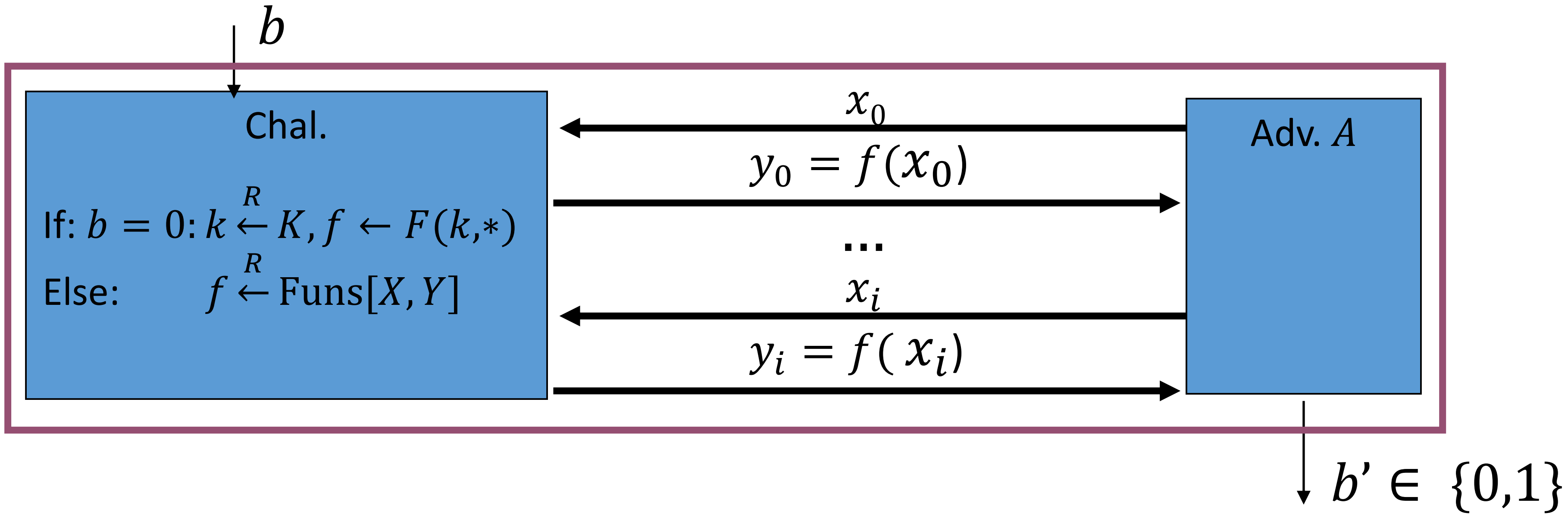


$PRF_{adv}[A, F] = |\Pr[W_0] - \Pr[W_1]|$

Игра на стойкость PRF

Альтернативное определение: рассмотри игру на угадывание бита (см лекцию 1) для противника A против PRF F. Определим $PRF^{*}_{adv}[A,F] = |\Pr[b' = b] - 1/2|$. Тогда F – стойкая PRF, если $\forall A$: A – эффективный алгоритм в игре на угадывание бита в игре на стойкость PRF величина $PRF^{*}_{adv}[A,F] \le \epsilon$, где ϵ – пренебрежимо малая величина.

$PRF_{adv}[A,F] = 2 * PRF^{*}_{adv}[A,F]$. (см лекцию 1)



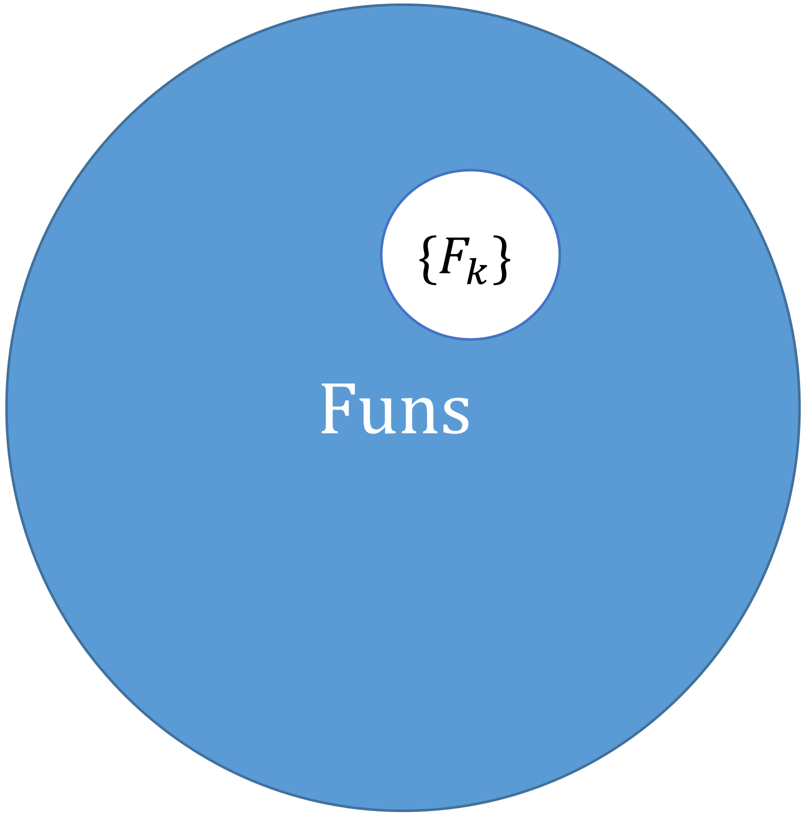
Вычислительная неразличимость

Пусть F – PRF на (K, X, Y)

Рассмотрим множество возможных значений $\{F_k\} \subset \mathrm{Funs}[\mathrm{X}, \mathrm{Y}] = \{f : X \to Y\}$.

Тогда если F – стойкая PRF, то эффективный Противник не может имея доступ к оракулу отличить $\{F_k\}$ от Funs.

$|\{F_k\}| = |K|, |\mathrm{Funs}| = |Y|^{|X|}$



Пример

Пусть $F: K \times X \to \{0,1\}^{128}$ стойкая PRF.

Является $G: K \times X \to \{0,1\}^{128}$ли стойкой PRF?

$$G(k,x) = \begin{cases} 0^{128}, x = 0 \\ F(k,x), x \neq 0 \end{cases}$$

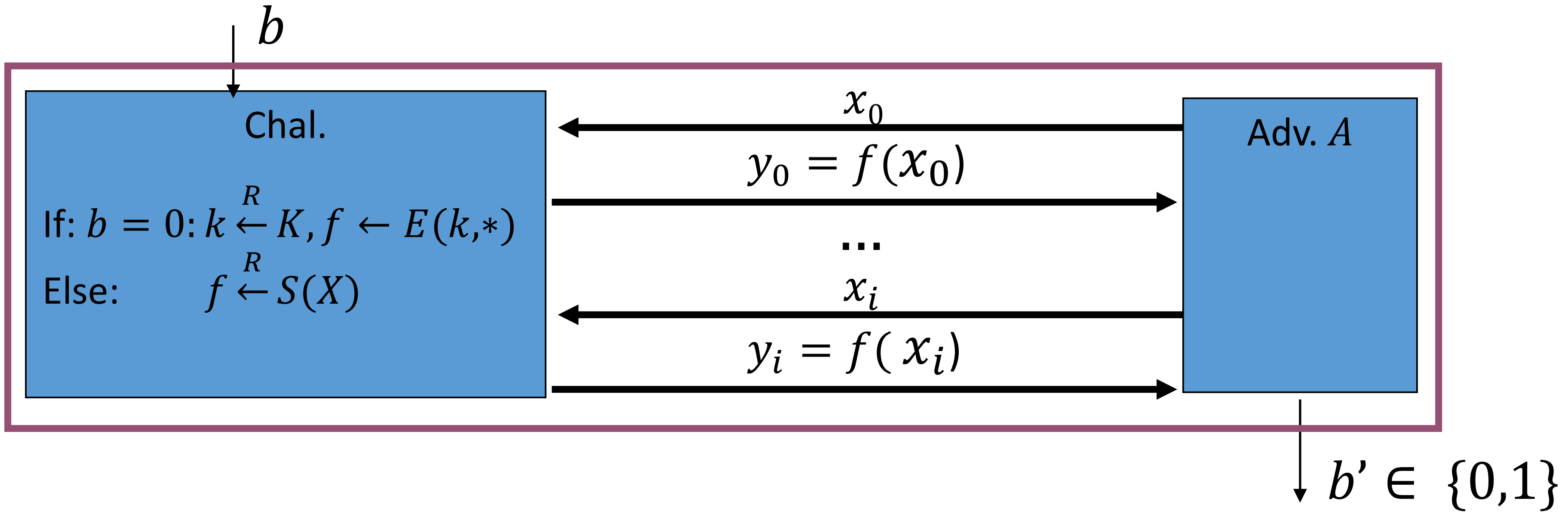
Нет, не является. A: передаёт сообщение $x = 0$, возвращает 0, если ответ претендента 0^{128}, иначе 1. $PRF_{adv}[A,G] = |1 - 2^{128}| > 1/2$

Игра на стойкость PRP

Строится аналогично игре на PRF, но для подстановок.

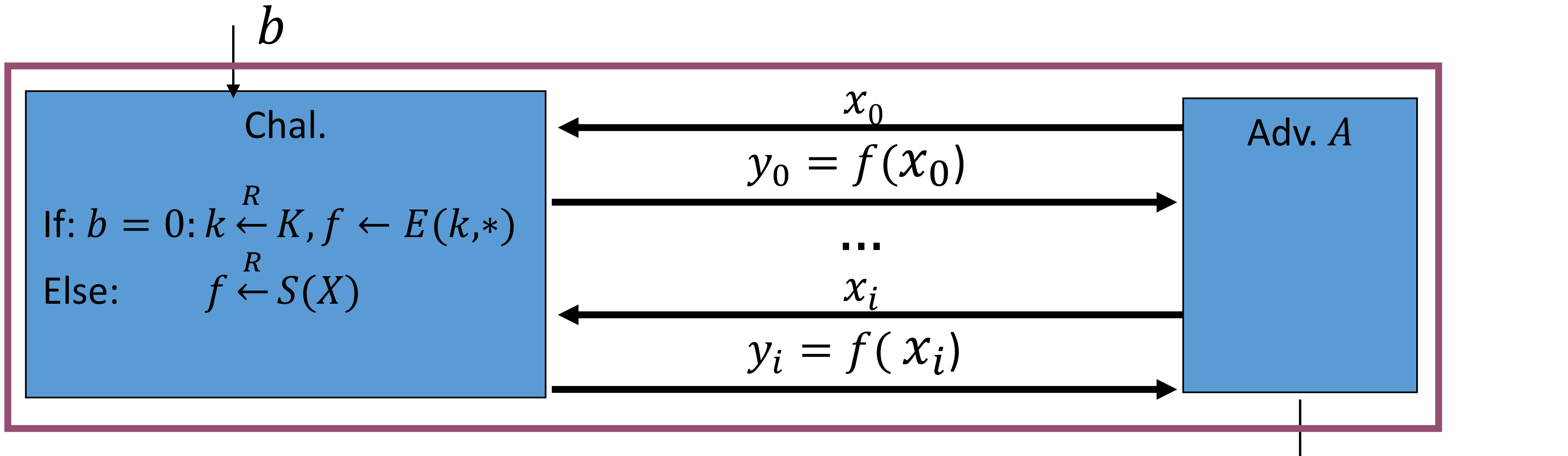
Для $b \in \{0,1\}$ пусть W_b событие того, что b'=1 в эксперименте b.

Тогда преимуществом алгоритма A против блочного шифра $\mathrm{E} = (E, D)$ на (K, X) называется величина $PRP_{adv}[A, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]|$.



Стойкая PRP

PRP E, определённая на (K, X), называется стойкой PRP, если $\forall A$: A – эффективный алгоритм в игре на стойкость PRP величина $PRP_{adv}[A, \mathrm{E}] \leq \epsilon$, где ϵ – пренебрежимо малая величина.

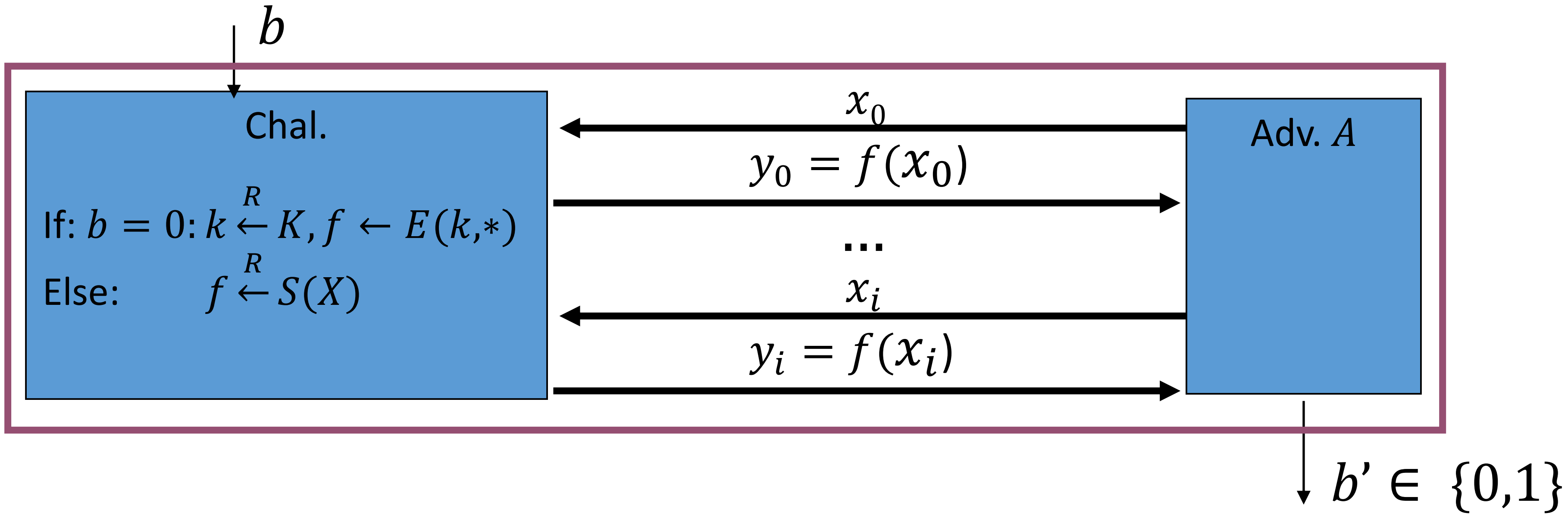


$$PRP_{adv}[A, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]|$$

Игра на стойкость PRP

Альтернативное определение: рассмотри игру на угадывание бита (см лекцию 1) для противника A против PRP E. Определим $PRP^*_{adv}[A, E] = |\Pr[b' = b] - 1/2|$. Тогда E – стойкая PRP, если $\forall A$: A – эффективный алгоритм в игре на угадывание бита в игре на стойкость PRP величина $PRP^*_{adv}[A, E] \le \epsilon$, где ϵ – пренебрежимо малая величина.

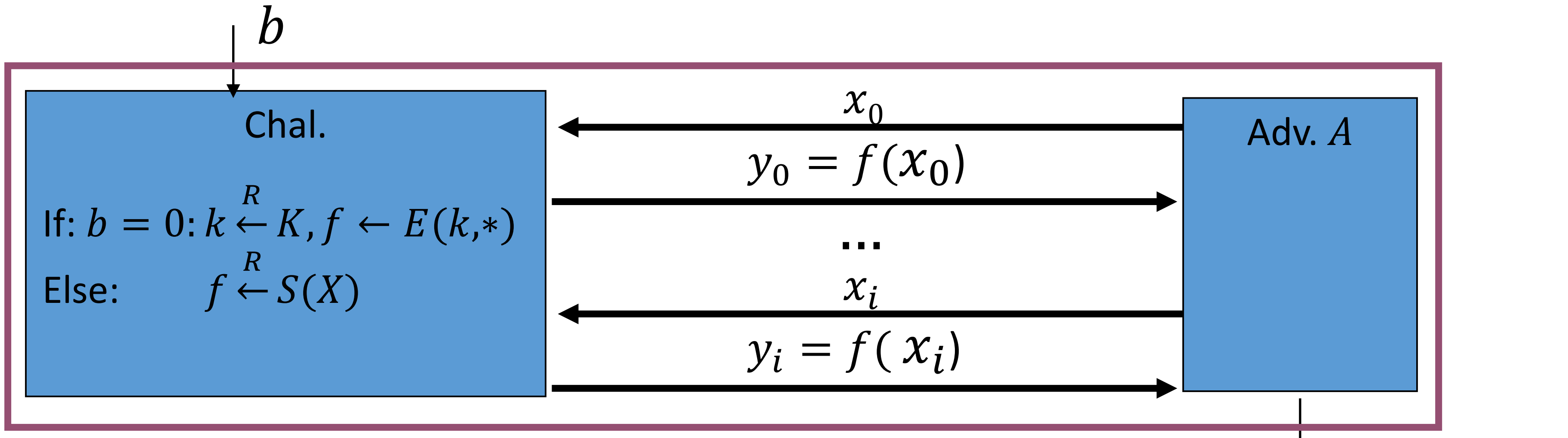
$PRP_{adv}[A, F] = 2 * PRP^*_{adv}[A, E]$. (см лекцию 1)



Стойкий блочный шифр

Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Тогда E – стойкий блочный шифр, если E – стойкая псевдослучайная перестановка.

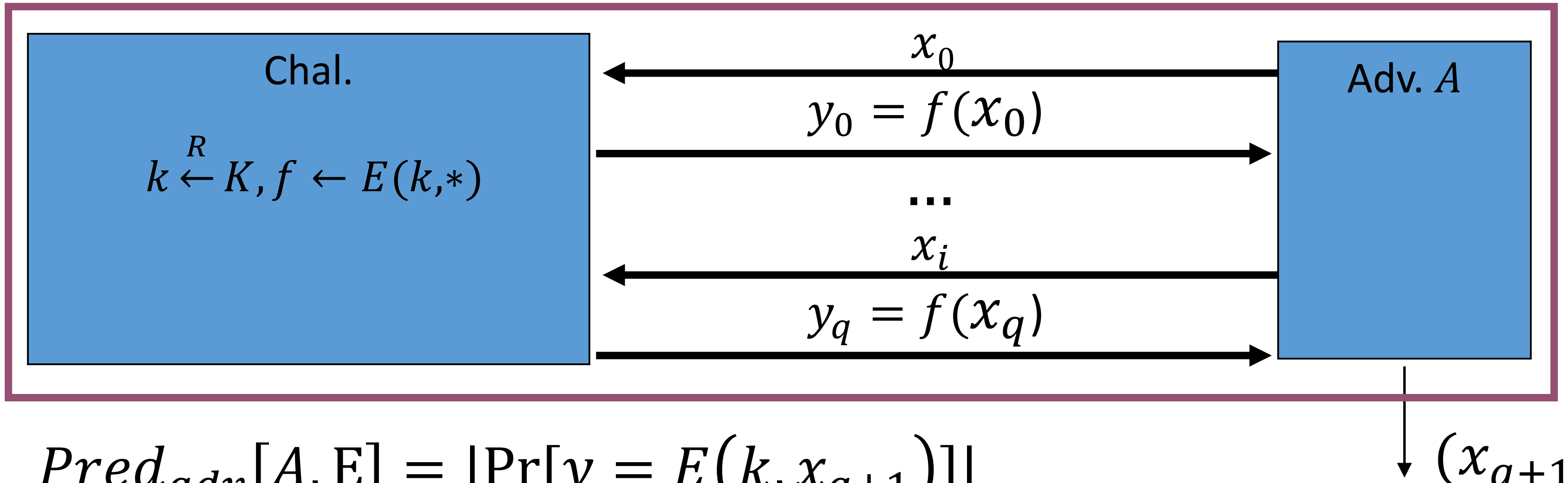
Т.е. $\forall A$: A – эффективный противник в игре на стойкость PRP величина $BC_{adv}[A, \mathrm{E}] = PRP_{adv}[A, E] \leq \epsilon$, где ϵ – пренебрежимо малая величина.



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

Непредсказуемость блочных шифров

Рассмотрим игру. Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Пусть претендент выбирает случайный ключ $k \in_R K$. Противник выбирает произвольные $x_0,\ldots x_q$ и получает шифтексты $y_i = E(k, x_i)$. Задача противника получить (x_{q+1}, y): $x_{q+1} \notin \{x_0, \ldots, x_q\}, y = E(k, x_{q+1})$.

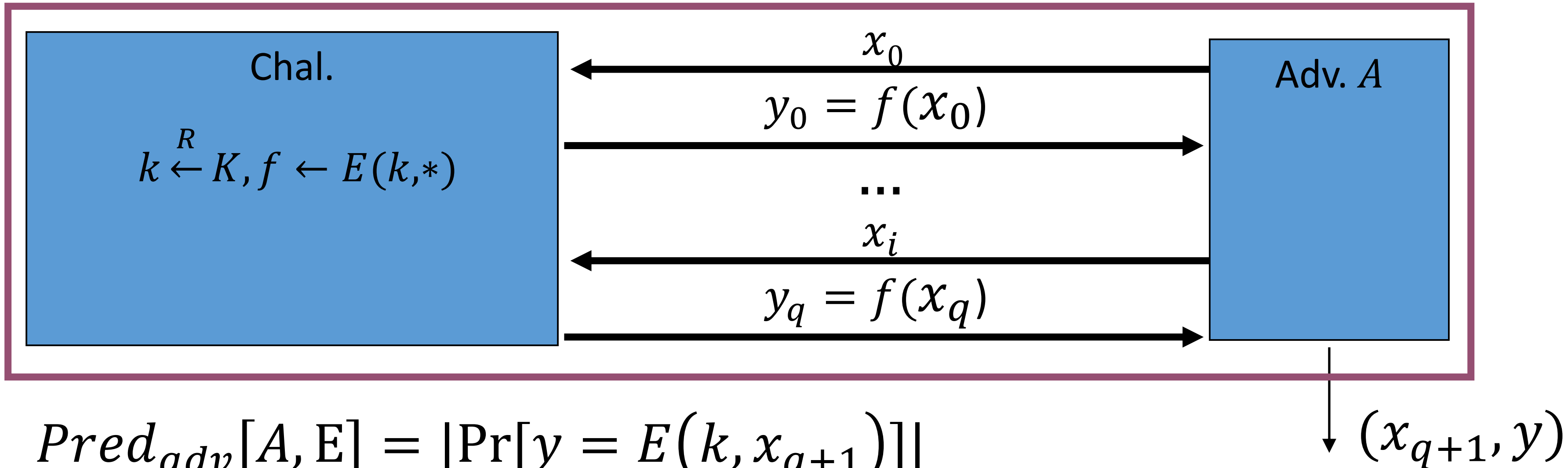


(x_{q+1}, y)

$Pred_{adv}[A, \mathrm{E}] = |\Pr[y = E(k, x_{q+1})]|$

Непредсказуемость блочных шифров

Блочный шифр называется стойким непредсказуемым блочным шифром, если для всех эффективных противников A величина $Pred_{adv}[A, \mathrm{E}] = |\Pr[y = E(k, x_{q+1})]| \leq \epsilon$, ϵ – пренебрежимо малая величина.

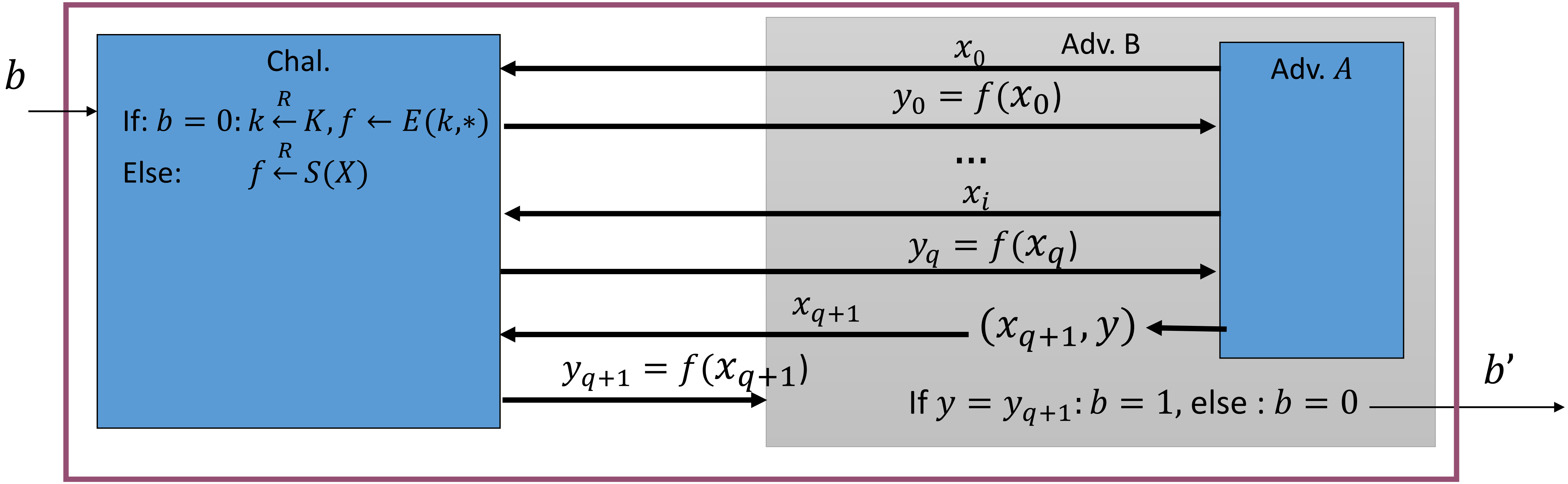


$$Pred_{adv}[A, \mathrm{E}] = |\Pr[y = E(k, x_{q+1})]|$$

Непредсказуемость блочных шифров

Теорема 4.1. Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Тогда если E – стойкий, то E – непредсказуемый.

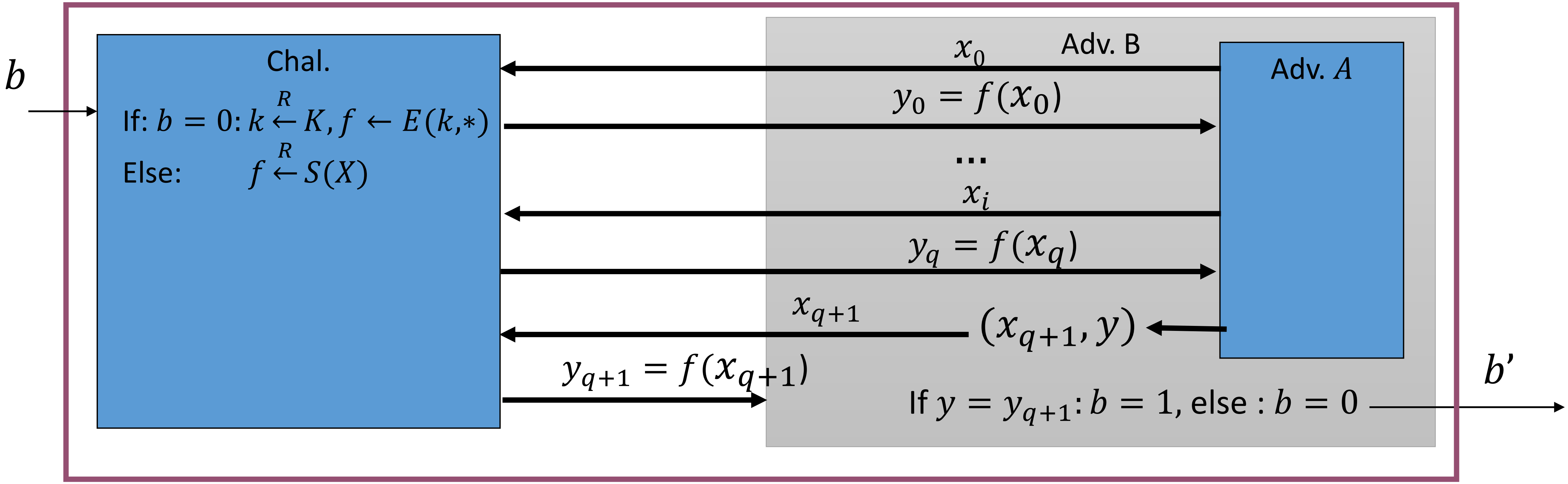
⊳Пусть E – предсказуемый. Тогда $\exists A$: $Pred[A, \mathrm{E}] = p, p$ – не пренебрежимо малая. Построим противника B следующим образом.



Непредсказуемость блочных шифров

Если $b = 0$: $W_0 = \Pr[b' = 1] = Pred_{adv}[A, \mathrm{E}] = p$.

Если $b = 1$: $W_1 = \Pr[b' = 1] =$
Prугадать результат случайной функции $= 1/|X|$ - пренебрежимо малая, для суперполиномиального значения $|X|$.



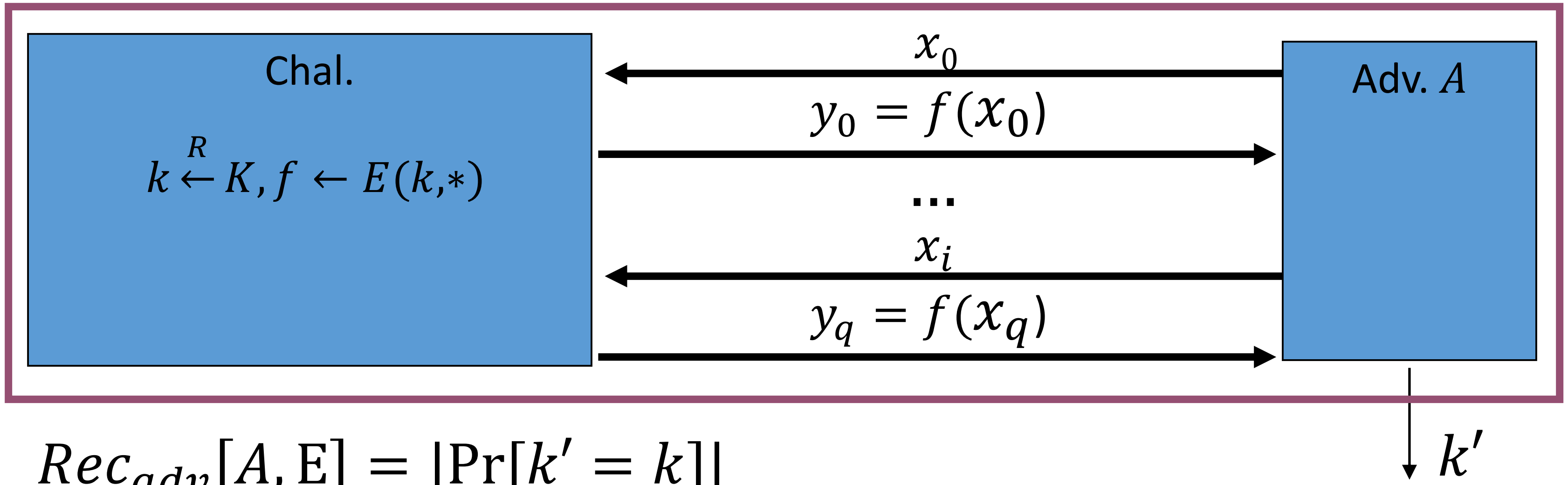
Непредсказуемость блочных шифров

Теорема 4.1. Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Тогда если E – стойкий, то E – непредсказуемый.

Тогда $PRP_{adv}[B, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]| = |p - \epsilon|$ - не пренебрежимо малая величина $\Rightarrow$ построили атаку на блочный шифр $\Rightarrow$ противоречие $\Rightarrow$ E – не предсказуемый $\Rightarrow$ теорема доказана. ⊲

Стойкость против восстановления ключа

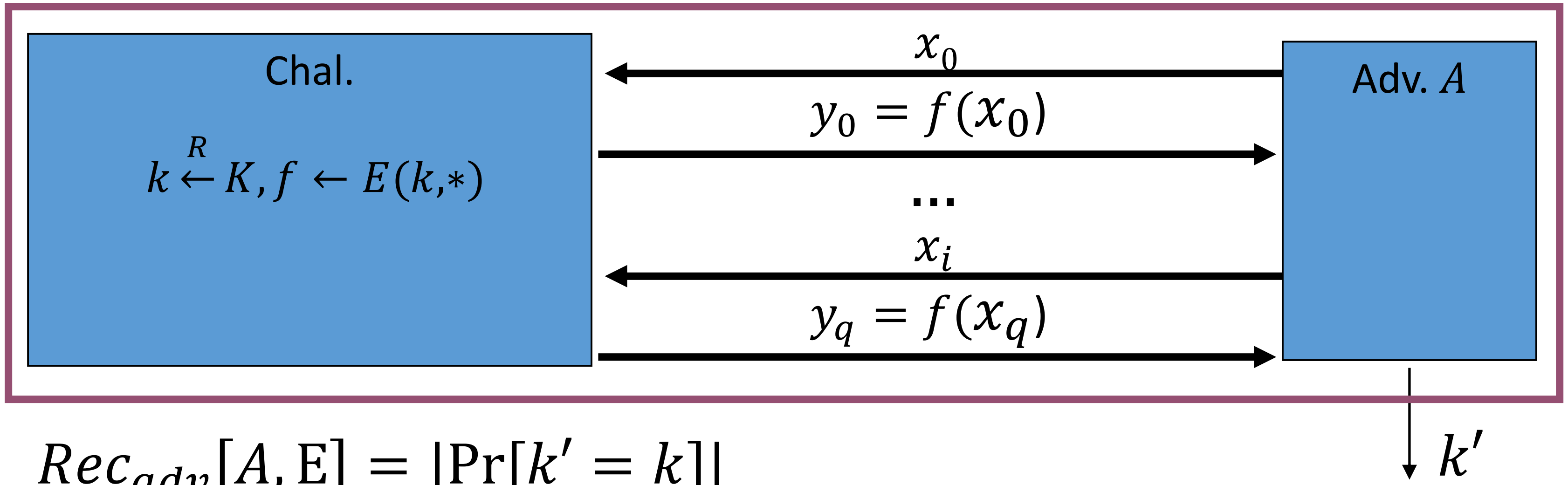
Рассмотрим игру. Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Пусть претендент выбирает случайный ключ $k \in_R K$. Противник выбирает произвольные $x_0, \ldots x_q$ и получает шифтексты $y_i = E(k, x_i)$. Задача противника получить $k' \in K \colon k = k$.



$$Rec_{adv}[A, \mathrm{E}] = |\Pr[k' = k]|$$

Стойкость против восстановления ключа

Блочный шифр называется стойким к восстановлению ключа блочным шифром, если для всех эффективных противников A величина $Rec_{adv}[A, \mathrm{E}] = |\Pr[k' = k]| \leq \epsilon$, ϵ – пренебрежимо малая величина.



$Rec_{adv}[A, \mathrm{E}] = |\Pr[k' = k]|$

Стойкость против восстановления ключа

Теорема 4.2. Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Тогда если E – непредсказуемый, то E – стойкий к восстановлению ключа.

⊳Доказательство аналогично теореме 4.1. Основная идея – если противник может восстановить ключ блочного шифра – то он может получить пару открытый текст – шифртекст, просто используя ключ. ⊲

Следствия стойкости

- Если E – стойкий блочный шифр, он должен быть стойким к восстановлению ключа.
- Если E – стойкий к восстановлению ключа, то $|K|$ - супер полиномиальная

⊵Противник всегда может выиграть игру на восстановлению ключа с преимуществом $Rec_{adv}[A, \mathrm{E}] = 1/|K|$, просто угадав ключ. Следовательно величина $1/|K|$ - должна быть пренебрежимо малой, $|K|$ - супер полиномиальной. ⊲

- Описанная выше атака на восстановление ключа называется exhaustive-search (полный перебор ключа, исчерпывающий поиск ключа, полная апробация). Если противник проверяет t ключей за время полиномиально ограниченное от t то вероятность совершить атаку составляет $p \approx t/|K|$.

Использование блочных шифров

Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X).

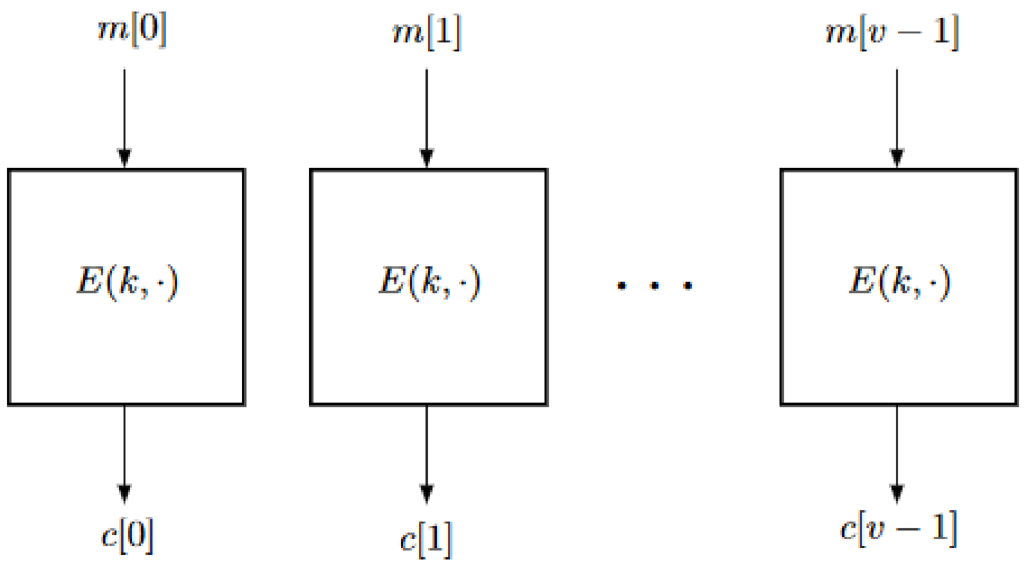
Можем ли мы использовать блочный шифр для построения семантически стойких шифров для сообщений произвольной длины?

ECB

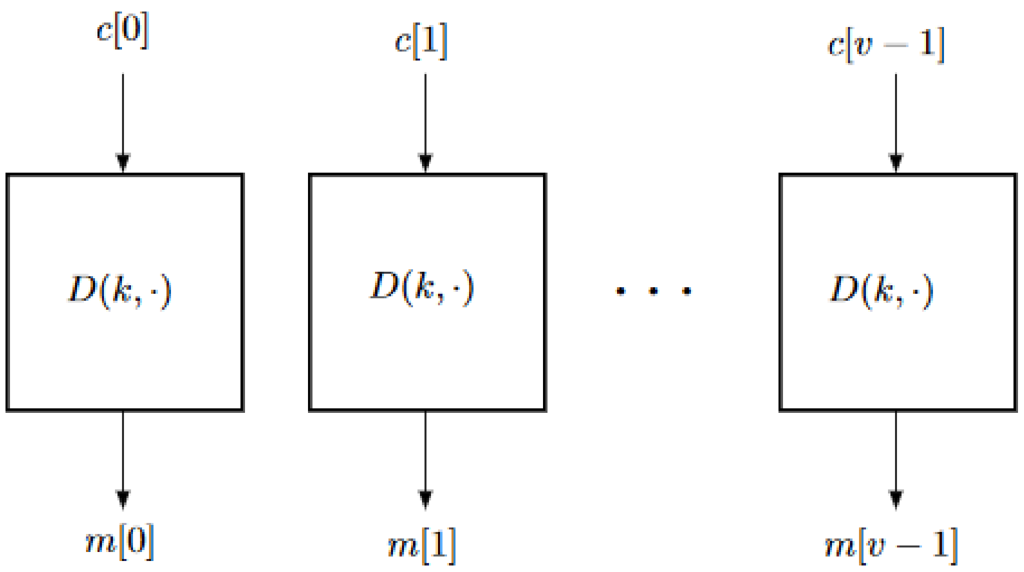
Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Для полиномиально ограниченной величины $l \geq 1$ определим шифр $\mathrm{E}' = (E', D')$ на $(K, X^{\leq l}, X^{\leq l})$ следующим образом:

- Для $k \in K, m \in X^{\leq l}, v = |m|$ определим
$$E'(k, m) = \big(E(k, m[0]), \dots, E(k, m[v-1])\big).$$
- Для $k \in K, c \in X^{\leq l}, v = |c|$ определим
$$D'(k, c) = \big(E(k, \mathrm{c}[0]), \dots, E(k, \mathrm{c}[v-1])\big).$$

ECB



Зашифрование



Расшифрование

Стойкость ECB

Теорема 4.3. Пусть $\mathrm{E} = (E, D)$ – блочный шифр на (K, X). Для полиномиально ограниченной величины $l \geq 1$ определим ECB шифр $\mathrm{E}' = (E', D')$ на $(K, X'^{\leq l}, X'^{\leq l})$, где $X'^{\leq l}$ - сообщения, длины не более чем из l попарно различных блоков. Тогда если E – стойкий блочный шифр, то E' - семантически стойкий. В частности $\forall A$ в игре на семантическую стойкость против E', $\exists B$ в игре на стойкость блочного шифра, такой что

$$SS_{adv}[A, \mathrm{E}'] = 2 * BC_{adv}[B, \mathrm{E}]$$

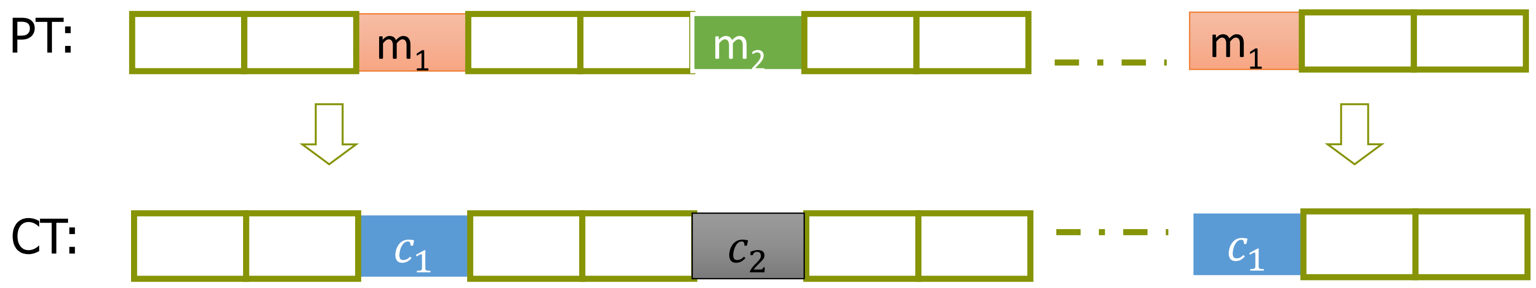
⊳Без доказательства, основная идея – для псевдослучайной подстановки противник не может отличить зашифрование уникальных блоков от случайных блоков, а значит не может отличить 2 различных зашифрования. ⊲

Стойкость ECB

- Стойкий блочный шифр в режиме ECB – семантически стойкий для
  - Сообщений, состоящих из уникальных, попарно различных блоков (например есть открытый текст – случайных ключ), не повторяющихся во время жизни ключа
  - Любых коротких, уникальных сообщений, длинной в один блок, не повторяющихся во время жизни ключа
- Что для произвольных сообщений произвольной длины?

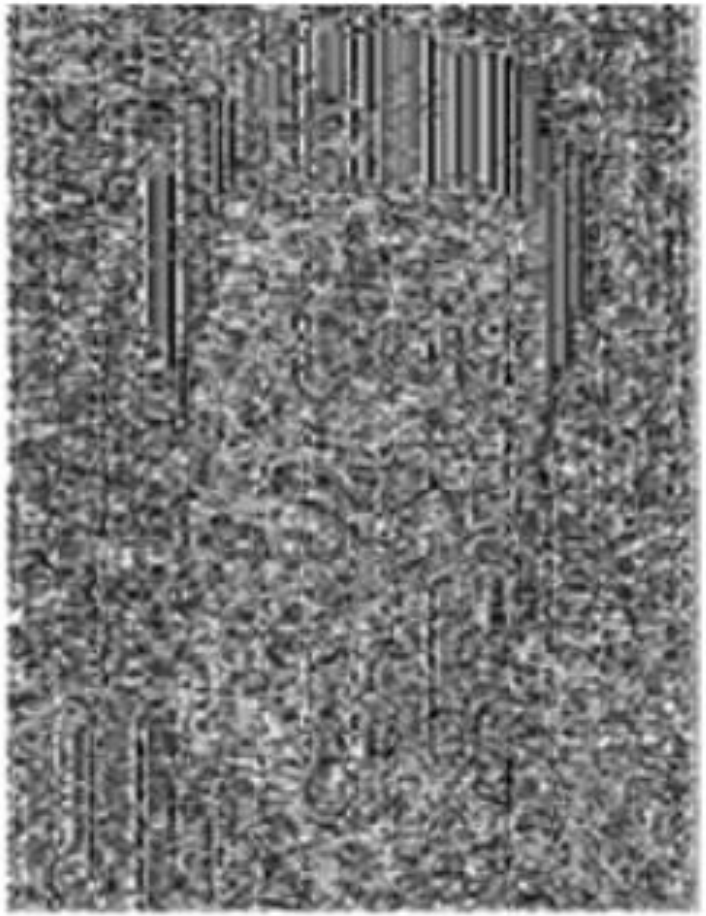
Стойкость ECB

Зашифрование в режиме ECB происходит детерминированно и поблочно, как следствие одинаковые блоки имеют одинаковый шифртекст.



Стойкость ECB

(a) plaintext



(b) plaintext encrypted in ECB mode using AES

Стойкость ECB

Теорема 4.4. Пусть $\mathrm{E} = (E, D) -$ на (K, X^l) блочных шифр в режиме ECB для произвольных сообщений из l блоков, $\mathrm{x} \in X^l$. E – не семантически стойкий.

⊳Построим противника A. A генерирует 2 сообщения $\mathrm{m}_1, \mathrm{m}_2 \colon \mathrm{m}_1 = (\mathrm{x}, \mathrm{x}), \mathrm{m}_2 = (\mathrm{x}, \mathrm{y}), \mathrm{x}, \mathrm{y} \in X$. От претендента он получает шифртекст $c = E(k, m_b)$. Тогда если $\mathrm{c} = (c_1, c_1)$ противник возвращает $b' = 0$, иначе 1.

Преимущество противника равно 1, т.к. одинаковые блоки открытого текста переходят в одинаковые блоки шифртекста ⊲

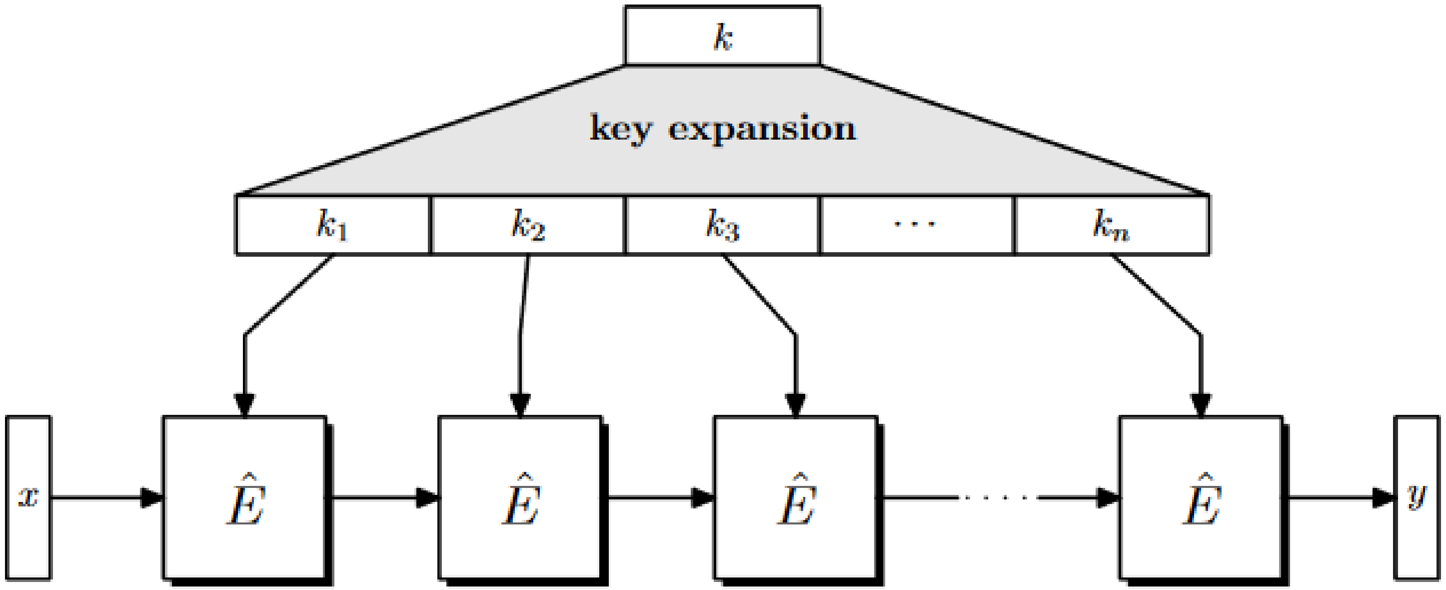
Построение блочных шифров

- Обычно блочные шифры строятся с использованием итеративных конструкций – несколько раз подряд используется некоторая функция (наз. итеративной или раундовой).
- В качестве итеративной функции выбирается простой (с точки зрения реализации) блочный шифр $\mathrm{E}' = (E', D')$, в общем случае может быть не стойкой.
- Выбирается простой (с точки зрения реализации) PRG G, используемый для расширения ключа k в d раундовых ключей $k_1, \dots, k_d$. G называется функцией выработки раундовых ключей или функцией расширения ключа.

Построение блочных шифров

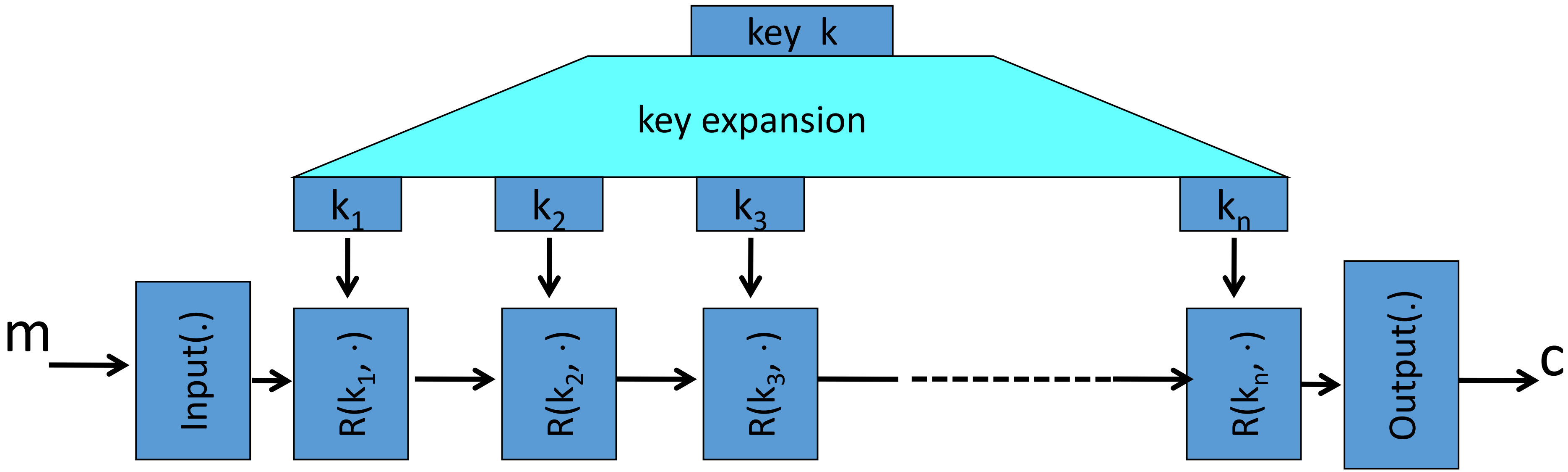
Алгоритм $E(k, x)$:

- Используя функцию G получить раундовые ключи: $(k_1, \ldots, k_d) \leftarrow G(k)$
- Для $i = 1..d$: $y \leftarrow E'(k_d, E'(k_{d-1}, \ldots, E'(k_2, E'(k_1, x)) \ldots))$



Построение блочных шифров

- Расшифрование происходит аналогично зашифрованию, но с использованием обратной раундовой функции $D'(k,x)$, и обратным порядком следования ключей.
- Иногда также могут использоваться входные и выходные преобразования : перед шифрованием используется некоторое входное преобразование над открытым текстов, после процедуры шифрования – некоторое выходное преобразование



Построение раундовых функций

- Как строить хорошие раундовые функции? Как определить стойкость раундовой функции? Никто не знает.
- Раундовая функция должна быть сильно нелинейной от ключа, т.к. использование линейной функции (или близкой к линейной) даёт линейный блочный шифр. Пример плохой раундовой функции - $E'(k, x) = kx \bmod q$.
- Качество раундовой функции определяется возможностью практических атак на полученный шифр.
- Сколько нужно использовать раундов для фиксированной раундовой функции? Никто не знает.

Использование блочных шифров

- Никогда не строить собственных блочных шифров
- Использовать AES, ГОСТ Р 34.12-2015 (Магма (ex ГОСТ 28147-89), Кузнечик)