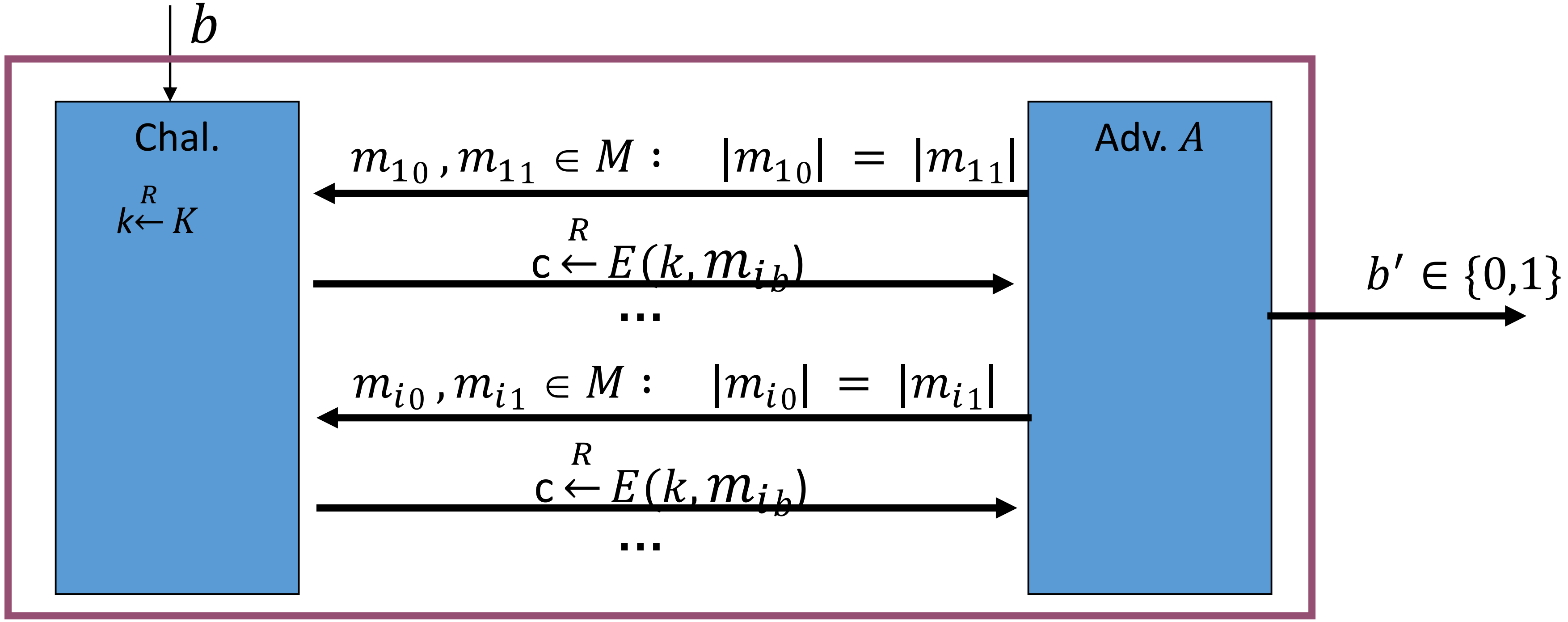
Прикладная Криптография: Симметричные криптосистемы СРА

Макаров Артём

МИФИ 2018

CPA

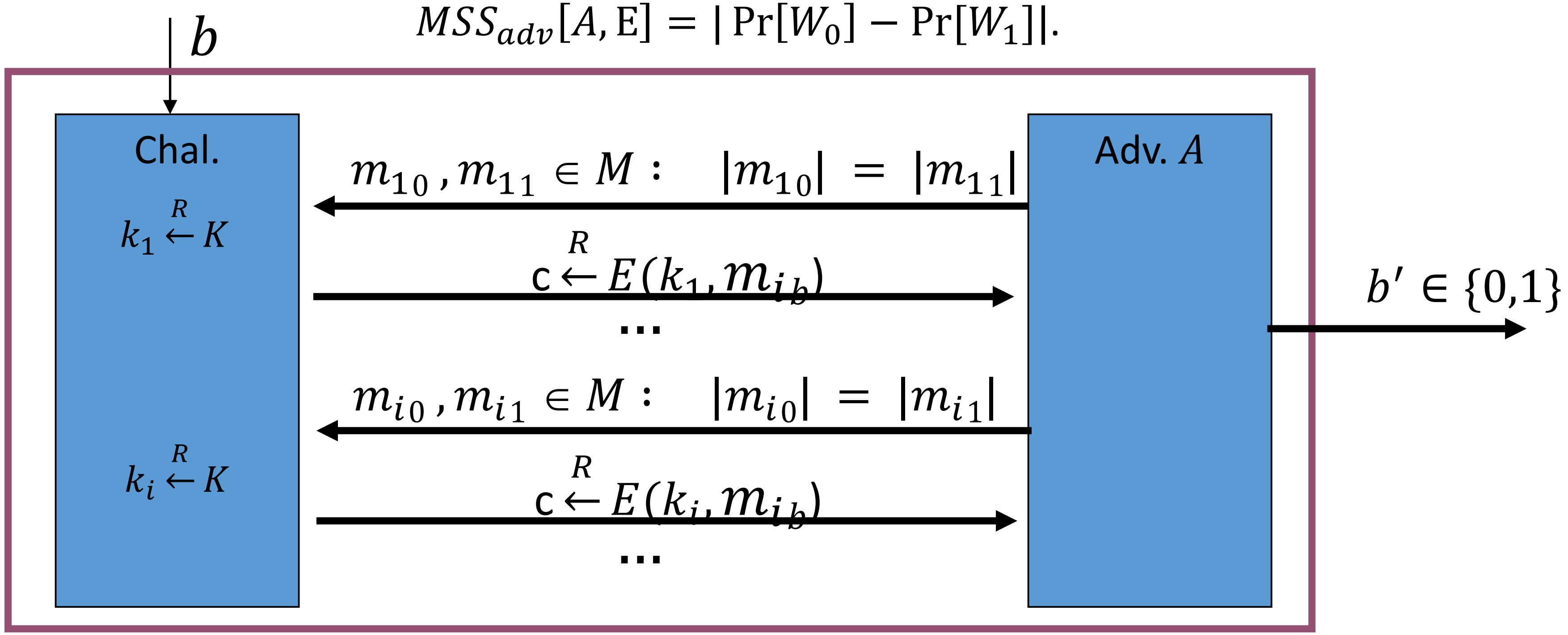
- Шифр называется CPA стойким, если для любого противника A величина $CPA_{adv}[A, \mathrm{E}] = |\Pr[W_0] - \Pr[W_1]| \leq \epsilon, \epsilon$ – пренебрежимо малая величина.
- Детерминированный шифр не может быть CPA стойким



Использование множества ключей

Шифр E называется семантически стойким при использовании множества ключей, если величина $MSS_{adv}[A, \mathrm{E}] \leq \epsilon$, где ϵ – пренебрежимо малая.

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



Построение CPA шифров из семантически стойких шифров

- Пусть $\mathrm{E} = (E, D)$ – семантически стойкий шифр на (K, M, C). Попробуем построить CPA стойкий шифр E' на $(K', M, X \times C)$ используя PRF F на (K', X, K).
- Ключом k' для E' будет ключ для PRF F. Для шифрования сообщения m выбирается случайный вход для PRF - x. Далее вычисляется ключ для E $k \leftarrow F(k', x)$. Затем m шифруется с использование ключа k: $c \leftarrow E(k, m)$. Шифр текстом является пара $\mathrm{c}' = (c, x)$.
- $E(k', m) = [x \leftarrow^{R} X, k \leftarrow F(k', x), c \leftarrow E(k, m), \mathrm{output}\ (x, c)]$
- $D(k', c') = [k \leftarrow F(k', x), m \leftarrow D(k, c), \mathrm{output}\, m]$
- Называется – **гибридная конструкция**.

Построение CPA шифров из семантически стойких шифров

Теорема 7.1. Если F – стойкая PRF, E – семантически стойкий шифр, $N = |X|$ - суперполиномиальная, то введённый ранее шифр E' - CPA стойкий шифр. В частности для любого противника в CPA игре, делающим не более Q запросов к претенденту существует противник B_F в игре на стойкость PRF и противник B_E в игре на семантическую стойкость, причём

$$CPA_{adv}[A, \mathrm{E}'] \leq \frac{Q^2}{N} + 2 * PRF_{adv}[B_F, F] + Q * SS_{adv}[B_E, \mathrm{E}]$$

Построение CPA шифров из семантически стойких шифров

$$\rhd \; CPA_{adv}[A, \mathrm{E}'] \le \frac{Q^2}{N} + 2 * PRF_{adv}[B_F, F] + Q * SS_{adv}[B_E, \mathrm{E}]$$

Перепишем формулу выше через альтернативные определения на угадывание бита

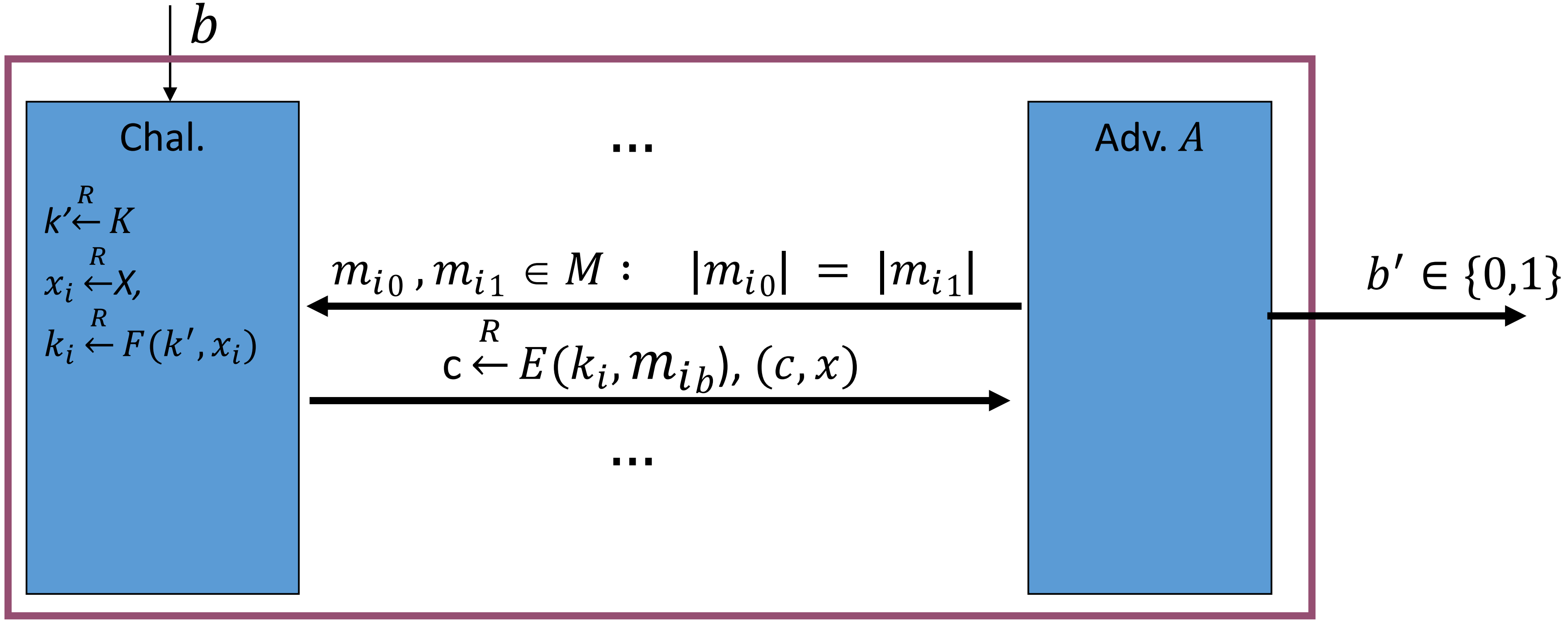
$$CPA_{adv}^{*}[A, \mathrm{E}'] \le \frac{Q^2}{2N} + PRF_{adv}[B_F, F] + Q * SS_{adv}^{*}[B_E, \mathrm{E}]$$

Основная идея доказательства – определим игру 0 между противником A и претендентом в игре против E'. Определим игры 1, 2, 3. В каждый из них противник A будет играть против разных претендентов. Покажем переходы между этими играми.

Определим W_j как событие того, что $b' = b$ в игре j.

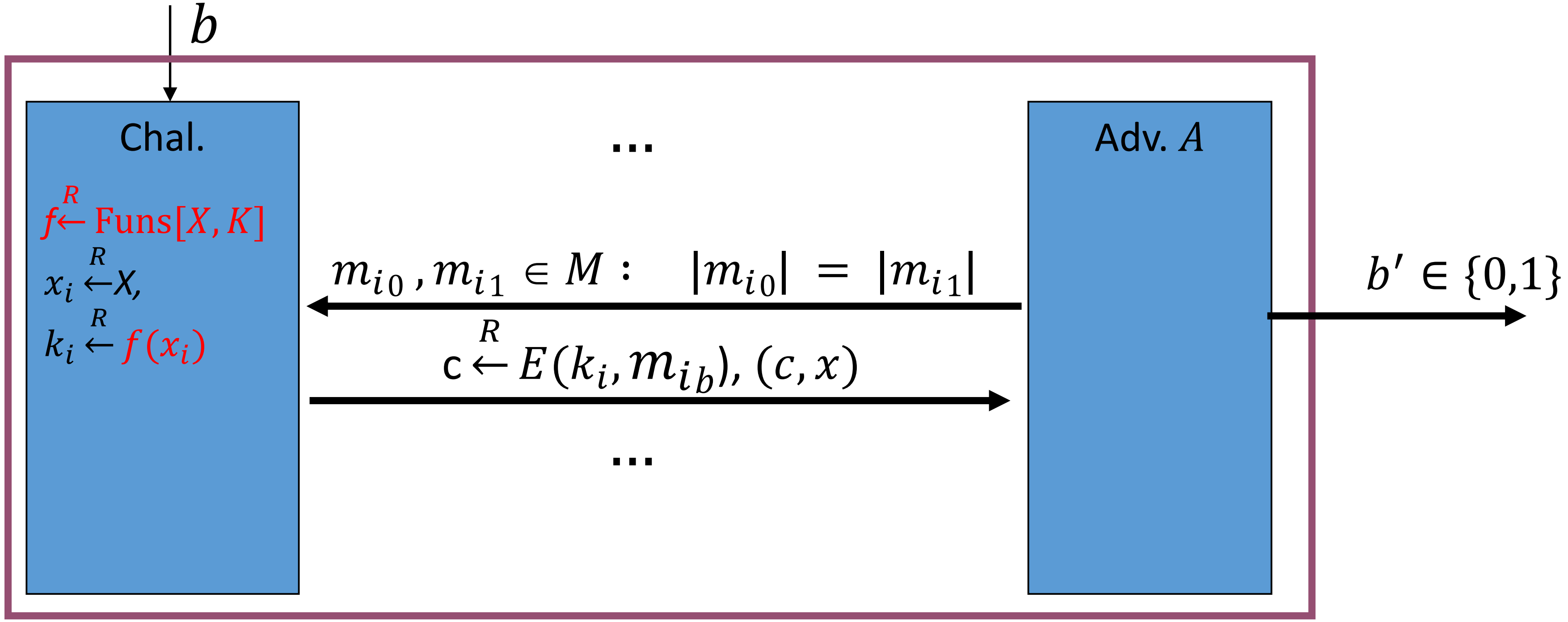
Игра 0

Для игры, введённой ниже, имеем $CPA^{*}_{adv}[A, \mathrm{E}'] = |\Pr[W_0] - 1/2|$



Игра 1

Введём игру 1, отличающуюся от игры 0, заменой псевдослучайной функции на случайную. Имеем $PRF_{adv}[B_F, F] = |\Pr[W_1] - \Pr[W_0]|$

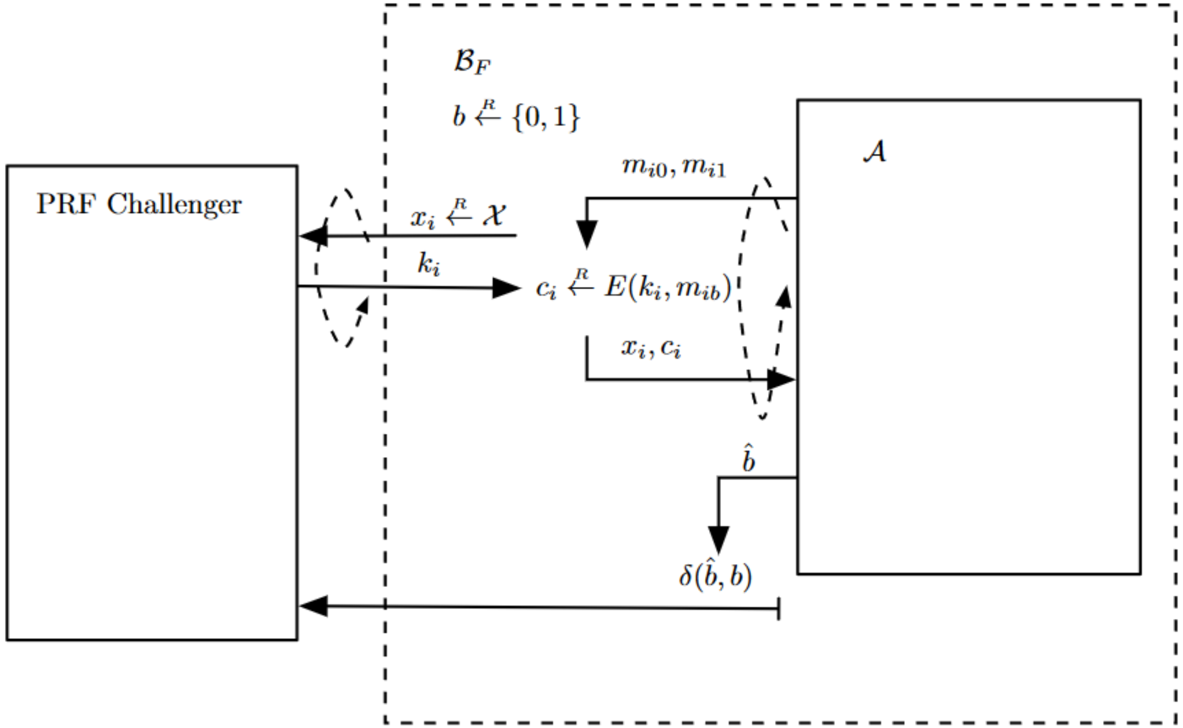


Структура противника B_F

Рассмотрим структуру противника B_F в игре на стойкость PRF, имеющим доступ к противнику A в игре на стойкость CPA.

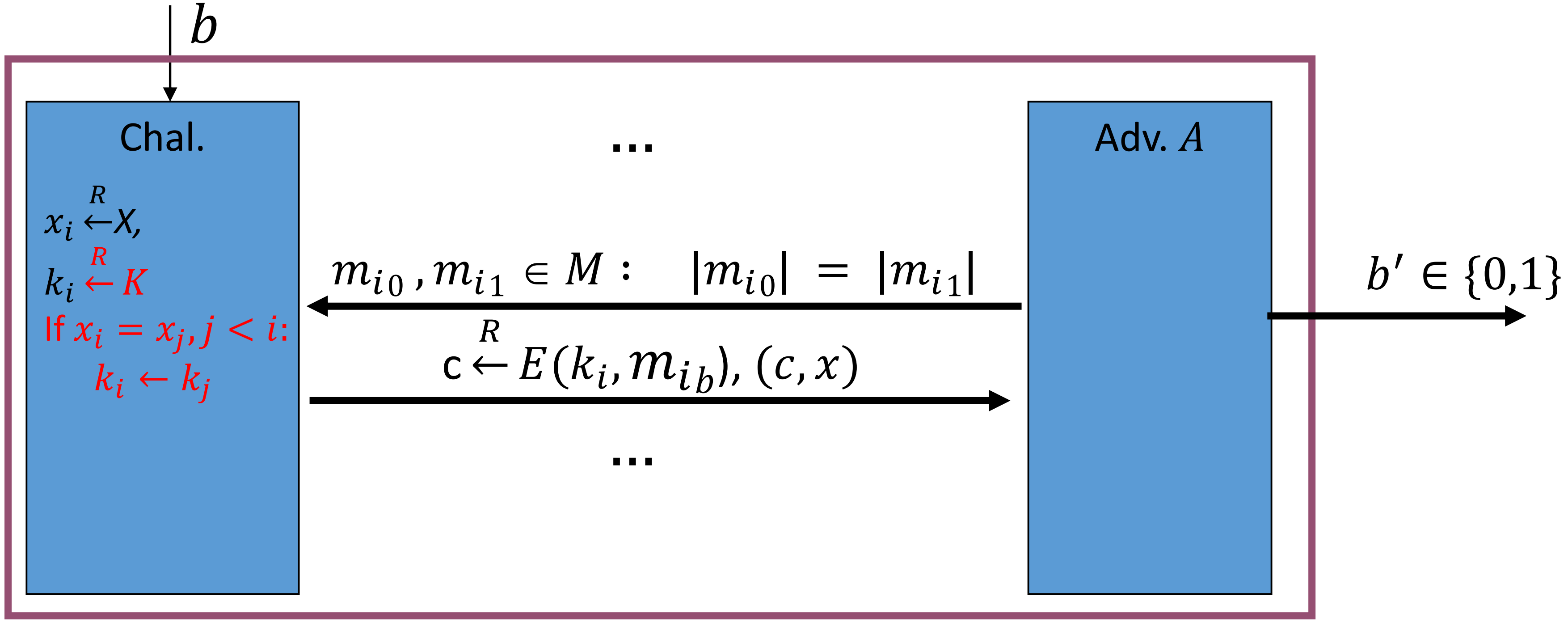
После получений пары сообщений от A, противник B_F выбирает случайный элемент $x_i \leftarrow^R X$, получая его образ от претендента (случайный или псевдослучайный). Затем он случайно выбирает одно из сообщений противника A и шифрует его на полученном образе.

После Q итераций он выдаёт результат противника A.



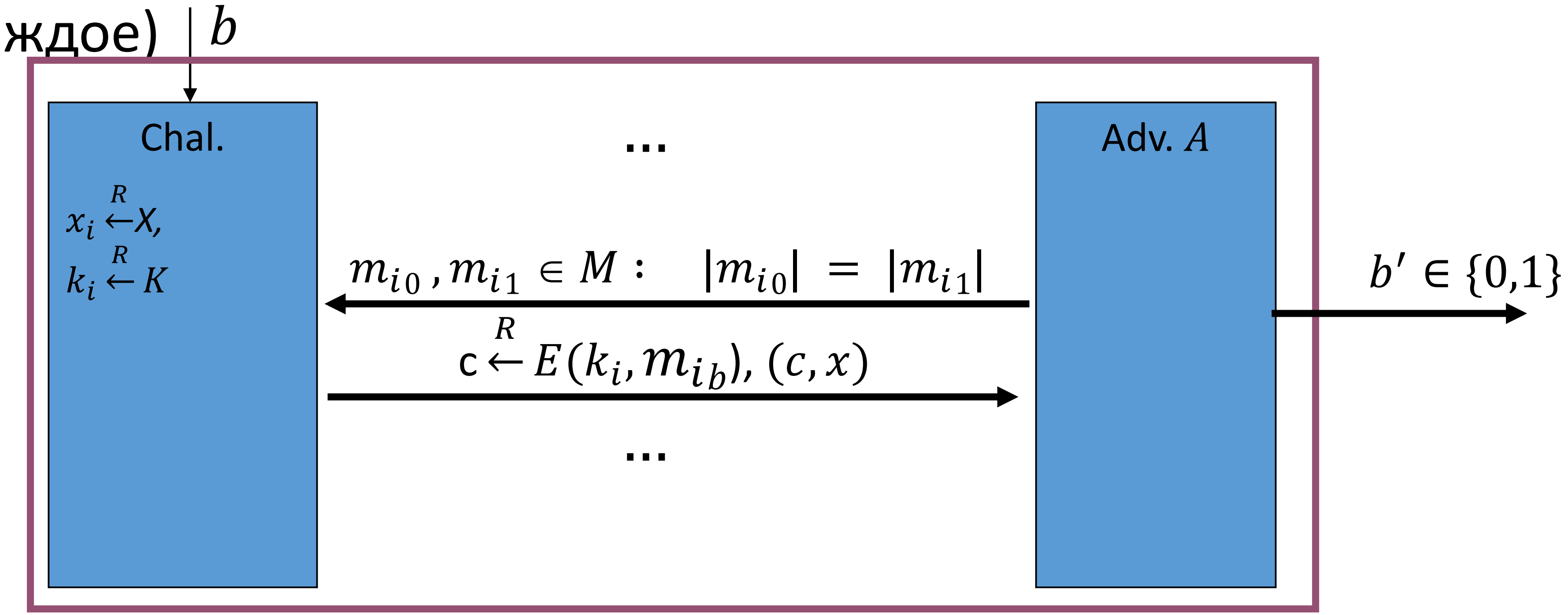
Игра 2

Рассмотрим игру, реализующую случайную функцию. Функция будет генерировать случайные входы на новых значениях, запоминая их. На старых (уже полученных ранее значениях) будет выдаваться результат, полученный ранее. Очевидно, что это просто «переопределение» игры 1, $\Pr[W_2] = \Pr[W_1]$



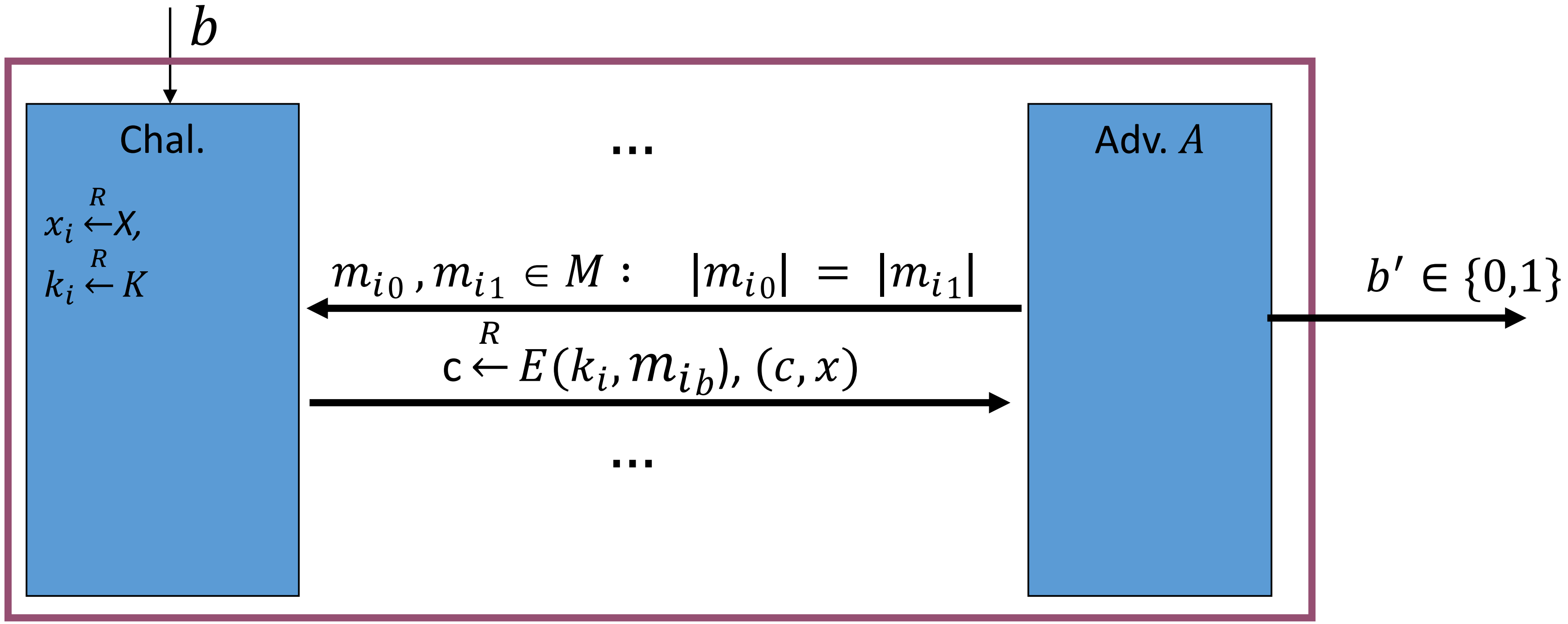
Игра 3

Рассмотрим «забывчивую» версию игры 2, в которой претендент не запоминает полученные величины. Заметим, что игры идентичны, если все x_i различны. Пусть Z событие того, что $x_i = x_j$. Тогда по **Теореме 6.1.1.1** и рассуждениям, аналогичным **Теореме 6.1.1** имеем $|\Pr[W_3] - \Pr[W_2]| \leq \Pr[Z] \leq Q^2/2N$ ($Q^2/2$ независимых событий с вероятностью $1/N$ каждое)



Игра 3.

Заметим, что в игре 3 используются независимые ключи шифрования, для каждого сообщения. Отсюда имеем шифрование на множестве независимых ключей и по определению $|\Pr[W_3] - 1/2| = MSS^{*}_{adv}[B^*, \mathrm{E}]$, где B^* противник, делающий не более Q запросов к противнику в игре на семантическую стойкость, при использовании множества ключей.

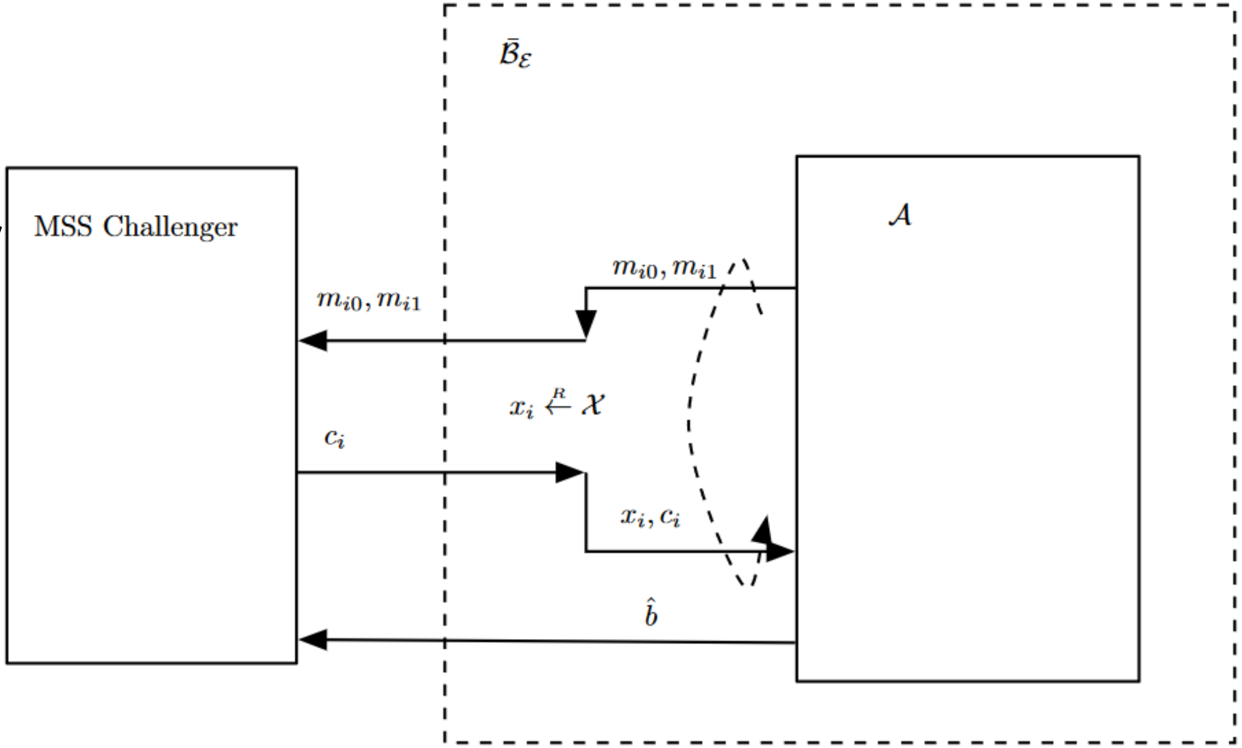


Структра противника B^*

Рассмотрим структуру противника B^*в игре на семантическую стойкость, при использовании множества ключей, имеющим доступ к противнику A в игре на стойкость CPA.

После получений пары сообщений от A, противник B_F Прозрачно отправляет их своему претенденту. После получения зашифрования одного из них, выбирает случаынй элемент $x_i \leftarrow^R X$, и отправляет (x_i, c_i) A.

После Q итераций он выдаёт результат противника A.



Построение CPA шифров из семантически стойких шифров

По теореме 6.4 имеем, что $MSS^*_{adv}[B^*, \mathrm{E}] = Q * SS^*_{adv}[B_E, \mathrm{E}]$, где B_E противник в игре на семантическую стойкость.

Итого:

- Игра 3 является игрой на использование множества ключей в семантическом стойком шифре, и отличается от игры на семантическую стойкость в Q раз
- Игра 3 и 2 отличаются не более чем на $Q^2/2N$,
- Игра 2 является переопределением игры 1
- Игра 1 – игра на стойкость PRF, преимущество (обычная версия) состоит из разности преимуществ в играх 0 и 1 (на угадывание бита) (собственно 0 и 2)
- Игра 0 – игра на стойкость CPA

$$CPA^*_{adv}[A, \mathrm{E}'] \le \frac{Q^2}{2N} + PRF_{adv}[B_F, F] + Q * SS^*_{adv}[B_E, \mathrm{E}] \lhd$$

Рандомизированный CRT режим

Рассмотрим ещё один способ построения – на основе CTR режима.

Пусть F PRF на (K, X, Y). Пусть $X = \{0, \ldots N-1\}$, $Y = \{0,1\}^n$. Для полиномиально ограниченной величины $l \geq 1$ определим шифр $\mathrm{E} = (E, D)$ на $(K, Y^{\leq l}, X \times Y^{\leq l})$ следующим образом:

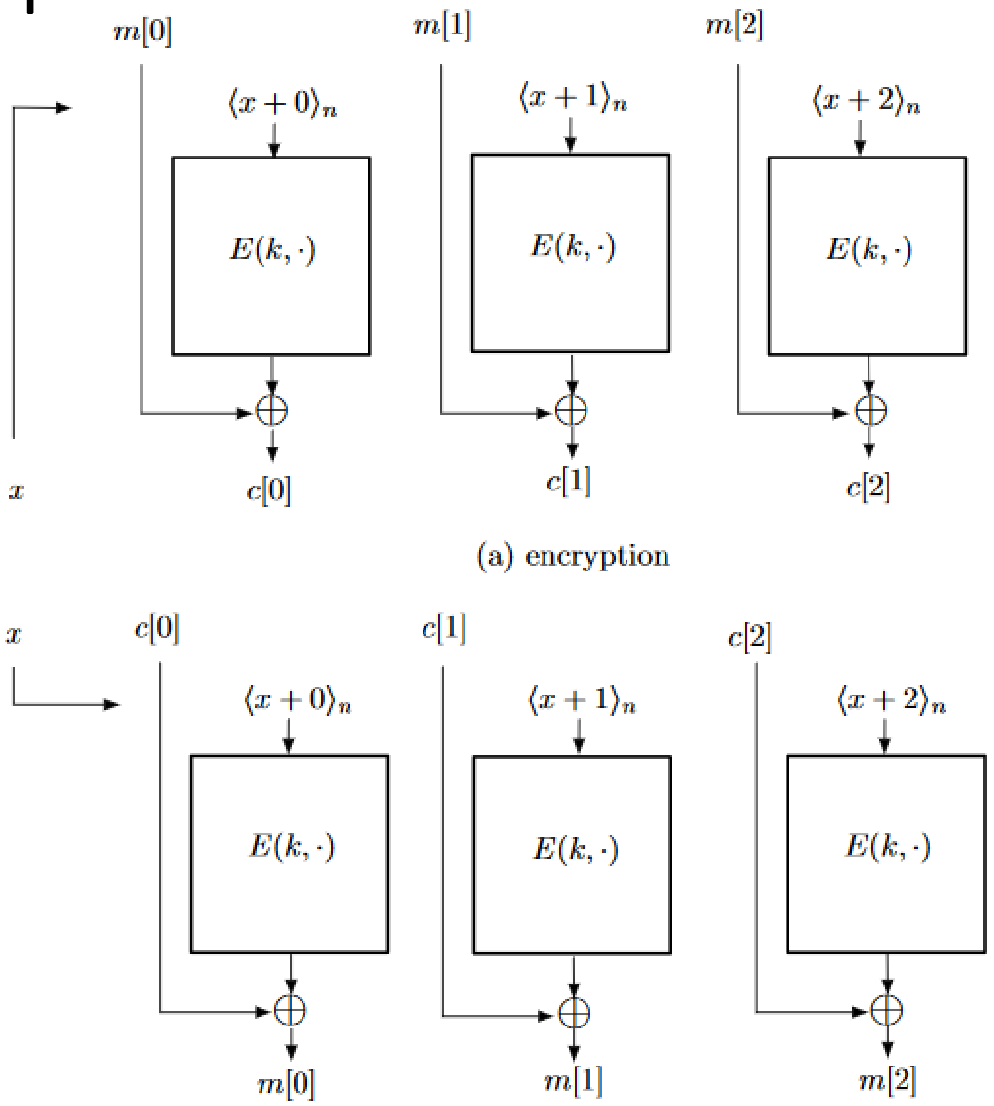
Для $k \in K, m \in Y^{\leq l}, v = |m|, = |\mathrm{c}|,\ \ c' = (x, c) \in X \times Y^{\leq l}$

$$
\begin{aligned}
&E(k, m) := \\
&\quad x \xleftarrow{R} \mathcal{X} \\
&\quad \text{compute } c \in \mathcal{Y}^v \text{ as follows:} \\
&\quad\quad \text{for } j \leftarrow 0 \text{ to } v-1 \text{ do} \\
&\quad\quad\quad c[j] \leftarrow F(k, x + j \bmod N) \oplus m[j] \\
&\quad \text{output } (x, c);
\end{aligned}
$$

$$
\begin{aligned}
&D(k, c') := \\
&\quad \text{compute } m \in \mathcal{Y}^v \text{ as follows:} \\
&\quad\quad \text{for } j \leftarrow 0 \text{ to } v-1 \text{ do} \\
&\quad\quad\quad m[j] \leftarrow F(k, x + j \bmod N) \oplus c[j] \\
&\quad \text{output } m.
\end{aligned}
$$

Рандомизированный CRT режим

- Шифр похож на детерминированный CRT режим, с той лишь разницей, что мы используем не фиксированное начальное значение счётчика, а выбираем его случайно равновероятно, а затем используем шифр аналогично детерминированному алгоритму.



Рандомизированный CRT режим

Теорема 7.2. Если F – стойкая PRF, N - суперполиномиальная, l – полиномиально ограниченная, то введённый ранее шифр E - CPA стойкий шифр. В частности для любого противника в CPA игре, делающим не более Q запросов к претенденту существует противник B в игре на стойкость PRF причём

$$CPA_{adv}[A, \mathrm{E}'] \leq \frac{4Q^2 l}{N} + 2 * PRF_{adv}[B, F]$$

Рандомизированный CRT режим

$$\rhd\ CPA_{adv}[A, \mathrm{E}'] \leq \frac{4Q^2 l}{N} + 2 * PRF_{adv}[B, F]$$

Перепишем формулу выше через альтернативные определения на угадывание бита

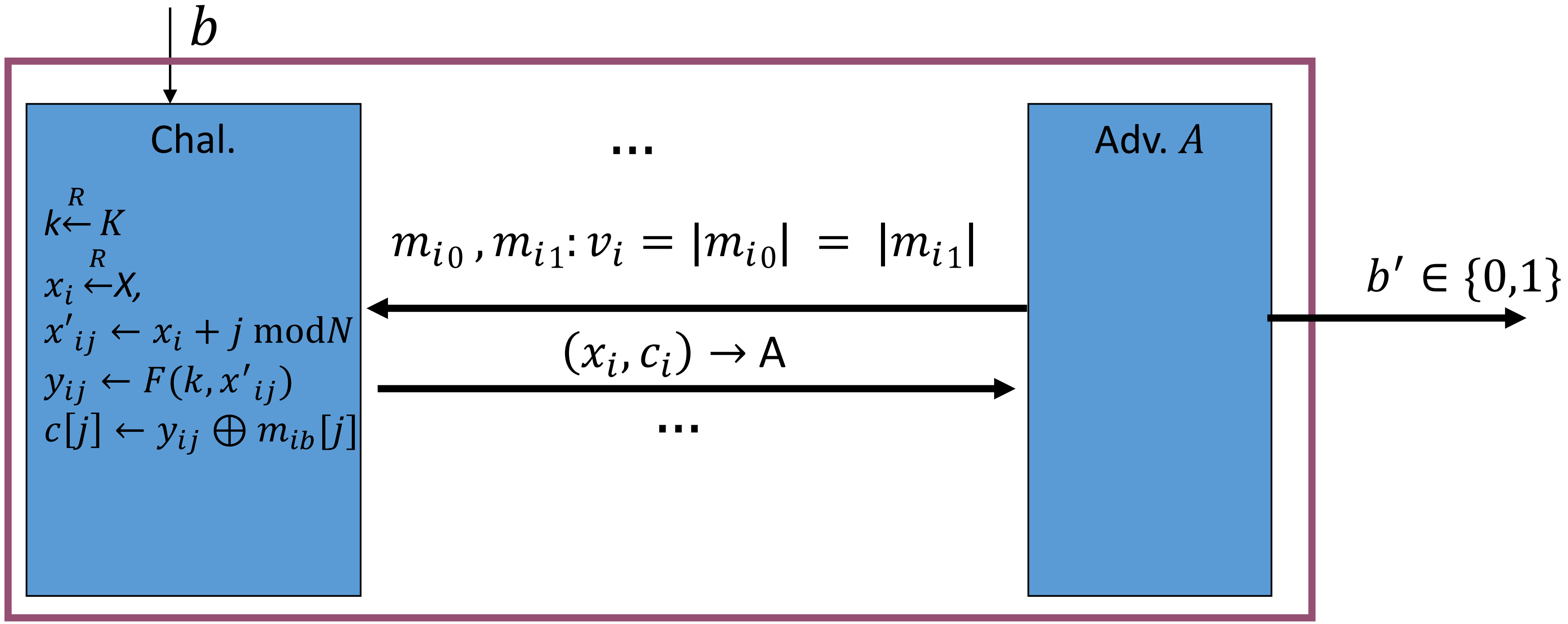
$$CPA^{*}_{adv}[A, \mathrm{E}'] \leq \frac{2Q^2 l}{N} + PRF_{adv}[B, F]$$

Основная идея доказательства – определим игру 0 между противником A и претендентом в игре против E. Определим игры 1, 2, 3. В каждый из них противник A будет играть против разных претендентов. Покажем переходы между этими играми.

Определим W_j как событие того, что $b' = b$ в игре j.

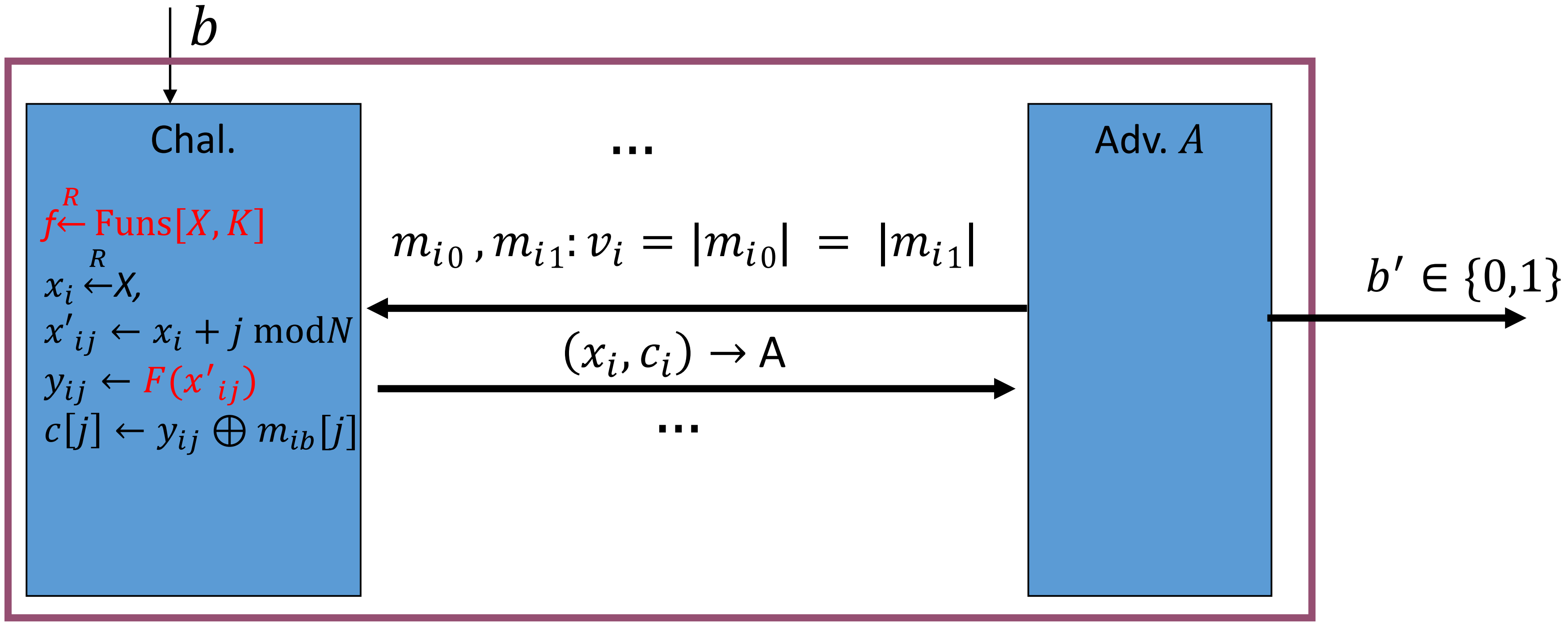
Игра 0

Для игры, введённой ниже, имеем $CPA^{*}_{adv}[A, \mathrm{E}] = |\Pr[W_0] - 1/2|$



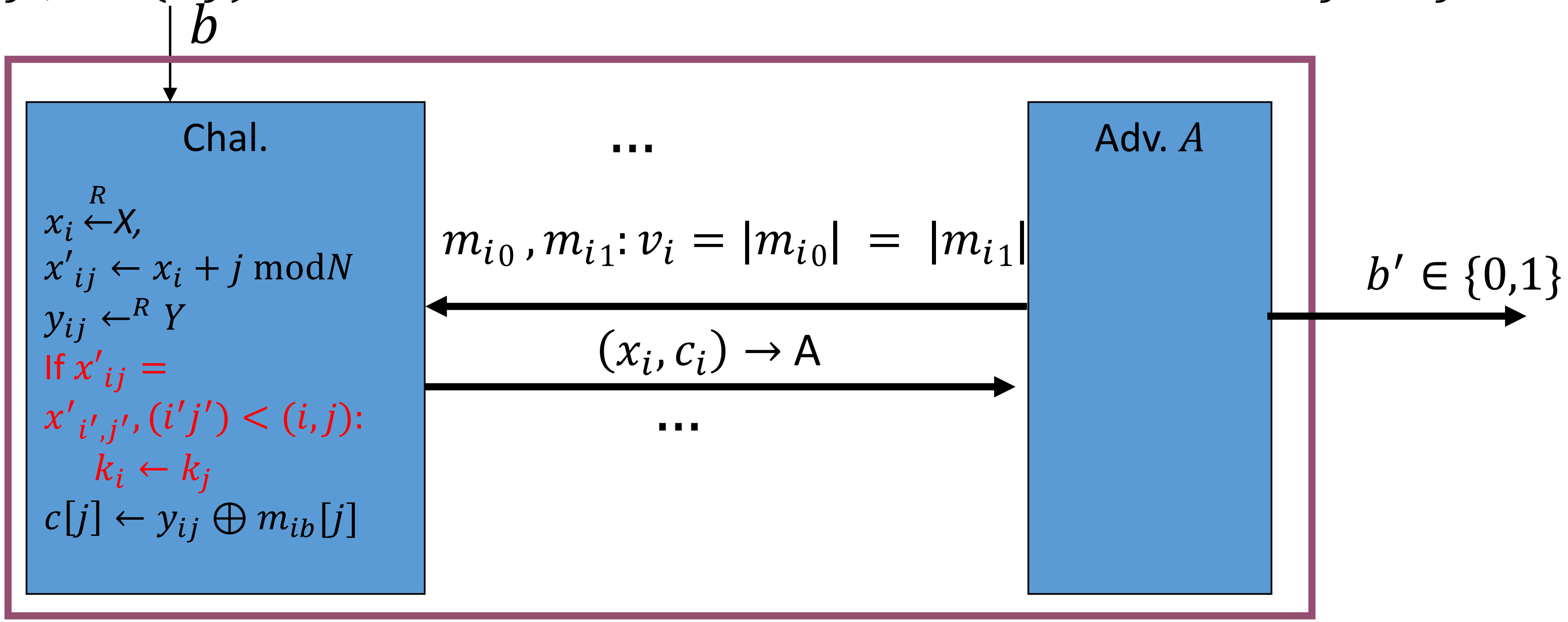
Игра 1

Введём игру 1, отличающуюся от игры 0, заменой псевдослучайной функции на случайную. Имеем $PRF_{adv}[B, F] = |\Pr[W_1] - \Pr[W_0]|$



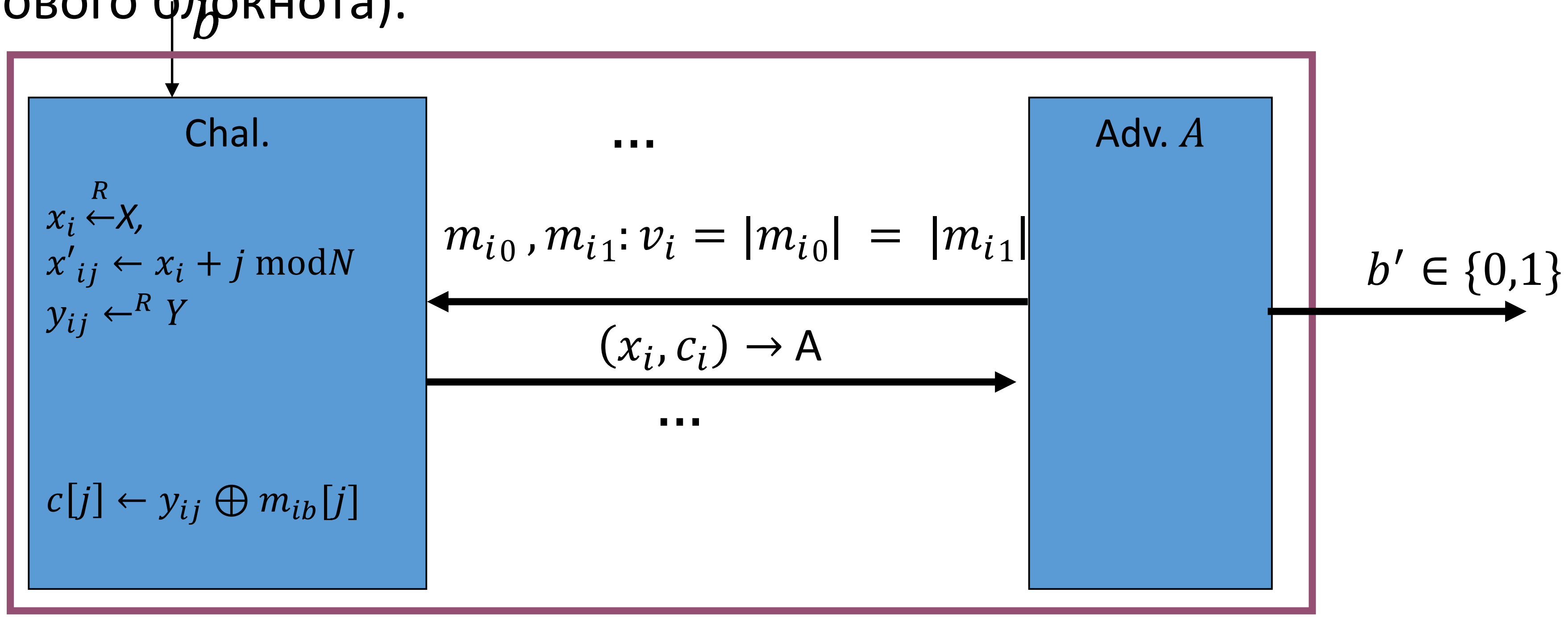
Игра 2

Рассмотрим игру, реализующую случайную функцию. Функция будет генерировать случайные входы на новых значениях, запоминая их. На старых (уже полученных ранее значениях) будет выдаваться результат, полученный ранее. Очевидно, что это просто «переопределение» игры 1, $\Pr[W_2] = \Pr[W_1]$. Здесь и далее используем стандартное отношение порядка на парах (i, j): $(i', j') < (i, j)$ тогда и только тогда, когда $i' < i$ или $i' = i, j' < j$.



Игра 3

Рассмотрим «забывчивую» версию игры 2, в которой претендент не запоминает полученные величины. Заметим, что игры идентичны, если все x_i различны. Пусть Z событие того, что $x'_{ij} = x'_{i',j'}, (i,j) \neq (i',j')$ Тогда по **Теореме 6.1.1.1** и рассуждениям, аналогичным **Теореме 6.1.1** имеем $|\Pr[W_3] - \Pr[W_2]| \leq \Pr[Z] \leq 2Q^2 l/N$. При этом $\Pr[W_3] = 1/2$ (игра против одноразового блокнота).



Лемма

В условии игры 3 имеем $|\Pr[W_3] - \Pr[W_2]| \leq \Pr[Z] \leq 2Q^2 l/N$

Без потери общности предположим что $N \geq 2l$ (что вообще говоря верно начиная с некоторого N, из условий на N и l). Событие Z происходит тогда, и только тогда когда $\{x_i, \ldots, x_i + l - 1\} \cap \{x_{i'}, \ldots, x_{i'} +$

Рандомизированный CRT режим

Итого:

- Игра 3 является игрой против одноразового блокнота
- Игра 3 и 2 отличаются не более чем на $2Q^2l/N$
- Игра 2 является переопределением игры 1
- Игра 1 – игра на стойкость PRF, преимущество (обычная версия) состоит из разности преимуществ в играх 0 и 1 (на угадывание бита) (собственно 0 и 2)
- Игра 0 – игра на стойкость CPA

$$CPA^*_{adv}[A, \mathrm{E}'] \le \frac{2Q^2l}{N} + PRF_{adv}[B, F] \triangleleft$$

Практическое использользование AES в режиме CTR

IPsec, RFC 3686. Выбор начального значения счётчика выполняется следующим образом:

- 32 наиболее значимых бита выбираются **случайно** в момент генерации ключа (**и независимо от него**), и **фиксируются** во время его жизни (nonce).
- Следующие 64 бита выбираются случайно из $\{0,1\}^{64}$ (IV).
- Последние 32 бита устанавливаются в $0^{31}1$.

Максимальная длина сообщения для зашифрования - 2^{32} блоков AES или 2^{36} байт.

CBC

Пусть $\mathrm{E} = (E, D)$ блочный шифр на (K, X) где $X = \{0,1\}^n, N = |X| = 2^n$. Для полиномиально ограниченной величины $l \geq 1$ определим шифр $\mathrm{E} = (E', D')$ на $(K, X^{\leq l}, X^{\leq l+1} \backslash \mathrm{X}^0)$. Зашифрование и разсшифрование определены следующим образом:

Для $k \in K, m \in M, v = |m| = |c| - 1$

$E'(k, m) :=$

  compute $c \in \mathcal{X}^{v+1}$ as follows:

    $c[0] \xleftarrow{\text{R}} \mathcal{X}$

    for $j \leftarrow 0$ to $v - 1$ do

      $c[j+1] \leftarrow E(k,\ c[j] \oplus m[j])$

  output c;

$D'(k, c) :=$

  compute $m \in \mathcal{X}^v$ as follows:

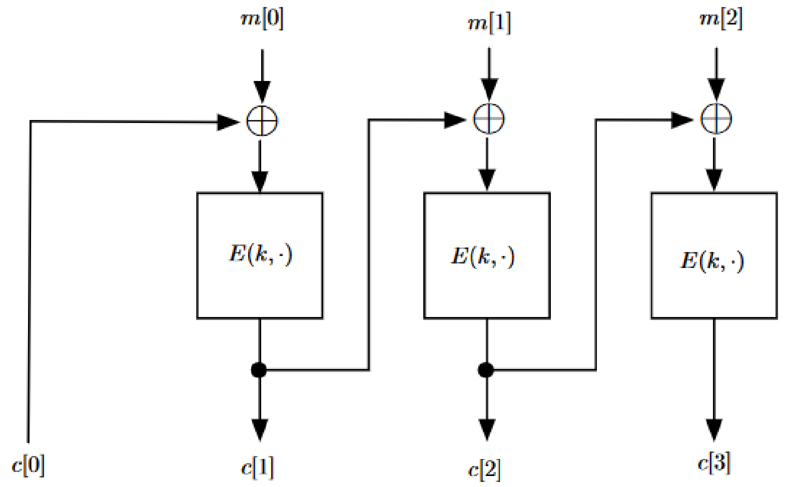
    for $j \leftarrow 0$ to $v - 1$ do

      $m[j] \leftarrow D(k,\ c[j+1]) \oplus c[j]$

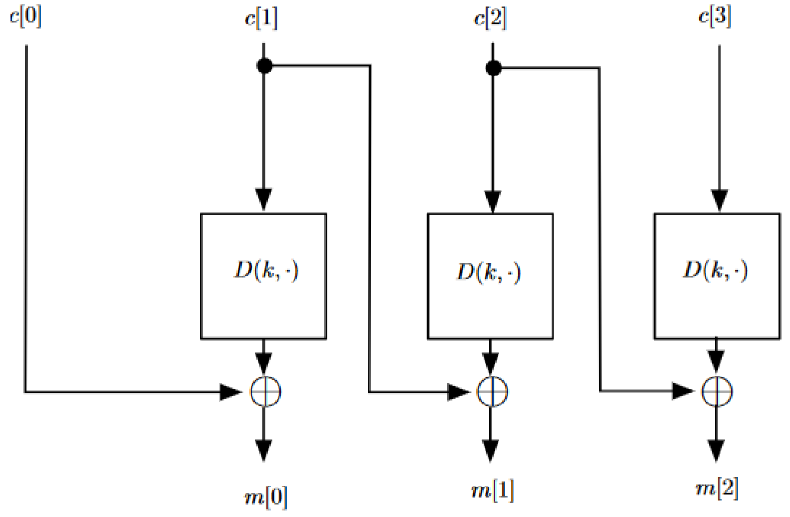
  output m.

CBC

- В отличии от режима CTR для реализации CBC необходима функция расшифрования блочного шифра
- $c[0]$ носит название вектора инициализации (IV)
- IV должны быть случайным для каждого передаваемого сообщения



(a) encryption



(b) decryption

CBC

Теорема 7.3. Пусть $\mathrm{E} = (E, D)$ – семантически стойкий шифр на (K, C), $N = |X|$ - суперполиномиальная, $l \geq 1$ – полиномиально ограниченная. Тогда введенный ранее CBC шифр является CPA стойким, причём для любого противника A в игре на CPA стойкость, делающим не более Q запросов к оракулу, существует противник B в игре на стойкость блочных шифров, при чём

$$CP_{adv}[A, \mathrm{E}'] \leq \frac{2Q^2l^2}{N} + 2 * BC_{adv}[B, \mathrm{E}]$$

Рандомизированный CRT режим

$$\rhd\, CP_{adv}[A, \mathrm{E}'] \le \frac{2Q^2 l^2}{N} + 2 * BC_{adv}[B, \mathrm{E}]$$

Перепишем формулу выше через альтернативные определения на угадывание бита

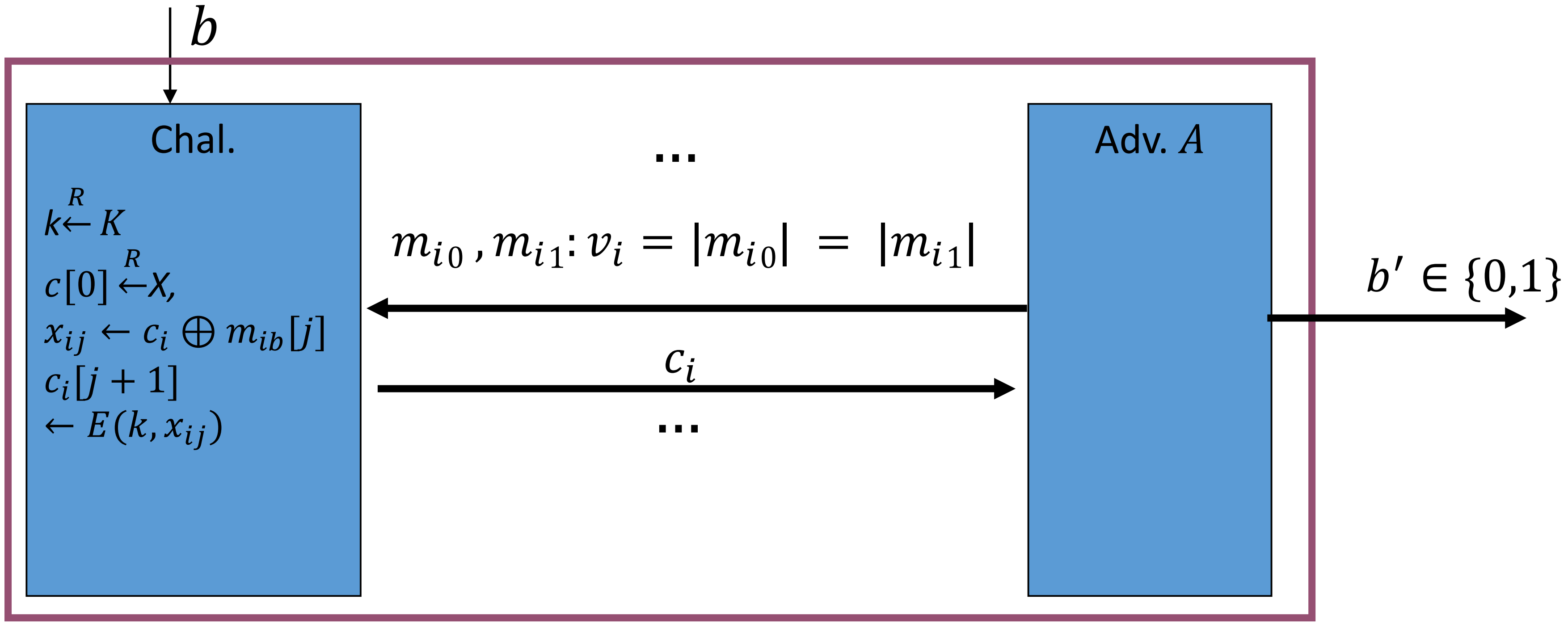
$$CP_{adv}^{*}[A, \mathrm{E}'] \le \frac{2Q^2 l^2}{N} + BC_{adv}[B, \mathrm{E}]$$

Основная идея доказательства – определим игру 0 между противником A и претендентом в игре против E. Определим игры 1, 2, 3. В каждый из них противник A будет играть против разных претендентов. Покажем переходы между этими играми.

Определим W_j как событие того, что $b' = b$ в игре j.

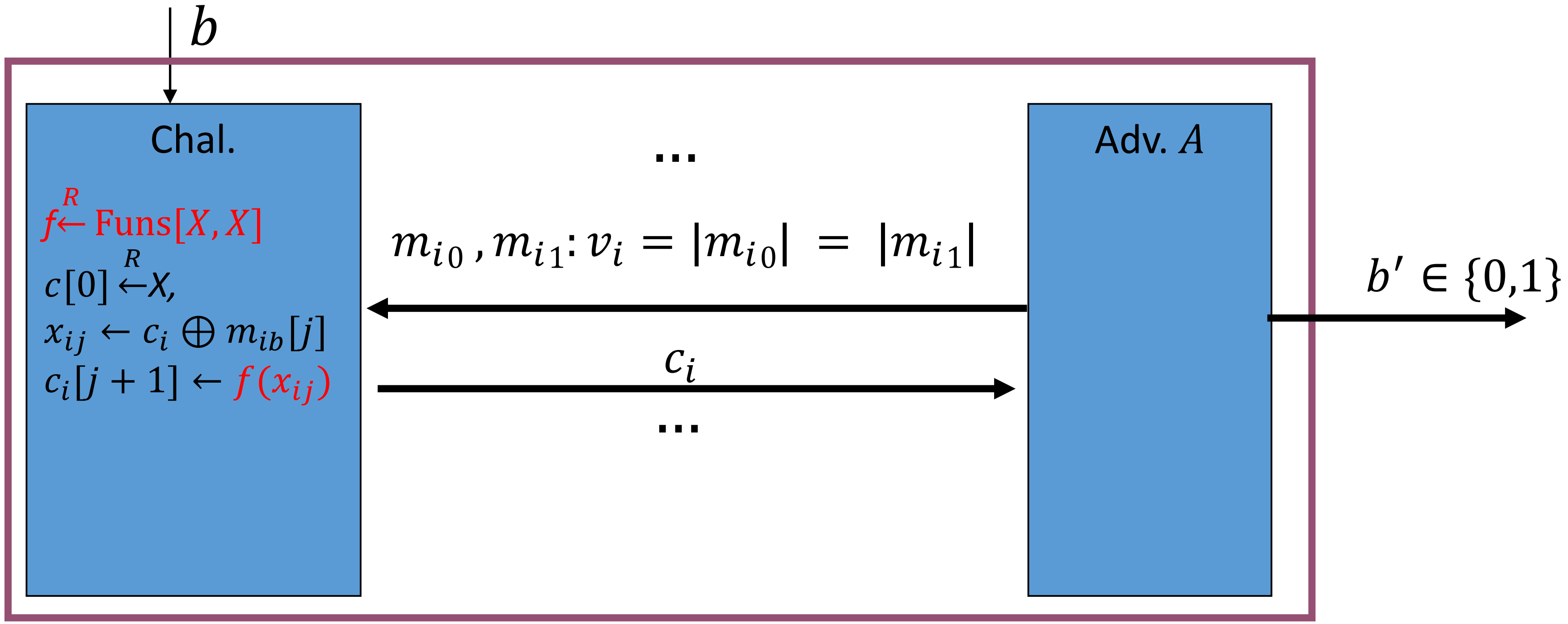
Игра 0

Для игры, введённой ниже, имеем $CPA^*_{adv}[A,\mathrm{E}] = |\Pr[W_0] - 1/2|$



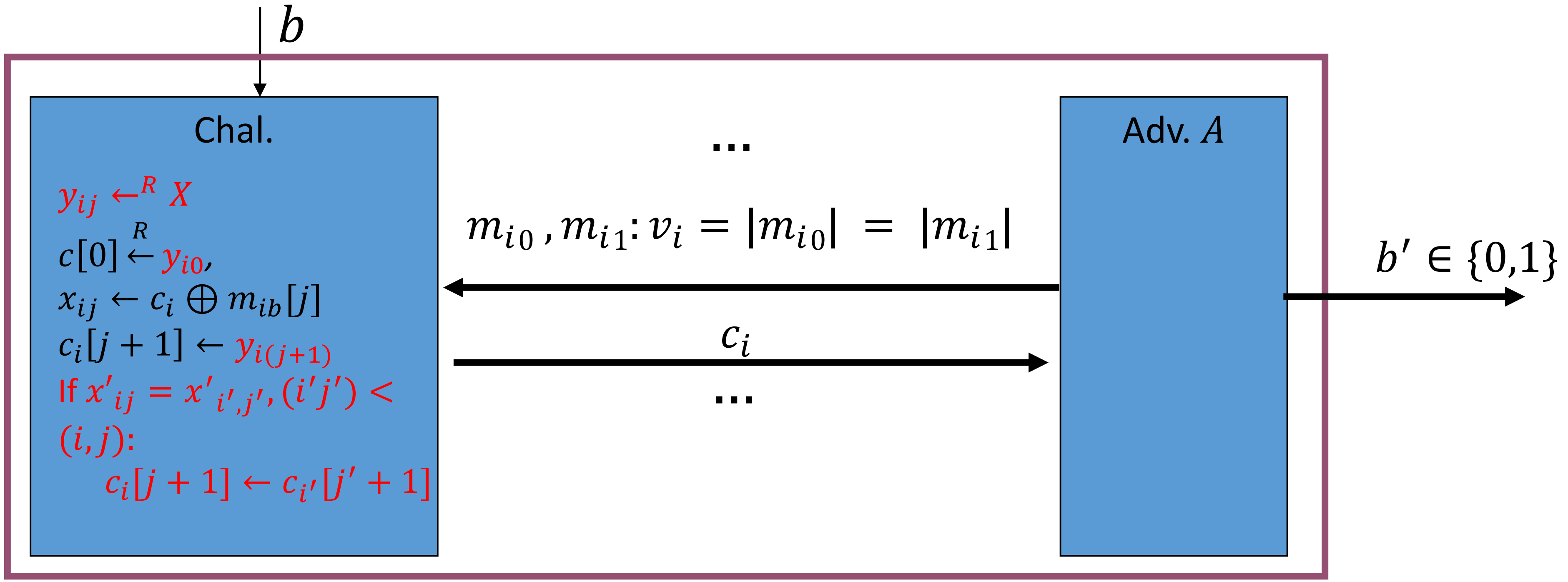
Игра 1

Введём игру 1, отличающуюся от игры 0, заменой псевдослучайной функции на случайную. Имеем $PRF_{adv}[B, E] = |\Pr[W_1] - \Pr[W_0]|$



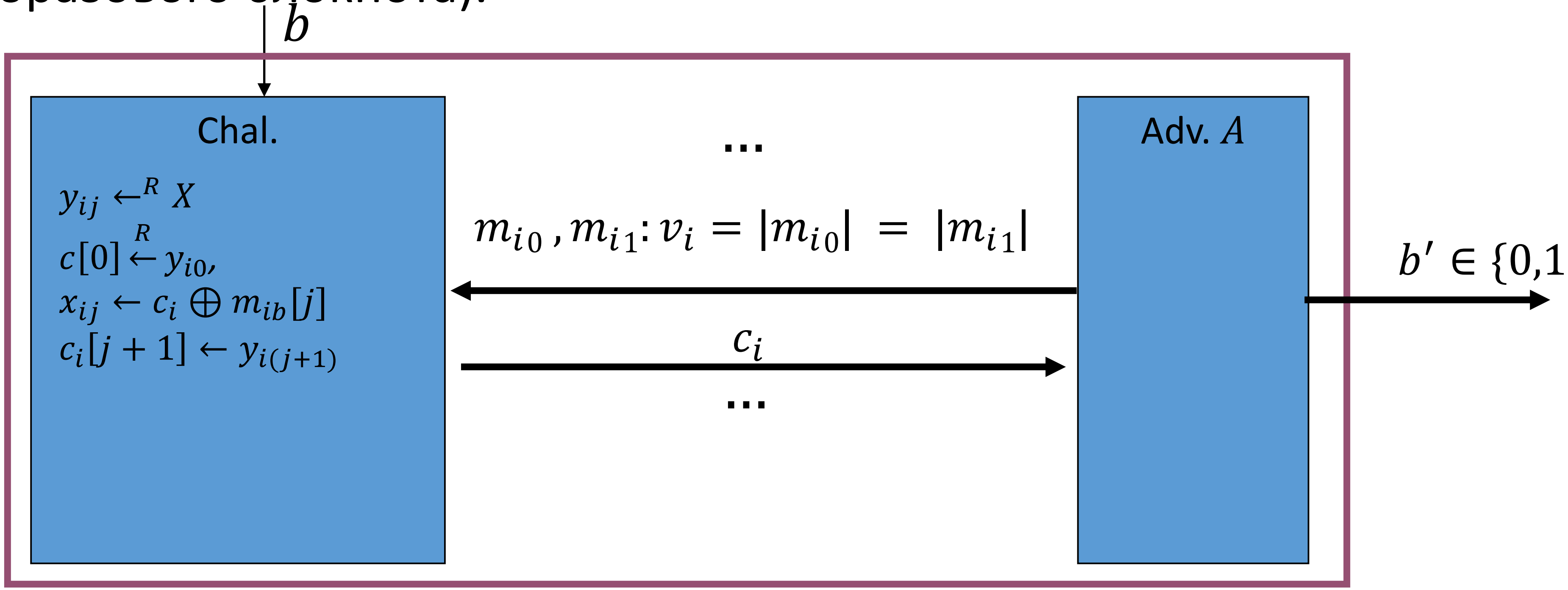
Игра 2

Рассмотрим игру, реализующую случайную функцию. Функция будет генерировать случайные входы на новых значениях, запоминая их. На старых (уже полученных ранее значениях) будет выдаваться результат, полученный ранее. Очевидно, что это просто «переопределение» игры 1, $\Pr[W_2] = \Pr[W_1]$.



Игра 3

Рассмотрим «забывчивую» версию игры 2, в которой претендент не запоминает полученные величины. Заметим, что игры идентичны, если все x_i различны. Пусть Z событие того, что $x'_{ij} = x'_{i',j'}, (i,j) \neq (i',j')$ Тогда по **Теореме 6.1.1.1** и рассуждениям, аналогичным **Теореме 6.1.1** имеем $|\Pr[W_3] - \Pr[W_2]| \leq \Pr[Z] \leq Q^2 l^2/2N$. При этом $\Pr[W_3] = 1/2$ (игра против одноразового блокнота).



Лемма

В условии игры 3 имеем $|\Pr[W_3] - \Pr[W_2]| \leq \Pr[Z] \leq Q^2 l^2 / 2N$

добавить док-во, стр 195#

CBC

Итого:

- Игра 3 является игрой против одноразового блокнота

Игра 3 и 2 отличаются не более чем на $Q^2 l^2 / 2N$

- Игра 2 является переопределением игры 1
- Игра 1 – игра на стойкость PRF, преимущество (обычная версия) состоит из разности преимуществ в играх 0 и 1 (на угадывание бита) (собственно 0 и 2)
- Игра 0 – игра на стойкость CPA

$$CP_{adv}^{*}[A, \mathrm{E}'] \leq \frac{Q^2 l^2}{2N} + PRF_{adv}[B, \mathrm{E}]$$

Используя Теорему 6.1 имеем

$$CP_{adv}^{*}[A, \mathrm{E}'] \leq \frac{2Q^2 l^2}{N} + BC_{adv}[B, \mathrm{E}] \lhd$$

Дополнение блока

В режиме CBC сообщения должны быть кратны длине блока блочного шифра.

Если сообщения не кратны длине блока – используется дополнение (padding).

Наиболее распространённый способ TLS (PKCS) padding:

- Если сообщение имеет длину m байт, а блок b байт, то дополнение $pad \in \{0, .., 15\}^p = (p-1, \dots, p-1), p = m - b$
- Если $b = m$, то $p = 16$.

CBC vs CTR

$$CPA_{adv}[A, \mathrm{E}_{ctr}] \leq \frac{4Q^2 l}{N} + 2 * PRF_{adv}[B, F]$$

$$CP_{adv}[A, \mathrm{E}_{cbc}] \leq \frac{2Q^2 l^2}{N} + 2 * BC_{adv}[B, \mathrm{E}]$$

- CTR режим имеет большую стойкость для фиксированных параметров и блочного шифра
- CTR может использоваться в параллельном режиме, так как зашифрование блоков производит независимо
- Для коротких сообщений CRT может иметь длины шифртекстов значительно короче, чем CBC, так как нет необходимости в дополнении до длины блока.
- CTR использует только функцию зашифрования блочного шифра.
- **IV должны быть случайными!**