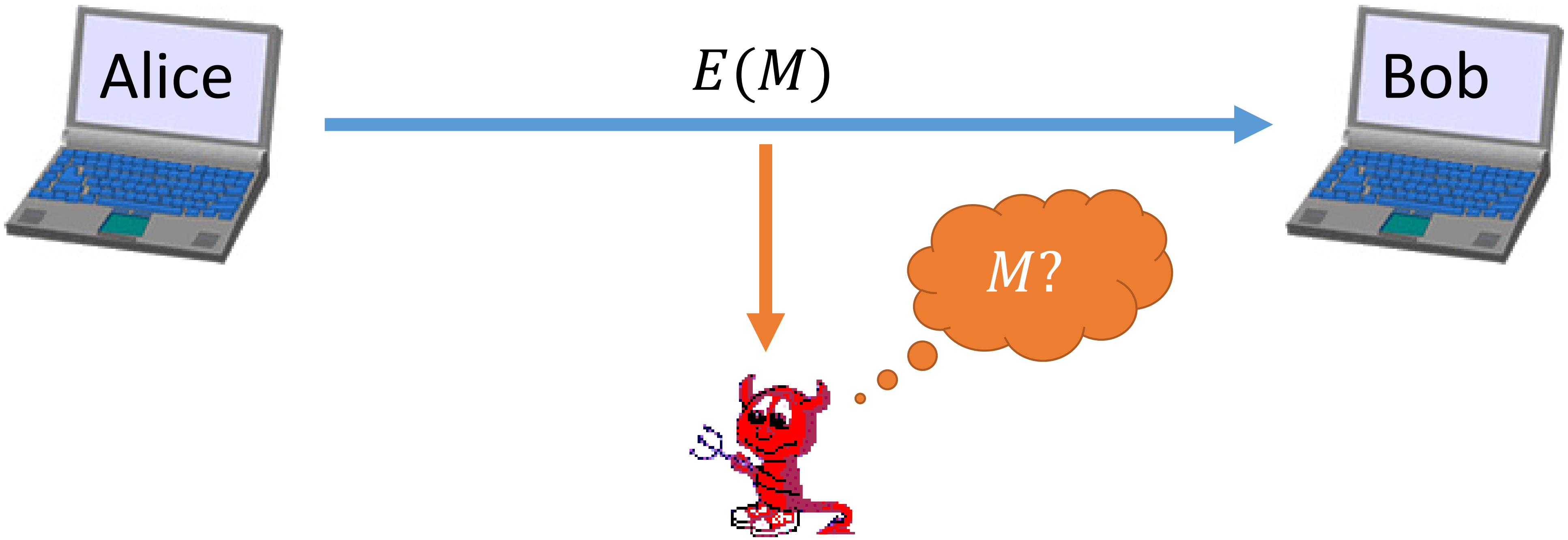
Прикладная Криптография: Симметричные криптосистемы MAC

Макаров Артём

МИФИ 2018

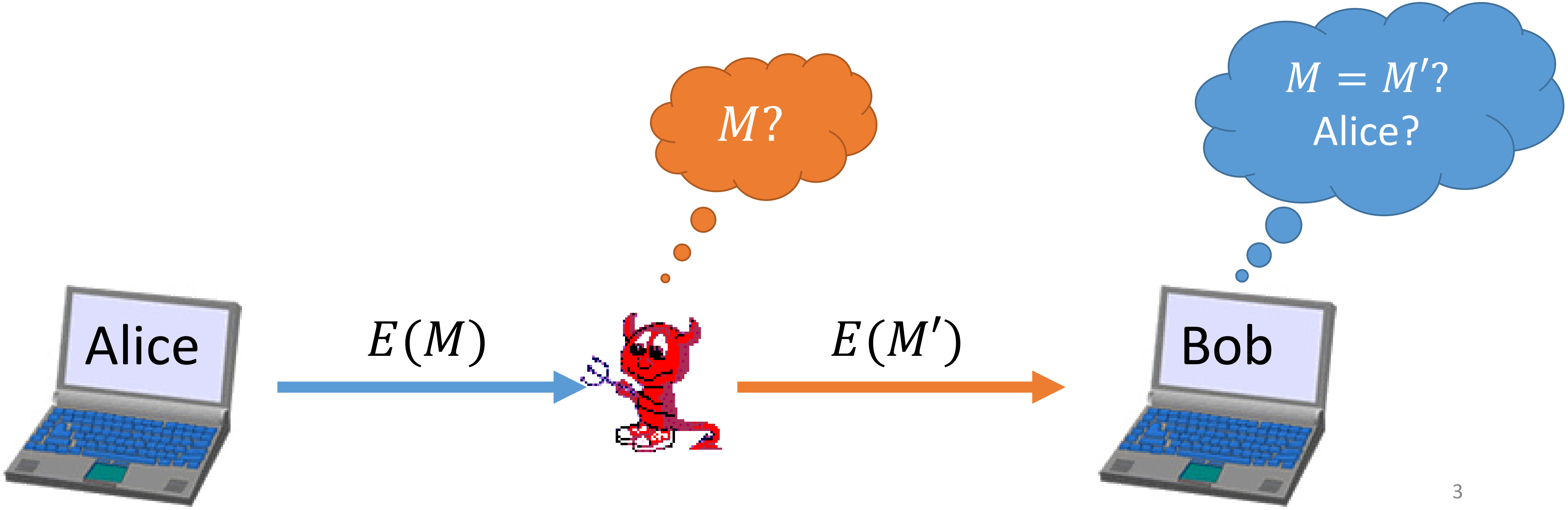
Защита от пассивного противника

- До этого мы рассматривали защиту информации от пассивного противника – противника, который не изменяет сообщения в канале информации



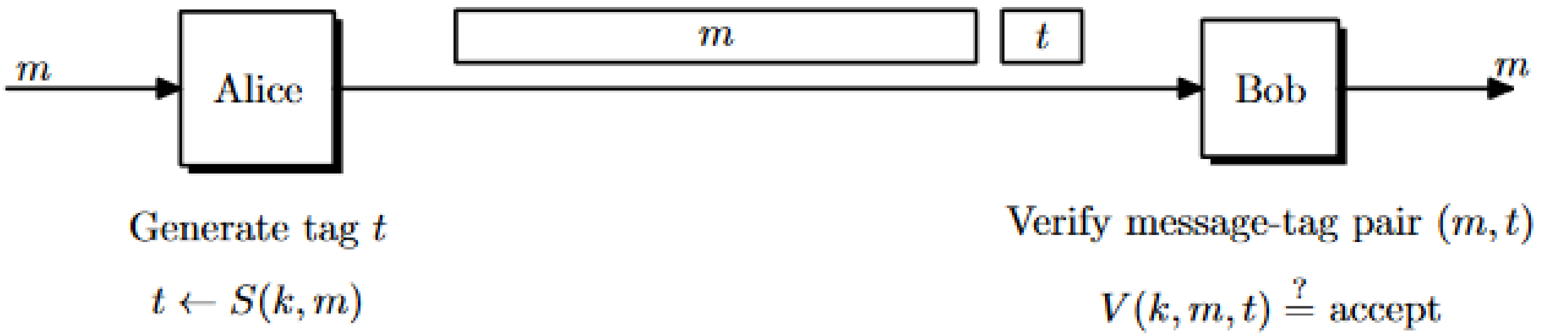
Защита от активного противника

В общем случае задача более сложная – защита от активного противника, который может подменять, изменять и передавать собственные сообщения в канале связи



Целостность сообщений

- Задача – обеспечить целостность сообщений m при передаче
- Обеспечиваем только **целостность**, сообщения предполагаются открытыми
- Основная идея – создать небольшую по длине величину t (tag, метка) на основе сообщения, и передать данную величину вместе с сообщением: (m, t). На стороне получателя величина t' вычисляется для полученного сообщения m' и производится сравнение $t = t'$. В случае равенства полагается, что целостность сообщения не нарушена.



Целостность сообщений

- В данной лекции рассматриваем только защиту целостности
- В дальнейшем в лекциях будем говорить и об обеспечении целостности и конфиденциальности (аутентифицированное шифрование)
- … но даже только обеспечение целостности имеет реальные приложения.
  - Пример – открытое распространение новостей об итогах торгов на бирже. Новости не являются секретными, но мы хотим удостоверится, что была обеспечена их целостность (т.е. их не подменили при передаче). Заметим, что порядок сообщений может быть обеспечен, при обеспечении целостности их нумерации (т.е. защищаем не только целостность сообщений, но их id).
  - Пример – обеспечение целостности дистрибутивов бесплатного программного обеспечения

Обеспечение целостности

- Как построить алгоритм обеспечения целостности?
- Очевидно он должен зависеть от сообщения
- Необходимо использование секретного ключа, неизвестного противнику, так как иначе противник может подменить сообщение и вычислить для него новый tag
- **ВАЖНО** CRC32 и другие циклические коды не подходят для решения указанной нами задачи. Задача циклических кодов – обеспечение целостности при защите от случайных изменений, вызванных передачей по каналу связи. Мы пытаемся защититься от преднамеренных изменений, внесённых противником, который может вычислить и CRC32 для произвольных сообщений. Более того, для CRC32 возможно эффективное построение коллизий.

Определение MAC

Введём определение кода аутентичности сообщения (MAC, message authentication code, имитовставка).

MAC на (K, M, T) называется пара эффективных алгоритмов $I = (S, V)$. S – алгоритм выработки MAC, V – алгоритм проверки MAC. Пусть M – множество сообщений, K – множество ключей, T – множество кодов аутентичности (меток). Тогда для $m \in M, t \in T, k \in K$

- $S: K \times M \rightarrow T$ - вероятностный алгоритм, вычисляющий $t \xleftarrow{R} S(k, m)$
- $V: K \times M \times T \rightarrow \{0,1\}$ – детерминированный алгоритм, вычисляющий результат проверки $r \leftarrow V(k, m, t)$.
- Свойство корректности - $\Pr\left[V\left(k, m, S(k, m)\right) = 1\right] = 1$

Детерминированный MAC

- Если функция S – детерминированная, то для любой такой функции мы можем ввести функцию

$$V(k,m,t) = \begin{cases} 1, S(k,m) = t \\ 0, S(k,m) \neq t \end{cases}$$

Очевидно, что полученный MAC обладает свойством корректности и называется детерминированным MAC. Т.е. для фиксированного ключа он выдает одинаковый код аутентичности для одинаковых сообщений.

- Если функция S – рандоминизованная то MAC называется рандомизированным.

Стойкий MAC

Введём понятие стойкости MAC.

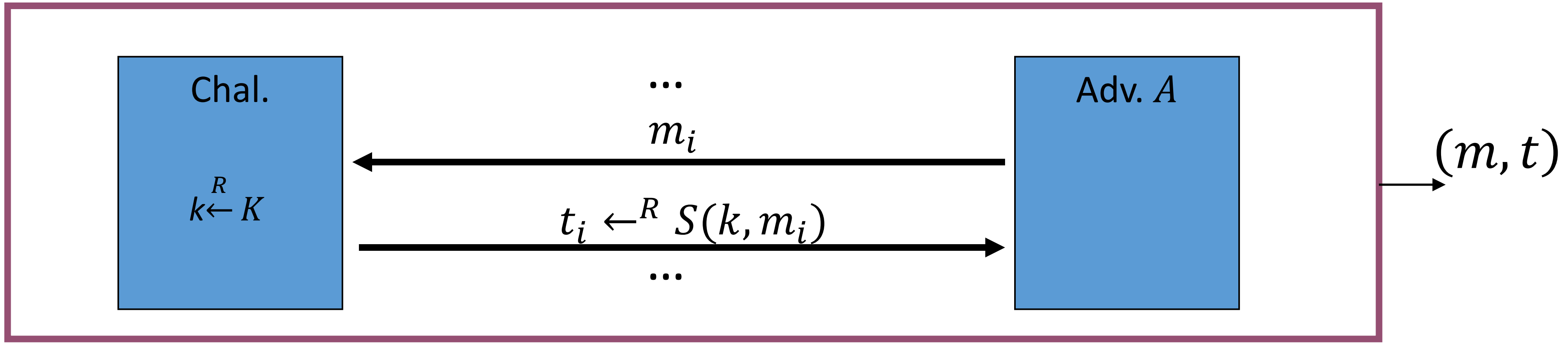
Возможности противника – выбор сообщений для получения MAC для них

Цель противника – получения новой верной пары сообщение-MAC

Стойкий MAC – MAC не позволяющий противнику получить такую пару

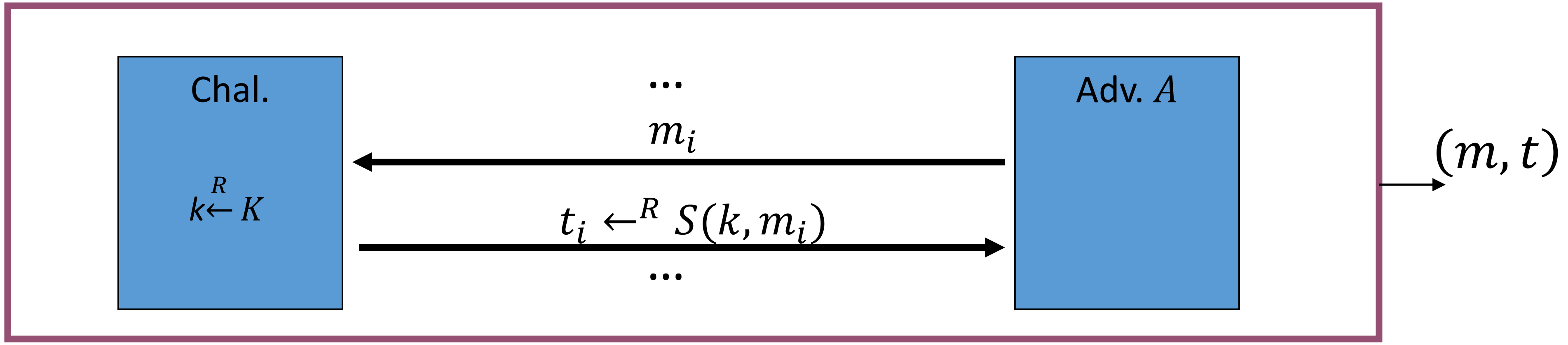
Игра на стойкость MAC (chosen message attack)

- Претендент выбирает случайный ключ $k \xleftarrow{R} K$
- Противник на i-м запросе отправляет произвольное сообщение $m_i \in M$
- Претендент отвечает на i-й запрос $t_i \xleftarrow{R} S(k, m_i)$
- Противник выдаёт пару $(m, t) \in M \times T$: $(m, t) \notin \{(m_1, t_1), (m_2, t_2) \ldots\}$



Игра на стойкость MAC (chosen message attack)

- Противник побеждает в игре, если пара (m, t) – верная пара сообщение – MAC, т.е. $V(k, m, t) = 1$.
- Преимуществом противника A в игре против MAC $I = (S, V)$ называется величина $MAC_{adv}[A, I] = \Pr[V(k, m, t) = 1]$.
- MAC $I = (S, V)$ называется стойким MAC, если $\forall A\ MAC_{adv}[A, I] \leq \epsilon, \epsilon$ – пренебрежимо малая величина.



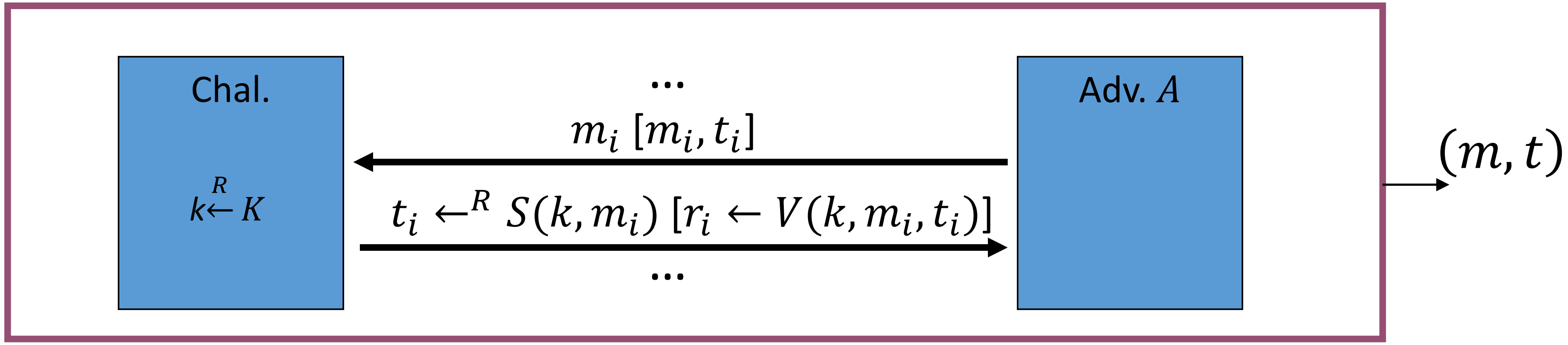
Игра на стойкость MAC

В описанной ранее игре противник не имеет доступа к ключу, соответственно не может проверить самостоятельно, выдаёт ли он корректную пару в результате игры. В реальности, как правило, противник может узнать, является ли его результат корректным, например по тексту ошибки от сервера. Модифицируем игру, чтобы отразить данную возможность.

Помимо запросов на получения MAC для произвольного сообщения, добавим возможность запросов на проверку для произвольной пары сообщение-MAC.

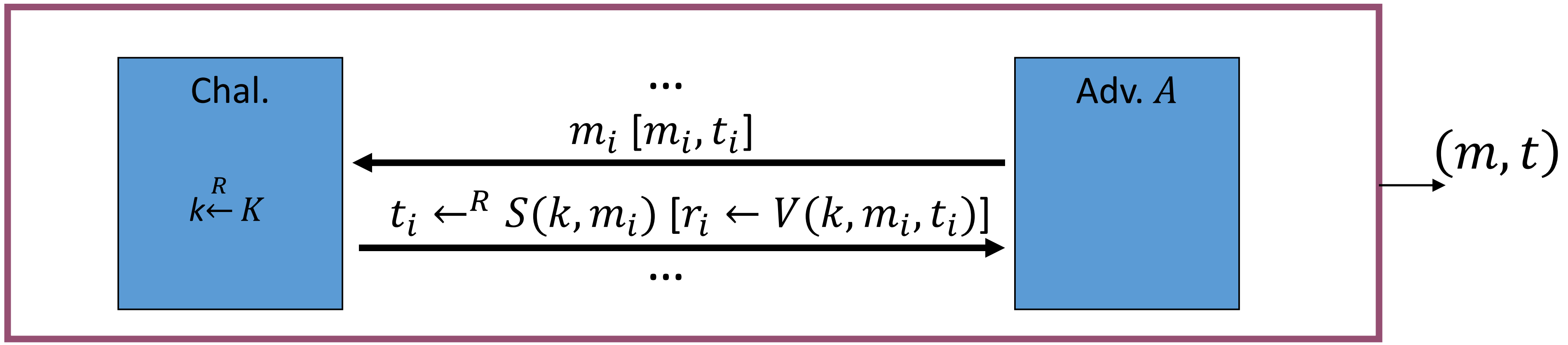
Игра на стойкость MAC (с запросами на проверку)

- Претендент выбирает случайный ключ $k \xleftarrow{R} K$
- Противник на i-м запросе отправляет произвольное сообщение $m_i \in M$ для получения MAC [или произвольную пару m_i, t_i для проверки, при условии что MAC для m_i ранее не запрашивали]
- Претендент отвечает на i-й запрос $t_i \xleftarrow{R} S(k, m_i)$ если было получено сообщение m_i, [или $r \leftarrow V(k, m_i, t_i)$, если было получено сообщение (m_i, t_i)]
- Противник выдаёт пару $(m, t) \in M \times T$: $(m, t) \notin \{(m_1, t_1), (m_2, t_2) \dots\}$



Игра на стойкость MAC (с запросами на проверку)

- Противник побеждает в игре, если пара (m, t) – верная пара сообщение – MAC, т.е. $V(k, m, t) = 1$.
- Преимуществом противника A в игре против MAC $I = (S, V)$ называется величина $MAC_{adv}^{vq}[A, I] = \Pr[V(k, m, t) = 1]$.
- MAC $I = (S, V)$ называется vq стойким MAC, если $\forall A \; MAC_{adv}[A, I] \leq \epsilon, \epsilon$ – пренебрежимо малая величина.

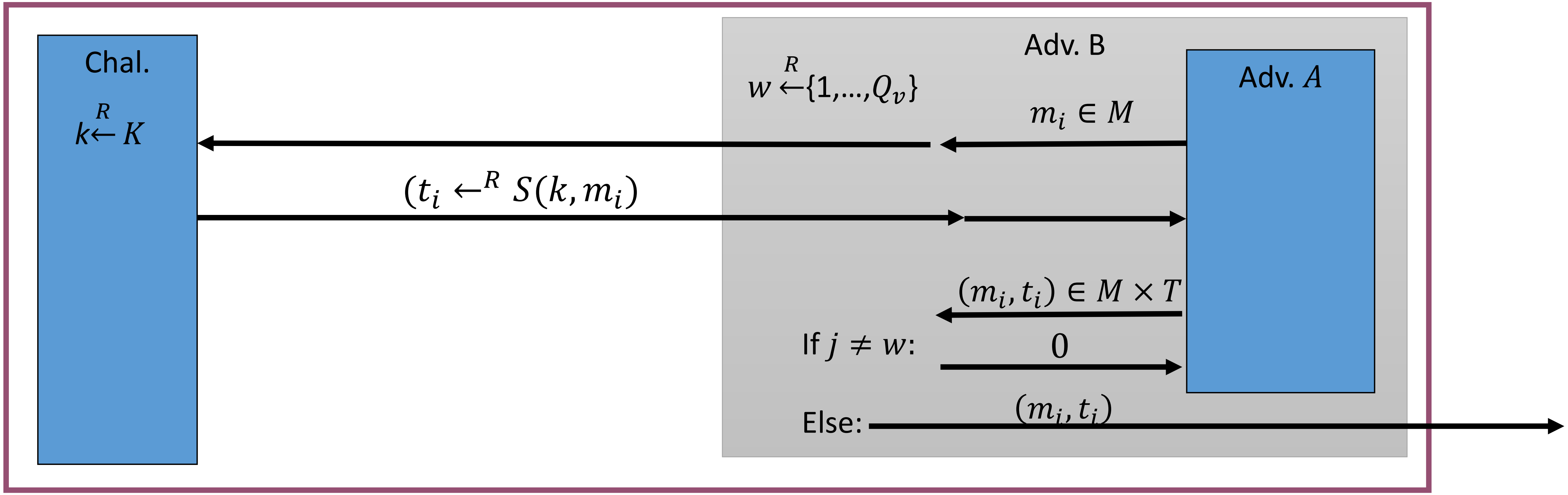


Эквивалентность определений

Теорема 9.1. Определения стойкость и vq стойкости эквивалентны, в частности для любого противника A в игре на vq стойкость MAC, делающего не более Q_s запросов на получение MAC, не более Q_v запросов на проверку MAC, существует противник B в игре на стойкость MAC, делающий не более Q_s запросов, причём

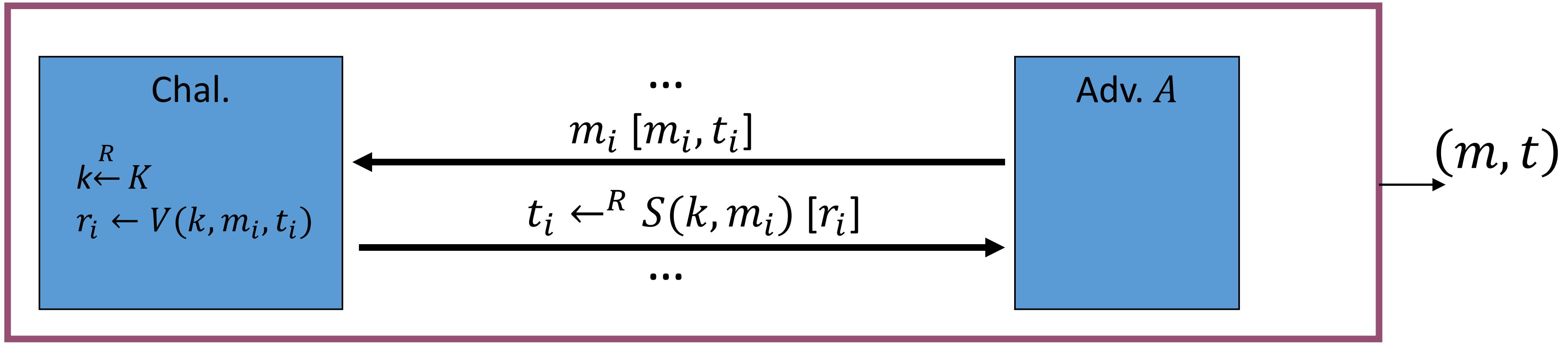
Имея противника A, построим противника B

Построение противника B



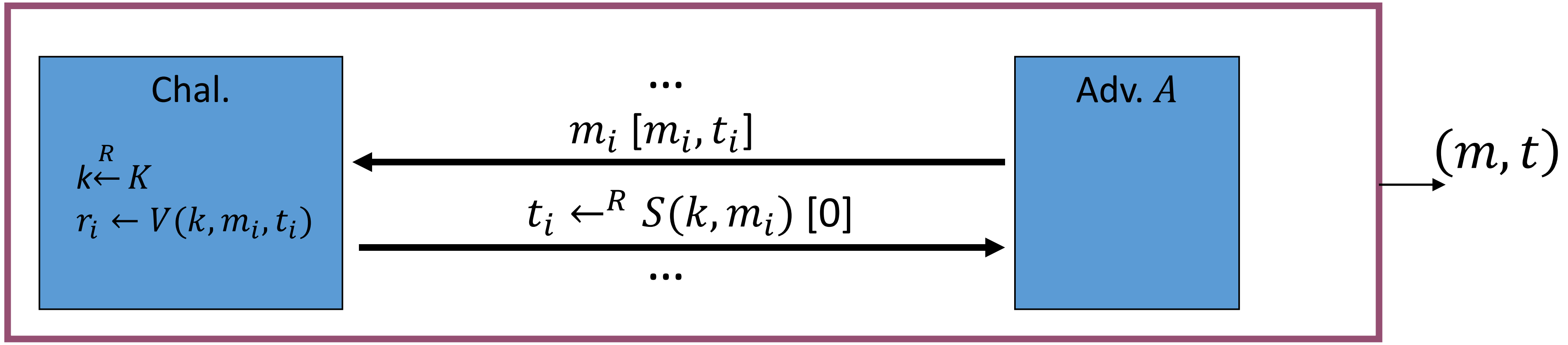
Игра 0

Рассмотрим игру на vq стойкость. Обозначим W_0 событие того, что $r_j = 1$ для некоторого j. $\Pr[W_0] = MAC_{adv}^{vq}[A, I]$



Игра 1

Аналогично игре 0, но претендент «вредный» и всегда отвечает 0 на любые запросы на проверку. Обозначим W_1 событие того, что в игре 1 величина $r_i \leftarrow V(k, m, t)$ =1 для некоторого j (т.е. хотя бы одна пара, полученная от противника была верной). Очевидно, что до события W_1, игры 0 и 1 идентичны (разница только когда, когда претендент возвращает 0, а должен был вернуть 1). Т.е. $\Pr[W_0] = \Pr[W_1]$ до события W_1 включительно.

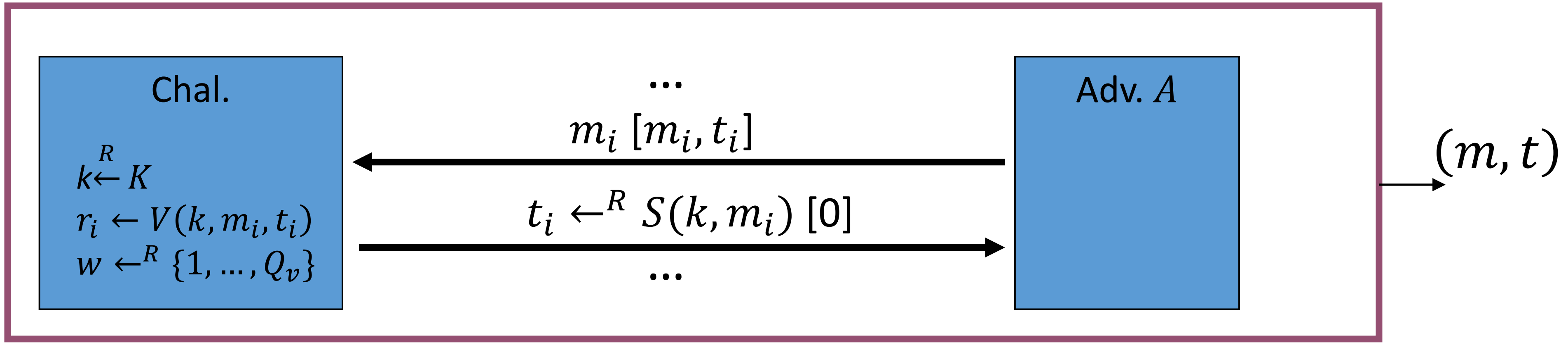


Игра 2

Модифицируем игру 1, но теперь в начале игры претендент выберет $w \leftarrow^R \{1, \dots, Q_v\}$. Обозначим W_2 событие того, что в игре 2 $r_w = 1$. Так как w выбирается независимо случайно и равновероятно, то $\Pr[W_2] \geq \Pr[W_1]/Q_v$. Заметим, что $\Pr[W_2] = MAC_{adv}[B, I]$ (для построенного ранее B).

Сводя игру 0 к игре 2 имеем:

$$MAC_{adv}^{vq}[A, I] \leq MAC_{adv}[B, I] * Q_v \triangleleft$$



Построение MAC на основе PRF

Построим MAC следующим образом. Пусть F – PRF.

- $S(k, m) = F(k, m)$
- $V(k, m, t) = \begin{cases} 1, F(k, m) = t \\ 0, F(k, m) \neq t \end{cases}$

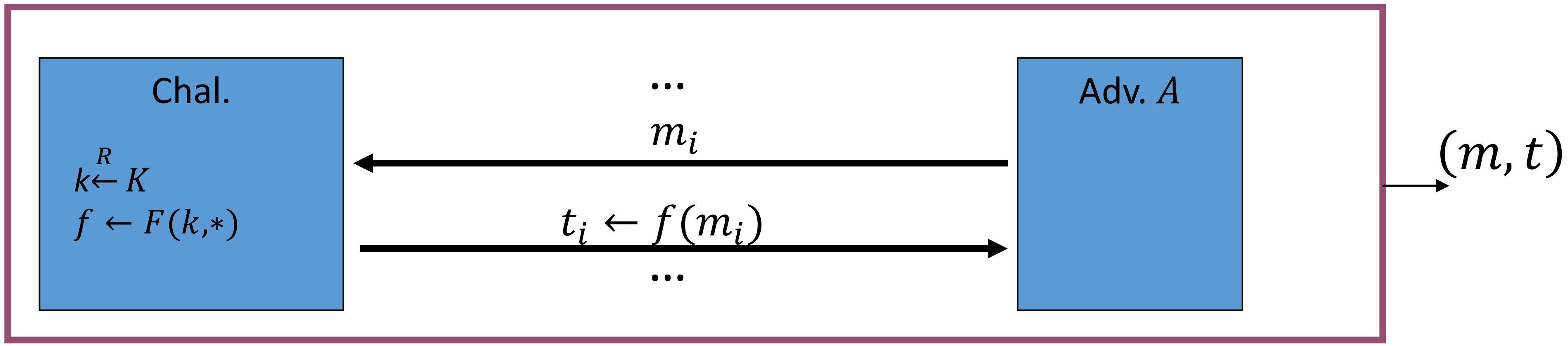
Теорема 9.2. Пусть F – стойкая PRF на (K, X, Y), $|Y|$ - суперполиномиальная. Тогда MAC $I = (S, V)$ полученный из F – стойкий, причём $\forall A$ противника в игре против MAC, делающим не более Q запросов, существует противник B в игре против PRF, причём

$$MAC_{adv}[A, I] \leq PRF_{adv}[B, F] + 1/|Y|$$

Игра 0

▻ Введём игру на стойкость MAC для описанной конструкции.

Обозначим W_0 - событие того в игре 0, что $t = f(m), m \neq \{m_1, m_2, \dots\}$.
Очевидно, что $\Pr[W_0] = MAC_{adv}[A, I]$

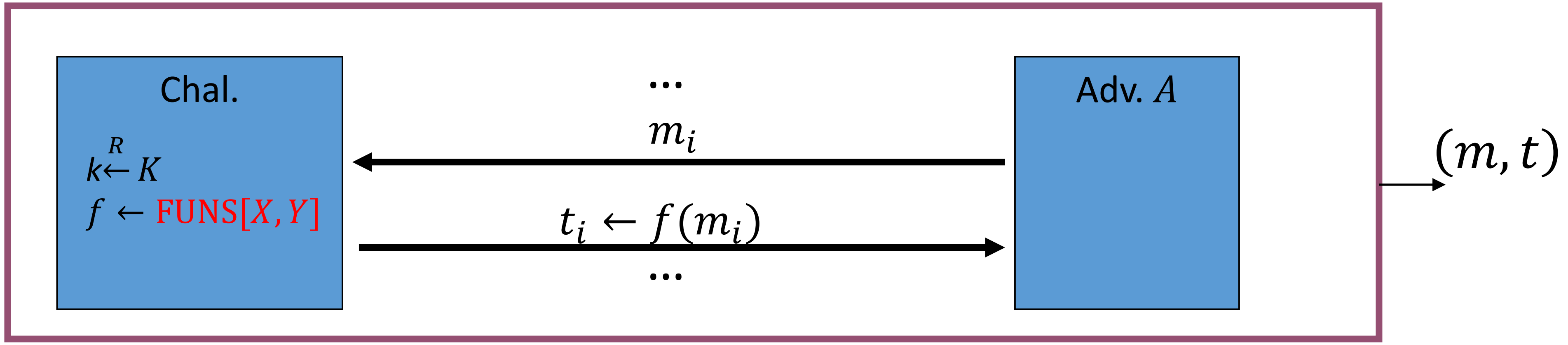


Игра 1

Модифицируем игру 0, заменив псевдослучайную функцию на случайную.

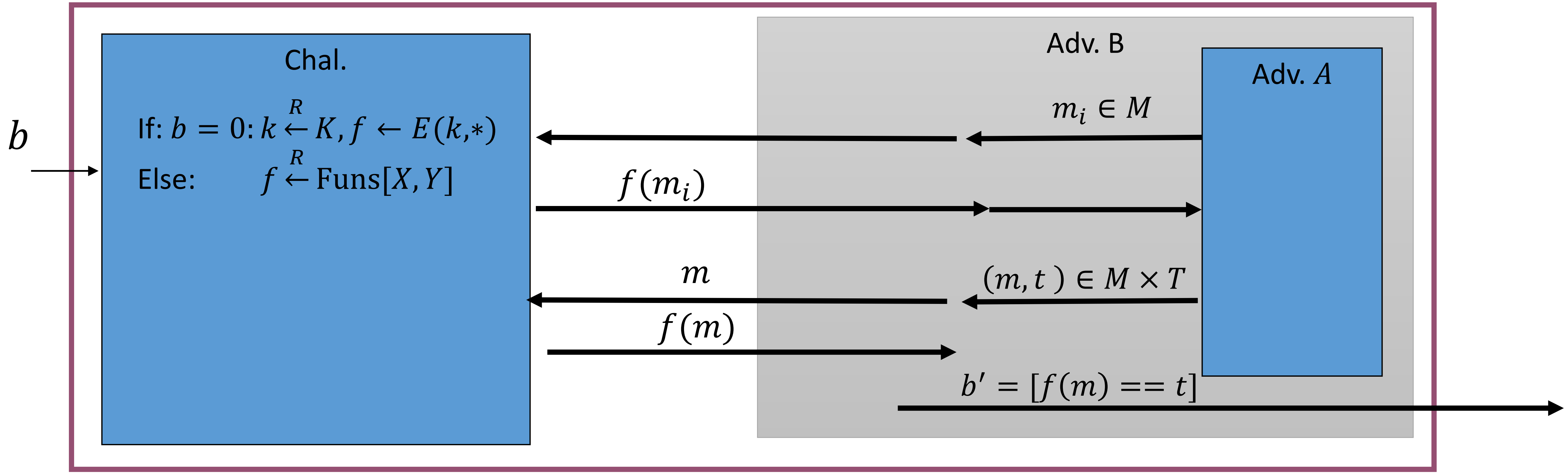
Обозначим W_1 - событие того в игре 1, что $t = f(m), m \neq \{m_1, m_2, \ldots\}$.

Очевидно, что выигрыш в такой игре есть фактически угадавание следующего значения случайной функции, что возможно с вероятность $1/|Y|$. $\Pr[W_1] \leq 1/|Y|$



Построим противника B в игре на PRF

Основная идея – если A умеет «ломать» MAC на основе PRF и не умеет на основе случайной функции, то можно понять, когда мы общались PRF, а когда со случайной функцией.



Построение MAC на основе PRF

Основная идея.

Ввели игру 0 на стойкость MAC. Обозначили вероятность победы $\Pr[W_0]$. Для любой точки $\Pr[W_1]$ верно $\Pr[W_0] \le |\Pr[W_0] - \Pr[W_1]| + \Pr[W_1]$.

Ввели игру 1, заменив PRF на случайную функцию.

Итого имеем $MAC_{adv}[A, I] = \Pr[W_0] \le |\Pr[W_0] - \Pr[W_1]| + \Pr[W_1] \le PRF_{adv}[B, F] + 1/|Y|$. Обозначили вероятность победы $\Pr[W_1]$. Замечаем, что $|\Pr[W_0] - \Pr[W_1]| = PRF_{adv}[B, F]$, так как мы смогли построить алгоритм B. Заметим также, что $\Pr[W_1] \le 1/|Y|$

Итого $MAC_{adv}[A, I] \le PRF_{adv}[B, F] + 1/|Y| \lhd$

Построение MAC на основе PRF

Любая стойкая PRF с суперполиномиальной областью значений является стойким MAC.

Проблема – рассмотренные ранее PRF имеют фиксированных вход (например размер блока в случае блочного шифра). Мы же ходим получать MAC для сообщений произвольной длины.

Хотим получить аналог «режимов шифрования» для коротких PRF, позволяющих вычислять MAC для произвольных сообщений

Беспрификсные PRF

Пусть $x = (a_1, \dots, a_s), y = (b_1, \dots, b_t)$ последовательности, $s < t$. x является полным префиксом y, если для $i = 1, \dots, s$ $a_i = b_i$.

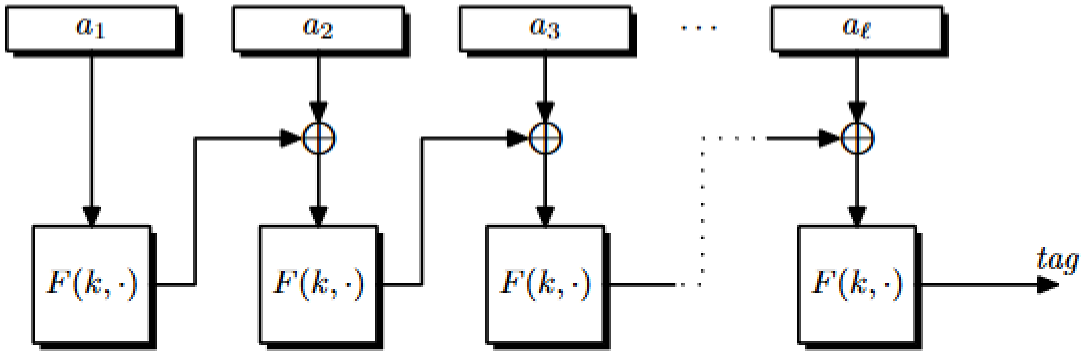
Пусть F – PRF на $(K, X^{\leq l}, Y)$. В введём беспрификсного противника в игре на PRF, отличающегося от обычного тем, что он запрашивает значения только для непустых сообщений длины не более l элементов из X, для которых ни одно из них не является полным префиксом другого.

PRF F называется стойкой беспрификсной PRF, если она стойкая против любых беспрификсных противников.

Беспрификсная стойкая PRF более слабое определение, чем стойкая PRF

Беспрификсные PRF

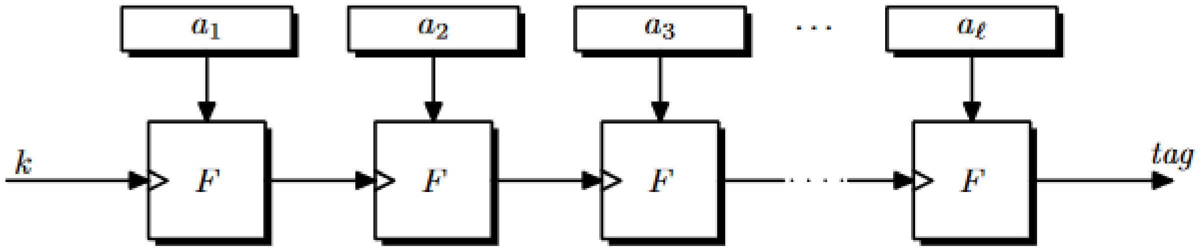
PRF $F_{CBC}(k, m)$ – цепочка CBC с использованием PRF. В качестве значение используется последний элемент цепочки.



(a) The CBC construction $F_{\text{CBC}}(k, m)$

Беспрификсные PRF

PRF $F^*(k, m)$ – каскадная конструкция. Выход каждой итерации PRF используется к качестве ключа в следующей итерации PRF.



(b) The cascade construction $F^*(k, m)$

Figure 6.3: Two prefix-free secure PRFs

Беспрификсные PRF

Теорема 9.3. Пусть F – стойкая PRF на $(K, X, X), X = \{0,1\}^n$. Для полиномиально ограниченной величины l PRF $F_{CBC}: K \times X^{\leq l} \rightarrow X$ является стойкой беспрификсной PRF, причём для любого беспрификсного противника A, делающего не более Q запросов существует противник в игре на PRF, причём

$$PRF^{pf}[A, F_{CBC}] \leq PRF_{adv}[B, F] + (Ql)^2/2|X|$$

Теорема 9.4. Пусть F – стойкая PRF на (K, X, K). Для полиномиально ограниченной величины l PRF $F^*: K \times X^{\leq l} \rightarrow K$ является стойкой беспрификсной PRF, причём для любого беспрификсного противника A, делающего не более Q запросов существует противник в игре на PRF, причём

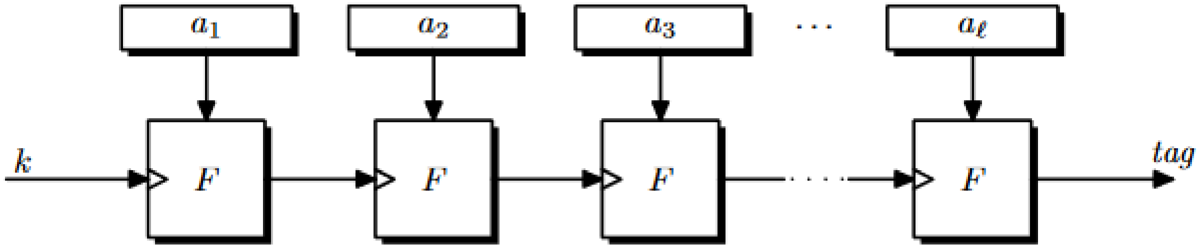
$$PRF^{pf}[A, F_{CBC}] \leq Ql * PRF_{adv}[B, F]$$

⊳ без доказательства⊲

Атака на F^* MAC

Пусть F^* MAC на основе беспрификсной PRF.

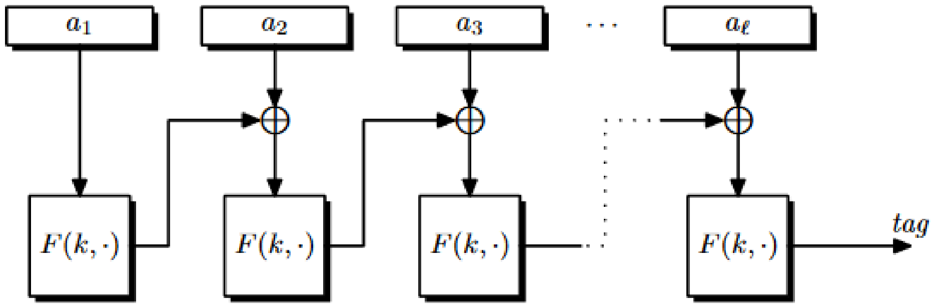
Для фиксированного сообщения $m \in X^{\leq l}$ MAC $t = F^*(k, m)$ и произвольного сообщения m' можно получить : $t' = F^*(k, m||m')$ без знания ключа, т.е. возможно осуществить атаку на MAC.



(b) The cascade construction $F^*(k, m)$

Figure 6.3: Two prefix-free secure PRFs

Атака на F_{CBC} MAC



(a) The CBC construction $F_{\text{CBC}}(k,m)$

Пусть F_{CBC} MAC на основе CBC. Построим атаку.

- Выберем произвольный $a_1 \in X$
- Запросим MAC t для сообщения a_1
- Вычислим $a_2 = a_1 \oplus t$. Тогда пара t является корректным MAC для сообщения (a_1, a_2)

$$t = F(k, a_1), a_1 = F(k, a_1) \oplus a_2$$
$$F_{CBC}\big(k, (a_1, a_2)\big) = F(k, F(k, a_1) \oplus a_2) = F(k, a_1) = t$$

Построение МАС

Стойкие МАС можно построить на основе беспрификсных PRF (сл лекция), но использование беспрификсных PRF в качестве МАС даёт нестойкие конструкции.