Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 4 - Одноразовый ключ и многоразовый ключ

Псевдослучайная функция и псевдослучайная перестановка

Опр.

$Perms(X)$ - множество всех обратимых функций (перестановок) $X \to X$

Опр.

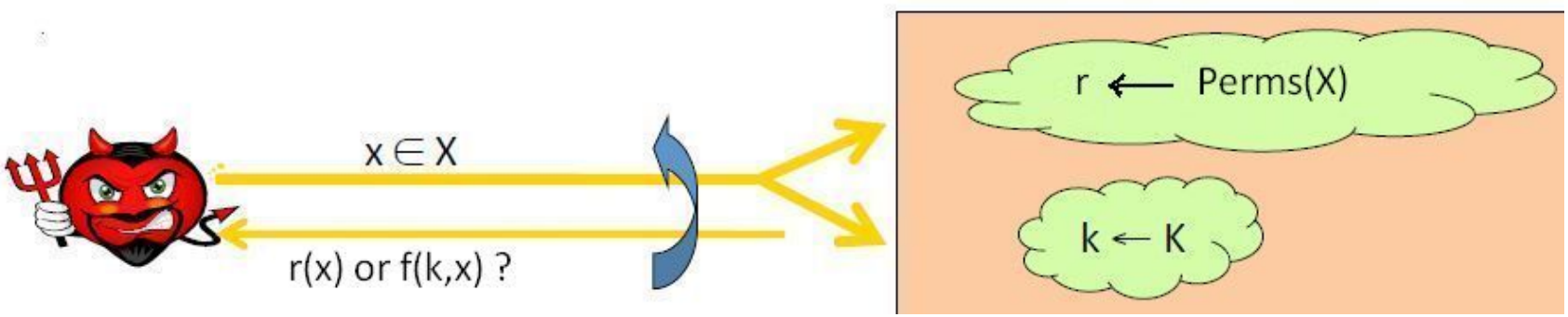
Функция $f : K \times X \to X$ - это *псевдослучайная перестановка*, если

$\forall k\ f(k, \cdot) \in Perms(X)$, $f \in \mathrm{PT}$, $f^{-1}(k, \cdot) \in \mathrm{PT}$,

$\forall$ оракула $A \in \mathrm{PPT}$ при $k \xleftarrow{R} K$, $r \xleftarrow{R} Perms(X)$

величина

$Adv(A, F) = |P[A(f(k, \cdot)) = 1] - P[A(r(\cdot)) = 1]| < \varepsilon(n)$,



ПСП всегда “эффективно” обратима, ПСФ - не обязательно обратима.
Для маленького множества X ПСФ просто отличить от ПСП, пример:
$X \to X$, $X = \{0, 1\}$.

Если множество X большое, нельзя эффективно отличить ПСП от ПСФ.

Лемма (О переключении)

Пусть f - ПСП на $K \times X \to X$. Тогда
$\forall$ алгоритма $A \in \mathrm{PPT}$, который вычисляет функцию в q точках, верно

$$|Adv_{PRF}(A, f) - Adv_{PRP}(A, f)| < q^2 / (2|X|)$$

Док-во: рассказать по [1]. (Чуть проще, чем там.)

$q = poly(n)$, $|X| = 2^n = exp(n)$.

Зачем это все нужно?

Если блочный шифр - ПСП,
тогда можно формально обосновать криптостойкость блочного шифра.

Если шифр - ПСП, по лемме он - ПСФ.

На основе ПСФ можно строить криптостойкий ГПСЧ. (Один из способов.)

Раздел 4 - Одноразовый ключ и многоразовый ключ

До сих пор шифровали один блок длины n бит. Перейдем к сообщению произвольной длины.

Модель:

- одноразовый ключ
- сообщение длиной более одного блока
- злоум-к может: видит только шифротекст
- цель злоум-ка: по шифротексту получить информацию о сообщении

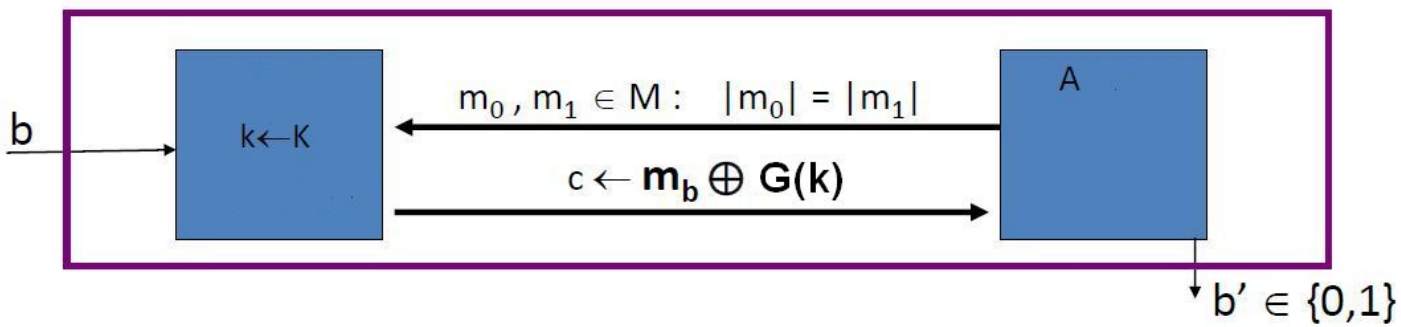
Режим электронной кодовой книги - ECB

Опр.

Режим работы блочного шифра, когда к каждому блоку применяется одна и та же детерминированная перестановка $E(k, \cdot)$, называется Электронная кодовая книга - Electronic codebook, ECB.

Эксперимент SS для одноразового ключа (повтор):

1. Система выбирает случайное значение бита $b \xleftarrow{R} \{0,1\}$. Оно секретное.
2. Злоумышленник выбирает длину n и отправляет два сообщения $m_0 \neq m_1$ длины n.
3. Система вычисляет $c = E(k, m_b)$ и отправляет его злоум-ку.
4. Злоум-к $A \in \mathrm{PPT}$ анализирует c и выдает результат - бит b'.
5. Если $b' = b$, A достиг успеха.



Один запрос, ответ.

Опр.

Шифр наз. *семантически стойким для одноразового ключа*, если в этом эксперименте вероятность успеха A не более $\frac{1}{2} + \varepsilon(n)$,
где $\varepsilon(n)$ - пренебр. малая,
вероятность вычисляется по случайным выборам: k, b, алгоритма A и шифрования E.

Эквивалентно:
$Adv_{SS}(A, E_{OTK}) = \left|P(b' = 1|b = 1) - P(b' = 1|b = 0)\right| < \varepsilon(n)$.

Задача

Доказать, что режим ECB не семантически стойкий.
Использовать сообщение длиной два блока, эти блоки - одинаковые.

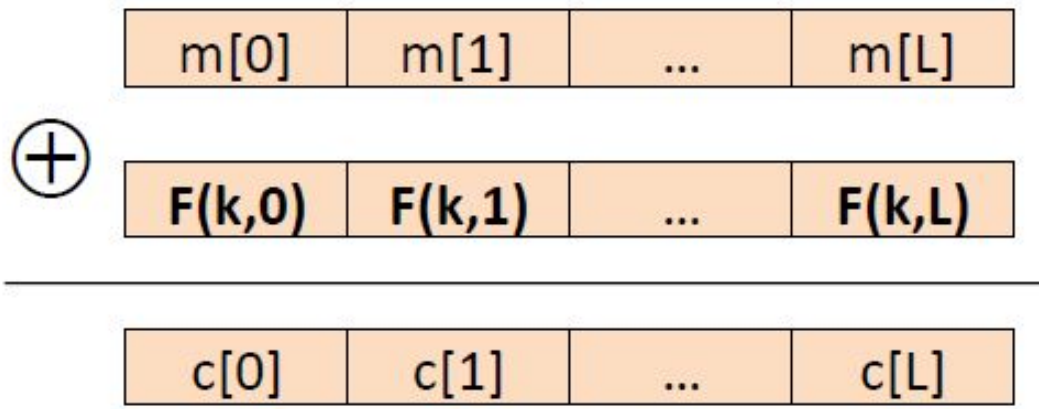
Режим счетчика без сцепления блоков - DetCTR

Deterministic counter mode.

Опр.

Пусть $f : K \times \{0,1\}^n \to \{0,1\}^n$ - ПСФ. Тогда i-й блок:
$E_{DetCtr}(k,m)[i] = m[i] \oplus f(k,i)$

$E_{DETCTR}(k, m) =$



Когда блочный шифр исп. как поточный, это наз. режимом *гаммирования*.

Утверждение

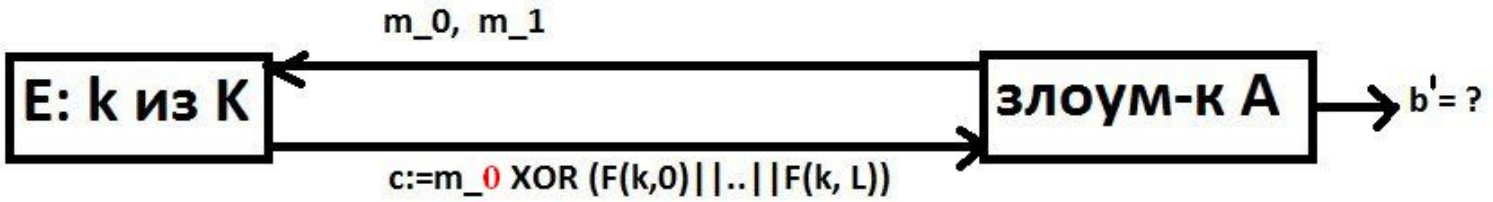
Пусть $f : K \times \{0,1\}^n \to \{0,1\}^n$ - ПСФ. Тогда $\forall L > 0$
при одноразовом ключе E_{DetCtr} - семант. стойкий шифр:
$K \times \{0,1\}^{nL} \to \{0,1\}^{nL}$.

В частности, $\forall$ алгоритма $A \in \mathrm{PPT}$, реализ. атаку на E_{DetCtr},
сущ. алгоритм $B \in \mathrm{PPT}$, осущ. атаку на ПСФ F:

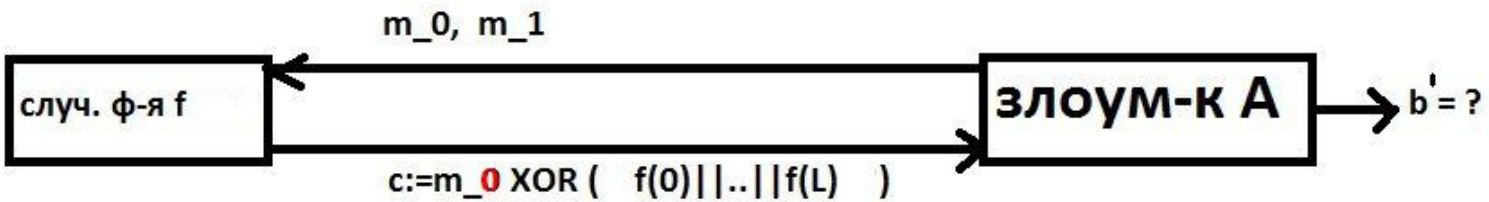
$$Adv_{SS}[A, E_{DetCtr}] \leq 2 \cdot Adv_{SS}[B, F]$$

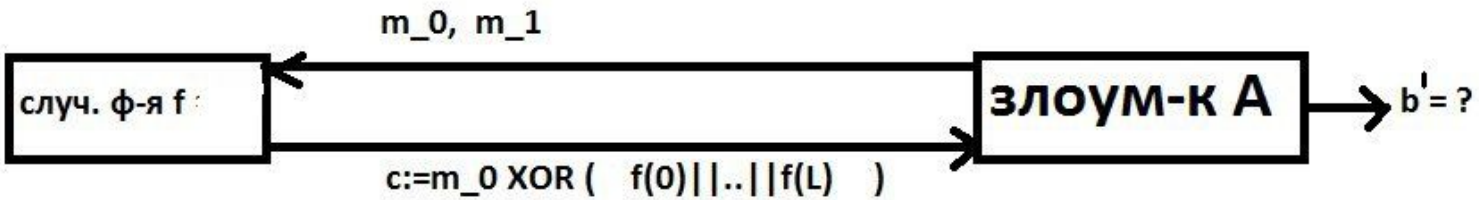
Док-во

Аналогично теореме 2 о семантической стойкости поточного шифра.

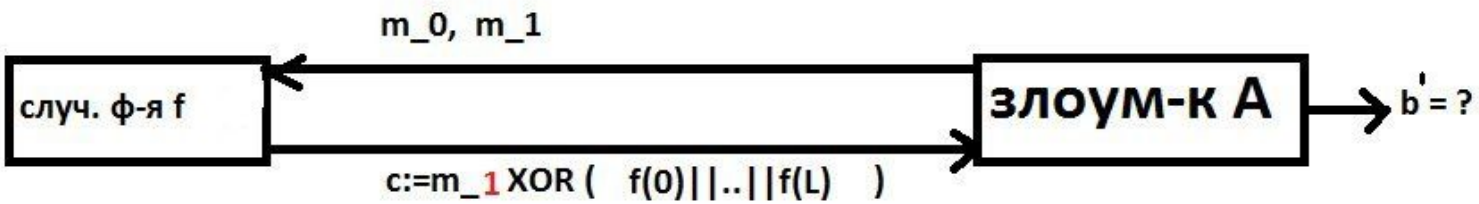


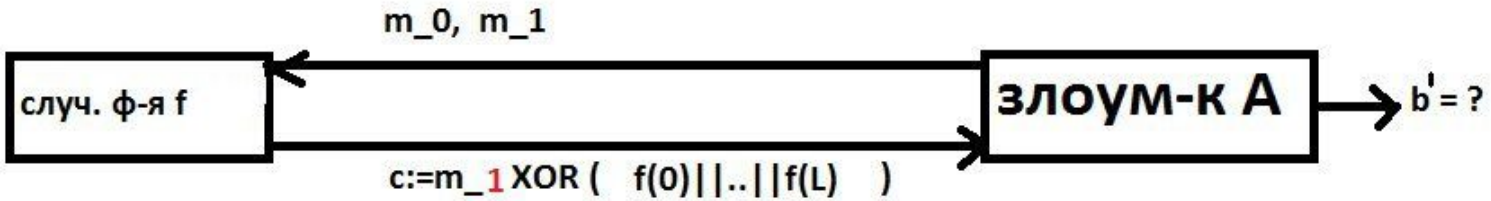
F - стойкая ПСФ, не отличима от случайно выбранной функции f



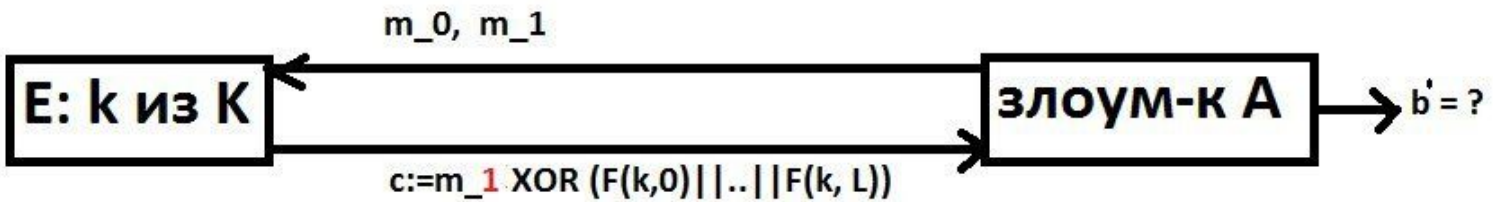


Одноразовый блокнот - абсолютно стойкий шифр





F - стойкая ПСФ, не отличима от случайно выбранной функции f



Для первого перехода вероятность отличить “верх” от “низа”: $\left|P(b' = 1|b = 0,\ E) - P(b' = 1|b = 0,\ OTP)\right| = Adv_{SS}[B, F] < \varepsilon(n)$

Для второго - отличить нельзя.

Для третьего: $\left|P(b' = 1|b = 1,\ E) - P(b' = 1|b = 1,\ OTP)\right| = Adv_{SS}[B, F] < \varepsilon(n)$

Поэтому $Adv_{SS}[A, E_{DetCtr}] \leq Adv_{SS}[B, F] + 0 + Adv_{SS}[B, F] = 2 \cdot Adv_{SS}[B, F]$.

Ч.т.д.

Раздел 4 - Одноразовый ключ и многоразовый ключ

Режимы использования, стойкие при многократном использовании ключа.

Злоум-к видит много шифротекстов, зашифрованных одним и тем же ключом.

Модель:

- Возможности злоум-ка: может получать шифротексты для любых сообщений, при этом ключ шифра один и тот же. Т.е. **атака с выбором открытого текста**, chosen plaintext attack.
- Цель злоум-ка: нарушить семантическую стойкость.

Далее всегда подразумевается, что ключ многоразовый.

Эксперимент “атака с выбором открытого текста” при многоразовом ключе:

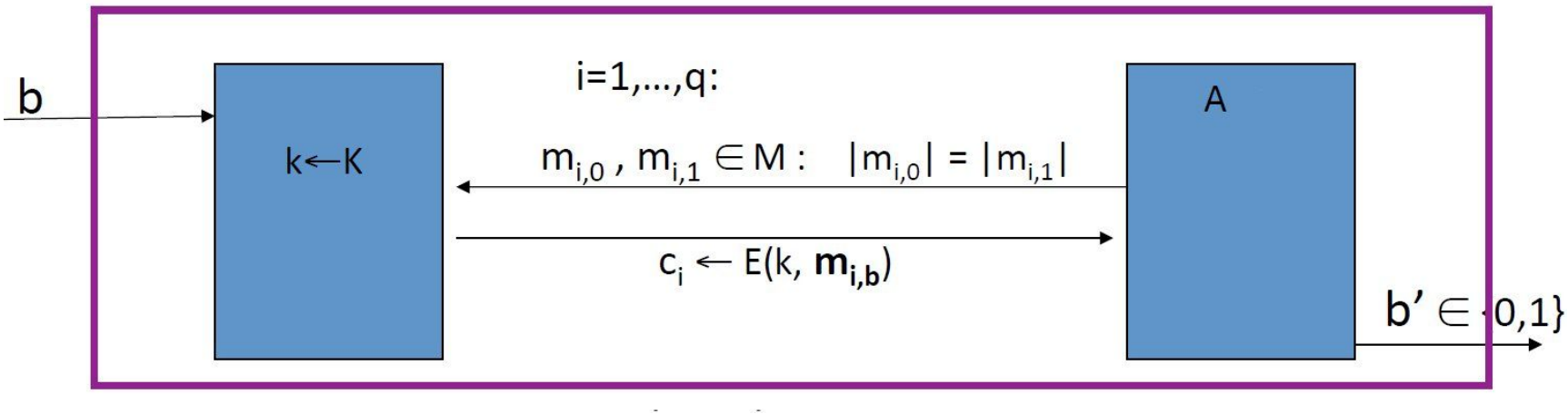
Пусть (E, D) - шифр.

1. Система выбирает ключ k и значение бита b, секр., фикс.
2. $q \in \mathbb{N}$ - число запросов злоумышленника.

$q = poly(log(|\{m\}|))$.

Каждый раз он отправляет $m_{i,0}, m_{i,1}$: $len(m_{i,0}) = len(m_{i,1})$.

3. Система вычисляет $c_i = E(k, m_{i,b})$, отправляет злоум-ку.
4. После q запросов злоум-к выдает b' - гипотезу о b.



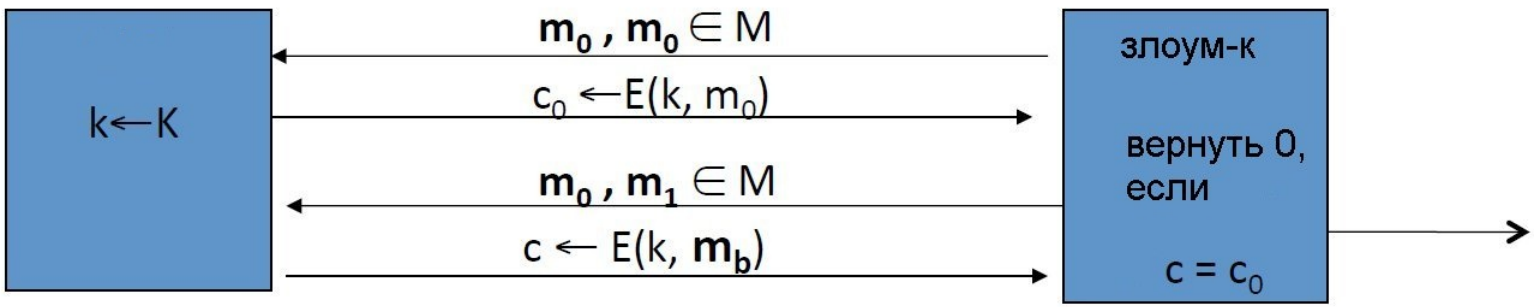
Сообщения могут повторяться.

Опр.

шифр $C = (E, D)$ наз. *семантически стойким к атаке с выбранным открытым текстом при многоразовом ключе*, если в этом эксперименте $\forall A \in \mathrm{PPT}$

$$Adv_{CPA}(A, C) := \left| P(b' = 1 | b = 0) - P(b' = 1 | b = 1) \right| < \varepsilon(n)$$

Если шифрование детерминированное,
простая атака нарушает сем. стойкость:



Решения:

1.**Рандомизированный алгоритм шифрования:**

$E_r(k, m) = c_1$, повторно $E_r(k, m) = c_2$, с высокой вероятностью $c_1 \neq c_2$.
D - детерминированный алгоритм!

Длина шифротекста больше длины сообщения.

(Рисунок: $m \to \{c_1, ..., c_t\} \to m$)

Пример реализации:

Пусть $f : K \times R \to M$ - ПСФ.
R - конечное множество чисел или других параметров.
Пусть $E(k, m) = [r \xleftarrow{R} R,$ вернуть $(r, f(k, r) \oplus m)]$

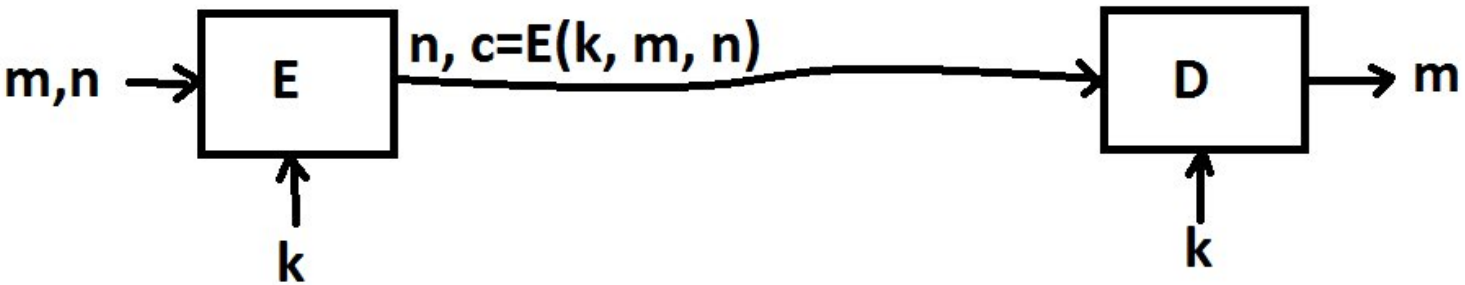
Задача

В каком случае этот шифр семант. стойкий относительно атаки с выбранным открытым текстом?

Подсказка: $f(k, \cdot) \approx$ случайная $g(\cdot)$.

2. Использование nonce

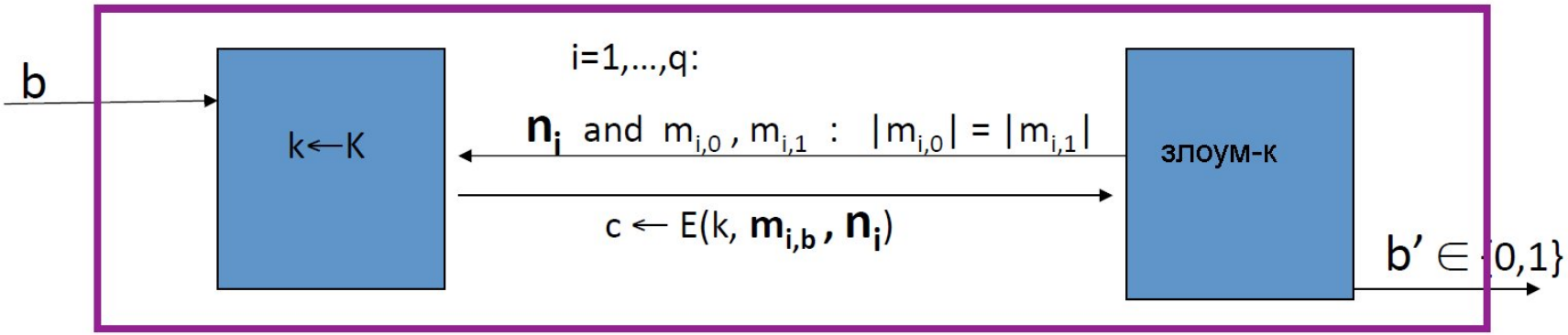
nonce - уникальное значение, “n used once”. Пара (n, m) никогда не повторится.



nonce:

- случайное число, выбир. из большого множества, так что оно никогда не повторится с большой вероятностью.
- счетчик (энегронезавис. память, можно не передавать nonce)

Эксперимент nCPA:



Все nonce n_i попарно различны, хоть их и выбирает злоум-к.

Опр.

шифр $C = (E, D)$, исп. nonce, семантически стойкий к атаке с выбранным открытым текстом, если $\forall A \in \mathrm{PPT}$
$Adv_{nCPA}[A, C] = \left|P(b' = 1|b = 0) - P(b' = 1|b = 1)\right| < \varepsilon(n)$.

Пример реализации:

Пусть $f : K \times R \to M$ - ПСФ.
R - конечное множество чисел.
Пусть $E(k, m) = [++ r,$ вернуть $(r, f(k, r) \oplus m)]$

Задача

В каком случае этот шифр семант. стойкий относительно атаки с выбранным открытым текстом?

Некоторые итоги:

A. Стойкость шифров с одноразовым ключом:
A.1. Абсолютная стойкость к атаке с известным шифротекстом.
A.2. Семант. стойкость к атаке с известным шифротекстом.

B. Стойкость шифров с многоразовым ключом:
B.1. Семант. стойкость к атаке с выбором открытого текста.

C. Шифры:
C.1. Алфавитные.
C.2. Одноразовый блокнот.
C.3. Поточные шифры, ГПСЧ.
C.4. Блочные шифры. Шифр DES и его анализ.

D. Режимы использования блочных шифров:
D.1. ECB.
D.2. DetCTR.
D.3. Начали рассматривать использование многоразового ключа.

Литература к лекции:

1. D.Chang, M.Nandi, *A short proof of the PRP/PRF Switching Lemma*, `https://eprint.iacr.org/2008/078.ps`