

# Прикладная Криптография:

## Симметричные

## крипtosистемы

# Аутентифицированное

## шифрование

Макаров Артём

МИФИ 2025

# Тест.

1 вопрос.

- Положить телефон экраном вниз справа от себя
- Не разговаривать с соседями
- Не пользоваться конспектами и электронными устройствами
- Написать номер (по таблице) и ФИО на листочке
- Написать краткий ответ на вопрос
- Дождаться окончания теста

Тест.

4 модели криптографических хэш-функций. Их взаимосвязь.

TIME IS  
UP

# Криптографическая защита информации

## Обеспечение конфиденциальности

- семантическая стойкость против CPA атаки
- Защита только против пассивных противников (не вносящих изменения в канал связи)
- Поточные и блочные шифры

## Обеспечение целостности

- Защита от подделки при атаке по выбранным сообщениям
- CBC-MAC, HMAC, CMAC

# Криптографическая защита информации

## Аутентифицированное шифрование

- Шифрование с защитой от подделки шифртекстов (т.е. обеспечение аутентичности и конфиденциальности)
- Защита от активных и пассивных противников

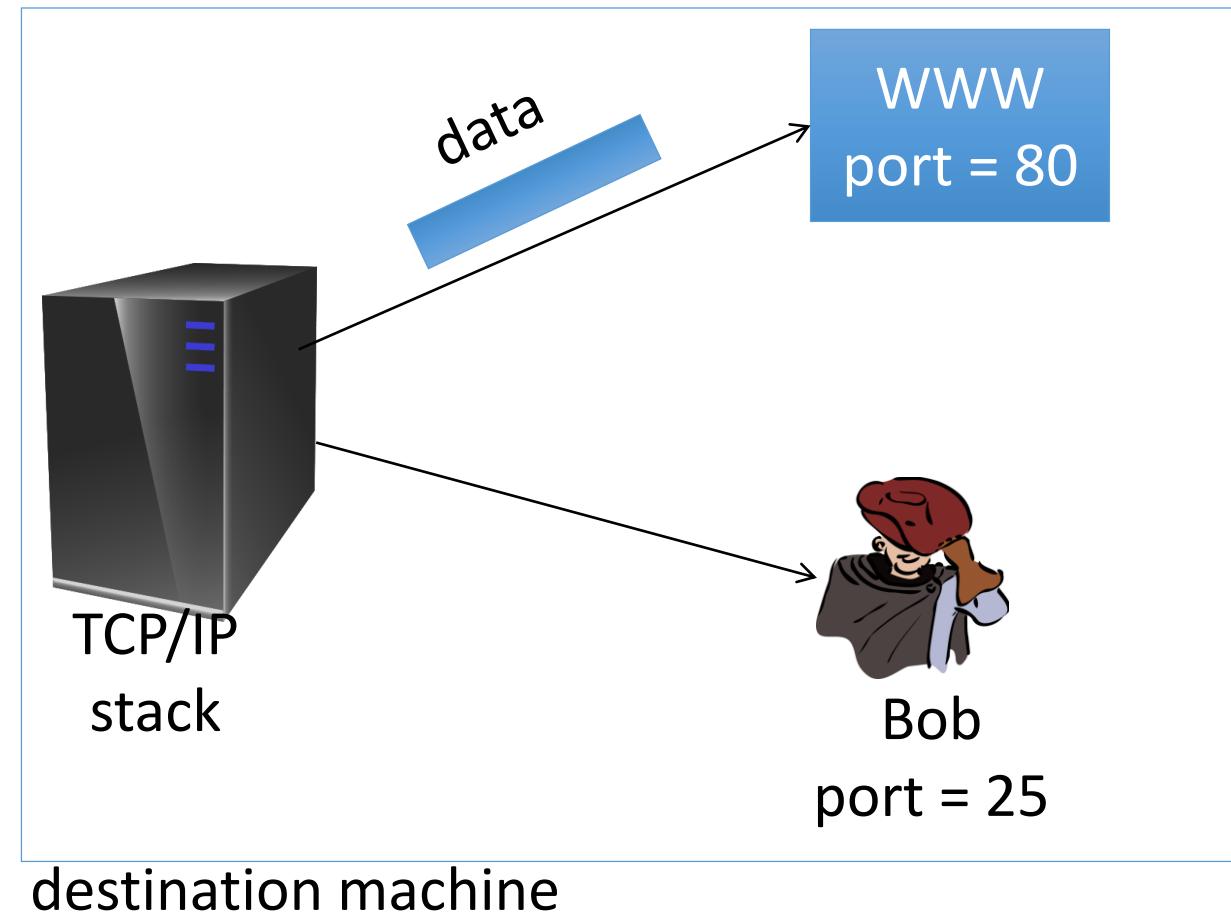
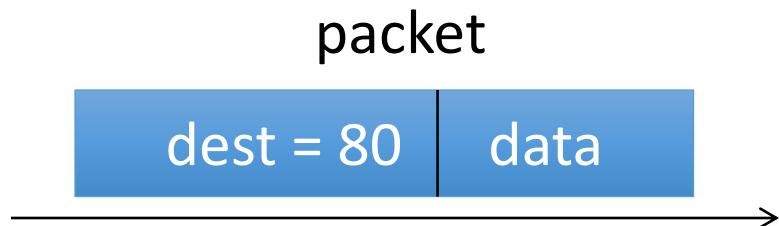
# Пример перехвата сообщений

TCP/IP: (highly abstracted)



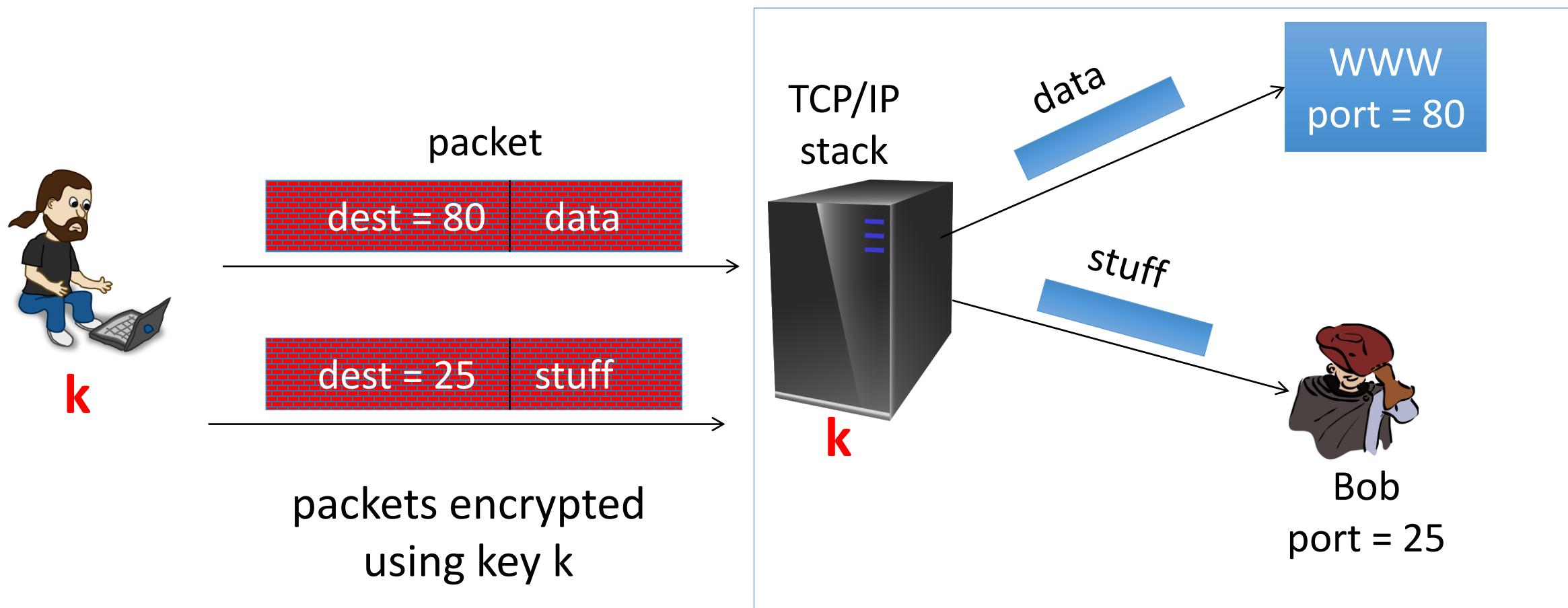
source machine

Противник получает любые  
пакеты, имеющие заголовок  
“dest=25”

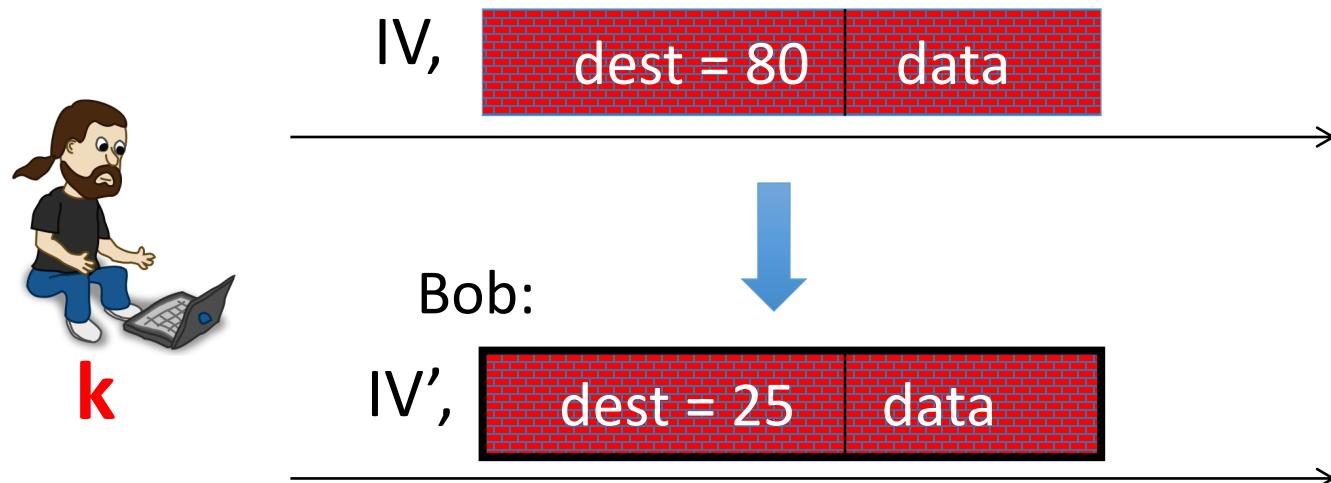


# Пример перехвата сообщений

IPsec: (highly abstracted)

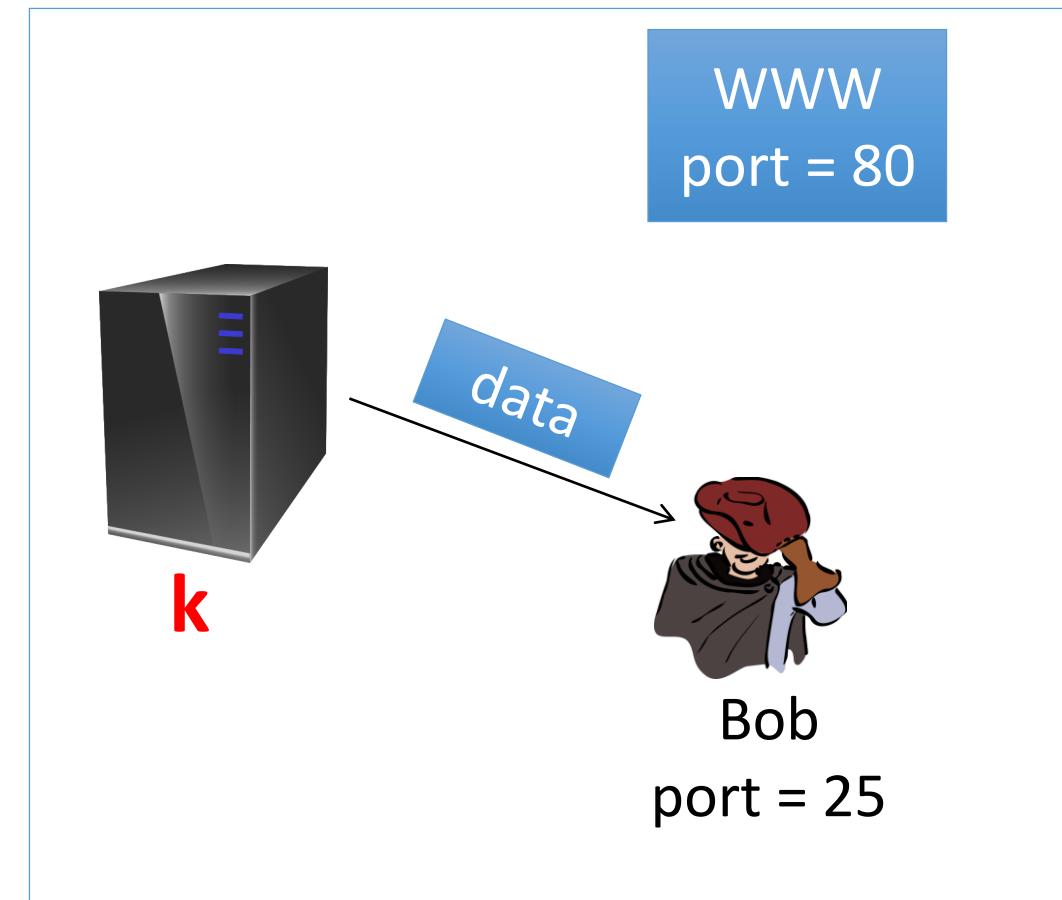


# Пример перехвата сообщений



Easy to do for CBC with rand. IV

(only IV is changed)



# Выводы

CPA стойкость не гарантирует стойкость против активных противников

Для обеспечения безопасности:

- Если необходимо обеспечить целостность, но не конфиденциальность  
- нужно использовать MAC
- Если необходимо обеспечить конфиденциальность и целостность –  
использовать аутентифицированное шифрование

# Аутентифицированное шифрование

Введём понятие аутентифицированного шифра.

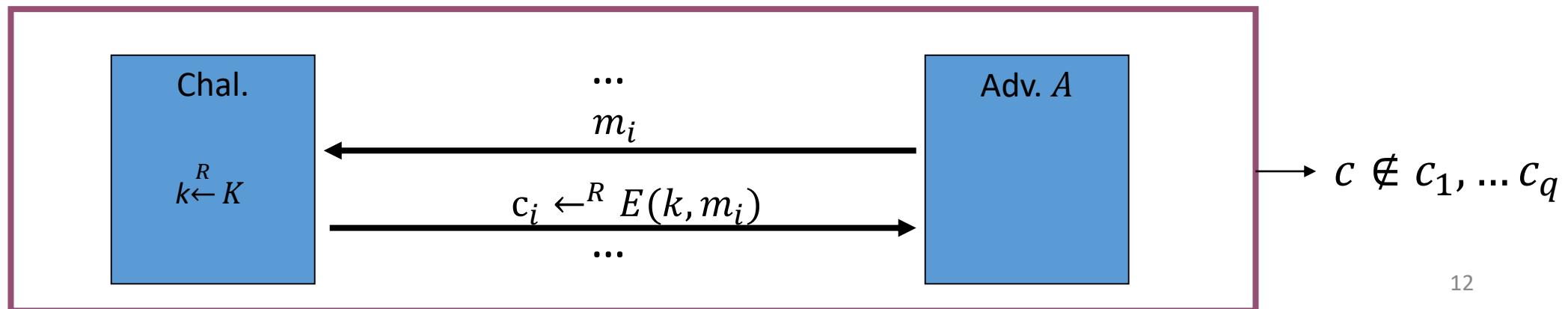
$E = (E, D)$  аутентифицированный шифр на  $(K, M, C)$ .

- $E: K \times M \rightarrow C$
- $D: K \times C \rightarrow M \cup \{\perp\}$
- $\perp$  - шифртекст отклонён (не пройдена проверка аутентичности)
- Свойство корректности:  $D(k, E(k, m)) = m$

# Целостность шифртекстов

Пусть  $E = (E, D)$  – **аутентифицированный шифр (AE)** на  $(K, M, C)$ . Введём игру на **целостность шифртекстов (INT-CTXT)** (аналогично игре на MAC):

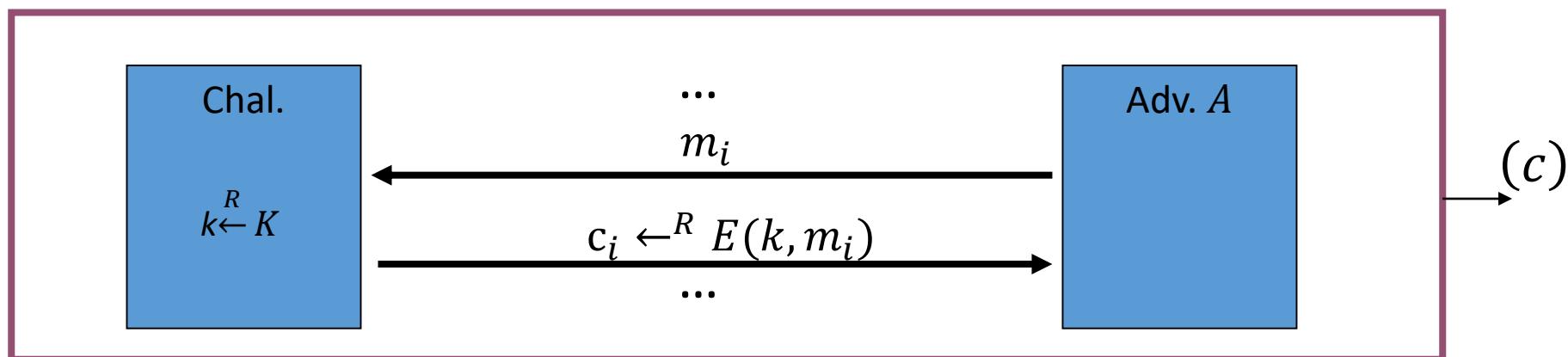
- Претендент выбирает случайный ключ
- Противник запрашивает зашифрование нескольких открытых текстов в адаптивной атаке
- Цель противника – получить **новый корректный шифртекст**



# Целостность шифртекстов

Преимущество противника  $CI_{adv}[A, E] = \Pr[D(k, c) \neq \perp]$

Шифр Е является **шифром обеспечивающим целостность шифртекстов**, если  $\forall A \ CI_{adv}[A, E] \leq \epsilon$ , где  $\epsilon$  – пренебрежимо малая величина.

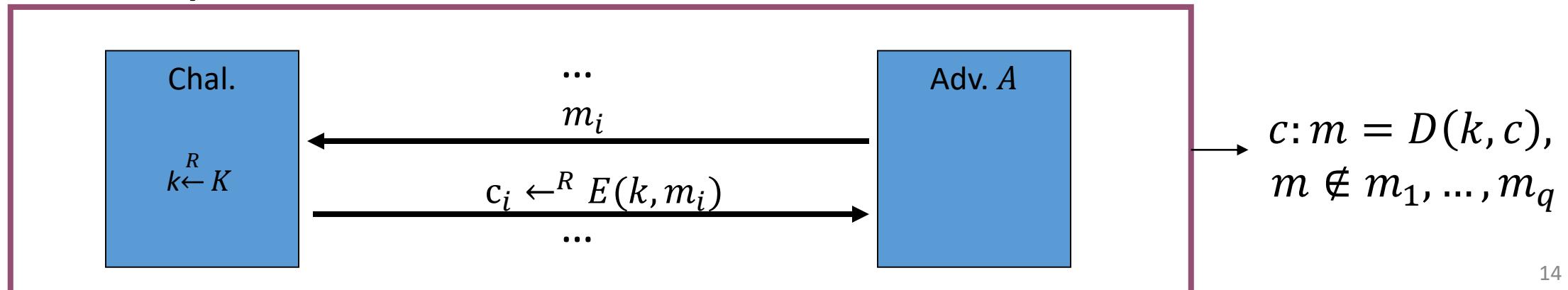


# Целостность открытых текстов

Пусть  $E = (E, D)$  – **аутентифицированный шифр (AE)** на  $(K, M, C)$ .

Введём игру на **целостность открытых текстов (INT-PTXT)**

- Претендент выбирает случайный ключ
- Противник запрашивает зашифрование нескольких открытых текстов в аддитивной атаке
- Цель противника – получить **корректный шифртекст для нового сообщения**



# Целостность открытых текстов

Преимущество противника  $PI_{adv}[A, E] = \Pr[D(k, c) \neq \perp]$

Шифр Е является **шифром обеспечивающим целостность открытых текстов**, если  $\forall A PI_{adv}[A, E] \leq \epsilon$ , где  $\epsilon$  – пренебрежимо малая величина.

# CA и CI стойкость

- CI более сильное понятие стойкости
- CI стойкость говорит, что сложно навязать новый шифртекст получателю
- PI стойкость говорит, что сложно навязать новые расшифрованные данные получателю
- Возможно существование шифра PI стойкого, но не CI стойкого

Например – пусть шифр недетерминированный. Тогда одному РТ соответствует множество СТ. Если противник может создавать **новые СТ для существующих сообщений, но не может для новых** то он PI, но не CI стойкий.

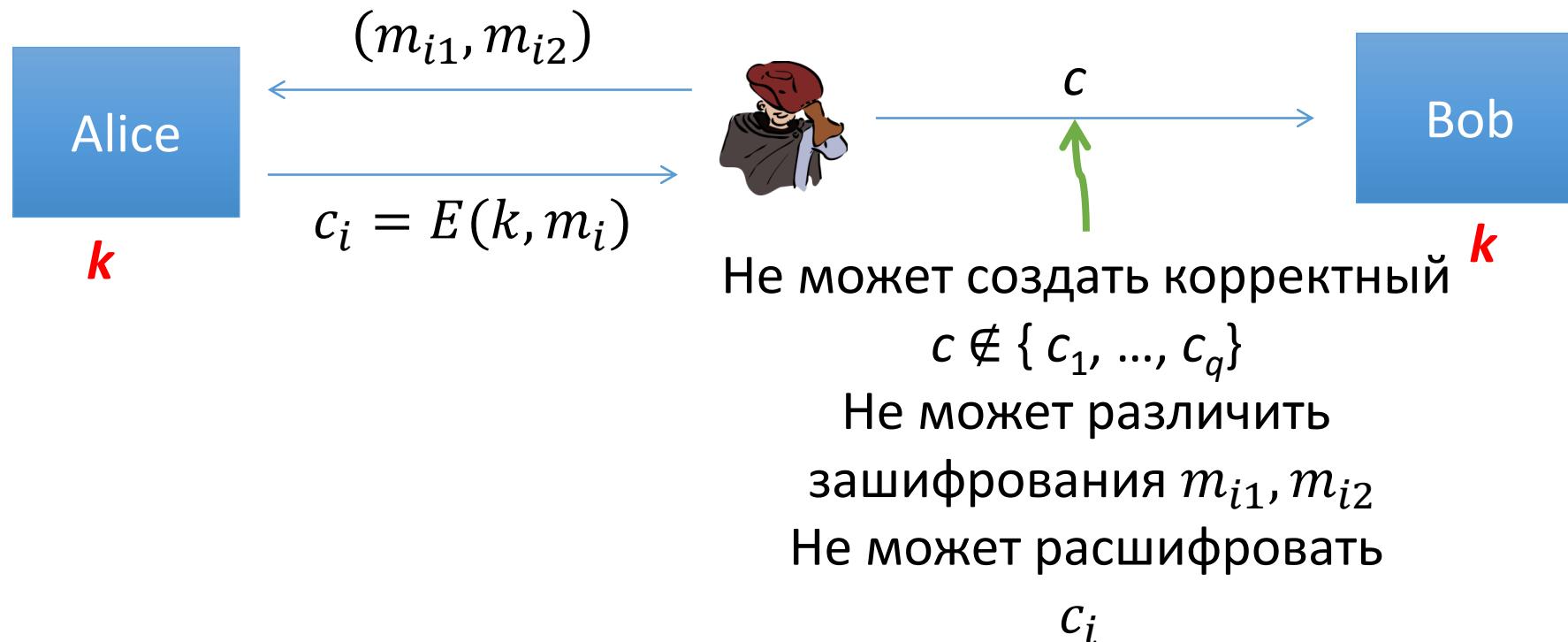
# Аутентифицированное шифрование

Стойкость:

- **Семантическая стойкость против CPA**
- **Целостность шифртекстов (CI)** (противник не может получить корректный шифртекст)

# Следствия аутентифицированного шифрования

- Пассивный противник не может расшифровать сообщения
- Активный противник не может вставлять или изменять сообщения в канале
- Целостность шифртекстов обеспечивает целостность открытых текстов



# Пример

Пусть Alice отправляет сообщение Bob. Для простоты рассмотрим email с фиксированным заголовком “To:”. (пример – To:Bob@SecretNet.gov)

Сообщения зашифровываются в сторону почтового сервера, расшифровываются им, и отправляются нужному адресату.

Идея атаки – модифицировать сообщения сервера так, чтобы адресатом выступал адрес противника.

# Пример

Для реализации атаки необходимо решить следующую задачу – имея шифртекст  $c$  некоторого сообщения  $(u||m)$  найти шифртекст  $c'$  для сообщения  $(v||m)$ .

Даная задача может быть легко решена для CPA стойких шифров

- Рандомизированный CTR:  $c'[1] = c[1] \oplus u \oplus v$
- Рандомизированный CBC:  $c'[0] = c[0] \oplus u \oplus v$

Т.е. если противник может расшифровывать шифртексты, CPA стойкости недостаточно

# CCA

Данная задача является частным случает атаки по выбранным шифртекстам

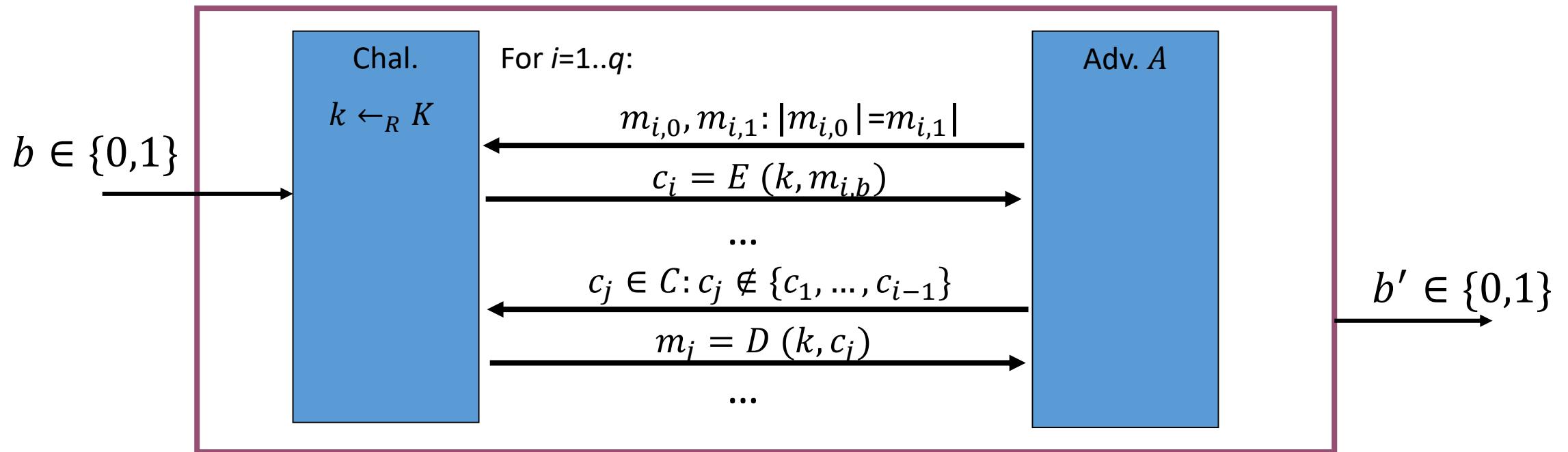
Для АЕ шифров данная атака невозможна, т.к. шифр гарантирует невозможность получения корректного шифртекста  $c'$  без знания секретного ключа.

# CCA

Пусть  $E = (E, D)$  – шифр на  $(K, M, C)$ . Рассмотрим игру

- Претендент выбирает случайный ключ
- Противник может запрашивать зашифрование произвольных сообщений
- Противник может запрашивать расшифрования произвольных шифртекстов
- Цель противника – атака на семантическую стойкость

# CCA



# CCA стойкость

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

Введём преимущество  $CCA_{adv}[A, E] = |\Pr[W_0] - \Pr[W_1]|$

Шифр Е называется **стойким CCA шифром** (стойким к атаке по выбранным шифртекстам, стойким к атаке по выбранным шифртекстам и соответствующим им открытым текстам, Chosen Ciphertext Attack) если  $\forall A: CCA_{adv}[A, E] \leq \epsilon$ , где  $\epsilon$  – пренебрежимо малая величина

Более сильное определение, чем CPA стойкость

# Аутентифицированное шифрование и CCA стойкость

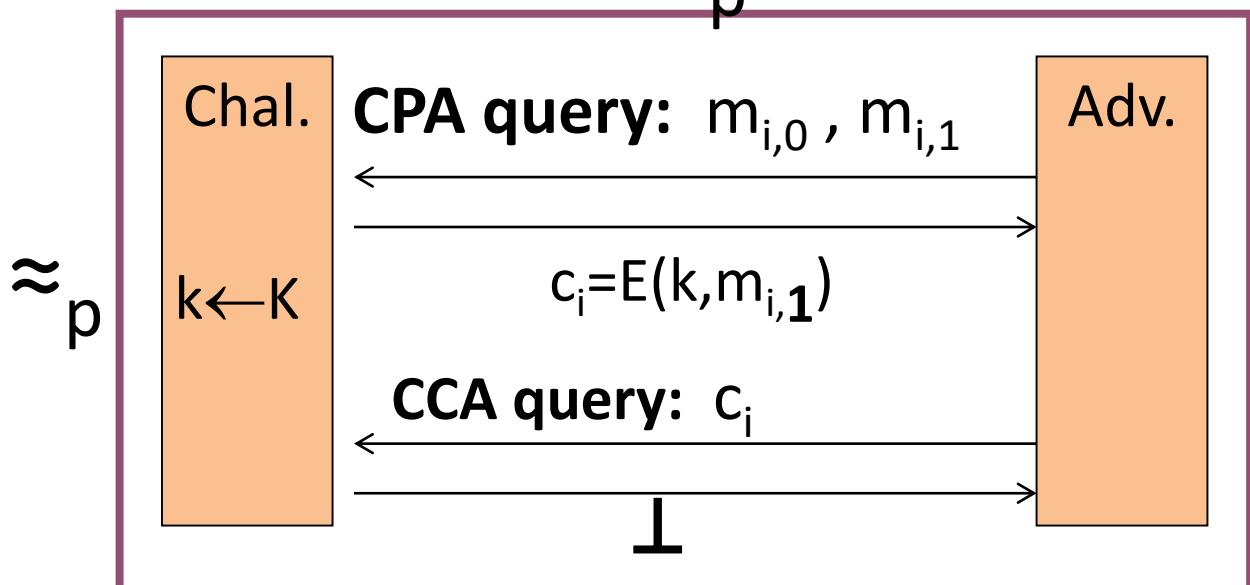
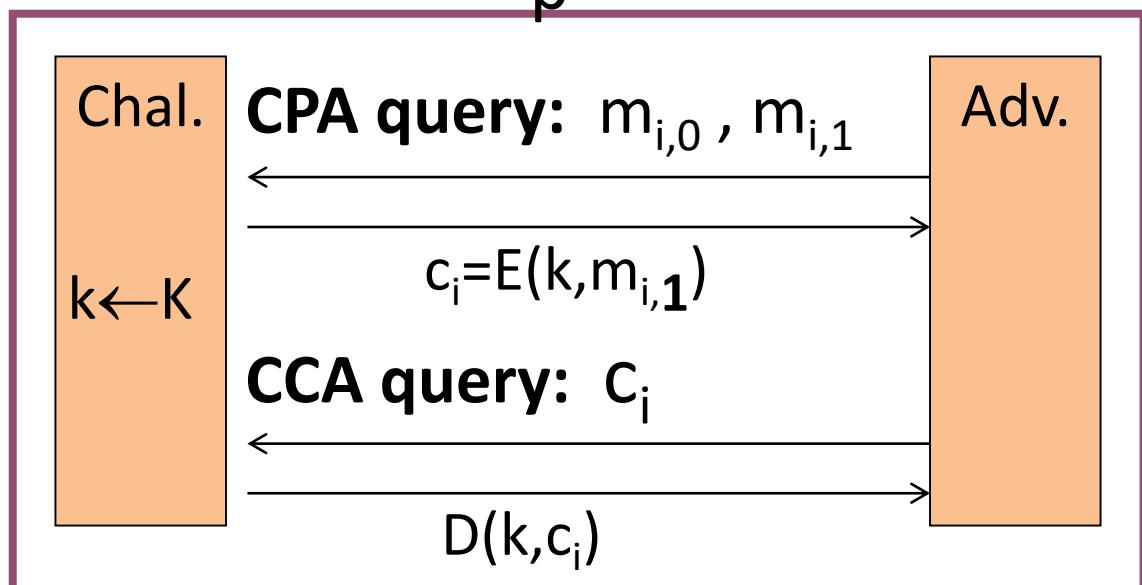
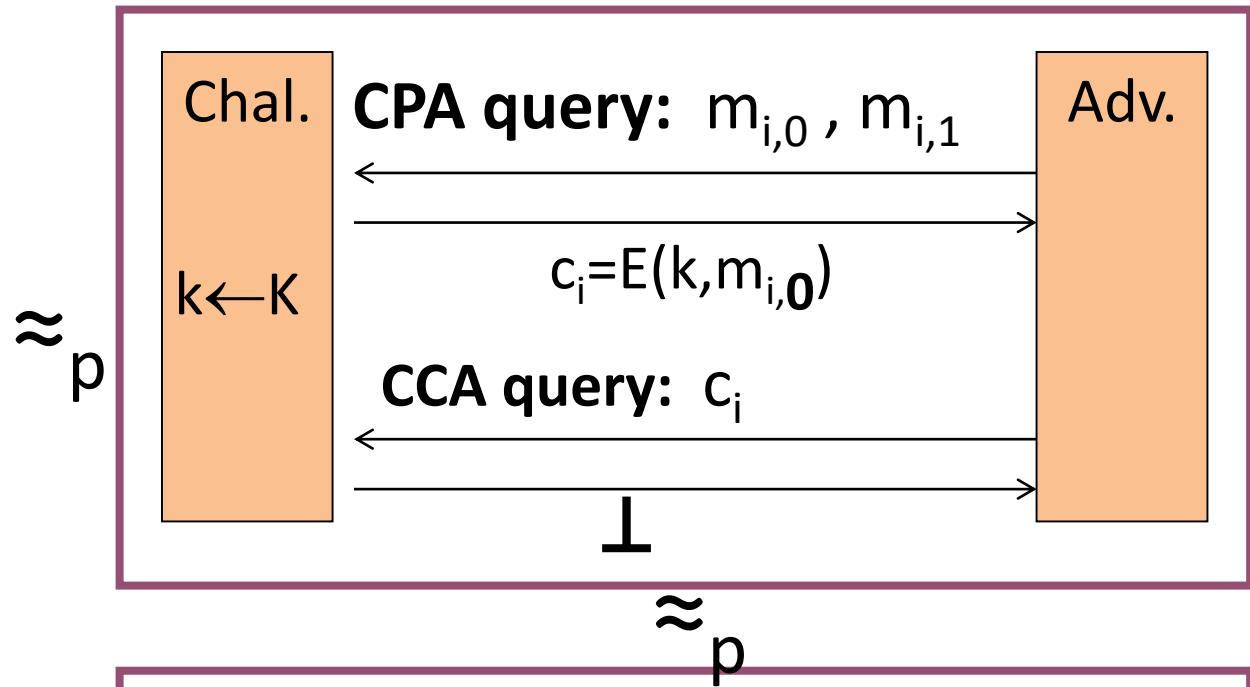
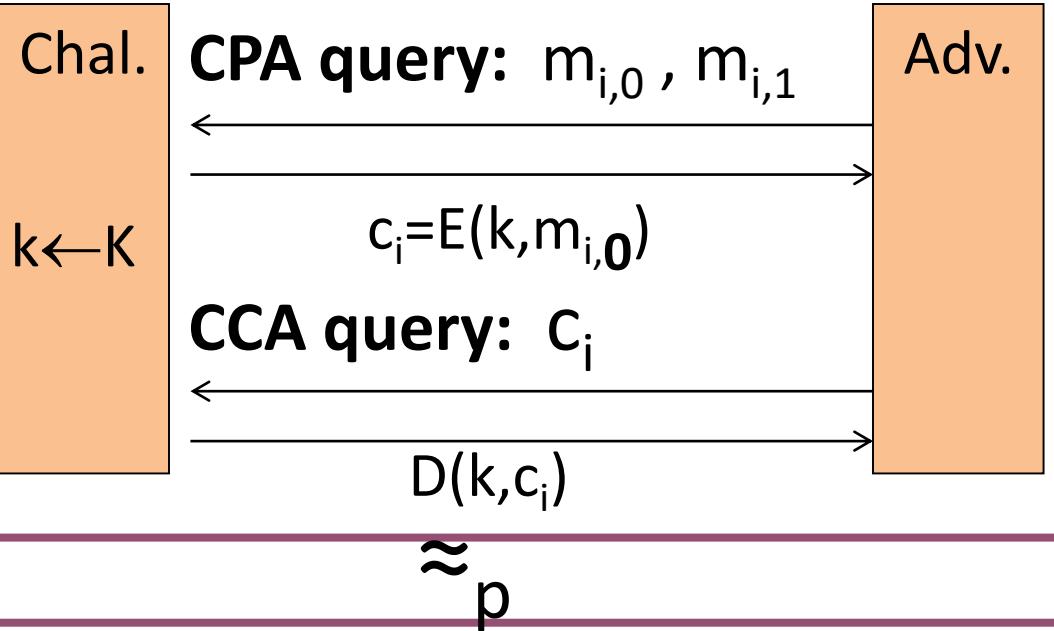
**Теорема 12.1.** Пусть  $E = (E, D)$  – шифр. Если он АЕ стойкий, то он ССА стойкий, причём

$\forall A$  в игре на ССА против  $E$ , делающего не более  $Q_e$  запросов на шифрование и не более  $Q_b$  запросов на расшифрование существует противник  $B_{cpa}$  в игре на CPA и  $B_{CI}$  в игре на целостность шифртекстов, делающих не более  $Q_e$  запросов:

$$CCA_{adv}[A, E] \leq CPA_{adv}[B_{cpa}, E] + 2Q_d CI_{adv}[B_{CI}, E]$$

▷ без доказательства ◁

# Proof by pictures



# Аутентифицированное шифрование и CCA стойкость

**Теорема 12.2.** Пусть  $E = (E, D)$  – шифр. Если он CCA стойкий и обеспечивает целостность открытых текстов, то он AE стойкий

▷ без доказательства ◁

Т.е. AE стойкость  $\Leftrightarrow$  CPA + CI (целостность CT)  $\Rightarrow$  CCA стойкость

CCA стойкость + PI (целостность PT)  $\Rightarrow$  AE стойкость

CCA стойкость  $\Rightarrow$  CPA стойкость

CI  $\Rightarrow$  PI

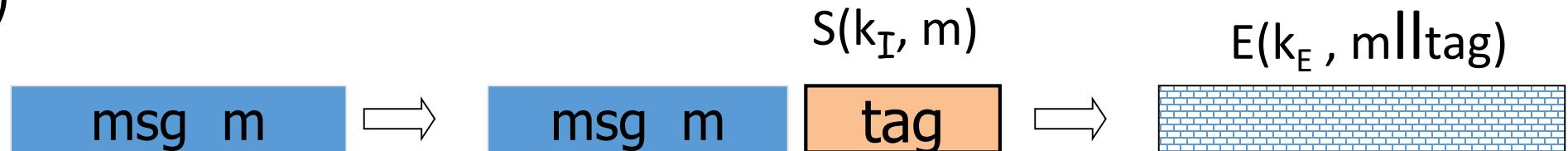
# Аутентифицированное шифрование

- Использует модель CPA + CI
- Обеспечивает целостность сообщений и шифртекстов
- Обеспечивает конфиденциальность
- Защита от активных противников
- В общем случае не защищает от атак повтором (повторная пересылка пакетов)
  - Можно решить введя специальный формат сообщений, включающих счётчики или идентификаторы
  - Вообще говоря это задача протоколов, а не конструкций (примитивов)
- Возможны атаки по побочным каналам (например, атаки по времени)

# Combining MAC and ENC

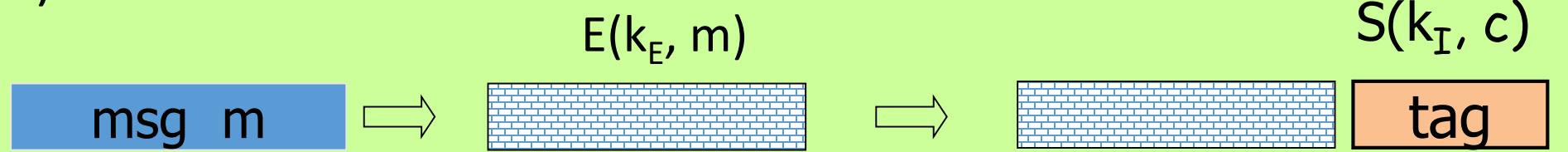
Encryption key  $k_E$ .    MAC key =  $k_I$

Option 1: (SSL)

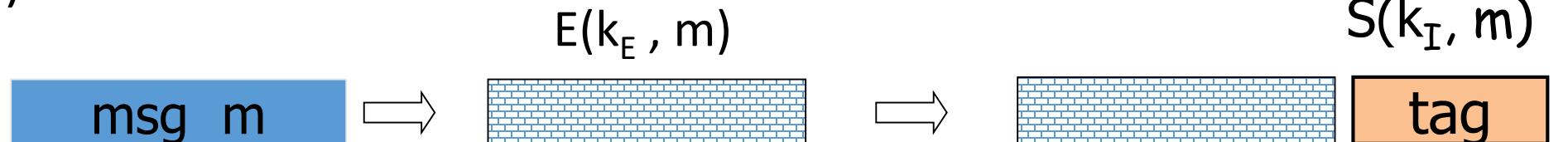


Option 2: (IPsec)

**always  
correct**



Option 3: (SSH)



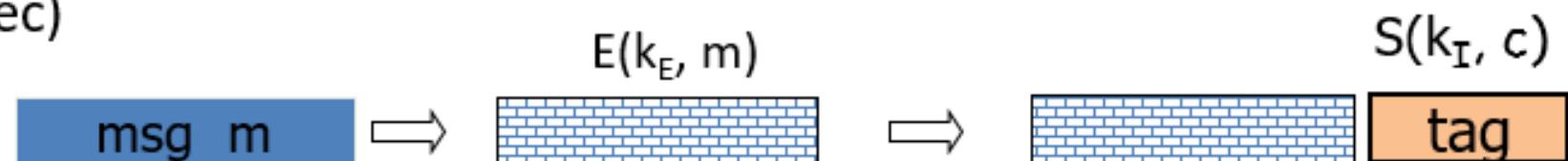
# Encrypt-then-MAC

Пусть  $E = (E, D)$  шифр на  $(K_e, M, C)$ ,  $I = (S, V)$  – MAC на  $(K_m, C, T)$ .

$E_{EtM} = (E_{EtM}, D_{EtM})$  на  $(K_e \times K_m, M, C \times T)$ :

- $E_{EtM}((k_e, k_m), m) = c \leftarrow^R E(k_e, m), t \leftarrow S(k_m, c), \text{return } (c, t)$
- $D_{EtM}((k_e, k_m), m) = \text{if } V(k_m, c, t) = 0: \text{return } \perp, \text{else: } D(k_e, c)$

Option 2: (IPsec)



# Encrypt-then-MAC

**Теорема 12.3.** Конструкция  $E_{EtM}$  - АЕ стойкая, причём

$$CI_{adv}[A_{CI}, E_{EtM}] = MAC_{adv}[B_{mac}, I]$$

$$CPA_{adv}[A_{cpa}, E_{EtM}] = CPA_{adv}[B_{cpa}, E]$$

▷ без доказательства ◁

- Необходимо использование **различных, независимых ключей** для МАС и шифрования (использование одинаковых ключей может вести к реальным атакам, например при использовании СВС шифрования и СВС МАС)
- МАС должны вычисляться для **всего** шифртекста (**включая IV**)
- Проверка целостности осуществляется **строго до** расшифрования

# MAC-then-encrypt

Пусть  $E = (E, D)$  шифр на  $(K_e, M, C)$ ,  $I = (S, V)$  – MAC на  $(K_m, C, T)$ .

$E_{EtM} = (E_{EtM}, D_{EtM})$  на  $(K_e \times K_m, M, C)$ :

- $E_{EtM}((k_e, k_m), m) = t \leftarrow S(k_m, m), c \xleftarrow{R} E(k_e, (m, t)), \text{return } c$
- $D_{EtM}((k_e, k_m), m) = (m, t) = D(k_e, c),$   
if  $V(k_m, c, t) = 0$ : return  $\perp$ , else:  $m$

Option 1: (SSL)



# MAC-then-encrypt

- Необходимо использование **различных, независимых ключей** для MAC и шифрования
- **Не является АЕ стойким в общем случае**, возможны атаки (сл. Лекция padding oracle)
- Является АЕ стойким для **некоторых CPA стойких шифров** (рандомизированный CTR, CBC без дополнения сообщений).
- Проверка аутентичности происходит после расшифрования (что и ведёт к ряду атак, в том числе по времени)

# Encrypt-and-MAC

Пусть  $E = (E, D)$  шифр на  $(K_e, M, C)$ ,  $I = (S, V)$  – MAC на  $(K_m, C, T)$ .

$E_{EtM} = (E_{EtM}, D_{EtM})$  на  $(K_e \times K_m, M, C \times T)$ :

- $E_{EtM}((k_e, k_m), m) = c \leftarrow^R E(k_e, m), t \leftarrow S(k_m, m)$ , return  $(c, t)$
- $D_{EtM}((k_e, k_m), m) = m = D(k_e, c)$ , if  $V(k_m, m, t) = 0$ : return  $\perp$ , else:  $m$

Option 3: (SSH)



# Encrypt-and-MAC

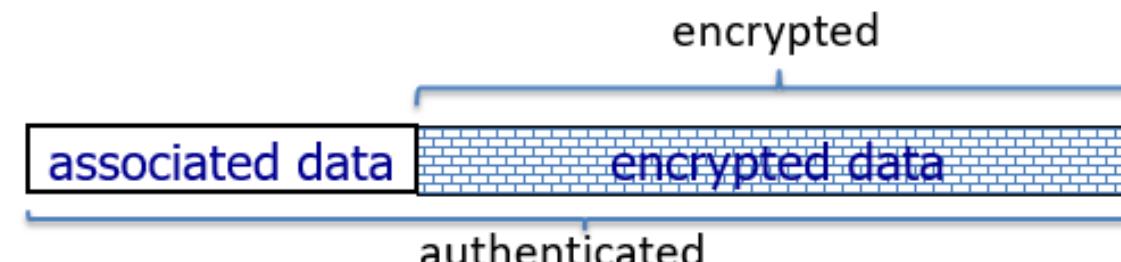
- Необходимо использование **различных, независимых ключей** для MAC и шифрования
- Не является AE стойким в общем случае
- Вообще говоря, из MAC можно восстановить часть сообщения (на стойкий MAC не накладывается требования не раскрывать биты сообщения)

# Режимы аутентифицированного шифрования

Можем ли мы построить режимы, при которых будет обеспечивать АЕ стойкость изначально?

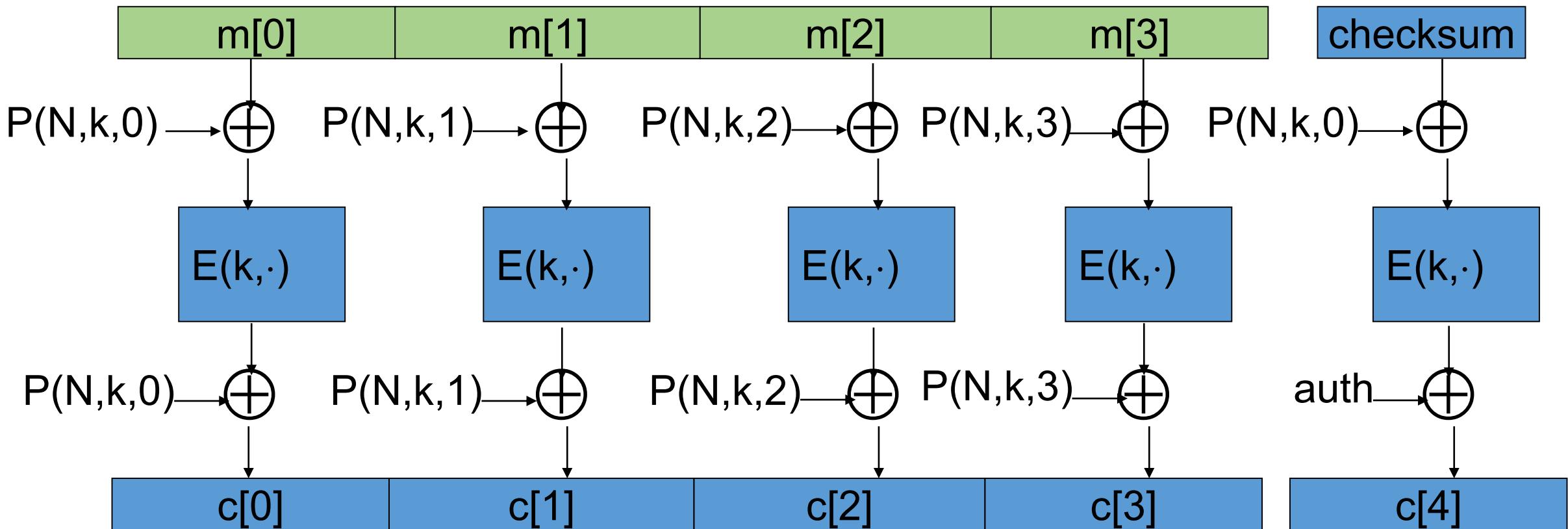
Можем –GCM, CCM, EAX, OCB

Описанные режимы являются не только АЕ шифрованием, но и AEAD (**authenticated encryption with associated data**), когда часть данных шифруется и аутентифицируется, а часть только аутентифицируется (**associated data**). Все режимы используют nonce.

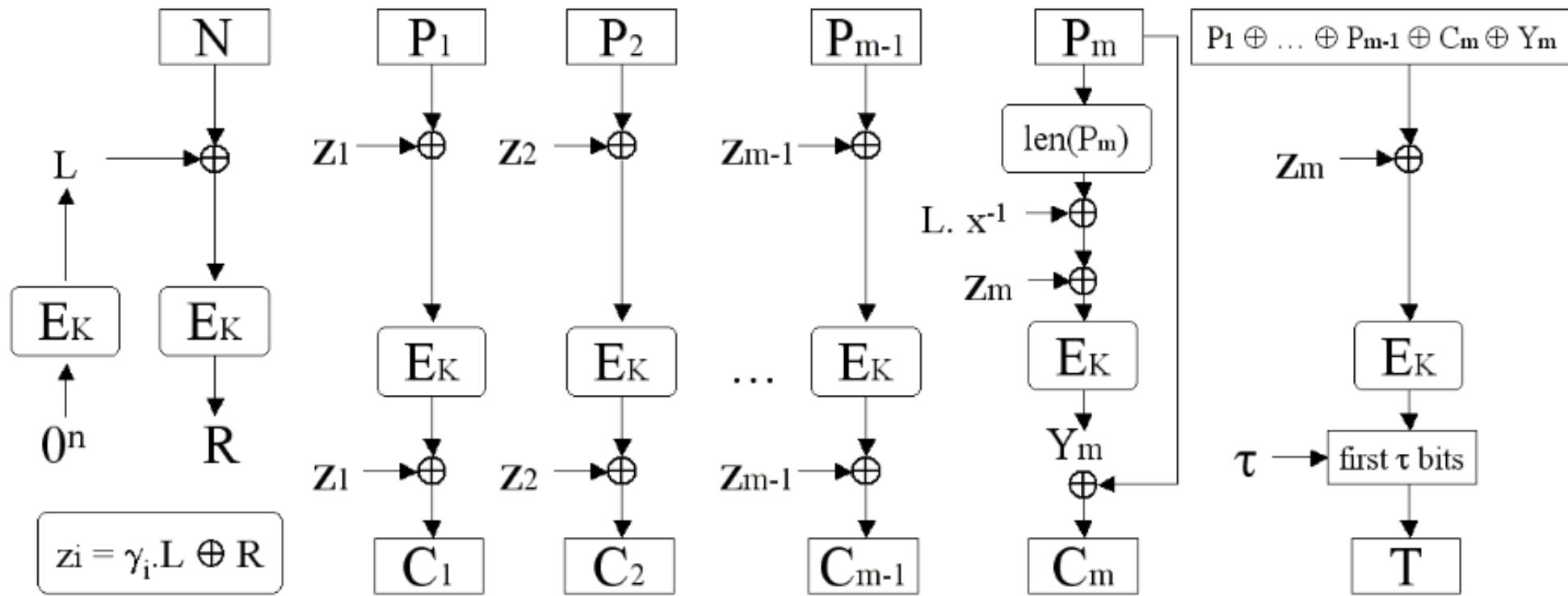


# OCB

One  $E()$  op. per block.



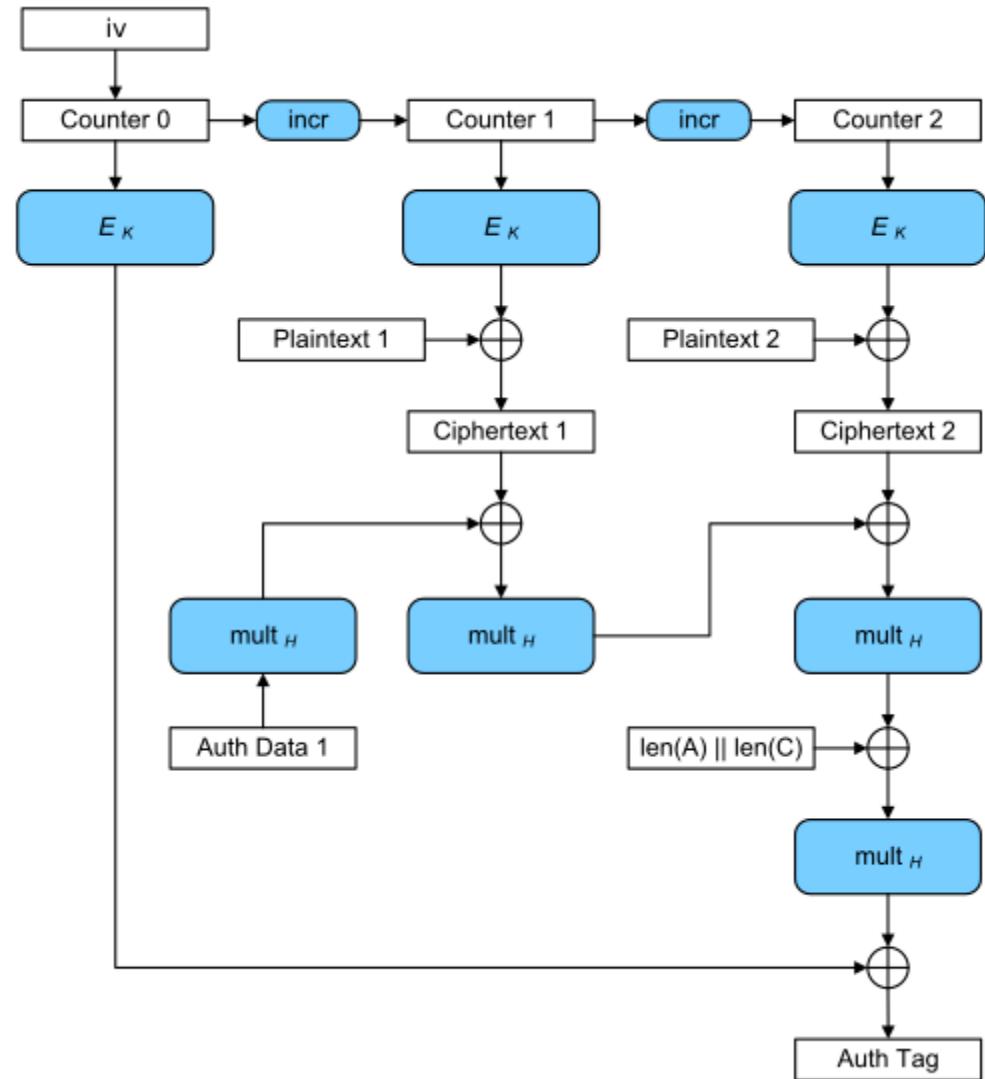
# OCB



- Полностью параллелизуется
- Патентовано (спасибо Rogaway!)

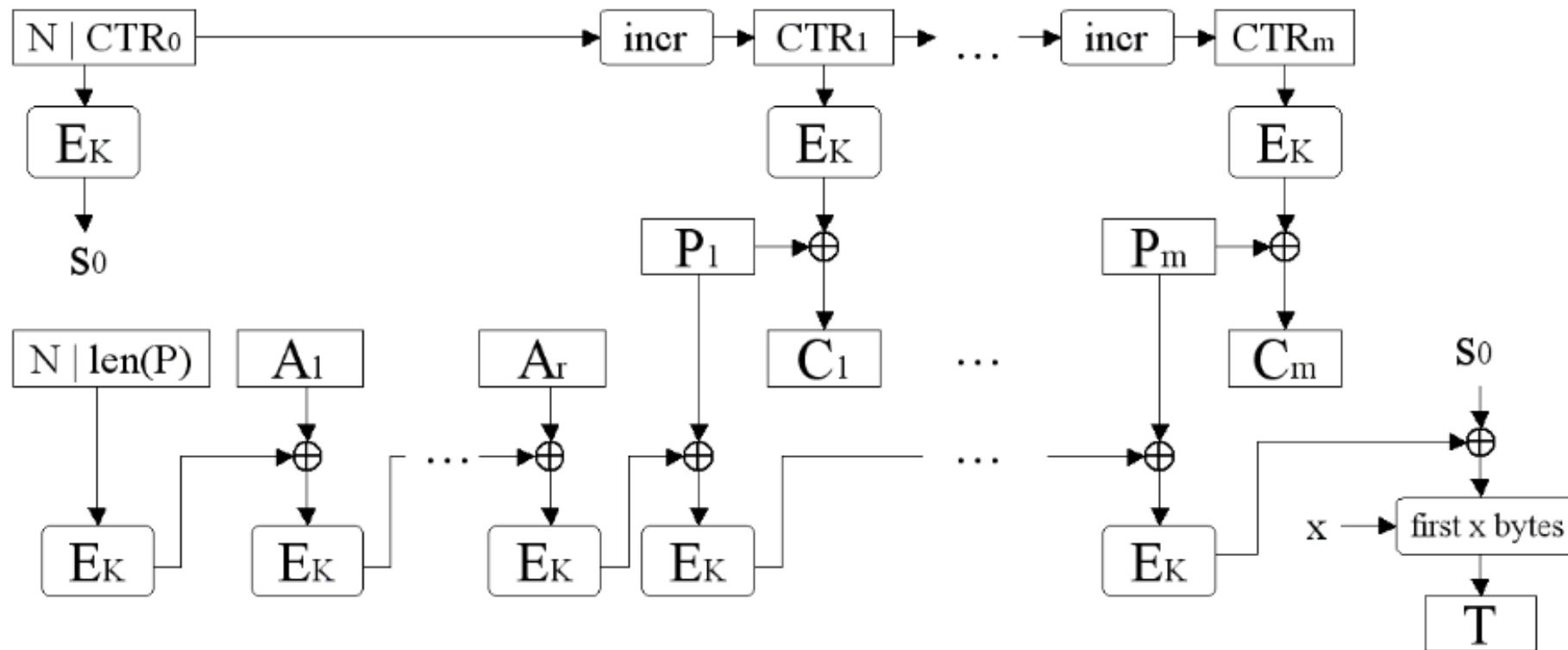
# GCM

- CTR-mode-then-CW-MAC
- Параллизуется только шифрование
- MAC последовательный, не требует вычисления PRP
- Стандарт NIST



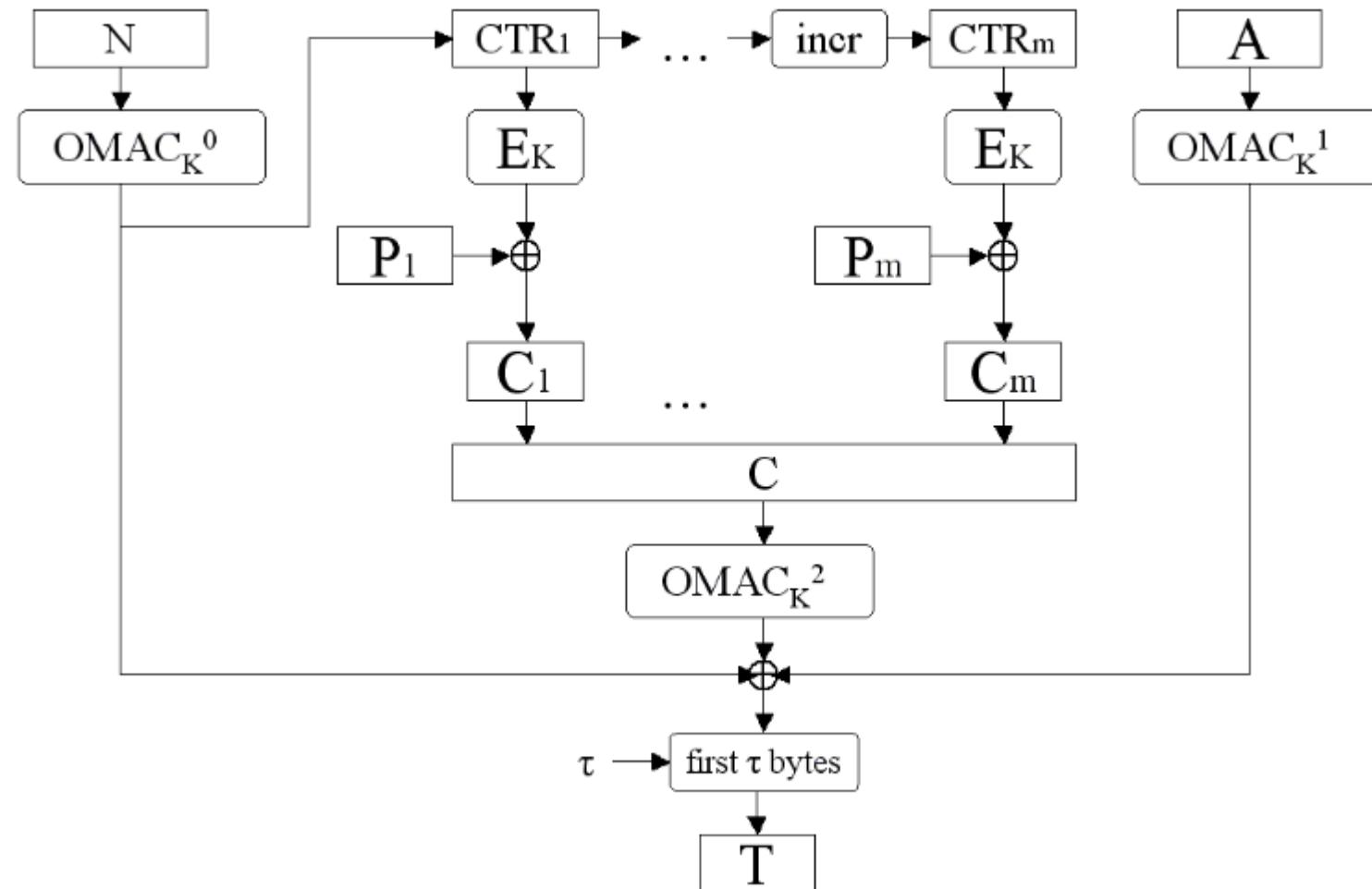
# CCM

- CTR-mode-and-CBC-MAC
- Параллелизуется только шифрование

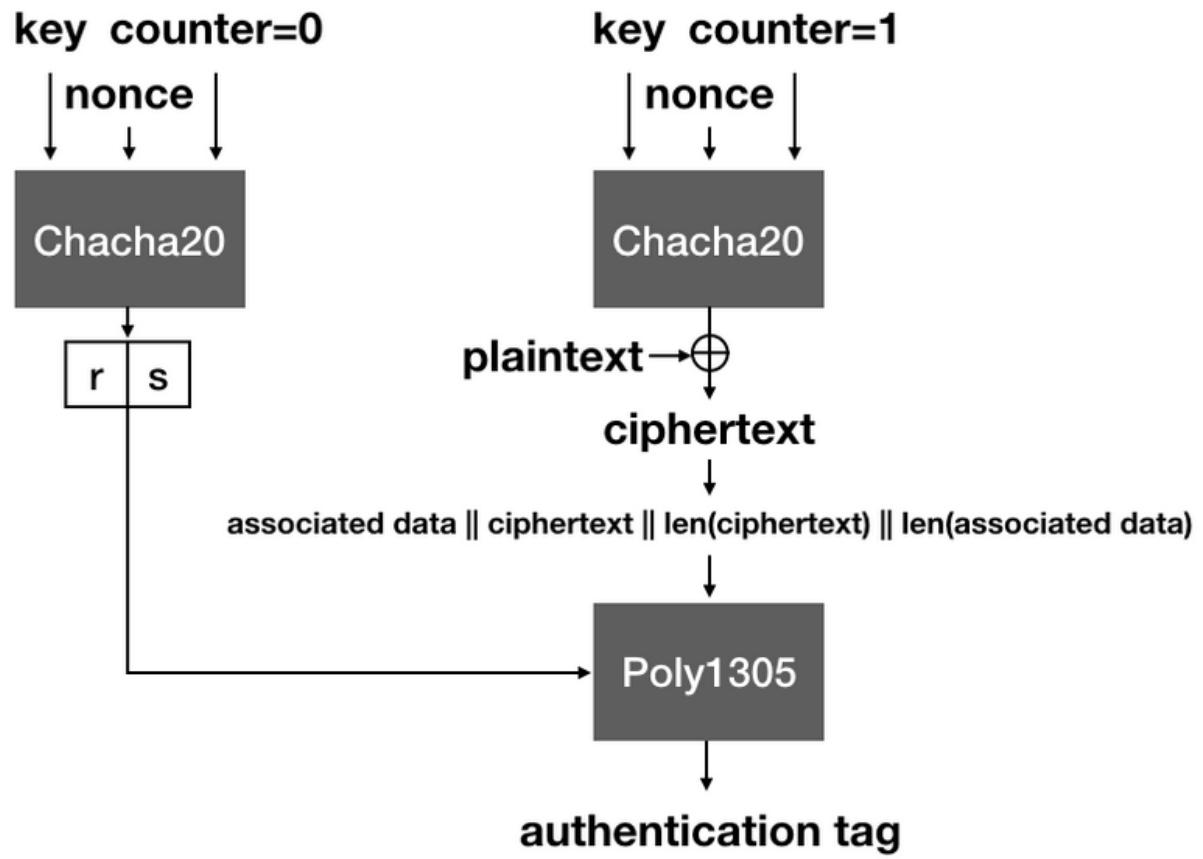


# EAX

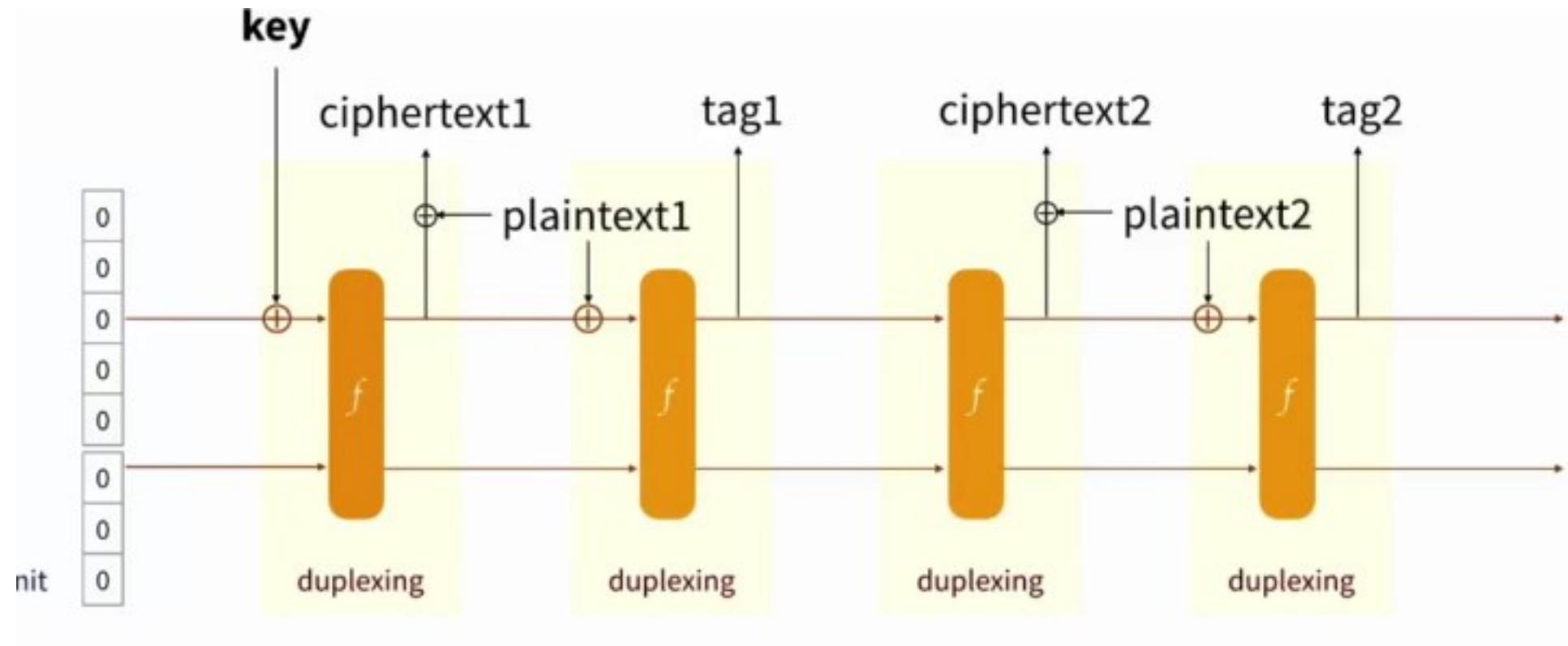
- Параллизуется только шифрование
- MAC последовательный, требует вычисления PRP



# ChaCha/Poly1305



# Построение аутентифицированного шифрования с помощью SHA-3 (Strobe)



# Выводы

- Для построения защищенных каналов необходимо использовать АЕ шифрование
- Лучше использовать Encrypt-Then-MAC или один из стандартов AEAD шифрования
- Никогда не реализовывать криптографию!