Прикладная Криптография: Симметричные криптосистемы Аутентифицированное шифрование

Макаров Артём

МИФИ 2020

Криптографическая защита информации

Обеспечение конфиденциальности

- семантическая стойкость против CPA атаки
- Зашита 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, CW-MAC

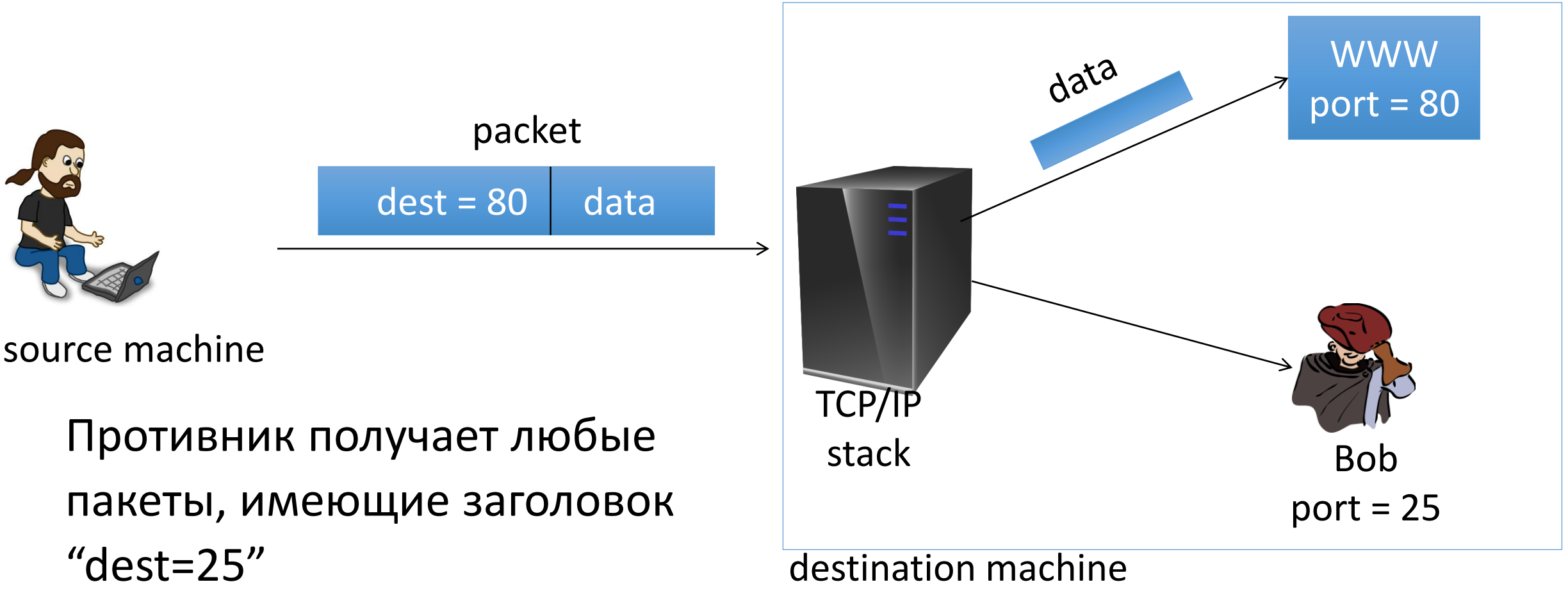
Криптографическая защита информации

Аутентифицированное шифрование

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

Пример перехвата сообщений

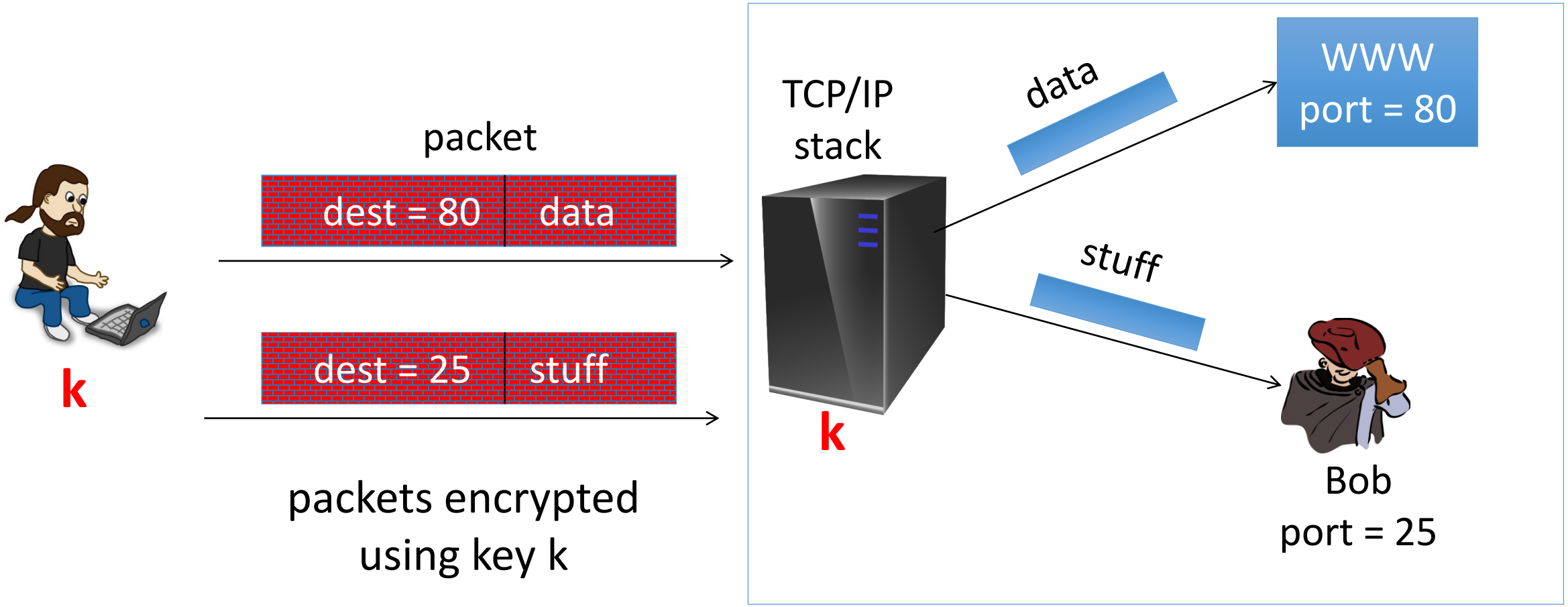
TCP/IP: (highly abstracted)



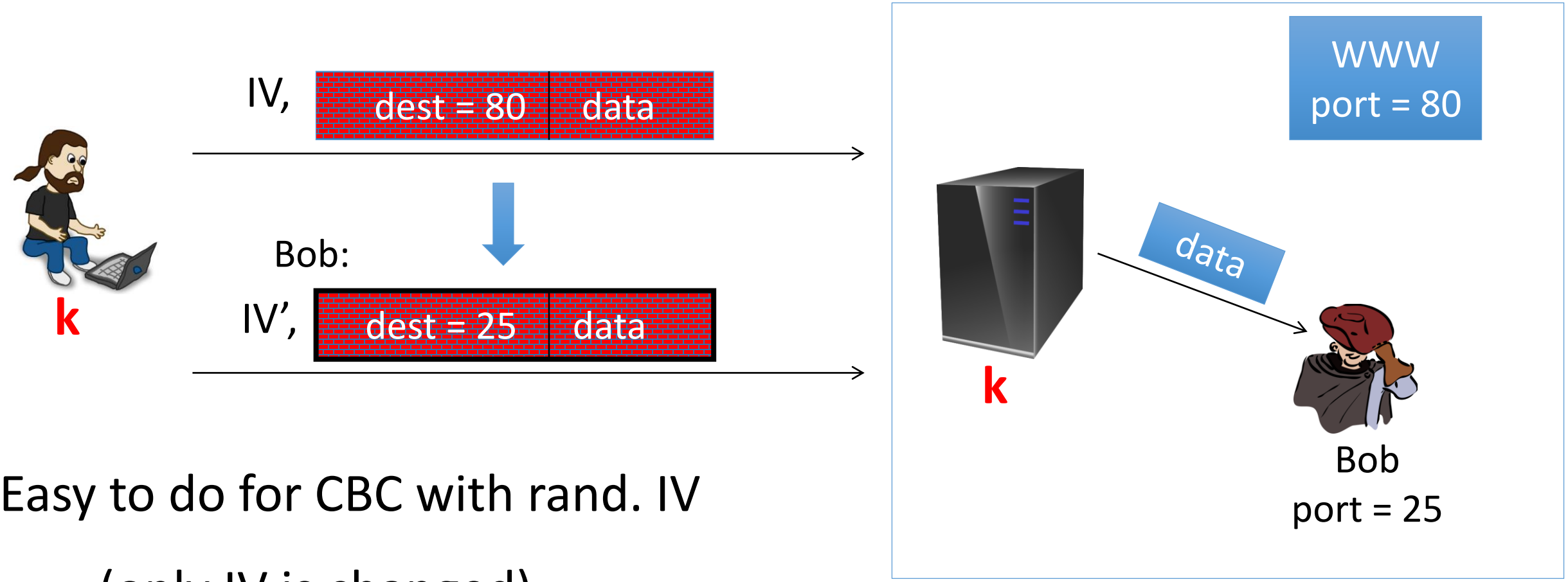
Противник получает любые пакеты, имеющие заголовок “dest=25”

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.

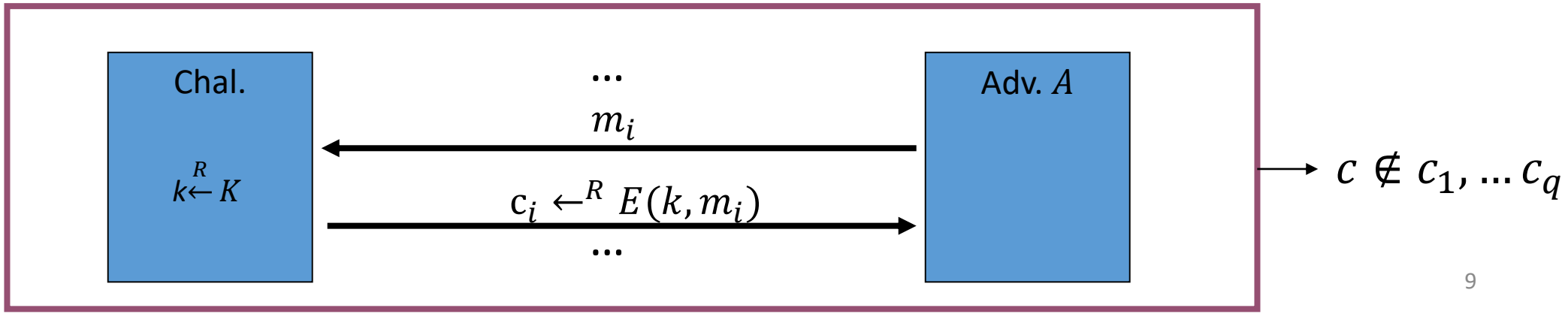
$\mathrm{E} = (E, D)$ аутентифицированный шифр на (K, M, C).

- $E: K \times M \to C$
- $D: K \times C \to M \cup \{\perp\}$
- $\perp$ - шифртекст отклонён (не пройдена проверка аутентичности)

Целостность шифртекстов

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

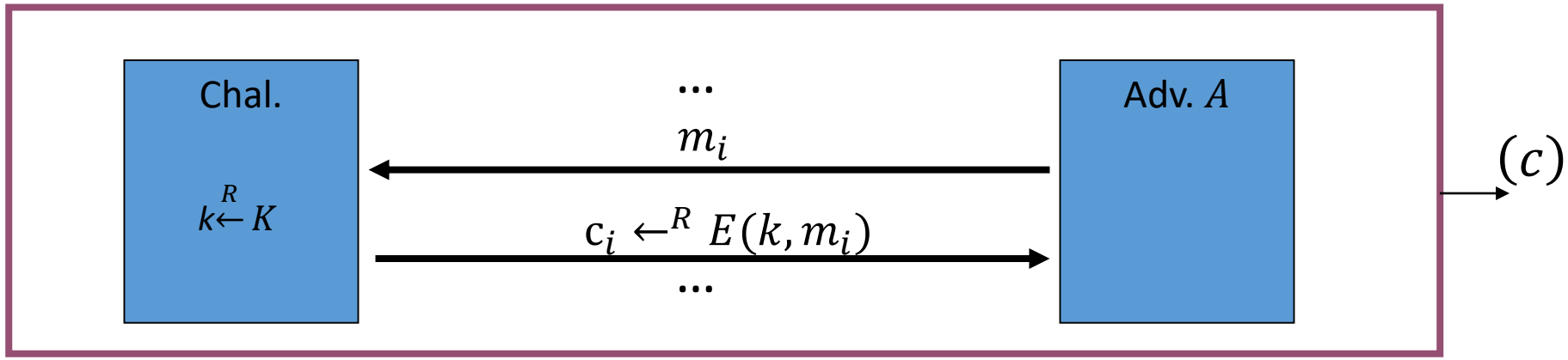
- Претендент выбирает случайный ключ
- Противник запрашивает зашифрование нескольких открытых текстов в адаптивной атаке
- Цель противника – получить **новый корректный шифртекст**



Целостность шифртекстов

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

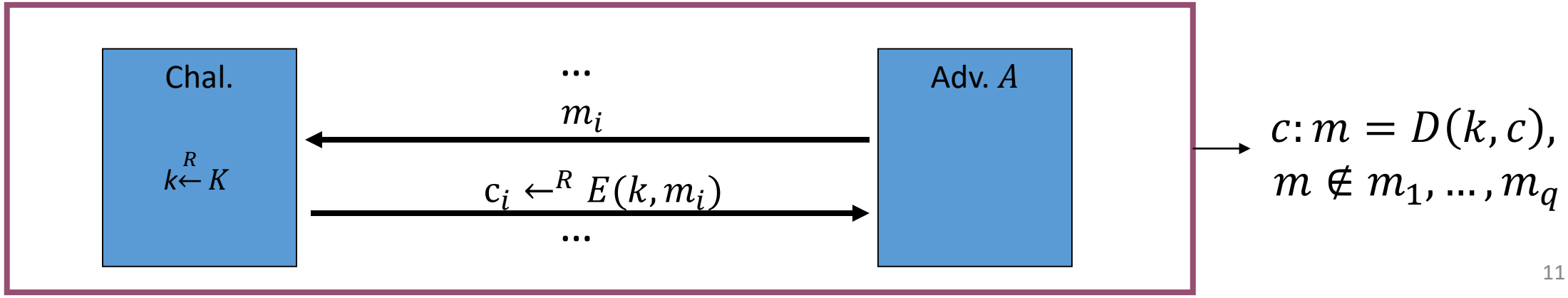
Шифр E является **шифром обеспечивающим целостность шифртекстов**, если $\forall A\ CI_{adv}[A, \mathrm{E}] \leq \epsilon$, где ϵ – пренебрежимо малая величина.



Целостность открытых текстов

Пусть $\mathrm{E} = (E, D)$ – **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 адаптивной атаке
- Цель противника – получить **корректный** шифртекст для **нового сообщения**



Целостность открытых текстов

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

Шифр E является **шифром обеспечивающим целостность открытых текстов**, если $\forall A \; PI_{adv}[A, \mathrm{E}] \leq \epsilon$, где ϵ – 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 PT соответствует множество CT. Если противник может создавать **новые CT** для **существующих сообщений**, **но не может для новых** то он PI, но не CI стойкий.

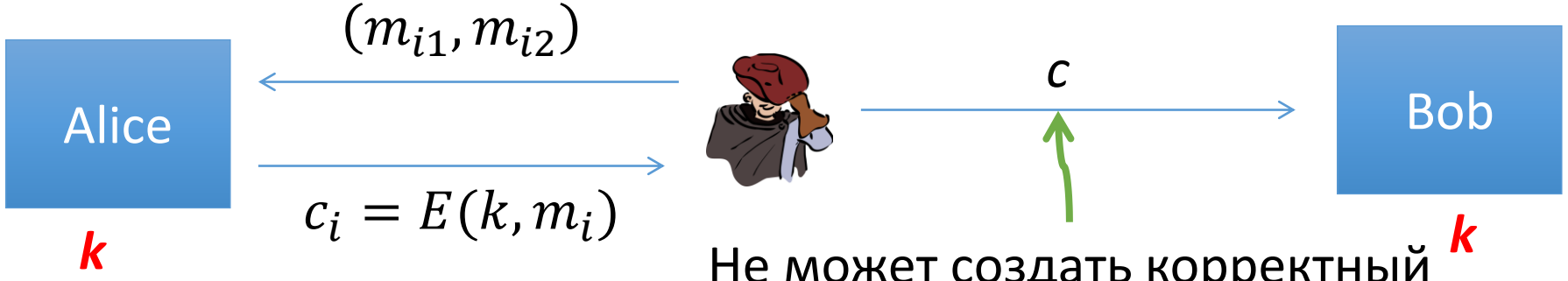
Аутентифицированное шифрование

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



Не может создать корректный $c \notin \{ c_1, \ldots, c_q \}$

Не может различить зашифрования m_{i1}, m_{i2}

Не может расшифровать c_i

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

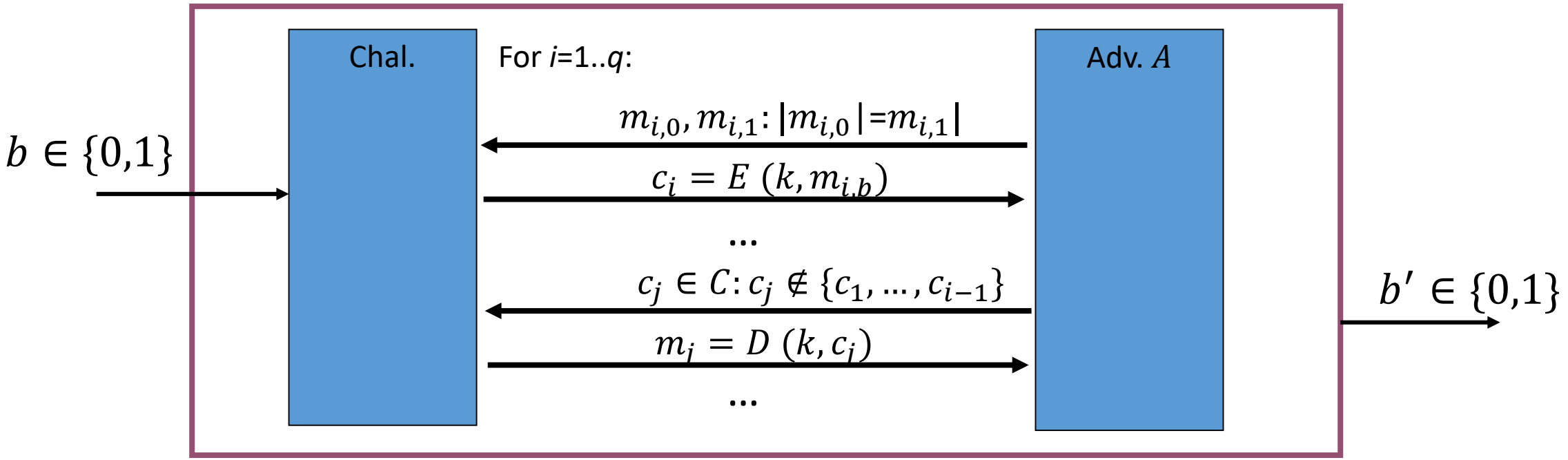
Для AE шифров данная атака невозможна, т.к. шифр гарантирует невозможность получения корректного шифртекста c' без знания секретного ключа.

CCA

Пусть $\mathrm{E} = (E, D)$ – 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


Chal.
For i=1..q:
Adv. A
$b \in \{0,1\}$
$m_{i,0}, m_{i,1}: |m_{i,0}| = m_{i,1}|$
$c_i = E\ (k, m_{i,b})$
...
$c_j \in C: c_j \notin \{c_1, \ldots, c_{i-1}\}$
$m_j = D\ (k, c_j)$
...
$b' \in \{0,1\}$

CCA стойкость

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

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

Шифр E 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 $\forall A: CCA_{adv}[A, \mathrm{E}] \leq \epsilon$, где ϵ – пренебрежимо малая величина

Более сильное определение, чем CPA стойкость

Аутентифицированное шифрование и CCA стойкость

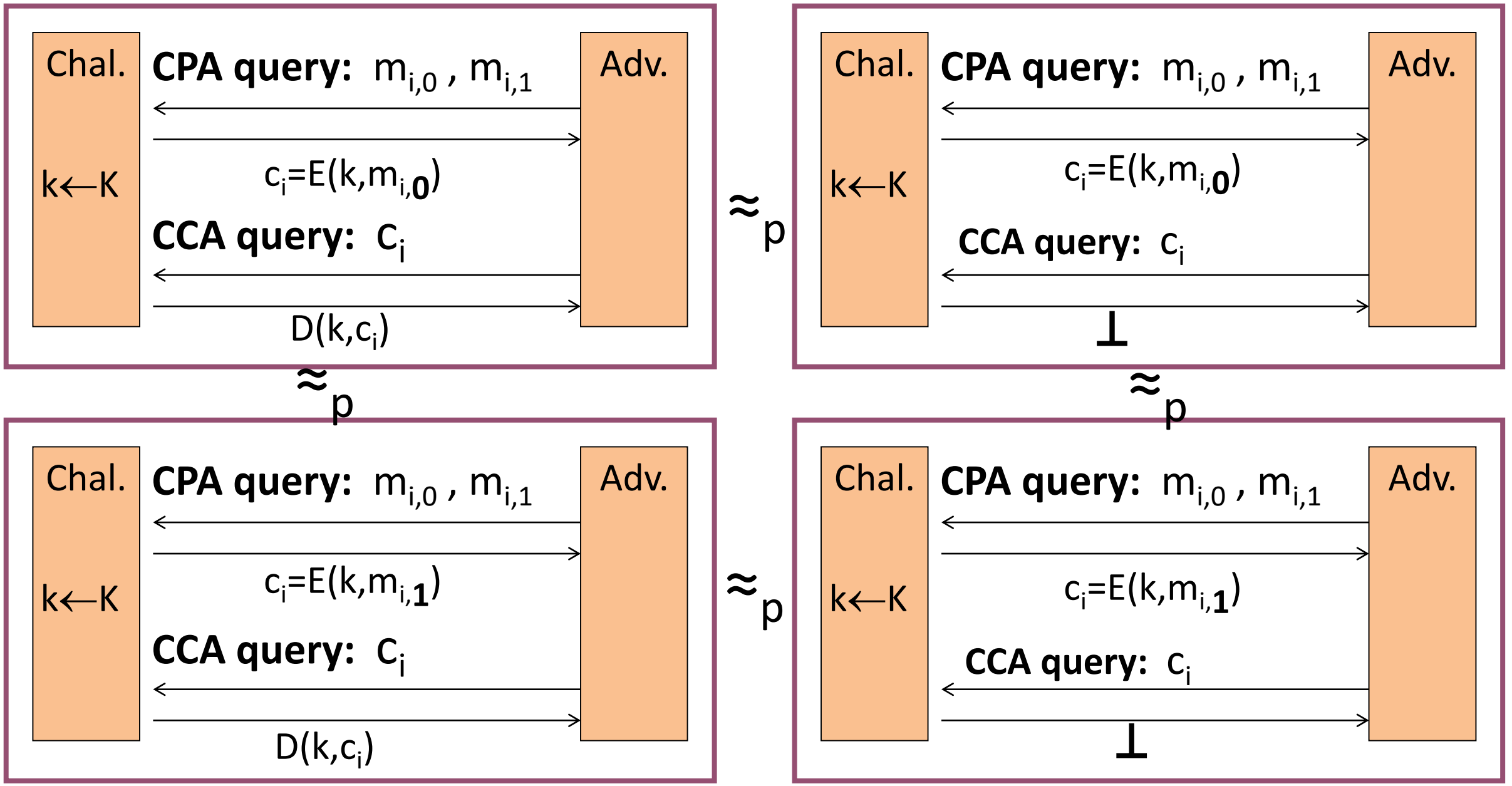
Теорема 12.1. Пусть $\mathrm{E} = (E, D)$ – шифр. Если он AE стойкий, то он CCA стойкий, причём

$\forall A$ в игре на CCA 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:

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

▻ без доказательства ◅

Proof by pictures



Аутентифицированное шифрование и CCA стойкость

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

$\triangleright$ без доказательства $\triangleleft$

T.e. AE стойкость <=> CPA + CI (целостность **CT**) => CCA стойкость

CCA стойкость + PI (целостность **PT**) => AE стойкость

CCA стойкость => CPA стойкость

CI => PI

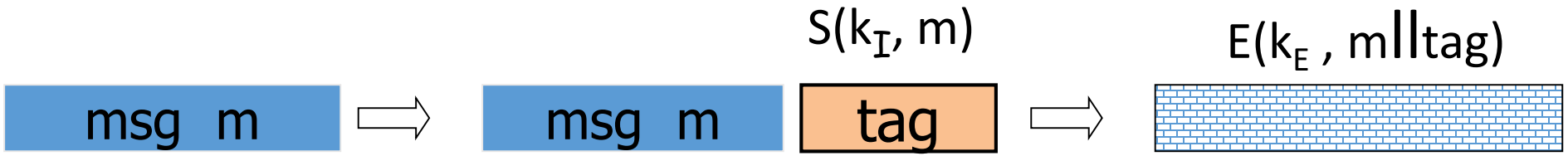
Аутентифицированное шифрование

- 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

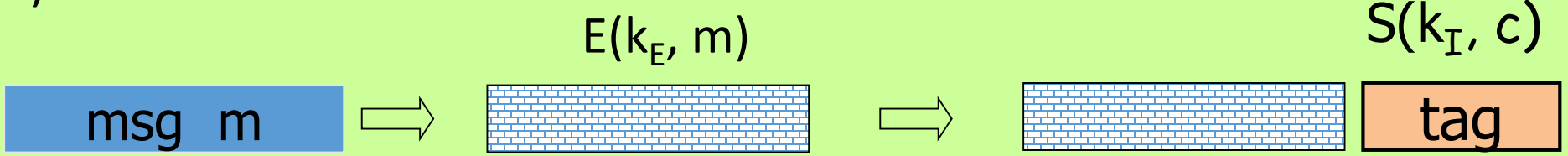
Encryption key k_E. MAC key = k_I

Option 1: (SSL)

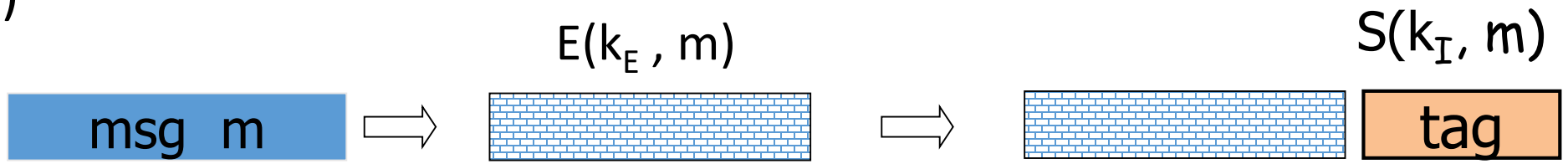


Option 2: (IPsec)

always correct



Option 3: (SSH)

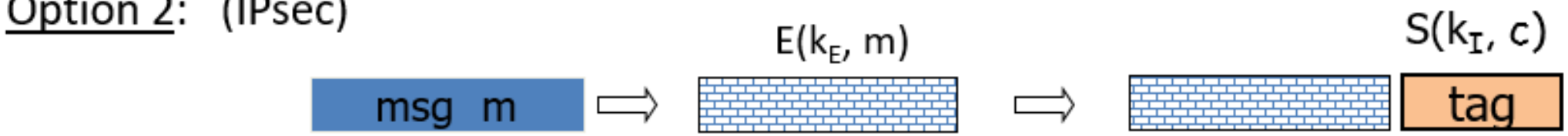


Encrypt-then-MAC

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

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

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



Encrypt-then-MAC

Теорема 12.3. Конструкция E_{EtM} - AE стойкая, причём

$$CI_{adv}[A_{CI}, \mathrm{E}_{EtM}] = MAC_{adv}[B_{mac}, I]$$
$$CPA_{adv}[A_{cpa}, \mathrm{E}_{EtM}] = CPA_{adv}[B_{cpa}, \mathrm{E}]$$

▻ без доказательства ◅

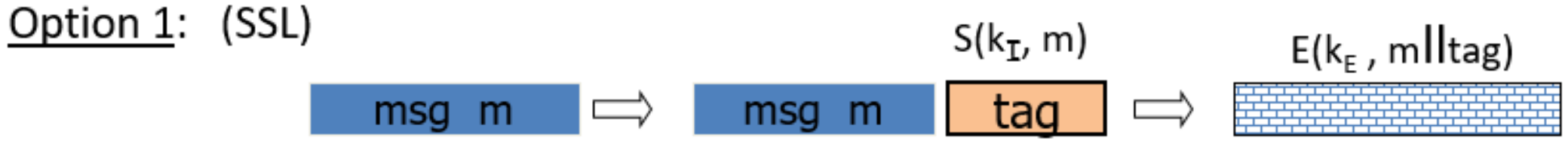
- Необходимо использование **различных, независимых ключей** для MAC и шифрования (использование одинаковых ключей может вести к реальным атакам, например при использовании CBC шифрования и CBC MAC)
- MAC должны вычисляться для **всего** шифртекста (**включая** IV)
- Проверка целостности осуществляется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

MAC-then-encrypt

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

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

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



MAC-then-encrypt

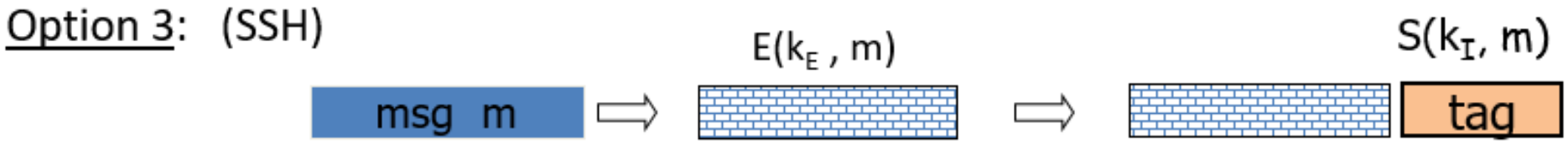
- Необходимо использование **различных, независимых ключей** для MAC и шифрования
- **Не является AE стойким в общем случае**, возможны атаки (сл. Лекция padding oracle)
- Является AE стойким для **некоторых CPA стойких шифров** (рандомизированный CTR, CBC без дополнения сообщений).
- Проверка аутентичности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

Encrypt-and-MAC

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

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

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



Encrypt-and-MAC

- Необходимо использование **различных, независимых ключей** для MAC и шифрования

- Не является AE стойким в общем случае

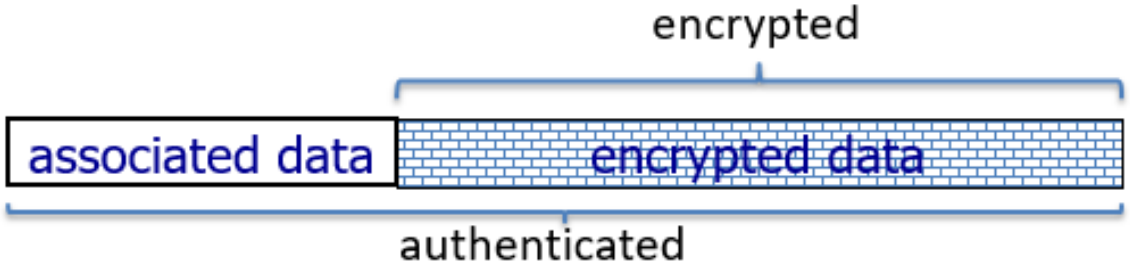
- Вообще говоря, из MAC можно восстановить часть сообщения (на стойкий MAC не накладывается требования не раскрывать биты сообщения)

Режимы аутентифицированного шифрования

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

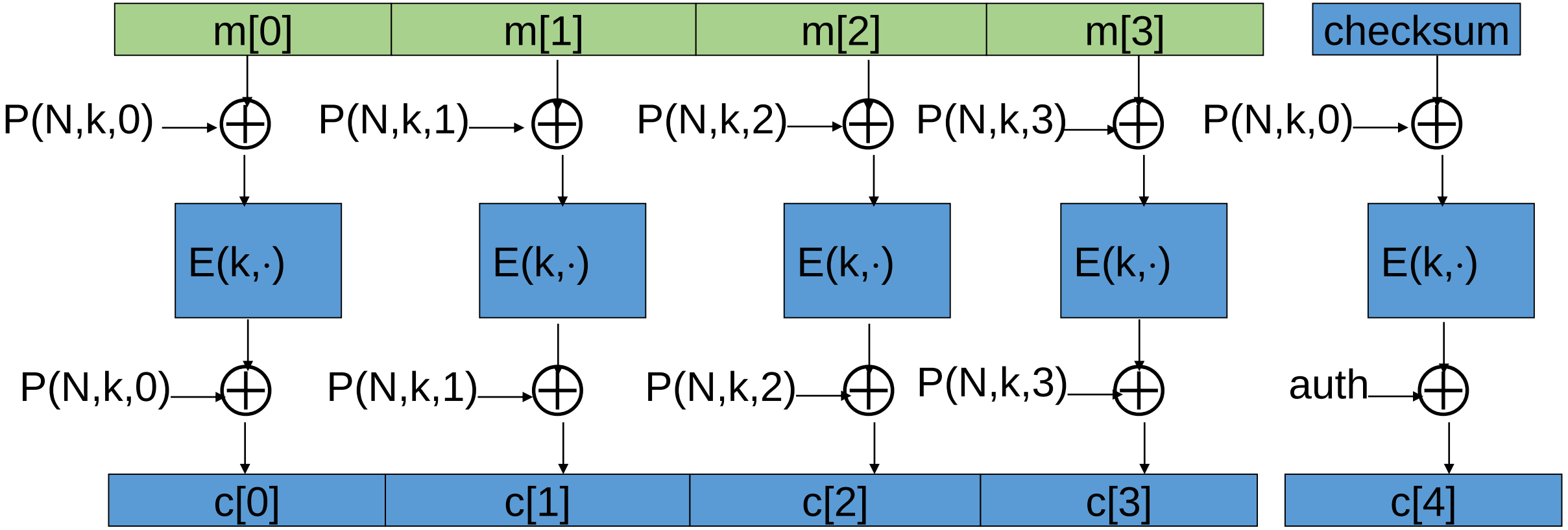
Можем –GCM, CCM, EAX, OCB

Описанные режимы являются не только AE 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.

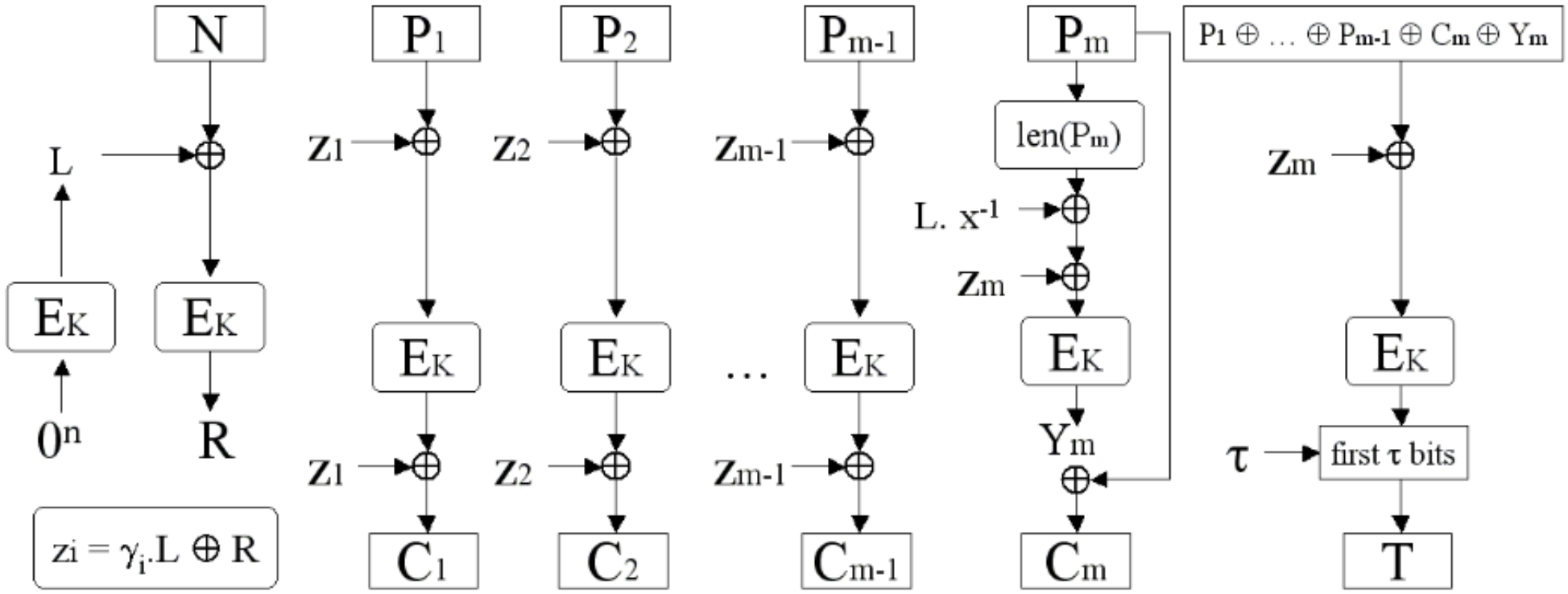


OCB

One E() op. per block.



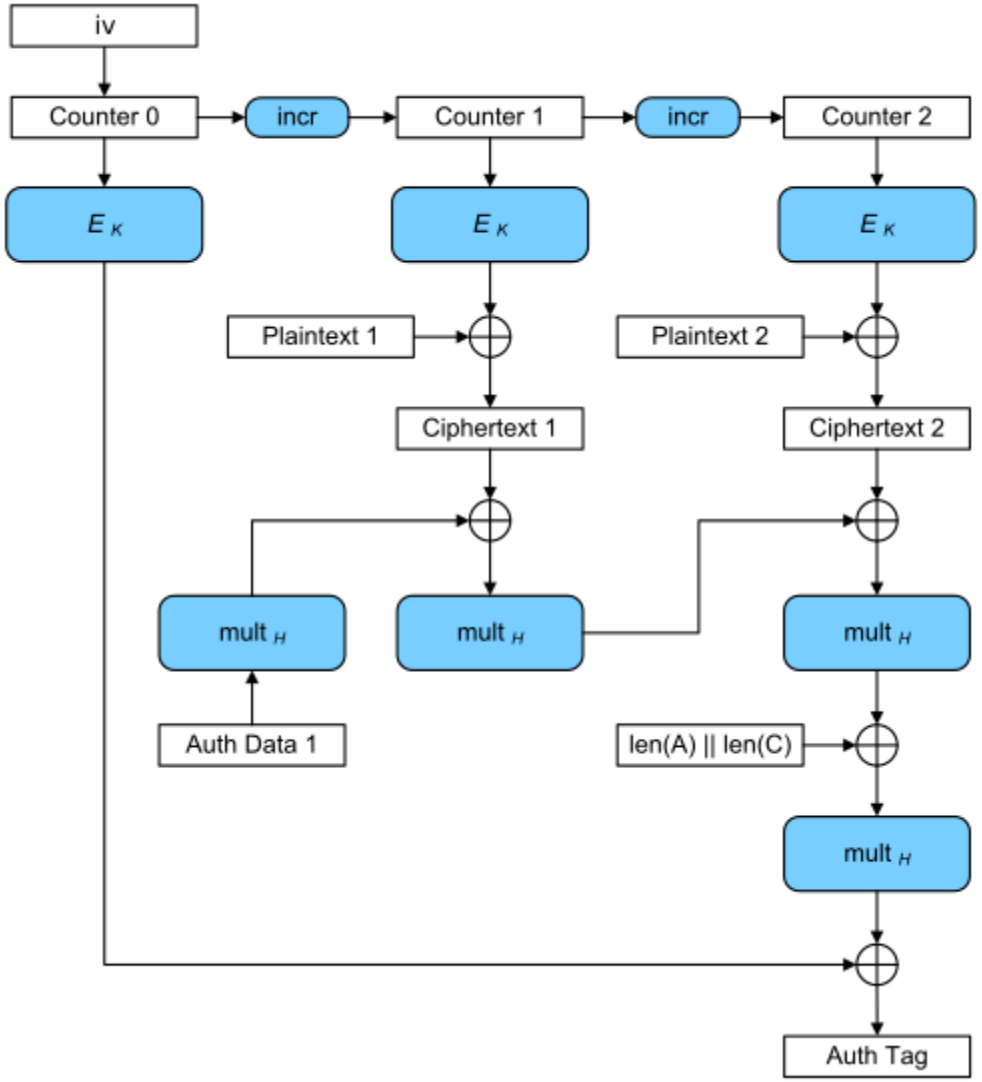
OCB



- Полностью параллелизуется
- Патентовано (спасибо Rogaway!)

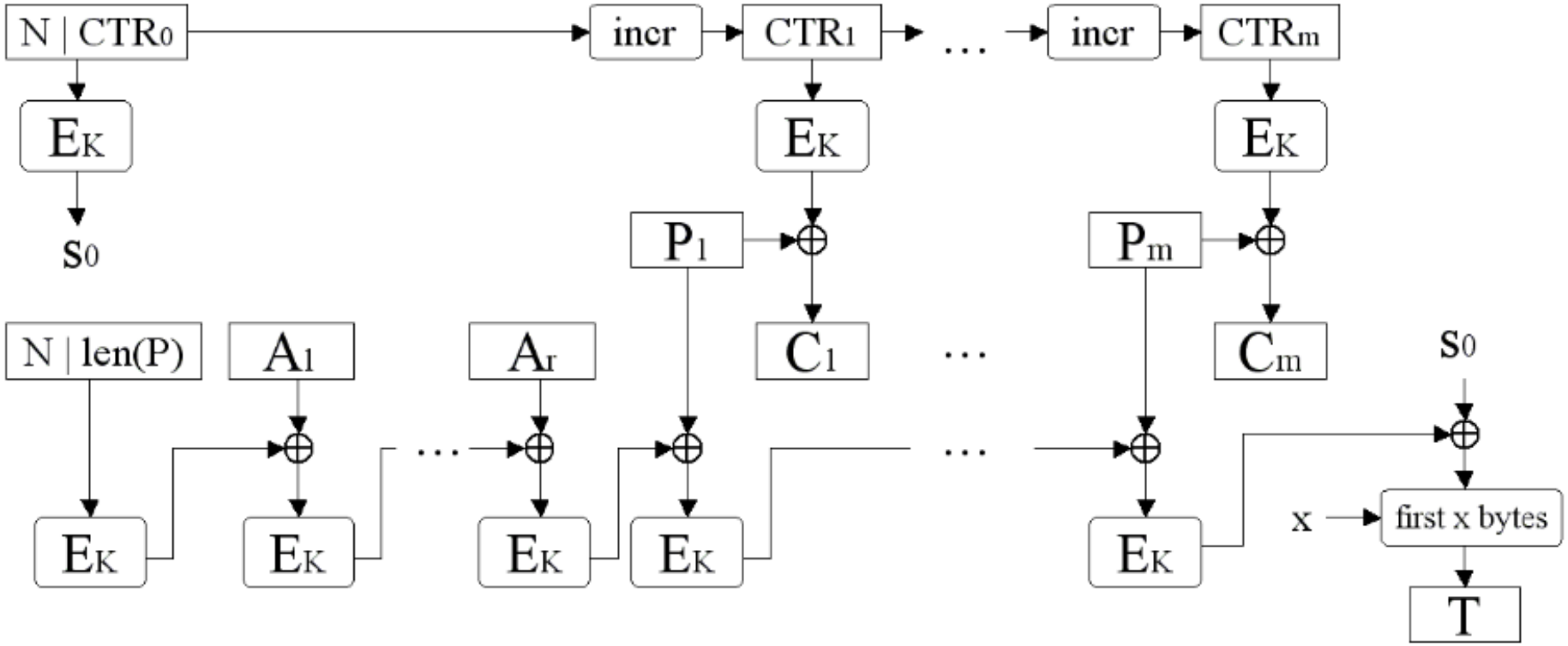
GCM

- CTR-mode-then-CW-MAC
- Параллелизуется только шифрование
- MAC последовательный, не требует вычисления PRP
- Стандрат NIST



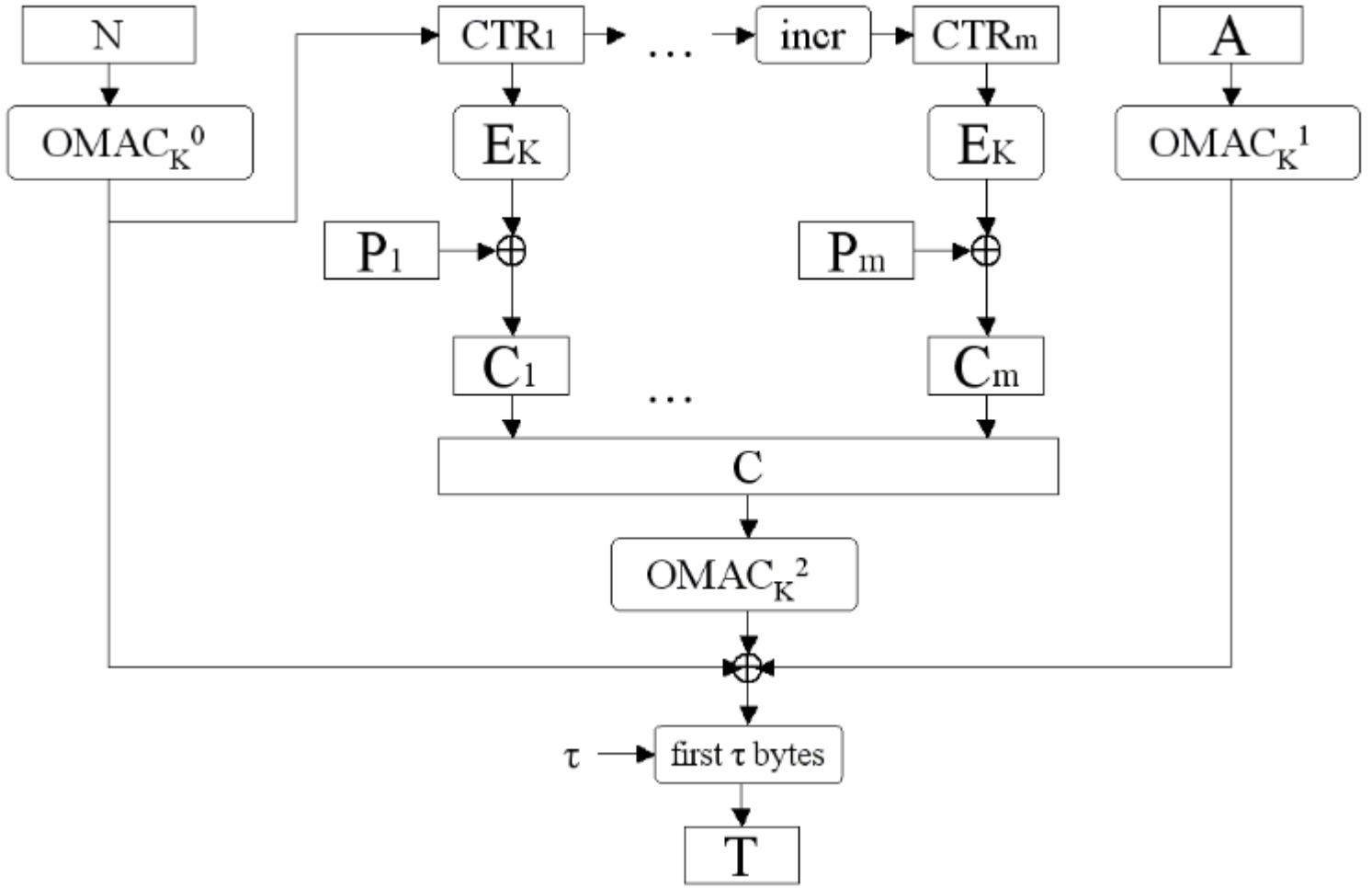
CCM

- CBC-MAC-then-CTR-mode
- Не параллелизуется

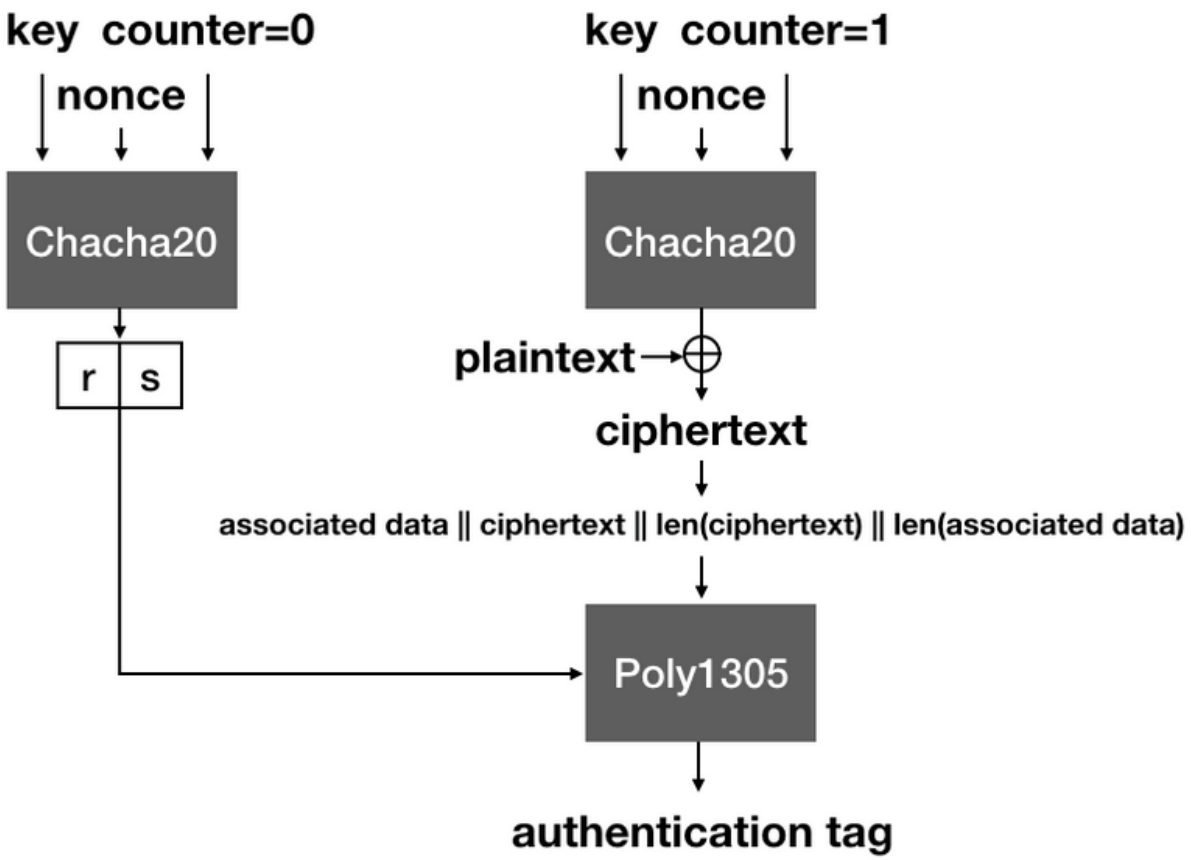


EAX

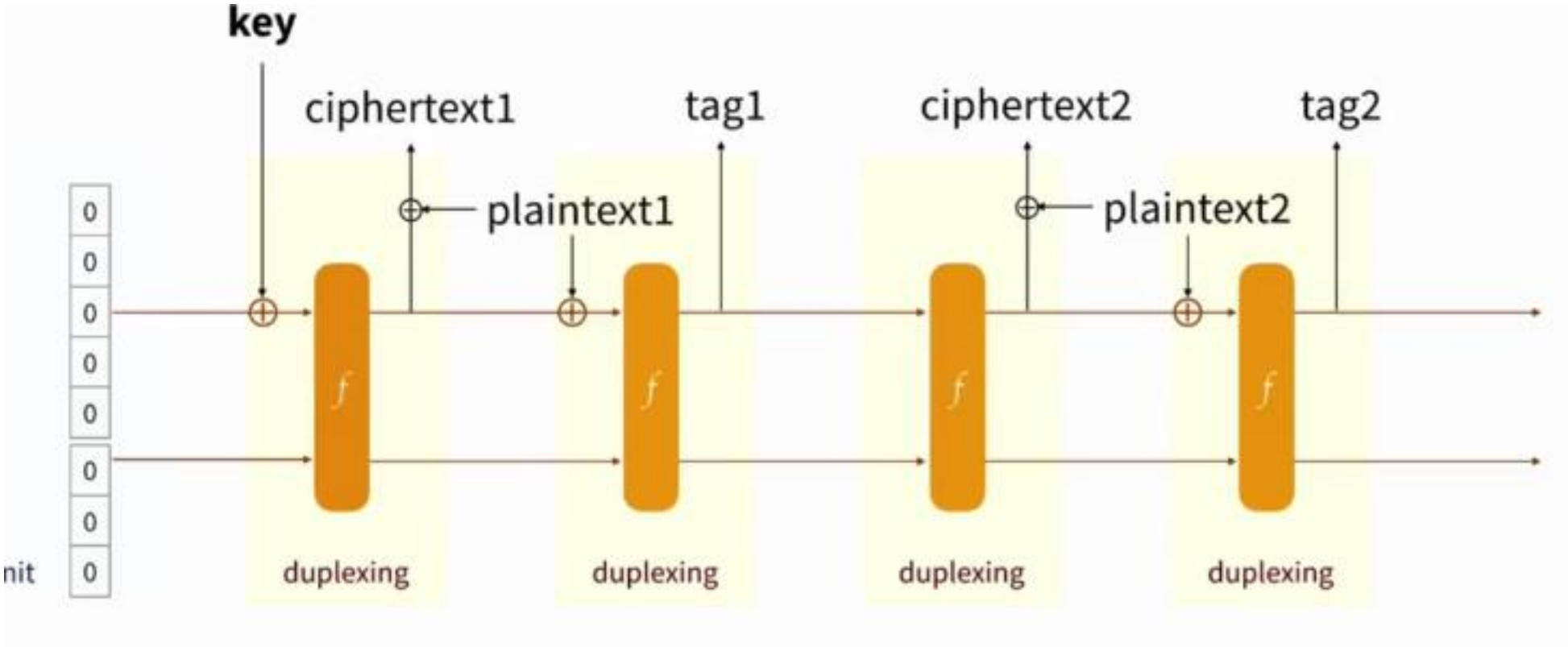
- Параллелизуется только шифрование
- MAC последовательный, требует вычисления PRP



ChaCha/Poly1305



Построение аутентифицированного шифрования с помощью SHA-3 (Strobe)



Выводы

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