Аутентифицированное шифрование

Макаров Артём

МИФИ 2020

Криптографическая защита информации

Обеспечение конфиденциальности

- 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

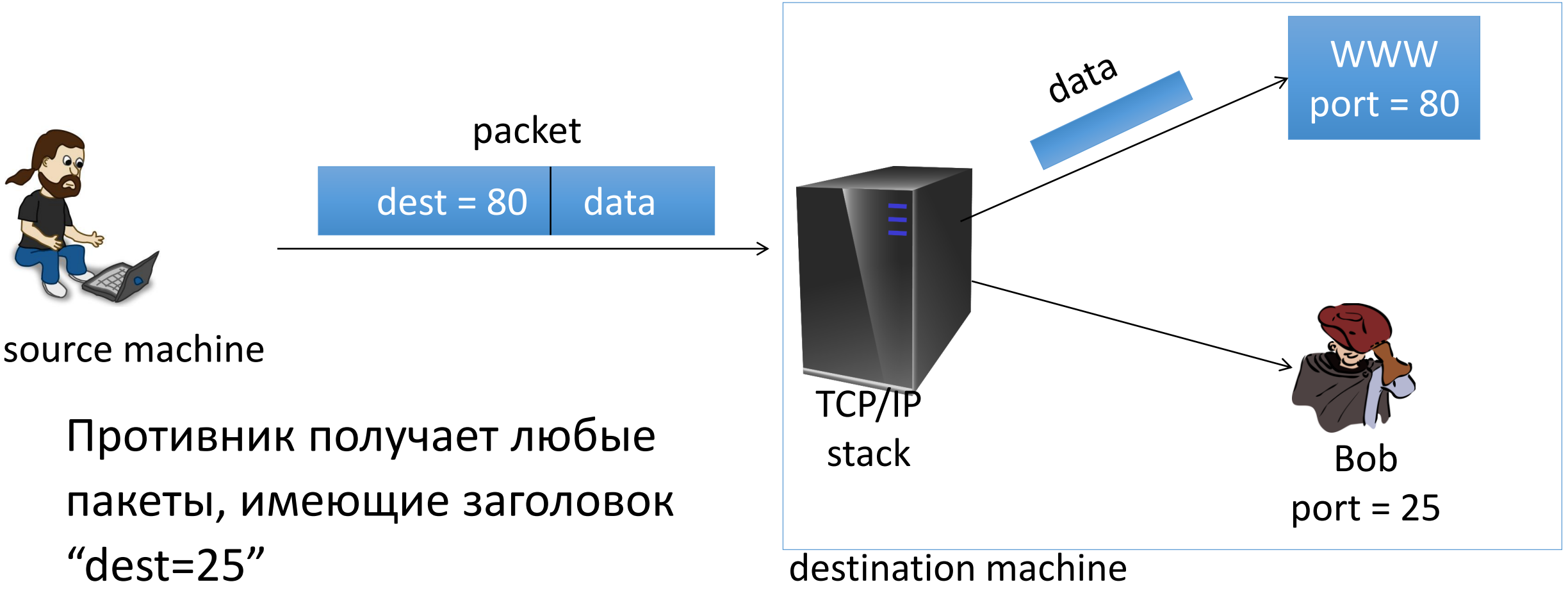
Криптографическая защита информации

Аутентифицированное шифрование

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

Пример перехвата сообщений

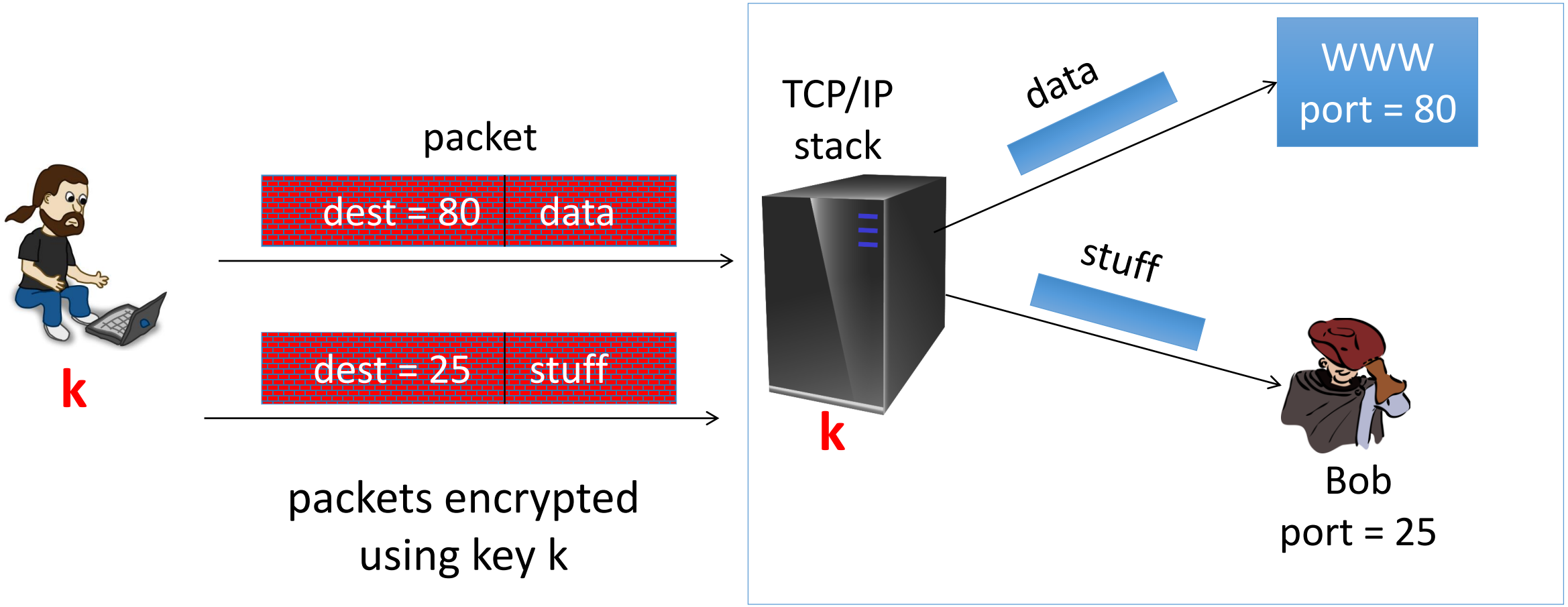
TCP/IP: (highly abstracted)



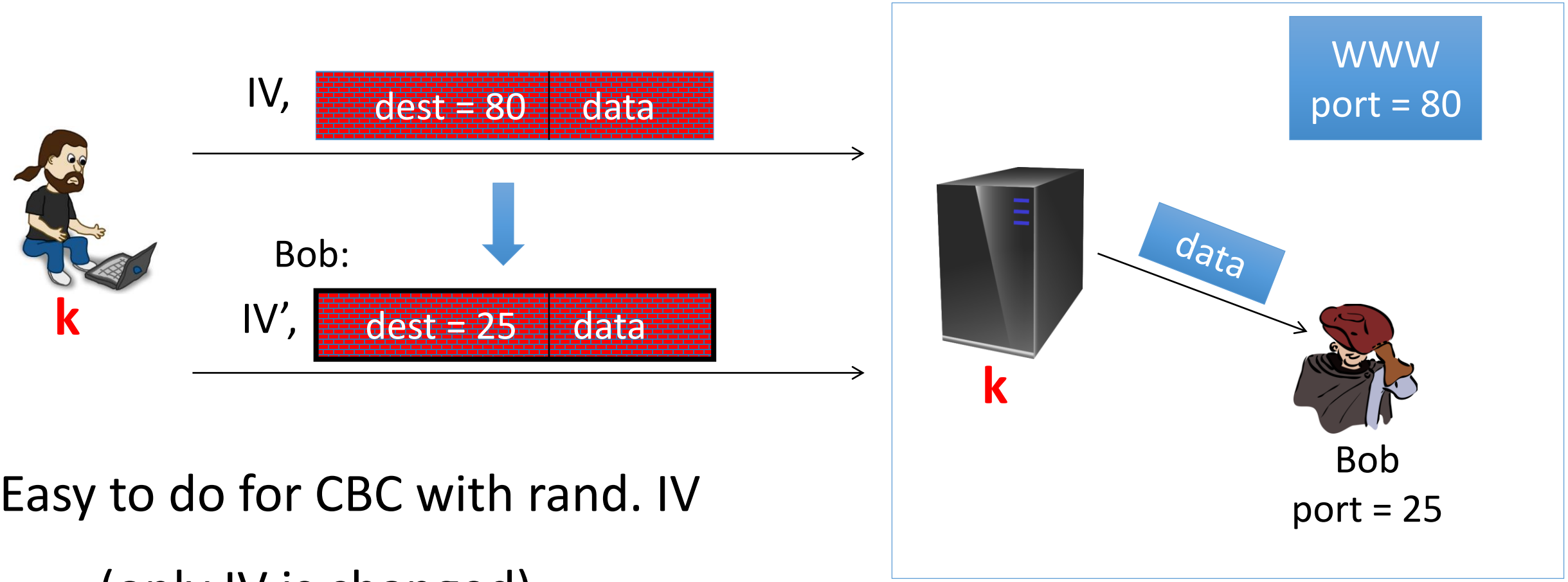
Противник получает любые пакеты, имеющие заголовок “dest=25”

Пример перехвата сообщений

IPsec: (highly abstracted)



Пример перехвата сообщений



Easy to do for CBC with rand. IV

(only IV is changed)

Выводы

Стойкое шифрование 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)

- CI – (ciphertext integrity) целостность шифртекстов
- PI – (plaintext integrity) целостность откртых текстов

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.

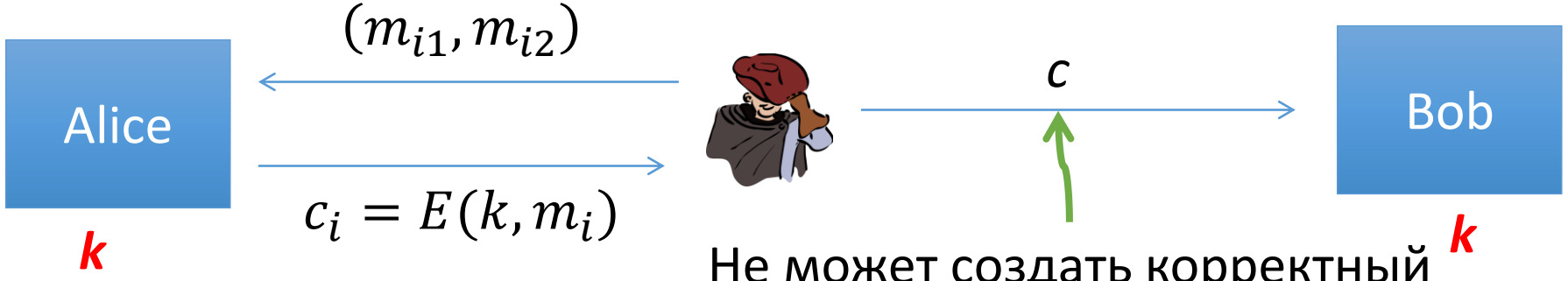
Аутентифицированное шифрование

Стойкость:

- **Стойкое шифрование, простив пассивных противников**
- **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

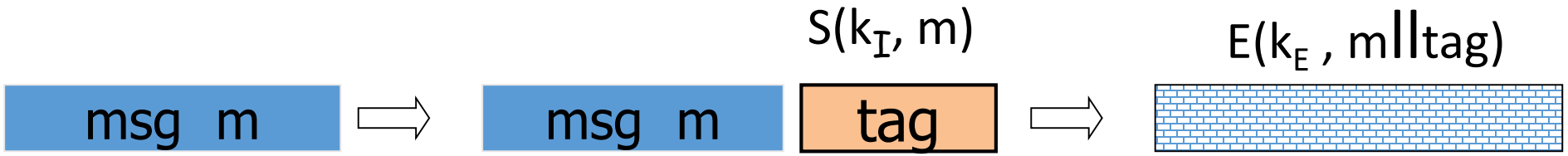
Аутентифицированное шифрование

- Использует модель стойкого шифрования + 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

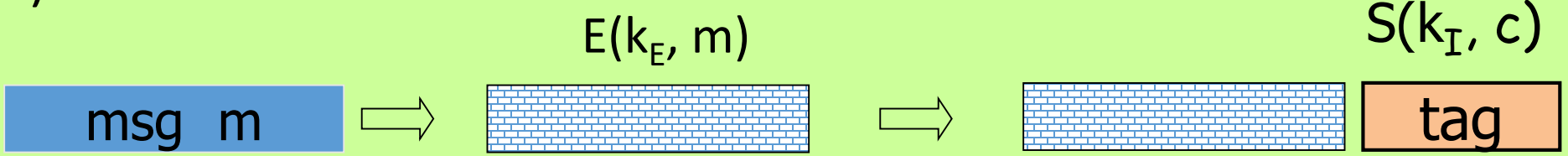
Encryption key k_E. MAC key = k_I

Option 1: (SSL)

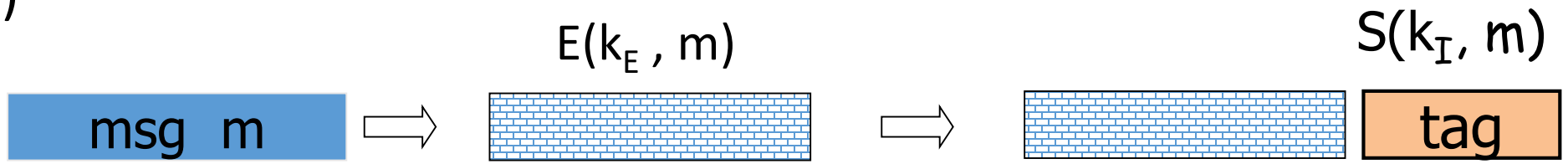


Option 2: (IPsec)

always correct



Option 3: (SSH)

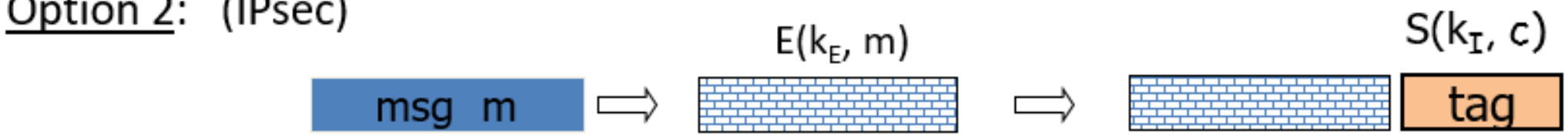


Encrypt-then-MAC

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

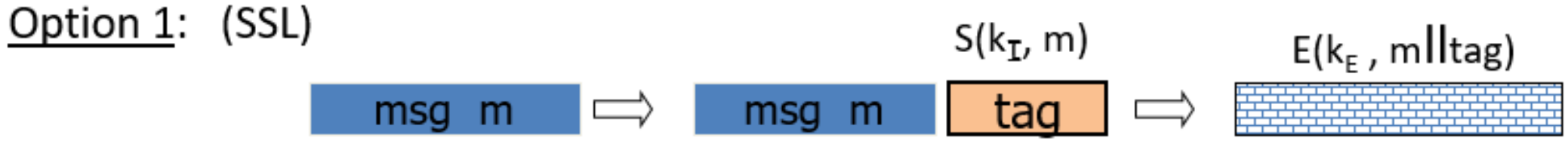
- Необходимо использование **различных, независимых ключей** для MAC и шифрования (использование одинаковых ключей может вести к реальным атакам, например при использовании CBC шифрования и CBC MAC)
- MAC должны вычисляться для **всего** шифртекста (**включая** IV)
- Проверка целостности осуществляется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

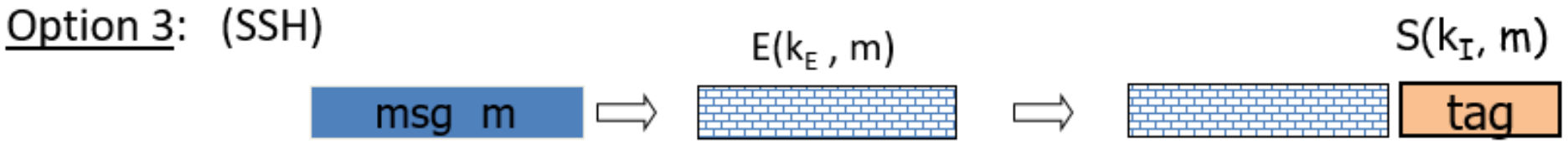
- Необходимо использование **различных, независимых ключей** для MAC и шифрования
- **Не является AE стойким в общем случае**, возможны атаки (сл. padding oracle)
- Является AE стойким для **некоторых стойких шифров** (рандомизированный CTR, CBC без дополнения сообщений).
- Проверка аутентичности происходит 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

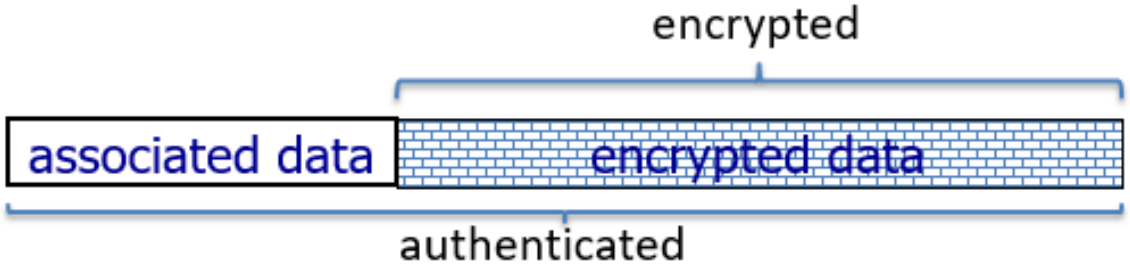
- Вообще говоря, из MAC можно восстановить часть сообщения (на стойкий MAC не накладывается требования не раскрывать биты сообщения)

Режимы аутентифицированного шифрования

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

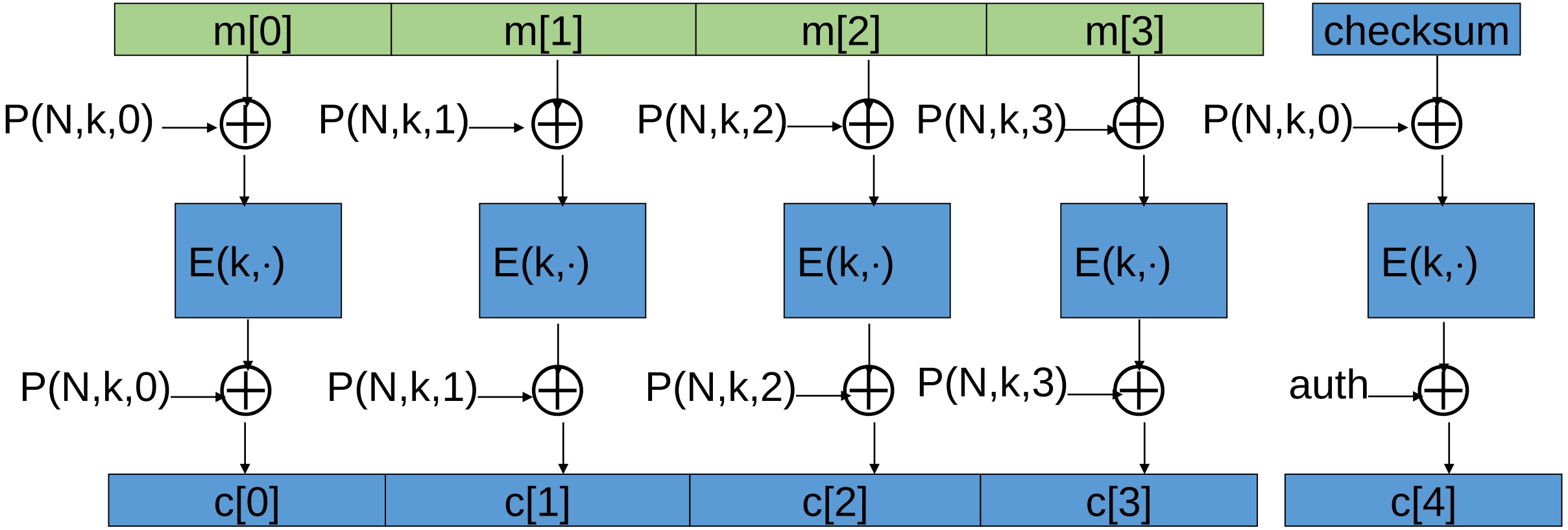
Можем – GCM, CCM, EAX, OCB

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.

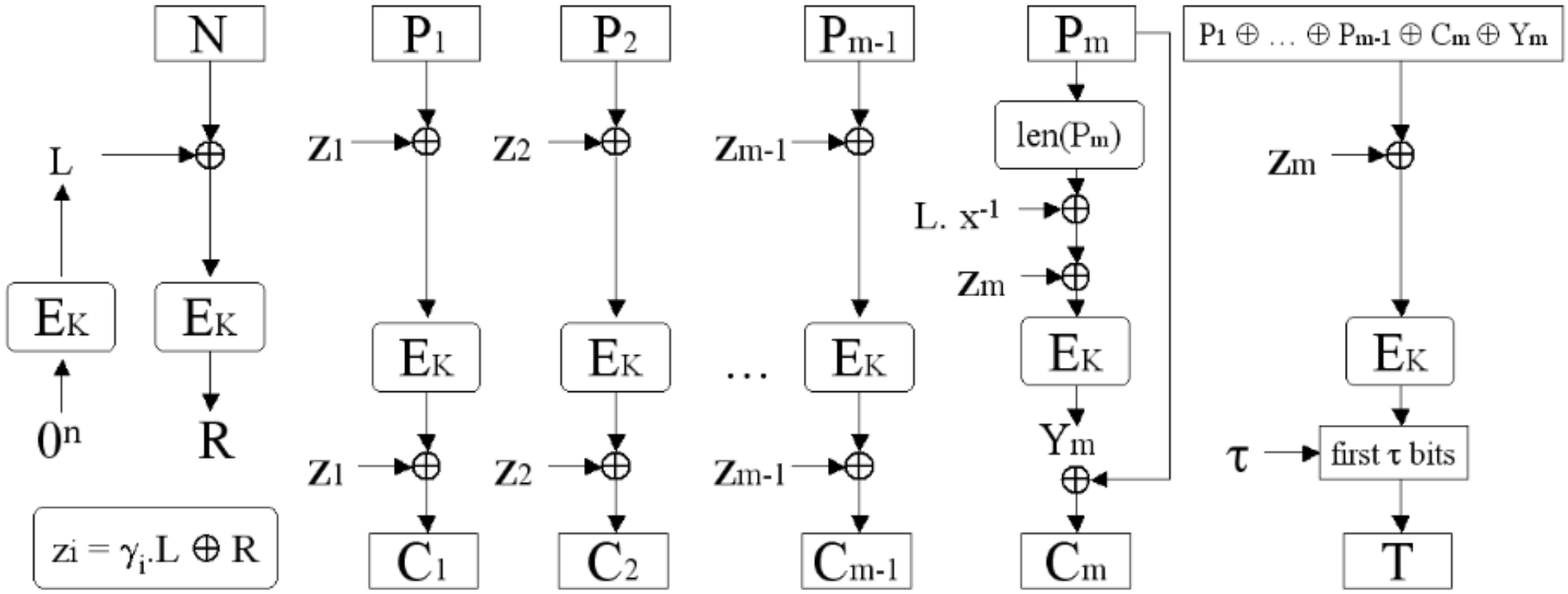


OCB

One E() op. per block.



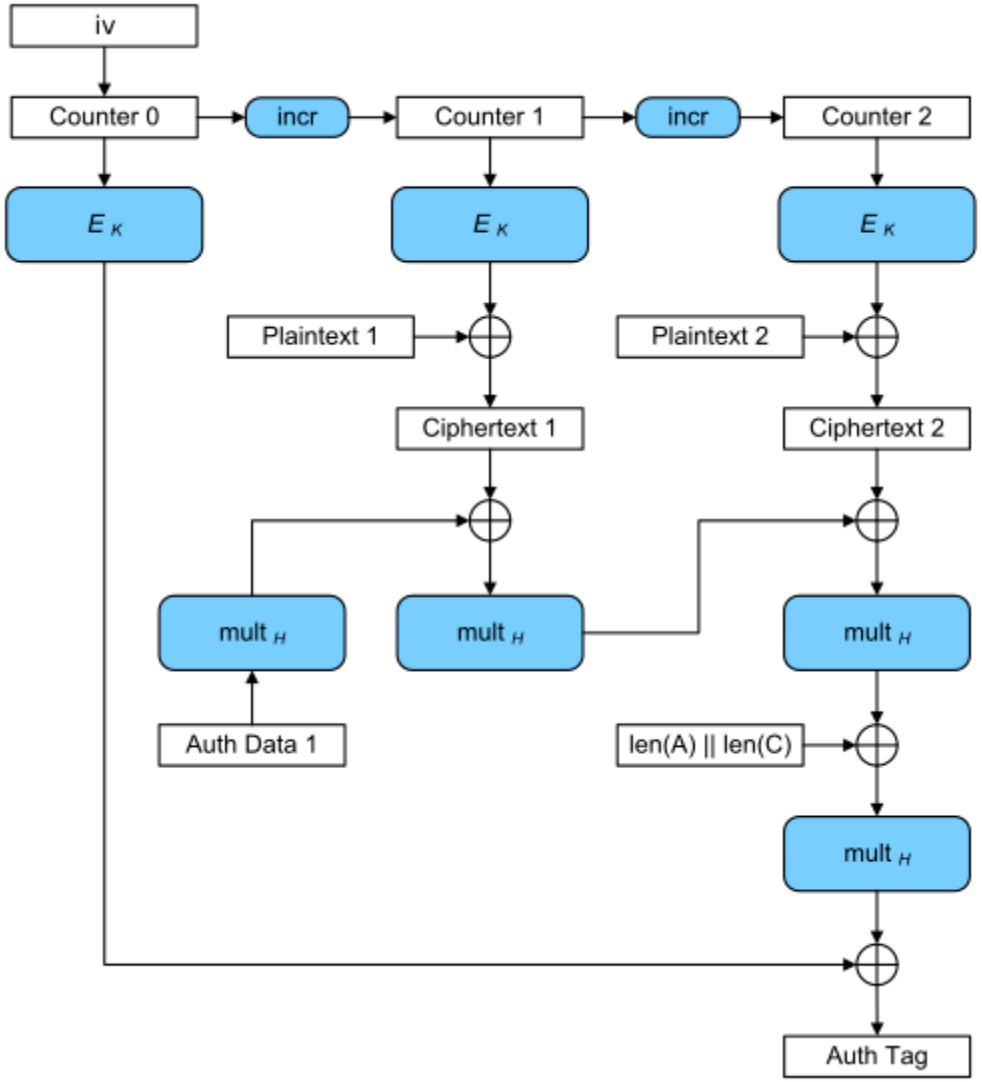
OCB



- Полностью параллелизуется
- Патентовано (спасибо Rogaway!)

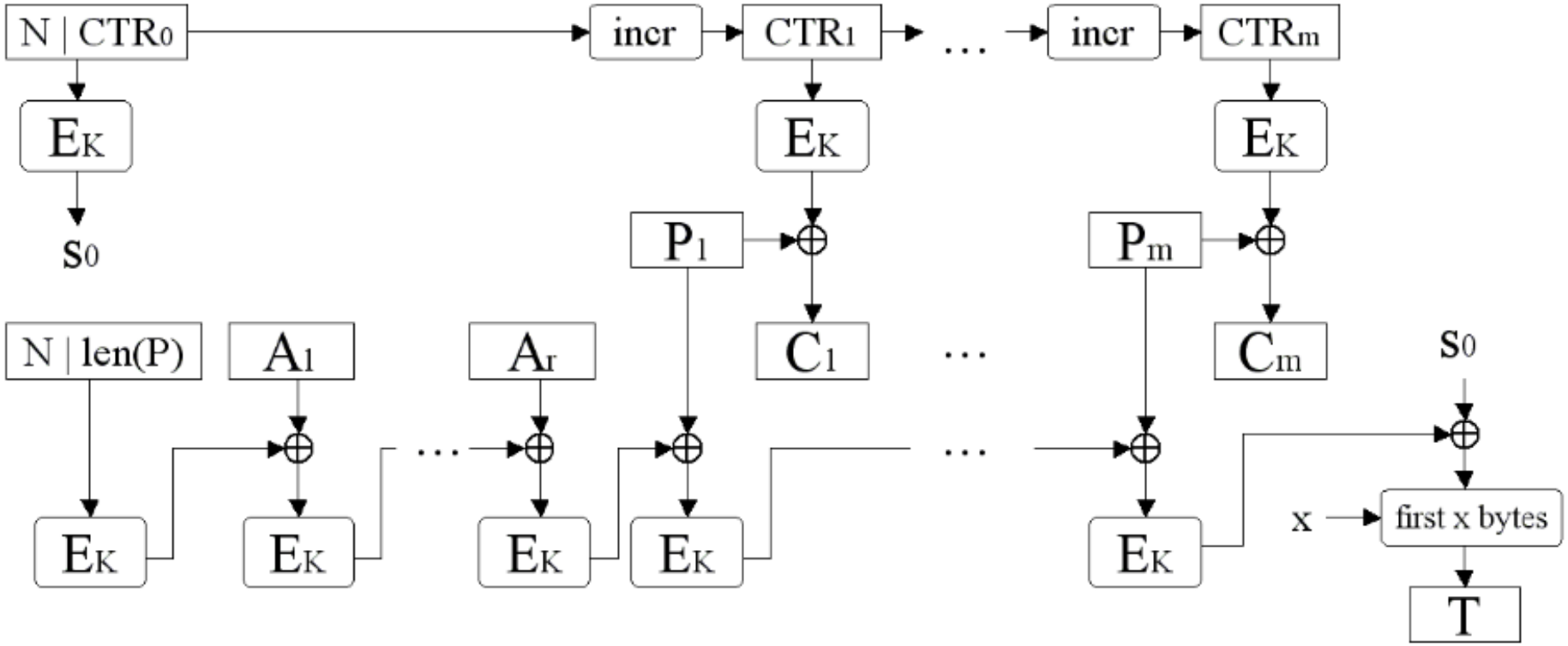
GCM

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



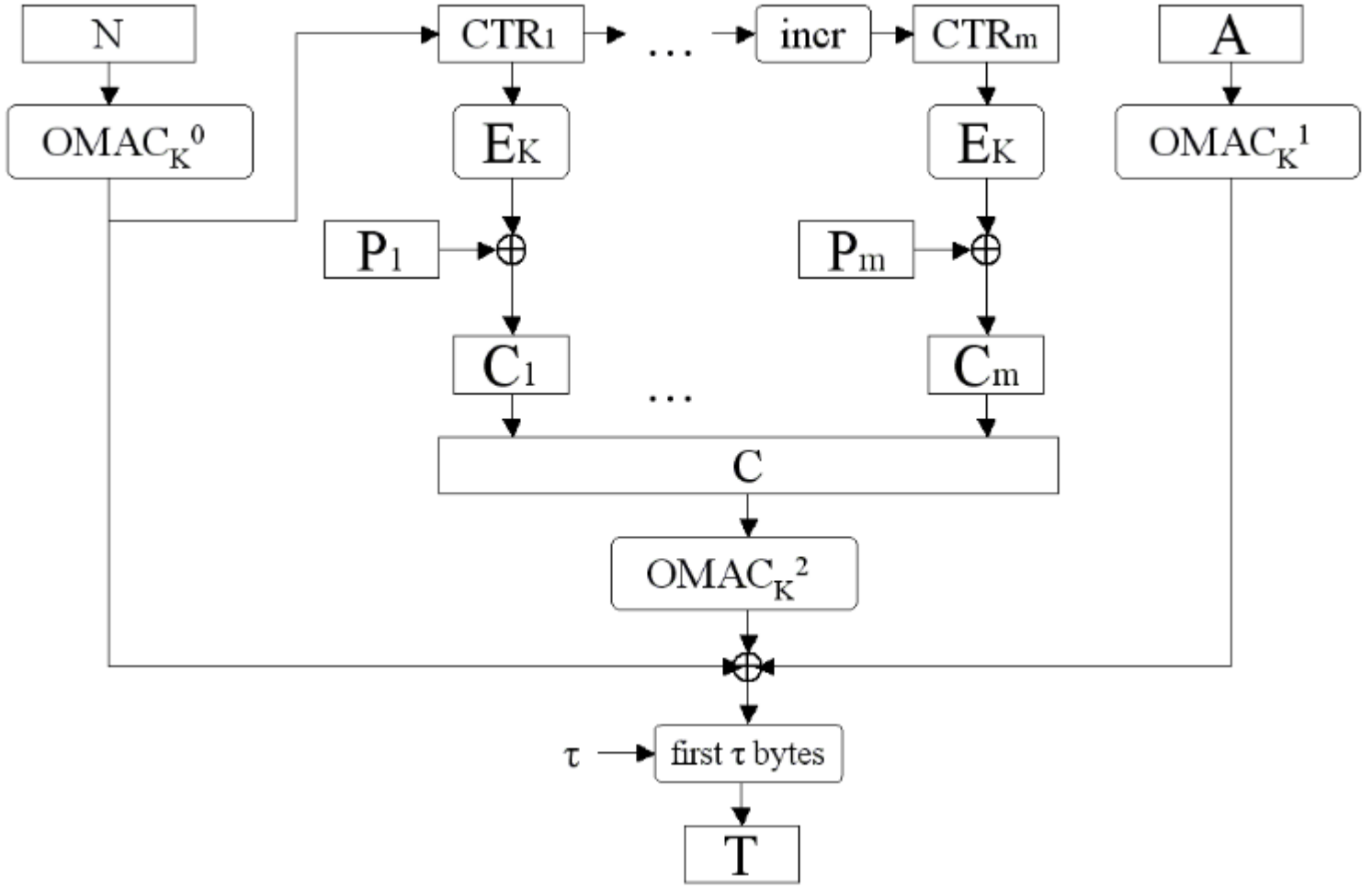
CCM

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



EAX

- Параллелизуется только шифрование
- MAC последовательный, требует вычисления PRP



Выводы

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