Криптография

Лекция 9. Защищенные сетевые соединения.

Дмитрий Яхонтов *“Кочерга”, 2018*

Сетевая модель OSI
(Open Systems Interconnect)

уровень		единица данных	что обеспечивает	примеры
L7	прикладной		взаимодействие сетевых приложений	HTTP
L6	представительский		представление и формат данных	TLS
L5	сеансовый		создание и поддержание сеанса связи	CHAP
L4	транспортный	сегмент	связь между конечными пунктами	TCP, UDP
L3	сетевой	пакет	адресацию и построение маршрута	IP
L2	канальный	кадр	связь точка–точка между устройствами	Ethernet
L1	физический	бит	среду для передачи данных	100BASE-TX

Протоколы SSL и TLS
(Secure Socket Layer / Transport Layer Security)

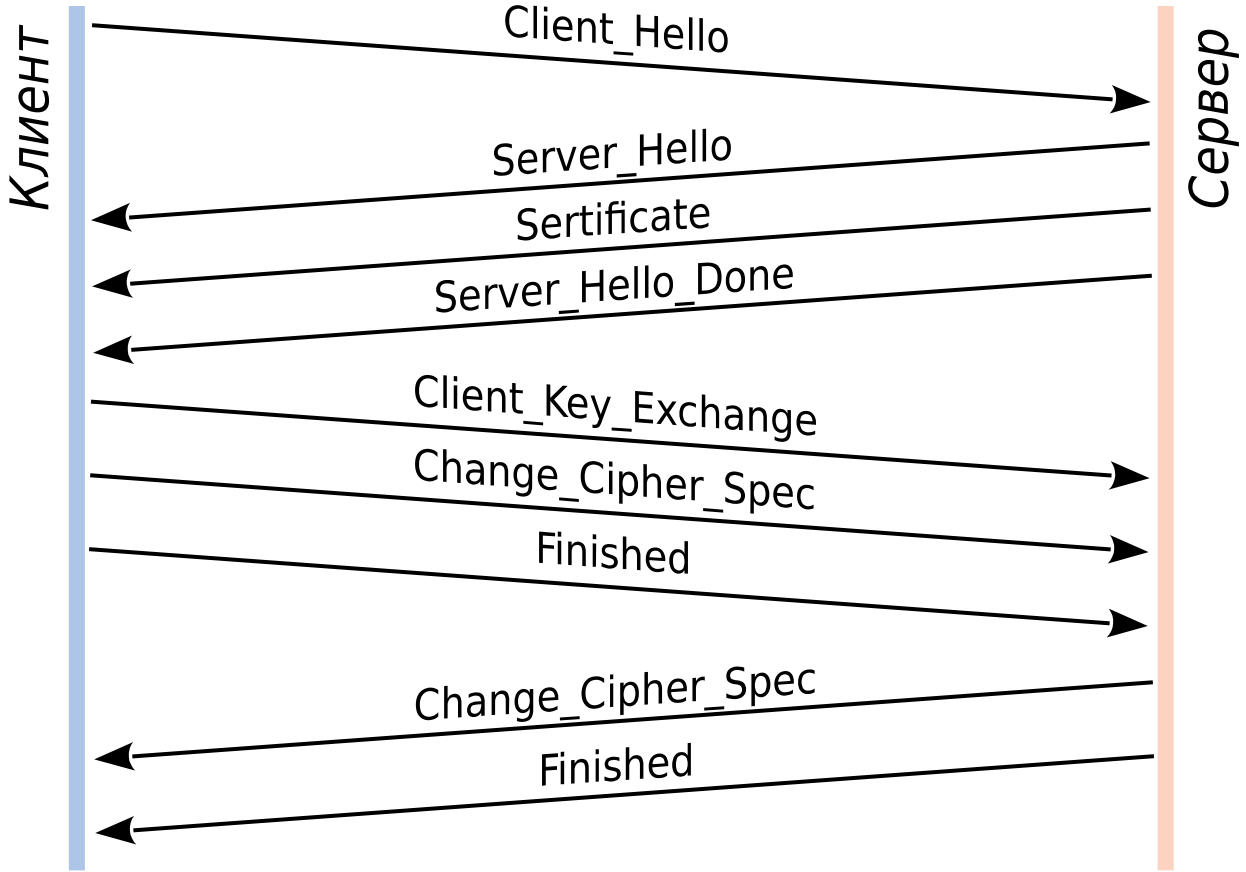
SSL/TLS — протокол представительского (L6) и сеансового (L5) уровней, который обеспечивает:

- аутентификацию
- шифрование
- контроль целостности

для произвольного прикладного (L7) протокола.

Пример: HTTPS = HTTP (L7) поверх TLS (L5+L6)

Рукопожатие TLS



Цели рукопожатия:

- договориться об алгоритмах
- провести аутентификацию сторон
- обменяться ключами шифрования

Приветствие

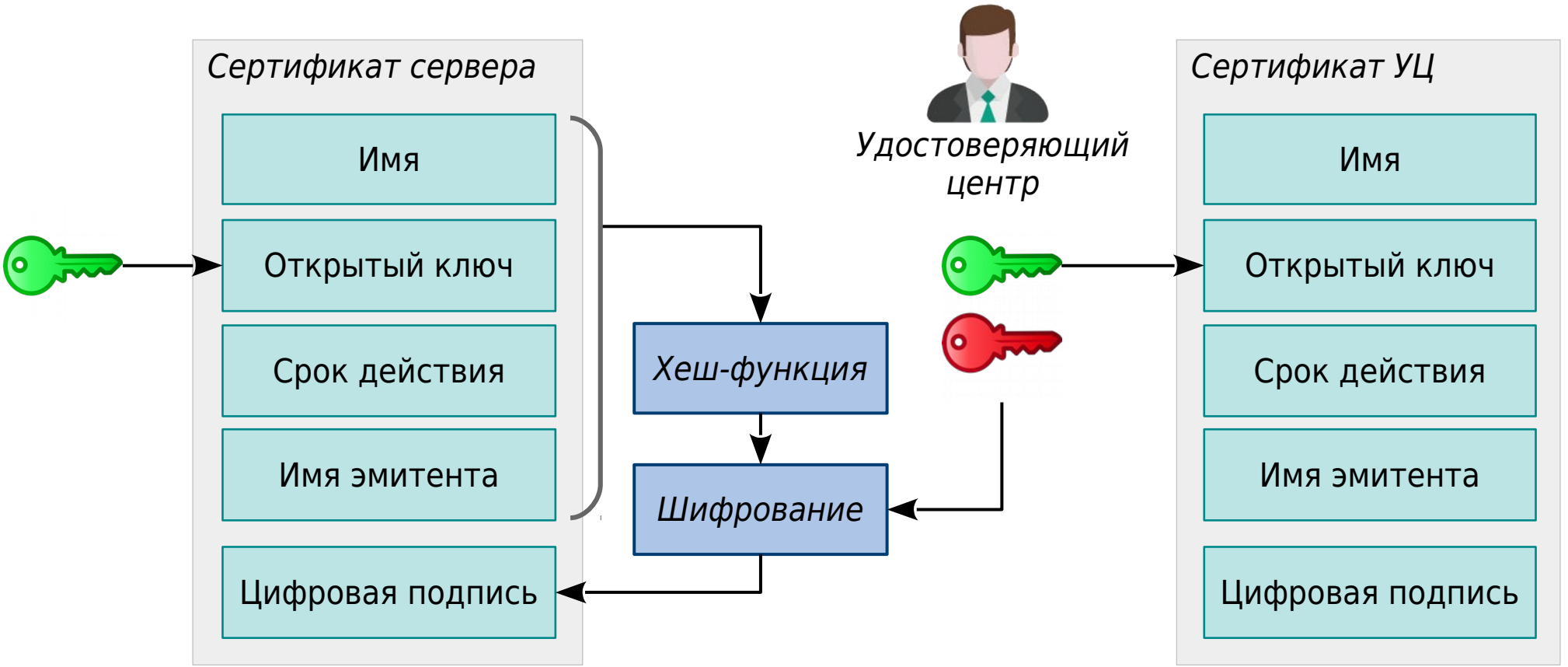
Client_Hello — приветствие клиента:

- метка времени, Unix time (количество секунд с 1 января 1970 года)
- случайное число Client Nonce
- ID сессии, если первый раз — это поле пустое
- список всех поддерживаемых алгоритмов шифрования
- имя сервера, для доступа к разным сайтам на одном IP

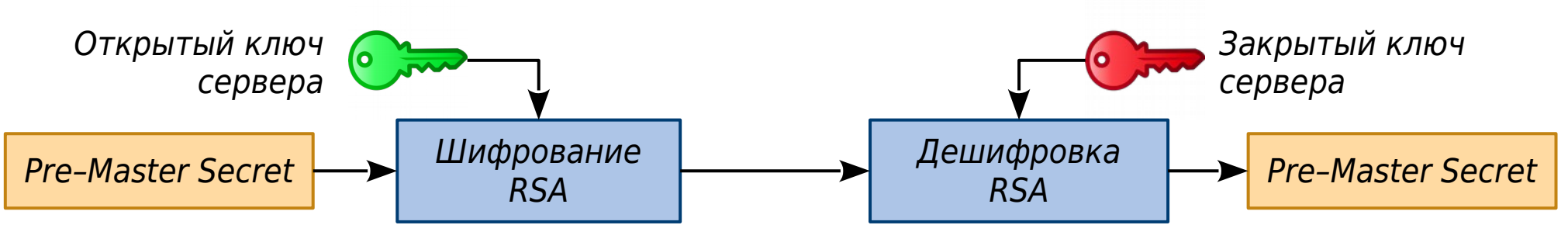
Server_Hello — приветствие сервера:

- метка времени, Unix time
- случайное число Server Nonce
- ID сессии для ускорения последующих подключений
- выбранный набор алгоритмов

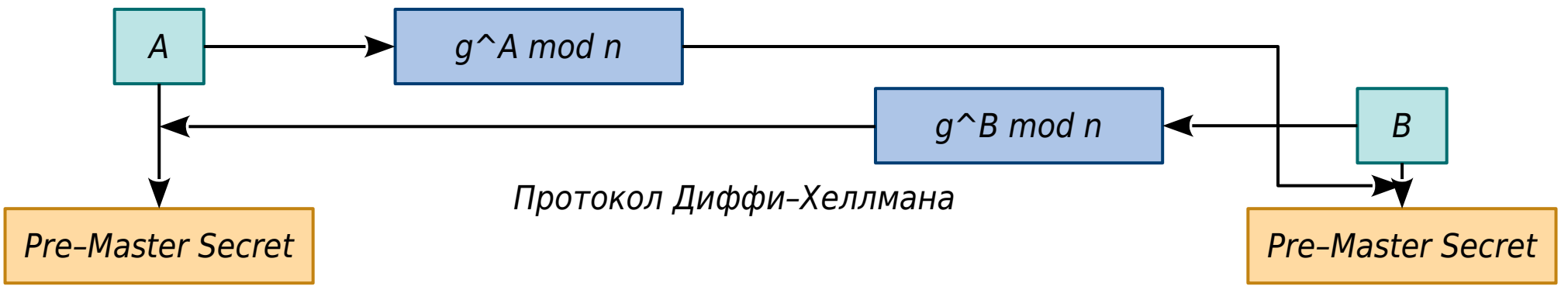
Сертификаты



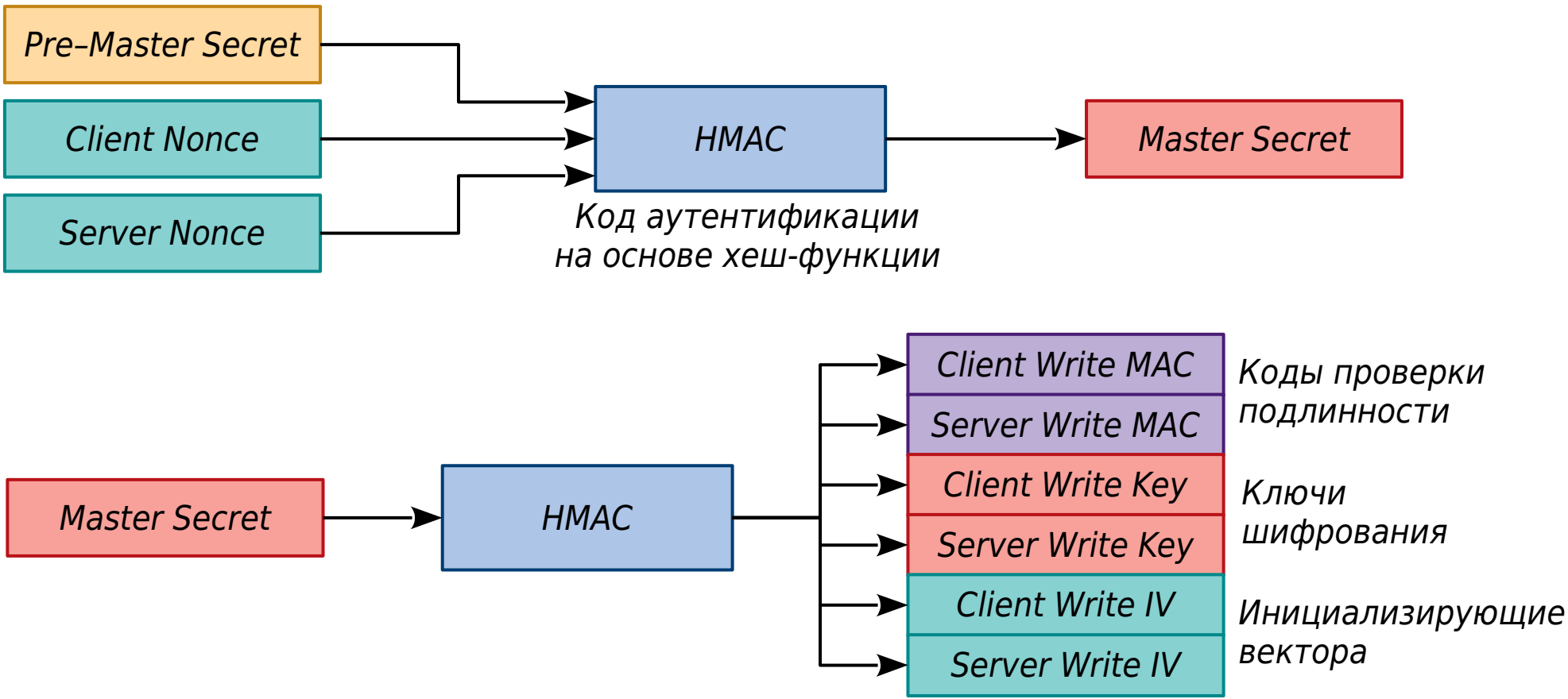
Генерация общего секрета



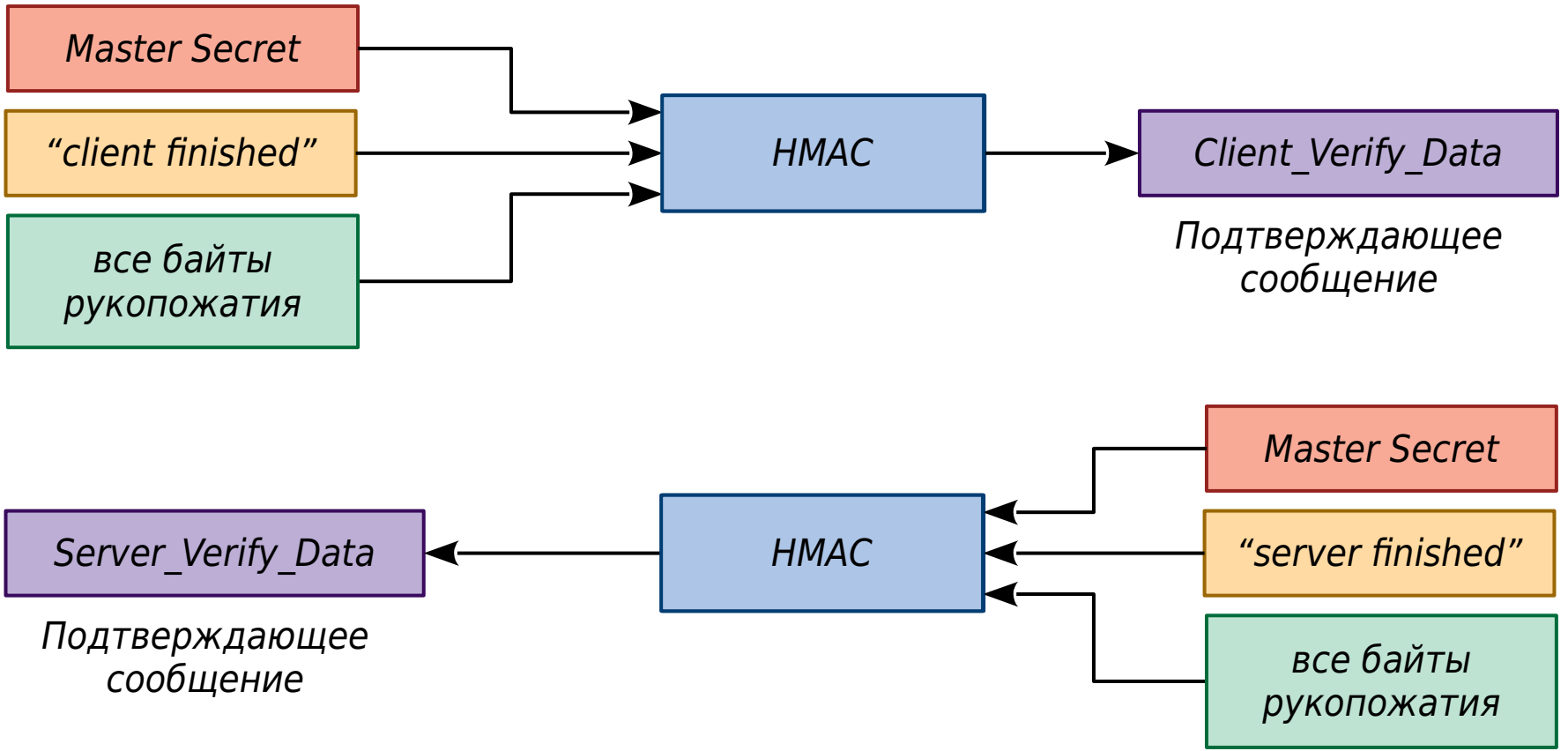
или



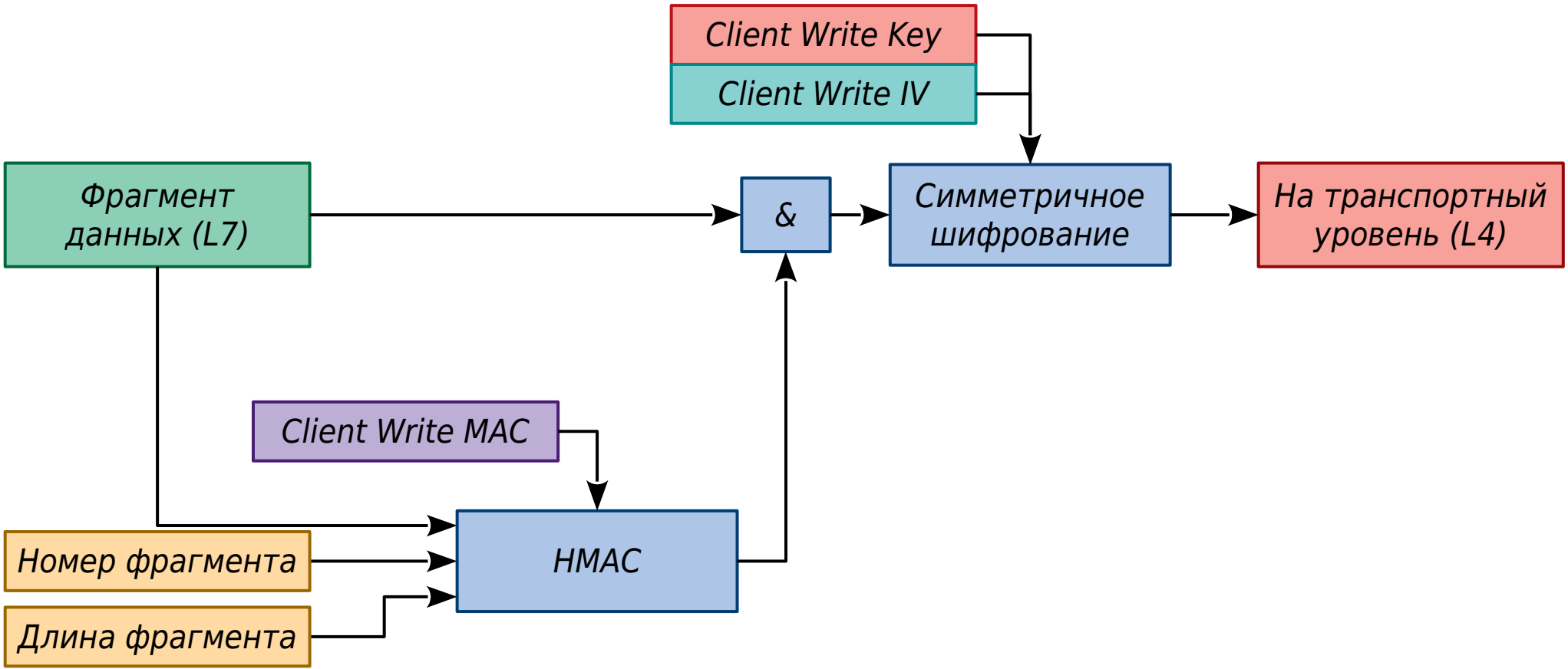
Вычисление сеансовых ключей



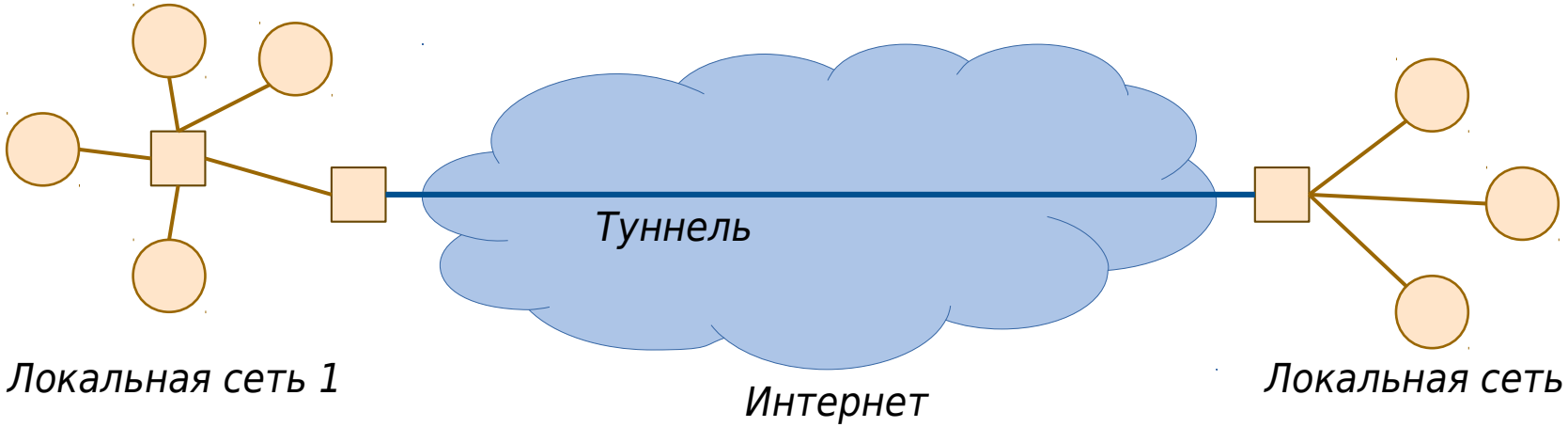
Завершение рукопожатия

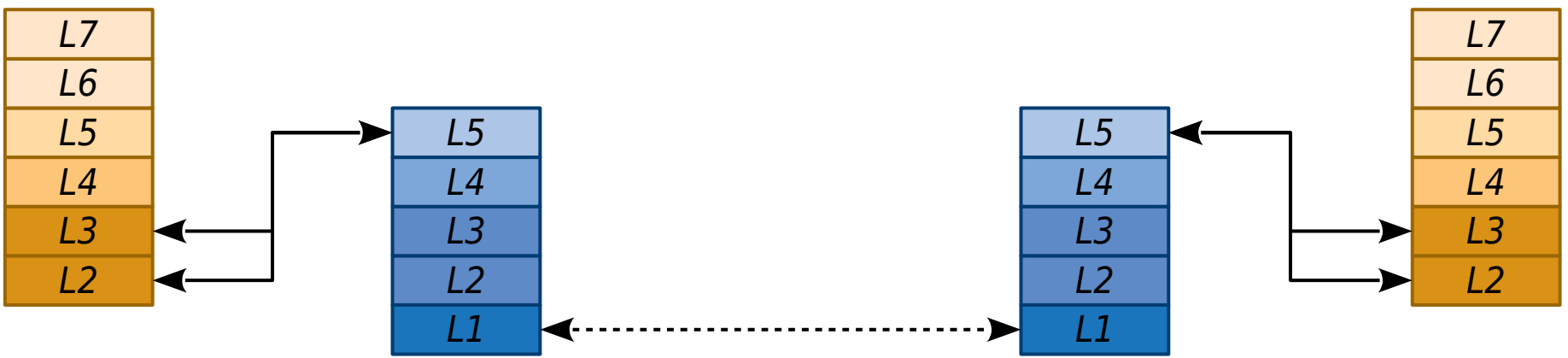


Шифрование трафика прикладного уровня



Виртуальные частные сети
(VPN — Virtual Private Network)





Реализации VPN

- **L2TP** (Level 2 Tunneling Protocol)
  туннель канального (L2) уровня поверх протокола UDP (L4)
- **PPPoE** (Point-to-Point Protocol over Ethernet)
  туннель канального (L2) уровня поверх протокола Ethernet (L2)

- **IPSec**
  туннель сетевого (L3) уровня поверх протокола IP (L3)

- **OpenVPN**
  туннель сетевого (L3) или канального (L2) уровня
  поверх протоколов TCP или UDP (L4)

- **Hamachi**
  туннель сетевого (L3) уровня поверх TCP или UDP (L4);
  для установки соединения используется внешний сервер,
  затем обмен данными идёт напрямую

Ссылки

- Обратная связь:
  - android.ruberoid@gmail.com
  - lesswrongru.slack.com @android_ruberoid
- Анонсы:
  - facebook.com/kocherga.club
  - vk.com/kocherga_club
  - vk.com/kocherga_prog
- Материалы лекций:
  - github.com/notOcelot/Kocherga_crypto
- Видео:
  - youtube.com/channel/UCeLSDFOndl4eKFutg3oowHg